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

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

УЧРЕДИТЕЛЬ ЖУРНАЛА:
ООО «Журнал «Надежность»

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

Официальный печатный орган Российской академии надежности

Издатель журнала
ООО «Журнал «Надежность»
Генеральный директор
Саламатин Д.А.
Адрес: 109029, г. Москва,
ул. Нижегородская, д. 27, стр. 1
ООО «Журнал «Надежность»
www.dependability.ru
Отпечатано в ООО «Отмара. нет». 107140,
г. Москва, ул. Русаковская, д. 13, стр. 5,
2 этаж, пом. III/6-7

Подписано в печать 11.06.2025
Объем 92, Тираж 500 экз, Заказ № 19620
Формат 60x90/8, Бумага глянец

Журнал издается ежеквартально с 2001 года,
стоимость одного экземпляра 1210 руб.,
годовой подписки 4840 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 надежность
- Функциональная надежность
- Функциональная безопасность систем
- Отказоустойчивость систем
- Управление рисками
- Сертификация и стандартизация
- Инновационные технологии в области надежности и безопасности
- Техническая эффективность систем управления
- Управление техническими активами
- Обработка больших данных. Системы управления и искусственный интеллект
- Методы и системы защиты информации
- Системный анализ в задачах надежности и безопасности
- Интеллектуальные транспортные системы
- Терминологические вопросы надёжности, отказоустойчивости, безопасности, рисков и живучести
- Сообщения

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

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

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

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

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

СОДЕРЖАНИЕ

Надежность, том 25, №2, 2025 / Dependability 2, 2025
Системный анализ в задачах надежности и безопасности

УДК: 629.039.58
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-3-11

О формировании групп однородности однотипного оборудования АЭС при объединении статистических данных в рамках модели Пуассона

On the homogeneity grouping of same-type NPP equipment when aggregating statistical data using the Poisson model

Морозов В.Б.[1]
Morozov V.B.[1]

[1]*АО «Атомэнергопроект», Российская Федерация, Москва*
[1]*JSC Atomenergoproekt, Russian Federation, Moscow*
morozov_vb@aep.ru

Морозов В.Б.

Резюме. Цель. *В статье в рамках модели Пуассона, применяемой при анализе потоков отказов элементов систем АЭС, описан подход к формированию групп однородности, т.е. максимально широких групп однотипных элементов, для которых интенсивности отказов можно полагать неизменными. Выделение таких групп позволяет объединять эксплуатационные данные по отказам и наработкам оборудования, что повышает качество статистических оценок интенсивностей отказов при оценке надежности систем, составленных из высоконадежных элементов.* **Методы.** *При формировании групп предлагается использовать методы: структурный (на основе симметричности позиций однотипных элементов в составе резервированных каналов систем, позволяющий объединять элементы в составе одной системы) и статистический (использующий результаты статистического теста проверки гипотезы на однородность любых объединяемых групп однотипных элементов). Приведено обоснование применения структурного метода. Предложен статистический тест, основанный на отношении оценок дисперсий интенсивностей отказов без учета и с учетом предположения об однородности объединяемых данных. Исследованы свойства теста, получены соотношения для первых двух моментов его статистики. Показано, что дискретное распределение статистики при большом числе объединяемых групп может быть описано гамма распределением. Предложено правило для определения областей принятия и отклонения основной гипотезы.* **Результаты.** *Представлен пример применения статистического анализа объединения данных по 10-ти группам электроприводных клапанов разных систем АЭС. На основе полученной оценки статистики теста сделано заключение о необходимости исключения из общей популяции группы с резко выпадающей частной оценкой интенсивности отказов. Для оставшихся групп проведена повторная проверка на однородность, получен результат, позволяющий объединить данные 9-ти групп. В статье также представлено обсуждение подходов к решению задачи оценки параметров надежности оборудования новых АЭС, когда эксплуатационной информации недостаточно для получения представительных оценок показателей надежности. Для подобных задач предложено применять эмпирический метод Байеса, в котором априорное распределение формируется на основе метода объединения данных объектов-аналогов с учетом возможной их неоднородности. Показано, что данный метод, ориентированный на конструирование априорных распределений на основе максимума функции правдоподобия также может быть полезен и для решения задач проверки однородности, рассмотренных в статье. На основе предложенных методов разработан общий подход к решению задач оценки надежности высоконадежных систем АЭС с использованием информации, полученной при эксплуатации как объекта анализа (конкретной АЭС), так и аналогичных объектов (референтных АЭС, АЭС с одинаковым типом атомного реактора). Данный подход также эффективен при разработки ВАБ для проектируемых АЭС и АЭС, находящихся на начальном периоде эксплуатации.*

