

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

В НОМЕРЕ

- КОМБИНАТОРНЫЙ СПОСОБ ИДЕНТИФИКАЦИИ МАЛОЙ ВЫБОРКИ
- АЛГОРИТМ УЛУЧШЕНИЯ СОГЛАСОВАННОСТИ СТРУКТУРНОЙ ИНТЕРОПЕРАБЕЛЬНОСТИ
- УЛУЧШЕНИЕ АЛГОРИТМА ДЕЙКСТРЫ ДЛЯ ОЦЕНКИ ХАРАКТЕРИСТИК И КРИТИЧЕСКОГО ПУТИ ПРОЕКТА
- ОСОБЕННОСТИ ОБНАРУЖЕНИЯ ОШИБОК ПРИ КОНТРОЛЕ ВЫЧИСЛЕНИЙ В ЦИФРОВЫХ УСТРОЙСТВАХ ПО ПРИЗНАКУ САМОДВОЙСТВЕННОСТИ БУЛЕВЫХ ФУНКЦИЙ
- ОЦЕНКА УРОВНЯ НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ ФИЛИАЛОВ ПАО РОССЕТИ РОССИИ
- К ОЦЕНИВАНИЮ ТЕХНИЧЕСКОГО УРОВНЯ РАЗВЕДЫВАТЕЛЬНО-УДАРНЫХ И УДАРНЫХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ НА СТАДИИ ЭКСПЛУАТАЦИИ
- КОНЦЕПЦИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ В СТРУННОМ ТРАНСПОРТНОМ КОМПЛЕКСЕ
- КОНЦЕПТУАЛЬНЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ ВОДНЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ

НИИАС

Информатизация, автоматизация
и связь на железнодорожном транспорте

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПУБЛИКАЦИЙ В ЖУРНАЛЕ «НАДЕЖНОСТЬ»

■ СТРУКТУРНАЯ НАДЕЖНОСТЬ

ТЕОРИЯ И ПРАКТИКА

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

■ ФУНКЦИОНАЛЬНАЯ НАДЕЖНОСТЬ

ТЕОРИЯ И ПРАКТИКА

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

■ ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ

ТЕОРИЯ И ПРАКТИКА

- Объект, предмет и цели исследования, показатели функциональной безопасности; функции безопасности, полнота безопасности, терминология в области функциональной безопасности.
- Математические методы и модели задания требований к полноте безопасности и допустимому времени обнаружения опасного отказа, модели функциональной безопасности многоканальных и многоуровневых систем.
- Технологии обеспечения функциональной безопасности систем на всех этапах жизненного цикла.

■ ОТКАЗОУСТОЙЧИВОСТЬ СИСТЕМ

ТЕОРИЯ И ПРАКТИКА

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

- Методы активной защиты от структурных отказов и ошибок в выполнении информационных процессов, принципы и способы активной защиты, теоретические основы активной защиты, технические решения, оценки эффективности активной защиты.

■ УПРАВЛЕНИЕ РИСКАМИ

ТЕОРИЯ И ПРАКТИКА

- Постулаты и принципы безопасности. Доказательство безопасности. Методы и практические результаты ранжирования опасностей.
- Классификация рисков объектов. Принципы и методы оценивания рисков. Инструменты оценивания рисков. Методы определения допустимых уровней риска. Методология управления рисками. Управление эксплуатационными, техногенными, пожарными, профессиональными, экологическими рисками.
- Интегральные риски. Методы и модели определения интегральных рисков систем. Интегральные риски процессов. Интегральные риски услуг.

■ СЕРТИФИКАЦИЯ И СТАНДАРТИЗАЦИЯ

ТЕОРИЯ И ПРАКТИКА

- Аккредитация органов по сертификации и испытательных лабораторий – состояние проблемы в России и за рубежом. Как добиться взаимопризнания результатов испытаний в России и за рубежом? Пути сертификации программно – аппаратных комплексов по требованиям международных стандартов по функциональной безопасности.
- Обязательная и добровольная сертификации – опыт, мнения, предложения.
- Сертификация в области качества и надежности систем – требования стандартов, методики испытаний, практические результаты.
- 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

ТЕОРИЯ И ПРАКТИКА

- Применение методов искусственного интеллекта в задачах надежности и безопасности.
- Методы и модели Data Science.
- Алгоритмы прогнозирования отказов и опасных событий с помощью технологии Data Science.
- Методы проактивного управления надежностью и безопасностью.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Главный редактор:

Шубинский Игорь Борисович – доктор технических наук, профессор, эксперт Научного совета при Совете Безопасности РФ, заместитель руководителя Научно-технического комплекса АО «НИИАС» (Москва, РФ)

Заместители главного редактора:

Бочков Александр Владимирович – доктор технических наук, ученый секретарь НТС АО «НИИАС» (Москва, РФ)

Шебе Хендрик – доктор естественных наук, главный эксперт по надежности, эксплуатационной готовности, ремонтнопригодности и безопасности, TÜV Rheinland InterTraffic (Кёльн, Германия)

Ястребенецкий Михаил Анисимович – доктор технических наук, профессор, начальник отдела Национальной академии наук Украины «Государственный научно-технический центр ядерной и радиационной безопасности» (Харьков, Украина)

Технический редактор:

Новожилов Евгений Олегович – кандидат технических наук, начальник отдела АО «НИИАС» (Москва, РФ)

Председатель редакционного совета:

Розенберг Игорь Наумович – доктор технических наук, профессор, член-корреспондент РАН, заведующий кафедрой «Геодезия, геоинформатика навигация», проректор, Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет транспорта» (Москва, РФ)

Сопредседатель редакционного совета:

Махутов Николай Андреевич – доктор технических наук, профессор, член – корреспондент РАН, главный научный сотрудник Института машиноведения им. А.А. Благонравова, председатель Рабочей группы при Президенте РАН по анализу риска и проблем безопасности (Москва, РФ)

РЕДАКЦИОННЫЙ СОВЕТ

Аврамович Зоран Ж. – доктор технических наук, профессор, профессор Института транспорта Университета г. Белград (Белград, Сербия)

Алиев Вугар Амирович – доктор физико-математических наук, профессор, Генеральный директор компании AMIR Technical Services (Баку, Азербайджан)

Баранов Леонид Аврамович – доктор технических наук, профессор, заведующий кафедрой «Управления и защиты информации» Российского университета транспорта (МИИТ) (Москва, РФ)

Бочков Константин Афанасьевич – доктор технических наук, профессор, научный руководитель – заведующий НИЛ «Безопасность и ЭМС технических средств (БЭМС ТС), УО «Белорусский государственный университет транспорта» (Гомель, Республика Беларусь)

Боян Димитров – профессор, доктор математических наук, профессор теории вероятности и статистики, университет Кеттеринга, Флинт (Мичиган, США)

Вэй Куо – ректор и заслуженный профессор, профессор электротехники, компьютерного анализа данных, ядерной техники, городской университет Гонконга, Член Национальной инженерной академии США (Гонконг, Китай)

Гапанович Валентин Александрович – кандидат технических наук, президент Ассоциации «Объединение производителей железнодорожной техники» (Москва, РФ)

Каштанов Виктор Алексеевич – доктор физико-математических наук, профессор, профессор департамента прикладной математики Национального исследовательского университета «Высшая школа экономики» (Москва, РФ)

Климов Сергей Михайлович – доктор технических наук, профессор, начальник управления 4 Центрального научно-исследовательского института Министерства обороны РФ (Москва, РФ)

Кофанов Юрий Николаевич – доктор технических наук, профессор, профессор Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики» (Москва, РФ)

Кришнамурти Ачътха – доктор физико-математических наук, профессор, почетный профессор Департамента математики Университета науки и технологий (Кочин, Индия)

Лецкий Эдуард Константинович – доктор технических наук, профессор, профессор кафедры «Цифровые технологии управления транспортными процессами» Российского университета транспорта (МИИТ) (Москва, РФ)

Манджей Рам – профессор, доктор, отделение математики, вычислительной техники и технических наук, Университет Graphic Era, (Дехрадун, Индия)

Нетес Виктор Александрович – доктор технических наук, профессор ФГБОУ ВО «Московский технический университет связи и информатики» (МТУСИ) (Москва, РФ)

Папич Любиша – доктор технических наук, профессор, директор Исследовательского центра по управлению качеством и надёжностью (DQM), (Приевор, Сербия)

Поляк Роман А. – доктор физико-математических наук, профессор, приглашенный профессор Школы математических наук технологического Университета Технион (Хайфа, Израиль)

Рыков Владимир Васильевич – доктор физико-математических наук, профессор, профессор кафедры Прикладной математики и компьютерного моделирования РГУ нефти и газа (НИУ) имени И.М. Губкина, профессор кафедры Теории вероятностей и кибербезопасности РУДН (Москва, РФ)

Соколов Борис Владимирович – доктор технических наук, профессор, заместитель директора по научной работе Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИ-РАН), (Санкт-Петербург, РФ)

Тимашев Святослав Анатольевич – доктор технических наук, профессор, научный руководитель и главный научный сотрудник НИЦ «Надежность и безопасность больших систем и машин» Уральского Отделения РАН РФ (Екатеринбург, РФ)

Уткин Лев Владимирович – доктор технических наук, профессор Института компьютерных наук и технологий Санкт-Петербургского политехнического университета Петра Первого (Санкт-Петербург, РФ)

Юркевич Евгений Викторович – доктор технических наук, профессор, Главный научный сотрудник лаборатории Технической диагностики и отказоустойчивости ИПУ РАН. (Москва, РФ)

УЧРЕДИТЕЛИ ЖУРНАЛА:

АО «НИИАС», ОПЖТ,
Шубинский И.Б.

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

Издатель журнала

ООО «Журнал «Надежность»

Генеральный директор

Дубровская А.З.

Адрес: 109029, г. Москва,
ул. Нижегородская, д. 27, стр. 1, оф. 209

ООО «Журнал «Надежность»

www.dependability.ru

Отпечатано в ООО «Отмара. нет». 107140,

г. Москва, ул. Русаковская, д. 13, стр. 5,

2 этаж, пом. III/6-7

Подписано в печать 15.05.2024

Объем 92, Тираж 500 экз, Заказ № 19620

Формат 60х90/8, Бумага глянец

Журнал издается ежеквартально с 2001 года,
стоимость одного экземпляра 1045 руб.,
годовой подписки 4180 руб.,
телефон редакции 8 (495) 967-77-05,
e-mail: dependability@bk.ru

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 надёжность
- Функциональная надёжность
- Отказоустойчивость
- Функциональная безопасность
- Системный анализ в задачах надёжности и безопасности
- Управление рисками
- Живучесть
- Техническая эффективность автоматизированных систем управления
- Управление активами
- Обработка больших данных. Системы управления и искусственный интеллект
- Интеллектуальные транспортные системы
- Методы и системы защиты информации. Информационная безопасность
- Дискуссия по терминологии надёжности, отказоустойчивости, безопасности, рисков и живучести
- Стандартизация и сертификация
- 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 «Надёжность» входит в категорию К2 перечня рецензируемых научных изданий ВАК (строка 1483), утвержденного информационным письмом Высшей аттестационной комиссии при Минобрнауки России от 6 декабря 2022 № 02-1198 «О категорировании Перечня рецензируемых научных изданий».

СОДЕРЖАНИЕ

Системный анализ в задачах надёжности и безопасности

Воловик А.В. Комбинаторный способ идентификации малой выборки 3

Дулин С.К., Рябцев А.Б. Алгоритм улучшения согласованности структурной интероперабельности 8

Ширипурапу А., Шанкар Наупада Р., Шриниваса Рао К. Улучшение алгоритма Дейкстры для оценки характеристик и критического пути проекта 16

Структурная надёжность. Теория и практика

Ефанов Д.В., Погодина Т.С. Особенности обнаружения ошибок при контроле вычислений в цифровых устройствах по признаку самодвойственности булевых функций 24

Наумов И.В., Подъячих С.В., Полковская М.Н., Шеръязов С.К., Бастрон А.В. Оценка уровня надёжности функционирования филиалов ПАО Россети России 38

Интеллектуальные системы управления

Микони С.В. Семенов С.С. К оцениванию технического уровня разведывательно-ударных и ударных беспилотных летательных аппаратов на стадии эксплуатации 52

Функциональная безопасность систем управления

Юницкий А.Э., Гарах В.А., Литвинович Т.С., Шевченко Д.Н. Концепция безопасности движения в струнном транспортном комплексе 61

Защита информации

Михалевич И.Ф. Концептуальные проблемы безопасности водных интеллектуальных транспортных систем 72

Гнеденко – Форум 88

Комбинаторный способ идентификации малой выборки

A combinatorial method of small sample identification

Воловик А.В.
Volovik A.V.

АО «ОДК-Климов», Российская Федерация, Санкт-Петербург
JSC Klimov, Russian Federation, Saint Petersburg

volovik_aleksandr@mail.ru



Воловик А.В.

Резюме. Цель. Для повышения достоверности принимаемых решений о равномерности распределений по выборкам ограниченного объема разработан комбинаторный метод формирования критерия на основе сочетаний без повторений выборочных значений. **Методы.** В статье применяются методы теории вероятностей, математической статистики и комбинаторики. **Результаты.** Предложенный критерий обладает высокой эффективностью для различения выборок малого объема при проверке статистически близких гипотез, таких как гипотеза о равномерном законе распределения и гипотеза о бета-распределении 1-го рода. **Выводы.** Предлагаемый в статье подход позволяет реализовать процедуру последовательного анализа (обнаружение «разладки» процесса). Такая процедура дает возможность достоверно выявлять «разладку» (отклонение распределения наблюдений от равномерного закона) процесса с достаточной для практики интенсивностью при помощи рекуррентных соотношений.

Abstract. Aim. For the purpose of improving the reliability of decisions regarding the uniformity of distributions over samples of limited size, a combinatorial method has been developed for defining a criterion based on simple combinations of sample values. **Methods.** The paper uses methods of the probability theory, mathematical statistics, and combinatorics. **Results.** The proposed criterion is highly efficient for distinguishing small samples when testing statistically similar hypotheses, such as the hypothesis of a uniform distribution law and the hypothesis of a beta distribution of the first kind. **Conclusions.** The approach proposed in the paper enables a sequential analysis procedure (detection of process “imbalance”). This procedure makes it possible to reliably detect the “imbalance” (deviation of the distribution of observations from the uniform law) of a process with a practically sufficient intensity using recurrent relations.

Ключевые слова: малая выборка, вариационный ряд, плотность распределения, статистика, гипотеза, достигаемый уровень значимости, последовательный анализ.

Keywords: small sample, static series, distribution density, statistics, hypothesis, achieved significance value, sequential analysis.

Для цитирования: Воловик А.В. Комбинаторный способ идентификации малой выборки // Надежность. 2024. №2. С. 3-7. <https://doi.org/10.21683/1729-2646-2024-24-2-3-7>

For citation: Volovik A.V. A combinatorial method of small sample identification. Dependability 2024;2:3-7. <https://doi.org/10.21683/1729-2646-2024-24-2-3-7>

Поступила: 05.10.2023 / **После доработки:** 05.04.2024 / **К печати:** 10.06.2024
Received on: 05.10.2023 / **Revised on:** 05.04.2024 / **For printing:** 10.06.2024

Введение

Роль равномерного распределения вероятностей в задачах разработки стохастических моделей трудно переоценить. Используя вероятностное интегральное преобразование [1], к равномерному закону можно свести любое распределение вероятностей. В этом пространстве некоторые задачи могут быть решены наиболее эффективно, что предопределяет необходимость обоснования исходного допущения о равномерности с требуемой достоверностью.

Сложность решения задач идентификации равномерного распределения в условиях выборок малого объема обусловлена тем обстоятельством, что искомое решение часто в сильной степени зависит от объема выборки и не всегда является достаточно эффективным.

Одним из способов повышения достоверности принимаемых статистических решений по выборкам ограниченного объема может служить комбинаторный метод формирования критерия [2]. Его суть заключается в разработке статистики, которая объединяет комбинации частных решений, получаемых

на основе описанного в [3] вариационного критерия равномерности.

Метод

Для позиционирования предложенного в [3] вариационного критерия равномерности среди существующих и достаточно изученных критериев отклонения распределения от равномерного закона [4] целесообразно исследовать его мощность для случая проверки гипотезы H_0 о равномерном распределении случайной величины X на интервале $[0;1]$ при альтернативной гипотезе H_1 о бета-распределении [4, 5] с плотностью

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

где $B(\lambda, \mu)$ – бета-функция;

λ, μ – параметры распределения.

Бета-распределение (1) с параметрами $\lambda = 1$ и $\mu = 1$ вырождается в равномерное на интервале $[0;1]$. Для альтернативной гипотезы H_1 рассмотрим параметры [4] $\lambda = 1,5$ и $\mu = 1,5$.

Получить аналитическое выражение распределения вариационного критерия [3] для выборки минимального объема $n = 2$

$$v = \frac{x_{(1)}}{x_{(2)}}, \quad (2)$$

где $x_{(1)} \leq x_{(2)}$, представляется возможным только при параметрах $\lambda = 1$ и $\mu = 1$ (равномерный закон [6]). Для альтернативной гипотезы H_1 с параметрами $\lambda = 1,5$ и $\mu = 1,5$ решение возможно получить численным способом. На рис. 1 приведены графики плотности $g_v(v)$ критерия (2) для рассматриваемых гипотез.

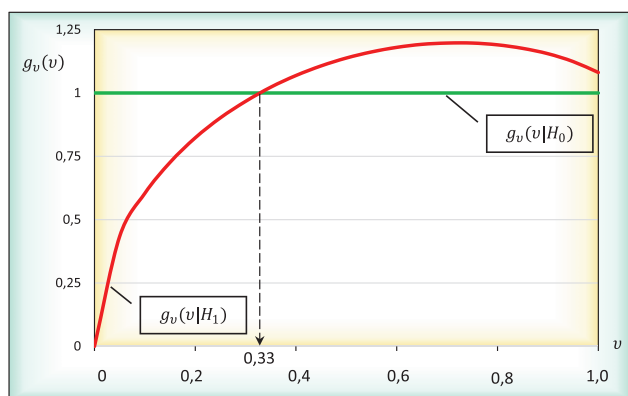


Рис. 1. Плотности распределений $g_v(v)$ для гипотез H_0 и H_1

Из рис. 1 видно, что для критерия v целесообразно выбрать правостороннюю критическую область. Численным решением было установлено, что вероятность отклонения гипотезы H_1 превышает вероятность отклонения гипотезы H_0 при значении $v \geq 0,33$. Это значение можно считать наиболее эффективным ($\max(1 - \beta - \alpha)$, где α и β – ошибки первого и второго рода соответственно) значением критерия $v_0 = 0,33$. Это такое теоретически достигаемое значение критерия, для которого [4, 9]: достигаемый уровень значимости

$$p_{H_0} = \int_{v_0}^1 g_v(v | H_0) dv; \quad (3)$$

достигаемая мощность

$$p_{H_1} = \int_{v_0}^1 g_v(v | H_1) dv. \quad (4)$$

Заметим, что v_0 совпадает с абсциссой пересечения функций плотностей на рис. 1, что свидетельствует о верности расчетов.

Результаты исследования теоретической достигаемой мощности вариационного критерия для выборок объемом $n = 2 \dots 5$ приведены в табл. 1. Там же приведены результаты имитационного моделирования при числе испытаний 10^6 .

Анализ табл. 1 показывает, что независимо от объема выборки n результаты различаются не более чем на 0,01–0,03. При этом мощность критерия с увеличением объема выборки практически не растет, что подтверждено имитационными экспериментами. Данный факт можно объяснить уменьшением энтропии двух наименьших порядковых статистик относительно энтропии всей анализируемой выборки при увеличении ее объема. Тем не менее, теоретически критерий уверенно ($p_{H_1} > 0,7$ и $p_{H_0} \gg \alpha = 0,1$) различает достаточно близкие гипотезы H_0 и H_1 даже для выборок минимального объема.

На рис. 2 приведены графики функций распределения статистики v критерия при проверке гипотез H_0 и H_1 .

На рисунке наглядно представлена разность между достигаемыми уровнями значимости и мощности при проверке гипотез H_0 и H_1 . Для выборок объемом $n > 2$ это позволяет воспользоваться элементами комбинаторики, т.к. количество k подвыборок объемом $m = 2$ с возвращением из исходной выборки больше, чем n .

Пусть имеется выборка объемом n наблюдений случайной величины X из генеральной совокупности с

Табл. 1. Результаты исследования мощности вариационного критерия

Характеристики		n	2	3	4	5
Наиболее эффективное значение критерия		$v_{кр}$	0,33	0,36	0,33	0,36
Достигаемый уровень значимости, рассчитанный	аналитически	p_{H_0}	0,67	0,64	0,67	0,64
	имитацией	$\hat{p}_{H_0}$	0,65	0,64	0,64	0,65
Достигаемая мощность критерия, рассчитанная	аналитически	p_{H_1}	0,77	0,75	0,77	0,75
	имитацией	$\hat{p}_{H_1}$	0,74	0,76	0,76	0,77

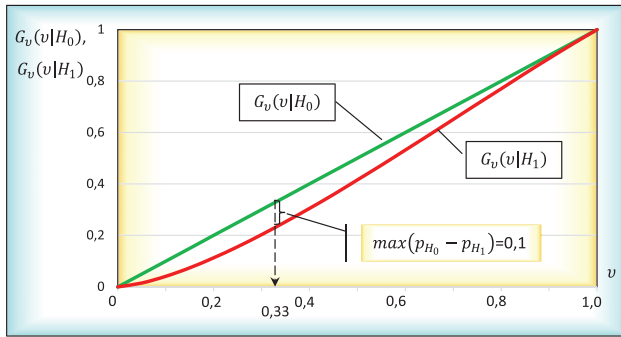


Рисунок 2 – Графики функций распределения статистики v критерия при проверке гипотез H_0 и H_1

равномерным в интервале $[0; 1]$ законом распределения (свойство Ψ). Наибольшее число вариантов подвыборок из нее возможно получить путем сочетаний наблюдений по 2. Тогда из этой выборки последовательно извлекаются с возвращением выборки объемом $m = 2$, из элементов которых формируются порядковые статистики $x_{(1)} \leq x_{(2)}$ (вариационный ряд [7]). Из них создаются вариационные критерии аналогично (2)

$$v_i = \frac{x_{(1)}}{x_{(2)}}, \quad i = 1, 2, \dots, k, \quad (5)$$

распределения которых в интервале $[0; 1]$ также равномерны [3] (обладают свойством Ψ). Количество k таких критериев равно числу сочетаний без повторений [5]

$$k = C_n^2 = \frac{n!}{(n-2)!2!}. \quad (6)$$

Возможность использования совокупности критериев обусловлена низким уровнем их коррелированности для сочетаний без повторений по два наблюдения, взятых из выборки объемом n [8]. Так, для выборок объемом до $n = 10$ $\max \text{corr} \approx 0,43$. Поэтому предлагается комбинаторный критерий, для которого достигнутый уровень значимости [4] свидетельствует против проверяемой гипотезы. Причем, аргументом у него является количество k подвыборок.

Критерии (5) сравниваются с критическим значением $v_{кр}$, на основании чего делается вывод о наступлении одного из двух событий:

- i -тая подвыборка также распределена равномерно в интервале $[0; 1]$ (обладает свойством Ψ), если $v_i \leq v_o$;
- оснований считать i -тую подвыборку распределенной равномерно в интервале $[0; 1]$ недостаточно (не обладает свойством Ψ), если $v_i > v_o$.

Общее число подвыборок, обладающих свойством Ψ в выборке объема n , описывается биномиальным законом распределения [5].

По результатам тестирования подвыборок с помощью критериев v_i решение принимается в соответствии с правилом: *проверяемая H_0 или альтернативная H_1 гипотезы отклоняются, если эти гипотезы отклоняются при проверке хотя бы одной подвыборки, составленной из исходной выборки путем сочетаний по два наблюдения без повторений.*

Для комбинаторного критерия оценками эффективности будут также достигаемые уровни значимости и мощности. Тогда, в соответствии с приведенным выше правилом, достигаемый уровень значимости при проверке k подвыборок

$$p_{H_0}^* = 1 - (1 - p_{H_0})^k. \quad (7)$$

Аналогично достигаемая мощность критерия по k подвыборкам

$$p_{H_1}^* = 1 - (1 - p_{H_1})^k. \quad (8)$$

В табл. 2 приведены расчетные значения достигаемых уровней значимости (7) для гипотезы H_0 и мощности (8) для гипотезы H_1 критерия для выборок различного объема n .

Табл. 2. Расчетные достигаемые уровни значимости и мощности

n	2	3	4	5
k	1	3	6	10
$p_{H_0}^*$	0,670	0,964	0,999	1,000
$p_{H_1}^*$	0,770	0,988	1,000	1,000

В результате имитационного моделирования процедуры проверки гипотез H_0 и H_1 с помощью предлагаемого критерия получены оценки достигнутых уровней значимости $\hat{p}_{H_0}^*$ и мощности $\hat{p}_{H_1}^*$, приведенные в табл. 3.

Табл. 3. Оценки достигнутых уровней значимости и мощности

n	2	3	4	5
k	1	3	6	10
$\hat{p}_{H_0}^*$	0,669	0,953	0,999	1,000
$\hat{p}_{H_1}^*$	0,767	0,981	1,000	1,000

Анализ табл. 2 и 3 свидетельствует о практическом соответствии оценок, полученных в результате имитации, и рассчитанных теоретически достигнутых уровней значимости и мощности критерия.

На рис. 3 приведены диаграммы достигаемых уровней значимости и мощности.

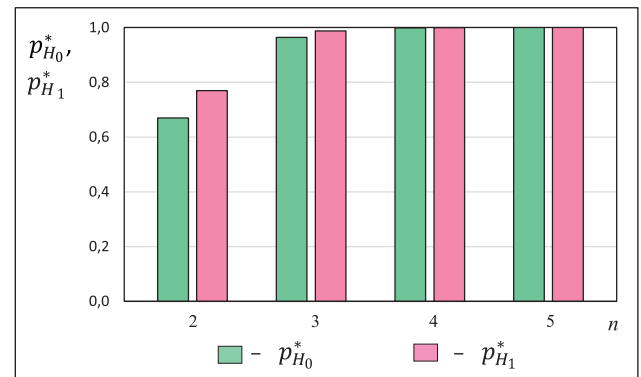


Рис. 3. Диаграммы достигаемых уровней значимости и мощности

Из рис. 3 наглядно видна их быстрая сходимость к 1 при увеличении объема исследуемой выборки до $n = 4$. Причем, при $n > 3$ достигаемые уровни значимости и мощности практически равны 1, что свидетельствует о высокой эффективности критерия для идентификации особо малых выборок.

Результат

Для демонстрации методики применения предлагаемого критерия рассмотрим задачу проверки выборки объемом $n = 3$ из генеральной совокупности с равномерным распределением в интервале $[0; 1]$ на равномерность (гипотеза H_0).

Пусть в результате наблюдений получена выборка

$$x = \{0,02; 0,079; 0,106\}. \quad (9)$$

Количество подвыборок $k = 3$ объемом $m = 2$. Матрица подвыборок примет вид

$$\begin{bmatrix} 0,02 & 0,079 \\ 0,02 & 0,106 \\ 0,079 & 0,106 \end{bmatrix}. \quad (10)$$

Вектор значений вариационных критериев (5)

$$v = [0,255 \quad 0,191 \quad 0,749]. \quad (11)$$

Для равномерного закона распределения $F(v_i) = v_i$, поэтому оценка достигнутого уровня значимости (7)

$$p_{H_0}^* = 1 - \prod_{i=1}^3 (1 - v_i) = 0,85. \quad (12)$$

Достигнутый уровень значимости (12) намного больше используемого обычно уровня $\alpha = 0,1$. Поэтому отклонить гипотезу H_0 оснований недостаточно.

Пусть теперь дана выборка такого же объема $n = 3$

$$y = \{0,584; 0,039; 0,766\} \quad (13)$$

из генеральной совокупности с бета-распределением (гипотеза H_1) с параметрами $\lambda = 1,5$ и $\mu = 1,5$. Матрица подвыборок примет вид

$$\begin{bmatrix} 0,584 & 0,039 \\ 0,584 & 0,766 \\ 0,039 & 0,766 \end{bmatrix}. \quad (14)$$

Вектор значений вариационных критериев (5)

$$v = [0,067 \quad 0,762 \quad 0,051]. \quad (15)$$

Оценка достигнутого уровня значимости (7)

$$p_{H_1}^* = 1 - \prod_{i=1}^3 (1 - v_i) = 0,79. \quad (16)$$

Заметим, что оценка достигнутого уровня значимости (16) при проверке гипотезы H_1 ниже аналогичной оценки (12) при проверке гипотезы H_0 . Это свидетельствует о том, что критерий позволяет достаточно уверенно $p_{H_0}^* - p_{H_1}^* = 0,85 - 0,79 = 0,06$ различить статистически близкие гипотезы H_0 и H_1 .

Комбинаторный критерий целесообразно использовать и при реализации последовательного анализа. В этом случае исходная выборка в общем виде запишется следующим образом

$$x = \{x_1; x_2; \dots; x_n\}. \quad (17)$$

Матрица подвыборок будет формироваться по следующей рекуррентной схеме

$$[x_1 \ x_2] + x_3 \rightarrow \begin{bmatrix} x_1 & x_2 \\ x_1 & x_3 \\ x_2 & x_3 \end{bmatrix} + x_4 \rightarrow \begin{bmatrix} x_1 & x_2 \\ x_1 & x_3 \\ x_1 & x_4 \\ x_2 & x_3 \\ x_2 & x_4 \\ x_3 & x_4 \end{bmatrix} + \dots \rightarrow \begin{bmatrix} x_1 & x_2 \\ \dots & \dots \\ x_1 & x_n \\ x_2 & x_3 \\ \dots & \dots \\ x_2 & x_n \\ x_3 & x_4 \\ \dots & \dots \\ x_{n-1} & x_n \end{bmatrix}. \quad (18)$$

То есть, при каждом новом появлении случайной величины x_n в матрице подвыборок добавляется ее $n - 1$ сочетание с предыдущими наблюдениями.

Наиболее быстродействующую и эффективную процедуру последовательного анализа можно реализовать путем обнаружения «разладки процесса» при снижении достоверности анализа ниже заданного уровня. Суть ее заключается в том, что полученное на каждом шаге процедуры значение статистики (2) является случайной величиной, равномерно распределенной в интервале $[0; 1]$, и содержит информацию обо всех предыдущих наблюдениях. Поэтому дальнейший анализ с ней и поступившей новой случайной величиной аналогичен предыдущему шагу.

Таким образом, комбинаторный критерий позволяет реализовать преимущества вариационного критерия равномерности при анализе выборок объемом $n > 2$. При этом мощность критерия значительно возрастает, а простота использования не выдвигает каких-либо дополнительных требований. Кроме того, в силу наивысшей энтропии равномерного закона распределения [10] представляется целесообразным формирование и других положений и критериев математической статистики на его основе. Это позволит получать некоторые решения в аналитическом виде с более высокой эффективностью по сравнению с традиционными.

Заключение

Использование подвыборок объемом $m = 2$ из исходной выборки малого объема путем сочетания наблюдений без повторений при $n > 3$ увеличивает количество k частных критериев. Построенный на основе их совокупности комбинаторный критерий обладает более высокими достигнутыми уровнями значимости и мощности при различении даже весьма близких гипотез. Такой критерий может служить основой эффективной процедуры последовательного анализа малой выборки.

Библиографический список

1. 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.
2. Виноградова М.С., Кандаурова И.Е., Ткачева О.С. Комбинаторный метод вычисления вероятностей // *Modern European Researches*. 2021. No 3 (Т.1). Рр. 67-79.
3. Воловик А.В. Вариационный критерий равномерности // *Надежность*. 2023. № 1. С. 52-55. DOI: 10.21683/1729-2646-2023-23-1-52-55.
4. Лемешко Б.Ю., Блинов П.Ю. Критерии проверки отклонения распределения от равномерного закона. Руководство по применению. Новосибирск: НГТУ, 2015. 182 с.
5. Корн Г., Корн Т. Справочник по математике. Для научных работников и инженеров. М.: Наука, 1974. 832 с.
6. Способ сигнализации наличия стружки в масле и устройство для его реализации: пат. 2791174 Рос. Федерация. № 2022116675 / Воловик А.В.; заявл. 20.06.2022; опубл. 03.03.2023, Бюл. № 7. 9 с.
7. Джонсон Н. Одномерные непрерывные распределения. Ч. 2. М.: БИНОМ. Лаборатория знаний, 2010–2012. 600 с.
8. Нейросетевой анализ нормальности малых выборок биометрических данных с использованием хи-квадрат критерия и критериев Андерсона – Дарлингa / В.И. Волчихин [и др.] // *Инженерные технологии и системы*. 2019. Т. 29. № 2. С. 205-217. DOI: 10.15507/2658-4123.029.201902.205-217
9. ГОСТ Р 50779.10-2000 Статистические методы. Вероятность и основы статистики. Термины и определения. М.: Стандартинформ, 2005. IV, 41 с.
10. Ивченко Б.П., Мартыщенко Л.А., Табухов М.Е. Управление в экономических и социальных системах. Системный анализ. Принятие решений в условиях неопределенности. СПб.: «Нордмед-Издат», 2001. 248 с.

References

1. Johnson N., Leone F. Statistics and Experimental Designs and Engineering and the Physical Sciences. Methods of Data Processing. Moscow: Mir; 1980.
2. Vinogradova M.S., Kandaurova I.E., Tkachiova O.S. [A combinatorial method of calculating probabilities]. *Modern European Researches* 2021;3(1):67-79. (in Russ.)
3. Volovik A.V. Variational criterion of evenness. *Dependability* 2023;23(1):52-55. DOI: 10.21683/1729-2646-2023-23-1-52-55. (in Russ.)
4. 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.)

5. Korn G., Korn T. Mathematical handbook. Moscow: Nauka; 1974.
6. Volovik A.V. A method of signalling the presence of shavings in oil and a device to implement it: patent 2791174 Russian Federation. No. 2022116675; submitted 20.06.2022; published 03.03.2023, Bul. no. 7.
7. Johnson N. Continuous univariate distributions. Vol. 2. Moscow: BINOM. Laboratoria znaniy; 2010-2012.
8. Volchikhin V.I. 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. DOI: <https://doi.org/10.15507/2658-4123.029.201902.205-217>. (in Russ.)
9. GOST R 50779.10-2000 Statistical methods. Probability and general statistical terms. Terms and definitions. Moscow: Standartinform; 2005. (in Russ.)
10. Ivchenko B.P., Martyschenko L.A., Tabukhov M.E. [Control in economic and social systems. Systems analysis-making under uncertainty]. Saint Petersburg: Nordmed-Izdat; 2001. (in Russ.)

Сведения об авторе

Воловик Александр Васильевич – кандидат технических наук, ведущий инженер-конструктор АО «ОДК-Климов», Санкт-Петербург, Российская Федерация, e-mail: volovik_aleksandr@mail.ru

About the author

Alexander V. Volovik, Candidate of Engineering, Lead Design Engineer, JSC Klimov, Saint Petersburg, Russian Federation, e-mail: volovik_aleksandr@mail.ru.

Вклад автора в статью

Воловик А.В. Предложен критерий согласия на основе совокупности комбинаций вариационного ряда, составленного из наблюдений в выборке малого объема. Проведены эксперименты по статистической оценке эффективности критерия по отношению к близкой альтернативе при разных объемах выборки, начиная с минимальной. Сделан вывод о целесообразности использования критерия для последовательного анализа и проверки гипотез о других законах распределения с помощью вероятностного интегрального преобразования.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Алгоритм улучшения согласованности структурной интероперабельности

An algorithm for improving the consistency of structural interoperability

Дулин С.К.^{1*}, Рябцев А.Б.²
Dulin S.K.^{1*}, Ryabtsev A.B.²

¹Федеральный исследовательский центр «Информатика и управление» Российской академии наук; Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте (АО НИИАС), Москва

²Московский физико-технический институт (Государственный университет), Москва

¹Federal Research Center Computer Science and Control of the Russian Academy of Sciences, Joint Stock Company Research and Design Institute for Information Technology, Signalling and Telecommunications in Railway Transportation (JSC NIAS), Moscow, Russian Federation

²Moscow Institute of Physics and Technology (Public university), Moscow

*skdulin@mail.ru



Дулин С.К.



Рябцев А.Б.

Резюме. Цель. Одной из наиболее сложных задач искусственного интеллекта является проблема согласованности совместно формируемой совокупности знаний. При этом существует весьма важный аспект процесса приобретения знаний – наличие средств сопровождения знаний. В общей схеме функционирования процедур сопровождения системы знаний особое место занимают процедуры, связанные с контролем согласованности взаимосвязанных компонентов. Среди направлений в области представления знаний выделилось исследование условий функционирования корпоративной системы знаний, в рамках которого одной из самых открытых проблем оказался поиск предпочтительной структуры интероперабельности компонентов системы знаний. Рассмотрим некоторое множество из n элементов, представляющих собой агенты, информационные системы или компоненты знаний, тогда можно поставить цель – оценить уровень интероперабельности и представить структуру интероперабельности на основании анализа предпочтительности установления отношений между элементами. **Методы.** Таким образом, необходимо учитывать влияние структуры взаимодействующих элементов на мотивацию к интероперабельности на основе определенных признаков или характеристик в структуре элементов, которые способствуют или препятствуют достижению интероперабельности. Было отмечено, что потенциальная возможность установления интероперабельности на основе структуры взаимосвязанных элементов, может быть определена как структурная интероперабельность. Соответственно, для изучения тенденции информационных систем или элементов к интероперабельности в зависимости от соотношения собственных признаков или характеристик была предложена методология структурного соответствия, позволяющая оценивать группы потенциально близких друг к другу элементов на основе аппарата структурной согласованности. Моделирование структурной интероперабельности на основе анализа структуры связей с помощью выбранного критерия согласованности позволяет найти ближайший к исходному множеству согласованный прообраз. Найденный прообраз своими подмножествами указывает на предпочтительную группировку элементов, при которой интероперабельность между ними устанавливается с наименьшей рассогласованностью. **Результаты.** В результате возникает разбиение множества потенциально взаимодействующих элементов на наборы мотивированных к взаимодействию элементов. В работе предлагается и обосновывается алгоритм нахождения для произвольной структуры элементов наиболее близкой согласованной структуры, на основе которой можно сделать вывод о выборе структуры интероперабельности. **Выводы.** Из анализа предлагаемого алгоритма и его альтернативы следует, что при сформулированных условиях существования структурной интероперабельности существует несколько вариантов выбора приемлемой структуры интероперабельности. Однако поиск оптимального варианта потребует перебора среди всех приемлемых вариантов, либо использование разумных эвристик, учитывающих специфику матрицы связности исходного знакового графа. Сравнивая представленные алгоритмы, необходимо заметить, что, алгоритм распространения меток носит оценочный характер, при этом, несмотря на сложность комбинаторных оценок и преобразований, алгоритм уменьшения рассогласованности на основе вектора попершинных различий представляет собой инструмент перманентного анализа и управления согласованностью наборов мотивированных к интероперабельности элементов.

Abstract. Aim. The consistency of a collectively generated body of knowledge is one of the most difficult problems of artificial intelligence. Additionally, there is a very important aspect of

the knowledge acquisition process, i.e., the availability of knowledge support tools. Within the overall scheme of operation of knowledge system maintenance procedures, those associated with ensuring the consistency of interrelated components hold a special place. Out of the lines of knowledge representation research, the study of the operating procedures of corporate knowledge systems stood out. One of its most unconquered challenges is finding an optimal structure for the interoperability of knowledge system components. Let us consider a set of n elements that represent agents, information systems or knowledge components, then we can set the goal of assessing the level of interoperability and present the structure of interoperability based on an analysis of preferred relationships between elements. **Methods.** Thus, the effect of the structure of interacting elements on the motivation for interoperability is to be taken into account based on certain features or characteristics in the structure of elements that contribute or hinder the achievement of interoperability. It was noted that the potential for establishing interoperability based on a structure of interrelated elements can be defined as structural interoperability. Accordingly, for the purpose of studying the tendency of information systems or elements to be interoperable depending on the correlation of their own features or characteristics, a structural correspondence methodology was proposed that allows evaluating groups of potentially close elements using the structural consistency apparatus. Modelling structural interoperability based on the analysis of the connections structure using the selected consistency criterion allows finding the consistent preimage that is the closest to the original set. The subsets of the found preimage indicate the preferred grouping of elements that enables interoperability with the least inconsistency. **Results.** As a result, the set of potentially interacting elements is divided into sets of elements motivated to interact. This paper proposes and justifies an algorithm for finding – for a random structure of elements – the closest consistent structure that allows concluding on the choice of the interoperability structure. **Conclusions.** Out of the analysis of the proposed algorithm and its alternative follows that, under defined conditions for the existence of structural interoperability, there are several options for an acceptable interoperability structure. However, finding the optimal option will require searching through all acceptable options, or using reasonable heuristics that take into account the specifics of the connectivity matrix of the original signed graph. Comparing the presented algorithms, it must be noted that the label propagation algorithm is evaluative in its nature. Meanwhile, despite the complexity of combinatorial estimates and transformations, the inconsistency reduction algorithm based on the vertex-to-vertex difference vector is a tool for permanent analysis and managing the consistency of sets of elements motivated for interoperability.

Ключевые слова: интероперабельность, структурная согласованность, матрица связности
Keywords: interoperability, structural consistency, connectivity matrix

Для цитирования: Дулин С. К., Рябцев А.Б. Алгоритм улучшения согласованности структурной интероперабельности // Надежность. 2024. №2. С. 8-15. <https://doi.org/10.21683/1729-2646-2024-24-2-8-15>

For citation: Dulin S.K., Ryabtsev A.B. An algorithm for improving the consistency of structural interoperability. Dependability 2024;2:8-15. <https://doi.org/10.21683/1729-2646-2024-24-2-8-15>

Поступила: 21.03.2024 г. / **После доработки:** 19.04.2024 / **К печати:** 10.06.2024
Received on: 18.10.2023 / **Revised on:** 08.04.2024 / **For printing:** 10.06.2024

Введение

В работе [1] было рассмотрено влияние структуры взаимодействующих элементов на мотивацию к интероперабельности на основе определенных признаков или характеристик в структуре элементов, которые способствуют или препятствуют достижению интероперабельности [2]. Было отмечено, что потенциальная возможность установления интероперабельности на основе структуры взаимосвязанных элементов [3] может быть определена как структурная интероперабельность [4]. Соответственно, для изучения тенденции информационных систем или элементов к интероперабельности в зависимости от соотношения собственных признаков или характеристик была предложена модель структурного соответствия, позволяющая оценивать группы потенциально близких друг к другу элементов.

Используемая терминология и источники

Задача поиска предпочтительной структуры интероперабельности компонентов системы знаний определяет разбиение множества потенциально взаимодействующих элементов на наборы мотивированных к взаимодействию элементов. Эти элементы могут быть описаны вектором параметров (признаков), из сравнения которых можно сделать вывод о сходстве между элементами и, соответственно, потенциальной мотивации к интероперабельности.

В общем случае представим множество элементов $O = \{o_i\}$ ($i = 1, \dots, n$), где описание каждого элемента представлено в виде вектора из m признаков – атрибутов: $o_i = (p_1^i, \dots, p_m^i)$. Сравнивая любые два элемента этого множества на основе этих признаков, можно оценить их сходство.

Для двух элементов o_i и o_j , сходство которых устанавливается на основе k признаков $\{p_k\}$, функция сходства может выглядеть как [1]:

$$F(o_i, o_j) = 1 - \frac{1}{k} \sum_{i=1}^k w_{ml} \frac{|p_{ml}^i - p_{ml}^j|}{\max |p_{ml}^i - p_{ml}^j|},$$

где $0 \leq w_{ml} \leq 1$ – вес ml -того признака;

$\max |p_{ml}^i - p_{ml}^j|$ – диапазон значений ml -того признака.

Функция F принимает значения из $[0, 1]$, так что $F = 1$ – это абсолютное сходство элементов o_i и o_j , а $F = 0$ – абсолютное различие.

Далее предлагается перейти к знаковому графу, позволяющему на основе анализа согласованности его связей по выбранному критерию согласованности сгруппировать n элементов в P групп. Переход к знаковому графу осуществляется в результате выбора порогового значения α для функции F , так что когда $0 \leq F(o_i, o_j) \leq \alpha$ элементы o_i и o_j считаются несходными по k признакам, а в случае $\alpha < F(o_i, o_j) \leq 1$ – сходными. Сопоставляя знак «минус» связям с $0 \leq F(o_i, o_j) \leq \alpha$ и знак «плюс» – иначе, получим знаковую структуру, являющуюся дискретной знаковой моделью множества потенциально взаимодействующих элементов.

Знаковому графу может быть поставлена в соответствие матрица связности. Задача согласованности структурной интероперабельности решается на основе учета тернарных отношений, которые могут быть отнесены к согласованному или рассогласованному состоянию. В [1] эти состояния названы консонансными и диссонансными, соответственно. Если представить знаковый граф в виде совокупности тернарных отношений, то получится система анализа структурной согласованности потенциально взаимодействующих элементов. В качестве критерия согласованности предлагается выбрать тернарный критерий Хайдера [5], относящий тернарные отношения (треугольники) к консонансным, если положительная связь между любыми парами вершин задает тождественность связей этих вершин с третьей, в противном случае – к диссонансным.

При разбиении знакового графа на треугольники и исследовании согласованности множества по критерию Хайдера выясняется, что консонансное множество M_K (состоящее только из консонансных треугольников) представимо в виде двух подмножеств M_1 и M_2 : $M_K = M_1 \cup M_2$, так что любые два элемента o_i и o_j из одного подмножества связаны положительной связью, а принадлежащие разным подмножествам – отрицательной. Если M_1 или M_2 пустое, то такое множество называется тривиальным – оно содержит только положительные связи. Ассонансным множеством назовем множество, содержащее как консонансные, так и диссонансные треугольники.

Приведение ассонансного множества в консонанс по Хайдеру означает возможность представления его в виде двух классов эквивалентности элементов. Для поиска согласованного множества, состоящего более чем из двух подмножеств, необходимо расширить критерий Хайдера

до понятия поликонсонанса и консонанса степени P [1]. Поликонсонанс степени P соответствует согласованному состоянию множества, состоящего не более, чем из P подмножеств, так что элементы внутри каждого подмножества связаны только положительными связями, а из разных подмножеств – только отрицательными. Под консонансом степени P будем понимать поликонсонанс степени P , состоящий в точности из P классов.

Описание алгоритма

Алгоритм поиска структурного соответствия, позволяющий оценивать связность групп потенциально близких друг к другу элементов, заключается в оценке состояния ассонансного множества, моделирующего потенциальную возможность элементов к интероперабельности. Полученное в результате моделирования ассонансное множество сравнивается с некоторым консонансным множеством – прообразом и преобразуется, используя операцию повершинного переброса (изменение всех знаков элемента как вершины знакового графа на противоположные) так, чтобы найти ближайший по количеству различаемых связей консонансный прообраз.

Определим контур множества как совокупность множеств, образованную в результате всевозможных повершинных изменений, то есть изменений всех знаков связей у каждого элемента (вершины в представлении этого множества в виде знакового графа). Если ограничиться повершинным изменением каждой вершины не более одного раза, то получим цикл.

Отсюда следует, что экземпляры консонансных (диссонансных) множеств образует контур.

В контуре множества взаимно преобразуются не более чем за $\lfloor n/2 \rfloor$ повершинных изменений, и каждая пара множеств контура единственным образом задает содержащий их цикл.

Предлагаемый алгоритм нахождения ближайшего консонансного прообраза для заданного ассонансного множества заключается в его сопоставлении с неким консонансным прообразом для приближения этого прообраза на основе повершинного изменения связей так, чтобы различие консонансного прообраза от ассонансного множества стало меньше.

Возьмем два множества M_1 и M_2 из одних и тех же n объектов с различными связями между объектами. Для каждой пары объектов o_i и o_j из этих множеств определим число r_{ij} так, что:

- а) $r_{ij} = 0$, если $i = j$;
- б) $r_{ij} = 0$, если $i \neq j$ и связи между o_i и o_j в этих множествах совпадают;
- в) $r_{ij} = 1$, если $i \neq j$ и связи между o_i и o_j в этих множествах различны.

Зададим набор из n чисел $(r_1, r_2, r_3, \dots, r_n)$, так что каждое из $r_i = \sum_{j=1}^n r_{ij}$ ($0 < r_i \leq n - 1$) равно числу различающихся знаков связей у объекта (вершины) o_i в том и другом множествах.

Можно рассматривать вектор $(r_1, r_2, r_3, \dots, r_n) = \vec{r}$ как критерий попершинного различия двух множеств из одних и тех же объектов, назвав его вектором попершинных различий (ВПП).

Сумма r_i равна двум суммам различающихся знаков связей.

Однако ВПП не позволяет однозначно задавать множество парой $(m, \vec{r})$ где m – экземпляр множества, $\vec{r}$ – ВПП m с заданным множеством [1].

Множеству, минимально удаленному по сумме изменяемых знаков связей от некоторого множества m , соответствует минимальная сумма компонентов вектора попершинных различий с m .

Обозначим через $M(\varphi)$ множество позиций, в которых располагаются φ различающихся знаков у двух строк матрицы связности, а через $K(M)$ – количество элементов множества M , то есть $K(M(\varphi)) = \varphi$.

Теорема 1. Пусть даны три строки с одинаковым количеством бинарных элементов: m_1, m_2, m_3 ; и числа несовпадающих значений элементов у каждой пары этих строк: r_{12}, r_{13}, r_{23} . Тогда справедливы следующие соотношения:

$$M(r_{13}) = (M(r_{12}) \cup M(r_{23})) / M(r_{12}) \cap M(r_{23});$$

$$r_{13} = r_{12} + r_{23} - 2K(M(r_{12}) \cap M(r_{23})).$$

Доказательство. Рассмотрим объединение позиций, по которым различаются строка m_1 от m_2 и строка m_2 от m_3 , то есть $M(r_{12}) \cup M(r_{23})$. Среди них есть позиции, в которых либо m_1 отличается от m_2 но m_2 не отличается от m_3 , либо m_1 не отличается от m_2 , а m_2 отличается от m_3 . Очевидно, что в этих позициях m_1 отличается от m_3 . Оставшиеся позиции являются позициями отличия m_1 от m_2 и m_2 от m_3 , и вследствие бинарности значений элементов строк значения элементов строк m_1 и m_3 в этих позициях не совпадают. Значит, если их исключить из числа позиций $M(r_{12}) \cup M(r_{23})$, то оставшееся множество и будет $M(r_{13})$, так как других различий нет. Множество исключаемых позиций состоит из $M(r_{12}) \cap M(r_{23})$. Учитывая вышесказанное, нетрудно заметить, что $K(M(r_{12}) \cup M(r_{23})) = r_{12} + r_{23} - K(M(r_{12}) \cap M(r_{23}))$. Отсюда $K(M(r_{13})) = r_{13} = K(M(r_{12}) \cup M(r_{23})) - K(M(r_{12}) \cap M(r_{23})) = r_{12} + r_{23} - 2K(M(r_{12}) \cap M(r_{23}))$.

Отметим, что теорема верна для любых трех последовательностей одинаковой длины с фиксированным положением бинарных элементов.

Лемма. Пусть проведена последовательность попершинных изменений из k вершин. Если начальные значения попершинных различий у этих вершин с теми же вершинами другого, множества были $\{r_i\}$, $i = 1 \dots k$; то после изменений они станут равными $(n - k) - r_i + 2\beta_i$, где β_i – количество позиций в i -й строке, в которых находятся знаки взаимных связей k вершин, одновременно являющиеся знаками различения, учитываемыми в r_i .

Доказательство. Поскольку у i -й вершины последовательности имеется $k - 1$ знаков связей с другими вершинами этой последовательности, то среди $k - 1$ знаков α_i знаков не являются знаками различения и не входят в число r_i , а остальные β_i – являются. Тогда в

результате попершинного изменения i -й вершины (то есть одновременного изменения всех знаков ее связей на противоположные) ее попершинное различие станет равным $(n - 1) - r_i$, а α_i теперь будет количеством знаков различения, β_i – наоборот. Последующие $k - 1$ попершинных изменений остальных вершин последовательности приведут к тому, что $(n - 1) - r_i$ уменьшится на α_i и увеличится на β_i , став равным $(n - 1) - r_i - \alpha_i + \beta_i$. Но $\alpha_i + \beta_i = k - 1$, отсюда получим $(n - k) - r_i + 2\beta_i$.

Теорема 2. Пусть множества m_1 и m_2 состоят из одних и тех же объектов. Рассмотрим в цикле множества m_1 состояние m_1^k , полученное k попершинными изменениями, и в цикле множества m_2 состояние m_2^k , полученное k попершинными изменениями тех же k вершин. Тогда вектора попершинных различий множества m_1 от m_2^k и множества m_2 от m_1^k совпадают.

Доказательство. Согласно лемме, k строк m_1 и m_2^k будут различаться на $(n - k) - r_i + 2\beta_i^*$ и $n - k$ строк m_1 и m_2^k будут различаться на $k - r_i + 2\beta_i^*$, где r_i – компоненты вектора попершинных различий m_1 от m_2 . Аналогично для k строк m_2 и m_1^k : $(n - k) - r_i + 2\beta_i^{**}$ и $n - k$ строк m_2 и m_1^k : $k - r_i + 2\beta_i^{**}$. Но β_i^* и β_i^{**} входят в число знаков между k вершинами или $n - k$ вершинами, которые остались неизменными, значит, все $\beta_i^* = \beta_i^{**}$.

Отсюда следует, что рассматривая в качестве m_1 произвольное ассонансное множество, а в качестве m_2 – консонансное, можно искать минимально удаленный консонансный прообраз, находясь в цикле ассонансного множества m_1 , поставив затем в соответствие m_1 множество m_2^k , полученное той же последовательностью попершинных изменений, что и найденное нами минимально удаленное от m_2 состояние m_1^k .

Казалось бы, что достаточно брать произвольное консонансное множество, сравнивать с ним исходное ассонансное и производить последовательные попершинные изменения пока все попершинные различия не станут меньше или равными половине связей, получив в минимально удаленное состояние. Но этого оказывается недостаточно. Пример ассонансного множества на рис. 1 показывает, что различие этого множества с тривиальным консонансным множеством (0:9) характеризует вектор r_1 , у которого только первый компонент равен половине связей вершины, а остальные – меньше. Но (0:9) – не минимальный консонансный прообраз, так как вектор r_2 , различающий указанное консонансное множество и консонантное множество (5:4), имеет все

0:9					5:4				r_1	r_2
01	+	+	+	+	-	-	-	-	4	0
+	02	+	+	+	-	+	-	+	2	2
+	+	03	+	+	+	-	+	-	2	2
+	+	+	04	+	-	+	-	+	2	2
+	+	+	+	05	+	-	+	-	2	2
-	-	+	-	+	06	+	+	+	3	2
-	+	-	+	-	+	07	+	+	3	2
-	-	+	-	+	+	+	08	+	3	2
-	+	-	+	-	+	+	+	09	3	2

Рис. 1. Матрица ассонансного множества и ВПП с консонансами 0:9 и 4:5

компоненты меньше половины связей и действительно определяет минимально удаленное консонансное множество (5:4).

Теорема 3. Перемещаясь по циклу множества можно обнаружить несколько векторов повершинных различий, у каждого из которых все компоненты меньше половины количества связей вершины. При этом соответствующие состояния отстоят друг от друга не менее чем на два повершинных изменения для четного n и не менее чем на три – для нечетного n .

Доказательство. Пусть мы находимся в состоянии с вектором $\vec{r}$: $r_i < \gamma$, где γ – половина количества связей вершины. Постараемся достичь еще одно состояние за k повершинных изменений, характеризуемое вектором $\vec{r}^k$: $r_i^k < \gamma$, $r_j^k < \gamma$, предположив, что оно существует. Для каждой из k вершин, согласно Лемме, компонента вектора $r_j^k = (n - k) - r_j + 2\beta_j$. Но у вектора $\vec{r}^k$ все компоненты также должны быть меньше γ , значит $(n - k) - r_j + 2\beta_j < \gamma$ и $k > n - \gamma - r_j + 2\beta_j$. Ясно, что k будет минимальным, когда $\beta_j = 0$ (следствие 1 из Леммы), а r_j принимает максимальное значение, равное $\gamma - 1$. Отсюда $k > n - 2\gamma + 1$.

Для четного n получаем $k > 1$, а для нечетного – $k > 2$.

Пример множества из четного числа объектов, равноудаленного от трех консонансных множеств, отстоящих друг от друга на два повершинных изменения, приведен на рис. 2. При этом все $r_i < \gamma$.

0:8				2:6				4:4			
o ₁	+	+	+	-	-	-	+	3	3	1	
+	o ₂	+	+	+	-	-	-	3	3	1	
+	+	o ₃	+	-	+	+	+	1	3	3	
+	+	+	o ₄	-	+	+	+	1	3	3	
-	+	-	-	o ₅	+	+	+	3	3	1	
-	-	+	+	+	o ₆	+	+	2	0	2	
-	-	+	+	+	+	o ₇	+	2	0	2	
+	-	+	+	+	+	+	o ₈	1	1	3	

Рис. 2. Матрица ассонансного множества и ВПР с консонансами 0:8, 2:6 и 4:5

Другой пример на рис. 3 показывает существование двух векторов со значениями компонентов меньше γ , но задающих разное удаление приведенного на рис. 3 ассонансного множества от консонансных множеств (0:9) и (4:5). Таким образом, не только при равенстве повершинных различий числу γ нельзя считать, что это минимальное удаление, но и при достижении состояния,

0:9				4:5				0:9				4:5			
o ₁	+	+	+	+	-	+	-	3		3		2			
+	o ₂	+	+	-	+	-	-	3		3		2			
+	+	o ₃	+	+	-	+	-	3		3		2			
+	+	+	o ₄	-	+	-	+	3		3		2			
+	-	+	-	o ₅	-	+	+	3		3		3			
-	+	-	+	-	o ₆	+	+	3		3		3			
+	-	+	-	+	+	o ₇	+	2		2		2			
-	-	-	+	+	+	+	o ₈	3		3		1			
-	+	-	-	+	+	+	+	o ₉		3		1			

Рис. 3. Два ВПР с неулучшаемыми компонентами, но с разным удалением по связям

где все $r_i < \gamma$, также нельзя быть уверенным, что именно оно и есть минимально удаленное.

Из вышесказанного следует, что алгоритм, основанный на уменьшении повершинных различий, должен обеспечивать нахождение всех потенциально минимальных состояний, а не останавливаться на первом найденном. В принципе, для множества m может не существовать вектора $\vec{r}$: $r_i < \gamma$, а количество минимальных состояний будет равно количеству типов консонансного множества, так что поиск состояния с вектором $\vec{r}$: $r_i < \gamma$ в этом случае ничего не даст.

Основная идея уменьшения рассогласованности множества за счет вершинных перебросов заключается в следующем. Возьмем некоторое консонансное множество и «испорчим» часть связей, переводя его в ассонанс. Представим теперь, что мы забыли этот ближайший консонансный прообраз полученного ассонанса, и будем искать его среди возможных консонансов в рамках выбранной степени. Если взять произвольное консонансное множество и сравнить с ним имеющееся ассонансное множество, то ВПР в общем случае будет содержать нулевые компоненты. Каждая компонента ВПР будет представлять собой число, учитывающее различие в связях ближайшего консонансного прообраза, взятого наугад консонансного множества, и различие, возникшее из-за «испорченных» связей. Итак, рассматриваемый ВПР учитывает два вида различий. Однако ближайший консонансный прообраз и взятое наугад консонансное множество принадлежат одному контуру как переводимые друг в друга некоторой последовательностью вершинных перебросов, и тогда останется только минимальный набор диссонансных связей. Но простым перебором это сделать очень трудно, т.к. надо перебирать экземпляры консонансных множеств, а их даже для поликонсонанса степени 2 порядка 2^{n-1} .

Алгоритм уменьшения рассогласованности был предложен для поликонсонанса степени 2. Обобщим его применение для степени n .

Пусть имеется некоторое ассонансное множество. Возьмем произвольное консонансное множество $A_1 A_2 A_3 \dots A_N (n_1; n_2; n_3 \dots n_N)$ степени N , составленное из тех же объектов. Тогда некоторому объекту $o_i \in A_1 A_2 A_3 \dots A_N$ соответствует r_i – ВПР этих множеств. Рассмотрим знаки связей объекта o_i , например, в A_1 и A_2 , составленные из n_1 и n_2 объектов, соответственно. Если окажется, что у o_i среди связей с объектами подмножеств A_1 и A_2 более чем $1/2 (n_1 + n_2 - 1)$ отличаются от аналогичных связей того же o_i в ассонансном множестве, то o_i целесообразно перебросить из A_2 в A_1 , т.к. это уменьшит r_i , а следовательно, и общую сумму $\sum r_i$, равную, как уже отмечалось, удвоенной сумме диссонансных связей. Действуя аналогичным образом с другими объектами, мы придем к ситуации, когда ни один из объектов уже не имеет смысла перебрасывать в другое подмножество. Тогда, казалось бы, уничтожен один вид различия – межконсонансный, и остались только диссонансные связи в полученном минимально удаленном консонансном прообразе. Однако

это не всегда верно, т.е. из того, что каждый единичный вершинный переброс не выгоден, еще не следует, что нецелесообразно перебросить группу объектов.

Рассмотрим последовательность повершинных перебросов из k объектов. Любой r_i может быть записан как $r_i = \beta_i + \psi_i + v_i$, где β_i – количество различающихся знаков связей между k объектами переброса, ψ_i – количество различающихся знаков с остальными $n_1 + n_2 - k$ объектами обоих подмножеств и v_i – различающиеся знаки с $n - (n_1 + n_2)$ объектами, не принадлежащими рассматриваемым подмножествам. Если начальные значения повершинных различий у этих объектов с теми же объектами другого множества были r_i , то после произведенных перебросов они станут равными $n_1 + n_2 - k - r_i + 2\beta_i + 2v_i$. Доказательство этого легко проводится по аналогии с Леммой. Пусть имеется все то же консонансное множество, в котором нет ни одного объекта $o_i \in A_2$, такого, что соответствующие связи с n_1 и n_2 объектами A_1 и A_2 имеют более чем $1/2 (n_1 + n_2 - 1)$ различий со связями тех же объектов ассонансного множества. Найдем условие, при котором целесообразно перебросить целую группу объектов из A_2 в A_1 . Обозначим через γ число $1/2 (n_1 + n_2 - 1)$. Различающиеся знаки v_i можно опустить из рассмотрения, т.к. они не имеют отношения к проводимым перебросам. Итак, до проводимых перебросов каждый объект из группы перебрасываемых объектов имел $\beta_i + \psi_i$ различающихся знаков со всеми остальными $n = n_1 + n_2$ объектами обоих подмножеств. После проведенных перебросов число различий стало $(n_1 + n_2 - k) - \psi_i + \beta_i$. По начальному условию ни один объект из группы перебрасывать нецелесообразно, т.е. все $\beta_i + \psi_i \leq \gamma$, аналогично после перебросов мы не должны выйти из локального минимально удаленного состояния, т.е. все $(n_1 + n_2 - k) - \psi_i + \beta_i \leq \gamma$. Отсюда возникают ограничения на β_i : $\beta_i \leq \frac{k-1}{2}$ и на ψ_i : $\beta_i + \gamma - (k-1) \leq \psi_i \leq \gamma - \beta_i$. Условие улучшения минимальной удаленности по знакам

$$\sum_{i=1}^k \beta_i + \sum_{i=1}^k \psi_i > \sum_{i=1}^k (n-k) - \sum_{i=1}^k \psi_i + \sum_{i=1}^k \beta_i \text{ дает}$$

$$\sum_{i=1}^k \psi_i > 1/2(n-k) \cdot k.$$

$$\text{Кроме того, } \sum_{i=1}^k \psi_i + \sum_{i=1}^k \beta_i \leq \gamma \cdot k, \text{ значит}$$

$$\sum_{i=1}^k \beta_i < \frac{k(k-1)}{2}.$$

Предположим, что последовательность из $k-1$ перебросов еще не обеспечивает улучшение локального минимума, т.е. $\sum_{i=1}^{k-1} \psi_i \leq \frac{(n+k+1)(k-1)}{2}$. Тогда переброс группы из k объектов будет целесообразен, если существует o_k : $\sum_{i=1}^{k-1} \psi_i + \psi_k > \frac{(n-k) \cdot k}{2}$, т.е. $\psi_k > \gamma - (k-1)$.

Интерпретация условия $\sum_{i=1}^k \psi_i > \frac{(n-k) \cdot k}{2}$ почти оче-

видна: если среди связей некоторой группы из k объектов с остальными $n-k$ объектами более половины отличается от связей тестируемого ассонансного множества, значит, эта группа имеет тенденцию к перебросу в другое подмножество, что тем самым поставит в соответствие ассонансному множеству менее удаленное по сумме различающихся знаков связей консонансное множество [6]. Поиск такой группы объектов даже для поликонсонанса степени 2 является очень сложной задачей, т.к. заранее невозможно определить даже потенциальную возможность вхождения каждого объекта в конструируемую для предполагаемого переброса группу.

Альтернативный подход

Другим подходом к поиску близкого консонансного прообраза, не требующим решения тяжелых комбинаторных задач, является алгоритм распространения меток [7].

В основе алгоритма лежит идея о том, что у вершины графа сообщество будет таким же, как и у большинства ее соседей.

Сам алгоритм работает следующим образом:

Изначально каждой вершине графа присваивается своя уникальная метка.

В цикле, пока решение не сойдется, или не будет достигнуто максимальное количество итераций, у каждой вершины обновляется метка на ту, которая чаще встречается у ее соседей. Если среди соседей самых часто встречаемых меток несколько, выбирается случайная.

Для перехода к формальному описанию алгоритма, нужно ввести ряд понятий:

Матрица связности $\mathbf{A}$ – симметричная квадратная матрица, показывающая наличие или отсутствие связей между объектами.

Диагональная матрица степеней $\mathbf{D}$ – диагональные элементы равны степеням вершин графа, а степень вершины графа – число связей этой вершины с другими вершинами:

$$\mathbf{D} = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}.$$

Матрица перехода $P = \mathbf{D}^{-1} \mathbf{A}$, где

$$\mathbf{D}^{-1} = \begin{pmatrix} \frac{1}{d_1} & 0 & \dots & 0 \\ 0 & \frac{1}{d_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \frac{1}{d_n} \end{pmatrix}.$$

Матрица «цветов» Y имеет размерность $N \times M$, где N – число объектов (вершин графа), а M – число уникальных цветов на нулевой итерации алгоритма (максимальное число кластеров). В нашем случае удобно считать, что $N = M$, то есть изначально каждая вершина графа имеет свой уникальный цвет. Тогда без потери общности

$$Y(0) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}, \quad Y(t+1) = PY(t).$$

При этом новые цвета вершин определяются как $\arg \max_{color} Y$.

На рис. 4 приведен пример работы данного алгоритма. Сначала каждому узлу присваивается своя уникальная метка, и далее запускается их распространение по графу. По ходу распространения меток соседи внутри одного сообщества достаточно быстро приходят к общему значению метки. Далее такие сообщества начинают расширяться,

пока это возможно. На примере видно, что вершины 3 и 5 хоть и соединены ребром, имеют разные цвета. Так получилось, потому что основная часть соседей каждой из двух этих вершин (вершины 2 и 4 – для вершины 3, и вершины 6, 7 и 8 – для вершины 5) имеют общий цвет метки.

Является ли решение, найденное данным алгоритмом, оптимальным с точки зрения достижения минимального по сумме компонент ВПР, неизвестно. Однако алгоритм имеет эффективную реализацию для распределенных вычислительных систем, что делает его удобным для использования на практике. Говоря про оптимальность, стоит отметить, что алгоритм можно как минимум использовать как быстрый метод для поиска первоначального консонансного прообраза для алгоритма из предыдущего раздела.

Заключение

Из приведенного описания предлагаемого алгоритма и его альтернативы следует, что при сформулированных условиях существования структурной интероперабельности существует несколько вариантов

выбора приемлемой структуры интероперабельности. Однако поиск оптимального варианта потребует перебора среди всех приемлемых вариантов, либо использование разумных эвристик, учитывающих специфику матрицы связности исходного знакового графа. Сравнивая представленные алгоритмы, необходимо заметить, что алгоритм распространения меток носит оценочный характер, при этом, несмотря на сложность комбинаторных оценок и преобразований, алгоритм уменьшения рассогласованности на основе вектора попершинных различий представляет собой инструмент перманентного анализа и управления согласованностью наборов мотивированных к интероперабельности элементов.

Библиографический список

1. Розенберг И.Н., Дулин С.К., Дулина Н.Г. Моделирование структуры интероперабельности средствами структурной согласованности // Информатика и ее применения. 2023. Т. 17. Вып. 1. С. 57-65. DOI 10.14357/19922264230108

Algorithm: Label propagation, Zhu et al. 2002

Input: Graph G , labels Y_k

Output: labels $\hat{Y}$

Compute adjacency matrix A

Compute $d_i = \sum_j A_{ij}$

Compute $D = \text{diag}(d)$

Compute $P = D^{-1}A$

Initialize $Y(0) = (Y_k, 0), t = 0$

repeat

$Y(t+1) = PY(t)$

$Y_k(t+1) = Y_k(t)$

$t = t + 1$

until $Y(t)$ converges;

$\hat{Y} = Y(t)$

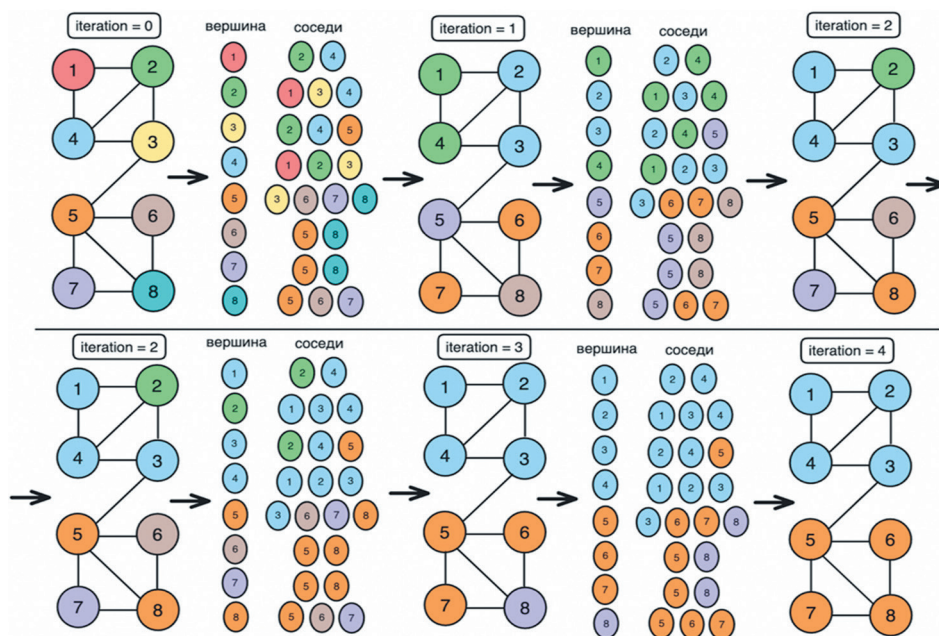


Рис. 4. Схема работы алгоритма распространения меток. Цвет вершины соответствует метке / кластеру

2. ГОСТ Р 55062-2012 Информационные технологии (ИТ). Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения. М.: Стандартинформ, 2014. IV, 8 с.

3. Ullberg Johan, Johnson Pontus, Buschle Markus. A Modeling Language for Interoperability Assessments // *Lecture Notes in Business Information Processing*. 2011. V. 76. Pp. 61-74. DOI: 10.1007/978-3-642-19680-5_7

4. Макаренко С.И., Соловьева О.С. Основные положения концепции семантической интероперабельности сетевых систем // *Журнал радиоэлектроники*. 2021. № 4. 24 с. DOI:10.30898/1684-1719.2021.4.10

5. Heider F. The psychology of interpersonal relation. N.Y., 1982. 336 p. DOI: 10.30898/1684-1719.2021.6.3

6. Дулин С.К., Дулина Н.Г., Кожунова О.С. Синтез геоанализа в пространственных инфраструктурах на основе связанных данных // *Информатика и ее применения*. 2019. Т. 13. № 1. С. 82-90. DOI: 10.14357/19922264190112

7. Xiaojin Zhu, Ghahramani Zoubin. Learning from labeled and unlabeled data with label propagation // *Tech. Rep., Technical Report CMU-CALD-02-107*, Carnegie Mellon University. 2002. URL: <https://mlg.eng.cam.ac.uk/zoubin/papers/CMU-CALD-02-107.pdf> (дата обращения: 01.04.2024)

References

1. Rozenberg I.N., Dulin S.K., Dulina N.G. Modeling the structure of interoperability by means of structural consistency. *Informatics and Applications* 2023;17(1):57-65. DOI 10.14357/19922264230108. (in Russ.)

2. GOST R 55062-2012. Information technologies. Industrial automation systems and integration. Interoperability. Basic principles. Moscow: Standartinform; 2014. (in Russ.)

3. Ullberg J., Johnson P., Buschle M. A Modeling language for interoperability assessments. *Lecture Notes in Business Information Processing* 2011;76:61-74. DOI: 10.1007/978-3-642-19680-5_7.

4. Makarenko S.I., Solovieva O.S. [Key provisions of the concept of semantic interoperability of network-centric systems]. *Journal of radio electronics* 2021;4. DOI:10.30898/1684-1719.2021.4.10. (in Russ.)

5. Heider F. The psychology of interpersonal relation. New York; 1982. DOI: 10.30898/1684-1719.2021.6.3.

6. Dulin S.K., Dulina N.G., Kozhunova O.S. Synthesis of geodata in spatial infrastructures based on related data. *Informatics and Applications* 2019;13(1):82-90. DOI: 10.14357/19922264190112. (in Russ.)

7. Xiaojin Z., Ghahramani Z. Learning from labeled and unlabeled data with label propagation. Technical Report CMU-CALD-02-107, Carnegie Mellon University; 2002. (accessed 01.04.2024). Available at: <https://mlg.eng.cam.ac.uk/zoubin/papers/CMU-CALD-02-107.pdf>.

Сведения об авторах

Дулин Сергей Константинович (Dulin Sergey Konstantinovich) – 109029, Россия, Москва, Нижегородская ул., д.27 стр.1, АО «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС»), главный научный сотрудник, доктор технических наук, профессор; 119333, Россия, Москва, ул. Вавилова, д.44 к.2, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, ведущий научный сотрудник, e-mail: skdulin@mail.ru; *Надежность* № 3, 2018; *Системы и средства информатики* Т. 28, № 2. 2018; Т. 29 № 3. 2019; Т. 30, № 2. 2020; Т. 31, № 3. 2021; Т. 32, № 1. 2022; Т. 33, № 2, 2023; *Железнодорожный транспорт* № 8, 2018; *Информатика и ее применения* Т. 13. № 1. 2019; Т. 14, Вып. 1, 2020; Т. 17, Вып. 1, 2023; *Автоматика, связь, информатика*. №11, 2021.

Рябцев Антон Борисович (Ryabtsev Anton Borisovich) – 117303, Россия, Москва, Керченская ул., д.1а к.1, Московский физико-технический институт (Государственный университет), аспирант, ryabtsev.ab@phystech.edu; *Образовательные ресурсы и технологии* № 3(44), 2023.

About the authors

Sergey K. Dulin, Doctor of Engineering, Professor, Chief Researcher, JSC Research and Design Institute for Information Technology, Signalling and Telecommunications in Railway Transportation (JSC NIIS), 27, bldg 1 Nizhegorodskaya St., Moscow, 109029, Russia; Lead Researcher, Federal Research Center Computer Science and Control of the Russian Academy of Sciences, 44, korp. 2 Vavilova St., Moscow, 119333, Russia, e-mail: skdulin@mail.ru; *Dependability* 2018;3; *Systems and Means of Informatics* 2018;28(2); 2019;29(3); 2020;30(2); 2021;31(3); 2022;32(1); 2023;33(2); *Zheleznodorozhny transport* 2018;8; *Informatics and Applications* 2019;13(1); 2020;14(1); 2023;17(1); *Automation, Communications, Informatics* 2021;11.

Anton B. Ryabtsev, post-graduate student, Moscow Institute of Physics and Technology (Public university), 1a, korp. 1 Kerchenskaya St., Moscow, 117303, Russia, ryabtsev.ab@phystech.edu; *Educational Resources and Technologies* 2023;3(44).

Вклад авторов в статью

Дулин С.К. разработал алгоритм улучшения согласованности структурной интероперабельности. Рябцев А.Б. исследовал и развил алгоритм распространения меток, сравнил его возможности с разработанным Дулиным С.К. алгоритмом улучшения согласованности структурной интероперабельности.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Улучшение алгоритма Дейкстры для оценки характеристик и критического пути проекта¹

Improving Dijkstra's algorithm for Estimating Project Characteristics and Critical Path

Адилакшми Ширипурапу¹, Рави Шанкар Наупада², К. Шриниваса Рао³
Adilakshmi Siripurapu¹, Ravi Shankar Nowpada², K. Srinivasa Rao³

¹Кафедра естественных и гуманитарных наук, Институт информатики им. Вигнана, Дуввада, Вишакхапатнам, Андхра-Прадеш, Индия, ²Кафедра математики, Институт естественных наук, Институт техники и управления им. Ганди, Вишакхапатнам, Андхра-Прадеш, Индия, ³Кафедра организации, Школа предпринимательства, Институт техники и управления им. Ганди, Вишакхапатнам, Андхра-Прадеш, Индия

¹Dept. of Basic Science and Humanities, Vignan's Institute of Information Technology (A), Duvvada, Visakhapatnam, AP, India, ²Dept. of Mathematics, Institute of Science, GITAM (Deemed to be University), Visakhapatnam, AP, India, ³Dept. of Operations, GITAM school of Business, GITAM (Deemed to be University), Visakhapatnam, AP, India

^{*}laxmimaths2008@gmail.com



Адилакшми
Ширипурапу



Рави Шанкар
Наупада



К. Шриниваса Рао

Резюме. В любой отрасли разработка структуры планирования проекта представляет собой сложную техническую задачу, которая включает в себя оценку факторов, ограничивающих выполнение задач по каждому виду работ, и соответствующие инструменты планирования. Любое ограничение влияет на время выполнения работ, эксплуатационные издержки и общую эффективность выполнения проекта. Процессы метода оценки и пересмотра программ (Programme Evaluation Review Technique, PERT) и метода критического пути (Critical Path Method, CPM) побудили многих исследователей изучать возможные способы поиска критических путей и работ в сетевом графике. CPM и PERT пока еще очень далеки от реализации вероятностной среды. Однако подходы на основе искусственного интеллекта, такие как генетический алгоритм, алгоритм Дейкстры и другие, используются для анализа сети в рамках управления проектами. Настоящее исследование призвано помочь менеджеру проекта спланировать график выполнения строительного проекта для определения ожидаемого времени его завершения. В данной исследовательской работе мы описываем метод получения раннего и позднего значений времени критического пути с помощью модифицированного алгоритма Дейкстры с треугольными нечеткими числами. Для поиска оптимального пути для предложенного метода разработаны алгоритмы прохода вперед и назад. Также приведены численные примеры. Результаты моделирования приведены с использованием программы «С». Наконец, проводится сравнение с традиционным методом PERT.

Abstract. Developing a project planning structure for all industries is a technological challenge involving evaluating several restrictions for each activity's respective task and its planning tools. Any restriction affects the completion time, operating costs, and overall project performance. Programme Evaluation Review Technique (PERT) and Critical Path Method (CPM) processes made many researchers study the possible ways of finding the critical paths and activities in the network. The advancement of the CPM and PERT towards a probabilistic environment is still a long way off. However, Artificial intelligence approaches such as the Genetic Algorithm, Dijkstra's algorithm, and others are utilized for network analysis within the project management framework. This study is to help the project manager plan schedule for a construction project to determine the expected completion time. In this research paper, we describe a method for obtaining the earliest and latest times of a critical path using modified Dijkstra's algorithm with triangular fuzzy numbers. Forward pass and backward pass algorithms are designed to find the optimal path for the proposed method. Numerical examples are also illustrated for the same. Simulation results are included by the use of the "C" program. Finally, a comparison is made with the traditional method PERT.

Ключевые слова: критический путь, алгоритм Дейкстры, раннее и позднее время, модифицированный алгоритм Дейкстры, PERT.

Keywords: Critical Path, Dijkstra's Algorithm, Earliest and latest times, modified Dijkstra's algorithm, PERT.

¹ Adilakshmi Siripurapu, Ravi Shankar Nowpada, and K. Srinivasa Rao. Improving Dijkstra's algorithm for Estimating Project Characteristics and Critical Path Reliability // Theory & Applications. 2022. Vol. 17. No. 4(71). Pp. 65-73. doi:10.24412/1932-2321-2022-471-65-73

Для цитирования: Адиллакшми Ширипурапу, Рави Шанкар Наупада, К. Шриниваса Рао
Улучшение алгоритма Дейкстры для оценки характеристик и критического пути проекта
// Надежность. 2024. №2. С. 16-23. <https://doi.org/10.21683/1729-2646-2024-24-2-16-23>

For citation: Adilakshmi Siripurapu, Ravi Shankar Nowpada, K. Srinivasa Rao. Improving Dijkstra's algorithm for Estimating Project Characteristics and Critical Path. Dependability 2024;2: 16-23. <https://doi.org/10.21683/1729-2646-2024-24-2-16-23>

Поступила: 31.03.2023 / **После доработки:** 17.04.2024 / **К печати:** 10.06.2024

Received on: 31.03.2023 / **Revised on:** 17.04.2024 / **For printing:** 10.06.2024

1. Введение

В процессе разработки сетевого графика проекта задачей контролера проекта ставится разработка первичного плана. Метод критического пути – один из наиболее известных подходов к подготовке сетевого графика проекта. Концепция критического пути позволяет лицу, принимающему решения, контролировать стоимость и график проекта, а также может повысить качество выполняемых работ. Этот метод широко используется в различных отраслях промышленности для анализа и повышения эффективности проектов. Было рассмотрено много случаев, когда время выполнения работ детерминировано. Метод PERT применим к вероятностным средам. В управлении проектами применяются различные методы и техники. Каждая процедура имеет запас времени, отведенного для выполнения задачи. Для управления проектами, в частности, применяются диаграмма Ганта, сетевая диаграмма, CPM и PERT.

В CPM при оценке самого длинного пути учитывается продолжительность каждой работы. В PERT расчетное время выполнения работы задается. В связи с этим, в PERT применяются трехточечные оценки (наиболее вероятная $[m]$, оптимистическая $[a]$ и пессимистическая $[b]$) при условии, что распределение работ соответствует бета-распределению. Аппроксимация PERT с использованием бета-распределения была впервые предложена Малкомом в 1959 году [7]. В 1993 году Чаном был предложен эффективный алгоритм анализа методом критического пути (CHAN), основанный на методе автоматической генерации тестовых шаблонов (ATPG) PODEM [1]. Традиционно в PERT использовалось бета-распределение. В 2018 г. Соломон Саки и др. предложили расширить измененную модель PERT и использовать ее для моделирования риска планирования. Предложенная модель PERT была основана на подозрении с 95-процентным уровнем уверенности. В соответствии с крайним сроком и вероятностью отставания вычисляется вероятность завершения проекта в пяти перспективах для обоих подходов. Для оценки частоты ошибок для каждого примера взята выборка. Средняя частота ошибок была рассчитана с использованием традиционного метода PERT и обновленного метода PERT для всех случаев. Обновленная версия PERT улучшила среднюю частоту ошибок на 2,46% против 3,31% для традиционного метода PERT. Такой подход подтвер-

дил, что пересмотренный PERT способен обеспечить более точную оценку вероятности завершения работ лучше, чем традиционный PERT. К слову, поскольку новый PERT был полностью основан на подозрениях, можно с уверенностью сказать, что он намного превосходит традиционную модель PERT [8]. Ли и др. в 2007 с помощью моделирования по методу Монте-Карло была изучена сетевая программа реального проекта. Результат показал, что стохастическая сетевая программа дала значительные данные по планированию лучше, чем обычная сетевая программа [4]. Ли (2005) предложен программный подход Стохастическое имитационное моделирование календарного планирования проекта (Stochastic Project Scheduling Simulation, SPSS), который влияет на возможность завершения проекта в срок, установленный оператором программного обеспечения. Программное обеспечение SPSS обеспечивает моделирование времени осуществления работ, используя ряд распределений вероятностей, а также равномерное, треугольное и нормальное распределения. SPSS также рассчитывает постоянное улучшение (CI) для всех работ по проекту [3]. В целом, моделирование сетевого графика проекта используется для повышения обоснованности и надежности исследования PERT. Чен и др. (2004) объяснили использование имитационного моделирования по методу Монте-Карло в рамках PERT для обеспечения стохастического периода реализации работ [2]. Имитационная модель формирует гистограмму распределения сети завершённых работ. Метод имитационного моделирования CPM/PERT добавляет план имитационного моделирования дискретных событий и процесс определения критического пути. По словам авторов, «в рамках анализа на основе критического пути проекта для каждого вида работ необходимо определить раннее начало (ES_{ij}), позднее начало (LS_{ij}), раннее завершение (EF_{ij}), позднее завершение (LF_{ij}) и общий резерв времени (TF_{ij})». ES_{ij} и EF_{ij} сетевого графика проекта вычисляются во время прохода вперед, тогда как LS_{ij} , LF_{ij} и TF_{ij} определяются во время прохода назад. Лю и др. (2000) использовали TF_{ij} для оценки важности проекта [5]. Согласно Маккриммону и др. (1964) один из недостатков PERT заключается в том, что хотя для завершения проекта необходимо пройти много путей, время проекта сокращается и не превышает соответствующего среднего показателя [6]. Шанкар и др. (2010) использовали модифицированный алгоритм Дейкстры для оценки продолжительности проекта [9]. Сяокан Хань и

др. в 2021 году предложили улучшенный алгоритм муравьиной колонии для определения критического пути, задавая расстояние и время пути отрицательными при неизменной вероятности перехода [10].

В 1965 году Заде [11] представлена концепция теории нечетких множеств. Современный высококонкурентный мир породил множество проблем в нечеткой математике. Когда периоды осуществления работ в среде проекта детерминированы, многие реальные события проходят быстрее за счет использования идеи нечеткости.

В данной работе с помощью метода оценки и переосмотра программ (PERT) и метода критического пути (CPM) наряду с алгоритмом Дейкстры рассмотрен пример формирования критического пути и продолжительности проекта. Значения главной цели взяты в нечетких числах. Мы можем ранжировать нечеткие числа с целью нахождения наилучшей альтернативы.

2. Методология

2.1. Алгоритм предложения

Измененный алгоритм Дейкстры определяет максимальное время между начальным узлом (называемым «узлом-источником») и последующими узлами в сети. В этом методе веса ребер используются для определения пути, который оптимизирует общее расстояние (вес) между начальным узлом и последующими узлами. Модифицированный алгоритм Дейкстры подходит только для положительно взвешенных графов, поскольку веса ребер должны быть добавлены во время процедуры определения самого длинного пути.

Основные понятия применительно к измененному алгоритму Дейкстры:

- измененный алгоритм Дейкстры начинается с выбранного вами узла (исходного узла) и анализирует граф с целью определить самый длинный путь внутри этого узла и всех последующих узлов сети;
- при помощи модели рассматривается известный на данный момент самый длинный путь в пределах отдельного узла и исходного узла, и при обнаружении длиннейшего пути изменяются значения;
- при помощи модели находится максимальное расстояние от одного события до другого. Узел помечается как «посещенный» и добавляется к пути;
- процедура продолжается до тех пор, пока все узлы графа не будут включены в путь. В результате мы получаем путь, который добавляет исходный узел ко всем последующим узлам, выбирая самый длинный возможный путь к отдельному узлу;
- исходный узел находится на нулевом расстоянии от самого себя. Изначально всем вершинам присвоена метка «0»;
- используем знак бесконечности, чтобы указать расстояние от исходного узла до всех остальных узлов на текущий момент, поскольку оно еще не оценено;

- мы находим ранние значения времени с использованием модифицированного алгоритма Дейкстры с помощью алгоритма прохода вперед и поздние значения времени с помощью алгоритма прохода назад.

2.2. Вычисления вперед в алгоритме Дейкстры

Шаг 1: В последовательности $v_1=1, v_2=2, \dots, v_n=n$ выделить n вершин.

Шаг 2: Присвоить постоянную метку «0» первичной вершине $v_1=1$ и временную метку «0» остальным $n-1$ ребрам.

Шаг 3: Каждая вершина j , не имеющая постоянной метки, получает новую временную метку, т.е.

$$E_j = \max\{\text{oldlabel}of i, (\text{oldlabel}of i + t_{ij})\},$$

где i имеет постоянную метку новой вершиной, а t_{ij} – продолжительность работы между вершинами i и j , если ребро не соединено с i и j , $t_{ij}=\infty$.

Шаг 4: Следующая вершина превращается в фиксированную (посещенную) метку.

Шаг 3 и шаг 4 повторяются до тех пор, пока $v_n=n$ не получит фиксированную метку. Постоянно помеченные значения E_j являются самыми ранними сроками, поскольку $E_1=0$.

2.3. Вычисления назад в алгоритме Дейкстры

Шаг 1: Задайте n вершины как $v_n=n, v_{n-1}=n-1, \dots, v_1=1$.

Шаг 2: Присвойте фиксированную метку $L_n=E_n$ вершине $v_n=n$ и временные метки остальным $n-1$ вершинам.

Шаг 3: Любой узел j , который не получил постоянную метку, получает новую временную метку, т.е.

$$L_j = \min\left[\text{oldlabel}of i, (\text{oldlabel}of i + t_{ij})\right],$$

где j имеет фиксированную метку, а новая вершина t_{ij} – это продолжительность работ между вершинами i и j .

Шаг 4: как и в шаге 1, следующая вершина становится фиксированной или постоянной меткой.

Повторить шаги 3 и 4 до тех пор, пока начальная вершина $v_1=1$ не получит фиксированную метку.

2.4. Ранжирование предложений в треугольном нечетком числе

Пусть $\tilde{A} = (a, b, c)$ – треугольное нечеткое число. Рассмотрим центроид треугольника как ранжирование в треугольном нечетком числе (ТНЧ). Его диаграмма представлена на рис. 1.

Центроид треугольника равен $(a+b+c)/3$. Обратите внимание, что центроид треугольника является новым рангом в треугольном нечетком числе.

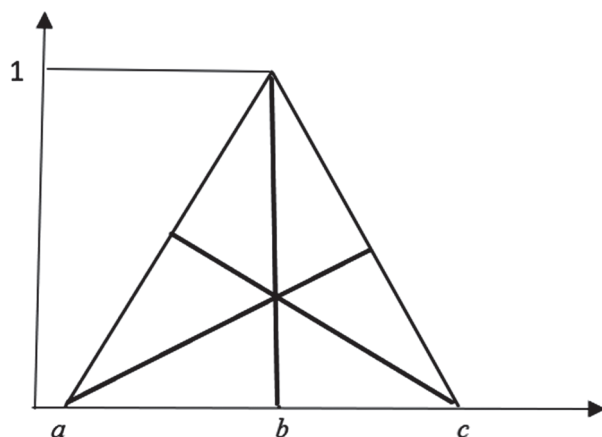


Рис. 1. Схематичное представление центроида ТНЧ

Таким образом, новый ранг в треугольном нечетком числе –

$$\mathcal{R}(\tilde{A}) = \frac{a+b+c}{3}.$$

3. Численный анализ

Здесь мы собрали практические примеры из сетевых источников, которые представлены в табл. 1. Кроме того, соответствующая сетевая диаграмма представлена на рис. 2.

Табл. 1. Проблема применения

Работы	Код	Предшественник	a	m	b
1→2	P	-	5	6	7
1→3	Q	-	1	3	5
1→4	R	-	1	4	7
2→5	S	P	1	2	3
3→6	T	Q	1	2	9
4→6	U	R	1	5	9
4→7	V	R	2	2	8
6→7	W	T, U	4	4	10
5→8	X	S	2	5	8
7→8	Y	W, V	2	2	8

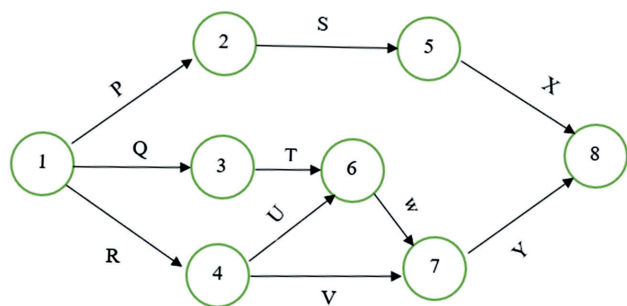


Рис. 2. Проблема применения, представленная в виде диаграммы

3.1. Продолжительность работ, рассчитанная путем принятия треугольных нечетких чисел

Продолжительность работ, принятая в треугольных нечетких числах, представлена в табл. 2. Соответствующая диаграмма представлена на рис. 3.

Табл. 2. Ожидаемое время выполнения работ с ТНЧ

Работы	a	m	b	ТНЧ
1→2	5	6	7	(5,6,7)
1→3	1	3	5	(1,3,5)
1→4	1	4	7	(1,4,7)
2→5	1	2	3	(1,2,3)
3→6	1	2	9	(1,2,9)
4→6	1	5	9	(1,5,9)
4→7	2	2	8	(2,2,8)
6→7	4	4	10	(4,4,10)
5→8	2	5	8	(2,5,8)
7→8	2	2	8	(2,2,8)

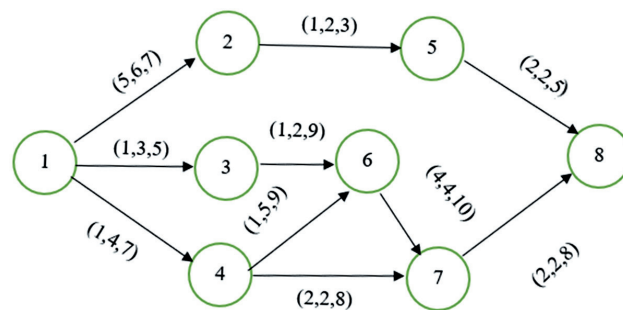


Рис. 3. Пункты сетевого графика работ с ТНЧ

3.2. Самые ранние сроки

Самые ранние сроки для каждого узла сетевого графика проекта, рассчитанные с использованием алгоритма прохода вперед на основе треугольных нечетких чисел, показаны в табл. 3.

3.3. Поздние значения времени

Поздние значения времени каждой вершины сетевого графика, рассчитанные с использованием алгоритма прохода назад по формуле упорядочивания с треугольными нечеткими числами, показаны в Табл. 4.

Из двух вышеприведенных таблиц (табл. 3 и табл. 4) следует, что

$$E_1 = L_1 = (0, 0, 0), E_4 = L_4 = (1, 4, 7), E_6 = L_6 = (2, 9, 16), \\ E_7 = L_7 = (6, 13, 26) E_8 = L_8 = (8, 15, 34).$$

Табл. 3. Ранние значения времени каждого узла с ТНЧ

Номер вершины								Раннее время
1	2	3	4	5	6	7	8	
(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	$E_1=(0,0,0)$
(0,0,0)(F)	(5,6,7)	(1,3,5)	(1,4,7)	∞	∞	∞	∞	
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)	(1,4,7)	∞	∞	∞	∞	$E_2=(5,6,7)$
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)	(1,4,7)	(6,8,10)	∞	∞	∞	
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)	(6,8,10)	∞	∞	∞	$E_3=(1,3,5)$
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)	(6,8,10)	(2,5,14)	∞	∞	
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)	(2,5,14)	∞	∞	$E_4=(1,4,7)$
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)	(2,9,16)	(3,6,15)	∞	
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)(F)	(2,9,16)	(3,6,15)	∞	$E_5=(6,8,10)$
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)(F)	(2,9,16)	(3,6,15)	(8,10,15)	
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)(F)	(2,9,16)(F)	(3,6,15)	(8,10,15)	$E_6=(2,9,16)$
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)(F)	(2,9,16)(F)	(6,13,26)	(8,10,15)	
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)(F)	(2,9,16)(F)	(6,13,26)(F)	(8,10,15)	$E_7=(6,13,26)$
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)(F)	(2,9,16)(F)	(6,13,26)(F)	(8,15,34)	
(0,0,0)(F)	(5,6,7)(F)	(1,3,5)(F)	(1,4,7)(F)	(6,8,10)(F)	(2,9,16)(F)	(6,13,26)(F)	(8,15,34)(F)	$E_8=(8,15,34)$

В результате критический путь – 1→4→6→7→8, а продолжительность проекта – (8, 15, 34).

Теперь треугольное нечеткое число (8, 15, 34) преобразуется в нормальное время с помощью формулы ранжирования треугольных нечетких чисел $(a + b + c)/3$. Приведенное к четкости значение (8, 15, 34) составляет 19. Таким образом, проект заканчивается через 19 дней.

4. Традиционные методы

4.1. Метод оценки и пересмотра программ (PERT)

Метод оценки и пересмотра программ (PERT) – это метод управления проектами, предназначенный для оценки того, сколько времени потребуется для успешного завершения проекта. В управлении проектами существует подход, согласно которому проект делится

на мелкие проекты или работы. Каждая работы имеет свои временные рамки, требования и конечные результаты. Чаще всего эти сроки не детерминированы. В конкретных обстоятельствах традиционный PERT выдает трехточечные оценки: оптимистическую, пессимистическую и наиболее вероятную. Это простая стратегия, использующая механизм бета-распределения.

Оценка продолжительности для каждой работы может быть спрогнозирована с помощью средств бета-распределения следующего средневзвешенного значения:

$$ET = \frac{\left(\begin{array}{l} \text{Оптимистическая} + \\ + 4 * \text{Наиболее вероятная} + \\ + \text{Пессимистическая} \end{array} \right)}{6}.$$

Здесь мы рассчитываем продолжительности работ, используя среднее значение вероятностных значений

Табл. 4. Поздние значения времени каждого узла с ТНЧ

Номер вершины								Позднее значение времени
8	7	6	5	4	3	2	1	
(8,15,34)(F)	(8,15,34)	(8,15,34)	(8,15,34)	(8,15,34)	(8,15,34)	(8,15,34)	(8,15,34)	$L_8=E_8=(8,15,34)$
(8,15,34)(F)	(6,13,26)	(8,15,34)	(6,13,29)	(8,15,34)	(8,15,34)	(8,15,34)	(8,15,34)	
(8,15,34)(F)	(6,13,26)(F)	(8,15,34)	(6,13,29)	(8,15,34)	(8,15,34)	(8,15,34)	(8,15,34)	$L_7=(6,13,26)$
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)	(6,13,29)	(4,11,18)	(8,15,34)	(8,15,34)	(8,15,34)	
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)	(4,11,18)	(8,15,34)	(8,15,34)	(8,15,34)	$L_6=(2,9,16)$
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)	(1,4,7)	(1,7,7)	(8,15,34)	(8,15,34)	
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)(F)	(1,4,7)	(1,7,7)	(8,15,34)	(8,15,34)	$L_5=(6,13,29)$
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)(F)	(1,4,7)	(1,7,7)	(5,11,26)	(8,15,34)	
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)(F)	(1,4,7)(F)	(1,7,7)	(5,11,26)	(8,15,34)	$L_4=(1,4,7)$
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)(F)	(1,4,7)(F)	(1,7,7)	(5,11,12)	(0,0,0)	
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)(F)	(1,4,7)(F)	(1,7,7)(F)	(5,11,12)	(0,0,0)	$L_3=(1,7,7)$
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)(F)	(1,4,7)(F)	(1,7,7)(F)	(5,11,12)	(0,0,0)	
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)(F)	(1,4,7)(F)	(1,7,7)(F)	(5,11,12)(F)	(0,0,0)	$L_2=(5,11,12)$
(8,15,34)(F)	(6,13,26)(F)	(2,9,16)(F)	(6,13,29)(F)	(1,4,7)(F)	(1,7,7)(F)	(5,11,12)(F)	(0,0,0)(F)	$L_1=(0,0,0)$

времен, и представляем их в табл. 5. Соответствующая сетевая диаграмма представлена на рис. 4.

Табл. 5. Продолжительность работ со средним вероятностным значением

Работы	a	m	b	$ET=(a+4m+b)/6$
1→2	5	6	7	6
1→3	1	3	5	3
1→4	1	4	7	4
2→5	1	2	3	2
3→6	1	2	9	3
4→6	1	5	9	5
4→7	2	2	8	3
6→7	4	4	10	5
5→8	2	5	8	5
7→8	2	2	8	3

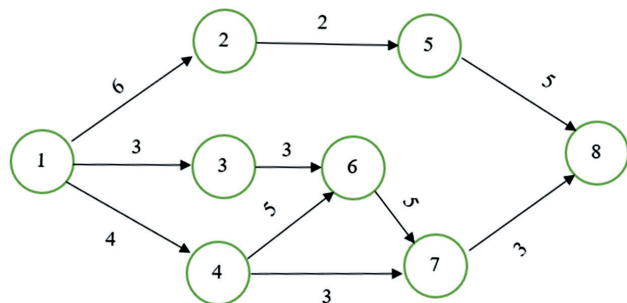


Рис. 4. Продолжительность работ с сетевой диаграммой вероятностных значений времени

4.2. Процедура нахождения критического пути:

Шаг 1: Создайте сетевой график проекта $G(V, E)$.

Шаг 2: Выразите время каждой работы как вероятностное время.

Шаг 3: Определите самое раннее время начала работы, используя расчет вперед. Пусть ранее время начального события равно нулю, $\tilde{E}_1 = 0$. Тогда $\tilde{E}_j = \max\{\tilde{E}_i + \tilde{t}_{ij}\}$, где i – число предшествующих событий.

Шаг 4: Вычислите раннее время окончания работы

$(E\tilde{F}_{ij}) = \text{Раннее время окончания} + \text{длительность работ}$,

$$\text{i.e. } E\tilde{F}_{ij} = E\tilde{S}_{ij} + \tilde{t}_{ij} = \tilde{E}_i + \tilde{t}_{ij}.$$

Шаг 5: Оцените позднее время окончания работы, используя расчет назад: $\tilde{E}_n = \tilde{L}_n$.

Таким образом, чтобы $\tilde{L}_i = L\tilde{F}_{ij} = \min\{\tilde{L}_j - \tilde{t}_{ij}\}$, $i = n-1, n-2, \dots, 2, 1$.

Шаг 6: Рассчитайте позднее время начала работы $(L\tilde{S}_{ij}) = L\tilde{F}_{ij} - \tilde{t}_{ij}$.

Шаг 7: Общий резерв времени $(T\tilde{F}_{ij}) = L\tilde{F}_{ij} - E\tilde{F}_{ij}$ или $L\tilde{S}_{ij} - E\tilde{S}_{ij}$.

Результаты представлены в табл. 6.

Табл. 6. Ранние и поздние значения времени выполнения проектных работ с вероятностным средним значением

Работы	Вершина	Длительность работ	$E\tilde{S}_{ij}$	$E\tilde{F}_{ij}$	$L\tilde{S}_{ij}$	$L\tilde{F}_{ij}$	$T\tilde{F}_{ij}$
1→2	P	6	0	6	4	10	4
1→3	Q	3	0	3	3	6	3
1→4	R	4	0	4	0	4	0*
2→5	S	2	6	8	10	12	4
3→6	T	3	3	6	6	9	3
4→6	U	5	4	9	4	9	0*
4→7	V	3	4	7	11	14	7
6→7	W	5	8	13	12	17	4
5→8	X	5	9	14	9	14	0*
7→8	Y	3	14	17	14	17	0*

Критические работы: 1→4, 4→6, 5→8, 7→8. Соответственно, критический путь – 1→4→6→7→8, а время завершения проекта – 17.

5. Результаты работы

В табл. 7 представлены критический путь и продолжительность проекта с вероятностным и треугольным нечетким значениями времени работ соответственно.

Табл. 7. Результаты

Продолжительности работ	Критический путь	Время окончания проекта
Вероятностные значения времени	1→4→6→7→8	17
Треугольное нечеткое число	1→4→6→7→8	19

На графике на рис. 5 представлены результаты корреляции между математическим ожиданием и треугольным нечетким средним.