Abstract. Aim. *The paper uses the Poisson model to analyse failure flows of NPP systems' elements and thus describes an approach to defining homogeneity groups, i.e., the broadest possible groups of same-type elements whose failure rates may be considered constant. Defining such groups allows aggregating operational data on equipment failures and times-to-failure, which improves the quality of statistical estimates of failure rates as part of assessing the dependability of systems made up of highly dependable elements.* **Methods.** *For the*

purpose of grouping, it is proposed to use the following methods: structural (based on the positional symmetry of the same-type elements in redundant system channels, which allows combining the elements within a system) and statistical (using the results of the statistical test of the homogeneity hypothesis of any combined groups of same-type elements). The structural method was substantiated. The author proposes a statistical test based on the correlation of the estimated variations in the failure rates with and without regard to the assumption of the homogeneity of the aggregated data. The properties of the test were examined; the correlations for the first two moments of its statistics were obtained. It was shown that a discrete distribution of statistics with a large number of groups to be combined can be described by a gamma distribution. A rule for identifying the main hypothesis acceptance and rejection regions was proposed. **Results.** *The paper presents an example of the application of statistical analysis of aggregated data on 10 groups of motor-operated valves of various NPP systems. Based on the obtained assessment of the test statistics, it is concluded that a group with a sharply deviating partial assessment of the failure rate is to be excluded from the general population. For the remaining groups, the homogeneity test was repeated. A result was obtained that allows combining the data of the 9 groups. The paper also discusses potential ways of solving the problem of assessing the dependability parameters of new NPP equipment, when operational information is not sufficient for obtaining representative estimates of dependability indicators. For such purposes, it is proposed using the empirical Bayes method, whereas the a priori distribution is obtained by aggregating data on similar items taking into account their possible heterogeneity. It is shown that the method that is focused on the construction of a priori distributions based on a likelihood function maximum can also be used for solving the homogeneity verification problems examined in this paper. Based on the proposed methods, a general approach has been developed for assessing the dependability of highly dependable NPP systems using information obtained in the course of operation of both the object of analysis (a specific NPP) and similar facilities (reference NPPs, NPPs with the same type of nuclear reactor). The method is also effective as regards probabilistic safety analysis of NPPs at the stage of their design and initial operation.*

Ключевые слова: *модель Пуассона, анализ данных, интенсивность отказов, объединение данных, группа однородности, структурный метод, статистический тест.*
Keywords: *Poisson model, data analysis, failure rate, data aggregation, homogeneity group, structural method, statistical test.*

Для цитирования: *Морозов В.Б. О формировании групп однородности однотипного оборудования АЭС при объединении статистических данных в рамках модели Пуассона // Надежность. 2025. №2. С. 3-11. https://doi.org/10.21683/1729-2646-2025-25-2-3-11*
For citation: *Morozov V.B. On the homogeneity grouping of same-type NPP equipment when aggregating statistical data using the Poisson model. Dependability 2025;2:3-11. https://doi.org/10.21683/1729-2646-2025-25-2-3-11*

Поступила: *26.09.2024* / **После доработки:** *01.12.2024* / **К печати:** *09.06.2025*
Received on: *26.09.2024* / **Revised on:** *01.12.2024* / **For printing:** *09.06.2025*

Введение

В [1] рассмотрена задача получения исходных данных – интенсивностей отказов оборудования для выполнения вероятностного анализа безопасности (ВАБ) АЭС на стадии проектирования, когда эксплуатационные данные для объекта анализа отсутствуют. Для ее решения применяется байесовский эмпирический подход, позволяющий учитывать всю имеющуюся информацию по объектам-аналогам. Для эксплуатируемых АЭС применение метода [1] позволяет получить распределение, которое можно использовать в качестве априорного совместно со специфической информацией для конкретного блока. При учете же специфических данных актуальна задача формирования т.н. групп однородности, поскольку оборудование АЭС является высоконадежным и количество отказов отдельных единиц оборудования (далее элементов АЭС) даже за десятилетний период работы АЭС мало.