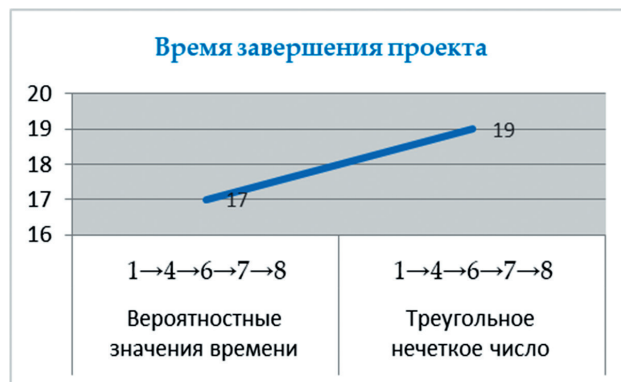


Рис. 5. Корреляция времени завершения проекта и математического ожидания и треугольного нечеткого среднего значения

6. Обсуждение

В настоящей статье определяется ранний и поздний сроки осуществления проекта с применением модифицированного алгоритма Дейкстры с треугольным нечетким числом и вероятностными значениями времени. Критический путь сети определяется с помощью раннего и позднего значений времени осуществления работ проекта. Кроме того, рассчитывается время всего проекта. Критический путь проекта идентичен в обоих случаях, но время завершения проекта различается. Вероятностное среднее обеспечивает более короткие сроки в сравнении с нечетким треугольным средним. Однако в ненаучном примере на это число влияют различные обстоятельства, такие как наличие аналитиков и тип работ.

Библиографический список

1. Chang H., Abraham J.A. CHAN: An efficient critical path analysis algorithm // 1993 European Conference on Design Automation with the European Event in ASIC Design, Paris, France, 22-25 February 1993. Pp. 444-448. DOI: 10.1109/EDAC.1993.386435
2. Cheng X.L., Zhang Y.L., Cui X.S. Applied in Resource Constrained Project Scheduling Problem // *Industrial Engineering Journal*. 2004. Vol. 7(3). Pp. 51-54.
3. Lee D. Probability of project completion using stochastic project scheduling simulation // *Journal of Construction Engineering and Management*. 2005. Vol. 131(3). Pp. 310-318.
4. Li Q, Zhang J., Zhang R.T. Application of Monte Carlo Simulation in Project Schedule // *Journal of Yangtze University (Natural Science Edition)*. 2007. Vol. 4(2). Pp. 62-66.
5. Lu M., AbouRizk S.M. Simplified CPM/PERT simulation model // *Journal of Construction Engineering and Management*. 2000. Vol. 126(3). Pp. 219-226.
6. MacCrimmon K.R., Ryavec C.A. An Analytical Study of the PERT Assumptions // *Operation Research*. 1964. Vol. 12. No. 1. Pp. 16-37.
7. Malcon D.G., Roseboom J.H., Clark C.E. et al. Application of a Technique for Research and Development Program Evaluation // *Operation Research*. 1959. Vol. 7. Issue 5. Pp. 646-669.
8. Sackey Solomon, Kim Byung-Soo. Schedule Risk Analysis using a proposed Modified Variance and Mean of the Original Program Evaluation and Review Technique Model // *KSCE Journal of Civil Engineering*. 2018. Vol. 23(4). Pp. 1484-1492.
9. Ravi Shankar N., Sireesha V. Using modified Dijkstra's algorithm for critical path method in a project network // *International Journal of Computational and Applied Mathematics*. 2010. Vol. 5. No. 2. Pp. 217-225.
10. Xiaokang Han, Wenzhou Yan, Mei Lu. Intelligent Critical Path Computation Algorithm Utilising Ant Colony Optimisation for Complex Project Scheduling //

Complexity. 2021. Vol. 2021. Article ID 9930113. 8 p. DOI: 10.1155/2021/9930113

11. Zadeh L.A. Fuzzy sets // *Information and Control*. 1965. Vol. 8. Issue 3. Pp 338-353.

References

1. Chang H., Abraham J.A. CHAN: An efficient critical path analysis algorithm. In: proceedings of the 1993 European Conference on Design Automation with the European Event in ASIC Design. Paris (France), 22-25 February 1993. Pp. 444-448. DOI: 10.1109/EDAC.1993.386435
2. Cheng X.L., Zhang Y.L., Cui X.S. Applied in Resource Constrained Project Scheduling Problem. *Industrial Engineering Journal* 2004;7(3):51-54.
3. Lee D. Probability of project completion using stochastic project scheduling simulation. *Journal of Construction Engineering and Management* 2005;131(3):310-318.
4. Li Q, Zhang J., Zhang R.T. Application of Monte Carlo Simulation in Project Schedule. *Journal of Yangtze University (Natural Science Edition)* 2007;4(2):62-66.
5. Lu M., AbouRizk S.M. Simplified CPM/PERT simulation model. *Journal of Construction Engineering and Management* 2000;126(3):219-226.
6. MacCrimmon K.R., Ryavec C.A. An Analytical Study of the PERT Assumptions. *Operation Research* 1964;12(1):16-37.
7. Malcon D.G., Roseboom J.H., Clark C.E. et al. Application of a Technique for Research and Development Program Evaluation. *Operation Research* 1959;7(5): 646-669.
8. Sackey Solomon, Kim Byung-Soo. Schedule Risk Analysis using a proposed Modified Variance and Mean of the Original Program Evaluation and Review Technique Model. *KSCE Journal of Civil Engineering* 2018;23(4):1484-1492.
9. Ravi Shankar N., Sireesha V. Using modified Dijkstra's algorithm for critical path method in a project network. *International Journal of Computational and Applied Mathematics* 2010;5(2):217-225.
10. Xiaokang Han, Wenzhou Yan, Mei Lu. Intelligent Critical Path Computation Algorithm Utilising Ant Colony Optimisation for Complex Project Scheduling. *Complexity* 2021; 2021. Article ID 9930113. 8 p. DOI: 10.1155/2021/9930113.
11. Zadeh L.A. Fuzzy sets. *Information and Control* 1965;8(3):338-353.

Сведения об авторах

Адиллакши Ширипурапу, PhD, ассистент профессора, Кафедра естественных и гуманитарных наук, Институт информатики им. Вигнана, Дуввада, Вишакхапатнам, Андхра-Прадеш, Индия, e-mail: laxmimaths2008@gmail.com

Рави Шанкар Наупада, профессор, Кафедра математики, Институт естественных наук, Институт техники и управления им. Ганди, Вишакхапатнам, Андхра-Прадеш,

Индия, научные интересы включают прикладную теорию групп, исследование операций (в частности, управление проектами, транспортные проблемы, сети цепей поставок), теорию нечетких множеств, включая нечеткое принятие решений, и криптографию, e-mail: Drravi68@gmail.com

К. Шриниваса Рао, PhD, кафедра организации, Школа предпринимательства, Институт техники и управления им. Ганди, Вишакхапатнам, Андхра-Прадеш, Индия, Темы исследований: квантовая теория углового момента, специальные функции и ортогональные полиномы, вычислительные методы, e-mail: skolli2@gitam.edu

About the authors

Adilakshmi Siripurapu, PhD, Assistant Professor, Dept. of Basic Science and Humanities, Vignan's Institute of Information Technology (A), Duvvada, Visakhapatnam, AP, India, e-mail: laxmimaths2008@gmail.com.

Ravi Shankar Nowpada, Professor, Dept. of Mathematics, Institute of Science, GITAM (Deemed to be University), Visakhapatnam, AP, India, the academic interests include the applied group theory, operations research (including project management, transportation, supply chain management), fuzzy set theory, including fuzzy decision-making, and cryptography, e-mail: Drravi68@gmail.com.

K. Srinivasa Rao, PhD, Dept. of Operations, GITAM school of Business, GITAM (Deemed to be University), Visakhapatnam, AP, India, research topics: quantum theory of angular momentum, special functions and orthogonal polynomials, computational methods, e-mail: skolli2@gitam.edu.

Вклад авторов в статью

Рави Шанкар Наупада выполнил постановку задачи раннего и позднего сроков осуществления проекта с применением модифицированного алгоритма Дейкстры с треугольным нечетким числом и вероятностными значениями времени.

Адилакшми Ширипурапу выполнен обзор традиционных работ по теме статьи и сравнение предлагаемого подхода к с традиционным методом PERT.

К. Шриниваса Рао осуществил программную реализацию поиска оптимального пути для предложенного метода. Разработаны алгоритмы прохода вперед и назад и выполнены численные расчеты на языке C.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Особенности обнаружения ошибок при контроле вычислений в цифровых устройствах по признаку самодвойственности булевых функций

The specificity of error detection as part of computing testing in digital devices based on self-duality of Boolean functions

Ефанов Д.В.^{1*}, Погодина Т.С.²
Efanov D.V.^{1*}, Pogodina T.S.²

¹Высшая школа транспорта Института машиностроения, материалов и транспорта Санкт-Петербургского политехнического университета Петра Великого, Санкт-Петербург, Российская Федерация; «Научно-исследовательский и проектный институт «Транспортной и строительной безопасности», Санкт-Петербург, Российская Федерация; Российский университет транспорта (МИИТ), Москва, Российская Федерация; Ташкентский государственный транспортный университет, Ташкент, Республика Узбекистан

²Российский университет транспорта (МИИТ), Москва, Российская Федерация

¹Higher School of Transportation, Institute of Engineering, Materials, and Transportation, Peter the Great St. Petersburg Polytechnic University, Saint Peteresburg, Russian Federation; Research and Design Institute for Transportation and Construction Safety, Saint Peteresburg, Russian Federation; Russian University of Transport (MIIT), Moscow, Russian Federation; Tashkent State Transport University, Tashkent, Republic of Uzbekistan

²Russian University of Transport (MIIT), Moscow, Russian Federation

*TrES-4b@yandex.ru



Ефанов Д.В.



Погодина Т.С.

Резюме. Цель. Установить особенности обнаружения ошибок при самодвойственном контроле вычислений устройствами автоматики, а также предложить способ организации контроля вычислений с обнаружением любых неисправностей из заданной модели.

Методы. Использованы методы технической диагностики дискретных систем, булевой алгебры, комбинаторики. **Результаты.** Проанализированы особенности обнаружения ошибок на выходах самодвойственных цифровых устройств комбинационного типа. Формализованы условия обнаружения и не обнаружения ошибок на выходах самодвойственных комбинационных схем, которые позволяют на практике путем анализа потенциальных ошибок на их выходах организовывать полностью самопроверяемые схемы встроенного контроля. При этом отмечается, что если полного покрытия всех ошибок на выходах самодвойственных схем не удастся достичь при контроле вычислений только по признаку принадлежности функций классу самодвойственных, то в ряде случаев это возможно за счет дополнительного контроля принадлежности формируемых кодовых векторов заранее выбранному избыточному коду. Установлено, за счет каких особенностей для реальных цифровых устройств потенциально возможно большое количество компенсируемых при самодвойственном контроле ошибок. Теоретически определено, что в реальных практических приложениях при самодвойственном контроле вычислений чем больше число входных переменных, тем выше вероятность не обнаружения ошибки за счет большего числа сочетаний искажений на выходах. Но чем больше число реализуемых устройством функций, тем выше и вероятность обнаружения ошибки. Тем не менее, на практике нужно индивидуально подходить к процессу организации контроля вычислений по признаку самодвойственности вычисляемых функций для каждого из цифровых устройств. Приведены некоторые результаты экспериментов, демонстрирующие особенности обнаружения ошибок на выходах самодвойственных комбинационных схем с использованием различных схемотехнических способов, основанных на сжатии сигналов от объектов контроля с применением модифицированных кодов Хэмминга (кодов Сяо). **Заключение.** Установленные в работе условия обнаружения ошибок на выходах самодвойственных цифровых устройств позволяют на практике синтезировать самопроверяемые вычислительные системы с улучшенными показателями контролепригодности по сравнению с традиционными подходами к их реализации.

Abstract. Aim. To identify the specificity of error detection as part of self-dual calculations testing by automation devices, as well as to propose a method for organising calculations testing that would allow detecting any malfunctions from the defined model. **Methods.** The paper used methods of technical diagnostics of discrete systems, Boolean algebra, and

combinatorics. **Results.** The specificity of error detection at the outputs of self-dual digital devices of combination type were analysed. The conditions for detecting and not detecting errors at the outputs of self-dual combinational circuits were formalised. In practice, the latter allow – by analysing potential errors at the outputs – creating fully self-checking circuits. At the same time, it is noted that if full coverage of all errors at the outputs of self-dual circuits cannot be achieved when computing-testing only on the basis of whether a function belongs to the self-dual class, then in some cases that can be made possible through additional checking of whether the generated code vectors belong to a pre-selected redundant code. It is established, what features of actual digital devices enable large numbers of errors compensated for by self-dual testing. It is theoretically determined that, in real practical applications with self-dual computing testing, the larger is the number of input variables, the higher is the probability of not detecting an error due to a larger number of combinations of distortions at the outputs. However, the greater is the number of functions implemented by a device, the higher is the probability of error detection. Nonetheless, in practice, each case of computations testing based on the self-duality of calculated functions should be treated individually for each digital device. The paper presents some experimental results that demonstrate the specificity of error detection at the outputs of self-dual combinational circuits using various circuit design methods based on compressing the signals received from the monitored facilities using modified Hamming codes (Hsiao codes). **Conclusion.** The conditions for detecting errors at the outputs of self-dual digital devices established in this paper allow practically synthesising self-checking computer systems with improved checkability as compared with conventional approaches to their implementation.

Ключевые слова: самопроверяемые цифровые устройства; самодвойственные комбинационные схемы; обнаружение ошибок в вычислениях; контроль вычислений по признаку самодвойственности булевых функций; компенсация ошибки при самодвойственном контроле; условия обнаружения ошибок при самодвойственном контроле.

Keywords: self-checking digital devices; self-dual combinational circuits; computational error detection; computations checking based on self-duality of Boolean functions; error compensation as part of self-dual checking; conditions for error detection as part of self-dual checking.

Для цитирования: Ефанов Д.В., Погодина Т.С. Особенности обнаружения ошибок при контроле вычислений в цифровых устройствах по признаку самодвойственности булевых функций // Надежность. 2024. №2. С. 24-37. <https://doi.org/10.21683/1729-2646-2024-24-2-24-37>

For citation: Efanov D.V., Pogodina T.S. The specificity of error detection as part of computing testing in digital devices based on self-duality of Boolean functions. Dependability 2024;2:24-37. <https://doi.org/10.21683/1729-2646-2024-24-2-24-37>

Поступила: 04.09.2023 / **После доработки:** 11.04.2024 / **К печати:** 10.06.2024

Received on: 04.09.2023 / **Revised on:** 11.04.2024 / **For printing:** 10.06.2024

Введение

Реализация высоконадежных и безопасных устройств и вычислительных систем невозможна без применения методов контроля вычислений. В современных технических решениях часто применяют контроль остатков, контроль мантисс, сигнатурный анализ, кодовые методы, контроль вычислений по принадлежности к особым классам функций и многие другие [1–7]. Одним из эффективных подходов к организации контроля вычислений является контроль принадлежности вычисляемых функций классу самодвойственных булевых функций, или так называемый *самодвойственный контроль вычислений* [8].

При реализации самодвойственного контроля некоторого устройства в общем случае можно выделить два основных технических решения. Первое состоит в том, что устройство, на выходах которого реализуются произвольные булевы функции, преобразуется в такое устройство, выходы которого описываются исключи-

тельно самодвойственными булевыми функциями – в *самодвойственное устройство*. Такое преобразование возможно всегда и реализуется с использованием всего одной переменной (для некоторых устройств, например, с частично определенными функциями выходов, дополнительная переменная может и не потребоваться) [9]. Способы преобразования устройств в самодвойственные описаны, например, в [10]. В общем, можно сказать, что все они основаны на использовании известного разложения К. Э. Шеннона (разложения булевых функций по одной переменной) (см., например, теорему 1.16 из [11]). Второе техническое решение при организации контроля вычислений по признаку самодвойственности функций состоит в использовании метода логической коррекции сигналов при синтезе схемы встроенного контроля (СВК) [12, 13]. В этом случае устройство, формирующее произвольные булевы функции, не преобразуется, а дополняется блоками, в которых уже производится самодвойственное преобразование и в последующем

осуществляется контроль самодвойственности вычисляемых функций [14]. Данный способ контроля вычислений по признаку самодвойственности вычисляемых функций также реализуем всегда.

Особенности синтеза самодвойственных устройств и вычислительных систем рассмотрены не только в многочисленных публикациях отечественных и зарубежных ученых, но и в трех монографиях [15–17]. Отметим, что общей особенностью всех самодвойственных устройств является использование для реализации временной избыточности и импульсного режима функционирования, что как раз и позволяет контролировать вычисления по принадлежности формируемых функций к классу самодвойственных. Это приводит к подаче на входы устройства пар ортогональных по всем переменным комбинаций.

Во всех работах, посвященных реализации самодвойственных устройств и их тестированию, обсуждаются особенности обнаружения ошибок в вычислениях и указывается, что ошибка не будет обнаружена только в том случае, если она возникнет при поступлении на входы ортогональных по всем переменным входных комбинаций. Другими словами, проявится в обеих комбинациях из пары. Однако не обсуждается, какое именно число таких ошибок возможно.

В ходе исследований авторов настоящей статьи в части реализации самодвойственных устройств и моделирования их работы выяснилось, что только при самодвойственном контроле вычислений с применением схем сжатия сигналов с наблюдаемых выходов вне зависимости от способа реализации схемы сжатия может появляться большое число маскируемых ошибок. Например, при использовании в этих целях кодов Хэмминга и их различных модификаций не во всех случаях удается покрывать все ошибки, возникающие на выходах устройств [18, 19]. Повысить число обнаруживаемых ошибок можно за счет применения дополнительного контроля вычислений по принадлежности формируемых кодовых слов на выходах устройств заранее выбранным двоичным избыточным кодам [20, 21]. Однако возникает закономерный вопрос: что же, все-таки, влияет на появление в некоторых случаях структур цифровых устройств большого числа маскируемых ошибок?

Целью настоящей работы является установление формальных условий обнаружения ошибок при самодвойственном контроле вычислений устройствами автоматики и определения числа потенциально маскируемых ошибок при данном виде контроля.

1. Основные положения и постановка задачи

В фундаментальной работе [22] рассматривается задача построения самодвойственных логических схем, защищенных по отношению к неисправностям. Введено понятие самодвойственно тестируемой по какому-либо выходу схемы неисправности из рассматриваемой модели неисправностей. Его можно перефразировать

следующим образом: *самодвойственно тестируемой по j -му выходу схемы неисправностью* называется такая неисправность, для которой существует хотя бы одна пара входных комбинаций, ортогональных по всем переменным, для которой неисправность проявляется в виде искажения значения функции, реализуемой на данном выходе, только на одной из комбинаций. *Неисправность из рассматриваемой модели называется самодвойственно тестируемой*, если она самодвойственно тестируема хотя бы по одному из ее выходов. Важным в данных определениях является то, что неисправность самодвойственно тестируема в том случае, если существует хотя бы одна пара комбинаций, при поступлении на входы устройства которой данная неисправность проявится в виде искажения функции только на одной из комбинаций.

Неисправность вызывает в схеме ошибку, которая либо компенсируется (маскируется), либо транслируется на один или несколько ее выходов. При этом неисправность при подаче на входы различных комбинаций будет транслироваться на выходы по-разному: для каких-то входных комбинаций она не будет вызывать искажений функций, для каких-то – наоборот. Поэтому в ряде случаев (например, при реализации отказоустойчивых устройств) целесообразно говорить не о возможности обнаружения ошибки хотя бы на одной из пар входных комбинаций, а о возможности обнаружения любых ошибок в функциях, реализуемых на выходах самодвойственных устройств.

В той же работе [22] введено понятие *самодвойственно защищенного по отношению к неисправности из заданной модели выхода* как выхода, для которого эта неисправность либо не приводит к появлению ошибки, либо если искажение возникает, то оно проявляется в виде искажения значения функции, реализуемой на выходе, только при подаче одной из комбинаций, входящих в пары ортогональных по всем переменным комбинаций. Это условие должно выполняться для всех пар входных комбинаций. Схема называется *самодвойственно защищенной от рассматриваемой неисправности*, если каждый выход этой схемы самодвойственно защищен от этой неисправности. Вводится также понятие *самодвойственно защищенного от ошибок по отношению к j -ому выходу логического элемента* – элемента, для которого j -ый выход самодвойственно защищен от всех ошибок данного элемента. Если каждый выход схемы самодвойственно защищен от всех ошибок рассматриваемого логического элемента, то данный элемент называется самодвойственно защищенным по отношению ко всем неисправностям из рассматриваемой модели. Далее в описываемой работе вводятся условия защищенности логических элементов схемы и предлагается алгоритм преобразования любой самодвойственной схемы в самодвойственно защищенную от проявления однонаправленных (монотонных) ошибок.

Данная преамбула весьма важна, поскольку при реализации самодвойственных схем с точки зрения

технической диагностики важно обеспечить их защищенность от проявления всех неисправностей и обеспечить обнаружение всех их проявлений в виде ошибок, возникающих на их выходах. Рассмотрим задачу определения условий обнаружения ошибок на выходах самодвойственных устройств, а также учета событий появления необнаруживаемых (компенсируемых, или маскируемых) ошибок.

Число входов устройства обозначим через n . Тогда число входных комбинаций равно 2^n . Входные комбинации соответствуют двоичным числам от $\langle 00 \dots 00 \rangle$ и $\langle 11 \dots 11 \rangle$, которые, в свою очередь, пронумеруем соответствующими им десятичными числами: $0, 1, \dots, 2^n - 1$. При построении самодвойственных устройств реализуется импульсный режим работы, поэтому входные комбинации подаются парами: первая комбинация $i \in \{0, 1, \dots, 2^{n-1} - 1\}$, а вторая комбинация – ортогональная по всем переменным с десятичным номером $2^n - 1 - i$. Далее, у самодвойственного устройства может быть m выходов. Обозначим принадлежность пары и конкретного значения функции, реализуемой на j -ом ($j \in \{1, 2, \dots, m\}$) выходе, верхним индексом j у конкретной пары и конкретного значения. Сами значения j -ой функции при поступлении векторов входных переменных i и $2^n - 1 - i$ обозначим через A_i^j и $B_{2^n - 1 - i}^j$. Конкретную пару входных комбинаций и значений вычисляемой j -ой функции, таким образом, обозначим через $P_{i/2^n - 1 - i}^j(A_i^j, B_{2^n - 1 - i}^j)$. Задача формулируется следующим образом: требуется установить формальные условия, при которых любые ошибки на выходах самодвойственных устройств будут обнаруживаться, а также оценить общее возможное количество ошибок, которое может быть не обнаружено при самодвойственном контроле.

2. Условия обнаружения ошибок при самодвойственном контроле цифровых устройств

Так как у самодвойственного устройства каждая реализуемая на выходах функция принадлежит классу самодвойственных булевых функций, имеет место следующее: $A_i^j \neq B_{2^n - 1 - i}^j$ [22]. Это следует непосредственно из особенностей самодвойственных булевых функций [10].

Утверждение 1. Ошибка на j -ом выходе самодвойственного устройства при поступлении на входы комбинаций i и $2^n - 1 - i$ обнаруживается тогда и только тогда, когда:

$$A_i^j \oplus B_{2^n - 1 - i}^j = 0. \quad (1)$$

Доказательство. Введем еще два обозначения: T – значение функции при отсутствии неисправностей (корректное значение); F – значение функции с ошибкой (некорректное значение). Тогда имеет место четыре случая для конкретной пары входных комбинаций: $P_{i/2^n - 1 - i}^j(T, T)$, $P_{i/2^n - 1 - i}^j(F, T)$, $P_{i/2^n - 1 - i}^j(T, F)$, $P_{i/2^n - 1 - i}^j(F, F)$. Случай $P_{i/2^n - 1 - i}^j(T, T)$ соответствует отсутствию ошибок в

вычислениях; остальные случаи соответствуют присутствию ошибки в вычислениях. Для случая $P_{i/2^n - 1 - i}^j(T, T)$, так как $A_i^j \neq B_{2^n - 1 - i}^j$ имеем $A_i^j \oplus B_{2^n - 1 - i}^j = 1$. Для случаев $P_{i/2^n - 1 - i}^j(F, T)$ и $P_{i/2^n - 1 - i}^j(T, F)$ получаем, что $A_i^j = B_{2^n - 1 - i}^j$ и $A_i^j \oplus B_{2^n - 1 - i}^j = 0$. Для случая $P_{i/2^n - 1 - i}^j(F, F)$ имеют место искажения функции на обеих входных комбинациях, а значит, A_i^j и $B_{2^n - 1 - i}^j$ поменяли свои значения: $A_i^j \neq B_{2^n - 1 - i}^j$ и $A_i^j \oplus B_{2^n - 1 - i}^j = 1$. Такая «двойная» ошибка при самодвойственном контроле обнаруживаться не будет. Обнаружатся те ошибки, для которых $A_i^j \neq B_{2^n - 1 - i}^j$. Следовательно, выражение (1) определяет условия для обнаружения ошибок при самодвойственном контроле цифрового устройства.

Из утверждения 1 непосредственно следует

Утверждение 2. Ошибка на j -ом выходе самодвойственного устройства обнаруживается тогда и только тогда, когда:

$$\forall i \in \{0, 1, \dots, 2^{n-1} - 1\}: A_i^j \oplus B_{2^n - 1 - i}^j = 0. \quad (2)$$

Доказательство. Если условие (1) выполняется для каждой пары $P_{i/2^n - 1 - i}^j(A_i^j, B_{2^n - 1 - i}^j)$, то все ошибки в вычислениях j -ой функции обнаруживаются.

До сих пор рассматривалось устройство с одним выходом. Рассмотрим устройство с m выходами.

Утверждение 3. Ошибка на выходах самодвойственного устройства при поступлении на входы комбинаций i и $2^n - 1 - i$ обнаруживается тогда и только тогда, когда:

$$\bigg\bigwedge_{i=1}^m (A_i^j \oplus B_{2^n - 1 - i}^j) = 0. \quad (3)$$

Доказательство. Если значения j -ой функции при поступлении на входы комбинаций i и $2^n - 1 - i$ корректны или оба неверны, то $A_i^j \neq B_{2^n - 1 - i}^j$ и $A_i^j \oplus B_{2^n - 1 - i}^j = 1$. В этом случае при самодвойственном контроле только j -ой функции такая «двойная» ошибка не обнаруживается. Однако если ошибка проявляется в виде «одиночного» искажения какой-либо другой функции, описывающей другой выход устройства, то $A_i^j = B_{2^n - 1 - i}^j$ и $A_i^j \oplus B_{2^n - 1 - i}^j = 0$ (случаи $P_{i/2^n - 1 - i}^j(F, T)$ или $P_{i/2^n - 1 - i}^j(T, F)$). Тогда, если значение хотя бы одной из m функций исказится только на одной комбинации из пары i и $2^n - 1 - i$, то и любая «двойная» ошибка других функций будет обнаружена на этой паре.

Утверждение 4. Ошибка на выходах самодвойственного устройства обнаруживается тогда и только тогда, когда:

$$\forall i \in \{0, 1, \dots, 2^{n-1} - 1\}: \bigg\bigwedge_{i=1}^m (A_i^j \oplus B_{2^n - 1 - i}^j) = 0. \quad (4)$$

Доказательство. Если условие (4) выполняется для каждой пары $P_{i/2^n - 1 - i}^j(A_i^j, B_{2^n - 1 - i}^j)$, то все ошибки в вычислениях обнаруживаются.

Условие утверждения 4 определяет самодвойственно защищенные устройства.

Аналогично в статье [22] сформулированы условия самодвойственной защищенности для логических схем, реализованных на стандартных функциональных

элементах при рассмотрении модели одиночных константных неисправностей их выходов.

Из утверждения 4 непосредственно следует

Утверждение 5. *Ошибка на выходах самодвойственного устройства не обнаруживается в том случае, если хотя бы для одного i не выполняется условие (4).*

Тогда становится ясным, что чем больше значение m , тем больше и вероятность того, что ошибка будет обнаружена при самодвойственном контроле. Однако при этом структура устройства должна быть таковой, чтобы имелись пути, связывающие внутренние элементы устройства с различными его выходами.

В том случае, если на выходах самодвойственного устройства при рассматриваемой модели неисправности допускается необнаруживаемая ошибка, то есть, устройство самодвойственно защищенным не является, можно схемотехническими методами добиться ее обнаружения. К примеру, возможна дополнительная организация контроля самодвойственного устройства по кодовым методам [20, 21].

Обозначим вектор значений функций, вычисляемых на выходах устройства (информационный вектор), через $\langle F \rangle = \langle f_m f_{m-1} \dots f_2 f_1 \rangle$. Дополнительно будем вычислять значения проверочных символов контрольного вектора для данного информационного вектора по правилам формирования проверочных символов какого-либо двоичного разделимого кода. Этот код обозначим через (m, k) , где m и k – число информационных и проверочных символов. Контрольный вектор обозначим как $\langle G \rangle = \langle g_k g_{k-1} \dots g_2 g_1 \rangle$. Тогда можно сформулировать условие обнаружения ошибок при контроле по двум диагностическим признакам (принадлежности каждой функции, формируемой на выходах устройства, классу самодвойственных булевых функций и принадлежности каждого кодового слова $\langle FG \rangle = \langle f_m f_{m-1} \dots f_2 f_1 g_k g_{k-1} \dots g_2 g_1 \rangle$ выбранному (m, k) коду) следующим образом (оно вытекает из предыдущих рассуждений).

Утверждение 6. *Ошибка при контроле самодвойственного устройства по двум диагностическим признакам будет обнаружена в случае, если выполнено условие (4), либо, если оно не выполнено для какой-либо пары i и $2^n - 1 - i$ входных комбинаций, но хотя бы на одной из них кодовое слово $\langle FG \rangle = \langle f_m f_{m-1} \dots f_2 f_1 g_k g_{k-1} \dots g_2 g_1 \rangle$ не принадлежит выбранному (m, k) коду:*

$$\begin{cases} \forall i \in \{0, 1, \dots, 2^{n-1} - 1\} : \bigoplus_{j=1}^m (A_i^j \oplus B_{2^n-1-i}^j) = 0; \\ \forall P_{i/2^n-1-i}^j (A_i^j, B_{2^n-1-i}^j) \in P_{ND}^j, (A_i^j \vee B_{2^n-1-i}^j) : \\ A_i^j, B_{2^n-1-i}^j \rightarrow \langle FG \rangle \notin C_{(m,k)}. \end{cases} \quad (5)$$

где P_{ND}^j – множество пар, на которых ошибка проявляется на обеих комбинациях i , тем самым, не обнаруживается; $P_{ND}^j = P^j \setminus (P_0^j \cup P_D^j)$, $P^j = \bigcup_{i=0}^{2^{n-1}} P_{i/2^n-1-i}^j (A_i^j, B_{2^n-1-i}^j)$ – множество пар, P_0^j – подмножество пар, на которых ошибка не проявляется, P_D^j – множество пар, на которых ошибка проявляется только на одной из двух

комбинаций i , тем самым, обнаруживается; $C_{(m,k)}$ – множество кодовых слов выбранного (m, k) кода.

Отдельно отметим, что случай применения схем сжатия на основе (m, k) кодов, например, описанных в [19], не относится к контролю вычислений по двум диагностическим признакам, а относится к случаю уменьшения числа наблюдаемых выходов устройства для контроля вычислений.

3. Число потенциально необнаруживаемых ошибок при самодвойственном контроле

Определим, какое число ошибок может быть не обнаружено при самодвойственном контроле.

Введем параметр γ – число входных комбинаций, при поступлении которых возникает искажение значения функции, реализуемой на выходе самодвойственного устройства: $\gamma \in \{0, 1, \dots, 2^n\}$. Будем учитывать, что γ характеризует кратность возникающих ошибок на полном множестве комбинаций аргументов функции. Число искажений с кратностью γ равно $N_\gamma = C_{2^n}^\gamma$. Общее же число возможных искажений определяется величиной $N = \sum_{\gamma=0}^{2^n} N_\gamma = \sum_{\gamma=0}^{2^n} C_{2^n}^\gamma = 2^{2^n}$. Число N существенно растет при увеличении n и уже при $n = 5$ является астрономическим (в табл. 1 приведены числа N_γ и N для случаев $n = 2 \dots 5$). Заметим, что оно равно числу булевых функций от n переменных [23].

Всегда обнаруживаются только одиночные ошибки (при $\gamma = 1$). Их число равно $N_1 = C_{2^n}^1 = 2^n$. Не обнаруживаются ошибки при $\gamma \in \{2, 3, \dots, 2^n\}$. К примеру, в табл. 2 и 3 приведены рассчитанные показатели ошибок в самодвойственных функциях от $n = 2$ и $n = 3$ входных переменных. Из анализа данных таблиц можно сделать вывод о том, что с ростом значения γ доли необнаруживаемых ошибок от общего числа ошибок с данной кратностью γ (величины $\delta_\gamma = \frac{N_\gamma^{ND}}{N_\gamma}$) не убывают.

Минимальное значение δ_γ для случаев $\gamma \in \{2, 3, \dots, 2^n\}$ достигается при самом первом значении $\gamma = 2$. Не обнаруживаются те ошибки с $\gamma > 2$, которые содержат в себе группы «двойных» необнаруживаемых искажений и искажений, возникающих на каких-либо иных входных комбинациях.

Для исключения необнаруживаемых при самодвойственном контроле ошибок необходимо исключить одновременные искажения при подаче на входы обеих комбинаций из пар $P_{i/2^n-1-i}^j (A_i^j, B_{2^n-1-i}^j)$. Всего существует 2^{n-1} пар для функции от n переменных. Таким образом, возможно $N_2^{ND} = 2^{n-1}$ вариантов возникновения «двойных» ошибок. Общее же число таких ошибок в функции от n переменных определяется величиной

$$N_2 = C_{2^n}^2 = \frac{2^n!}{(2^n-2)!2!} = \frac{(2^n-2)!(2^n-1)2^n}{(2^n-2)!2!} = 2^{n-1}(2^n-1).$$

Доля таких ошибок равна:

$$\delta_2 = \frac{2^{n-1}}{C_{2^n}^2} = \frac{2^{n-1}}{2^{n-1}(2^n - 1)} = \frac{1}{2^n - 1}.$$

При увеличении n и в пределе при $n \rightarrow \infty$ имеем:

$$\lim_{n \rightarrow \infty} \delta_2 = \lim_{n \rightarrow \infty} \frac{1}{2^n - 1} = 0.$$

Табл. 1. Число ошибок, возникающих на γ выходах самодвойственного устройства

γ	n			
	2	3	4	5
0	1	1	1	1
1	4	8	16	32
2	6	28	120	496
3	4	56	560	4960
4	1	70	1820	35960
5	—	56	4368	201376
6	—	28	8008	906192
7	—	8	11440	3365856
8	—	1	12870	10518300
9	—	—	11440	28048800
10	—	—	8008	64512240
11	—	—	4368	129024480
12	—	—	1820	225792840
13	—	—	560	347373600
14	—	—	120	471435600
15	—	—	16	565722720
16	—	—	1	601080390
17	—	—	—	565722720
18	—	—	—	471435600
19	—	—	—	347373600
20	—	—	—	225792840
21	—	—	—	129024480
22	—	—	—	64512240
23	—	—	—	28048800
24	—	—	—	10518300
25	—	—	—	3365856
26	—	—	—	906192
27	—	—	—	201376
28	—	—	—	35960
29	—	—	—	4960
30	—	—	—	496
31	—	—	—	32
32	—	—	—	1
N	16	256	65536	4294967296

Табл. 2. Показатели ошибок в самодвойственных функциях от $n=2$ переменных

Показатель	γ				
	0	1	2	3	4
N_{γ}^{ND}	0	0	2	4	1
N_{γ}	1	4	6	4	1
δ_{γ}	0	0	0,333	1	1

Табл. 3. Показатели ошибок в самодвойственных функциях от $n=3$ переменных

Показатель	γ								
	0	1	2	3	4	5	6	7	8
N_{γ}^{ND}	0	0	4	24	52	56	28	8	1
N_{γ}	1	8	28	56	70	56	28	8	1
δ_{γ}	0	0	0,143	0,429	0,743	1	1	1	1

К примеру, в табл. 4 приведены данные для некоторых значений n .

Табл. 4. Характеристики «двойных» ошибок

n	N_2^{ND}	N_2	δ_2
2	2	6	0,333
3	4	28	0,143
4	8	120	0,067
5	16	496	0,032
...	...	...	...
10	512	523776	0,001

Таким образом, в реальных практических приложениях при самодвойственном контроле вычислений чем больше число аргументов n , тем выше вероятность не обнаружения ошибки. Однако, с другой стороны, чем больше число функций m , тем вероятность обнаружить ошибку выше. Для реальных устройств требуется анализ их структур для оценки показателей обнаружения ошибок.

4. Экспериментальные результаты

Покажем на простейшем примере, за счет чего контроль по двум диагностическим признакам позволяет увеличить число тестовых входных комбинаций для устройства среди рабочих.

Рассматривалась следующая несамодвойственная схема (рис. 1).

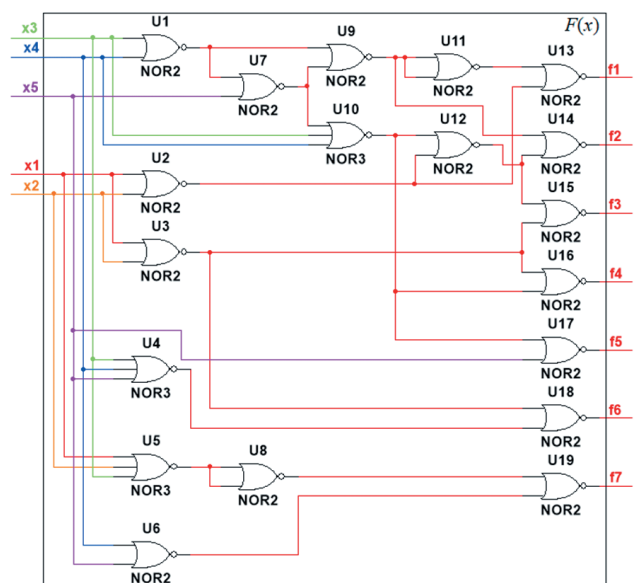


Рис. 1. Исходная схема $F(x)$

В статье [24] представлен метод организации СВК по двум диагностическим признакам – самодвойственности вычисляемых функций и принадлежности формируемого кодового слова модифицированному коду Хэмминга (коду Сяо). Доказано, что для числа выходов устройства $m = 7$ можно подобрать способ построения такого кода Сяо, для которого кодер будет самодвойственным устройством. Один из таких способов построения кода – использование следующей проверочной матрицы:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \quad (6)$$

Этот способ обозначим таким кортежем $\langle 7, 11, 13, 14, 19, 21, 22 \rangle$, где каждое десятичное число определяет

двоичное число, записанное в соответствующем столбце проверочной матрицы.

Преобразуем схему, приведенную на рис. 1, в самодвойственную путем замены каждого логического элемента самодвойственным аналогом [10]. Преобразованная схема приведена на рис. 2. Ясно, что она может быть оптимизирована, однако в данной задаче в этом нет необходимости.

Построим СВК для рассматриваемой схемы на основе кода Сяо с проверочной матрицей (6) и протестируем ее работу с контролем вычислений по двум диагностическим признакам на основании структуры из [24]. Группу элементов, реализующих самодвойственный аналог, будем отождествлять с исходным логическим элементом. Например, на рис. 2 выделен самодвойственный аналог элемента U10.

Объект диагностирования $F(x)$, имеющий в рассматриваемом случае $t = 5$ рабочих входов и один допол-

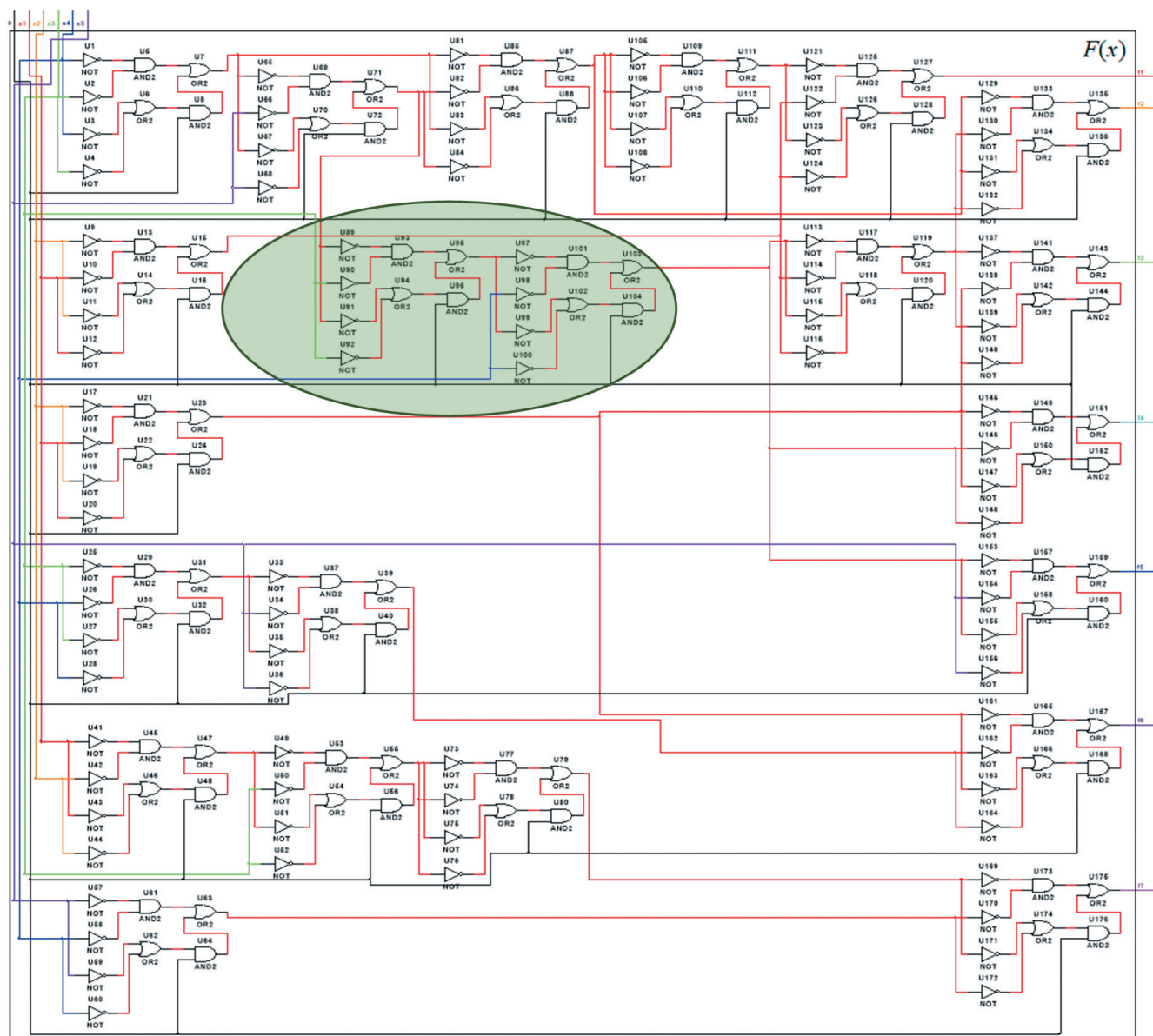


Рис. 2. Самодвойственный аналог схемы $F(x)$

можно контролировать по признаку самодвойственности, для чего реализуется схема контроля самодвойственности сигналов. Она образована из пяти устройств *SSC*, каждый из которых контролирует вычисления на одном выходе кодера, а также из компаратора *5TRC1*, позволяющего сжимать пять контрольных сигналов в один. На выходах данного устройства осуществляется контроль вычислений по признаку самодвойственности. Выходы двух устройств контроля подключены к единственному *TRC*, выходы которого являются контрольными выходами СВК – выходами z^0 и z^1 .

Используя программную среду Multisim, авторы реализовали СВК для схемы, изображенной на рис. 2 по структуре, приведенной на рис. 3. Самопроверяемое самодвойственное устройство приводится на рис. 4. Элементы на рисунке достаточно мелкие. Он приведен здесь для понимания того, как спроектировано самопроверяемое самодвойственное устройство.

Для представленного устройства производилось моделирование одиночных константных неисправ-

ностей (*stuck-at faults*) [26] выходов внутренних логических элементов – аналогов элементарных логических элементов. В ходе эксперимента исследовались особенности обнаружения вызываемых неисправностями объекта диагностирования ошибок на его выходах. При этом контрольные сигналы выводились с точек, показанных на рис. 4, – именно они представляют интерес.

Для примера рассмотрим тестирование неисправности вида «константа 1» на выходе аналога элемента U10 (см. рис. 2). На рис. 5 они обозначены следующим образом: *TRC7* – выходы подсхемы контроля самодвойственности, *TRC8* – выходы подсхемы контроля принадлежности кодовых слов коду Сяо, *TRC9* – контрольные выходы СВК. На рис. 6 более подробно выделена часть временных диаграмм, по которой можно проследить, как обнаруживались ошибки на выходах объекта диагностирования в трех контрольных точках.

Особенностью самодвойственных схем является импульсный режим функционирования при подаче на

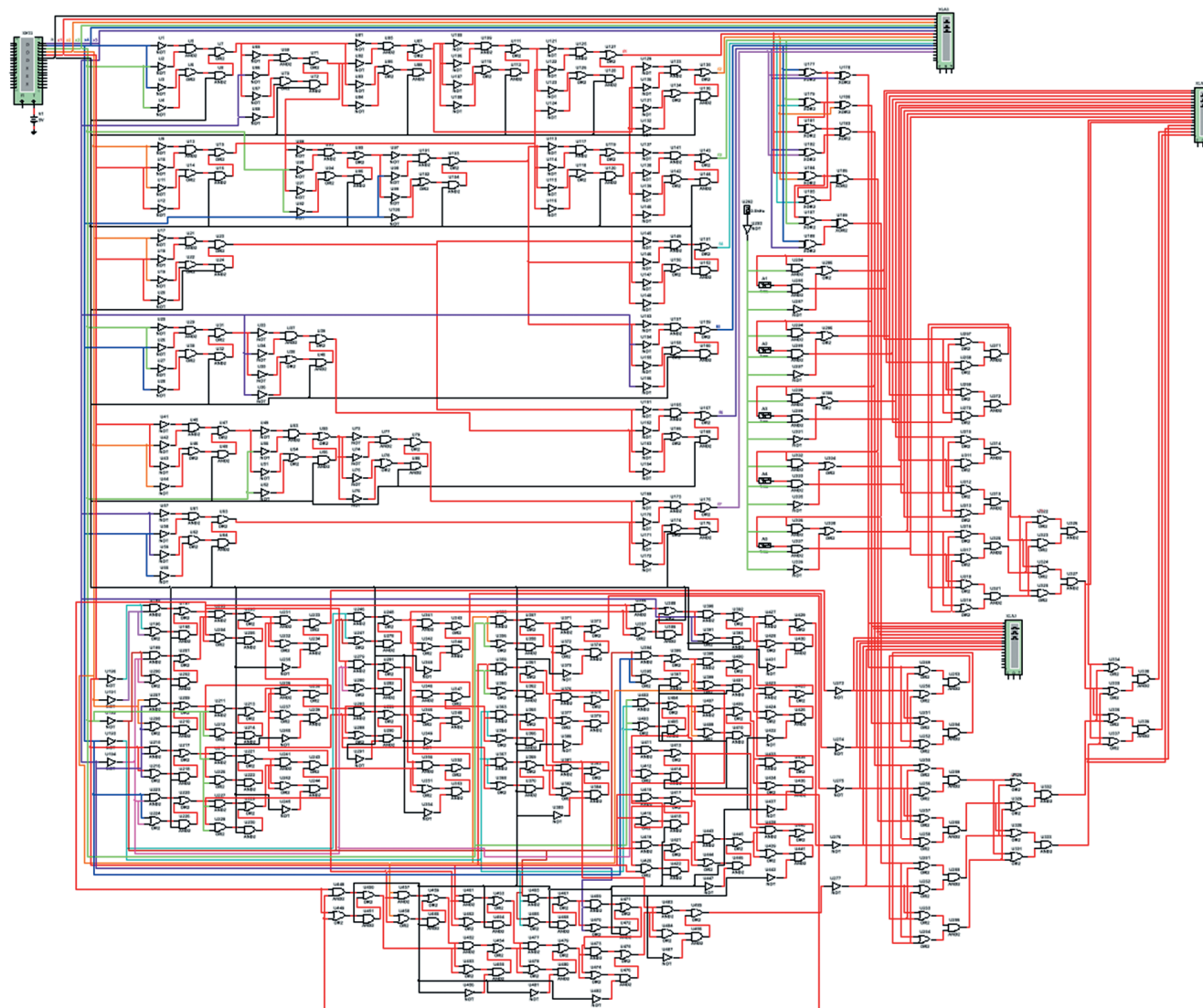


Рис. 4. Устройство с СВК

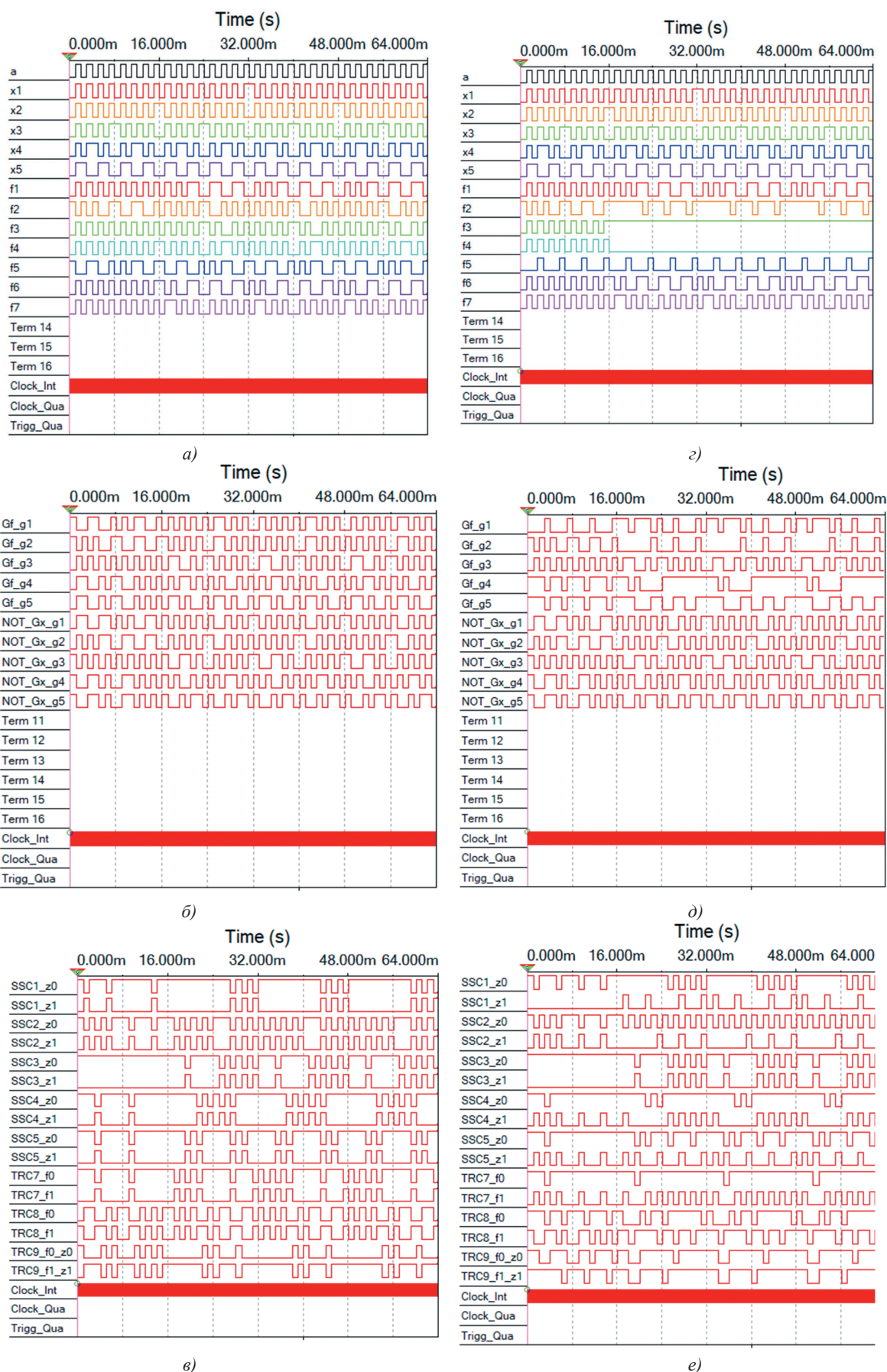


Рис. 5. Временные диаграммы работы устройства: а) сигналы на выходах устройства $F(x)$ при отсутствии неисправностей; б) сигналы на выходах устройств $G(f), G(x)$ при отсутствии неисправностей; в) сигналы на контрольных выходах $SSC1, SSC2, SSC3, SSC4, SSC5, TRC7, TRC8, TRC9$ при отсутствии неисправностей; г) сигналы на выходах устройства $F(x)$ при неисправности типа «константа 1» на выходе элемента $U10$; д) сигналы на выходах устройств $G(f), G(x)$ при неисправности типа «константа 1» на выходе элемента $U10$; е) сигналы на контрольных выходах $SSC1, SSC2, SSC3, SSC4, SSC5, TRC7, TRC8, TRC9$ при неисправности типа «константа 1» на выходе элемента $U10$

входы пар комбинаций, в которых вторая комбинация ортогональна по всем переменным по отношению к первой. На диаграмме зафиксирована работа на всех 32 парах комбинаций $\langle a x_1 x_2 x_3 x_4 x_5 \rangle$, подаваемых последовательно: $\langle 000000 \rangle$, $\langle 111111 \rangle$, $\langle 000001 \rangle$, $\langle 111110 \rangle$, ..., $\langle 011111 \rangle$, $\langle 100000 \rangle$.

На диаграмме (рис. 6) черным маркером выделены такты, соответствующие комбинациям, на которых неисправность фиксируется в соответствующей контрольной точке.

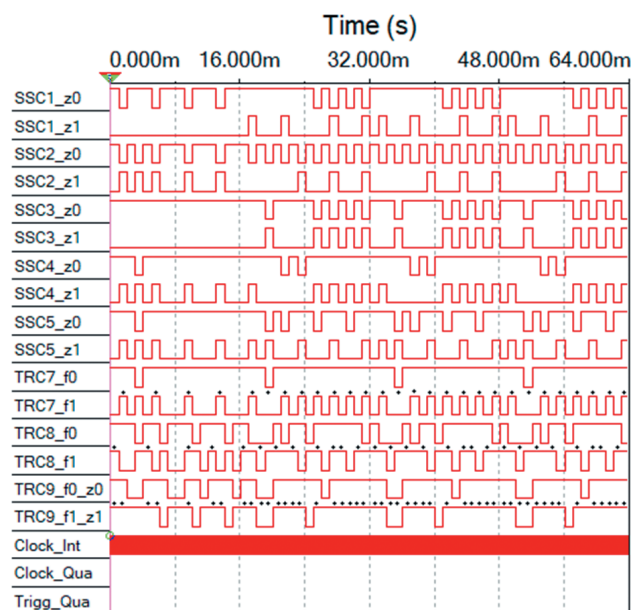


Рис. 6. Диаграмма работы устройства с СВК с неисправностью типа «константа 1» на выходе самодвойственного аналога элемента U10

В качестве примера объясним, за счет чего обнаруживается ошибка при подаче на входы самой первой пары комбинаций (первый такт на временных диаграммах рис. 5 и 6). Из сравнения диаграмм на рис. 5, в) и е) следует, что на первой комбинации тестеры самодвойственности не фиксируют ошибку. Она была бы пропущена, если бы не было подсхемы контроля по признаку принадлежности формируемых кодовых слов кодам Сяо. Обратим внимание на рис. 5, б) и д) – в первом такте меняются значения проверочных символов, что и приводит к фиксации ошибки в подсхеме контроля по кодам Сяо. Как итог – ошибка обнаруживается. Противоположно работают тестеры на второй комбинации из пары – тестер самодвойственности фиксирует ошибку, а тестер кода Сяо – нет. Однако на выходах СВК ошибка обнаруживается. Таким образом, контроль по двум диагностическим признакам позволяет повысить контролепригодность СВК в части наблюдаемости ошибок [18, 24].

Всего имеется 64 комбинации. Рассматриваемая неисправность тестируется на 28 комбинациях при контроле только по признаку самодвойственности и на 28 комбинациях (43,75 % всех комбинаций) при контроле только по признаку принадлежности кодовых комбинаций коду

Сяо. При контроле по двум признакам тестовых комбинаций среди всех остальных становится 49 (76,56 % всех комбинаций). Аналогичный эффект в повышении контролепригодности в части наблюдаемости неисправностей на входных комбинациях наблюдается и для всех остальных элементов в структуре самодвойственной схемы.

Следует отметить, что приведенный выше пример только демонстрирует эффект в части повышения контролепригодности схем за счет использования двух диагностических признаков, однако в дальнейшем важным этапом является постановка и проведение многочисленных экспериментов с так называемыми контрольными схемами (benchmarks), повсеместно используемыми для проверки и демонстрации эффективности разрабатываемых методов технической диагностики [27, 28].

Заключение

Организация контроля вычислений с использованием свойств самодвойственных функций позволяет реализовывать самопроверяемые цифровые устройства, которые как компоненты входят в более сложные управляющие микроэлектронные и микропроцессорные комплексы. При этом для обеспечения свойств самопроверяемости и контролепригодности их структур требуется выполнение особых условий при синтезе.

В случае, если ошибка возникнет на обеих комбинациях из подаваемой пары комбинаций на входы устройства, она не будет зафиксирована тестером самодвойственности. Многочисленные эксперименты с произвольными комбинационными схемами показали, что данное событие может оказаться частым. Кроме того, расчеты показывают, что существует большое число сочетаний ошибок, возникающих на выходах устройств, при которых они не фиксируются тестерами самодвойственности. Чем больше число входов у устройства, тем выше потенциальное число маскируемых ошибок. Однако использование специальных схемотехнических приемов, например, контроля вычислений не только по признаку самодвойственности формируемых сигналов, но и по принадлежности кодовых слов заранее выбранным блоковым кодам, позволяет перевести ошибку из класса необнаруживаемых в класс обнаруживаемых. Приведенный в статье пример отлично демонстрирует увеличение числа обнаруживаемых тем самым ошибок.

В дальнейших исследованиях методов синтеза самопроверяемых самодвойственных устройств следует учитывать особенности обнаружения ошибок при контроле по признаку самодвойственности сигналов. В самом выбранном признаке как раз и кроется наиболее весомый недостаток – маскировка ошибки при ее проявлении на обеих комбинациях из пары. Сокращение и даже исключение таких ошибок может достигаться различными путями: выделением групп контролепригодных выходов, реконfigurацией структуры объекта диагностирования в контролепригодную

структуру, контролем отдельных сигналов на выходах объекта диагностирования, выделением дополнительных диагностических признаков.

Библиографический список

1. Согомонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. М.: Радио и связь, 1989. 208 с.
2. Lala P.K. Self-Checking and Fault-Tolerant Digital Design. San Francisco: Morgan Kaufmann Publishers, 2001. 216 p.
3. Fujiwara E. Code Design for Dependable Systems: Theory and Practical Applications. John Wiley & Sons, 2006. 720 p.
4. Ubar R., Raik J., Vierhaus H.-T. Design and Test Technology for Dependable Systems-on-Chip (Premier Reference Source). Information Science Reference, Hershey, New York, IGI Global, 2011. 578 p.
5. Дрозд А.В., Харченко В.С., Антошук С.Г. и др. Рабочее диагностирование безопасных информационно-управляющих систем / Под ред. А.В. Дрозда и В.С. Харченко. Харьков: Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2012. 614 с.
6. Ярмолик В.Н. Контроль и диагностика вычислительных систем. Минск: «Бестпринт», 2019. 387 с.
7. Матросова А.Ю., Чернышов С.В., Ким О.Х., Николаева Е.А. Построение последовательности, обнаруживающей робастно тестируемые неисправности задержек путей в схемах с памятью // Автоматика и телемеханика. 2021. № 11. С. 148-168. DOI: 10.31857/S0005231021110106
8. Reynolds D.A., Meize G. Fault Detection Capabilities of Alternating Logic // IEEE Transactions on Computers. 1978. Vol. C-27. Issue 12. Pp. 1093-1098. DOI: 10.1109/TC.1978.1675011
9. Аксенова Г.П. Восстановление в дублированных устройствах методом инвертирования данных // Автоматика и телемеханика. 1987. № 10. С. 144-153.
10. Гессель М., Мошанин В.И., Сапожников В.В. и др. Обнаружение неисправностей в самопроверяемых комбинационных схемах с использованием свойств самодвойственных функций // Автоматика и телемеханика. 1997. № 12. С. 193-200.
11. Crama Y., Hammer P.L. Boolean Function: Theory, Algorithms, and Applications. Cambridge University Press, 2011. 687 p.
12. Гессель М., Морозов А.В., Сапожников В.В. и др. Логическое дополнение – новый метод контроля комбинационных схем // Автоматика и телемеханика. 2003. № 1. С. 167-176.
13. Гессель М., Морозов А.В., Сапожников В.В. и др. Контроль комбинационных схем методом логического дополнения // Автоматика и телемеханика. 2005. № 8. С. 161-172.
14. Гессель М., Дмитриев А.В., Сапожников В.В. и др. Самотестируемая структура для функционального обнаружения отказов в комбинационных схемах // Автоматика и телемеханика. 1999. № 11. С. 162-174.
15. Сапожников В.В., Сапожников Вл.В., Гессель М. Самодвойственные дискретные устройства. СПб: Энергоатомиздат (Санкт-Петербургское отделение), 2001. 331 с.
16. Сапожников В.В., Сапожников Вл.В., Валиев Р.Ш. Синтез самодвойственных дискретных систем. СПб: Элмор, 2006. 220 с.
17. Göessel M., Ocheretny V., Sogomonyan E. et al. New Methods of Concurrent Checking: Edition 1. Dordrecht: Springer Science+Business Media B.V., 2008. 184 p.
18. Ефанов Д.В., Погодина Т.С. Исследование свойств самодвойственных комбинационных устройств с контролем вычислений на основе кодов Хэмминга // Информатика и автоматизация. 2023. Т. 22. № 2. С. 349-392. DOI: 10.15622/ia.22.2.5
19. Ефанов Д.В., Погодина Т.С. Анализ эффективности схем встроенного контроля на основе оценки принадлежности вычисляемых функций классу самодвойственных и предварительного сжатия сигналов с применением линейных кодов // Программная инженерия. 2023. Т. 14. № 4. С. 175-186. DOI: 10.17587/prin.14.4.175-186
20. Efanov D., Sapozhnikov V., Sapozhnikov V.I. et al. Self-Dual Complement Method up to Constant-Weight Codes for Arrangement of Combinational Logical Circuits Concurrent Error-Detection Systems // Proceedings of 17th IEEE East-West Design & Test Symposium (EWDTS'2019), Batumi, Georgia, September 13-16, 2019. Pp. 136-143. DOI: 10.1109/EWDTS.2019.8884398
21. Efanov D.V., Pivovarov D.V. The Hybrid Structure of a Self-Dual Built-In Control Circuit for Combinational Devices with Pre-Compression of Signals and Checking of Calculations by Two Diagnostic Parameters // Proceedings of 19th IEEE East-West Design & Test Symposium (EWDTS'2021), Batumi, Georgia, September 10-13, 2021. Pp. 200-206. DOI: 10.1109/EWDTS52692.2021.9581019
22. Гессель М., Морозов А.А., Сапожников В.В. и др. Построение самопроверяемых комбинационных схем на основе свойств самодвойственных функций // Автоматика и телемеханика. 2000. № 2. С. 151-163.
23. Поспелов Д.А. Логические методы анализа и синтеза схем. М.: «Энергия», 1974. 368 с.
24. Ефанов Д.В., Погодина Т.С. Самодвойственные цифровые устройства с контролем вычислений по кодам Сяо // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2023. № 63. С. 118-136. DOI: 10.17223/19988605/63/14
25. Carter W.C., Duke K.A., Schneider P.R. Self-Checking Error Checker for Two-Rail Coded Data // United States Patent Office, filed July 25, 1968, ser. No. 747533, patented Jan. 26, 1971, N.Y. 10 p.
26. Багдади А.А.А., Хаханов В.И., Литвинова Е.И. Методы анализа и диагностирования цифровых устройств (аналитический обзор) // Автоматизированные системы управления и приборы автоматизации. 2014. № 166. С. 59-74.

27. Sentovich E.M., Singh K.J., Lavagno L. et al. SIS: A System for Sequential Circuit Synthesis // Electronics Research Laboratory, Department of Electrical Engineering and Computer Science, University of California, Berkeley, 4 May 1992. 45 p.

28. Sentovich E.M., Singh K.J., Moon C. et al. Sequential Circuit Design Using Synthesis and Optimization // Proceedings IEEE International Conference on Computer Design: VLSI in Computers & Processors, 11-14 October 1992, Cambridge, MA, USA, USA. Pp. 328-333. DOI: 10.1109/ICCD.1992.276282

References

1. Sogomonyan E.S., Slabakov E.V. [Self-checking devices and fault-tolerant systems]. Moscow: Radio i svyaz; 1989. (in Russ.)

2. Lala P.K. Self-Checking and Fault-Tolerant Digital Design. San Francisco: Morgan Kaufmann Publishers; 2001.

3. Fujiwara E. Code Design for Dependable Systems: Theory and Practical Applications. John Wiley & Sons; 2006.

4. Ubar R., Raik J., Vierhaus H.-T. Design and Test Technology for Dependable Systems-on-Chip (Premier Reference Source). Information Science Reference, Hershey (New York), IGI Global; 2011.

5. Drozd A.V., Kharchenko V.S., Antoshchuk S.G. et al. Drozd A.V., Kharchenko V.S., editors. [Operational diagnostics of secure information management systems]. National Aerospace University – “Kharkiv Aviation Institute”, NAU “KhAI”; 2012. (in Russ.)

6. Yarmolik V.N. [Supervision and diagnostics of computer systems]. Minsk: “Bestprint”; 2019. (in Russ.)

7. Matrosova A.Y., Chernyshov S.V., Kim O.K., Nikolaeva E.A. Constructing a sequence detecting robustly testable path delay faults in sequential circuits. *Automation and Remote Control* 2021;11:1949-1965. DOI: 10.31857/S0005231021110106. (in Russ.)

8. Reynolds D.A., Meize G. Fault Detection Capabilities of Alternating Logic. *IEEE Transactions on Computers* 1978;C-27(12):1093-1098. DOI: 10.1109/TC.1978.1675011.

9. Aksenova G.P. [Restoration in redundant devices using data inversion]. *Automation and Remote Control* 1987;10:144-153. (in Russ.)

10. Gessel M., Moshanin V.I., Sapozhnikov V.V. et al. [Fault detection in self-checking combinational circuits using the properties of self-dual functions]. *Automation and Remote Control* 1997;12:193-200. (in Russ.)

11. Crama Y., Hammer P.L. Boolean Function: Theory, Algorithms, and Applications. Cambridge University Press; 2011.

12. Gessel M., Morozov A.V., Sapozhnikov V.V., Sapozhnikov V.I. Logic complement, a new method of checking the combinational circuits. *Automation and Remote Control* 2003;64(1):153-161. (in Russ.)

13. Goessel M., Morozov A.V., Sapozhnikov V.V., Sapozhnikov V.I. Checking combinational circuits by

the method of logic complement. *Automation and Remote Control* 2005;66(8):1336-1346. (in Russ.)

14. Gessel M., Dmitriev A.V., Sapozhnikov V.V., Sapozhnikov V.I. A self-testable structure for functional fault detection in combination circuits. *Automation and Remote Control* 1999;11:162-174. (in Russ.)

15. Sapozhnikov V.V., Sapozhnikov V.I., Goessel M. [Self-dual discrete devices]. St. Petersburg: Energoatomizdat (St. Petersburg branch); 2001. (in Russ.)

16. Sapozhnikov V.V., Sapozhnikov V.I., Valiev R.Sh. [Synthesis of self-dual discrete systems]. St. Petersburg: Elmor; 2006. (in Russ.)

17. Göessel M., Ocheretny V., Sogomonyan E. et al. New Methods of Concurrent Checking: Edition 1. Dordrecht: Springer Science+Business Media B.V.; 2008.

18. Efanov D.V., Pogodina T.S. Properties Investigation of Self-Dual Combinational Devices with Calculation Control Based on Hamming Codes. *Informatics and Automation* 2023;22(2):349-392. DOI: 10.15622/ia.22.2.5. (in Russ.)

19. Efanov D. V., Pogodina T. S. Efficiency Analysis of Concurrent Error-Detection Circuits on the Basis of Assessment by Belonging of Calculated Functions to Self-Dual Class and Preliminary Compression of Signals Using Linear Codes. *Software Engineering* 2023;14(4):175-186. DOI: 10.17587/prin.14.175-186. (in Russ.)

20. Efanov D., Sapozhnikov V., Sapozhnikov V.I. et al. Self-Dual Complement Method up to Constant-Weight Codes for Arrangement of Combinational Logical Circuits Concurrent Error-Detection Systems. In: Proceedings of the 17th IEEE East-West Design & Test Symposium (EWDTS'2019); Batumi (Georgia); 2019. Pp. 136-143. DOI: 10.1109/EWDTS.2019.8884398.

21. Efanov D.V., Pivovarov D.V. The Hybrid Structure of a Self-Dual Built-In Control Circuit for Combinational Devices with Pre-Compression of Signals and Checking of Calculations by Two Diagnostic Parameters. In: Proceedings of the 19th IEEE East-West Design & Test Symposium (EWDTS'2021), Batumi (Georgia); 2021. Pp. 200-206. DOI: 10.1109/EWDTS52692.2021.9581019.

22. Gessel M., Morozov A.A., Sapozhnikov V.V., Sapozhnikov V.I. Design of self-testable combination circuits using the properties of self-dual functions. *Automation and Remote Control* 2000;2:151-163. (in Russ.)

23. Pospelov, D.A. [Logical methods of analysis and synthesis of schemes]. Moscow: Energia; 1974. (in Russ.)

24. Efanov D.V., Pogodina T.S. Self-dual digital devices with calculations testing by Hsiao codes. *Tomsk State University Journal of Control and Computer Science* 2023;63:118-136. DOI: 10.17223/19988605/63/14. (in Russ.)

25. Carter W.C., Duke K.A., Schneider P.R. Self-Checking Error Checker for Two-Rail Coded Data. United States Patent Office, filed July 25, 1968, ser. No. 747533, patented Jan. 26, 1971, N.Y.

26. Baghdadi A.A.A., Hahanov V.I., Litvinova E.I. Digital system analysis and diagnosis methods (analytical review). *Management Information System and Devices* 2014;166:59-74. (in Russ.)

27. Sentovich E.M., Singh K.J., Lavagno L. et al. SIS: A System for Sequential Circuit Synthesis. Electronics Research Laboratory, Department of Electrical Engineering and Computer Science, University of California, Berkeley; 1992.

28. Sentovich E.M., Singh K.J., Moon C. et al. Sequential Circuit Design Using Synthesis and Optimization. In: Proceedings IEEE International Conference on Computer Design: VLSI in Computers & Processors, 11-14 October 1992, Cambridge, MA (USA). Pp. 328-333. DOI: 10.1109/ICCD.1992.276282.

Сведения об авторах

Ефанов Дмитрий Викторович – доктор технических наук, профессор, Действительный член Международной Академии транспорта, член Института инженеров электротехники и электроники (IEEE), Санкт-Петербург, Российская Федерация, e-mail: TrES-4b@yandex.ru

Высшая школа транспорта Института машиностроения, материалов и транспорта Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого», профессор, ул. Политехническая, д. 29, лит. Б, Санкт-Петербург, РФ, 195251.

Кафедра «Автоматика, телемеханика и связь на железнодорожном транспорте» Федерального государственного автономного образовательного учреждения высшего образования «Российский университет транспорта», профессор, ул. Образцова, д. 9, стр. 9, Москва, Российская Федерация, 127994.

Кафедра «Автоматика и телемеханика» Ташкентского государственного транспортного университета, профессор, пр-д 1-й Темирюлчилар, 1, Мирабадский район, Ташкент, Республика Узбекистан, 100167.

ООО «Научно-исследовательский и проектный институт «Транспортной и строительной безопасности», заместитель генерального директора по научно-исследовательской работе, ул. Фучика, д. 4, лит. К, Санкт-Петербург, Российская Федерация, 192102.

Погодина Татьяна Сергеевна – студент, кафедра «Автоматика, телемеханика и связь на железнодорожном транспорте» Федерального государственного автономного образовательного учреждения высшего образования «Российский университет транспорта», ул. Образцова, д. 9, стр. 9, Москва, Российская Федерация, 127994, e-mail: pogodina-ts@mail.ru

About the authors

Dmitry V. Efanov, Doctor of Engineering, Professor, Full Member of the International Academy of Transportation, Member of the Institute of Electrical and Electronics Engineers (IEEE), Saint Petersburg, Russian Federation, e-mail: TrES-4b@yandex.ru.

Higher School of Transportation, Institute of Engineering, Materials, and Transportation, Peter the Great St. Petersburg Polytechnic University, Professor, 29, lit. B Politekhnikeskaya St., Saint Petersburg, 195251, Russian Federation.

Department of Railway Signalling and Telecommunications, Russian University of Transport, Professor, 9, bldg 9 Obraztsova St., Moscow, 127994, Russian Federation.

Department of Railway Signalling, Tashkent State Transport University, Professor, 1 Temiryolchilar St., Tashkent, 100167, Uzbekistan.

Research and Design Institute for Transportation and Construction Safety, Deputy Director General for Research, 4, lit. K Fuchika St., Saint Petersburg, 192102, Russian Federation.

Tatiana S. Pogodina, student, Department of Railway Signalling and Telecommunications, Russian University of Transport, 9, bldg 9 Obraztsova St., Moscow, 127994, Russian Federation, e-mail: pogodina-ts@mail.ru.

Вклад автора в статью

Ефановым Дмитрием Викторовичем проведен анализ основных достижений в теории синтеза самодвойственных самопроверяемых цифровых устройств, сформулированы и обоснованы условия обнаружения ошибок на выходах самодвойственных цифровых устройств при использовании при контроле вычислений признаков самодвойственности функций и принадлежности формируемых кодовых слов заранее выбранным блоковым равномерным кодам.

Погодиной Татьяной Сергеевной проведено моделирование самодвойственных цифровых схем и получены экспериментальные результаты, подтверждающие эффективность использования при контроле вычислений на их выходах признаков самодвойственности функций и принадлежности формируемых кодовых слов заранее выбранным блоковым равномерным кодам.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Оценка уровня надежности функционирования филиалов ПАО Россети России

Assessment of the functional reliability of branches of PAO Rosseti

Наумов И.В.^{1,2*}, Подъячих С.В.¹, Полковская М.Н.¹, Шерьязов С.К.³, Бастрон А.В.⁴
Naumov I.V.^{1,2*}, Podyachikh S.V.¹, Polkovskaya M.N.¹, Sheryazov S.K.³, Bastron A.V.⁴

¹Иркутский государственный аграрный университет имени А.А. Ежевского, Иркутская область, поселок Молодежный, Российская Федерация, ²Иркутский национальный исследовательский технический университет, Иркутск, Российская Федерация, ³Южно-Уральский государственный аграрный университет, Троицк, Российская Федерация, ⁴Красноярский государственный аграрный университет, Красноярск, Российская Федерация
¹Irkutsk State Agricultural University named after Ezhevsky, Molodezhny, Irkutsk Region, Russian Federation, ²National Research Irkutsk State Technical University, Irkutsk, Russian Federation, ³South Ural State Agrarian University, Troitsk, Russian Federation, ⁴Krasnoyarsk State Agrarian University, Krasnoyarsk, Russian Federation

*professornaumov@list.ru



Наумов И.В.



Подъячих С.В.



Полковская М.Н.



Шерьязов С.К.



Бастрон А.В.

Резюме. В статье представлен анализ динамики аварийных ситуаций в электрических сетях Единой энергетической системы (ЕЭС) России за 2014-2021 годы. Программные алгоритмы, разработанные авторами, использованы для аппроксимации рядов аварийных отключений. На основе этих алгоритмов произведен расчет и представлена визуализация изучаемых показателей. На основании методов корреляционного и регрессионного анализа рассчитаны параметры уравнений авторегрессии и тренда, используемых для прогнозирования аварийных отключений. В качестве объекта исследования рассмотрены режимы аварийной динамики в крупнейших российских сетевых компаниях напряжением 110 кВ и выше. Проанализированы данные о возникновении аварийных ситуаций в 23 объединениях электрических сетей, входящих в структуру ЕЭС России, за 2014-2021 годы. Определены проценты аварий на крупнейших предприятиях электрических сетей с учетом их протяженности, а также сезонных особенностей территорий, через которые проходят линии электропередачи. Кроме того, проанализированы данные об износе основных элементов сети, а также федеральные инвестиции в развитие исследуемой компании. Согласно исследованию, наиболее надежной оценкой реального состояния аварийных электрических сетей следует считать конкретный показатель, зависящий от протяженности сетей и уровня организации их эксплуатации. Оценка уровня износа исследуемых сетей показала, что наибольший износ соответствует ПАО «Россети Урала» (Екатеринбург, Россия) (более 60%), наименьший – АО «Россети Янтарь» (25%) (Калининград, Россия). При оценке сезонной составляющей как одного из критериев аварийности установлено, что наибольший ущерб приходится на летний период: июнь, июль и август. Выявлено, что уравнения авторегрессии и тренда могут быть использованы для прогнозирования исследуемых показателей в краткосрочной перспективе.

Abstract. The paper presents an analysis of emergency situation dynamics in the electrical networks of the Unified Energy System (UES) of Russia for the period between 2014 and 2021. The software algorithms developed by the authors were used for approximating a series of emergency outages. These algorithms were used to calculate and visualise the examined indicators. Methods of correlation and regression analysis were used to calculate the autoregressive parameters and trend equations used to predict emergency outages. The paper discusses the emergency dynamics modes in the largest Russian grid companies with voltages of 110 kV and above. The authors analyse data on the occurrence of emergency situations in 23 electric grid associations that are part of the UES of Russia for the period between 2014 and 2021. The percentages of accidents at the largest electrical network facilities were determined, taking into account their length, as well as the seasonal characteristics of the territories that the power lines run through. In addition, data on the deterioration of the key network elements, as well as federal investments in the development of the examined company were taken into account. According to the findings, a specific indicator that depends on the length of the networks and the quality of maintenance organization should be regarded as the most reliable assessment of the actual state of faulty electrical networks. An assessment of the deterioration level of the examined networks showed that the greatest deterioration is observed in PAO Rosseti Ural (Yekaterinburg, Russia) (more than 60%), while the lowest deterioration

is observed in JSC Rosseti Yantar (25%) (Kaliningrad, Russia). When assessing the seasonal component as one of the accident criteria, it was established that the greatest damage occurs in the summer period, i.e., in June, July, and August. It was revealed that the autoregression and trend equations can be used to predict the examined indicators in the short term.

Ключевые слова: надежность электроснабжения, прогнозирование надежности электрических сетей, отказ электрооборудования, аварийные отключения оборудования.

Keywords: reliability of power supply, prediction of electrical network reliability, electrical equipment failure, emergency equipment shutdown.

Для цитирования: Наумов И.В., Подъячих С.В., Полковская М.Н., Шерьязов С.К., Бастрон А.В. Оценка уровня надежности функционирования филиалов ПАО Россети России // Надежность. 2024. №2. С. 38-51. <https://doi.org/10.21683/1729-2646-2024-24-2-38-51>

For citation: Naumov I.V., Podyachikh S.V., Polkovskaya M.N., Sheryazov S.K., Bastron A.V. Assessment of the functional reliability of branches of PAO Rosseti. Dependability 2024;2:38 51. <https://doi.org/10.21683/1729-2646-2024-24-2-38-51>

Поступила: 31.10.2023 / **После доработки:** 16.04.2024 / **К печати:** 10.06.2024

Received on: 31.10.2023/ **Revised on:** 16.04.2024 / **For printing:** 10.06.2024

Введение

Электроэнергетические системы любых стран включают большое количество электростанций, линий электропередачи и трансформаторов, которые не могут работать безупречно в течение длительного времени из-за износа оборудования, природных и климатических условий, ошибок персонала и т.д. Бесперебойное электроснабжение потребителей является основной задачей функционирования электросетевого комплекса [6, 8, 19, 34, 36]. В то же время можно выделить ряд проблем, с которыми сталкивается электроснабжающая организация при передаче электроэнергии: потери при электропередаче; нарушение электромагнитной совместимости; особенности инфраструктуры; внешние атмосферно-климатические факторы; прерывание электроснабжения в силу различных причин; вопросы, связанные с законодательно оформленным землепользованием [5]; ветровые нагрузки [3, 9, 20] и т.д. Для оценки рисков сбоев в электросетях используются различные методы [1, 16, 26, 35]. Так, в [1] была предложена 3-ступенчатая модель определения индекса риска, которая учитывает корректирующие затраты на диспетчеризацию электроэнергии, а также затраты на электроэнергию, недоиспользуемую из-за возникновения событий отказов. При этом перечисленные проблемы являются следствием профессиональной работы генерирующих компаний, построивших свою деятельность на олигархических принципах. Во многих публикациях отмечается, что состояние элементов системы электроснабжения однозначно связано с неудовлетворительным качеством и рисками надежности электроснабжения [17]. В то же время, наряду с критериями, характеризующими уровень надежности электроснабжения, всегда учитывается реализация мер по повышению качества электроэнергии. В [24] было проведено комплексное моделирование наиболее популярных устройств FACTS для изучения потока мощностей.

Эти вероятностные характеристики отказов используются для оценки событий отказа, характеризующих уровень надежности. В то же время для расчета необходима многоуровневая информация о вероятностях этих случайных событий. Эта информация включает в себя не только данные о периодических отключениях, но и особенностях влияний климатических зон, через которые передается электроэнергия. Такая информация лежит в основе моделирования изменений показателей надежности элементов электросети с использованием интеллектуальных сетевых платформ [11] и нейронных сетей [12, 25].

По состоянию на 1 января 2020 года установленная мощность всех объектов по производству электроэнергии в России составляла 246 342,45 МВт. При этом доля тепловых электростанций – 66,82%, гидроэлектростанций – 20,24%, атомных электростанций – 12,31% и ветроэлектростанций – 0,07% [31]. В то же время, по итогам 2020 года ввод новых мощностей на электростанциях Российской Федерации с учетом электростанций промышленных предприятий составил 2067,77 МВт, в том числе: ввод новых мощностей – 1865,22 МВт; увеличение установленной мощности существующего генерирующего оборудования за счет его модернизации – 202,55 МВт [28]. В соответствии с Приказом Министерства энергетики Российской Федерации, «задачами формирования схемы и программы ЕЭС России являются обеспечение надежного функционирования ЕЭС России в долгосрочной перспективе». В то же время объем потребления электроэнергии в ЕЭС России в целом в 2020 году составил 1 033,718 млрд кВт·ч, что на 2,4% ниже аналогичного показателя 2019 года. В соответствии с [27] спрос на электрическую энергию в 2027 году в России составит 1 159,905 млрд кВт. Это превышает уровень потребления электроэнергии в 2020 году в России на 126,187 млрд кВт·ч. Другими словами, уровень потребления электроэнергии будет увеличиваться из года в год. В связи с этим средства доставки электрической энергии потребителю должны

соответствовать требуемым критериям надежности, чтобы снизить уровень недопоставки и уменьшить соответствующий экономический ущерб [6, 8, 19, 34, 36].

Единая энергетическая система (Федеральная сетевая компания Россети ФСК ЕЭС имеет публичное наименование ПАО «ФСК ЕЭС») (Москва, Россия). Эта организация была создана в соответствии с программой реформирования электроэнергетики Российской Федерации как организация по управлению Единой национальной (Общероссийской) электрической сетью (ЕЭС). В то же время, в соответствии с [29], ПАО «ФСК – Россети» признано национальным достоянием и гарантией государственной энергетической безопасности. На 2021 год протяженность линий электропередачи ПАО «ФСК – Россети», включая воздушные, кабельные и воздушно-кабельные линии электропередачи, составляет 149 тыс. км. Количество подстанций, которыми управляет компания, составляет 889. Мощность силовых трансформаторов – 352 ГВА. Поставка электроэнергии из сети ЕЭС потребителям услуг в 2020 году составила 535,7 млрд кВт·ч [23]. Структурно в состав ПАО «ФСК – Россети» входят 7 филиалов Магистральных электрических сетей (МЭС: Поволжье, Восток, Северо-Запад, Сибирь, Урал, Центр и Юг); 36 филиалов «Предприятия магистральных электрических сетей» и один филиал «Специализированная производственная база «Белая ржавчина» [22].

В большинстве стран для оценки уровня надежности электроснабжения Международный институт инженеров по электротехнике и электронике (IEEE) устанавливает специальные индексы, которые характеризуют взаимосвязь между количеством отказов (продолжительностью) и количеством потребителей, подключенных к шинам энергоцентров: SAIFI – средний индекс частоты прерываний системы; SAIDI – показатель средней продолжительности прерываний передачи электроэнергии; CAIDI – индекс средней продолжительности прерываний потребителей; STAIIDI – индекс общей средней продолжительности прерываний потребителей; CAIFI – средний индекс частоты прерываний работы потребителей; ASAI – средний индекс доступности услуг. Следует отметить, что в Минске в 2019 году SAIFI составил 0,5635; SAIDI – 0,5271. По оценкам экспертов, среднее значение этого показателя для европейских стран колеблется в диапазоне от 0,2 до 4,35. Например, индекс надежности энергосистем в следующих странах имеет средние значения: Австрия – 0,73; Великобритания – 0,53; Германия – 0,51; Норвегия – 1,59; Финляндия – 1,42 [10].

В России аналогом этого показателя является показатель средней продолжительности перерывов в передаче электрической энергии в каждом расчетном периоде регулирования в течение долгосрочного периода регулирования (ПП), определяемый по формуле [32]:

$$П_{\Pi} = \frac{T_{\Pi}}{N_{\Pi}}, \quad (1)$$

где T_{Π} – фактическая общая продолжительность всех перерывов в передаче электрической энергии по отно-

шению к потребителям услуг сетевой организации за расчетный период регулирования, час;

N_{Π} – максимальное количество точек подключения потребителей сетевой организации к электрической сети, шт.

Согласно [31] для сетей ФСК ЕЭС изменение значения этого показателя с 2015 по 2020 год включительно изменяется соответственно, как: 0,03602; 0,03548; 0,03495; 0,03443; 0,03391; 0,0334. В то же время износ основных средств, принадлежащих дочерним компаниям «Россетей», увеличился с 46,4% (показатель на начало 2016 года) до 52% на начало 2020 года [33]. И многочисленные аварийные ситуации, возникающие в результате этого износа, всегда связаны со значительным недостатком электроэнергии у потребителей.

Материалы и методы

Целью исследования является анализ динамики чрезвычайных ситуаций, возникающих в электрических сетях ЕЭС России за период 2014–2021 годы.

Достижение этой цели предполагает решение следующих задач:

- 1) проанализировать уровень повреждения исследуемых электрических сетей на основе конкретного показателя, учитывающего структурные особенности каждой компании;
- 2) установить, насколько сезонная составляющая года влияет на повреждение элементов электрических сетей;
- 3) выполнить математическую и статистическую обработку проанализированной информации о повреждениях с целью получения авторегрессионных уравнений, позволяющих с достаточной вероятностью провести превентивную оценку повреждений в электрических сетях отдельных компаний.

Общая протяженность линий электропередачи на конец 2017 года составила 2 323 990 км, в том числе линии электропередачи 110 кВ и выше – 395 078,3 км (17%) [18]. Уровень надежности электрических сетей напряжением 0,4–35 кВ неоднократно рассматривался во многих публикациях, где исследовались количество случаев сбоев, продолжительность перерывов и экономический ущерб от недопоставки электроэнергии и причины этих сбоев [4, 7, 14–16].

Для аппроксимации рядов аварийных отключений использованы разработанные авторами алгоритмы программирования, с помощью которых в среде Matlab, представлена визуализация исследуемых характеристик. С помощью методов корреляционного и регрессионного анализа рассчитаны параметры уравнений авторегрессии и тренда, применяемых для прогнозирования аварийных отключений.

Корреляционно-регрессионный анализ заключается в построении и анализе экономико-математической модели в форме уравнения регрессии (корреляционной зависимости), которая характеризует зависимость признака от его определяющих факторов.

Корреляционно-регрессионный анализ включает в себя следующие этапы:

- предварительный анализ (здесь формулируются основные направления всего анализа, определяется методология оценки показателя эффективности и перечень наиболее значимых факторов);
- сбор информации и ее первичная обработка;
- построение модели (один из наиболее важных этапов);
- оценка и анализ модели.

Задачи корреляционного анализа заключаются в выявлении наиболее важных факторов, влияющих на эффективную характеристику, измерении близости взаимосвязи между факторами, выявлении неизвестных причин взаимосвязи и оценке факторов, оказывающих максимальное влияние на результат.

Задачи регрессионного анализа заключаются в том, чтобы установить форму зависимости, определить уравнение регрессии и использовать его для оценки числа зависимых неизвестных отказов, предсказать возможные значения отказов с учетом заданных значений коэффициентов.

Результаты и обсуждение

В наших исследованиях мы неоднократно обращались к теме аварийности электрических сетей. В то же время была проведена оценка не только уровня износа отдельных элементов электрических сетей и причин их отказов, но также были предприняты попытки создать прогностические модели оценки повреждения отдельных элементов. Использовались разработанные программные продукты для превентивной оценки повреждений элементов электрических сетей [14–17, 38–39]. Но в подавляющем большинстве случаев в качестве объекта исследования были взяты различные филиальные сети Иркутской электросетевой компании (Иркутск, Россия). Впервые возник интерес к сравнению того, как уровень аварийности в узкотерриториальных электрических сетях может быть соотнесен с аналогичными характеристиками центральной электроэнергетической системы.

Анализ результатов будет проводиться в три этапа. На первом этапе анализа мы исследуем, на какие межрегиональные и региональные сетевые компании приходится наибольшее количество отказов и как это связано со структурой исследуемых сетей. На втором этапе будет рассмотрено, насколько уровень аварийности в электрических сетях связан с сезонностью периода наблюдения, и, наконец, на третьем этапе будет проведена математико-статистическая обработка полученных результатов с целью установления корреляций между критериями оценки чрезвычайных ситуаций.

На основании опубликованных данных [13, 37], согласно составленным программам, были получены диаграммы изменения числа аварийных ситуаций в электрических сетях исследуемых организаций по месяцам, начиная с 2014 года и заканчивая первыми 4 месяцами 2021 года (рис. 1).

Анализ полученных диаграмм показал следующее. За полные 7 лет и 4 месяца 2021 года в общей сложности 86 584,0 аварийных ситуаций произошло в электрических сетях разной продолжительности и, соответственно, с разными последствиями в зависимости от степени повреждения. Основываясь на анализе диаграмм (рис. 1), отметим 7 компаний, которые имеют самый высокий уровень аварийности за исследуемый период (рис. 2). Для упрощения анализа давайте проведем следующее цифровое обозначение исследуемых компаний (на 01 мая 2021 г.): «1» – ПАО «ФСК ЕЭС», «2» – ПАО «Россети Сибирь», «3» – ПАО «МРСК Центра», «4» – ПАО «Россети Волга», «5» – ОАО «МРСК Урала», «6» – ПАО «Россети Северный Кавказ» и «7» – АО «Россети Янтарь» (компания с наименьшим из рассматриваемых уровнем аварийности). Введем понятие среднегодовой удельной аварийности (Аварии/1 тыс. км):

$$A_{AAR} = \frac{N_{AAR}}{L}, \quad (2)$$

где N_{AAR} – среднегодовое (за исследуемый период) количество аварийных ситуаций;

L – протяженность электрических сетей, 1000 км.

Чтобы более достоверно оценить уровень повреждения исследуемых сетей, необходимо сравнить количественную оценку аварийных ситуаций с соответствующей протяженностью сетей. К сожалению, многочисленные источники обзора информации о протяженности сетей определенного класса напряжения показали, что данные отличаются. Обратим особое внимание на высоковольтные сети 110 кВ и выше, поскольку данные по аварийным ситуациям в анализируемых сетях представлены именно для этого класса напряжения.

Наиболее достоверная информация, на наш взгляд, представлена в материалах исследования [7], где установлено процентное отношение длины линий электропередачи с различными номинальными напряжениями к общей длине линий электропередачи. Исходя из таких соотношений, предполагая, что сети 110 кВ и выше составляют не менее 17% общей протяженности, и используя информацию об общей протяженности сетей ПАО «Россети» [21], получаем протяженность электрических сетей компаний: «1» – 25,99 тыс. км; «2» – 43,33 тыс. км; «3» – 70,86 тыс. км; «4» – 38,32 тыс. км; «5» – 23,22 тыс. км; «6» – 22,69 тыс. км и «7» – 2,5 тыс. км.

Как видно из рис. 2, ПАО «Федеральная сетевая компания – «1» занимает первое место по количеству аварий – 12 176,0 аварийных ситуаций, что составляет 14,06% от общего числа аварий. В состав этой компании входит 8 крупнейших электросетевых организаций. Со средним числом отказов за 7 лет (без учета 4 месяцев 2021 года), равным 1582, и полученной длиной изученных сетей, согласно выражению (1), $A_{AAR} = 60,87$. При этом, согласно утвержденной инвестиционной программе на 2017–2020 годы [28], на развитие сети «1» было выделено 289,1 млрд рублей. Второе место по количеству отказов

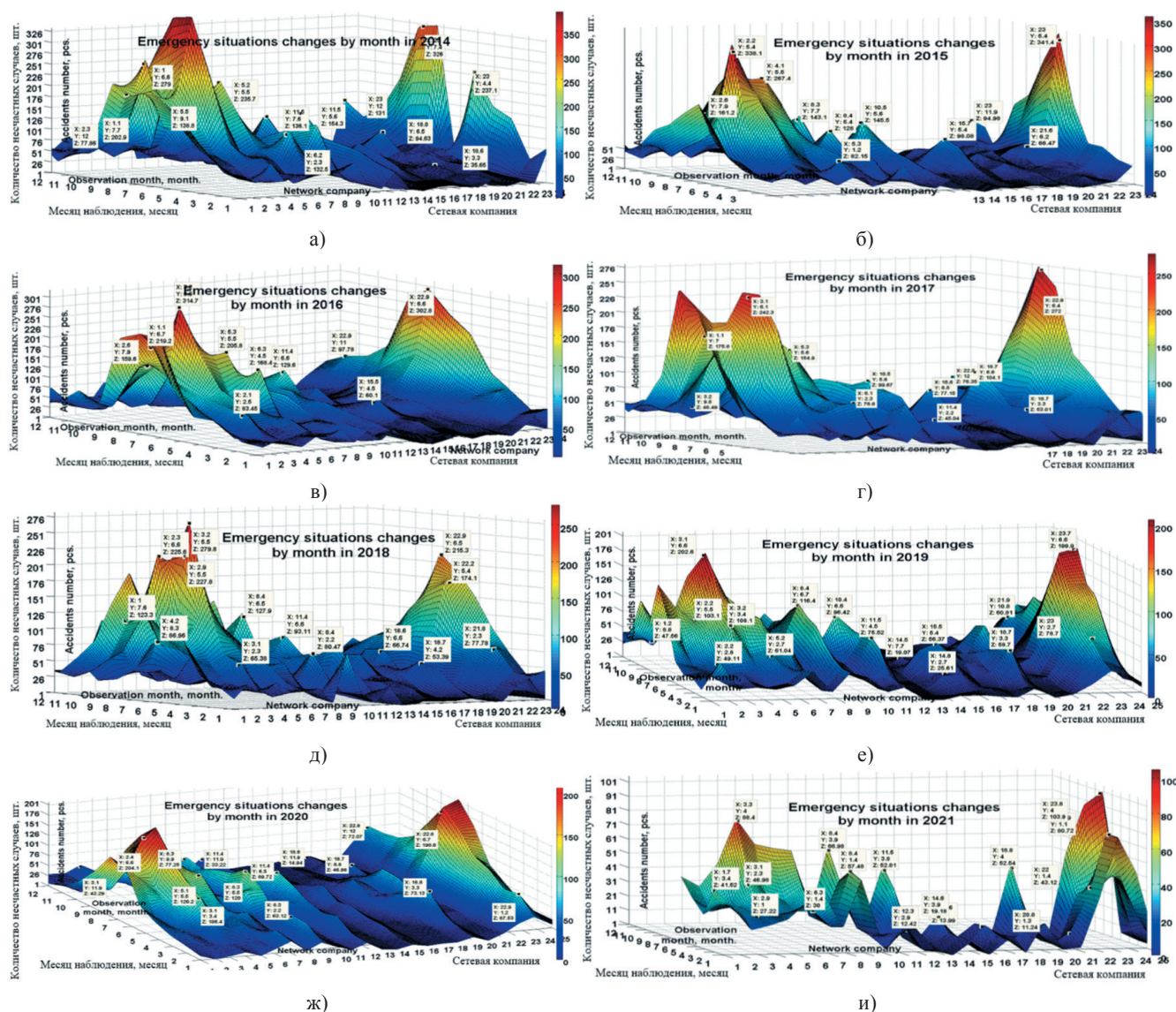


Рис. 1. Изменение аварийных ситуаций по месяцам года:
2014 (а); 2015 (б); 2016 (в); 2017 (г); 2018 (д); 2019 (е); 2020 (ж); 2021 (и)

занимает ПАО «2» – 10 537 аварийных ситуаций. Эта компания обеспечивает электроэнергией территорию площадью более 4 миллионов км² с населением около 10 миллионов человек. При среднегодовом уровне аварийности, равном 1477,0, показатель $A_{AAR} = 34,1$. Инвестиции в поддержку этих сетей составили 22,76 млрд рублей.

На третьем месте по количеству аварий находится ПАО «3», которое обеспечивает электроснабжение на площади 458 тыс. км². Согласно ежегодным отчетам [2] за последние 40–50 лет режимы загрузки этих сетей определялись пропускной способностью потребителей, устраняя при этом системные потоки между электростанциями. На территории, получающей электроэнергию от этой компании, проживает 13,2 миллиона человек (около 9% от общей численности населения России). Для этих сетей со средним ежегодным числом аварий, равным 1146, удельный коэффициент аварийности составил: $A_{AAR} = 16,17$. Как

видно, в этих сетях удельная аварийность значительно меньше, чем в первых двух компаниях. Инвестиции в эти сети составили 58,1 млрд рублей.

Четвертое место по количеству аварий принадлежит ПАО «4» – 7781 авария при общей протяженности сетей 38,32 тыс. км. Для этих сетей показатель $A_{AAR} = 29$. Пятое место по количеству аварий занимает ОАО «5» – 7121 шт., с $A_{AAR} = 43,81$. Шестое место занимают сети «6» – 6790 отказов, с $A_{AAR} = 42,75$. Инвестиции в развитие трех последних сетевых компаний составили соответственно: 23,98; 26,98 и 5,4 млрд рублей. Аварийность АО «7» и (дополнительного) ПАО «ТРК» (региональная компания Томска) составила, соответственно, 0,66%, а общее количество чрезвычайных ситуаций – 0,57% (рис. 2). Для сравнения, удельный коэффициент аварийности для АО «7» составляет $A_{AAR} = 32,06$.

Таким образом, с учетом показателя A_{AAR} иерархия аварийных ситуаций несколько меняется. Как видно из

анализа, инвестиции в значительной степени несопоставимы с отмеченным относительным уровнем аварийности исследуемых сетевых структур. Конечно, это связано с территориальными и климатическими особенностями регионов, через которые прокладываются маршруты электрических сетей. Кроме того, первостепенное значение имеет уровень износа основных элементов сетей. Например, согласно [21], уровень износа основного электросетевого оборудования (линий электропередачи и ПС) по ПАО «Россети» на 01 января 2020 года в целом составил 53,1%. Рассмотрим ситуацию с уровнем износа основных элементов исследуемых электрических сетей и сравним полученные данные с удельным уровнем аварийности и соответствующими инвестициями в развитие этих электрических сетей.

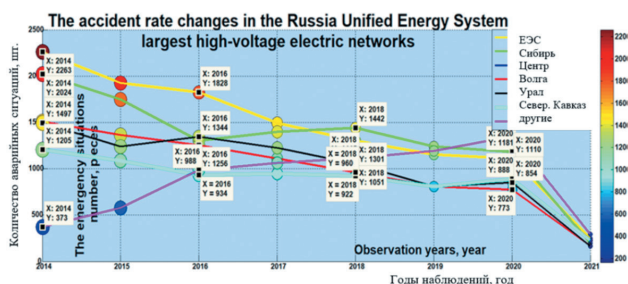


Рис. 2. Диаграммы изменения аварийности в крупнейших сетевых компаниях России

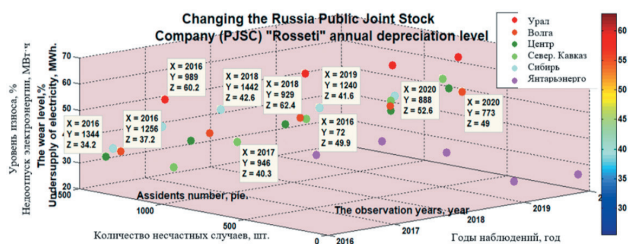


Рис. 3. Диаграммы изменения амортизации по Российскому ПАО «Россети»

Анализ графиков (рис. 2 и 3) показывает, что устойчивый рост износа наблюдается в трех компаниях: компании «6» (с 35,1% в 2016 году до 52,6% – в 2020 году), компании «4» (с 37,2 до 49%) и компании «3» – (с 34,2 до 49,3%). В то же время, принимая во внимание среднегодовой удельный уровень аварийности этих трех компаний (A_{AAR}), компания «6» должна считаться наиболее аварийной ($A_{AAR} = 42,75$). Две компании: «5» и «2» имеют нестабильный рост износа. В МРСК «5» износ увеличивается с 60,2% (2016 год) до 62,9 (2019 год), а к 2020 году он незначительно снизится до 61,2%. В компании «2» увеличение износа происходит с 37,8% (2016) до 42,6% (2018), затем, в 2019 году, наблюдается небольшое снижение (до 41,6%), а затем, в 2020 году, оно снова увеличивается до 42,6%.

Любопытная перемена происходит с ПАО «7». Как видно из рис. 3, износ этих сетей, начиная с 2017 года, явно снижается с 51% (2017 год) до 25,6% в 2020 году. В то же время количество аварийных ситуаций несрав-

нимо меньше, по сравнению с другими компаниями, хотя уровень аварийности неравномерно распределен по годам: в 2014 году их число составило 126, в 2015 году произошло снижение на 37,3%, а в 2016 году снижение к 2015 году составило 8,9%. В 2017 году еще одно снижение на 1,4%, в 2018 году количество аварийных ситуаций увеличилось на 7,8%, в 2019 году снова снижение на 16,9% (к 2017 году), а в 2020 году количество аварийных ситуаций увеличилось на 11,2%. Из вышеизложенного следует, что несмотря на небольшое количество аварий, по сравнению с другими компаниями, а также значительные инвестиции в развитие электрических сетей (на 10,4% больше, чем в сетях Северного Кавказа), это АО по удельной аварийности находится на 5-м месте.

Основываясь на этом выводе, сравним, как взаимосвязаны удельная аварийность, уровень износа и федеральные инвестиции в развитие исследуемых электрических сетей для 7 исследуемых компаний (рис. 4).