Для однородных групп минимально достаточной статистикой в модели, основанной на анализе потока Пуассона является суммарное число отказов элементов, отнесенное к их суммарной наработке. Вместе с тем однотипное оборудование может поставляться разными изготовителями, эксплуатироваться в различных условиях, отличаться по конструктивному исполнению и т. д. То есть необходимо разработать подход к формированию однородных групп, включающий наряду с инженерными принципами группировки элементов, основанными на качественном анализе признаков общности, статистическую проверку однородности объединяемых данных. Под группой однородности понимается совокупность элементов, обладающих одинаковыми показателями безотказности (для модели Пуассона – одинаковыми значениями интенсивностей отказов). Понятие группы однородности является условным, однако интенсивности отказов элементов таких групп должны быть в

максимальной степени близки друг другу, так чтобы их отличие было статистически неразличимым либо приемлемым для целей ВАБ (например, обеспечивало консервативность результатов расчетов вероятностных показателей безопасности). Способ решения указанной задачи представлен в настоящей статье.

Группирование резервированных однотипных элементов в границах одной системы

Принцип резервирования широко применяется при проектировании систем АЭС, что обусловлено высокими требованиями к вероятностным показателям безопасности и показателям готовности блоков. Это отражается в канальной структуре систем, спроектированных по мажоритарному принципу «*r* из *N*». В каналах систем безопасности (или в части каналов, если система спроектирована с учетом принципа разнообразия) на одинаковых схемных позициях применяются одинаковые по типу элементы одного производителя, как правило находящиеся в одинаковом режиме при работе энергоблока. Таким образом, однотипные резервированные элементы в разных каналах одной системы безопасности обладают большинством признаков общности, что позволяет предположить близость их интенсивностей отказов. Кроме того, следуя принципу консерватизма можно показать, что для подобных структур допущение об одинаковости интенсивностей отказов приводит к наименьшей надежности систем по сравнению с вариантами, при которых указанные параметры различаются (при постоянном средне групповом значении параметра интенсивности).

Обозначим общую вероятность отказа на требование *i*-го канала символом q_i. Тогда вероятность отказа на требование ма жоритарной системы с приемлемой степенью точности можно представить в виде:

$$Q = A \cdot \sum q_{i1} q_{i2} \ldots q_{ir}, \qquad (1)$$

где сумма берется по всем возможным сочетаниям *r* элементов из *n* (*r* – число каналов, отказ которых приводит к отказу системы). Рассмотрим, при каких условиях выражения, задаваемые (1), могут достигать максимума. В качестве ограничения положим: $\sum_i q_i \le R$ (то есть, учитывая малость величин q_i, ограничим общую суммарную вероятность отказа элементов всей системы.

Решение данной задачи на экстремум тривиально в случае $r = n$ (т.е. когда каналы обладают 100%-й эффективностью). В этом случае искомый результат $q_1=q_2=\ldots=q_n=R/n$ является следствием известного неравенства о среднем арифметическом и среднем геометрическом, так как $q_1 q_2 \ldots q_n \le (\frac{1}{n}\sum_i q_i)^n = (R/n)^n$.

Типовые резервированные системы с меньшей, чем 100% эффективностью каналов при $n = 3, 4$ составляют следующие варианты структур: ($r = 2$ $n = 3$); ($r = 2$ $n = 4$); ($r = 3$ $n = 4$). Можно показать [2], что и в этих случаях максимум (1) также будет отвечать равной вероятности отказа на требование каналов. Из сказанного выше следует, что максимум (1) достигается, если вероятности равны.

Теперь поясним смысл ограничения. Если рассматривать однотипные элементы, расположенные в разных каналах систем на определенной схемной позиции, то такие элементы обслуживаются и испытываются по одинаковой процедуре и с равной периодичностью. Это значит, что их вероятности отказов с высокой степенью точности пропорционально зависят от интенсивности отказов: $q_i=\alpha\lambda_i$, где α – некоторый неизменный коэффициент. Следовательно, ограничение $\sum_i q_i \le R$ на практике эквивалентно $\sum_i \lambda_i \le \lambda_\Sigma$, где λ_Σ – суммарная интенсивность отказов в канале. Известно, что сумма пуассоновских потоков есть также поток Пуассона с параметром, равным сумме параметров потоков. Таким образом, для оценки суммарного параметра можно использовать общую статистику событий, не заботясь, насколько различаются параметры составляющих потоков. Следовательно, оценку среднего параметра группы $\frac{1}{n}\sum_i \lambda_i$ можно напрямую получить по суммарной статистике. В частности, поскольку наработки элементов группы одинаковы и равны наработке системы *T*, следуя статье [1] можно показать, что оценка $\hat{\lambda} = \frac{\sum_i r_i}{nT}$ будет эффективной в классе линейных оценок и ее дисперсия будет тем меньше, чем больше наработка и количество элементов в группе.

Аналогичный прием с некоторыми уточнениями применим к резервируемому оборудованию нормальной эксплуатации, с учетом того, что резервированная группа разбивается на подгруппы с элементами, которые находятся в одинаковых эксплуатационных условиях. Полагается, что элементы разных подгрупп имеют разные интенсивностями отказов.