Анализ рис. 4 показывает, что в зависимости от среднего удельного уровня аварийности (A_{AAR}) (в порядке убывания) исследуемые компании расположены следующим образом. 1 место – компания «1», 2 – компания «5», 3 – компания «6», 4 – компания «2», 5 – компания «7», 6 – компания «4» и 7 место – компания «3». В то же время наибольший износ соответствует сетям компании «5» (61,74%), хотя инвестиции в развитие этих сетей составляют 9,33% от уровня инвестиций в сети компании «1», которые имеют меньший (на 9,54%) износ. Наименьший объем инвестиций (5,4 млрд рублей) был направлен в компанию «6», которая в то же время занимает 3-е место по удельной аварийности ($A_{AAR} = 42,75$) и такое же место по износу основных элементов сетей (44,52%).

Аналогичным образом, меньший объем инвестиций (6,03 млрд рублей) также был направлен на развитие сетей компании «7» (по сравнению с другими компаниями) несмотря на то, что как уровень аварийности, так и уровень износа этой компании находятся на довольно высоком уровне (соответственно: $A_{AAR} = 32,06$, износ – 39,22%). Компания «3», хотя и занимает второе место (после компании «1») по объему инвестиций (58,1 млрд рублей), но в то же время имеет самый низкий удельный уровень аварийности (16,17) при значительном (41,64%) износе. Этот факт свидетельствует о квалифицированном управлении эксплуатацией сетей, а также о рациональном использовании денежных вложений. Компании Сибири «2» и Поволжья «4» имеют примерно одинаковый уровень износа (41,1 и 44,12%), удельный уровень аварийности (34,1 и 29) и инвестиций (22,76 и 23,98 млрд рублей). Таким образом, как показывает анализ, политика управления инвестициями в развитие и совершенствование структуры отдельных сетевых компаний далека от совершенства и в значительной степени не учитывает особенности отдельных компаний.

Рассмотрим, какое влияние оказывает сезонная составляющая на уровень аварийности. Результаты анализа диаграмм на рис. 4 показывают, что наиболее «аварийными» месяцами года являются 7 месяцев:

с марта по сентябрь включительно. И этот вывод соответствует практически всем исследованным компаниям. Для большей наглядности представим диаграммы изменений количества несчастных случаев в наиболее «разрушительные» месяцы в течение исследуемого периода для компании «3» (рис. 5) и компании «1» (рис. 6).

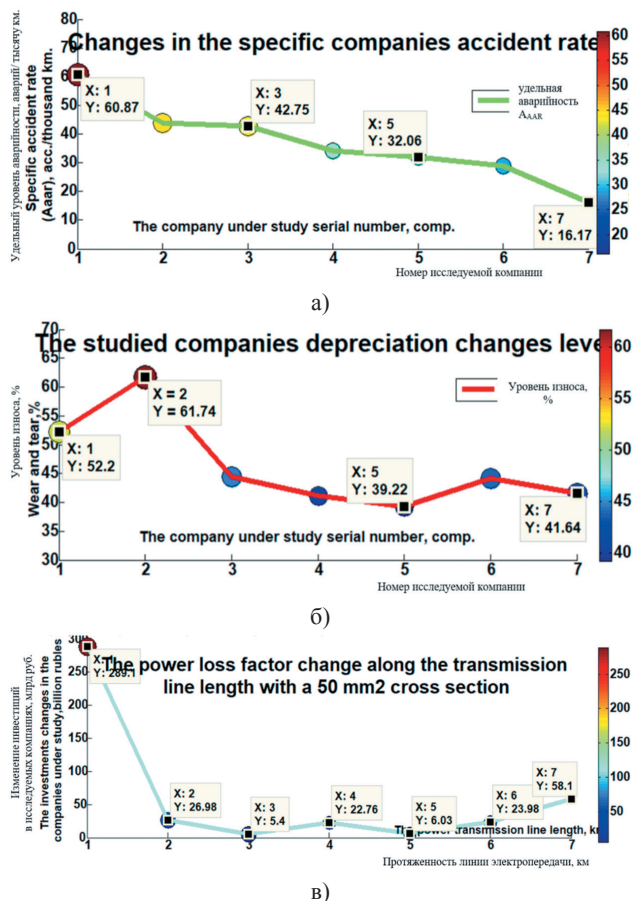


Рис. 4. Изменения среднего уровня аварийности (а), износа (б) и инвестиций (в) в исследуемых компаниях

Произведенный анализ (рис. 5 и 6) показал следующее. На долю этих семи месяцев (март, апрель, май, июнь, июль, август и сентябрь) в компании «3» прихо-

дится 81,23% всех аварийных ситуаций в 2014 году, в 2015 году – 74,6%; в 2016 году – 81,77%; в 2017 году – 78,81%; в 2018 году – 87,35%; в 2019 году – 81,09; в 2020 году – 80,68%. Для компании «1» соответственно: в 2014 году – 74,3%; в 2015 году – 79,61%; в 2016-78,06%; в 2017 году – 78,6%; в 2018 году – 76,17; в 2019 году – 80,75; в 2020 году – 78,83%.

Аналогичный анализ был проведен и для других компаний. Ситуация в компании «2» выглядит следующим образом: в 2014 году на эти месяцы приходится 84% всех чрезвычайных ситуаций; в 2015 году – 79,81%; в 2016 году – 87,48%; в 2017 году – 81,09%. В 2018 году – 78,16%; в 2019 году – 77,34% и в 2020 году – 86,28%.

В компании «5»: 2014 – 73,38%; 2015 – 81,81%; 2016 – 83,92%; 2017 – 82,3%; 2018 – 80,41%; 2019 – 78,92% а в 2020 году – 8,81%. Для компании «6»: 2014 – 73,78%; 2015 – 70,07%; 2016 – 68,74%; 2017 – 63,74%; 2018 – 68,33%; 2019 – 68,82%; 2020 – 67,12%. В компании «4»: 2014 – 80,23%; 2015 – 75,88%; 2016 – 78,58%; 2017 – 80,29%; 2018 – 81,56%; 2019 – 84,2%, а в 2020 году – 79,43%. Наибольшее количество аварийных ситуаций за каждые 12 месяцев наблюдения для компании «3» приходится на общее количество несчастных случаев в июне – 16,21% за все годы наблюдения; для «1» в июле – 16,83%; для «2» в июле – 18,32%; в «5» также в июле – 17,79%; в сетях компаний «6» – август (11,73%) и для компании «4» наибольшее количество аварий ежегодно происходит в августе – 16,84%.

В заключение, на третьем этапе произведена математико-статистическая обработка результатов аварий 6 крупнейших электросетевых компаний. Этот этап анализа необходим для превентивной оценки возможности аварийных ситуаций в исследуемых электрических сетях на определенную перспективу. Произведем оценку наличия тенденции в рейтинге аварийных отключений исследуемых компаний. Для нахождения уравнений регрессии использовалась программа «Статистика 10» [30]. Результирующие тенденции представлены в табл. 1.

Согласно тенденциям, количество отказов оборудования в электрических сетях ежегодно снижается, что подтверждается результатами анализа рис. 1 и 2.

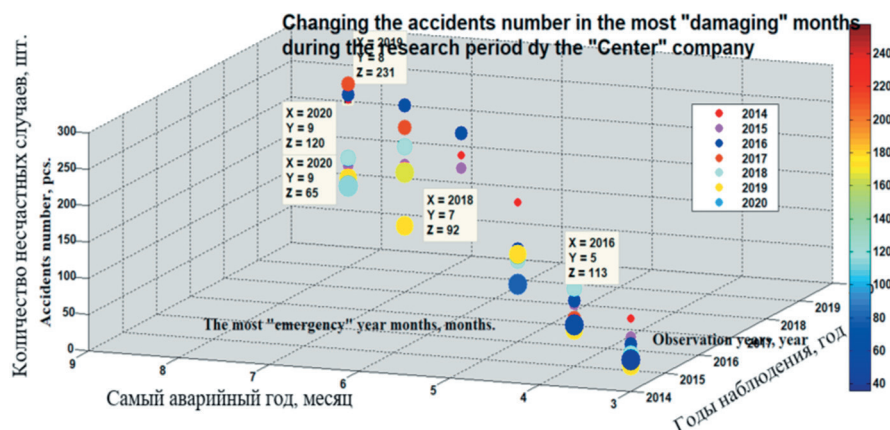


Рис. 5. Изменение количества аварийных ситуаций в сетях ПАО «МРСК Центра» за наиболее «повреждаемые» месяцы в 2014-2020 годах

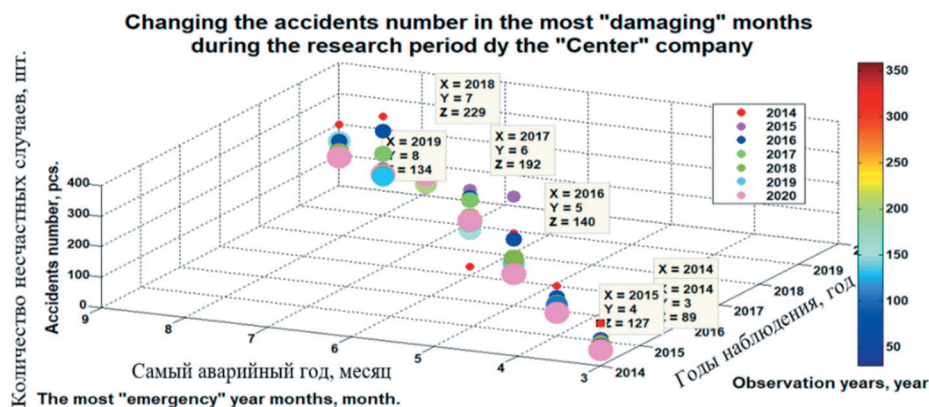


Рис. 6. Изменение количества аварийных ситуаций в ПАО «ФСК ЕЭС» за наиболее «повреждаемые» месяцы 2014-2020 гг.

Табл. 1. Уравнения трендов для годовых значений аварийности в структурных подразделениях электрических сетей «ЕЭС России» за 2014-2021 годы

Компания	Уравнение тренда	Коэффициент детерминации (R^2)
ПАО «МРСК Центра» («3»)	$y_t = -110,14t + 1586,6$	0,88
ОАО «МРСК Урала» («5»)	$y_t = -99,86t + 1416,7$	0,88
ПАО «Россети Волга» («4»)	$y_t = -128,79t + 1626,7$	0,99
ПАО «Россети Северный Кавказ» («6»)	$y_t = -45,75t + 1169,9$	0,74
ПАО «Россети Сибирь» («2»)	$y_t = -118,61t + 1955,3$	0,73
ПАО «ФСК ЕЭС» («1»)	$y_t = -142,21t + 2064,6$	0,91

В этой связи следует отметить, что увеличение федеральных инвестиций и их рациональное использование электросетевыми компаниями, безусловно, способствует снижению аварийности сетей. В то же время рациональное распределение этих средств должно быть обосновано компетентными аналитическими службами, которые должны отвечать за качество превентивных оценок ущерба электросетевым структурам различных компаний.

В то же время обращает на себя внимание тот факт, что при значениях исследуемых параметров для разных структурных подразделений за 12 месяцев (табл. 2) было получено разное количество трендов. Таким образом, для рядов аварийных отключений компании «1» тренды выделены для 10 месяцев, в то время как для компании «2» только для четырех, а для сетей компании «6» – для трех.

Табл. 2. Уравнения трендов по месяцам для исследуемых структурных подразделений электрических сетей ЕЭС России за 2014-2021 годы

Месяц	Уравнение тренда	Коэффициент детерминации R^2
ПАО «МРСК Центра» (3-я компания)		
Февраль	$y_t = 52,404t^{-0,225}$	0,61
Март	$y_t = 102,86t^{-0,488}$	0,90
Апрель	$y_t = 141,28t^{-0,443}$	0,64
Май	$y_t = 179,52t^{-0,327}$	0,75

Месяц	Уравнение тренда	Коэффициент детерминации R^2
Июнь	$y_t = 240,41t^{-0,229}$	0,51
Ноябрь	$y_t = 93,43t^{-0,544}$	0,58
ПАО «ФСК ЕЭС» (1-я компания)		
Январь	$y_t = 88,23t^{-0,454}$	0,80
Февраль	$y_t = 61,11t^{-0,215}$	0,66
Март	$y_t = 137,60t^{-0,448}$	0,95
Апрель	$y_t = 147,55t^{-0,25}$	0,52
Май	$y_t = 253,12t^{-0,361}$	0,75
Июнь	$y_t = 346,83t^{-0,233}$	0,71
Август	$y_t = 325,79t^{-0,458}$	0,72
Сентябрь	$y_t = 204,03t^{-0,384}$	0,97
Ноябрь	$y_t = 111,00t^{-0,381}$	0,75
Декабрь	$y_t = 131,46t^{-0,418}$	0,92
ПАО «Россети Северный Кавказ» (6-я компания)		
Март	$y_t = 116,32t^{-0,375}$	0,50
Апрель	$y_t = 127,28t^{-0,472}$	0,76
Август	$y_t = 156,73t^{-0,265}$	0,75
ОАО «МРСК Урала» (5-я компания)		
Январь	$y_t = 66,44t^{-0,607}$	0,83
Май	$y_t = 172,35t^{-0,371}$	0,68
Июнь	$y_t = 308,24t^{-0,596}$	0,64

Месяц	Уравнение тренда	Коэффициент детерминации R^2
Август	$y_t = 208,52 t^{-0,33}$	0,63
Сентябрь	$y_t = 104,09 t^{-0,202}$	0,58
Ноябрь	$y_t = 63,37 t^{-0,449}$	0,89
Декабрь	$y_t = 67,49 t^{-0,462}$	0,82
ПАО «Россети Волга» (4-я компания)		
Май	$y_t = 166,27 t^{-0,32}$	0,82
Июнь	$y_t = 265,59 t^{-0,435}$	0,81
Июль	$y_t = 178,91 t^{-0,203}$	0,52
Август	$y_t = 326,73 t^{-0,504}$	0,88
Сентябрь	$y_t = 214,35 t^{-0,362}$	0,62
Октябрь	$y_t = 78,71 t^{-0,547}$	0,65
Ноябрь	$y_t = 55,67 t^{-0,326}$	0,51
Декабрь	$y_t = 125,99 t^{-0,627}$	0,81
ПАО «Россети Сибирь» (2-я компания)		
Май	$y_t = 249,15 t^{-0,334}$	0,63
Июнь	$y_t = 368,00 t^{-0,346}$	0,68
Июль	$y_t = 385,59 t^{-0,31}$	0,86
Август	$y_t = 268,90 t^{-0,267}$	0,67

Следует отметить, что тенденция к снижению характерна для всех месяцев, при этом тренды имеют степенную форму, поскольку использование линейной зависимости подразумевает снижение рассматриваемого показателя до 0 и отрицательных значений, что недопустимо. Полученные зависимости могут быть использованы для прогнозирования в краткосрочной перспективе.

Для оценки надежности системы профилактического электроснабжения часто используются следующие законы распределения вероятностей: нормальный, гамма, Вейбулла, экспоненциальный и т.д. [30]. В этом случае необходимо, чтобы число исследуемого показателя было случайной величиной. Для выявления взаимосвязи между выборочными значениями или для опровержения этой гипотезы используется коэффициент автокорреляции, рассчитываемый по формуле:

$$R_\tau = \frac{\sum_{i=1}^{n-\tau} (x_i - \bar{x}_i) \cdot (x_{i+\tau} - \bar{x}_{i+\tau})}{\sigma_i \sigma_{i+\tau} (n - \tau - 1)}, \quad (3)$$

где n – размер выборки;

τ – порядок сдвига, изменяющийся от 0 до m ;

x_i – значения ряда от x_1 до $x_{n-\tau}$;

$\bar{x}_i$ и σ_i – среднее значение и стандарт для части выборки от 1 до $n-\tau$;

$x_{i+\tau}$ – значения ряда от $x_{1+\tau}$ до x_n ;

$\bar{x}_{i+\tau}$ и $\sigma_{i+\tau}$ – среднее значение и стандарт для части выборки от $1+\tau$ до n .

Расчет коэффициентов автокорреляции рядов аварийных отключений за весь период в рассматриваемых

структурных подразделениях показал, что в большинстве случаев внутрирядная взаимосвязь является сильной и значимой ($R_1 > 0,7$). В связи с этим построение вероятностных законов невозможно. В то же время для прогнозирования значений исследуемого показателя на краткосрочную перспективу могут быть использованы авторегрессионные зависимости, согласно которым последующее значение ряда зависит от предыдущего. Другими словами, если рассматриваемое значение параметра увеличилось в предыдущем периоде (месяце, году), оно увеличится в следующем, если между значениями существует прямая зависимость. В случае, когда зависимость обратная (коэффициент автокорреляции имеет отрицательное значение), будущее значение будет уменьшаться. Наибольший интерес для прогнозирования представляют уравнения, полученные по месяцам (табл. 3), а не за весь период.

Табл. 3. Модели авторегрессии по месяцам, построенные для структурных подразделений электрических сетей ЕЭС России на 2014-2021 годы

Месяц	Уравнение авторегрессии	R^2
ПАО «МРСК Центра» («3»)		
Январь	$y_t = 0,72 y_{t-1} + 7,39$	0,73
Май	$y_t = 0,53 y_{t-1} + 42,21$	0,54
Июнь	$y_t = 0,71 y_{t-1} + 29,90$	0,74
Август	$y_t = 0,87 y_{t-1} - 3,21$	0,95
Сентябрь	$y_t = 1,46 y_{t-1} - 89,99$	0,9
Октябрь	$y_t = 0,95 y_{t-1} - 3,57$	0,76
Декабрь	$y_t = 0,78 y_{t-1} + 3,84$	0,8
ПАО «МРСК Центра» («3»)		
Март	$y_t = 0,51 y_{t-1} + 21,26$	0,67
ОАО «МРСК Урала» («5»)		
Январь	$y_t = 0,13 y_{t-1} + 22,30$	0,53
Ноябрь	$y_t = 0,57 y_{t-1} + 11,55$	0,64
Декабрь	$y_t = 0,26 y_{t-1} + 23,22$	0,68
ПАО «ФСК ЕЭС» («1»)		
Март	$y_t = 0,40 y_{t-1} + 38,19$	0,62
Сентябрь	$y_t = 0,63 y_{t-1} + 33,25$	0,87
Октябрь	$y_t = -0,68 y_{t-1} + 124,47$	0,64
Декабрь	$y_t = 0,57 y_{t-1} + 24,21$	0,77

Согласно полученным результатам, значимых авторегрессионных зависимостей по месяцам для ПАО «Россети Северный Кавказ» и ПАО «Россети Сибирь» не выявлено, в то время как для суммарных значений по годам для этих структурных подразделений были получены качественные уравнения авторегрессии (табл. 4).

Полученные зависимости позволяют спрогнозировать общее количество аварийных отключений на следующий год.

Поскольку в течение некоторых месяцев в определенных структурных подразделениях отсутствуют зависимости от времени и предыдущих значений, в дальнейшем необходимо оценить влияние климатиче-

Табл. 4. Уравнения авторегрессии для суммарных годовых значений аварийности в структурных подразделениях электрических сетей ЕЭС России за 2014-2021 годы

Месяц	Уравнение авторегрессии	R ²
ПАО «МРСК Центра» («3»)	$y_t = 0,72 y_{t-1} + 221,51$	0,62
ОАО «МРСК Урала» («5»)	$y_t = 0,68 y_{t-1} + 238,36$	0,83
ПАО «Россети Волга» («4»)	$y_t = 0,91 y_{t-1} - 20,23$	0,97
ПАО «Россети Северный Кавказ» («6»)	$y_t = 0,51 y_{t-1} + 440,42$	0,74
ПАО «Россети Сибирь» («2»)	$y_t = 0,47 y_{t-1} + 667,17$	0,52
ПАО «ФСК ЕЭС» («1»)	$y_t = 0,77 y_{t-1} + 215,11$	0,66

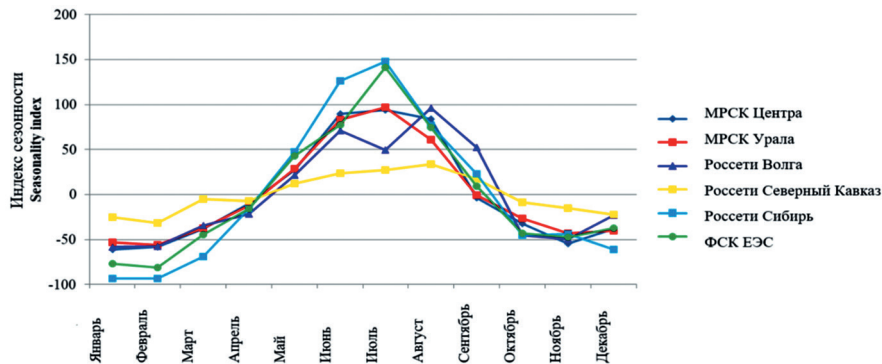


Рис. 7. Сезонная составляющая аварийных отключений структурных подразделений ЕЭС России на 2014-2021 годы

ских условий (температуры и осадков) на исследуемый показатель.

Описанные выше модели отражают только зависимость отказов в электрических сетях от времени и предыдущих значений, поэтому сезонная составляющая оценивается на следующем этапе.

Расчет компонентов временного ряда проводился с помощью программы, описанной в [37], основанной на методе наименьших квадратов.

Согласно полученным результатам, наибольшее количество аварийных отключений приходится на весенне-летние 5 месяцев (рис. 7), что может быть связано с увеличением нагрузки на сети из-за повышения температуры.

В то же время наибольший разброс показателей сезонности был выявлен по данным ПАО «Россети Сибирь» («2») и ПАО «ФСК ЕЭС» («1»). Другими словами, количество повреждений, происходящих в летний период для этих подразделений, значительно превышает значения этого показателя в другие месяцы, как было сказано ранее.

Таким образом, полученные уравнения позволяют провести превентивную оценку повреждений в исследуемых электрических сетях ЕЭС России, что в достаточной степени коррелирует с уравнениями, полученными авторами при оценке повреждений электрических сетей «Иркутской электросетевой компании».

Выводы

На основании анализа, проведенного по обработке статистической информации по аварийным режимам в высоковольтных электрических сетях ЕЭС России, в качестве выводов можно отметить следующее.

- Наиболее надежной оценкой реального состояния аварийности электрических сетей следует считать конкретный показатель, зависящий от протяженности сетей и уровня организации их эксплуатации.

- При оценке аварийности по конкретному показателю было установлено, что для семи компаний ЕЭС России была получена следующая последовательность (в порядке убывания): ФСК ЕЭС ($A_{AAR} = 60,87$); МРСК Урала ($A_{AAR} = 43,81$); Россети Северный Кавказ ($A_{AAR} = 42,75$); Россети Сибирь ($A_{AAR} = 34,1$); АО «Янтарьэнерго» ($A_{AAR} = 32,06$); Россети Волга ($A_{AAR} = 29$); МРСК Центра ($A_{AAR} = 16,17$).

- Оценка уровня износа исследуемых сетей показала, что наибольший износ электрических сетей соответствует компании «МРСК Урала» (свыше 60%), наименьший – АО «Россети Янтарь» (25%).

- При оценке сезонной составляющей установлено, что наибольший ущерб приходится на летний период: июнь, июль, август.

- Статистическая оценка аварийных ситуаций позволила получить высококачественные уравнения трендов и авторегрессии, позволяющие прогнозировать общее количество аварийных отключений на следующий год.

- Анализ деятельности крупнейших электросетевых компаний России позволил акцентировать внимание на ключевых вопросах безопасности функционирования исследуемых электрических сетей.

Направление дальнейших исследований

Мы продолжим наши исследования в направлении оценки ущерба электрическим сетям различных

электросетевых компаний. При этом предполагается использовать не только авторегрессионную модель оценки прогнозирования возникающих отказов, но также и различные иные ресурсы, использующие нейронные сети, включая библиотеки Simulink MATLAB.

Библиографический список

1. Abdin I, Li Y-F, Zio E. Risk assessment of power transmission network failures in a uniform pricing electricity market environment // *Energy*. 2017. Vol. 138. Pp. 1042-1055. DOI: 10.1016/j.energy.2017.07.115
2. Campbell RJ (2012) Weather-related power outages and electric system resiliency. Available via DIALOG [Электронный ресурс] URL: <https://sgp.fas.org/crs/misc/R42696.pdf> (дата обращения 06.08.2023).
3. Deng Ch-J. Challenges and prospects of power transmission line. Intelligent monitoring technology // *American Research Journal of Computer Science and Information Technology*. 2019. Vol. 4. Part 2. Pp. 1-11.
4. Doukas H, Psarras J. Electric power transmission: An overview of associated burdens // *International Journal of Energy Research*. 2011. Vol. 35. Part 11. Pp. 979-988. DOI: 10.1002/er.1745
5. Dovgalyuk O., Omelianenko H., Pirotti A., Bondarenko R., Syromyatnikova T. Reliability Increase of the Distribution Electric Networks Operation in the Implementation of the Energy Market in Ukraine // 2019 IEEE 6th International Conference on Energy Smart Systems (ESS), Kyiv, Ukraine. 2019. Pp. 70-75. DOI: 10.1109/ESS.2019.8764243
6. Electric Power Council of the Commonwealth of Independent States (nd) Independent States Commonwealth Electric Power Industry 2007-2017 (annual collection) [Электронный ресурс] URL: <http://energo-cis.ru/rumain675> (дата обращения 06.08.2023).
7. Jamsek S., Bakic K. Slovenian Approach in Reliability Centered Maintenance of Transmission System Provider // 2005/2006 IEEE/PES Transmission and Distribution Conference and Exhibition, Dallas, TX, USA. 2006. Pp. 799-802. DOI: 10.1109/TDC.2006.1668598
8. Kazim M, Khawaja A, Zabit U, et al. Fault Detection and Localization for Overhead 11-kV Distribution Lines With Magnetic Measurements // *IEEE Transactions on Instrumentation and Measurement*. 2020. Vol. 69. Part 5. Pp. 2028-2038. DOI: 10.1109/TIM.2019.2920184
9. Kirillov V. The electric grid infrastructure wear in Russia // *Scales and prospects. Energy: Economics, Technology, Ecology*. 2018. Vol. 5. Pp. 53-57.
10. Leite J.B., Mantovani J. R. S., Dokic T., et al. Failure probability metric by machine learning for online risk assessment in distribution networks // 2017 IEEE PES Innovative Smart Grid Technologies Conference – Latin America (ISGT Latin America), Quito, Ecuador. 2017. Pp. 1-6. DOI: 10.1109/ISGT-LA.2017.8126683
11. Lu R, Hong SH, Zhang X, Ho S. A Dynamic pricing demand response algorithm for smart grid: Reinforcement learning approach // *Applied Energy*, Elsevier. 2018. Vol. 220(C). Pp. 220-230. DOI: 10.1016/j.apenergy.2018.03.072
12. Министерство энергетики Российской Федерации. Информация об авариях в электросетях и генерации. Аварии в электрических сетях напряжением 110 кВ и выше. [Электронный ресурс] URL: http://szap.gosnadzor.ru/activity/energonadzor/nesc_sluch/Анализ%20причин%20аварий%20за%202021.pdf (дата обращения 06.08.2023).
13. Министерство энергетики Российской Федерации (официальный сайт). Вводы И Выводы Оборудования [Электронный ресурс] URL: <https://minenergo.gov.ru/node/537> (дата обращения 06.08.2023).
14. Министерство энергетики Российской Федерации (официальный сайт). Основные характеристики российской электроэнергетики [Электронный ресурс] URL: <https://minenergo.gov.ru/node/532> (дата обращения 06.08.2023).
15. Наумов И.В., Карамов Д.Н. К вопросу о повреждаемости воздушных линий электропередачи в системах электроснабжения // *Надежность и безопасность энергетики*. 2021. Том 14. № 2. С. 92-99. DOI: 10.24223/1999-5555-2021-14-2-92-99
16. Наумов И.В., Карпова Е.В. Анализ причин ущерба распределительным электрическим сетям напряжением 10 кВ (на примере Иркутских южных электрических сетей) // *Надежность и энергетическая безопасность*. 2018. Том 11. № 4. С. 299-304. DOI: 10.24223/1999-5555-2018-11-4-299-304
17. Naumov I.V., Karpova E.V., Karamov D.N. Reliability level research in distribution electrical networks of Irkutsk // *E3S Web of Conferences*. 2019. T. 114. ID: 03005. DOI: 10.1051/e3sconf/201911403005
18. Наумов И.В., Ланин А.В., Ерин В.Н. Математическая модель прогнозирования уровня надежности электроснабжения в электрических сетях 10 кВ // *Вестник Алтайского государственного аграрного университета*. 2011. № 8(82). С. 88-91.
19. Наумов И.В., Полковская М.Н. Анализ работы единых энергетических электрических сетей Иркутской области в 2019 году // *Вестник Алтайского государственного аграрного университета*. 2021. № 5(199). С. 118-126.
20. Наумов И.В., Васильев Н.В., Ланин В.Н. и др. Прогнозирование повреждаемости элементов сельских распределительных сетей 10 кВ (на примере Восточных электрических сетей города Иркутска) // *Известия Санкт-Петербургского государственного аграрного университета*. 2011. № 25. С. 161-166.
21. Невская А. Средний показатель износа электросетевой инфраструктуры «Россети» может превысить 60% к 2025 году // *Энергетика и промышленность России – информационный портал энергетика*. [Электронный ресурс] URL: <https://www.eprussia.ru/news/base/2021/2875181.htm> (дата обращения 06.08.2023).
22. Olusuyi K., Oluwol A.S., Adefarati T. et al. A fault analysis of 11 kV distribution system (a case study of ado Ekiti electrical power distributional district) // *Applied*

Energy. 2014. Vol. 3(2). Pp. 27-36. DOI: 10.11648/j.epes.20140302.13

23. ПАО «ФСК ЕЭС» Целевые показатели надежности и качества услуг по передаче электрической энергии на 2015-2020 годы [Электронный ресурс]. URL: https://www.fsk-ees.ru/consumers/uslugi_po_peredache_elektroenergii/ (дата обращения 06.08.2023).

24. Reed D.A. Electric utility distribution analysis for extreme winds // *Journal of Wind Engineering and Industrial Aerodynamics*. 2008. Vol. 96. Pp. 123-140. DOI: 10.1016/j.jweia.2007.04.002

25. Репетюк С.В., Шеваль Ю.В. Экспертно-аналитическая записка по теме: «Электросетевой комплекс Российской Федерации: анализ состояния и организационная структура». Институт экономики естественных монополий РАНХиГС [Электронный ресурс]. URL: <https://www.eprussia.ru/upload/iblock/17f/17f7ecbb1df3670f406e3e0f19ea0da8.pdf> (дата обращения: 06.08.2023).

26. Россети. Филиалы ОАО «ФСК ЕЭС» [Электронный ресурс]. URL: <https://www.fsk-ees.ru/about/affiliates> (дата обращения: 06.08.2023).

27. Россети. Годовой отчет 2020 [Электронный ресурс]. URL: http://www.rustocks.com/put.phtml/MRKH_2020_RUS.pdf (дата обращения: 04.07.2023).

28. Российская федерация. Постановление «О реформировании электроэнергетики Российской Федерации», № 526, 11 июля 2001 г., Москва.

29. Российская федерация. Приказ Министерства энергетики РФ от 29 ноября 2016 г. № 1256 «Об утверждении Методических указаний по расчету уровня надежности и качества поставляемых товаров и оказываемых услуг для организации по управлению единой национальной (общероссийской) электрической сетью и территориальных сетевых организаций» (с изменениями и дополнениями).

30. Sahoo A.K., Dash S.S., Thyagarajan T. Power flow study including facts devices // *Journal of Applied Sciences*. 2010. Vol. 10. Part 15. Pp.1563–1571. DOI:10.3923/JAS.2010.1563.1571

31. Shilin A.N., Shilin A.A., Dementiev S.S. Smart electromechanical systems in electric power engineering: Concept, technical realization, prospects // *Studies in Systems, Decision and Control*. 2019. Vol. 174. Pp. 251-262. DOI: 10.1007/978-3-319-99759-9_20

32. StatSoft. The program Statistics-10 [Электронный ресурс]. URL: <http://statsoft.ru/products/new-features/STATISTICA10.php> (дата обращения: 04.07.2023).

33. Sultan V, Hilton B. A spatial analytics framework to investigate electric power-failure events and their causes // *ISPRS International Journal of Geo-Information*. 2020. Vol. 9. Part 1. P. 54. DOI: 10.3390/ijgi9010054

34. Vasilevsky D. PJSC “ROSSETI” in numbers [Электронный ресурс]. URL: <https://pro-rza.ru/pao-rosseti-v-tsifrah> (дата обращения: 06.08.2023).

35. Wang G, Wang Q, Qiao Z et al. Optimal planning of multi-micro grids based-on networks reliability // *Energy Reports*. 2020. Vol. 6. Pp.1233–1249.

36. Россети – Википедия. Свободная энциклопедия. [Электронный ресурс]. URL: <https://ru.wikipedia.org/w/index.php?search=%D0%A0%D0%BE%D1%81%D1%81%D0%B5%D1%82%D0%B8&title=%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F%3A%D0%9F%D0%BE%D0%B8%D1%81%D0%BA&ns0=1> (дата обращения: 06.08.2023).

37. Xie K, Zhang H, Singh C. Reliability forecasting models for electrical distribution systems considering component failures and planned outages international // *Journal of Electrical Power & Energy Systems*. 2016. Vol. 79. Pp. 228-234. DOI: 10.1016/j.ijepes.2016.01.020

38. Zheng X, Menezes F, Nepal R. In between the state and the market: An empirical assessment of the early achievements of China 2015 electricity reform // *Energy Economics*. 2020. Vol. 93(C). DOI: 10.1016/j.eneco.2020.105003

39. Zorkaltsev V.I., Mokry I.V. Date Selection of the Beginning of the Economic Year on the Minimization Criteria of the Seasonal Oscillations Amplitude // *The Bulletin of Irkutsk State University. Series Mathematics*. 2017. Vol. 22. Pp. 50-62. DOI: 10.26516/1997-7670.2017.22.50

References

1. Abdin I., Li Y.-F., Zio E. Risk assessment of power transmission network failures in a uniform pricing electricity market environment. *Energy* 2017;138:1042-1055. DOI: 10.1016/j.energy.2017.07.115.

2. Campbell R.J. Weather-related power outages and electric system resiliency. (accessed 06.08.2023). Available at: <https://sgp.fas.org/crs/misc/R42696.pdf>.

3. Deng Ch.-J. Challenges and prospects of power transmission line. Intelligent monitoring technology. *American Research Journal of Computer Science and Information Technology* 2019;4(2):1-11.

4. Doukas H., Psarras J. Electricpower transmission: An overview of associated burdens. *International Journal of Energy Research* 2011;35(11):979-988. DOI: 10.1002/er.1745.

5. Dovgalyuk O., Omelianenko H., Pirotti A., Bondarenko R., Syromyatnikova T. Reliability Increase of the Distribution Electric Networks Operation in the Implementation of the Energy Market in Ukraine. In: proceedings of the 2019 IEEE 6th International Conference on Energy Smart Systems (ESS). Kyiv (Ukraine); 2019. Pp. 70-75. DOI: 10.1109/ESS.2019.8764243.

6. Electric Power Council of the Commonwealth of Independent States. Independent States Commonwealth Electric Power Industry 2007-2017. (accessed 06.08.2023). Available at: <http://energo-cis.ru/rumain675>.

7. Jamsek S., Bakic K. Slovenian Approach in Reliability Centered Maintenance of Transmission System Provider. In: proceedings of the 2005/2006 IEEE/PES Transmission and Distribution Conference and Exhibition. Dallas (Texas, USA); 2006. Pp. 799-802. DOI: 10.1109/TDC.2006.1668598.

8. Kazim M., Khawaja A., Zabit U. et al. Fault Detection and Localization for Overhead 11-kV Distribution Lines with Magnetic Measurements. *IEEE Transactions on Instrumentation and Measurement* 2020;69(5):2028-2038. DOI: 10.1109/TIM.2019.2920184.
9. Kirillov V. The electric grid infrastructure wear in Russia. Scales and prospects. *Energy: Economics, Technology, Ecology* 2018;5:53-57.
10. Leite J.B., Mantovani J.R.S., Dokic T. et al. Failure probability metric by machine learning for online risk assessment in distribution networks. In: proceedings of 2017 IEEE PES Innovative Smart Grid Technologies Conference – Latin America (ISGT Latin America). Quito (Ecuador); 2017. Pp. 1-6. DOI: 10.1109/ISGT-LA.2017.8126683.
11. Lu R., Hong S.H., Zhang X., Ho S. A dynamic pricing demand response algorithm for smart grid: Reinforcement learning approach. *Applied Energy* 2018;220(C):220-230. DOI: 10.1016/j.apenergy.2018.03.072.
12. [Ministry of Energy of the Russian Federation. Information on accidents in the power grid and generation. 2021. Accidents in 110 kV electric networks and above]. (accessed 06.08.2023). Available at: http://szap.gosnadzor.ru/activity/energonadzor/nesc_sluch/Анализ%20причин%20аварий%20за%202021.pdf. (in Russ.)
13. [Ministry of Energy of the Russian Federation. The equipment inputs and outputs]. (accessed 06.08.2023). Available at: <https://minenergo.gov.ru/node/537>. (in Russ.)
14. [Ministry of Energy of the Russian Federation. The installed capacity structure of the united power systems power plants and the Russia UES as January 01, 2020]. (accessed 06.08.2023). Available at: <https://minenergo.gov.ru/node/532>. (in Russ.)
15. Naumov I.V., Karamov D.N. On the damage issue to overhead power transmission lines in power supply systems. *Reliability and Safety of Energy* 2021;14(2):84-91. DOI: 10.24223/1999-5555-2021-14-2-92-99. (in Russ.)
16. Naumov I.V., Karpova E.V. The damage analysis causes to 10 kV distribution electric networks (On the Irkutsk Southern Electric Networks Example). *Reliability and Energy Safety* 2018;11(4):299-304. DOI: 10.24223/1999-5555-2018-11-4-299-304. (in Russ.)
17. Naumov I.V., Karpova E.V., Karamov D.N. Reliability level research in distribution electrical networks of Irkutsk. In: proceedings of the E3S Web of Conferences; 2019. V. 114. ID: 03005. DOI: 10.1051/e3sconf/201911403005.
18. Naumov I.V., Lanin A.V., Erin V.N. [Mathematical model of forecasting the level of reliability of power supply in 10 kV electric networks]. *Bulletin of AltGAU* 2011;8:88-91. (in Russ.)
19. Naumov I.V., Polkovskaya M.N. The analysis of the operation of electric networks of the Oblkommunenergo of the Irkutsk region in 2019. *Bulletin of AltGAU* 2021;5:118-126. (in Russ.)
20. Naumov I.V., Vasiliev N.V., Lanin V.N. et al. [Prediction of damage to elements of rural distribution networks of 10 kV (on the example of the Eastern electric networks of Irkutsk)]. *Journal "Izvestia of St. Petersburg State Agrarian University"* 2011;25:161-166. (in Russ.)
21. Nevskaya A. [Energy news. Electric power industry/ Electrical networks]. (accessed 06.08.2023). Available at: <https://www.eprussia.ru/news/base/2021/2875181.htm>. (in Russ.)
22. Olusuyi K., Oluwol A.S., Adefarati T. et al. A fault analysis of 11 kV distribution system (a case study of ado Ekiti electrical power distributional district). *Applied Energy* 2014;3(2):27-36. DOI: 10.11648/j.epes.20140302.13. (in Russ.)
23. [PJSC FGC UES. The reliability target indicators and electric energy quality transmission services for 2015-2020]. (accessed 06.08.2023). Available at: https://www.fsk-ees.ru/consumers/uslugi_po_peredache_elektroenergii/. (in Russ.)
24. Reed D.A. Electric utility distribution analysis for extreme winds. *Journal of Wind Engineering and Industrial Aerodynamics* 2008;96:123-140. DOI: 10.1016/j.jweia.2007.04.002.
25. Repetyuk S.V., Sheval Yu.V. [Expert and analytical note on the topic: The electric grid complex of the Russian Federation: The state and organizational structure analysis]. (accessed 06.08.2023). Available at: https://em.ranepa.ru/files/docs/research/2020_133_ex_sum_1.pdf. (in Russ.)
26. [Rosseti FGC UES. Branches]. (accessed 06.08.2023). Available at: <https://www.fsk-ees.ru/about/affiliates>. (in Russ.)
27. [Rossetti Annual reports 2020]. (accessed 06.08.2023). Available at: http://www.rustocks.com/put.phtml/MRKH_2020_RUS.pdf. (in Russ.)
28. [Russian Federation. Resolution "On reforming the Russian Federation electric power industry" dated 2001 no. 526. July 11, 2001; Moscow]. (in Russ.)
29. [Russian Federation. Order of the Ministry of Energy of the Russian Federation dated November 29, 2016 no. 1256 "On methodological guidelines approval for calculating the reliability and goods supplied quality level and services rendered for the managing organization the unified national (all-Russian) electric grid and territorial grid organizations"]. (in Russ.)
30. Sahoo A.K., Dash S.S., Thyagarajan T. Power flow study including facts devices. *Journal of Applied Sciences* 2010;10(15):1563-1571. DOI:10.3923/JAS.2010.1563.1571.
31. Shilin A.N., Shilin A.A., Dementiev S.S. Smart electromechanical systems in electric power engineering: Concept, technical realization, prospects. *Studies in Systems, Decision and Control* 2019;174:251-262. DOI: 10.1007/978-3-319-99759-9_20.
32. [StatSoft. The program Statistics-10]. (accessed 06.08.2023). Available at: <http://statsoft.ru/products/new-features/STATISTICA10.php>. (in Russ.)
33. Sultan V., Hilton B. A spatial analytics framework to investigate electric power-failure events and their causes. *ISPRS International Journal of Geo-Information* 2020;9(1):54. DOI: 10.3390/ijgi9010054.
34. Vasilevsky D. [PJSC "ROSSETI" in numbers]. (accessed 06.08.2023). Available at: <https://pro-rza.ru/pao-rosseti-v-tsifrah>.
35. Wang G., Wang Q., Qiao Z. et al. Optimal planning of multi-micro grids based-on networks reliability. *Energy Reports* 2020;6:1233-1249.

36. [Rosseti]. (accessed 06.08.2023). Available at: <https://ru.wikipedia.org/w/index.php?search=%D0%A0%D0%BE%D1%81%D1%81%D0%B5%D1%82%D0%B8&title=%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F%3A%D0%9F%D0%BE%D0%B8%D1%81%D0%BA&ns=1>. (in Russ.)

37. Xie K., Zhang H., Singh C. Reliability forecasting models for electrical distribution systems considering component failures and planned outages international. *Journal of Electrical Power & Energy Systems* 2016;79:228-234. DOI: 10.1016/j.ijepes.2016.01.020.

38. Zheng X., Menezes F., Nepal R. In between the state and the market: An empirical assessment of the early achievements of China 2015 electricity reform. *Energy Economics* 2020;93(C). DOI: 10.1016/j.eneco.2020.105003.

39. Zorkaltsev V.I., Mokry I.V. Date Selection of the Beginning of the Economic Year on the Minimization Criteria of the Seasonal Oscillations Amplitude. *The Bulletin of Irkutsk State University. Series Mathematics* 2017;22:50-62. DOI: 10.26516/1997-7670.2017.22.50.

Сведения об авторах

Наумов Игорь Владимирович – доктор технических наук, профессор, профессор кафедры электроснабжения и электротехники ИРНИТУ и Иркутского ГАУ, ул. Черемуховая, дом 196, поселок Молодежный, Иркутский район, Иркутская область, Российская Федерация, 664038, e-mail: professornaumov@list.ru

Подъячих Сергей Валерьевич – кандидат технических наук, доцент, заведующий кафедрой электроснабжения и электротехники Иркутского ГАУ, поселок Молодежный, дом 1, Иркутский район, Иркутская область, Российская Федерация, 664038, e-mail: psv78@yandex.ru

Полковская Марина Николаевна – кандидат технических наук, доцент, доцент кафедры информатики и математического моделирования Иркутского ГАУ, поселок Молодежный, дом 1, Иркутская область, Российская Федерация, 664038, e-mail: polk_mn@mail.ru

Шерьязов Сакен Койшыбаевич – доктор технических наук, профессор, профессор кафедры энергообеспечения и автоматизации технологических процессов Южно-Уральского ГАУ, ул. им. Ю.А. Гагарина, дом 13, г. Троицк, Челябинская область, Российская Федерация, 457103, e-mail: sakenu@yandex.ru.

Бастрон Андрей Владимирович – кандидат технических наук, доцент, заведующий кафедрой электроснабжения сельского хозяйства Красноярского ГАУ, проспект Мира, дом 90, г. Красноярск, Российская Федерация, 660049, e-mail: abastron@yandex.ru

About the authors

Igor V. Naumov, Doctor of Engineering, Professor, Chair Professor, Department of Power Supply and Power Engineering, Irkutsk National Research Technical University and A.A. Yezhevsky Irkutsk State Agrarian University, 19b Cheriomukhovaya St., Molodiozhny, Irkutsky District, Irkutsk Oblast, 664038, Russian Federation, e-mail: professornaumov@list.ru.

Sergey V. Podyachikh, Candidate of Engineering, Associate Professor, Head of Chair, Department of Power Supply and Power Engineering, A.A. Yezhevsky Irkutsk State Agrarian University, 1 Molodiozhny, Irkutsky District, Irkutsk Oblast, 664038, Russian Federation, e-mail: psv78@yandex.ru.

Marina N. Polkovskaya, Candidate of Engineering, Associate Professor, Senior Lecturer, Department of Computer Science and Computer Simulation, A.A. Yezhevsky Irkutsk State Agrarian University, 1 Molodiozhny, Irkutsky Oblast, 664038, Russian Federation, e-mail: polk_mn@mail.ru.

Saken K. Sheryazov, Doctor of Engineering, Professor, Chair Professor, Department of Power Supply and Process Automation, South Ural State Agrarian University, 13 Gagarina St., Troitsk, Chelyabinsk Oblast, 457103, Russian Federation, e-mail: sakenu@yandex.ru.

Andrey V. Bastron, Candidate of Engineering, Associate Professor, Head of Chair, Department of Agricultural Power Supply, Krasnoyarsk State Agrarian University, 90 Prospekt Mira, Krasnoyarsk, 660049, Russian Federation, e-mail: abastron@yandex.ru.

Вклад авторов

Наумов И.В. – идея статьи, сбор и анализ исходной информации, разработка программ визуализации данных, анализ полученных результатов, написание статьи.

Подъячих С.В. – сбор исходной информации, обработка результатов расчетов, анализ полученных результатов.

Полковская М.Н. – сбор и анализ исходной информации, статистическая обработка полученных результатов, построение и анализ прогностических моделей чрезвычайных ситуаций.

Шерьязов С.К. – сбор исходной информации, анализ полученных результатов.

Бастрон А.В. – сбор исходной информации, анализ полученных результатов.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

К оцениванию технического уровня разведывательно-ударных и ударных беспилотных летательных аппаратов на стадии эксплуатации

On assessing the technical level of scout/attack unmanned aerial vehicles at the operational stage

Микони С.В.^{1*}, Семенов С.С.²
Mikoni S.V.^{1*}, Semionov S.S.²

¹ФГБУН "Санкт-Петербургский Федеральный исследовательский Центр РАН", Санкт-Петербург, Российская Федерация, ²АО "Государственное научно-производственное предприятие "Регион", Москва, Российская Федерация

¹St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint Petersburg, Russian Federation,

²Region Public Research and Development Enterprise, Moscow, Russian Federation

*smikoni@mail.ru



Микони С.В.



Семенов С.С.

Резюме. Цель. Целью данной статьи является: показать актуальность оценивания технического уровня БЛА в целом, выявить и отразить особенности проблемы оценивания технического уровня (ТУ) на этапе эксплуатации. **Методы.** При формировании материалов статьи используется метод системного анализа. **Результаты.** Показана роль оценки ТУ разведывательно-ударных беспилотных летательных аппаратов (БЛА) как индикатора их технического совершенства, представлены состояние, методология и результаты оценивания ТУ БЛА на всех этапах жизненного цикла, основные направления развития БЛА, выявлены особенности оценивания ТУ БЛА на этапе проектирования с целью поддержания требуемого уровня на этапе эксплуатации. **Выводы.** Предложены рекомендации по структурированию показателей, отражающих стабильность и развитие БЛА. Подбор модулей под требования, предъявляемые к показателям развития, позволит поддерживать надлежащий технический уровень БЛА на этапе эксплуатации.

Abstract. Aim. The paper aims to show the relevance of assessing the technical level of UAVs in general, to identify and set forth the specificity of technical level (TL) assessment at the operational stage. **Methods.** The paper uses the method of systems analysis. **Results.** The paper shows the role of TL assessment of scout/attack unmanned aerial vehicles (UAVs) as an indicator of their technological excellence, presents the state of the art, methodology and results of UAV TL assessment at all life cycle stages, key trends in UAV development, identifies the specificity of UAV TL assessment at the design stage for the purpose of maintaining the required level at the operational stage. **Conclusions.** The paper provides recommendations for structuring indicators that reflect the stability and development of UAVs. If modules are selected according to the required development indicators, the proper technical level of the UAV will be maintained at the operational stage.

Ключевые слова: разведывательно-ударные и ударные беспилотные летательные аппараты, жизненный цикл, технический уровень, оценочные показатели, эксплуатация.

Keywords: scout\attack and attack unmanned aerial vehicles, life cycle, technical level, estimated indicators, operation.

Для цитирования: Микони С.В., Семенов С.С. К оцениванию технического уровня разведывательно-ударных и ударных беспилотных летательных аппаратов на стадии эксплуатации // Надежность. 2024. №2. С. 52-60. <https://doi.org/10.21683/1729-2646-2024-24-2-52-60>

For citation: Mikoni S.V., Semionov S.S. On assessing the technical level of scout/attack unmanned aerial vehicles at the operational stage. Dependability 2024;2:52-60. <https://doi.org/10.21683/1729-2646-2024-24-2-52-60>

Поступила: 18.10.2023 г. / **После доработки:** 08.04.2024 / **К печати:** 10.06.2024

Received on: 18.10.2023 / **Revised on:** 08.04.2024 / **For printing:** 10.06.2024

Введение

В настоящее время как в нашей стране, так и за рубежом большое внимание уделяется развитию беспилотных робототехнических комплексов различного назначения, которые воплощают в себе последние достижения в области микроэлектроники, информационных технологий, программного обеспечения, материалов и др. Одним из основных направлений развития таких комплексов является создание перспективных беспилотных авиационных систем (БАС) военного и гражданского назначения. 12 сентября 2023 г. было проведено заседание во главе с Председателем правительства РФ М. Мишустинным по развитию БАС, на котором были подробно рассмотрены задачи – от формирования промышленной базы, программного обеспечения, инфраструктуры, оказания услуг по использованию беспилотной авиации до развития научных и технологических компетенций, конструкторской и инженерной школы [1]. Предполагается создание сети научно-производственных центров, в которых сосредоточатся работы по апробированию и практической реализации передовых решений в отрасли, а также инфраструктуры для обеспечения полетов на территории страны в едином воздушном пространстве. При этом первостепенное значение в целях повышения обороноспособности страны приобретает разработка разведывательно-ударных и ударных комплексов беспилотных летательных аппаратов (КБЛА). Созданием беспилотных летательных аппаратов (БЛА) такого класса в мире занимаются более 20-ти стран. Передовые позиции в мире в этой области беспилотной авиации занимают такие страны как США, Китай, Израиль, Иран, Турция, Великобритания, Франция. Классическим прототипом в этом классе стал разведывательно-ударный БЛА Reaper MQ-9 (США), который принят многими странами за образец при создании и оснащении собственных ВС таким БЛА.

При проектировании КБЛА разработчики сталкиваются с необходимостью определить технический облик системы в целом и, в первую очередь, с решением задач выбора рационального конструктивно-компоновочного облика и технологических схем БЛА и их основных параметров. Технология разработки сложных технических систем (СТС) как КБЛА хорошо отработана. Вместе с тем, возникают предложения по повышению эффективности создания СТС авиационного направления. На основе анализа основных проблем, связанных с разработкой особо сложных образцов авиационной техники (АТ) военного назначения, недостатков существующего порядка создания, а также зарубежного опыта приобретения военной техники в работе [2] предлагается пересмотреть процесс создания сложных образцов АТ и осуществить переход на модель разработки, состоящую из трех основных стадий: внешнее проектирование; эскизно-техническое проектирование с разработкой демонстратора и проведением его испытаний; полномасштабная ОКР.

Быстрая смена инновационных технологий заставляет ведущие страны мира пересмотреть концепции ведения будущих воздушных операций и сформировать новые планы развития беспилотной авиации до 2035-40 гг. По мнению ведущих специалистов рабочей группы Института Митчелла (США), с целью поддержания боеготовности авиапарка на высоком уровне следует выводить из эксплуатации все авиационные средства быстрее, чем это происходило в течение последних нескольких десятилетий. И в этой связи этап эксплуатации АТ может стать важным звеном в жизненном цикле, в котором проявляется достигнутый уровень разработки. Оценивание технического уровня (ТУ) КБЛА на всем жизненном цикле системы может послужить инструментом (индикатором) для определения уровня разработки (проекта). Цель данной статьи – показать актуальность оценивания ТУ БЛА в целом, выявить и отразить особенности проблемы оценки ТУ на этапе эксплуатации.

1. Технический уровень как индикатор конкурентоспособности БЛА

Проблема формирования ожидаемых основных тактико-технических характеристик (ТТХ) при разработке БЛА является крайне актуальной, так как затрагивает финансовые, временные, кадровые и другие ресурсы. В конечном итоге нерешенность проблемы может негативно отразиться на эффективности и качестве будущего прототипа, которому изначально предполагается достаточно высокие значения ТТХ. Получение компонентов основных показателей из множества характеристик комплекса БЛА (КБЛА) происходит в процессе формирования задач, стоящих перед комплексом.

Когда говорят о конкурентоспособности создаваемой продукции, то под этим подразумевается успешность ее продажи в определенных сегментах рынка, в том числе на внешних рынках. В современной экономической науке конкурентоспособность принято оценивать соотношением «цена/качество». Сформировалось новое направление в проектировании новой техники – «управление жизненным циклом изделия» или CALS-технологии, которые с помощью автоматизированных систем управления обеспечивают выполнение технологических процессов или проведение проектных работ. Назначение CALS-технологий – обеспечивать представление необходимой информации в нужное время в нужном виде и в конкретном месте любому пользователю на всех этапах жизненного цикла.

Накопленный опыт в области разработки методического базиса и практического решения некоторых задач интегрированной логистической поддержки представлен в монографии [3]. В данной работе отмечается, что если речь идет о оценке конкурентоспособности вновь создаваемого изделия преимущественно оборонного назначения и понятие конкурентоспособности изделий

напрямую связано с обеспечением обороноспособности государства, то при формировании требований к создаваемому изделию необходимо учитывать мировой уровень. Иными словами, индикатором прогрессивности технических решений может стать ТУ разработки. Оценка ТУ создаваемого объекта техники по отношению к лучшим мировым образцам является одним из инструментов выбора наилучших проектных решений из числа альтернативных.

Процесс разработки комплекса БЛА начинается с постановки задач исследования его характеристик и выбора проекта. Для их решения обычно применяются методы исследования операций. В условиях недостаточности информации для принятия решений используются эвристические методы, методы теории игр и комбинированные методы с сочетанием имитационного моделирования [4].

Выбор модели многофункционального БЛА предполагает, исходя из заданных требований, определение наилучшего образца БЛА из определенного набора существующих альтернативных вариантов. Фактически существующие варианты отражают текущий уровень научно-технологического развития беспилотной авиации. Рассматривая задачу в подобной постановке, мы пытаемся определить такой вариант перспективного многоцелевого БЛА, который может быть реализован на существующем уровне научно-технологического развития. Она относится к задачам многокритериального проектного выбора, что согласуется с рецензией [5] д-ра техн. наук, проф. В.Н. Евдокименкова и канд. техн. наук И.В. Захарова на монографию по робототехническим комплексам [6].

Прорывные технологии, обеспечивающие конкурентоспособность отечественных разработок, традиционно генерируются в авиастроении. Отраслевые НИР, как показывает опыт, ориентируют на образцы, превосходящие по ТУ лучших предшественников на 10...15% [(7, стр. 15), 8].

Результаты научно-теоретических исследований по оцениванию ТУ корректируемых и управляемых авиационных бомб (УАБ) как одной из разновидностей БЛА подтверждают такую оценку [9]. Итогом анализа тенденций развития зарубежных УАБ является предлагаемая для УАБ аттестационная шкала для оценки перспективности разработок (табл. 1). Образцы УАБ, получившие коэффициент ТУ ($K_{\text{ТУ}}$) равный 1,135...1,265, считаются перспективными.

Табл. 1. Аттестационная шкала перспективности УАБ

Пределы изменения $K_{\text{ТУ}}$	Прогнозная оценка изделия в целом
1,05...1,065	Не перспективная УАБ
1,07...1,13	Малоперспективная УАБ
1,135...1,265	Перспективная УАБ
1,27 и выше	Весьма перспективная УАБ

2. Динамика технического уровня в течение жизненного цикла образца техники

Темпы технологических изменений, которые происходят сегодня, имели место в 1950-х и 1960-х гг., что привело к появлению истребителей реактивной авиации [10]. Каждые пять-семь лет США поставляли на вооружение новый военный самолет, который мог летать выше, быстрее и дальше. Также необходимо отметить, что в годы бурного развития авиации (1930-е годы), стремительного роста ее влияния как на военный, так и на гражданский сектор, в ней, как ни в какой другой области техники быстро устаревали еще недавно, казалось бы, совершенные образцы. Если срок от начала проектирования самолета до внедрения его в серию растягивался примерно на пять лет, то такой самолет морально устаревал, не успев даже дойти до армии [11].

На основе имеющегося опыта проведения НИОКР установлено, что поиск и внедрение технических усовершенствований в среднем на 33% эффективнее научных исследований и разработок [12]. При этом число оригинальных деталей, узлов и приборов при изготовлении нового сложного изделия не должно превышать 25...30% от общего числа деталей, узлов и пр. [13].

Основная цель оценивания ТУ вновь создаваемого образца техники состоит в том, чтобы убедиться, что к моменту промышленного выпуска образец не будет уступать лучшим аналогичным отечественным и зарубежным моделям, которые к тому времени появятся на рынке, т.е. предотвратить отставание создаваемого отечественного изделия от передовых достижений отечественной и мировой науки и техники в данной области. ТУ дает представление о том, соответствует ли технико-экономические показатели продукции современным отечественным и зарубежным образцам аналогичной техники.

Необходимость оценивания ТУ образцов сложной техники подтверждается в работе [14]. Здесь рассмотрен процесс старения военной техники на примере таких сложных систем как танки. При этом отмечается, что военно-технический уровень образцов танков, состоящих на вооружении, в 1,5–2,5 раза ниже, чем на момент их выпуска и поставки в войска.

Взаимосвязь понятий «качество» и «технический уровень» имеют различные трактовки. В работах 60-80-х годов XX в. [15, 16] утверждалось, что ТУ является важнейшей характеристикой качества новых разработок СТС, поскольку он представляет собой обобщенную характеристику физических свойств, возможностей и степени технической новизны рассматриваемой СТС. Требование новизны можно считать отличительной особенностью технического уровня по отношению к качественным характеристикам СТС.

ТУ, как интегральный показатель качества СТС, каковой является БЛА, в течение производственного и эксплуатационного этапов жизненного цикла имеет трапецевидный характер [17], что показано на рис. 1.

Медленное улучшение качества происходит в начальный период по мере выполнения заданных технических параметров (кривая 1). Затем следует стабилизация (кривая 2), а за ней – постоянное ухудшение качества вследствие морального и физического износа системы без ее модернизации (кривая 3). Ухудшение технического уровня системы на этапе ее эксплуатации можно предотвратить путем модернизации ее составляющих (кривая 4).

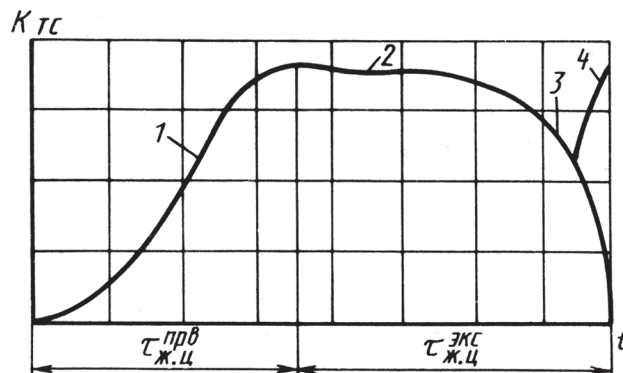


Рис. 1. Зависимость показателя качества СТС в течение жизненного цикла для усредненных условий его применения:
 $\tau_{\text{прв ж.ц}}$ – продолжительность производственного этапа жизненного цикла, $\tau_{\text{экс ж.ц}}$ – продолжительность эксплуатационного этапа жизненного цикла

3. Системный подход к формированию технического облика БЛА. Методология оценивания технического уровня БЛА

Как правило, проектирование КБЛА, и в частности БЛА, осуществляется с учетом системного подхода к формированию технического облика образца [6, 18-20]. При этом оценивание ТУ КБЛА (БЛА) рассматривается как важный инструмент для создания новой конкурентоспособной техники [21, 22]. Методология исследования летательного аппарата хорошо рассмотрена в работе [23]. Считается, что оценка ТУ летательного аппарата – это комплексная задача, включающая в себя:

1) выбор номенклатуры и определение численных значений показателей ТУ;

2) получение обобщающей характеристики системы на основе сравнения действительных значений показателей ТУ с соответствующими базовыми значениями.

В качестве основных оценочных показателей при разработке БЛА выбираются: целевые (боевые, тактические), экономические, весовые (массовые), временные показатели [24]. В период 2013-2020 гг. были разработаны методологические вопросы оценивания ТУ БЛА, содержащие обоснование и выбор оценочных показателей с определением степени их важности (значимости) [25-32], характеризующие в целом все этапы жизненного цикла. Разработке методики сравнительной

оценки уровня БЛА с привлечением современных программных средств посвящена статья [33].

4. Результаты оценивания ТУ разведывательно-ударных и ударных БЛА

На основе разработанного методического подхода по оцениванию ТУ БЛА, который учитывает интегральные показатели (боевой, тактический, выживаемость, эксплуатационно-технический, экономический, надежность, технологический) с их единичными показателями были определены ТУ и рейтинги разведывательно-ударных и ударных БЛА самолетного типа с взлетной массой от 300 кг и выше в классах 0,3-2, 2-6, 6-13, 13-25 т [34-37].

5. Особенности оценивания ТУ БЛА на стадии эксплуатации

Как отмечено в работе [38], использование рассмотренного подхода позволяет установить степень соответствия создаваемых БЛА мировому уровню на момент оценивания ТУ. Чтобы определить эффективную продолжительность производства образца и экономически целесообразные сроки его обновления и модернизации необходимо учитывать динамику развития техники, что требует применения принципа временной относительности получаемых оценок.

Действительно, статистические данные показывают, что сроки морального старения образцов, вследствие широкого внедрения новых технологий и технических решений, касающихся узлов и приборов, значительно меньше сроков их физического износа. По существу, **процесс морального старения образца начинается на стадии окончания его разработки и передачи в производство.** Постоянное обновление и завышение требований технического задания может привести к увеличению сроков разработки. Так, изменение требований при разработке институтом NCSIST с 2007 г. ударного БЛА Teng Yun с максимальным взлетным весом в 4,5 т и размахом крыльев около 20 м на Тайване привели к тому, что он до сих пор не принят на вооружение, хотя первый прототип его был представлен в 2015 г. [39]. Высказывается мысль, что оценку морального старения образца военной техники целесообразно проводить применительно к конкретным временному периоду и к реальным боевым задачам с учетом изменения оперативно-тактического фона и целей за время эксплуатации и в целом за жизненный цикл образца.

Следует отметить, что для поддержания ТУ БЛА на стадии эксплуатации необходимы ремонт и модернизация. Факторами, определяющими моральное старение, являются [40]: создание и начало производства нового образца с более высокими ТТХ и ТУ; принятие на вооружение в других странах новых образцов с повышенными ТТХ и ТУ по сравнению с отечественными образцами;

удешевление производства аналогичного образца с теми же ТТХ за счет применения новых физических принципов действия комплектующих систем и узлов, новых перспективных конструкторских и технических решений и более дешевых технологий и материалов.

К основным направлениям развития разведывательно-ударных и ударных БЛА следует отнести:

- увеличение высоты, скорости, дальности и продолжительности полета;
- обеспечение малой заметности;
- увеличение массы полезной нагрузки;
- обеспечение модульности конструкции;
- обеспечение защиты каналов боевого управления;
- обеспечение автономности;
- повышение маневренности;
- защиты аппарата от средств огневого и электронного поражения противника.

Разведывательно-ударные и ударные БЛА должны решать две основные задачи: ведение наблюдения и разведки и нанесение ударов по наземным/надводным целям. Для выполнения этих задач БЛА должен обладать современными средствами восприятия внешней среды за счет увеличения числа датчиков с определением местоположения целей. При этом, как отмечено в работе рабочей группы Института Митчелла [10], посвященной анализу модели будущей боевой обстановки, большое значение придается дальности действия, объему полезной нагрузки, маневренности и скорости полета.

Достижение превосходства в противоборстве двух сторон в цикле НОРД (наблюдение-ориентация-решение-действие) может быть обеспечено путем опережения противника в движении по циклу НОРД (быстрее обнаружить, оценить ситуацию, выработать решение и противодействовать продвижению противника (затруднение обнаружения за счет снижения заметности или осуществления радиоэлектронной борьбы, осуществление маневра и др.) [41].

В рамках одного борта невозможно объединить все лучшие характеристики. Чрезмерный рост мощности боевой нагрузки приведет к увеличению его массогабаритных параметров, ограничивающих маневрирование аппарата. Только оптимизация всех основных составляющих боевого БЛА дает возможность выполнить заданные требования технического задания. Следует отметить, что дальнейшее развитие БЛА будет связано с повышением уровня автономности за счет внедрения систем управления с элементами искусственного интеллекта.

Научно-исследовательская лаборатория AFRL (Air Force Research Laboratory) ВВС США разработала классификацию уровней автономности, которая содержит 10 уровней [41]. Уровень автономности современных БЛА соответствует 2 уровню (0 – дистанционно пилотируемый аппарат; 1 – выполнение заложенной программы; 2 – возможность изменения заложенной программы; 3 – реакция на события и отказы; 4 – адаптация к событиям и отказам).

Технический уровень существующих БЛА при эксплуатации может снижаться за счет появления новых систем БЛА с более совершенными летно-тактико-техническими характеристиками, подсистемами и конструктивными решениями. Примером модульного построения БЛА может служить концепция модульного БЛА, разработанного компанией Kratos Defence & Security Solutions [42], что дает возможность создания на единой основе нескольких вариантов, предназначенных для выполнения различных групп задач, но и возможность поддерживать ТУ БЛА, заменяя критически важные модули более совершенными модулями с новыми техническими решениями. Кроме того, все разрабатываемые БЛА данного класса должны быть защищены от воздействия молнии и обледенения, а также оборудованы системой предотвращения от столкновений с летательными аппаратами.

При определении ТУ на стадии эксплуатации необходимо отдельно оценивать свойства стабильности и развития БЛА, что должно быть отражено в структуре оценочных показателей. Показатели стабильности такие, как характеристики планера и энергетической установки, должны поддерживаться на уровне технического задания на проектирование БЛА. Показатели развития, характеризующие задачи, решаемые БЛА, следует нацеливать на текущий уровень достижений науки и техники. Решению этой задачи способствует модульный принцип проектирования БЛА. Условием его реализации является обеспечение взаимодействия (интероперабельности) всех подсистем БЛА на стадии проектирования. Такой подход позволит поддерживать надлежащий технический уровень БЛА на этапе эксплуатации с наименьшими затратами.

Заключение

1. При планировании технического уровня БЛА на этапе разработки следует учитывать функциональную разнородность его компонентов. В рамках одной системы она реализуется с применением модульного принципа оформления различных подсистем БЛА. Их исследование ведется в разных предметных областях, а разработка осуществляется разными изготовителями.

2. Технический прогресс в разных предметных областях продвигается с разной скоростью. Это определяет различные сроки морального старения модулей БЛА.

3. Модули БЛА разных изготовителей различаются разной функциональностью, энергетическими и информационными характеристиками и конструктивным исполнением. Это создает проблему замены модулей на более совершенные.

4. Поддержание современного технического уровня БЛА на этапе эксплуатации требует разработки принципов и средств унификации взаимодействия модулей различного назначения на конструктивном, энергетическом и информационном уровне.

5. Наилучшее выполнение цели, поставленной перед конкретным БЛА, требует решения задачи оптимизации состава и технического уровня включаемых в него модулей. Эта задача решается с применением методов многомерного оценивания БЛА по показателям развития путем сопоставления различных вариантов БЛА, либо отнесением варианта БЛА к одному из классов, характеризующих общий технический уровень системы.

Благодарности

Исследования, выполненные по данной тематике, проводились в рамках бюджетной темы FFZF–2022–0004.

Библиографический список

1. Стратегическая сессия по развитию беспилотных авиационных систем. Михаил Мишустин провел стратегическую сессию по развитию беспилотных авиационных систем. URL: <http://government.ru/news/49492> (дата обращения 01.04.2024).
2. Горчица Г.И., Никитин Н.Ф., Слюсарь Ю.Б. и др. Проблема разработки перспективных особо сложных образцов авиационной техники военного назначения и совершенствования порядка их создания // Полет. 2022. № 3. С. 43–50.
3. Судов Е.В., Левин А.И., Петров А.В. и др. Технологии интегрированной логистической поддержки изделий машиностроения. М.: ООО Издательский дом «ИнформБюро», 2006. 232 с.
4. Семенов С.С. Системные исследования беспилотных летательных аппаратов // Боеприпасы. 2021. № 3. С. 107–109.
5. Рецензия Евдокименкова В.Н. и Захарова И.В. на монографию // Боеприпасы. 2021. № 3. С. 114–117.
6. Полтавский А.В., Семенов С.С., Бурба А.А., Нгуен Зуи Фыонг. Информационные процессы в технике: моделирование систем и объектов многофункциональных робототехнических комплексов беспилотной авиации / Под ред. д-ра техн. наук, проф. В.М. Вишневого, ИПУ им. В. А. Трапезникова РАН. Королев: Изд. центр АО «ПСТМ», 2019. 408 с.
7. Семенов С.С. Оценка возможности и пути создания сложных технических систем опережающего уровня в области военных технологий / Выбор наилучших решений при создании сложных технических систем на основе экспертных оценок (отзывы и рецензии на научные издания, посвященные проблемам теории принятия решений) // Боеприпасы. 2020. № 1. С. 11–63.
8. Фаличев О. Перебор технологий. Главная проблема прикладной науки – разобщенность исследователей // Военно-промышленный курьер. 2017. № 21 (685). С. 1, 8.
9. Семенов С.С., Харчев В.Н., Иоффин А.И. Оценка технического уровня образцов вооружения и военной техники. М.: Радио и связь, 2004. 552 с.
10. Чабанов В.А., Яковлева Н.К. Воздушное доминирование как комплексная проблема для ВВС США // Авиационные системы. 2023. № 7. С. 2–18.
11. Петров И.Ф. Авиация и жизнь. М.: ЦАГИ, 1993. 96 с.
12. Кохно П., Костин Д. Модель будущего. М.: Алгоритм, 2013. 752 с.
13. Битунов В.В., Жолков А.С., Пилипчук В.А. Оптимизация уровня унификации новой техники в машиностроении. М.: Машиностроение, 1981. 88 с.
14. Соколов В., Степанов В. Оценка морального старения и военно-технического уровня военной техники // Защита и безопасность. 2007. № 4 (43). С. 18–20.
15. Консон А.С. Технический уровень, надежность и качество продукции: методическое пособие. Л.: ЛИЭИ им. П. Тольятти, 1966. 43 с.
16. Консон А.С. Методы определения технического уровня разработки новых приборов и систем // Экономика приборостроения. М.: Высш. шк., 1980. 572 с.
17. Автономов В.Н. Основы современной техники. М.: Машиностроение, 1991. 304 с.
18. Полтавский А.В., Маклаков В.В., Аверкин А.Е. и др. Системные принципы создания и применения многоцелевых комплексов беспилотных летательных аппаратов. М.: ИПУ РАН, 2010. 102 с.
19. Семенов С.С., Полтавский А.В. Системный подход к формированию облика ударного беспилотного летательного аппарата / Актуальные вопросы исследований в авионике: теория, обслуживание, разработки: Сб. науч. ст. по материалам докл. V Международной НПК «АВИАТОР» (14–15 февраля 2019 г.). Воронеж: ВУНЦ ВВС «ВВА», 2019. 434 с.
20. Семенов С.С., Полтавский А.В. Системные исследования в формировании технического облика беспилотных летательных аппаратов / Материалы XVI Всероссийской научно-технической конференции «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского»: сборник докладов. Гл. ред. С.П. Халютин. М.: Издательский дом Академии имени Н.Е. Жуковского, 2019. 364 с.
21. Семенов С.С., Полтавский А.В. Оценка технического уровня как концептуальный подход к созданию новой конкурентоспособной техники / Материалы XIV Всероссийской научно-технической конференции «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского»: сборник докладов. М.: Издательский дом Академии имени Н.Е. Жуковского, 2017. 592 с.
22. Семенов С.С., Полтавский А.В. Оценка технического уровня – важный инструмент анализа при создании высокотехнологичных систем опережающего уровня на примере оборонно-промышленного комплекса / Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта (CAD/CAM/PDM – 2018). Труды XVIII-й Международной молодеж. конфер. 16–18 окт. 2018 г., г. Москва. Под ред. А.В. Толока. М.: ИПУ РАН, 2018. 400 с.
23. Голубев И.С. Соизмерение технического уровня и эффективности при проектировании конструкций летательных аппаратов. М.: МАИ, 1986. 90 с.

24. Дракин И.И. Основы проектирования беспилотных летательных аппаратов с учетом экономической эффективности. М.: Машиностроение, 1973. 224 с.

25. Семенов С.С., Полтавский А.В., Щербинин В.В. К определению функций ценности единичных оценочных показателей при оценке технического уровня ударных комплексов беспилотных летательных аппаратов // Вопросы оборонной техники. Серия 9. Специальные системы управления, следящие приводы и их элементы. 2012. № 5 (257). С. 56-63.

26. Семенов С.С., Коваленко И.Л., Полтавский А.В. Структура и системы интегральных и единичных оценочных показателей при оценке технического уровня многофункциональных беспилотных летательных аппаратов // Вестник компьютерных и информационных технологий. 2013. № 2. С. 22-27.

27. Семенов С.С., Полтавский А.В., Крянев А.В. Оценка технического уровня многоуровневых сложных технических систем на примере создания многофункциональных комплексов беспилотных летательных аппаратов (МФКБЛА) // Труды международной научно-технической конференции «Научно-технические проблемы построения систем и комплексов землеобзора, дозора и управления и комплексов с беспилотными летательными аппаратами» (23 мая 2013 года): В 2 т. М.: ОАО «Концерн «Вега», 2013. Т. 2. 180 с. С. 148-166.

28. Воронов Е.М., Крянев А.В., Полтавский А.В., Семенов С.С. Особенности оценки технического уровня комплексов беспилотных летательных аппаратов как иерархических систем // Вторая Всероссийская научно-техническая конференция «Навигация, наведение и управление летательными аппаратами» (22-23 сентября 2015 г.). Тезисы докладов. Москва–Раменское: ООО «Научмехиздат», 2015. 308 с. С. 108-113.

29. Микони С.В., Полтавский А.В., Семенов С.С. Системный анализ показателей беспилотных летательных аппаратов / XII мультиконференция по проблемам управления (МКПУ-2019): материалы XII мультиконференции (Дивноморское, Геленджик, 23–28 сентября 2019 г.): в 4 т. // Материалы докладов локальной научно-технической конференции «Управление аэрокосмическими системами» (УАКС-2019): Т. 4. Южный федеральный университет. Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2019. 164 с.

30. Полтавский А.В., Семенов С.С., Бурба А.А. Информационное моделирование оценки технического уровня сложных технических систем // Двойные технологии. 2019. № 4 (89). С. 68-75.

31. Крянев А.В., Семенов С.С., Калдаева А.Э. Методический подход к определению показателей приоритета разведывательно-ударных и ударных беспилотных летательных аппаратов // Надежность. 2020. Т. 20. № 4. С. 50-60.

32. Крянев А.В., Климанов С.Г., Полтавский А.В. и др. Характеристика многофункциональных беспилотных летательных аппаратов по методу Варда // Полет. 2020. № 12. С. 7-25.

33. Свистун И.С. Разработка программного обеспечения к методике сравнительной оценки беспилотных летательных аппаратов / Совершенствование обеспечения полетов авиации. Тезисы докладов XI военно-научной конференции курсантов и молодых ученых БГАА (30.04.2021 г.). Минск: Белорусская государственная академия авиации, 2021. 225 с.

34. Семенов С.С., Полтавский А.В. Оценка технического уровня комплексов беспилотных летательных аппаратов // Материалы Всероссийской научно-технической конференции «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского». Сборник докладов. М.: Издательский дом Академии имени Н.Е. Жуковского, 2013. 568 с.

35. Микони С.В., Семенов С.С. Оценивание рейтинга разведывательно-ударных и ударных беспилотных летательных аппаратов // Полет. 2021. № 6. С. 28-40.

36. Микони С.В., Семенов С.С. Оценивание рейтинга разведывательно-ударных и ударных беспилотных летательных аппаратов в классах массой 0,3-2, 2-6, 6-13, 13-25 т / Материалы XVIII Научно-технической конференции «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского». Сборник докладов под ред. С.П. Халютина. М.: Издательский дом Академии имени Н.Е. Жуковского, 2022. 420 с.

37. Микони С.В., Семенов С.С. Системное оценивание технического совершенства БЛА // Радиоэлектронные технологии. 2023. № 1. С. 66-72.

38. Рецензия Дубовского В.А. на монографию // Боеприпасы. 2021. № 3. С. 117-120.

39. Кошкин Р. О подходах военно-политического руководства Тайваня к разработке БПЛА национального производства // Аэрокосмическое обозрение. № 3. 2023. С. 42-47.

40. Семенов С.С. Вопросы оценки технического уровня сложных технических систем для создания образцов вооружения и военной техники опережающего уровня // Авиационные системы. 2021. № 12. С. 4-10.

41. Самойлов Д.В. Беспилотные комплексы с технологиями искусственного интеллекта как приоритетное направление развития вооружения и военной техники в ведущих зарубежных странах // Авиационные системы. 2022. № 8. С. 2-29.

42. Самойлов Д.В. Беспилотные комплексы с технологиями искусственного интеллекта как приоритетное направление развития вооружения и военной техники в ведущих зарубежных странах // Авиационные системы. 2022. № 9. С. 35-56.

References

1. [Strategic session on the development of unmanned aircraft systems. Mikhail Mishustin held a strategic session on the development of unmanned aircraft systems]. (accessed 01.04.2024). Available at: <http://government.ru/news/49492>. (in Russ.)

2. Gorchitsa G.I., Nikitin N.F., Slyusar Yu.B., Stepanov V.D. On the problem of developing promising especially complex samples of military aviation equipment and enhancement the procedure of their development. *Polyot* 2022;3:43-50. (in Russ.)
3. Sudov E.V., Levin A.I., Petrov A.V. et al. [Technologies of integrated logistics support for mechanical engineering products]. Moscow: Izdatelsky dom "InformBuro"; 2006. (in Russ.)
4. Semionov S.S. [System research of unmanned aerial vehicles]. *Boepripasy* 2021;3:107-109. (in Russ.)
5. [Monograph review by Evdokimenkov V.N. and Zakharova I.V.]. *Boepripasy* 2021;3:114-117. (in Russ.)
6. Poltavsky A.V., Semionov S.S., Burba A.A., Nguyen Zui Phuong, Vishnevsky V.M., Doctor of Engineering, Professor, editor. [Information processes in technology: simulating systems and devices as part of multifunctional robotic unmanned aviation systems]. V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences. Korolyov: Izd. tsentr AO "PSTM"; 2019. (in Russ.)
7. Semionov S.S. [Assessing the feasibility and roadmap for the development of complex, highly advanced military technological systems / Selecting the best solutions as part of complex technological systems development using expert assessments (reviews of research papers in decision-making theory)]. *Boepripasy* 2020;1:11-63. (in Russ.)
8. Falichev O. [Too much technology. The main problem of applied science is the disunity of researchers]. *Voennopromyshlennyi kurier* 2017;21(685):1, 8. (in Russ.)
9. Semionov S.S., Kharchev V.N., Ioffin A.I. [Performance evaluation of weapon systems and hardware]. Moscow: Radio i svyaz; 2004. (in Russ.)
10. Chabanov V.A., Yakovleva N.K. [Air dominance as a multi-pronged problem for the US Air Force]. *Aviatsionnye sistemy* 2023;7:2-18. (in Russ.)
11. Petrov I.F. [Aviation and life]. Moscow: TsAGI; 1993. (in Russ.)
12. Kokhno P., Kostin D. [A model of the future]. Moscow: Algoritm; 2013. (in Russ.)
13. Bitunov V.V., Zholkov A.S., Pilipchuk V.A. [Optimising the degree of component commonality of new technology in mechanical engineering]. Moscow: Mashinostroenie; 1981. (in Russ.)
14. Sokolov V., Stepanov V. [Assessing the obsolescence of the technological level of military equipment]. *Zashchita i bezopasnost* 2007;4(43):18-20. (in Russ.)
15. Konson A.S. [Technological level, reliability and quality of products: a guidance manual]. Leningrad: LIEI im. P. Togliatti; 1966. (in Russ.)
16. Konson A.S. [Methods for identifying the technological level of development of new devices and systems]. Moscow: Vysh. shk.; 1980. (in Russ.)
17. Avtonomov V.N. [Fundamentals of modern technology]. Moscow: Mashinostroyeniye; 1991. (in Russ.)
18. Poltavsky A.V., Maklakov V.V., Averkin A.E., et al. [System principles of the development and application of multipurpose unmanned aerial systems]. Moscow: IPU RAS; 2010. (in Russ.)
19. Semionov S.S., Poltavsky A.V. [A systematic approach to defining the concept of an attack unmanned aerial vehicle]. In: [Topical matters of avionics research; theory, maintenance, developments: Collected papers of the V AVIATOR International Research and Practice Conference]. Voronezh: VUNTS VVS "VVA"; 2019. (in Russ.)
20. Semionov S.S., Poltavsky A.V. [System research as part of defining the technical concept of unmanned aerial vehicles]. In: Khalyutin S.P., editor-in-chief. Proceedings the XVI All-Russian Research and Engineering Conference Scientific Readings on Aviation in memory of N.E. Zhukovsky. Moscow: Zhukovsky Air Force Engineering Academy Publishing; 2019. (in Russ.)
21. Semionov S.S., Poltavsky A.V. [Assessing the technological level as a conceptual approach to the creation of new, competitive engineering products]. In: Proceedings the XIV All-Russian Research and Engineering Conference Scientific Readings on Aviation in memory of N.E. Zhukovsky. Moscow: Zhukovsky Air Force Engineering Academy Publishing; 2017. (in Russ.)
22. Semionov S.S., Poltavsky A.V. [The assessment of the technological level is an important analysis tool as part of advanced high-technology systems development. Case study of the military industrial complex]. In: Tolok A.V., editor. Systems for designing, manufacturing preparation and managing the life cycle of an industrial product (CAD/CAM/PDM – 2018). Proceedings of the XVIII International Youth Conference. Moscow: IPU RAS; 2018. (in Russ.)
23. Golubev S.I. [Commensuration of the technological level and efficiency as part of aircraft structural design]. Moscow: MAI Publishing; 1986. (in Russ.)
24. Drakin I.I. [Fundamentals of the design of unmanned aerial vehicles taking into account the economic efficiency]. Moscow: Mashinostroenie; 1973. (in Russ.)
25. Semionov S.S., Poltavsky A.V., Shcherbinin V.V. [On the definition of individual estimators in assessing the technological level of attack unmanned aerial systems]. In: [Matters of defense technology. Series 9. Special control systems, tracking drives and their components] 2012;5(257):56-63. (in Russ.)
26. Semionov S.S., Kovalenko I.L., Poltavskiy A.V. Estimated figures of the technical level of multi-unmanned aerial vehicles. *Vestnik komp'yuternykh i informatsionnykh tekhnologii* 2013;2:22-27. (in Russ.)
27. Semionov S.S., Poltavsky A.V., Kryanev A.V. [Assessing the technological level of multilevel complex technical systems. Case study of the development of multifunctional unmanned aerial systems (MFUAS)]. In: [Proceedings of the International Science and Engineering Conference Scientific and Technological Problems of the Design of Earth Remote Sensing, Surveillance and Control and Unmanned Aerial Systems: In 2 volumes]. Moscow: JSC Concern Vega. 2013; 2. Pp. 148-166. (in Russ.)
28. Voronov E.M., Kryanev A.V., Poltavsky A.V., Semionov S.S. [The specificity of the evaluation of the technological level of unmanned aerial systems as hierarchical systems]. In: Abstracts of the Second All-Russian Science and Engineering Conference Aircraft Navigation, Guidance

and Control. Moscow-Ramenskoye: Nauchmekhizdat; 2015. Pp. 108-113. (in Russ.)

29. Mikoni S.V., Poltavsky A.V., Semionov S.S. [System analysis of unmanned aerial vehicle performance indicators]. In: proceedings of the XII Multiconference on Management (MCM-2019): materials of the XII Multiconference (Divnomorskoye, Gelendzhik, September 23-28, 2019): in 4 volumes. Local Science and Engineering Conference Aerospace Systems Control (ASC-2019): Vol. 4. Southern Federal University. Rostov-on-Don; Taganrog: Southern Federal University Press; 2019. (in Russ.)

30. Poltavsky A.V., Semionov S.S., Burba A.A. [Information modeling of the assessment of the technological level of complex technical systems]. *Dvoynye tekhnologii* 2019;4(89):68-75. (in Russ.)

31. Kryanev A.V., Semionov S.S., Kaldaeva A.E. A methodological approach to identifying the priority of scout/attack and attack unmanned aerial vehicles. *Dependability* 2020;4:50-60.

32. Kryanev A.V., Klimanov S.G., Poltavsky A.V., Semionov S.S. Characteristics of multifunctional unmanned aircraft by the Ward's method. *Polyot* 2020;12:7-25. (in Russ.)

33. Svistun I.S. [Development of the software for unmanned aerial vehicles benchmarking methodology]. In: [Improving flight operations support. Abstracts of the XI Military Research Conference of Cadets and Young Scientists of the BGAA]. Minsk: Belarusian State Aviation Academy; 2021. (in Russ.)

34. Semionov S.S., Poltavsky A.V. [Assessing the technological level of unmanned aerial systems]. In: [Proceedings of the All-Russian Science and Engineering Conference Scientific Readings on Aviation in Memory of N.E. Zhukovsky]. Moscow: Zhukovsky Air Force Engineering Academy Publishing; 2013. (in Russ.)

35. Mikoni S.V., Semyonov S.S. Rating Assessment of Reconnaissance-Strike and Strike Unmanned Aerial Vehicles. *Polyot* 2021;6:28-40. (in Russ.)

36. Mikoni S.V., Semionov S.S. [Rating of scout and attack unmanned aerial vehicles in the 0.3-2, 2-6, 6-13, and 13-25-ton weight classes]. In: [Khaliutin S.P., editor. Proceedings of the XVIII Science and Engineering Conference Scientific Readings on Aviation in Memory of N.E. Zhukovsky]. Moscow: Zhukovsky Air Force Engineering Academy Publishing; 2022. (in Russ.)

37. Mikoni S.V., Semionov S.S. [System assessment of the technological performance of UAVs]. *Radioelektronnyye tekhnologii* 2023;1:66-72. (in Russ.)

38. [Monograph review by Dubovsky V.A.]. *Boepripasy* 2021;3:117-120. (in Russ.)

39. Koshkin R. [On the approaches of the political and military leadership of Taiwan to the development of domestically-designed UAVs]. *Aerokosmicheskoye obozreniye* 2023;3:42-47. (in Russ.)

40. Semionov S.S. [Matters of assessment of the technological level of complex technical systems for creating

advanced weapons and military equipment]. *Aviatsionnyye sistemy* 2021;12:4-10. (in Russ.)

41. Samoilov D.V. [AI-enabled unmanned aerial systems as a priority direction for the development of weapons and military equipment in the leading foreign countries]. *Aviatsionnyye sistemy* 2022;8:2-29. (in Russ.)

42. Samoilov D.V. [AI-enabled unmanned aerial systems as a priority direction for the development of weapons and military equipment in the leading foreign countries]. *Aviatsionnyye sistemy* 2022;9:35-56. (in Russ.)

Сведения об авторах

Микони Станислав Витальевич – доктор технических наук, профессор, член Российской ассоциации искусственного интеллекта, ведущий научный сотрудник, Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН). Санкт-Петербургский институт информатики и автоматизации Российской Академии Наук (СПИИ-РАН). Санкт-Петербург, Российская Федерация, e-mail: smikoni@mail.ru

Семенов Сергей Сергеевич – кандидат технических наук, руководитель группы анализа и перспективного проектирования, АО «Государственное научно-производственное предприятие «Регион», Москва, Российская Федерация, e-mail: gnppregion@sovintel.ru

About the authors

Stanislav V. Mikoni, Doctor of Engineering, Professor, Member of the Russian Association of Artificial Intelligence, Lead Researcher, St. Petersburg Federal Research Center of the Russian Academy of Sciences. St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences. Saint Petersburg, Russian Federation, e-mail: smikoni@mail.ru.

Sergey S. Semionov, Candidate of Engineering, Head of Group for Analysis and Advanced Engineering, Region Public Research and Development Company, Moscow, Federation Moscow, e-mail: gnppregion@sovintel.ru.

Вклад авторов в статью

Микони С.В. Постановка задачи, разработка методологии и результаты оценивания ТУ, рассмотрение особенностей ТУ БЛА на этапе эксплуатации, заключение.

Семенов С.С. Постановка задачи, ретроспективный анализ исследований по оцениванию и динамике ТУ на жизненном цикле БЛА, разработка методологии оценивания ТУ и рассмотрение особенностей ТУ БЛА на этапе эксплуатации, библиографический список литературы.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Концепция безопасности движения в струнном транспортном комплексе

The concept of movement safety in a string transportation system

Юницкий А.Э.¹, Гарах В.А.¹, Литвинович Т.С.¹, Шевченко Д.Н.^{1*}
Unitsky A.E.¹, Harakh V.A.¹, Litvinovich T.S.¹, Shevchenko D.N.¹

¹ЗАО «Струнные технологии», Минск, Республика Беларусь

¹Unitsky String Technologies Inc., Minsk, Republic of Belarus

*d.shevchenko@unitsky.com



Юницкий А.Э.



Гарах В.А.



Литвинович Т.С.



Шевченко Д.Н.

Резюме. Цель. Рассмотреть структуру и составляющие безопасности существующих транспортных систем, чтобы на их основе рассматривать все множество опасностей и угроз, характерных для инновационного рельсо-струнного транспорта. Определить конкретные условия и функции эффективного и безопасного движения рельсовых транспортных средств, чтобы на их основе формировать требования к разрабатываемой АСУ перевозочным процессом. **Методы.** Проведен анализ нормативных документов, посвященных вопросам безопасности существующих транспортных систем, а также условий и функций обеспечения безопасности движения рельсового транспорта. Рассмотрены вопросы полноты и корректности предлагаемых функций, особенностей их реализации, предусмотренных различными стандартами. **Результаты.** Предложен набор базовых элементарных функций безопасности движения рельсового транспорта, на основе которых детализируются алгоритмы функционирования подсистем струнного транспортного комплекса. Даны комментарии об особенностях реализации функций. Предложена терминология безопасности струнного транспортного комплекса и взаимосвязи ее составляющих: безопасности эксплуатации, функциональной безопасности и безопасности движения. **Заключение.** Предлагаемая терминология и набор базовых функций безопасности движения позволяют систематизировать разработку современной безопасной АСУ перевозочным процессом. Использование элементарных несовместных функций безопасности движения допускает их модульную (независимую) реализацию, позволяет минимизировать их количество. Это способствует снижению трудоемкости разработки и подтверждения соответствия АСУ предъявляемым требованиям.

Abstract. Aim. To examine the structure and safety components of existing transportation systems to use them as the foundation for the study of the whole set of hazards and threats that are typical for innovative string rail transportation. To identify specific conditions and functions of efficient and safe movement of rail vehicles in order to enable the definition of the requirements for the automated traffic management system under development. **Methods.** The authors analyse the regulatory documents dealing with the safety of existing transportation systems, as well as the conditions and functions associated with ensuring the safety of rail vehicles. The paper examines the matter of completeness and correctness of the proposed functions, distinctive features of their implementation required by various standards. **Results.** The authors propose a set of basic elementary functions of rail vehicle movement that are used for constructing detailed algorithms of operation of a string transportation systems. Comments are given regarding the implemented functionalities. The authors propose a terminology of string transportation system safety and its components interrelation, i.e., operational safety, functional safety, and movement safety. **Conclusion.** The proposed terminology and set of basic movement safety functions allow organising the development of a modern safe automated traffic management system. The use of elementary incompatible movement safety functions allows for their modular (independent) implementation and minimisation. That helps reduce the efforts associated with the development and confirmation of compliance of the automated management system with the relevant requirements.

Ключевые слова: рельсовое транспортное средство, струнный транспорт, безопасность транспортного комплекса, безопасность эксплуатации, безопасность движения рельсовых транспортных средств, функция безопасности.

Keywords: rail vehicle, string transportation, transportation system safety, operational safety, safe movement of rail vehicles, safety function.

Для цитирования: Юницкий А.Э., Гарах В.А., Литвинович Т.С., Шевченко Д.Н. Концепция безопасности движения в струнном транспортном комплексе // Надежность. 2024. №2. С. 61-71. <https://doi.org/10.21683/1729-2646-2024-24-2-61-71>

For citation: Unitsky A.E., Harakh V.A., Litvinovich T.S., Shevchenko D.N. The concept of movement safety in a string transportation system. Dependability 2024;2:61-71. <https://doi.org/10.21683/1729-2646-2024-24-2-61-71>

Поступила: 26.01.2024 / **После доработки:** 08.04.2024 / **К печати:** 10.06.2024

Received on: 26.01.2024 / **После доработки:** 08.04.2024 / **К печати:** 10.06.2024

Введение

Важным условием успешного внедрения инновационных транспортных систем является высокий уровень безопасности перевозочного процесса. В том числе, в сравнении с существующими видами транспорта (например, концепция допустимого риска ГАМАВ [1]). Поэтому требуется уточнить понятия безопасности транспортной системы, безопасности перевозочного процесса, безопасности движения транспортных средств, определить конкретные принципы, условия, критерии с учетом опыта существующих видов транспорта.

Базовое определение безопасности как отсутствие недопустимого риска [1] для транспортных систем уточняется и детализируется в зависимости от опасностей и угроз (прежде всего – видов опасностей и их причин), характерных для того или иного вида транспорта. Наиболее полное рассмотрение составляющих безопасности дается в технических регламентах таможенного союза (ТР ТС) для инфраструктуры (рис. 1) ж.-д. транспорта [2]; для ж.-д. подвижного состава [3], где составляющие аналогичны рис. 1, но отсутствует промышленная, информационная безопасность и безопасность зданий и сооружений, дополнительно присутствует химическая безопасность; для колесных транспортных средств [4].

Для реализации (синтеза) инновационных струнных транспортных комплексов (СТК) [5, 6] требуется корректный учет всех составляющих безопасности и взаимосвязи между ними. Тем не менее, четкая систематизация составляющих безопасности транспортного комплекса (системы) в ТР ТС и ссылочных стандартах отсутствует. В частности, не уточняются различия биологической, санитарно-эпидемиологической и экологической безопасности; безопасность работы приборов и оборудования при электромагнитных воздействиях, как и термическая безопасность, рассматривается отдельно от безопасности излучений. Некоторые составляющие в ТР ТС и ссылочных стандартах определены не точно или вовсе не определены (на рис. 1 выделены полужирным).

Отдельная терминологическая проблема связана с «безопасностью движения» (поездов). Фундаментальный анализ и предложения по указанному понятию даны в работах [7, 8], где было проанализировано более 15 альтернативных формулировок; а также в монографиях [9, 10]. Но внедрение результатов проведенного анализа нельзя считать успешным: в стандарте ГОСТ Р 55056-2012 [11] присутствовали определения «Безопасность движения (эксплуатации) железнодорожного транспорта», «Безопасность движения поезда»; но они были исключены из заменяющего ГОСТ 34530-2019 [12], где



Рис. 1. Составляющие безопасности инфраструктуры ж.д. транспорта

сохранено лишь понятие «Нарушение безопасности движения».

Анализируя существующие определения «безопасности движения» [7-12] можно заметить, что некоторые из них являются весьма абстрактными или, напротив, определяют значение частного количественного показателя (например, количество происшествий), или не являются актуальными, поскольку не используют современный риск-ориентированный подход. Но главная проблема существующих определений «безопасности движения» – отсутствие конкретных (формализованных) условий безопасного движения поездов. Зачастую условия безопасности движения скрываются за принципами и алгоритмами работы используемых систем ж.-д. автоматики и телемеханики (СЖАТ) [13, 14]. А при модернизации СЖАТ эти принципы чаще не уточняются, а наследуются.

Важно представлять базовые (исходные) и элементарные (неразложимые) условия безопасности движения рельсовых транспортных средств (РТС), на основе которых можно формировать требования к новым автоматизированным системам управления (АСУ) перевозочным процессом. Также важно определить базовые функции безопасности движения, чтобы на их основе без рудиментных подсистем и функций формировать требования для СТК [5].

Основные цели работы:

1) определить базовые (исходные) и элементарные (неразложимые) условия безопасности движения РТС,

на основе которых можно:

- формировать требования к новым АСУ,
- строить новые эффективные АСУ без рудиментных подсистем и функций;

2) определить место «безопасности движения» РТС в структуре составляющих безопасности СТК.

Анализ условий и функций обеспечения безопасности движения РТС

Для достижения поставленных целей были проанализированы определения отдельных видов нарушений безопасности движения поездов (табл. 1), перечисленные в пособии [8]; функции обеспечения безопасного движения поездов (АТР-функции, Automatic Train Protection), предусматриваемые пятью специализированными стандартами для рельсового транспорта [15-19]; а также статья [20], в которой помимо принципов построения безопасных систем автоведения указываются некоторые функции и условия безопасности движения автотранспорта (рулевое управление, торможение/ускорение, обнаружение и реакция на подвижные и неподвижные препятствия, помощь в соблюдении дистанции, формирование автоколонн, удержание на полосе, обеспечение скоростного режима).