Из сказанного выше следует, что, во-первых, имеются аргументы, позволяющие утверждать, что интенсивности отказов сформированных таким образом групп близки друг другу и, во-вторых, учет их отличия привел бы к недооценке результатов расчетов вероятностных показателей безопасности в терминах ВАБ. Таким образом, объединение элементов в группы однородности по описанному принципу не требует статистических проверок.

Расширение групп однородности (объединение однотипных элементов разных) систем

Формирование групп однородности в соответствии с подходом, изложенным в предыдущем разделе, может оказаться недостаточным для получения представительной статистики вследствие высокой надежности оборудования. В этом случае актуален вопрос дальней-

шего укрупнения групп однородности за счет других систем, содержащих оборудование, однотипное с ранее рассмотренным, и эксплуатирующихся в одинаковом с ним режиме.

Однако допущение об одинаковости интенсивностей отказов объединяемых групп элементов в этом случае уже не может быть принято без статистической проверки, поскольку игнорирование различия параметров объединяемых групп может привести к излишне оптимистическим результатам расчетов при выполнении ВАБ.

Для решения подобной задачи используются методы проверки гипотез. Основная гипотеза есть предположение о том, что объединяемые групповые выборки однородны. В статье [1] в рамках допущения, что совокупность имеющихся групповых интенсивностей отказов может быть описана некоторым «материнским» Г-распределением, показано, что данная гипотеза может быть интерпретирована как равенство нулю дисперсии данного распределения. В качестве конкурирующей рассмотрим гипотезу о неравенстве нулю указанной дисперсии.

Для проверки необходимо получить статистику, которая при верной гипотезе имеет независящее от результатов наблюдений распределение. Квантили этого распределения соответствуют различным уровням значимости, по которым судят о принятии либо отклонении основной гипотезы. Уровень значимости 0,1 часто рассматривают как типовой для отклонения гипотезы, если значение статистики превышает соответствующий ему квантиль распределения. В данной задаче рекомендуется также применить квантиль распределения статистики для уровня 0,2, рассматривая его как граничное значение для принятия гипотезы. Интервал значений статистики, отвечающих уровням значимости от 0,2 до 0,1, указывает на необходимость проведения дополнительного анализа данных, направленных на поиск возможных причин различий параметров групп.

Такой тест (критерий) однородности может быть построен на основе следующей статистики:

$$C = \frac{\sum_1^K w_i^2 \left(\frac{r_i}{T_i} - \hat{\lambda} \right)^2}{\hat{\lambda} / \left(\sum_1^K T_i \right)}, \qquad (2)$$

где $\hat{\lambda} = \left(\sum_1^K r_i \right) / \left(\sum_1^K T_i \right)$ представляет оценку интенсивности отказов объединенной популяции элементов (при условии однородности параметров групп), $w_i = T_i / \left(\sum_1^K T_i \right)$ – оптимальные весовые коэффициенты интенсивности отказов с применением метода МП для объединенной выборки при верной основной гипотезе [1].

Пояснить смысл (2) можно следующим образом. В статье [1] показано, что числитель представляет собой оценку дисперсии эффективной (в классе линейных оценок) оценки средней по популяции интенсивности отказов в частом случае однородных данных, то есть при равенстве нулю дисперсии материнского распределения ($V = 0$). Как следует из [1, формула (9)], в случае неоднородных групповых данных $V > 0$ и математическое ожидание числителя даже при сохранении неизменными в (2) коэффициентов w_i будет всегда больше математического ожидания знаменателя.

То есть по величине отклонения частного (2) от единицы[1] можно судить о наличии конечной дисперсии у материнского распределения межгрупповых интенсивностей отказов, а значит, об их различии. При этом для данной задачи интерес представляет условное распределение статистики при известном $\Sigma r_i > 0$.

На основе исследования распределения статистики теста при верной основной гипотезе можно сделать следующие выводы:

- первые моменты статистики C не зависят от абсолютных значений наработок групп (зависят только от их отношений), что интуитивно понятно и позволяет использовать масштабирование времени;

- математическое ожидание C, обозначенное $M[C]$ при известном Σr_i не зависит от результатов наблюдений, то же верно в отношении дисперсии $V[C]$;

- дискретное распределение статистики C при большом числе объединяемых групп хорошо аппроксимируется гамма распределением.

Указанные выше параметры $M[C]$ и $V[C]$ вычисляются по конечным формулам:

$$M[C] = 1 - S_2;$$

$$Var[C] = 2\left(S_2 - 2S_3 + S_2^2\right) - \frac{2}{\sum r_i}\left(S_2 - 4S_3 + 3S_2^2\right), \qquad (3)$$

где $S_2 = \Sigma(\frac{T_i}{T_\Sigma})^2$, $S_3 = \Sigma(\frac{T_i}{T_\Sigma})^3$, $T_\Sigma = \Sigma T_i$.

Вывод формул (3) использует понятие условного математического ожидания и здесь не приводится. Можно показать, что выражение для дисперсии будет положительным при любом числе групп не менее 2-х и количестве отказов не менее одного [2].

Следует отметить, что близкая по смыслу задача проверки гипотезы однородности значений интенсивностей разных пуассоновских потоков упоминается в литературе. В частности, в классической книге Кокса и Льюиса [3], для решения которой был предложен тест, известный как D-критерий. В [3] также указано, что при равных временных интервалах его статистика асимптотически сходится к χ^2-распределению с числом степеней свободы K-1, при этом среднее и дисперсия составляют $K-1 u 2(K-1)\left(1 - \frac{1}{r_\Sigma}\right)$ соответственно. Покажем, что первые моменты статистик C и D критериев при равных временных интервалах и в рамках допущения о допустимости применения Г-распределения для описания межгрупповых интенсивностей отличаются лишь постоянным множителем. В [1] приводится формула (10)

[1] В действительности математическое ожидание статистики смещено от единицы в меньшую сторону, так как вычисляется при фиксированном общем числе событий.

Табл. 1

Группа 1	Группа 2	Группа 3	Группа 4	Группа 5	Группа 6	Группа 7	Группа 8	Группа 9	Группа 10
40	30	20	40	30	30	30	30	30	30
4,00	3,00	2,00	3,00	3,00	3,00	3,00	3,00	3,00	3,00
1	1	2	2	0	1	0	4	1	0
$4{,}69\cdot10^{-7}$	$6{,}25\cdot10^{-7}$	$1{,}56\cdot10^{-6}$	$1{,}04\cdot10^{-6}$	$2{,}08\cdot10^{-7}$	$6{,}25\cdot10^{-7}$	$2{,}08\cdot10^{-7}$	$1{,}88\cdot10^{-6}$	$6{,}25\cdot10^{-7}$	$2{,}08\cdot10^{-7}$

для дисперсии, описывающей отклонение параметра некоторого случайно выбранного потока (полученной путем взвешенного усреднения дисперсий по группам) от среднего значения всей популяции. Оценка данной дисперсии при $w_i = \frac{T_i}{T_\Sigma}$ представима в виде:

$$\widehat{V_{ar}} = \sum_{i=1}^{K} w_i \left[\frac{(r_i - \hat{\lambda}T_i)^2}{T_i^2}\right] = \sum_{i=1}^{K} w_i \left[\frac{r_i^2 - \hat{\lambda}^2 T_i^2}{T_i^2}\right] =$$
$$= \frac{\hat{\lambda}}{T_\Sigma}\left[\sum_{i=1}^{K}\frac{r_i^2}{\hat{\lambda}T_i} - \hat{\lambda}T_\Sigma\right] = \frac{\hat{\lambda}}{T_\Sigma}\left[\sum_{i=1}^{K}\frac{r_i^2}{\hat{\lambda}T_i} - r_\Sigma\right]. \qquad (4)$$

Выражение в скобках (4) – это статистика *D*-критерия. Поэтому можно записать:

$$D = \frac{\left[\sum_{i=1}^{K} w_i \left(\frac{r_i}{T_i} - \hat{\lambda}\right)^2\right]}{\frac{\hat{\lambda}}{T_\Sigma}}. \qquad (5)$$

Сравнивая формулы (5) и (2) видим, что их отличие состоит в степени коэффициентов у w_i, то есть, вообще говоря, это разные статистики. При этом в [1] (формулы (11, 12)) показано, что при равенстве периодов наблюдений для первых двух моментов распределений это отличие выражено только в множителе K – числе групп элементов. Чтобы убедиться в этом, заметим, в частности, что при $\frac{T_i}{T_\Sigma} = \frac{1}{K}$

$$M[C] = 1 - \frac{1}{K};$$
$$Var[C] = 2\left(\frac{1}{K} - \frac{1}{K^2}\right) - \frac{2}{\sum r_i}\left(\frac{1}{K} - \frac{1}{K^2}\right) =$$
$$= 2\frac{1}{K}\left(1 - \frac{1}{K}\right)\left(1 - \frac{1}{r_\Sigma}\right). \qquad (6)$$

В общем случае сравнение критериев показывает следующее. Критерий *D* пропорционально учитывает отклонения числа отказов в группах от средних значений, что при значительном различии периодов наблюдений приводит к повышению его чувствительности к случайным выбросам, характерным для малых периодов. Применение квадратичных коэффициентов в *C* понижает значимость указанных периодов в общей статистике, это приводит к большей стабильности результатов.