В табл. 2–6 приведены перечни и выполнен анализ функций безопасности движения РТС, предписываемых стандартами, соответственно:

Табл. 1. Виды нарушений безопасности движения поездов [8]

Виды нарушений безопасности движения	Комментарий
Прием поезда на занятый путь	Фактически, подача ложной разрешающей команды на движение, без предварительной подготовки маршрута
Отправление поезда на занятый перегон (блок-участок)	
Прием поезда по неготовому маршруту	
Отправление поезда по неготовому маршруту	
Уход подвижного состава на маршрут приема, отправления поезда на перегон	Несанкционированное перемещение подвижного состава без команды
Столкновение поездов и подвижного состава	Является возможным следствием других видов нарушения безопасности движения
Сход подвижного состава	Может быть обусловлен 1) превышением допустимой скорости, 2) техническими отказами (пути, подвижного состава), 3) приемом поезда по неподготовленному маршруту
Остановка поезда на перегоне с занятием его более 1 часа сверх времени, установленного расписанием	Не является опасным событием, хотя влечет экономические потери
Отцепка вагонов от поездов в пути следования по причине букс и другим техническим неисправностям	
Перекрытие разрешающего показания сигнала на запрещающее	
Развал груза в пути следования	Касается технического состояния груза и РТС
Общий комментарий:	
- перечень условий безопасности движения не является полным. Отсутствует функция позиционирования подвижного состава, обеспечения безопасного гарантированного торможения;	
- часть условий – лишние, фактически являются нарушением лишь безотказности перевозочного процесса, но не его безопасности	

Табл. 2. Функции АТР, регламентируемые стандартом ИЕС 62290 [16, п. 6.2.1]

Функции АТР	Комментарий
I1) обеспечение безопасного маршрута, когда все требуемые элементы пути заблокированы в определенных состояниях для беспрепятственного пропуска РТС, а также для избежания их использования другими РТС	—
I2) обеспечение безопасного интервального регулирования РТС. Безопасное интервальное регулирование движения РТС должно быть основано на принципе мгновенной остановки впередиидущего поезда. Для предотвращения столкновения между попутно следующими поездами безопасное интервальное регулирование движения поездов должно обеспечиваться таким образом, чтобы постоянно соблюдалась безопасная дистанция между поездами, превышающая длину тормозного пути	Функция не является базовой (элементарной, исходной). Фактически подразумевается следующее: - недопустимо соударение РТС между собой; - впереди идущее РТС может останавливаться мгновенно; - должна обеспечиваться функция безопасного торможения. Памятка ОСЖД по интервальному регулированию [21, п. 5.4.13] дополнительно регламентирует требование I2 с использованием функции служебного торможения и дополнительным интервалом безопасности в 300 м
I3) обеспечение безопасной скорости передвижения	—
I4) движение РТС только после получения соответствующего разрешения	Поскольку в процессе движения возможно изменение технологического и технического состояния объектов транспортной системы (РТС, стрелок и других объектов инфраструктуры), то желательна реализация периодического разрешения на движение (продолжение). Подробные рекомендации к периодичности управляющих воздействий содержатся в стандарте [22]
Общий комментарий: - перечень условий безопасности движения не является полным. Отсутствует функция <i>позиционирования подвижного состава</i> , которая (однако) указана в области применения стандарта ИЕС 62290	

Табл. 3. Функции АТР, регламентируемые стандартом ГОСТ Р [18, п. 5.2.1]

Функции АТР	Комментарий
G1) Интервальное регулирование движения поездов	1) позиционирование поездов рассматривается подфункцией интервального регулирования; 2) функция G1 аналогична функции M2, но в стандарте [18] отсутствуют необходимые уточнения относительно дистанции между поездами, принципа мгновенной остановки предыдущего поезда, имеющихся в ИЕС 62290 [16], а также предполагаемой к использованию функции торможения (служебное или экстренное)
G2) Обеспечение безопасной скорости движения поезда	Функция не является базовой (элементарной, исходной). Фактически подразумевается следующее: - недопустимо соударение РТС между собой; - впереди идущее РТС может останавливаться мгновенно; - должна обеспечиваться функция безопасного торможения
G3) Разрешение на движение поезда включая: установление границ разрешения на движение РТС; определение профиля скорости для обеспечения безопасности движения поезда (для движения в пределах разрешенной скорости и разрешенной дистанции для проследования); разрешение на проследование РТС по путевым сигналам	Первая подфункция аналогична функции I1 [16] обеспечения безопасного маршрута. Вторая подфункция дублирует функцию G2
G4) Контроль движения поезда, включая: определение фактической скорости движения поезда; контроль безопасной скорости движения поезда; мониторинг ограничения скорости в отдельных местах; контроль скатывания поезда; реагирование при несанкционированном движении поездов без бортовой системы	Подфункция 1 дублирует функцию позиционирования. Подфункции 2 и 3 реализуются функцией G2. Контроль скатывания реализуется функцией позиционирования. Последняя подфункция обеспечивается совместно функцией позиционирования, функцией безопасного торможения и функцией I1 обеспечение безопасного маршрута [16]
G5) Обеспечение интерфейса с системами электрической централизации и интервального регулирования	Рассматриваемая система как раз выполняет функции СЖАТ на станциях/перегонах. Вероятно, подразумевается интерфейс с внешними СЖАТ, но это спорное требование, дублирующее все прочие требования
Общий комментарий: - состав функций безопасности движения стандарта [18] является неполным. Отсутствует обязательная <i>функция безопасного торможения</i> и функция <i>блокировки несанкционированного открытия дверей</i> , необходимая для РТС со стоячими местами для пассажиров. С учетом дополнительных функций сцепки/расцепки локомотива [18, п. 5.2.5], функция <i>контроля целостности поезда</i> должна быть перенесена из [18, п. 5.2.6] в обязательные функции безопасности движения [18, п. 5.2.1]; - функция <i>контроля свободности пути</i> [18, п. 5.2.2], фактически используемая для установления границ разрешения на движение (функция G3), некорректно вынесена из перечня обязательных функций безопасности движения; - функции плохо структурированы, имеются многочисленные пересечения и частичные дублирования	

Табл. 4. Функции АТР, регламентируемые стандартом ANSI [17]

Функции АТР	Комментарий
A1) Обнаружение присутствия и позиционирование РТС. АСУ должна контролировать наличие каждого РТС и его координату (с заданной точностью)	
A2) Интервальное регулирование, обеспечивающее защиту от столкновений попутно следующих поездов за счет сохранения дистанции, которая постоянно обеспечивает достаточный тормозной путь для следующего поезда при условии, что идущий впереди поезд может остановиться мгновенно. Тормозной путь определяется для наихудших условий (наибольшего ускорения, наибольшей массы, наименьшего сцепления колесо-рельс, наибольшей скоростью попутного ветра, наибольшие допустимые суммарные задержки и т. п.)	Данная функция не является базовой (элементарной, исходной), а обеспечивается тремя другими функциями: - обеспечения безопасного маршрута; - обеспечение позиционирования РТС (включая направление движения); - обеспечение безопасного торможения
A3) Обнаружение непреднамеренного движения (с реализацией экстренного торможения)	—
A4) Защита от превышения скорости	—
A5) Защита от проезда допустимой границы	Данная функция обеспечивается тремя другими функциями: - обеспечения безопасного маршрута; - обеспечение позиционирования РТС; - обеспечение безопасного торможения
A6) Защита от разделения состава (опционально, для составных РТС, если составляющие индивидуально не выполняют функцию A1)	Данная функция обеспечивается двумя другими функциями: - обеспечения безопасного маршрута; - обеспечение позиционирования разделенных фрагментов РТС
A7) Защита от потери сигнала. Предусматривается наличие периодического воздействия на объекты транспортной системы, указывающего на выполнение прочих условий безопасности. Отсутствие воздействия должно инициировать переход объектов транспортной системы в защитное состояние. Например, для РТС предусматривается экстренное торможение	—
A8) Обнаружение нулевой скорости. В стандарте [17] предлагается пороговое значение 0,3 м/с	Данная функция дублирует функцию позиционирования (включая измерение скорости)
A9) Блокировка несанкционированного открытия дверей РТС. Для РТС предполагается проверка 4 условий: позиционирование перед платформой, нулевая скорость, отключение тяги, активация удерживающего или стояночного торможения	Для СТК помимо 4-х условий, указанных в стандарте [17, п. 5.1.10] дополнительно предусматривается отсутствие запрета на открытие двери от ЦСУ, который может выдаваться в нестандартных ситуациях
A10) Защита от несанкционированного открытия дверей РТС или платформенных. При несанкционированном открытии дверей РТС должно инициироваться торможение. При несанкционированном открытии платформенных дверей должен запрещаться въезд РТС на станцию, или инициироваться торможение РТС, уже находящихся на станции. Восстановление автоматизированного режима перевозочного процесса должно выполняться после гарантированного устранения опасностей	Имеется большое количество других причин (связанных с отказами РТС), требующих замену точки прицельного торможения РТС и режима движения. Функция дублирует другие функции. Также функция занимается минимизацией последствий опасности, а не устранением причин
A11) Блокировка отправления РТС без проверки успешного запирания всех дверей	Это не единственная возможная причина блокировки отправления РТС. Для СТК кроме условия, указанного в стандарте [17, п. 5.1.11], предусматриваются дополнительные проверки: - наличие команды на начало движения; - отсутствие диагностируемых критических отказов, приводящих к снижению уровня безопасности выполнения перевозочного процесса; - штатное состояние подсистем РТС (достаточный заряд накопителя, объем жидкостей в гидросистемах и т. д.)
A12) Блокировка изменения направления движения	Данная функция не базовая. Она обеспечивается функциями: - обеспечения безопасного маршрута; - обеспечение позиционирования РТС (включая направление движения); - блокировка отправления
A13) Невозвратность функции экстренного торможения	Данное требование не является базовым. Кроме того, оно является спорным, учитывая, что экстренное торможение (в отличие от аварийного) является регулируемым/ контролируемым [23]. Стандарт CBTC [15] явно предусматривает отмену функции экстренного торможения после устранения причин опасностей, вызвавших активацию данной функции
A14) Блокировка стрелок. Запрещается въезд РТС на стрелку, неподготовленную для беспрепятственного проезда РТС в нужном направлении. Кроме того, блокируется изменение состояния стрелки, подготовленной для проследования некоторого РТС	Данная функция дублирует функцию обеспечения безопасного маршрута
<i>Общий комментарий:</i> многие функции не являются базовыми; часть функций дублируется	

Табл. 5. Функции АТР, регламентируемые стандартом СВТС [15, п. 6.1]

Функции АТР	Комментарий
С1) Определение местоположения/скорости поезда	—
С2) Безопасное интервальное регулирование с соблюдением следующих принципов: - возможна мгновенная остановка впередиидущего РТС; - расчет АТР-профиля для существующих скоростных ограничений трассы и команды на движение с обозначенной границей разрешения движения и модели безопасного торможения с использованием функции экстренного торможения	Функция не является базовой (элементарной, исходной). Фактически подразумевается следующее: - недопустимо соударение РТС между собой; - впередиидущее РТС может останавливаться мгновенно; - должна обеспечиваться функция безопасного торможения
С3) Защита от превышения скорости и обеспечение торможения	Данная функция не является базовой, очевидно разделяется на две. Причем функция обеспечения безопасной кривой торможения используется и в других функциях безопасности СВТС (например, С2)
С4) Защита от отката РТС (назад)	Несанкционированное движение РТС в противоположном направлении в целом более опасно, чем несанкционированное движение в установленном направлении, но вызывает сомнение необходимость выделения отдельной функции взамен совокупности функций: - позиционирования; - обеспечение гарантированного торможения; - построения маршрута (для следующего РТС с учетом новой позиции откатившегося РТС)
С5) Защита от предела пути	Данная функция является производной от функций: - позиционирования; - построения маршрута (для данного РТС); - обеспечение гарантированного торможения
С6) Защита разделения и сцепка/расцепка поездов	—
С7) Определение нулевой скорости	—
С8) Блокировка несанкционированного открытия двери РТС	—
С9) Блокировка начала движения РТС	—
С10) Экстренное торможение	Использование данной функции предполагается при расчете АТР-профиля (функция С2)
С11) Замыкание маршрута	Данная функция аналогична функции П1
С12) Блокировка изменения направления движения	—
С13) Защита рабочей зоны	Данная функция предусматривает использование временных ограничений и ограничений, устанавливаемых вручную
С14) Контроль исправности путевой структуры	Данная функция должна реализовываться не только для путевой структуры, но и для подвижного состава и для прочих объектов инфраструктуры, обеспечивающих перевозочный процесс (станционные ворота, платформенные двери, стрелки и т. д.). Данная функция не базовая. Она может реализовываться базовыми функциями: - периодическое разрешение на движение; - работа с маршрутами
С15) Переездная сигнализация	Данная функция не требуется для СТК, не имеющего пересечения в одном уровне с другими видами транспорта
С16) Защита ограничения маршрута	—
Общий комментарий: многие функции не являются базовыми; часть функций дублируется	

Табл. 6. Функции АТР, регламентируемые стандартом IMA [19, п. 11.1]

Функции АТР	Комментарий
М1) Определение (только) местоположения поезда	Определение скорости выделено в отдельную функцию; определение направления движения РТС не включено в перечень
М2) Безопасное интервальное регулирование с соблюдением следующих принципов: - в штатных алгоритмах используется служебное торможение, а в нештатных ситуациях – возможно экстренное торможение; - обеспечение функции безопасного торможения в соответствии с СВТС [15]	Кроме торможения функция М2 ничего не предполагает
М3) Блокировка несанкционированного движения с использованием безвозвратного экстренного торможения (отмена персоналом)	Невозвратность экстренного торможения спорна и противоречит СВТС [15]
М4) Защита от превышения скорости	–
М5) Защита от разделения поезда с использованием невозвратного экстренного торможения каждой части	Актуальность и невозвратность экстренного торможения спорны, особенно для частей с независимым позиционированием и управлением
М6) Безотказная и безопасная передача сообщений на/от подвижной состав. Предполагается периодическая передача разрешения на движение	По описанию функция схожа с функцией А7 Защита от потери сигнала. Функция дублирует функцию М3
М7) Блокировка несанкционированного открытия дверей РТС	–
М8) Открытие дверей при выполнении ряда условий, аналогичных функции А10 [17, п. 5.1.10]	–
М9) Блокировка отправления РТС при несоответствии технологического состояния дверей (закрыты и заперты) и тормозной системы (выключена)	Не рассмотрены другие подсистемы РТС, а также техническое состояние (наличие критических отказов) РТС
М10) Управление платформенными дверями	Функция спорно внесена в перечень функций безопасности; должна быть обоснована с учетом условий эксплуатации станции
М11) Блокировка участков пути на станции при неисправности платформенных дверей	Производная от функции обеспечения безопасного маршрута
М12) Блокировка обратного движения	Не введена функция определения направления движения
М13) Блокировка маршрутов	Функция аналогична функции П1 обеспечения безопасного маршрута
М14) Предотвращение отказа функции служебного торможения	Функция аналогична «обеспечению безопасного торможения» функцией М2
М15) Измерение скорости	Реализация данной функции непосредственно связана с определением местоположения РТС. Поэтому целесообразно объединение функций М1 и М15
М16) Защита конца пути	По описанию функция схожа с функцией С5
М17) Обнаружение дверей объекта и реагирование на них [19, п. 11.1.17].	Функция не определена
М18) Обнаружение препятствий при движении	С учетом наличия функции М13 данную функцию стоит вынести из перечня функций безопасности движения
М19) Безопасное управление стрелками	–
М20) Блокировка аварийного отпирания двери РТС изнутри	–
<i>Общий комментарий:</i> многие функции не являются базовыми; часть функций дублируется	

- ИЕС 62290-1:2014 [16] – стандарт по системам управления и контроля городским и пригородным ж.-д. транспортом (UGTMS);
- ГОСТ Р 70059-2022 [18] – стандарт, базирующийся на стандарте UGTMS;
- ANSI / ASCE / T&DI 21:2021 [17] – стандарт по перспективным видам рельсового транспорта;
- IEEE 1474.1:2004 [15] – стандарт по управлению поездами на основе радиосвязи (CBTC);
- стандарт международной ассоциации монорельсовых дорог (IMA) [19].

Предлагаемый набор условий и базовых АТР-функций СТК

На основе проведенного анализа (см. комментарии в табл. 1–6) предлагается следующий состав условий и базовых функций безопасности движения РТС для их реализации АСУ в условиях СТК.

Условие 1. Недопустимо соударение РТС с препятствиями (другими РТС, объектами инфраструктуры).

Условие 2. Возможна мгновенная остановка (впереди) движущегося РТС [15–17, 21].

U1) Позиционирование РТС: определение местоположения, скорости и направления движения каждого отдельного РТС с установленной точностью.

Примечание. Многомодульные (разделяемые) РТС должны обеспечивать независимое позиционирование каждого отдельного модуля (в противном случае список базовых функций должен быть дополнен функцией защиты от разделения состава).

U2) Защита от превышения скорости движения, установленной для каждого конкретного участка трассы с учетом его особенностей и технических характеристик РТС.

U3) Обеспечение безопасного торможения РТС, используемого в алгоритмах автоведения и интервального регулирования, с учетом всех задержек и составляющих, предусмотренных СВТС [15], а также с учетом гарантированных значений замедления, реализуемых для конкретного участка трассы и наихудших погодных условий (как предусмотрено стандартами [16, 17]) функцией служебного торможения (как предусмотрено стандартами [16, 17, 19, 21]) при наихудшем одиночном отказе тормозного оборудования (как предусмотрено стандартом [17]).

Примечание. Функция служебного торможения реализуется «рабочим» тормозным оборудованием РТС, не влекущим повышенный износ подвижного состава и путевой структуры, допускает отмену функции торможения и многократное повторное применение. Функции экстренного и аварийного торможения [23] предусматриваются для остановки РТС в качестве дополнительной эшелонированной защиты в нештатных ситуациях.

U4) Обеспечение безопасного маршрута, когда все требуемые участки пути и автоматизированные объекты инфраструктуры (стрелки и др.) заблокированы в определенных состояниях для беспрепятственного пропуска конкретного РТС, а также для исключения их использования другими РТС.

U5) Обеспечение движения РТС (продолжение или возобновление) только по команде, соответствующей подготовленному безопасному маршруту.

Примечание. Поскольку в процессе движения возможно изменение технологического и технического состояния объектов транспортной системы (РТС, стрелок и других объектов инфраструктуры), то команда

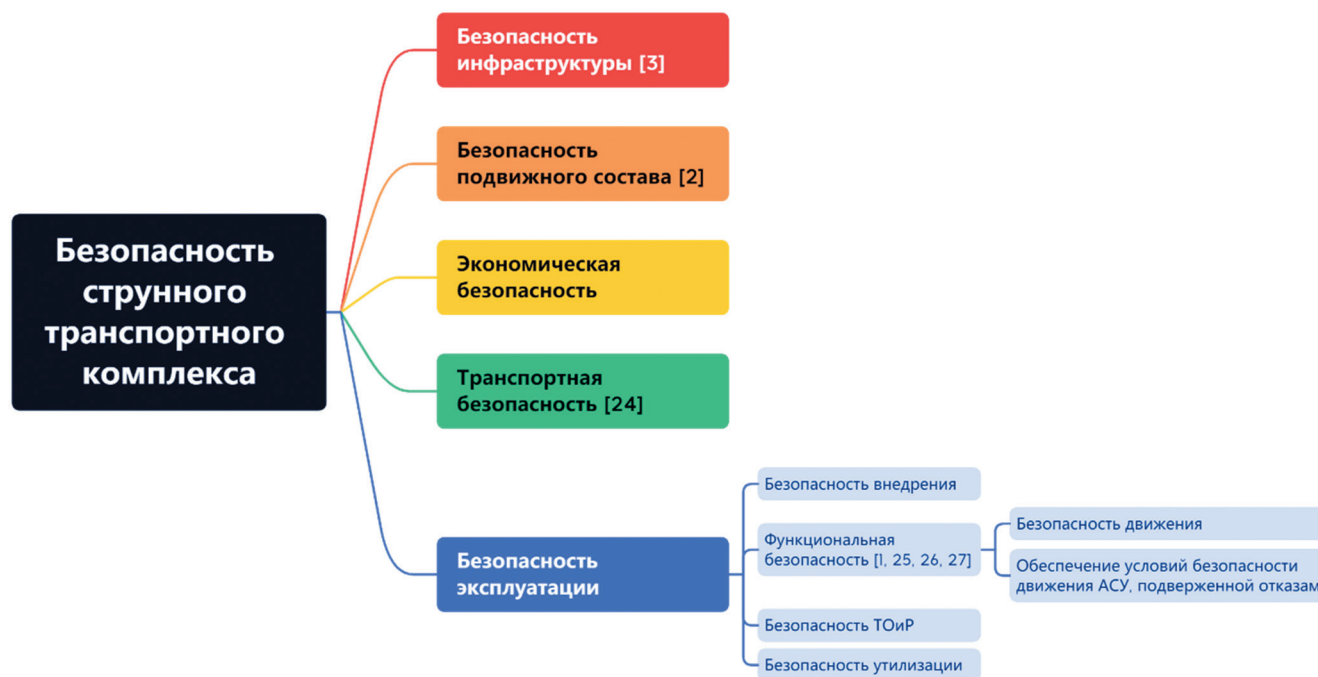


Рис. 2. Составляющие безопасности СТК

на движение должна периодически актуализироваться (повторяться или отменяться).

У6) Блокировка начала движения при невыполнении хотя бы одного условия, связанного с технологическим (заперты двери, заряжена батарея и т.д.) и техническим состоянием РТС (нет или не диагностированы отказы).

У7) Блокировка открытия дверей при невыполнении хотя бы одного условия: позиция двери РТС соответствует платформе; скорость РТС равна нулю; отключена тяга; включена функция удерживающего или стояночного торможения; имеется команда на открытие двери РТС из центра управления.

Полнота и корректность предложенного набора базовых функций подтверждается тем, что на его основе могут быть получены функции стандартов [15–19], а также возможностью формирования прочих умозаключений об алгоритмах организации перевозочного процесса. Например, из двух условий и функции безопасности движения U3 следует, что дистанция между попутно следующими РТС должна быть не меньше гарантированной длины тормозного пути РТС. Из условия 2 и функции U1 следует, что местоположение РТС считается неизменным до тех пор, пока не получена информация о новом местоположении РТС.

Понятие и структура безопасности струнного транспортного комплекса

На основе проведенного анализа терминологии безопасности и ее применения на ж.-д. транспорте, пользуясь правом разработчика СТК и его основных компонентов (путевой структуры, подвижного состава, АСУ), сформулируем следующие определения.

Безопасность СТК – свойство СТК и его компонентов, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью людей, имуществу, а также окружающей среде, жизни или здоровью животных и растений.

Безопасность эксплуатации СТК – свойство СТК, связанное с отсутствием недопустимых рисков, обусловленных технологическими процессами функционирования СТК, в частности, выполнения перевозочного процесса.

Безопасность движения РТС – свойство перевозочного процесса СТК, связанное с отсутствием недопустимых рисков, обусловленных нарушением условий и функций обеспечения безопасности движения (перечисленных в предыдущем разделе).

Также представим свое видение относительно структуры свойства безопасности СТК: предполагается учитывать все опасности, регламентируемые ТР ТС 001, ТР ТС 003, а также экономическую и транспортную безопасность [11, 24], характерные для транспортных систем (рис. 2).

Что касается взаимосвязи «безопасности эксплуатации», «безопасности движения» и «функциональной безопасности», то функциональную безопасность

предлагается рассматривать (см. рис. 2) частью безопасности эксплуатации, наряду с составляющими, характерными для этапов внедрения и утилизации, технического обслуживания и ремонта (ТОиР) объектов СТК. В свою очередь функциональную безопасность, как способность объекта выполнять все предусмотренные функции безопасности при всех предусмотренных условиях [1, 25–27] (в том числе при воздействии допустимых отказов), предлагается детализировать на «безопасность движения» (соответствующие условия и функции были рассмотрены выше), а также обеспечение условий безопасности движения при наличии отказов в компонентах СТК.

Библиографический список

1. IEC 61508-2010 Functional safety of electrical/electronic/programmable electronic safety-related systems.
2. ТР ТС 001/2011. О безопасности железнодорожного подвижного состава: Технический регламент Таможенного союза / Евразийская экономическая комиссия. Введ. 2014-08-02. Минск: Госстандарт: БелГИСС, 2012. VI, 52 с.
3. ТР ТС 003/2011. О безопасности инфраструктуры железнодорожного транспорта: Технический регламент Таможенного союза / Евразийская экономическая комиссия. Введ. 2014-08-02. Минск: Госстандарт: БелГИСС, 2012. VI, 56 с.
4. ТР ТС 018/2011. О безопасности колесных транспортных средств: Технический регламент Таможенного Союза / Евразийская экономическая комиссия. Введ. 2015-01-01. – URL: https://eec.eaeunion.org/upload/medialibrary/2a3/TR-TS-018_2011.pdf (дата обращения 05.04.2024).
5. Юницкий А.Э. Струнные транспортные системы: на Земле и в Космосе. Силакрогс: ПНБпринт, 2019. 576 с.
6. Новый уровень. Как эстакадный транспорт может решить проблему пробок // Фонтанка.ру. Санкт-петербург онлайн: сайт. URL: <https://www.fontanka.ru/longreads/72841475/?erid=Kra246Hbk> (дата обращения 25.11.2023).
7. Красковский А.Е. Что понимать под термином безопасность движения? // Железнодорожный транспорт. 1996. № 9. С. 39–41.
8. Пищик Ф.П. Безопасность движения на железнодорожном транспорте: учеб. пособие. Гомель: БелГУТ, 2009. 267 с.
9. Прогрессивные технологии обеспечения безопасности движения поездов и сохранности грузов: монография / В.А. Гапанович, И.И. Галиев, Ю.И. Матяш, В.П. Клюка. М.: ГОУ «Учебно-методический центр по образованию на ж.-д. транспорте», 2008. 220 с.
10. Замышляев А.М. Прикладные информационные системы управления надежностью, безопасностью, рисками и ресурсами на железнодорожном транспорте / А.М.Замышляев. Ульяновск: Областная типография «Печатный двор», 2013. 143 с.

11. ГОСТ Р 55056-2012 Транспорт железнодорожный. Основные понятия. Термины и определения (стандарт отменен). М.: Стандартиформ, 2013. IV, 49 с.

12. ГОСТ 34530-2019 Транспорт железнодорожный. Основные понятия. Термины и определения. М.: Стандартиформ, 2019. IV, 49 с.

13. ГОСТ 33894-2016 Системы железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля. М.: Стандартиформ, 2019. IV, 26 с.

14. ГОСТ 33895-2016 Системы железнодорожной автоматики и телемеханики на перегонах железнодорожных линий. Требования безопасности и методы контроля. М.: Стандартиформ, 2019. IV, 10 с.

15. IEEE 1474.1-2004 Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements. Управление поездами на основе связи. Требования к реализации и функциям.

16. IEC 62290-1:2014, Railway applications – Urban guided transport management and command/control systems – Part 1: System principles and fundamental concepts. Системы управления и контроля для ж.-д. пассажирских перевозок в городском и пригородном сообщении. Часть 1. Принципы и фундаментальные концепции построения.

17. ANSI / ASCE / T & DI 21 – 2021 Automated People Mover Standards.

18. ГОСТ Р 70059-2022 Системы управления и контроля ж.-д. транспорта для перевозок пассажиров в пригородном сообщении. Принципы построения и основные функциональные требования. М.: Российский институт стандартизации, 2022. IV, 11 с.

19. Performance Specification for a Turnkey Mass Transit Monorail System / IMA – 2022.

20. Шебе Х. Автономное вождение. О способах применения принципов безопасности // Надежность. 2019. № 3. С. 21-33.

21. Памятка Р817. Эксплуатационно-технические требования к системам интервального регулирования движения поездов на перегонах. Комитет ОСЖД. Варшава. Дата вступления в силу: 21 октября 2016 г.

22. IEEE 1474.3-2008 Recommended Practice for Communications-Based Train Control (CBTC). System Design and Functional Allocations.

23. EN 13452-1:2003 Railway applications. Braking. Mass transit brake systems – Part 1: Performance requirements.

24. Федеральный закон РФ «О транспортной безопасности» от 09.02.2007 № 16-ФЗ // Собрание законодательства Российской Федерации. 2007. № 7. Ст. 837.

25. ГОСТ 33432-2015 Безопасность функциональная. Политика, программа обеспечения безопасности. Демонстрация безопасности объектов железнодорожного транспорта. М.: Стандартиформ, 2019. IV, 23 с.

26. EN 50126-1:2017 Железные дороги. Требования и подтверждение надежности, готовности к эксплуатации, ремонтпригодности и безопасности (RAMS) – Часть 1: Общий процесс обеспечения RAMS.

27. Шубинский И.Б. Функциональная безопасность систем управления на железнодорожном транспорте: монография / И.Б. Шубинский, Е.Н. Розенберг. Москва; Вологда: Инфра-Инженерия, 2023. 360 с.

References

1. IEC 61508-2010 Functional safety of electrical/electronic/programmable electronic safety-related systems.

2. TR CU 001/2011. On the safety of railway rolling stock: Technical Regulations of the Customs Union / Eurasian Economic Union. Effective since 2014-08-02. Minsk: Gosstandart: BelGISS; 2012. (in Russ.).

3. TR CU 003/2011. On the safety of railway infrastructure: Technical Regulations of the Customs Union / Eurasian Economic Union. Effective since 2014-08-02. Minsk: Gosstandart: BelGISS; 2012. (in Russ.).

4. TR CU 018/2011. On the safety of wheeled vehicles: Technical Regulations of the Customs Union / Eurasian Economic Union. Effective since 2015-01-01. (accessed 05.04.2024). Available at: https://eec.eaeunion.org/upload/medialibrary/2a3/TR-TS-018_2011.pdf. (in Russ.).

5. Unitsky A.E. [String transportation systems: on Earth and in Space]. Silakrogs: PNBprint; 2019. (in Russ.).

6. [A new level. How overhead railways can solve the problem of traffic jams]. (accessed 25.11.2023). Available at: <https://www.fontanka.ru/longreads/72841475/?erid=Kr a246Hbk>. (in Russ.).

7. Kraskovsky A.E. [What is meant by the term traffic safety?]. *Zheleznodorozhny transport* 1996;9:39-41. (in Russ.).

8. Pishchik F.P. [Railway traffic safety: a textbook]. Gomel: BelGUT; 2009. (in Russ.).

9. Gapanovich V.A., Galiev I.I., Matyash Yu.I., Klyuka V.P. [Advanced technologies for train protection and cargo safety: a monograph]. Moscow: [State Educational Institution Railway Transportation Training Centre]; 2008. (in Russ.).

10. Zamyshliaev A.M. [Applied information systems for managing dependability, safety, risks, and resources in railway transportation]. Ulianovsk: Oblastnaya tipografia Pechatny dvor; 2013. (in Russ.)

11. GOST R 55056-2012 Railway transport. General. Terms and definitions (standard abolished). Moscow: Standartinform; 2013. (in Russ.).

12. GOST R 34530-2019 Railway transport. General. Terms and definitions. Moscow: Standartinform; 2019. (in Russ.).

13. GOST 33894-2016 Railway automatics and telemechanics systems on railway stations. Safety requirements and methods of checking. Moscow: Standartinform; 2019. (in Russ.).

14. GOST 33895-2016 Railway automatics and telemechanics systems on stages of railroad lines. Safety requirements and methods of checking. Moscow: Standartinform; 2019. (in Russ.).

15. IEEE 1474.1-2004 Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements.

16. IEC 62290-1:2014, Railway applications – Urban guided transport management and command/control systems – Part 1: System principles and fundamental concepts.

17. ANSI / ASCE / T & DI 21 – 2021 Automated People Mover Standards.

18. GOST R 70059-2022 Management and command/control systems for suburban railway passenger transport. Construction principles and general functional requirements. Moscow: Russian Standardization Institute; 2022. (in Russ.).

19. Performance Specification for a Turnkey Mass Transit Monorail System. IMA; 2022.

20. Schäbe H. Autonomous Driving – How to Apply Safety Principles. *Dependability* 3;3:21-33.

21. Leaflet R817. [Operational and technical requirements for open line train separation systems. The OSJD Committee. Warsaw. Effective date: October 21, 2016]. (in Russ.).

22. IEEE 1474.3-2008 Recommended Practice for Communications-Based Train Control (CBTC). System Design and Functional Allocations.

23. EN 13452-1:2003 Railway applications. Braking. Mass transit brake systems – Part 1: Performance requirements.

24. [Federal Law of the Russian Federation On Transportation Security dated 09.02.2007 no. 16-FZ]. *Collection of Legislation of the Russian Federation* 2007;7;837. (in Russ.).

25. GOST 33432-2015. Functional safety. Policy and program of safety provision. Safety proof of the railway objects. Moscow: Standartinform; 2019. (in Russ.).

26. EN 50126-1:2017 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS Process.

27. Shubinsky I.B., Rozenberg E.N. [Functional safety of control systems in railway transportation]. Moscow, Vologda: Infra-Inzheneria; 2023. (in Russ.).

Сведения об авторах

Юницкий Анатолий Эдуардович – генеральный конструктор ЗАО «Струнные технологии», ул. Железнодорожная, д. 33, г. Минск, Республика Беларусь, 220089.

Гарах Виктор Александрович – заместитель генерального конструктора по транспортным комплексам

ЗАО «Струнные технологии», ул. Железнодорожная, д. 33, г. Минск, Республика Беларусь, 220089.

Литвинович Тимофей Святославович – руководитель группы АСУ перевозочным процессом ЗАО «Струнные технологии», ул. Железнодорожная, д. 33, г. Минск, Республика Беларусь, 220089.

Шевченко Дмитрий Николаевич – кандидат технических наук, доцент, главный специалист ЗАО «Струнные технологии», Железнодорожная, д. 33, г. Минск, Республика Беларусь, 220089, e-mail: shevchenkodn@yandex.ru; d.shevchenko@unitsky.com

About the authors

Anatoli E. Unitsky, General Designer, Unitsky String Technologies Inc., 33 Zheleznodorozhnaya St., Minsk, 220089, Republic of Belarus.

Viktar A. Harakh, Deputy General Designer for Transport Complexes, Unitsky String Technologies Inc., 33 Zheleznodorozhnaya St., Minsk, 220089, Republic of Belarus.

Timofey S. Litvinovich, Team Leader Automated Traffic Management Systems, Unitsky String Technologies Inc., 33 Zheleznodorozhnaya St., Minsk, 220089, Republic of Belarus.

Dmitriy N. Shevchenko, Candidate of Engineering, Associate Professor, Chief Specialist, Unitsky String Technologies Inc., 33 Zheleznodorozhnaya St., Minsk, 220089, Republic of Belarus, e-mail: d.shevchenko@unitsky.com.

Вклад авторов в статью

Юницкий А.Э. – постановка задач и целей исследования, контроль результатов.

Гарах В.А. – подбор источников информации, обсуждение промежуточных результатов.

Литвинович Т.С. – анализ источников информации, обсуждение перечня функций, особенностей их реализации.

Шевченко Д.Н. – анализ источников информации, предложения по перечню функций безопасности движения, терминологии.

Конфликт интересов

Авторы заявляют об отсутствии конфликтов интересов.

Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем

Conceptual problems of transportation security of intelligent water transportation systems

Михалевич И.Ф.
Mikhalevich I.F.

Российский университет транспорта (МИИТ), Москва, Российская Федерация
Russian University of Transport (MIIT), Moscow, Russian Federation

mif-orel@mail.ru



Михалевич И.Ф.

Резюме. Цель. На водные пути выходят морские автономные и дистанционно-управляемые надводные суда (МАНС), безэкипажные суда внутреннего плавания (БЭС). Интеллектуальной становится инфраструктура водных путей. Повышается интеллектуальный уровень морских и речных портов, портовых терминалов и пристаней. Масштабное внедрение информационных технологий, технологий автоматизированного управления, автоматического управления и искусственного интеллекта существенно расширило ландшафт угроз транспортной безопасности водных интеллектуальных транспортных систем (ИТС) угрозами не физического происхождения. На изменение ландшафта угроз необходимо своевременно реагировать, чтобы не возникало разрыва между реально достигнутым уровнем интеллектуализации и совокупностью мер по обеспечению транспортной безопасности водных ИТС. **Проблемы.** Подмена или изменение показаний датчиков МАНС (БЭС) или сигналов, получаемых их исполнительными устройствами, может привести к изменению направления движения судов и вызвать их столкновения между собой или с объектами инфраструктуры, посадку на мель, а то и вовсе захват МАНС (БЭС) и находящихся на них пассажиров, грузов и сопровождающих их лиц. Несанкционированный доступ к информации в автоматизированных системах управления портовых терминалов может быть использован для злонамеренного шифрования информации. Это может вызвать блокировку погрузочно-разгрузочных работ в порту, срыв расписания движения судов, нарушение логистических операций в масштабах до национального уровня. Последствия национального уровня могут классифицироваться как нарушение безопасности критической информационной инфраструктуры страны, связанное с транспортной небезопасностью водной ИТС. Общей для различных ИТС является проблема цифрового неравенства автоматизированных систем технологического и корпоративного управления в сфере безопасности вышеуказанных технологий. **Методы.** Обеспечение транспортной безопасности водных ИТС требует применения всего доступного комплекса методов, средств и мер защиты. Правовая база обеспечения транспортной безопасности должна учитывать весь спектр актуальных видов незаконного вмешательства в функционирование водных ИТС и обязывать к планированию и выполнению соответствующего ему комплекса защитных мероприятий. В статье применены методы системного анализа и обеспечения комплексной безопасности сложных систем. **Результаты.** Проведен анализ новых видов угроз транспортной безопасности водных транспортных систем и нормативной правовой базы обеспечения их транспортной безопасности. Выявлено, что новые виды угроз транспортной безопасности водных транспортных систем в них не учтены и, как следствие, в планах обеспечения транспортной безопасности отражения не находят. Рассмотрена архитектура водных ИТС в виде интегрированной автоматизированной системы корпоративного и технологического управления, применение которой направлено на динамичное согласование моделей водных ИТС с моделями актуальных угроз транспортной безопасности в информационной сфере. **Заключение.** Для обеспечения транспортной безопасности водных ИТС необходимо учитывать новые виды угроз, которые связаны с недеklarированными возможностями и уязвимостями информационных технологий, технологий автоматизированного управления, автоматического управления и искусственного интеллекта. Рассмотренные проблемы носят системный характер, так как незаконное вмешательство в функционирование водных ИТС может негативно влиять на другие системы критической информационной инфраструктуры. Это следует учитывать при разработке нормативных правовых актов по обеспечению транспортной безопасности на водном и других видах транспорта.

Abstract. Aim. Autonomous and remote-controlled surface sea vessel (ASSV) and unmanned inland water vessels (UIWV) are entering the waterways. The infrastructure of waterways is becoming intelligent. The intellectual level of sea and river ports, port terminals, and harbours is improving. Large-scale deployment of information technologies, automated control, automatic control, and artificial intelligence has significantly expanded the landscape of transportation security threats to water intelligent transportation systems (ITS) and now includes non-physical threats. The evolving threat landscape requires timely response in order to avoid gaps between the current state of intellectual technology application and the set of measures to ensure the transportation security of water ITS. **Problems.** Spoofing or modifying sensors readings in ASSV (UIWV) or signals received by their executive units can cause vessels to lose direction and collide with each other or with infrastructure facilities, run aground, or even being hijacked along with the passengers, cargo, and attendants. Unauthorized access to information in automated control systems of port terminals can be used to maliciously encrypt information. That may block cargo handling operations in a port, disrupt ship traffic schedules and logistics operations up to the national level. National-level consequences can be classified as a disruption of the national information infrastructure security associated with the transportation insecurity in ITS. The various existing ITS have the common problem associated with the digital inequality of the automated systems employed by industrial enterprises and corporate governance in terms of the security of the above technologies. **Methods.** Ensuring the transportation security of water ITS requires the application of all available methods, means, and measures of protection. The legal framework of transportation security is to take into account the full range of relevant methods of illegal interference into the operation of water ITS and require planning and implementing a corresponding set of protective measures. The article uses methods of systems analysis and comprehensive security of complex systems. **Results.** The author analysed the new types of threats to the transportation security of water transportation systems and the corresponding regulatory framework. It was identified that the latter do not take into account the new types of threats to the transportation security of water transportation systems. Consequently, those are not covered by the transportation security planning. The paper examines the architecture of water ITS in the form of an integrated automated system of corporate and process management, whose application aims to dynamically coordinate water ITS models with those of current information-related threats to the transportation security. **Conclusion.** Ensuring the transportation security of water ITS requires taking into account the new types of threats associated with undocumented capabilities and vulnerabilities of information technologies, automated control, automatic control, and artificial intelligence technologies. The examined problems are of a systemic nature, since illegal interference in the operation of water ITS can negatively affect other systems of critical information infrastructure. That should be taken into account when developing regulations related to ensuring the transportation security of water and other modes of transportation.

Ключевые слова: Автоматизированная система корпоративного управления, автоматизированная система технологического управления, водный транспорт, интегрированная автоматизированная система корпоративного и технологического управления, интеллектуальная транспортная система, информационная безопасность, искусственный интеллект, недеklarированные возможности, уязвимость, цифровая трансформация.

Keywords: automated corporate management system, automated process management system, water transportation, integrated automated corporate and process management system, intelligent transportation system, information security, artificial intelligence, undocumented capabilities, vulnerability, digital transformation.

Для цитирования: Михалевич И.Ф. Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем // Надежность. 2024. №2. С. 72-87. <https://doi.org/10.21683/1729-2646-2024-24-2-72-87>

For citation: Mikhalevich I.F. Conceptual problems of transportation security of intelligent water transportation systems. Dependability 2024;2:72-87. <https://doi.org/10.21683/1729-2646-2024-24-2-72-87>

Поступила: 16.09.2023 / **После доработки:** 12.04.2024 / **К печати:** 10.06.2024

Received on: 16.09.2023 / **Revised on:** 12.04.2024 / **For printing:** 10.06.2024

Введение

Транспортная отрасль Российской Федерации находится в состоянии цифровой трансформации, в рамках которой осуществляется масштабное внедрение информационных технологий, технологий автоматизированного управления, автоматического управления и искусственного интеллекта. На основе этих технологий создаются и развиваются интеллектуальные транспортные системы (ИТС) всех видов транспорта, в том числе водного¹.

На водные просторы выходят морские автономные и дистанционно-управляемые надводные суда (МАНС) и безэкипажные суда внутреннего плавания (БЭС). Их поведение зависит от автоматически получаемой информации об окружающей навигационной обстановке и автоматически вырабатываемых решений о направлении, скорости и других параметрах движения судов, которая может быть злонамеренно подменена или изменена. Также возможна подмена или изменение показаний датчиков МАНС (БЭС), или сигналов, получаемых их исполнительными устройствами, что может привести к изменению направления движения и вызвать столкновения судов между собой или с объектами инфраструктуры, посадку на мель, а то и вовсе захват МАНС (БЭС) и находящихся на них пассажиров, грузов и сопровождающих их лиц.

Интеллектуальной становится инфраструктура водных путей. В 2021 году на подходном канале в Обской губе Карского моря для обеспечения безопасности судоходства были установлены 22 буя, оснащенные средствами автоматической идентификационной системы² (АИС). Такого рода интеллектуализированные знаки навигационного оборудования водных путей по радиосвязи передают информацию о типе знака и его координатах, состоянии навигационных огней, которая может быть злонамеренно подменена или изменена и негативно повлиять на поведение МАНС (БЭС).

Повышается интеллектуальный уровень морских и речных портов и терминалов, пристаней. В их составе функционируют информационные системы и автоматизированные системы управления, поведение которых также может быть изменено путем злонамеренных информационных воздействий. В частности, несанкционированный доступ к информации в автоматизированных системах управления портовыми терминалами может сопровождаться злонамеренным шифрованием информации и вызвать блокировку погрузочно-разгрузочных работ в порту, срыв расписания движения судов, нарушение логистических операций в масштабах вплоть

до национального уровня. Последствия национального уровня могут классифицироваться как нарушение безопасности критической информационной инфраструктуры страны, вызванное транспортной небезопасностью водной ИТС.

Такого рода акты незаконного вмешательства в деятельность водных ИТС принято классифицировать по критериям безопасности информации. Она может быть нарушена в части конфиденциальности, доступности, целостности, аутентичности и достоверности, а также в совокупности отмеченных свойств информации.

1. Расширение ландшафта угроз транспортной безопасности водных транспортных систем

Согласно закону³ и ГОСТ Р 56461-2015⁴ транспортная безопасность определяется как состояние защищенности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства, под которыми понимаются любые противоправные действия или бездействие, угрожающие безопасной деятельности транспортного комплекса, влекущие причинение или создающие угрозу причинения вреда жизни и здоровью людей или материальный ущерб. Следовательно, деятельность по обеспечению транспортной безопасности водных ИТС должна учитывать акты незаконного вмешательства как физического, так и не физического характера.

Информационные технологии, технологии автоматизированного управления, автоматического управления и искусственного интеллекта реализуются с использованием программных и аппаратных средств, программно-аппаратных комплексов, компьютеризированных и программируемых электронных систем, которые могут содержать программные закладки и уязвимости, позволяющие, в частности, осуществлять:

- несанкционированный доступ и несанкционированные воздействия на информацию, данные и информационные ресурсы водных ИТС;

- несанкционированный доступ и несанкционированные воздействия на объекты управления водных ИТС и их компоненты: датчики, исполнительные устройства, компьютеризированные и программируемые электронные системы управления судами, объектами инфраструктуры водных путей, портов и портовых терминалов, причалов, береговых центров управления безэкипажными судами и т.п., которые также должны быть защищены по требованиям безопасности информации⁵.

¹ Транспортная стратегия Российской Федерации до 2030 года с прогнозом на период до 2035 года (утверждена распоряжением Правительства Российской Федерации от 27.11.2021 №3363-р).

² На Севморпути впервые установлены буи со станциями автоматической идентификационной системы // Российское судоходство, 21.10.2021. Отраслевой портал Российской палаты судоходства <https://www.rus-shipping.ru/ru/service/news/?id=45658>

³ Федеральный закон от 09.02.2007 года № 16-ФЗ «О транспортной безопасности»

⁴ ГОСТ Р 56461-2015 «Безопасность транспортная. Общие требования».

⁵ Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах,

Программными закладками являются внесенные в программное обеспечение водных ИТС вредоносные программы и/или программный код, которые инициируют выполнение не описанных в документации функций программного обеспечения¹, реализацию его недекларированных возможностей². Это, например, вирусы, черви, трояны, программы-шифровальщики и др.

Уязвимость водных ИТС в общем случае можно определить как наличие слабых мест в их активах или элементах управления, которые могут быть использованы одной или несколькими угрозами³. Программной уязвимостью является недостаток (слабость) программного обеспечения, программно-технического средства или системы и сети в целом, который может быть использован для реализации угроз безопасности информации⁴. В водных ИТС они могут быть связаны, в частности, с уязвимостями программного кода, конфигурации, архитектуры или организации водной ИТС. Уязвимости могут быть также многофакторными.

Сложившийся исторически перечень видов актов незаконного вмешательства в функционирование объектов водных транспортных систем отражает действия, совершаемые исключительно путем физического доступа к объектам воздействия (транспортным средствам, инфраструктуре водных путей, портам, причалам, зданиям и т.п.) и с использованием исключительно физических средств воздействия (взрывчатки, газов, средств поджога и т.п.).

Для водных ИТС физический доступ к объектам воздействия не является обязательным и может осуществляться путем ближнего беспроводного доступа и удаленного доступа через сеть Интернет, что отражено на рис. 1.

Физический доступ предоставляет злоумышленнику полный перечень возможностей для незаконного вмешательства в функционирование МАНС (БЭС), интеллектуальных объектов инфраструктуры водных путей, причалов, информационных и автоматизированных систем управления портов и портовых терминалов. Но использоваться он может не только для совершения террористических, хулиганских и аналогичных актов, природа которых выявляется тут же по видимым следам и последствиям. Не менее опасными являются акты не-

законного вмешательства, связанные с программными закладками и программными уязвимостями, приводящие к нарушению или прекращению функционирования объектов водных ИТС. При этом природа совершения таких актов не столь очевидна, а следы их подготовки и совершения могут быть надежно скрыты и даже удалены.

При нахождении вблизи вышеуказанных объектов водных ИТС злоумышленник может осуществить беспроводной доступ и вмешаться в функционирование встроенного в них интеллектуального оборудования (компьютеризированных и/или программируемых электронных систем) и вызвать нарушение (прекращение) функционирования объекта. Такое же вмешательство доступно злоумышленнику в отношении интеллектуального оборудования водных ИТС, подключенного к Интернету.



Рис. 1. Возможные пути доступа для совершения актов незаконного вмешательства в функционирование объектов водных ИТС

Для преднамеренного незаконного вмешательства могут быть задействованы все пути. Например, несанкционированный физический или беспроводной доступ может быть использован для подготовки канала для последующего удаленного вмешательства через Интернет с использованием средств искусственного интеллекта и иных вычислительно затратных средств.

На рис. 2 приведены результаты исследования рейтинга новых видов актов незаконного вмешательства в функционирование объектов авиационного, морского, железнодорожного и автомобильного транспорта ЕС в 2021-2022 годах [1]. Некоторые виды актов незаконного вмешательства вызвали комплексные последствия и были учтены в нескольких видах, вследствие чего общий процент учтенных актов превышает 100%.

Аналогичные результаты представлены Лабораторией Касперского в исследовательском отчете за первое полугодие 2023 года в отношении систем промышленной автоматизации [2].

представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК от 14 марта 2014 г. № 31).

¹ Согласно ГОСТ Р 51624-2000. Автоматизированные информационные системы в защищенном исполнении. Общие положения.

² Согласно ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

³ Согласно ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary.

⁴ Согласно ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

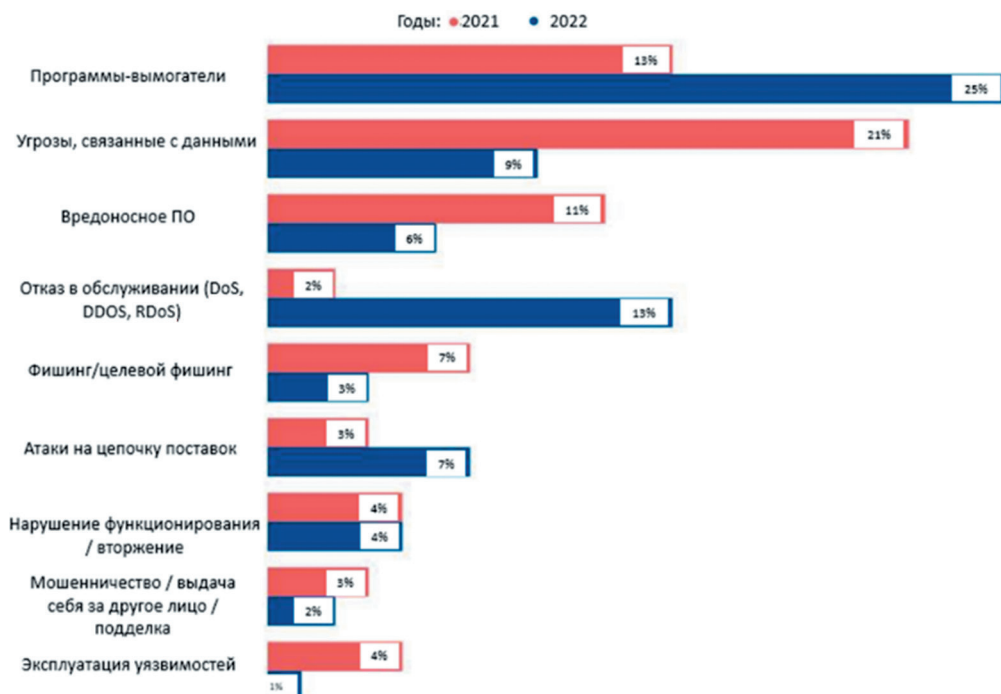


Рис. 2. Основные виды актов незаконного вмешательства в функционирование транспортного сектора ЕС в 2021-2022 годах (источник рисунка: [1])

В названных и других источниках обращено внимание на проблему неполноты отчетности о событиях нарушения информационной безопасности и на тот факт, что публично раскрытые сведения, использованные при подготовке исследовательских отчетов, являются лишь верхушкой айсберга. Это обстоятельство можно отнести к причинам, по которым опасность отраженных на рис. 2 видов воздействий на водные ИТС недооценивается, а проблематика информационной безопасности не находит должного отражения в действующей нормативной правовой базе обеспечения транспортной безопасности водных ИТС, что подтверждают приведенные далее результаты ее анализа.

Комментируя рис. 2 и упреждая приведенные далее примеры, отметим следующее.

Водная отрасль все чаще сталкивается с угрозами транспортной безопасности типа «отказ в обслуживании»: DoS – отказ в обслуживании; RDoS – отказ в обслуживании с требованием выкупа; DDoS – распределенный отказ в обслуживании. В 2022 году реализация таких угроз в транспортном секторе ЕС выросла в шесть с половиной раз по сравнению с 2021 годом. В 2023 году тенденция роста сохранилась.

Эта угроза достаточно проста в реализации и осуществляется путем направления многочисленных запросов на сайты (или другие публичные информационные ресурсы) объектов водного транспортного комплекса. Это вызывает недоступность информационных ресурсов, влечет для их владельцев (операторов) материальный вред и потерю репутации. Для проведения атаки могут задействоваться десятки и сотни тысяч устройств (компьютеры, устройства интернета-вещей и т.п.), о чем

их владельцы не подозревают, но непроизвольно этому способствуют.

Атакам типа «отказ в обслуживании» предшествует массированное сканирование Интернета и составление баз данных об устройствах, готовых к несанкционированному использованию («порабощению»). Эти базы могут использоваться самими составителями или продаваться другим злоумышленникам. В теневом Интернете существует услуга предоставления в аренду определенного количества «порабощенных» устройств. Возможности для пополнения «армии» «порабощенных» устройств обусловлены, в первую очередь, беспечностью легитимных владельцев (пользователей, администраторов) «порабощаемого» оборудования, которые игнорируют правила цифровой гигиены [3, 4]. Недопустимая беспечность заключается, например, в использовании устройств с предустановленными (заводскими) параметрами доступа: логином и паролем (admin/admin, root/root и т.п.). Эти параметры публично известны для каждой модели и модификации устройств, что открывает возможность для несанкционированного доступа к ним и несанкционированного использования.

Традиционно транспортной безопасности угрожают программы шифровальщики и похитители данных.

Использованию таких программ неизменно предшествует этап сбора информации об объекте будущего незаконного вмешательства. Делается это в крайне «деликатной» форме: путем посещения офиса, подслушивания или прослушки разговоров сотрудников с использованием технических средств, а также удаленно путем «невинных» электронных или голосовых запросов, направленных по адресам электронной почты или

высказанных голосом по публично известным адресам электронной почты и номерам телефонов планируемого объекта незаконного вмешательства. Однако за «деликатностью» кроется сбор (выманивание, выуживание) персонифицированной информации о легитимных пользователях (руководителях, администраторах, и т.п., адресах их электронной почты, номерах телефонов), назначении и архитектуре объекта, используемом в нем оборудовании и средствах защиты.

Наличие такой информации позволяет перейти к более сложным воздействиям, основанным на несанкционированном доступе к разведанному объекту, закреплению в нем и последующему перемещению по его архитектуре, пример которой будет рассмотрен далее (рис. 4). В зависимости от целей вмешательства (кража информации, получение выкупа, нарушение функционирования автоматизированной системы технологического управления и другие) злоумышленник может осуществлять горизонтальное перемещение по архитектуре водной ИТС, оставаясь на одном уровне, или углубляться внутрь архитектуры (вертикально), закрепляясь на достигнутом уровне и далее осуществлять в нем горизонтальное перемещение.

Зная адреса электронной почты, не выходя за пределы уровня архитектуры, реализующего функции системы корпоративного (административного) управления, злоумышленники могут массово отправлять письма, содержащие «невинные» ссылки и предложения перейти по ним. После перехода по ссылке на компьютер сотрудника может быть удаленно загружена и инсталлирована программная закладка, открывающая каналы для вертикального перемещения по архитектуре вплоть до самого нижнего уровня, на котором находятся датчики и исполнительные устройства систем автоматического управления движением судна, например.

Также незаметно может быть установлена программа-шифровальщик. Ее активация приведет к шифрованию информации. Недоступность несанкционированно зашифрованной информации SCADA портового терминала приведет к невозможности выполнения погрузочно-разгрузочных работ. За расшифровку информации или передачу ключей шифрования злоумышленники, как правило, требуют крупный выкуп.

С применением программной закладки может быть получен несанкционированный доступ к персональным данным и иной конфиденциальной информации (служебной, коммерческой тайне и т.п.), обрабатываемой на объектах водного транспортного комплекса и ее раскрытие в публичных источниках или требование выкупа за нераскрытие информации.

И это только вершина айсберга новых видов актов незаконного вмешательства, расширяющих ландшафт угроз транспортной безопасности водных ИТС. Более того, ландшафт угроз водных ИТС расширяют также акты незаконного вмешательства непреднамеренного характера. Непреднамеренные акты незаконного вмешательства могут быть связаны с аппаратными сбоями и

неисправностями средств вычислительной техники, не устраненными ошибками программного обеспечения, ошибочными действиями пользователей (операторов, администраторов) и т.п. событиями.

Некоторые из возможностей новых видов актов незаконного вмешательства в функционирование водных ИТС отражены в следующих примерах.

Без применения огнестрельного оружия или иных средств физического воздействия был изменен курс мегаяхты длиной 65 метров и стоимостью 80 миллионов долларов США (рис. 3) путем нефизического воздействия с использованием специализированного программно-аппаратного комплекса стоимостью 2 тысячи долларов США [5, 6].