Например, при наличии в общем числе групп *K* двух подгрупп с существенно разными периодами наблюдения, статистика *C* будет хорошо приближаться χ^2-распределением с меньшим числом степеней свободы (соответствующим количеству групп с большим периодом наблюдения), но при этом реализации *C* при неизменных параметрах межгруппового материнского распределения будут менее вариативными.

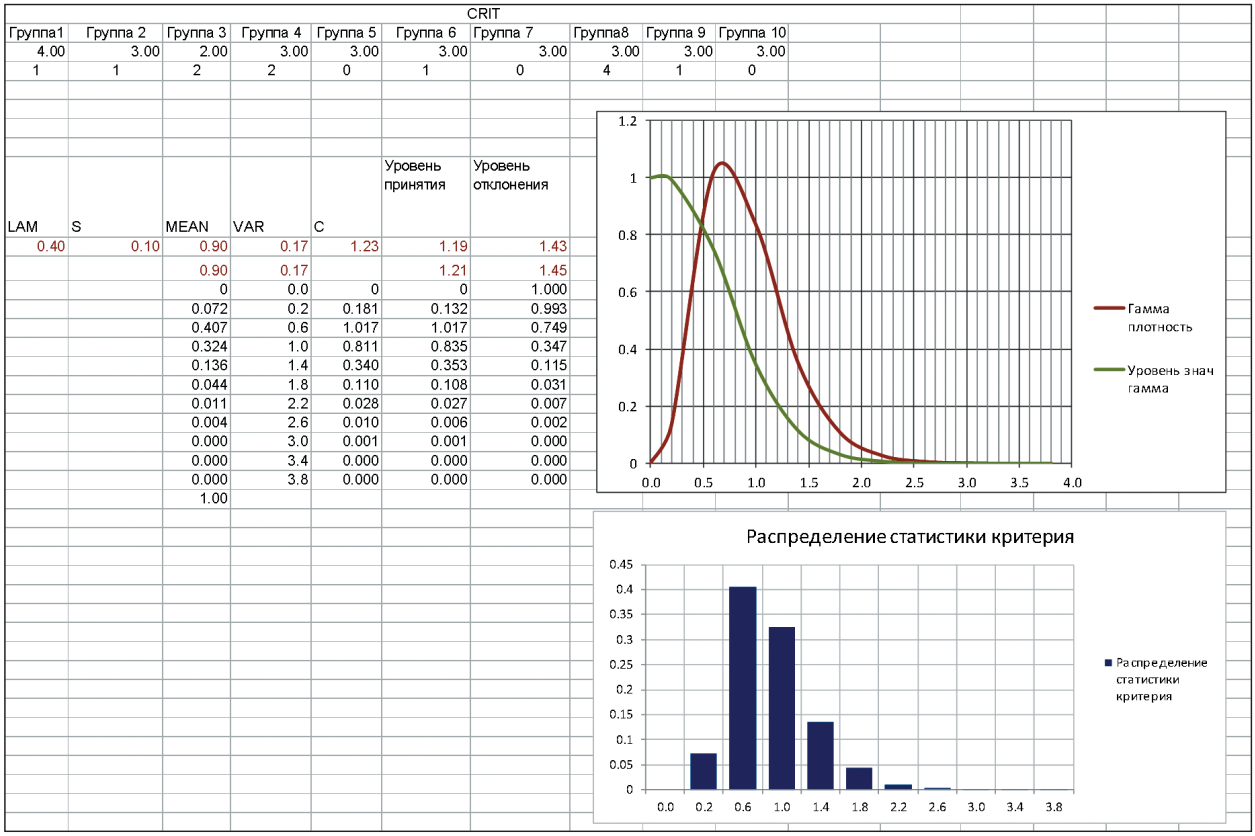
Задача исследования мощности критерия требует отдельного рассмотрения. Заметим, что на практике требуется исключить принятие гипотезы однородности в случаях, когда дисперсия материнского распределения становится сравнимой с дисперсией отклонений числа событий в группах от средних значений, обусловленных чисто статистическим разбросом, то есть образовывать с последней примерно равный вклад в величину общей дисперсии.

Как отмечалось выше (см. (2)), для конечных значений параметра масштаба τ исходного материнского Г-распределения, математическое ожидание числителя *C* будет больше его значения, вычисленного в предположении однородных данных (случай однородных данных отвечает бесконечному τ). Это говорит о том, что при значениях τ сравнимых со средним по группам периодом наблюдений или меньших, смещение числителя в большую сторону должно быть достаточным, чтобы при всех возможных реализациях $\{r_i\}$ при условии $\Sigma r_i = const$ обеспечить низкую вероятность ошибки 2-го рода.

В качестве иллюстрации применения предложенного теста рассмотрим несколько примеров. Пусть имеется 10 групп электроприводных клапанов, представляющих различные системы энергоблока. Данные представлены в табл. 1 за 10 лет эксплуатации энергоблока (80 000 ч наработки), число элементов в группах – от 20 до 40. Используя масштабирование, приведем данные по суммарным наработкам и отказам групп к удобному формату (во второй строке таблицы указано количество клапанов в каждой группе, в третьей – наработка в масштабированном формате, в четвертой – количество отказов, в последней – оценка средней интенсивности отказов групп с использованием неинформативного распределения Джеффриса [5] в размерности 1/ч[1].

Для выполнения вычислений была использована программа, версия которой реализована в виде макроса, встроенного в EXCEL.

[1] Априорные неинформативные распределения в рамках подхода Байеса применяются в ВАБ при отсутствии эксплуатационных данных по изделиям аналогам.



CRIT									
Группа1	Группа 2	Группа 3	Группа 4	Группа 5	Группа 6	Группа 7	Группа8	Группа 9	Группа 10
4.00	3.00	2.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00
1	1	2	2	0	1	0	4	1	0

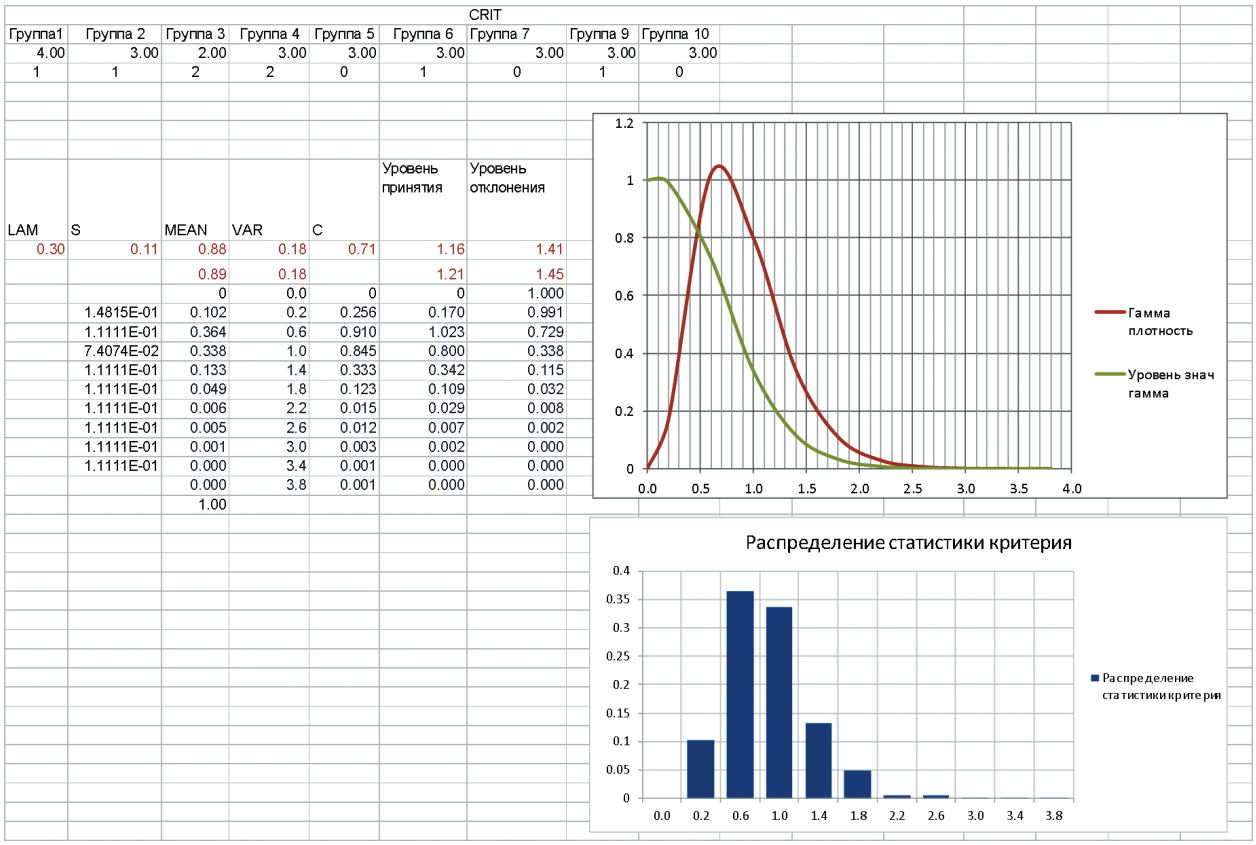
LAM	S	MEAN	VAR	C	Уровень принятия	Уровень отклонения
0.40	0.10	0.90	0.17	1.23	1.19	1.43
		0.90	0.17		1.21	1.45
		0	0.0	0	0	1.000
		0.072	0.2	0.181	0.132	0.993
		0.407	0.6	1.017	1.017	0.749
		0.324	1.0	0.811	0.835	0.347
		0.136	1.4	0.340	0.353	0.115
		0.044	1.8	0.110	0.108	0.031
		0.011	2.2	0.028	0.027	0.007
		0.004	2.6	0.010	0.006	0.002
		0.000	3.0	0.001	0.001	0.000
		0.000	3.4	0.000	0.000	0.000
		0.000	3.8	0.000	0.000	0.000
		1.00				