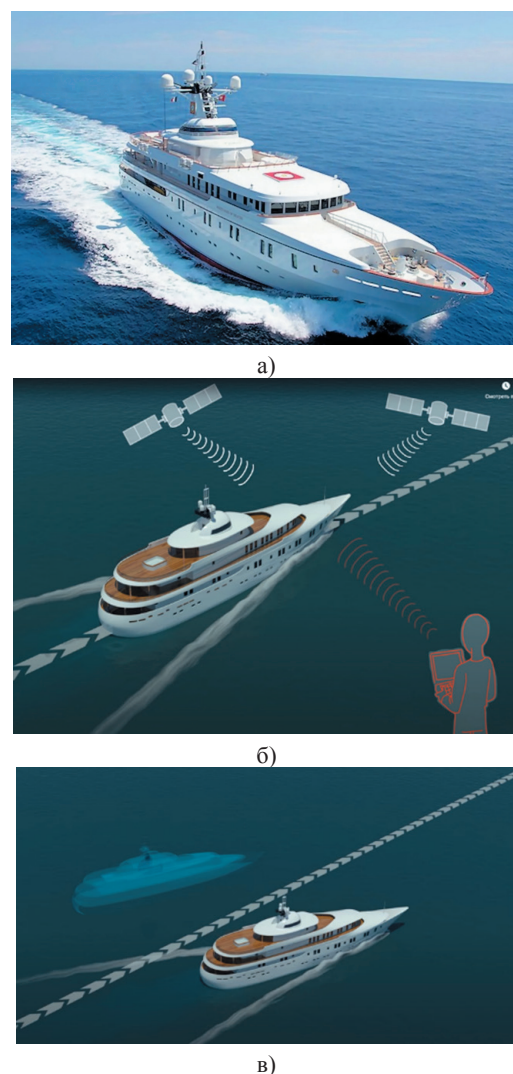


Рис. 3. Изменение курса мегаяхты длиной 65 метров и стоимостью 80 миллионов долларов США путем подмены сигнала GPS (источники рисунков: а) – [5], б), в) – [6])

Вмешательство заключалось в подмене сигнала спутника GPS на сигнал, формируемый комплектом «псевдоспутникового» оборудования злоумышленника. Когда уровень сигнала «псевдоспутника» превысил уровень сигнала реального спутника GPS цифровой

приемник яхты переключился на более сильный сигнал «псевдоспутника», находящегося невдалеке (в сравнении с 10 000–20 000 км расстояния до спутников), судовое оборудование произвело расчет по ложным пространственным координатам спутника и курс яхты был изменен. Таким образом, нарушение достоверности навигационной информации о пространственных координатах, получаемой приемником глобальной навигационной спутниковой системы (ГНСС) яхты, создало для злоумышленника возможность повлиять на ее курс. Природа такого вмешательства обусловлена уязвимостями ГНСС, в которых не применены криптографические средства аутентификации источников сигналов (спутников), что создает условия для реализации описанной угрозы [7, 8]. Если такое воздействие будет произведено против МАНС или БЭС, не исключено, что судно сможет попасть в руки злоумышленников или погибнуть в столкновении с каким-либо препятствием. Проблема с уязвимостями ГНСС является общей для всех видов транспорта, включая авиа, что подтверждают последние (на момент написания статьи) события¹.

Уязвимой является также АИС водных ИТС. В задачи АИС входит обеспечение навигационной информацией других систем МАНС и БЭС, включая ГНСС, систему радиолокационного наблюдения, электронную картографическую навигационно-информационную систему. Как и в случае с ГНСС, навигационная информация АИС может быть подменена или изменена, что обусловлено отсутствием средств, обеспечивающих надежную аутентификацию реальных объектов АИС (судов или оборудованных приборами АИС навигационных знаков инфраструктуры водных путей) и достоверность передаваемой ими навигационной информации. Например, информации о судне, его классе, техническом состоянии, направлении движения, грузе и так далее.

Используя такого рода уязвимости АИС [7, 9], злоумышленники могут посылать ложные сообщения о бедствиях для сближения с МАНС (БЭС) и последующего захвата судна, его пассажиров или груза, подменять идентификаторы судов для совершения любого рода противоправных деяний (контрабанды, перевозки нелегальных мигрантов, торговли людьми).

Как отмечалось ранее, высокой популярностью у злоумышленников пользуются угрозы типа «отказ в обслуживании». Так, в сентябре 2022 года была осуществлена DDoS-атака на сайт порта Нагоя, что привело к его недоступности около 40 минут. Последствия совершенного акта посчитали, по всей видимости, несущественными, что оказалось ошибочным.

В июле 2023 года порт Нагоя подвергся новым воздействиям, совершенным, по предположению автора, после первичного закрепления на уровне автоматизированной системы корпоративного управления порта и дальней-

шего проникновения (вертикального перемещения по архитектуре) на уровне автоматизированной системы технологического управления порта. Злоумышленником был получен несанкционированный доступ в «Единую терминальную систему порта Нагоя», что позволило установить программу-шифровальщик, провести несанкционированное шифрование информации и нарушить работу порта². Порт Нагоя является крупнейшим и самым оживленным морским портом в Японии, обеспечивает около 10% от общего объема торговли страны, имеет 21 причал и 290 стоянок, ежегодно обрабатывает более двух миллионов контейнеров и 165 миллионов тонн груза. В результате совершенного акта операции по погрузке и разгрузке контейнеров на терминалах порта с использованием прицепов были отменены. Это вызвало серьезные простои в процессе транспортировке товаров в национальном масштабе, затронуло многие крупные компании (Тойота и др.) и причинило огромные финансовые и репутационные потери порту.

В июне 2023 года в Нидерландах DDoS-атаке подверглись сайты четырех портов в Роттердаме, Амстердаме, Ден-Хелдере и Гронингене. Сайты трех портов были недоступны несколько часов, а на восстановление сайта порта Гронингена потребовалось около 10 дней³. О других способах воздействия не сообщалось, но дальнейшее проникновение «вглубь» портовых интегрированных автоматизированных систем корпоративного и технологического управления исключать нельзя, особенно после истории с портом Нагоя.

В июле 2023 года мишенью программы-вымогателя стала портовая и железнодорожная компания Transnet SOC Limited в ЮАР⁴. Воздействие привело к тому, что на контейнерных терминалах были вынуждены перейти к ручной обработке грузов, в том числе в порту Дурбане, который обрабатывает более половины грузов страны и является основными воротами для других экспортеров сырьевых товаров, включая Демократическую Республику Конго и Замбию.

В ноябре 2023 года австралийский оператор DP World, отвечающий за 40% морских перевозок Австралии, в результате установки и активации злоумышленником программы-шифровальщика был вынужден закрыть четыре порта в Сиднее, Мельбурне, Брисбене и Фримантле, ввести запрет на разгрузку судов и вывоз контейнеров из портов. За время устранения последствий воздействия

¹ Самолеты «заблудились» из-за хакеров. Frequent Flyers Ru, December 8, 2023. URL: https://www.frequentflyers.ru/2023/12/08/gps_sproof/ (дата обращения 12.12.2023).

² Nagoya Port Resumes Some Operations After Ransomware Attack. Bloomberg Businessweek, July 6, 2023. URL: <https://www.bloomberg.com/news/articles/2023-07-06/nagoya-port-delays-restart-following-alleged-ransomware-attack> (дата обращения 26.10.2023).

³ Dutch ports' websites offline for hours, days due to pro-Russian cyber attacks. NL TIMES, June 14, 2023. URL: <https://nltimes.nl/2023/06/14/dutch-ports-websites-offline-hours-days-due-pro-russian-cyber-attacks> (дата обращения 18.11.2023).

⁴ Cyber Pirates Prowling Ship Controls Threaten Another Big Shock. Bloomberg Businessweek, June 28, 2023. URL: <https://www.bloomberg.com/news/articles/2022-06-28/cyber-pirates-prowling-ship-controls-threaten-another-big-shock> (дата обращения 26.10.2023).

была задержана отправка 30 000 морских контейнеров, скопившихся в портах¹. На правительственном уровне отмечалось, что Австралия столкнулась с инцидентом национального значения, который продолжался в течение нескольких дней и повлиял на движение товаров в страну и из нее.

Приведенные примеры показывают, что с увеличением степени интеллектуализации перечень актов незаконного вмешательства в функционирование объектов водного транспорта будет только расширяться. Это вызывает необходимость обеспечить полноту учета актов незаконного вмешательства и соответствия мероприятий по обеспечению транспортной безопасности реальному ландшафту угроз.

2. Анализ полноты учета видов актов незаконного вмешательства в нормативной правовой базе обеспечения транспортной безопасности водного транспортного комплекса

На обеспечение транспортной безопасности водного комплекса направлены, в частности, следующие нормативные правовые акты:

- Технический регламент о безопасности объектов внутреннего водного транспорта (утвержден постановлением Правительства Российской Федерации от 12.08.2010 № 623);

- Требования по обеспечению транспортной безопасности, учитывающие уровни безопасности для транспортных средств морского и внутреннего водного транспорта (утверждены Постановлением Правительства Российской Федерации от 08.10.2020 № 1637);

- Требования по обеспечению транспортной безопасности, в том числе требования к антитеррористической защищенности объектов (территорий), учитывающие уровни безопасности для различных категорий объектов транспортной инфраструктуры морского и речного транспорта (утверждены Постановлением Правительства Российской Федерации от 08.10.2020 № 1638);

- Требования по обеспечению транспортной безопасности, в том числе требования к антитеррористической защищенности объектов (территорий), учитывающие уровни безопасности для объектов транспортной инфраструктуры морского и речного транспорта, не подлежащих категорированию (утверждены постановлением Правительства Российской Федерации от 10.10.2020 № 1651).

Технический регламент о безопасности объектов внутреннего водного транспорта (далее – технический регламент, регламент) содержит требования по обеспе-

чению транспортной безопасности как транспортных средств внутреннего водного транспорта, так и связанной с ним инфраструктуры. В связи с этим первичный анализ полноты учета актов незаконного вмешательства был проведен по нему.

Из анализа следует, что применение технического регламента направлено на достижение следующих целей:

- защиту жизни и здоровья граждан, имущества физических и юридических лиц, государственного или муниципального имущества от опасности, источником которой может стать деятельность внутреннего водного транспорта и связанная с ним инфраструктура;

- охрану окружающей среды, жизни и здоровья животных и растений;

- предупреждение действий, вводящих в заблуждение приобретателей в отношении объектов внутреннего водного транспорта и процессов, связанных с их проектированием, производством, строительством, монтажом, эксплуатацией и утилизацией (далее – объекты регулирования);

- обеспечение энергетической эффективности.

Учитывая приведенные выше примеры, функционирование водных транспортных средств и объектов инфраструктуры водных путей может быть нарушено актами незаконного вмешательства в информационной сфере. Следовательно, выполнение требований технического регламента должно быть направлено на обеспечение, в том числе, информационной безопасности.

Дальнейший анализ показал, что выполнение требований технического регламента должно обеспечить:

- а) биологическую безопасность объектов регулирования;

- б) взрывобезопасность объектов регулирования;

- в) гидрометеорологическую безопасность объектов регулирования;

- г) единство измерений;

- д) механическую безопасность объектов регулирования;

- е) пожарную безопасность объектов регулирования;

- ж) термическую безопасность объектов регулирования;

- з) химическую безопасность объектов регулирования;

- и) электрическую безопасность объектов регулирования;

- к) электромагнитную совместимость в части обеспечения работы приборов и оборудования, относящихся к объектам регулирования;

- л) экологическую безопасность объектов регулирования;

- м) энергетическую и экологическую эффективность объектов регулирования;

- н) другие виды безопасности объектов регулирования.

Содержание регламента отражает его направленность, указанную в пунктах с а) по м) приведенного выше перечня. Из перечня следует, что выполнение требований технического регламента не направлено на обеспечение информационной безопасности объектов

¹ Australia locks down ports after «nationally significant cyberattack». The Independent, November 11, 2023. URL: <https://www.independent.co.uk/news/world/australasia/australia-ports-cyber-attack-dp-world-b2445634.html> (дата обращения 11.11.2023).

регулирования, в отличие от обеспечения пожарной, экологической, биологической безопасности и безопасности в иных областях угроз физического происхождения. Отметим, что регламент уточняет требования, обязательность выполнения которых установлена федеральным законодательством, например: о пожарной безопасности¹, об охране окружающей среды², о биологической безопасности³. Но такие же обязательные требования для объектов регулирования технического регламента установлены федеральным законодательством в сфере информационных технологий^{4,5}. Таким образом, в техническом регламенте допущен разрыв между физическими и «не физическими» областями транспортной безопасности водных транспортных систем, что создает угрозу их транспортной безопасности при совершении актов незаконного вмешательства информационного характера.

Можно было бы предположить, что вопросы информационной безопасности водных транспортных систем рассматриваются в других нормативных правовых актах в соответствии с вышеуказанным подпунктом н) технического регламента. Но, как следует из [10–12], это не так. В частности, в [12] отмечается: «в области информационной безопасности в сфере водного транспорта отсутствует единый, системный и комплексный подход, унификация требований и правил. ... В России отсутствует транспортный отраслевой центр компетенции по информационной безопасности. Ни в положении о Минтрансе России, ни в положении о Росморречфлоте нет ничего об информационной безопасности. То есть формирование единой отраслевой политики в области информационной безопасности не является задачей или обязанностью федеральных органов власти в сфере транспорта».

Отраженные выше нормативные правовые акты, устанавливающие требования по обеспечению транспортной безопасности транспортных средств морского и внутреннего водного транспорта и объектов транспортной инфраструктуры морского и речного транспорта, требований по обеспечению информационной безопасности также не содержат.

Неполнота учета видов актов незаконного вмешательства в функционирование водного транспорта и объектов инфраструктуры водных путей ИТС приводит к их неучету в планах обеспечения транспортной безопасности и, соответственно, не отражению в них мероприятий по обеспечению информационной безопасности [10–12].

¹ Федеральный закон «О пожарной безопасности» от 21.12.1994 № 69-ФЗ

² Федеральный закон «Об охране окружающей среды» от 10.01.2002 № 7-ФЗ

³ Федеральный закон от 30.12.2020 № 492-ФЗ «О биологической безопасности в Российской Федерации»

⁴ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

⁵ Федеральный закон от 26.07.2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

В целом вышеизложенное можно отнести к проблемам цифровой трансформации, динамика которой в практической области существенно опережает развитие правовой сферы.

3. Проблемы цифровой трансформации водного транспорта

На ход цифровой трансформации водного транспорта значительно повлияла пандемия COVID-19, которая существенно обострила проблемы, характерные именно для ИТС [3, 13–15].

За пандемией COVID-19 последовали санкции, запрещающие экспорт в Российскую Федерацию высокотехнологичного оборудования и комплектующих, материалов и программного обеспечения, необходимых для водных ИТС. Однако это не стало полной неожиданностью, на что указывают предпринятые превентивные меры практического характера [16–20]. Они были направлены на создание отечественных аппаратно-программных платформ для объектов критической информационной инфраструктуры, частью которой, в соответствии с федеральным законодательством⁶, является транспортная отрасль.

Однако проблемные вопросы создания и развития водных ИТС вышеизложенным не ограничиваются. Так, составляющая ИТС, реализующая информационные технологии, технологии автоматизированного управления, автоматического управления и искусственного интеллекта, оказалась недостаточно готовой к защите от актов незаконного вмешательства именно в информационной сфере. Эта сфера имеет важное значение при выполнении высокотехнологичных функций в интегрированных системах, реализующих одновременно функционал информационных систем, автоматизированных систем управления и систем автоматического управления.

Архитектура такого рода интегрированных систем, предложенная автором в [13, 14, 21, 22], представлена на рис. 4. При ее разработке было принято, что полностью развернутая ИТС представляет собой интегрированную систему, реализующую именно одновременно функционал информационных систем, автоматизированных систем управления и систем автоматического управления. В интегрированной автоматизированной системе функционирование любой из ее составных систем зависит от результатов функционирования других. Такой подход позволяет формировать модели водных ИТС, адаптированные к актуальным угрозам транспортной безопасности, не нарушая целостности модели водной ИТС как единой системы. Это согласуется с методологией обеспечения безопасности критической информационной инфраструктуры, объекты которой могут одновременно содержать в себе

⁶ Федеральный закон от 26.07.2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».



Рис. 4. Архитектура интегрированной автоматизированной системы корпоративного и технологического управления водной ИТС (источник рисунка: [13, 21])

информационные системы, автоматизированные системы управления и системы автоматического управления или их фрагменты.

В целях исключения избыточной детализации описания систем при рассмотрении вопросов обеспечения транспортной безопасности все многообразие систем можно разделить на два базовых вида: автоматизированные системы корпоративного управления (АСКУ) и автоматизированные системы технологического управления (АСТУ). Совместно они образуют интегрированные автоматизированные системы корпоративного и технологического управления (ИАСКиТУ) представленной на рис. 4 архитектуры. Это позволяет при рассмотрении отношений между субъектами незаконного вмешательства (нарушителями безопасности) и защищаемыми объектами исключить факторы, в меньшей степени влияющие на транспортную безопасность.

При таком моделировании обеспечивается возможность по-разному формировать состав АСКУ и АСТУ, перераспределяя между ними соседние уровни архитектуры. Такая необходимость обусловлена различиями в основном назначении конкретных объектов водных ИТС, каждый из которых в конкретной ситуации в большей степени выполняет функции той или иной входящей

в его состав системы: информационной, автоматизированного управления или автоматической, для каждой из которых формируется свой перечень актуальных угроз транспортной безопасности. Это позволяет распределить актуальные угрозы между уровнями ИАСКиТУ, обеспечивает детальное рассмотрение каждой угрозы, способов ее реализации и связанных с нею рисков, выработку адресных мер по устранению (нейтрализации) угроз в составе АСКУ и АСТУ, комплексное обеспечение транспортной безопасности водной ИТС как единой системы.

Приведенная на рис. 4 архитектура была апробирована при моделировании угроз безопасности информации системы автономного судовождения на внутренних водных путях, выполненном в рамках стратегического проекта «Электронная навигация и безэкипажное (автономное) судовождение»¹ по Программе стратегического академического лидерства «Приоритет – 2030». Применение интегрированной архитектуры позволило рассмотреть акты незаконного вмешательства в функционирование водной ИТС через призму их влияния на элементы, реализующие функции корпоративного

¹ Стратегический проект № 3. Электронная навигация и беспилотное (автономное) судовождение. <https://www.mii.ru/page/178854>

управления (например, в части взаимодействия с информационными ресурсами Единой государственной информационной системы обеспечения транспортной безопасности) и технологического управления (например, дистанционного управления БЭС) как для каждого элемента в отдельности, так и в их взаимной связи, определить негативные последствия, возможность наступления которых обусловлена, в том числе, наличием межуровневых связей в водной ИТС, имеющей интегрированную архитектуру.

В модели ИАСКиТУ водных ИТС рассматриваются две группы и четыре типа сущностей. В зависимости от решаемых задач транспортной безопасности сущность каждого типа может выполнять роль субъекта или объекта незаконного вмешательства.

Первую группу образуют такие сущности как информация (сущность 1) и данные (сущность 2). Под информацией понимаются все виды сообщений, сведений, команд и сигналов в их естественной физической форме, то есть в форме, воспринимаемой людьми непосредственно без применения программируемых технических средств. Под данными – все виды сообщений, сведений, команд и сигналов, представленных в цифровой форме. То есть подразумевается, что данные, как таковые, не существуют в физическом мире, а являются результатом преобразования информации в форму, пригодную для автоматической обработки, в том числе при возможном участии человека^{1,2}. Таким образом учитывается, что информация и данные могут являться как объектом, на который направлено незаконное вмешательство, так и субъектом, которым незаконное вмешательство осуществляется. Например, подмена информации источника приведет к недостоверности данных, передаваемых от имени источника. Пусть их передача в сети осуществляется с соблюдением всех требований безопасности данных и при передаче данные не будут искажены. Пусть также они не будут искажены при преобразовании на стороне получателя в форму, воспринимаемую человеком. В этом случае измененная информация источника будет восприниматься ее получателем-человеком как истинная (достоверная), со всеми вытекающими для обеих сторон последствиями. В роли получателя может быть не только человек, но и техническое средство. В этом случае искаженная информация источника, которым может быть, например, физический (аналоговый) датчик, поступит в искаженном виде к физическому (аналоговому) исполнительному устройству, что вызовет реакцию, не соответствующую фактическому состоянию датчика.

Исходя из изложенного, вторую группу образуют такие сущности, как люди (сущность 3) и компьютеризиро-

ванные и программируемые электронные системы и их компоненты (сущность 4). Таким образом учитывается, что человек (группа людей) и программное обеспечение со всеми своими производными (аппаратно-программные средства, сети, системы и т.п.) могут являться как объектом, на который направлено незаконное вмешательство, так и субъектом, которым незаконное вмешательство осуществляется.

Такое разделение на сущности позволяет перераспределять уровни АСКИТУ между АСКУ или АСТУ по признаку, определяющему, кто или что является объектом незаконного вмешательства. Принято, что любое незаконное вмешательство в информационной сфере, независимо от субъектности (человек, бот, устройство интернета вещей и т.п.), может повлечь неблагоприятные последствия для человека (группы людей, бизнеса, государства) непосредственно. Например, побудить человека к совершению действий, приводящих к нарушению безопасности данных. Такими действиями могут быть: ввод в систему недостоверной информации; изменение уставок средств автоматики и т.п. Или, применение легитимным пользователем незарегистрированных флэш-накопителей в контролируемой зоне, защищенной воздушным зазором, межсетевыми экранами, одноподобными шлюзами (цифровыми диодами) и тому подобными средствами. Но указанное поведение человека способно свести на нет все предпринятые меры технической (в том числе криптографической) защиты информационных систем, автоматизированных систем управления и систем автоматического управления водных ИТС.

Также принято, что и любое нарушение безопасности данных способно повлечь неблагоприятные последствия для человека (группы людей, бизнеса, государства) опосредованно, вызвав нарушение или прекращение функционирования управляемого объекта, обеспечивающего информационные потребности людей, поддержку технологических и иных критически важных для них, бизнеса и государства процессов. В части водных ИТС нарушение безопасности данных, формируемых в ГНСС, АИС, системах управления движением МАНС и БЭС влекут крайне опасные последствия, описанные ранее.

Таким образом, АСКУ будут образовывать уровни ИАСКиТУ, которые содержат все виды систем (ERP, CRM, сайты, электронная почта и т.п.), выполняющих информационные и административные функции. В таких системах информация может контролироваться самими людьми непосредственно. Исходя из этого, в состав АСКУ будут включаться уровни ИАСКиТУ, в которых объектом незаконного воздействия, направленным на нарушение безопасности информации и/или данных, является человек.

Соответственно АСТУ будут образовывать уровни, содержащие все виды систем (ГНСС, АИС, автоматического сбора информации, управления движением и курсом судна, технологическими процессами производ-

¹ ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

² ГОСТ Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации.

ства продукции и оказания услуг, проведения денежных операций, технического обслуживания, экспериментов, функционирования IoT, ПоТ и т.п.), предназначенные для управления объектами, функционирование которых осуществляется без прямого (непосредственного) контроля со стороны человека, которому для контроля необходимы специализированные средства работы с данными. Соответственно АСТУ являются системы, в которых объектом незаконного воздействия, направленным на нарушение безопасности данных и/или информации, являются датчики, исполнительные устройства, программируемые логические контроллеры и иные технические средства, способные изменять свое состояние без обязательного участия человека (без обращения к человеку за получением или подтверждением команды и т.п.).

Общей проблемой, характерной для различных ИТС, является цифровое неравенство в защищенности их АСТУ и АСКУ (ОТ- и IT-систем в зарубежной терминологии [23–26]) от актов незаконного вмешательства в сфере вышеуказанных технологий, что рассмотрено в [3, 14, 22]. Свидетельством такого неравенства является наличие в Государственном реестре сертифицированных средств защиты информации ФСТЭК России¹ и Перечне средств защиты информации, сертифицированных ФСБ России², сотен наименований средств защиты информации, разработанных для АСКУ, и только десятков наименований средств, разработанных для защиты информации и данных в АСТУ.

Такая ситуация сложилась исторически, так как внимание к информационной безопасности раньше было акцентировано в основном в отношении АСКУ, которые в большинстве своем имели распределенный характер, могли использовать открытое информационное пространство и их масштабная цифровизация началась задолго до цифровой трансформации АСТУ.

Прежние АСТУ функционировали, как правило, в своих замкнутых информационных пространствах, которые ограничивались производственными сетями передачи данных, соединяющими объекты на нулевом и первом уровнях архитектуры, представленной на рис. 4. С интеллектуализацией водного транспорта ситуация существенно меняется, затрагивая все вышеуказанные уровни управления и оказывая непосредственное влияние на транспортную безопасность.

Традиционный и, фактически, неизменный характер АСКУ позволил разработать для них нормативную правовую и методическую базу обеспечения безопасности, в том числе транспортной. Интеграция в составе водных ИТС АСКУ и АСТУ требует реагирования в правовой области обеспечения транспортной безопасности, нарушение которой может быть вызвано нарушением безопасности информации и данных, обрабатываемых в водных ИТС. Учитывается ли это

обстоятельство, можно проверить на следующем примере.

4. Анализ проекта технического регламента обеспечения транспортной безопасности объектов внутреннего водного транспорта

В табл. представлены сведения о направленности требований действующего и проекта нового технического регламента обеспечения транспортной безопасности объектов внутреннего водного транспорта³.

Табл. Направленность требований действующего и проекта нового технического регламента обеспечения транспортной безопасности объектов внутреннего водного транспорта

№ п/п	Требования Технического регламента о безопасности объектов внутреннего водного транспорта должны обеспечить:	
	Действующий регламент	Проект нового регламента
1	биологическую безопасность объектов регулирования	
2	взрывобезопасность объектов регулирования	
3	гидрометеорологическую безопасность объектов регулирования	
4	единство измерений	
5	механическую безопасность объектов регулирования	
6	пожарную безопасность объектов регулирования	
7	термическую безопасность объектов регулирования;	
8	химическую безопасность объектов регулирования	
9	электрическую безопасность объектов регулирования	
10	электромагнитную совместимость в части обеспечения работы приборов и оборудования, относящихся к объектам регулирования	
11	экологическую безопасность объектов регулирования	
12	энергетическую и экологическую эффективность объектов регулирования	безопасность судоходства при воздействии на объект регулирования.
13	другие виды безопасности объектов, указанные в целях применения настоящего технического регламента	-

Как видно из табл., проект нового регламента по-прежнему не содержит требований, направленных на обеспечение безопасности информации и данных, нарушение которой в водных ИТС может повлечь гибель людей, привести к материальным и репутационным потерям, экологическим потрясениям.

³ Проект Постановления Правительства Российской Федерации «Об утверждении технического регламента о безопасности объектов внутреннего водного транспорта» (опубликован 30.08.2023 года). <https://www.garant.ru/products/ipo/prime/doc/56867381/?ysclid=lmamav7r6463806883> (доступ 08.10.2023).

¹ <https://reestr.fstec.ru/reg3?ysclid=lppmtjrme24662608>

² <http://clsz.fsb.ru/clsz/certification.htm>

5. Взаимосвязь областей безопасности водных ИТС

В ГОСТ Р 56461-2015 (пункт 3.20) отражено, что обеспечение транспортной безопасности осуществляется путем реализации определяемой государством системы правовых, экономических, организационных и иных мер в сфере транспортного комплекса, соответствующих угрозам совершения актов незаконного вмешательства.

Новые виды актов незаконного вмешательства в деятельность водного транспортного комплекса, связанные с угрозами информационной безопасности, многообразны и, частично, рассмотрены выше. Однако ситуация их неучета относима ко всем видам ИТС и является длящейся, несмотря на предпринимаемые инициативы по ее исправлению [10–12, 17–19, 27]. Применительно к водным ИТС информационная безопасность должна рассматриваться неразрывно с функциональной безопасностью [28], как это предусмотрено, например, ГОСТ Р 70732-2023¹.

В ГОСТ Р 56461-2015 (пункт 3.14) также указано, что транспортная безопасность является составной частью национальной безопасности. Связь составных частей комплексной безопасности водных ИТС, влияния информационной безопасности водных ИТС на иные области безопасности, включая транспортную, отражает рис. 5.

Представленная на рис. 5 система отношений отражает особенности правового регулирования Российской Федерации в областях информационной безопасности и безопасности критической информационной инфра-

структуры, в том числе в виртуальных средах, включая сеть Интернет^{2,3}.

Заключение

Транспортную безопасность водных ИТС следует рассматривать всесторонне, учитывая не только традиционные для водного транспорта акты незаконного вмешательства физического характера, но и специфические для ИТС события, связанные с ненаблюдаемыми физически, но при этом потенциально опасными недеklarированными возможностями и уязвимостями информационных технологий, технологий автоматизированного управления, автоматического управления и искусственного интеллекта, обеспечивающих функционирование водных ИТС.

Проведенный анализ показывает, что аспекты безопасности, связанные с указанными технологиями, не находят своего отражения в нормативных правовых актах по транспортной безопасности водного транспорта и, как следствие, в планах ее обеспечения, что создает дополнительные риски.

Водные ИТС функционируют в сложном окружении и взаимодействуют с ИТС других видов транспорта и иными объектами критической информационной инфраструктуры. По результатам упомянутого в статье моделирования угроз безопасности информации системы автономного судовождения на внутренних водных путях водные ИТС могут взаимодействовать с Единой государственной системой обеспечения транспортной безопасности, ведомственной информацион-

¹ ГОСТ Р 70732-2023. Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения и методы контроля.

² ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.

³ ГОСТ Р ИСО/МЭК 27033- 5-2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевое взаимодействия с помощью виртуальных частных сетей (ВЧС).



Рис. 5. Области влияния информационной безопасности ИТС на транспортную и национальную безопасность

ной системой Росморречфлота, речными и морскими информационными службами, информационными службами МЧС России и другими системами. Это требует решения проблемы исключения возможного негативного влияния водных ИТС на функционирование взаимодействующих систем.

Рассмотренные в статье проблемы носят системный характер и относимы к ИТС других видов транспорта, так как обусловлены общими факторами. В условиях бурного развития вышеназванных высоких технологий возникает разрыв между сферами технического и технологического характера обеспечения транспортной безопасности, с одной стороны, и правовой сферой – с другой. Возможность реализации достижений в первой сфере может сдерживаться отставанием второй.

Существует насущная потребность отражения в нормативных правовых актах по обеспечению транспортной безопасности водных ИТС вопросов их информационной безопасности, что справедливо и для ИТС других видов транспорта [13, 14].

Благодарности

Автор благодарен доктору технических наук, доценту Сабанову А.Г. за ценные комментарии и рекомендации, которые помогли акцентировать материал статьи на целевой аудитории (исследователи транспортной безопасности водных ИТС, разработчики нормативной правовой базы по ее обеспечению и лица, участвующие в обеспечении транспортной безопасности водных ИТС), исходя из чего была изменена структура изложения и дополнен материал статьи.

Библиографический список

1. Threat Landscape of Transport Sector. ENISA, March 21, 2023. URL: <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape> (дата обращения 15.09.2023).
2. Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2023. URL: <https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023> (дата обращения 15.09.2023).
3. Михалеви́ч И.Ф. Цифровая трансформация систем управления в условиях пандемии COVID-19 // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 4. С. 25-31.
4. Михалеви́ч И.Ф. Цифровая гигиена информационного общества: влияние пандемии COVID-19 // REDS: Телекоммуникационные устройства и системы. 2022. № 3. С. 10-17.
5. University of Texas team takes control of a yacht by spoofing its GPS. URL: <https://newatlas.com/gps-spoofing-yacht-control/28644> (дата обращения 15.09.2023).
6. Spoofing on the High Seas. URL: <https://youtu.be/ctw9ECgJ8L0> (дата обращения 15.09.2023).

7. INTERTANKO (2019). Jamming and Spoofing of Global Navigation Satellite Systems (GNSS). URL: <https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf> (дата обращения 15.09.2023).

8. Androjna A. Perkovic M. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. September 2021. Transactions on Maritime Science 10(2). DOI: 10.7225/toms.v10.n02.w08

9. Balduzzi M., Pasta A., Wilhoit K. A security evaluation of AIS automated identification system / In: Proceedings of the 30th annual computer security applications conference. 2014. Pp. 436-445. DOI:10.1145/2664243.2664257

10. Семенов С.А. Кибербезопасность морского и речного транспорта // Транспорт Российской Федерации. 2018. №1 (74). С. 43-46.

11. Семенов С. Морская кибербезопасность: оценка состояния и пути решения // Морские вести России. 2020. № 1. URL: <https://morvesti.ru/analitika/1692/82776/?ysclid=lmc8mqcng3762121902> (дата обращения 15.09.2023).

12. Семенов С. Морская кибербезопасность – ситуация, проблемы и риски. Экспертная колонка Российского совета по международным делам (РСМД), 8 сентября 2020 года. URL: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/?ysclid=ll572kfohg283787912> (дата обращения 15.09.2023).

13. Mikhalevich I.F. Problemic Issues of Deploying Cooperative Intelligent Transport Systems During of Digital Transformation // 2021 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. IEEE, 2021. DOI: 10.1109/IEEECONF51389.2021.9415999

14. Mikhalevich I.F. Priority Ways to Ensure Cybersecurity of Cooperative Intelligent Transport Systems” // 2022 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. IEEE, 2022. DOI: 10.1109/IEEECONF53456.2022.9744337

15. Radhakrishnan Subramaniam, Satya P. Singh, Parasuraman Padmanabhan, Balázs Gulyás, Prashobhan Palakkeel, Raja Sreedharan. Positive and Negative Impacts of COVID-19 in Digital Transformation // Sustainability 13(16):9470, August 2021. DOI: 10.3390/su13169470/

16. Mikhalevich I.F. Transformation of transport under conditions of digital inequality of control systems // International scientific conference International transport scientific innovation: ITSI-2021. P. 1-7. DOI: 10.1063/5.0105275.

17. Михалеви́ч И.Ф. Проблемы создания доверенной среды функционирования автоматизированных систем управления в защищенном исполнении / Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). М.: Институт проблем управления им. В.А.Трапезникова РАН, 2014. С. 9201-9207.

18. Mikhalevich I.F. Methodological foundations of creation of national protected hardware-software platforms

for critical information infrastructures // T-Comm. 2018. Vol. 12. No. 3. Pp. 75-81.

19. Mikhalevich I.F. Methodology development and implementation of protected hardware and software platform based on the existing // 2018 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. DOI: 10.1109/SOSG.2018.8350623

20. Михалевич И.Ф. Требования, принципы, практика создания отечественных аппаратно-программных платформ для автоматизированных систем в защищенном исполнении критической информационной инфраструктуры Российской Федерации // Интеллектуальные системы. Теория и приложения. 2018. Том. 22. Вып. 4. С. 11-30.

21. Михалевич И.Ф. Гармонизация требований безопасности цифровых систем корпоративного и технологического управления // В сборнике: Управление развитием крупномасштабных систем (MLSD'2020). Труды Тринадцатой международной конференции. 2020. С. 426-436. DOI: 10.25728/mlsd.2020.0426

22. Михалевич И.Ф. Проблема цифрового неравенства автоматизированных систем корпоративного и технологического управления // REDS: Телекоммуникационные устройства и системы. 2020. № 3. С. 43-47.

23. Andy Koronios, Abrar Haider, Kristian Steenstrup. Information and Operational Technologies Nexus for Asset Lifecycle Management // Proceedings of the 4th World Congress on Engineering Asset Management Athens, Greece, 28–30 September 2009 “Engineering Asset Lifecycle”. P. 112-119. URL: https://link.springer.com/chapter/10.1007/978-0-85729-320-6_13 (дата обращения 15.09.2023).

24. Cyber Attacks on Maritime OT Systems Increased 900% in Last Three Years. 2020. URL: <https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/#:~:text=Cyber%2Dattacks%2Don%20the%20maritime,security%20firm%20Naval%20Dome%20reveals> (дата обращения 15.09.2023).

25. The guidelines on Cyber security onboard ships. URL: <https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf> (дата обращения 15.09.2023).

26. Complete Guide to OT Threat Detection and Response By Sectrio | November 20th, 2023. URL: <https://sectrio.com/ot-threat-detection-and-response/#what-is-threat-detection-investigation-and-response> (дата обращения 15.09.2023).

27. Легуша С.Ф. Киберпроблемы на водном транспорте – усилия основных игроков морской индустрии и классификационных обществ на примере Российского морского регистра судоходства // Транспортное право и безопасность. 2022. № 4(44). С. 183-194.

28. Шубинский И.Б., Розенберг Е.Н. Общие положения обоснования функциональной безопасности интеллектуальных систем на железнодорожном транспорте // Надежность. 2023. №3. С. 38-45. DOI: 10.21683/1729-2646-2023-23-3-38-45

References

1. Threat Landscape of Transport Sector. ENISA; 2023. (accessed 15.09.2023). Available at: <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape>.

2. [Threat landscape for industrial automation systems. First half of 2023]. (accessed 15.09.2023). Available at: <https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023>. (in Russ.).

3. Mikhalevich I.F. [Digital transformation of control systems in the context of the COVID-19 pandemic]. *REDS: Telecommunication devices and systems* 2021;11(4):25-31. (in Russ.).

4. Mikhalevich I.F. [Digital hygiene of the information society: the impact of the COVID-19 pandemic]. *REDS: Telecommunication devices and systems* 2022;3:10-17. (in Russ.).

5. University of Texas team takes control of a yacht by spoofing its GPS. (accessed 15.09.2023). Available at: <https://newatlas.com/gps-spoofing-yacht-control/28644>.

6. Spoofing on the High Seas. (accessed 15.09.2023). Available at: <https://youtu.be/ctw9ECgJ8L0>.

7. INTERTANKO (2019). Jamming and Spoofing of Global Navigation Satellite Systems (GNSS). (accessed 15.09.2023). Available at: <https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf>.

8. Androjna A., Perkovic M. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. *Transactions on Maritime Science* 2021;10(2). DOI: 10.7225/toms.v10.n02.w08.

9. Balduzzi M., Pasta A., Wilhoit K. A security evaluation of AIS automated identification system. In: Proceedings of the 30th annual computer security applications conference; 2014. Pp. 436-445. DOI:10.1145/2664243.2664257.

10. Semenov S.A. [Cybersecurity of sea and river transport]. *Transport Rossiyskoy Federatsii* 2018;1(74):43-46. (in Russ.).

11. Semenov S. [Maritime cybersecurity: assessment of the state and solutions]. (accessed 15.09.2023). *Morskiye vesti Rossii* 2020;1. Available at: <https://morvesti.ru/analitika/1692/82776/?ysclid=lm8mqcng3762121902>. (in Russ.).

12. Semenov S. [Maritime cybersecurity – situation, problems, and risks]. (accessed 15.09.2023). Available at: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/?ysclid=ll572kfohg283787912>. (in Russ.).

13. Mikhalevich I.F. Problemic Issues of Deploying Cooperative Intelligent Transport Systems During of Digital Transformation. 2021 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. IEEE; 2021. DOI: 10.1109/IEEECONF51389.2021.9415999.

14. Mikhalevich I.F. Priority Ways to Ensure Cybersecurity of Cooperative Intelligent Transport Systems”. In: proceedings of the 2022 International Conference “Systems of Signals Generating and Processing in the Field of

on Board Communications”. IEEE; 2022. DOI: 10.1109/IEEECONF53456.2022.9744337.

15. Subramaniam R., Singh S.P., Padmanabhan P., Gulyás B., Palakkeel P., Sreedharan R. Positive and Negative Impacts of COVID-19 in Digital Transformation. *Sustainability* 2021;13(16):9470. DOI: 10.3390/su13169470.

16. Mikhalevich I.F. Transformation of transport under conditions of digital inequality of control systems. In: proceedings of the International scientific conference International transport scientific innovation: ITS-2021. Pp. 1-7. DOI: 10.1063/5.0105275.

17. Mikhalevich I.F. [Problems of creating a trusted environment for the functioning of automated control systems in a secure design]. In: Proceedings of the XII All-Russian Meeting on Control Problems (VSPU-2014, Moscow). Moscow: V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences; 2014. Pp. 9201-9207. (in Russ).

18. Mikhalevich I.F. Methodological foundations of creation of national protected hardware-software platforms for critical information infrastructures. *T-Comm* 2018;12(3):75-81. (in Russ.).

19. Mikhalevich I.F. Methodology development and implementation of protected hardware and software platform based on the existing. In: proceedings of the 2018 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. DOI: 10.1109/SOSG.2018.8350623.

20. Mikhalevich I.F. [Requirements, principles, practice of creating domestic hardware and software platforms for automated systems in a secure design for the critical information infrastructure of the Russian Federation]. *Intellektualnye sistemy. Teoriya i primeneniya* 2018;22(4):11-30. (in Russ).

21. Mikhalevich I.F. [Harmonization of security requirements for digital systems of corporate and technological management]. In: [Management of the development of large-scale systems (MLSD’2020). Proceedings of the Thirteenth International Conference]; 2020. Pp. 426-436. <https://DOI:10.25728/mlsd.2020.0426>. (in Russ).

22. Mikhalevich I.F. [The problem of digital inequality in automated corporate and technological management systems]. *REDS: Telecommunication devices and systems* 2020;3:43-47. (in Russ).

23. Koronios A., Haider A., Steenstrup K. Information and Operational Technologies Nexus for Asset Lifecycle Management. In: Proceedings of the 4th World Congress on Engineering Asset Management. Athens (Greece), 28–30 September 2009 “Engineering Asset Lifecycle”. (accessed 15.09.2023). P. 112-119. Available at: https://link.springer.com/chapter/10.1007/978-0-85729-320-6_13.

24. Cyber Attacks on Maritime OT Systems Increased 900% in Last Three Years. (accessed 15.09.2023). Available at: <https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/#:~:text=Cyber%2Dattacks%20on%20the%20maritime,security%20firm%20Naval%20Dome%20reveals>.

25. The guidelines on Cyber security onboard ships. (accessed 15.09.2023). Available at: <https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf>.

26. Complete Guide to OT Threat Detection and Response By Sectrio. November 20th; 2023. (accessed 15.09.2023). Available at: <https://sectrio.com/ot-threat-detection-and-response/#what-is-threat-detection-investigation-and-response>.

27. Legusha S.F. Cyber problems in water transport concerning the efforts of the main players in the maritime industry and classification societies on the example of the Russian Maritime Shipping Register. *Transport law and security* 2022;4(44):183-194. (in Russ).

28. Shubinsky I.B., Rozenberg E.N. General provisions of the substantiation of functional safety of intelligent systems in railway transportation. *Dependability* 2023;3:38-45. DOI: 10.21683/1729-2646-2023-23-3-38-45 (in Russ.).

Сведения об авторе

Михалевич Игорь Феодосьевич – кандидат технических наук, старший научный сотрудник, Российский университет транспорта (МИИТ), доцент кафедры «Управление и защита информации», ул. Образцова, д. 9, стр. 9, Москва, Российская Федерация, 127994, e-mail: mif-orel@mail.ru

About the author

Igor F. Mikhalevich, Candidate of Engineering, Senior Researcher, Russian University of Transport (MIIT), Senior Lecturer, Department of Management and Protection of Information, 9/9 Obratztsova St., Moscow, 127994, Russian Federation, e-mail: mif-orel@mail.ru.

Вклад автора

Автором проведен анализ новых видов угроз транспортной безопасности водных транспортных систем и нормативной правовой базы обеспечения их транспортной безопасности. Рассмотрена архитектура водных ИТС в виде интегрированной автоматизированной системы корпоративного и технологического управления, применение которой направлено на динамичное согласование моделей водных ИТС с моделями актуальных угроз транспортной безопасности в информационной сфере.

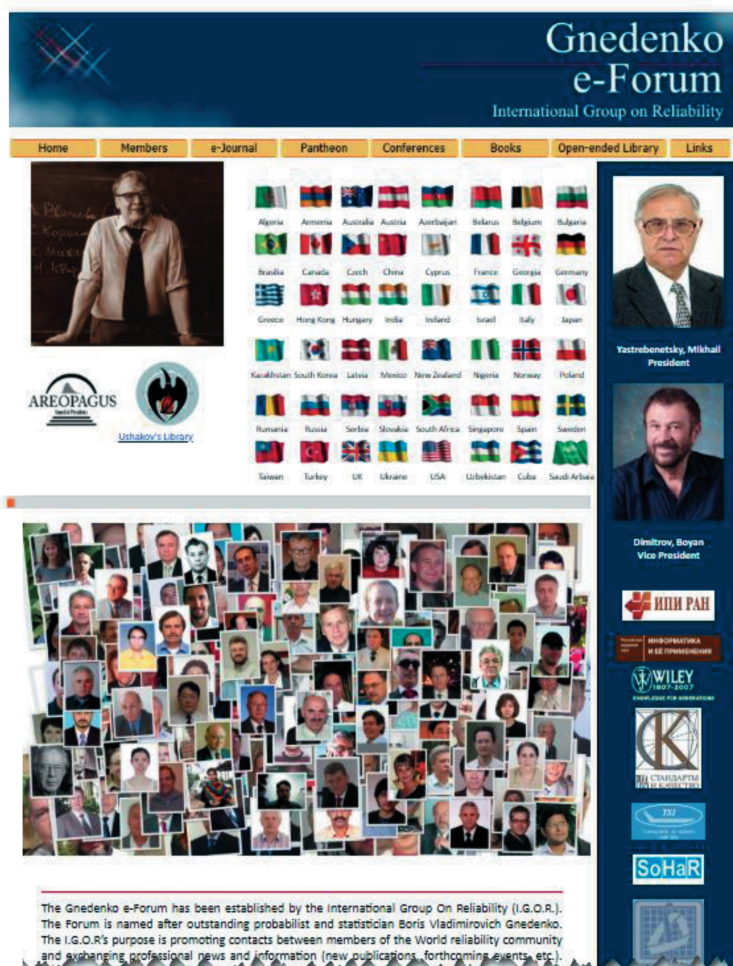
Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.



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, межстрочный 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, межстрочный 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, межстрочный 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:

¹Московский государственный университет, Российская Федерация, Москва

²Санкт-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, межстрочный 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, производственная 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 разде-

лов 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 подрисовочные 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). Подрисовочная 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 подрисовочной подписи не ставится. При выравнивании по центру абзацный отступ всегда должен отсутствовать! Все обозначения, приведенные на рисунках, необходимо пояснять в основном или подрисовочном тексте. Недопустимы отличия в обозначениях на рисунках и в тексте (включая различие прямых/наклонных символов). При проблемах с версткой 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:

$$y = a \cdot x + b. \quad (1)$$

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.

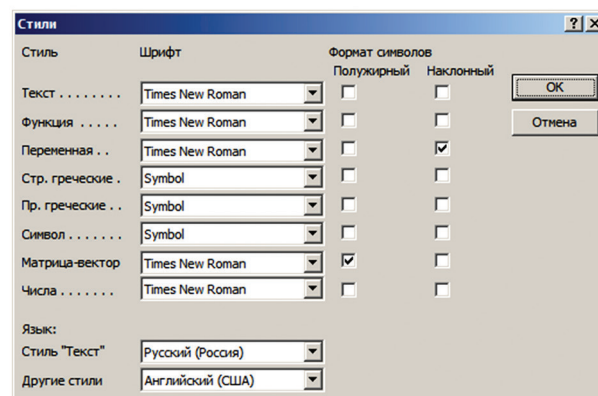
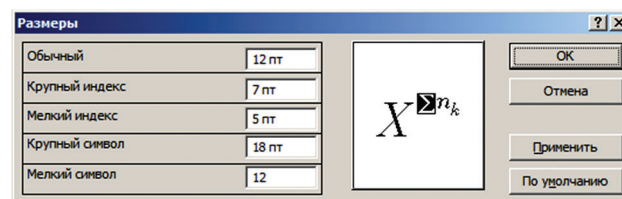
Простые формулы следует набирать без применения формульного редактора (использовать в MS Word русские и латинские буквы, а также меню «Вставка» + «Символ», если требуются греческие буквы и математические операторы), с соблюдением требуемого наклона для латинских символов, например:

$$\Omega = a + b \cdot \theta.$$

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 редак-

тированием формул и их версткой 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):

$$Z = \frac{a \cdot \left(\sum_{i=1}^n x_i + \sum_{j=1}^m y_j \right)}{n + m}. \quad (2)$$

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 удастся его найти (для зарубежных источников удастся 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 набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».

GUIDELINES FOR PUBLICATION IN THE JOURNAL «DEPENDABILITY»

STRUCTURAL DEPENDABILITY THEORY AND PRACTICE

- Methods of calculation, technology and methods of simulation, application software packages, practical calculations of complex systems dependability.
- Mathematical theory of maintenance, practical results of complex systems operation, system lifecycle, optimization of dependability and costs at all lifecycle stages.
- Test methods, criteria of test-based decision-making, accelerated testing, methods of test-based dependability assessment of systems, practical experience of dependability testing.

FUNCTIONAL DEPENDABILITY THEORY AND PRACTICE

- Object, subject and purposes of research, functional dependability indicators, terminology, principles and methods of calculation.
- Methods of assessment and prediction of software dependability, methods of calculation of information processes reliability in hardware and software systems subject to faults, software/operator/input information errors.
- Technology and methods of functional dependability: technology of functionally dependable software design, methods of design of fault-tolerant and operator error-tolerant information processing and management algorithms, methods and ways of protection against input information errors, practical results.

FUNCTIONAL SAFETY OF SYSTEMS THEORY AND PRACTICE

- Object, subject and purposes of research, functional safety indicators; safety functions, safety integrity, functional safety terminology.
- Mathematical methods and models of requirements definition for safety integrity and allowable time of hazardous failure detection, functional safety models of multichannel and multilevel systems.
- Technologies for ensuring functional safety of systems at all lifecycle stages.

FAULT TOLERANCE OF SYSTEMS THEORY AND PRACTICE

- Methods of passive failure protection, mathematical models of structural redundancy, gradual degradation of redundant systems, fault masking, practical results of application 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 assessment of active protection.

RISK MANAGEMENT THEORY AND PRACTICE

- Postulates and principles of safety. Safety case. Methods and practical results of hazard ranking.
- Classification of item risks. Principles and methods of risk assessment. Risk assessment tools. Methods of acceptable risk levels definition. Risk management methodology. Management of operational, technology-related, fire, occupational, environmental risks.
- Integral risks. Methods and models of identification of integral risks of systems. Integral risks of processes. Integral risks of services.

CERTIFICATION AND STANDARDIZATION THEORY AND PRACTICE

- Accreditation of certification bodies and test laboratories, state of the art in Russia and other countries. How to achieve mutual recognition of test results in Russia and other countries? Methods of certification of hardware and software systems for compliance with international functional safety standards.
- Mandatory and voluntary certifications: experience, opinions, suggestions.
- Certification of system quality and dependability: regulatory requirements, testing procedures, practical results.
- 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 development trends of standardization of dependability, fault tolerance and survivability, functional safety and risk management.

INNOVATIVE TECHNOLOGY OF DEPENDABILITY AND SAFETY THEORY AND PRACTICE

- Application of artificial intelligence-based methods in dependability and safety.
- Methods and models of Data Science.
- Algorithms of prediction of failures and hazardous events using Data Science.
- Methods of proactive dependability and safety management.

ЖУРНАЛ ИЗДАЕТСЯ ПРИ УЧАСТИИ И ПОДДЕРЖКЕ

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



АО «НИИАС» – ведущее предприятие ОАО «РЖД» в области создания комплексов и систем обеспечения безопасности движения, управления движением, геоинформационного обеспечения, мониторинга состояния подвижного состава и инфраструктуры железных дорог



Цели:

- ☐ эффективность
- ☐ безопасность
- ☐ надежность перевозок



Основные направления деятельности

- Интеллектуальные системы управления
- Технологии управления перевозками и транспортного обслуживания
- Системы автоматики и телемеханики
- Центры автоматизированного управления
- Информационные системы
- Геоинформационные системы и спутниковые технологии
- Системы транспортной безопасности
- Системы управления инфраструктурой
- Системы управления топливно-энергетическими ресурсами
- Испытания, сертификация и экспертиза
- Информационная безопасность
- Нормативно-правовое обеспечение



www.vniias.ru