Рис. 1

На рис.1 представлены исходная информация и результаты применения метода для данного примера. В верхних строках распечатки отображены исходные данные: в первой строке – условное наименование групп данных, во второй строке – наработки, во третьей строке – количество событий. Две строки с выделением красным цветом представляют оценки параметров распределения статистики теста: среднего значения (Mean) и дисперсии (Var), а также значений для уровней безусловного принятия и отклонения нулевой гипотезы. Верхние значения этих величин получены методом имитационного моделирования (Монте-Карло), а нижние – на основе параметров, определенных по формулам (3) с использованием аппроксимации распределения статистики критерия гамма распределением. Для контроля точности аппроксимации дискретного распределения статистики гамма распределением под графиком гамма-плотности расположена гистограмма, полученная способом имитационного моделирования.

Поскольку указанное распределение является дискретным, при малом количестве групп и малых числах отказов квантили для уровней значимости следует брать по результатам статистического моделирования. В данном же примере, как видно из графиков, их различие несущественно. На распечатке также указано значение статистики критерия при наблюдаемых исходных данных. Цветом выделены оцифровки графиков: эмпирической гистограммы и плотности, плотности гамма распределения и интегральной функции (гамма) для определения уровней принятия и отклонения основной гипотезы. В данном примере значение статистики равно 1,23, то есть находится в интервале (1,19–1,43), определенном уровнями принятия и отклонения гипотезы однородности. В соответствии с изложенным выше подходом, необходимо определить группу с наиболее выпадающей оценкой интенсивности отказов (такой в примере является группа № 8, для нее оценка интенсивности примерно в 4 раза превышает среднюю оценку). Далее следует провести оценку влияния данной группы на результат выполнения теста на однородность путем ее исключения. Результаты расчетов, полученные при исключении группы 8 представлены на рис. 2. Видно, что значение статистики в этом случае находится в зоне принятия основной гипотезы, что позволяет заключить, что объединяемые данные могут считаться однородными. При вычислении оценки интенсивности отказов формируемой таким образом общей группы можно использовать принцип простого суммирования информации (8 отказов за общую суммарную наработку $2{,}16 \cdot 10^7$ ч.).

В качестве подтверждения сделанных на основании результатов тестов выводов можно применить метод, изложенный в [1], в отношении оценки дисперсии т.н. материнского распределения объединенной выборки. Для практически однородных данных такая дисперсия должна быть мала в сравнении с дисперсией, соответствующей случайному разбросу статистики отказов в группах, обусловленному ограниченностью периода наблюдения. На рис. 3 представлены результаты вычислений для 9-ти групп (за исключением группы 8).



CRIT

Группа1	Группа 2	Группа 3	Группа 4	Группа 5	Группа 6	Группа 7	Группа 9	Группа 10
4.00	3.00	2.00	3.00	3.00	3.00	3.00	3.00	3.00
1	1	2	2	0	1	0	1	0

LAM	S	MEAN	VAR	C	Уровень принятия	Уровень отклонения
0.30	0.11	0.88	0.18	0.71	1.16	1.41
		0.89	0.18		1.21	1.45
		0	0.0	0	0	1.000
	1.4815E-01	0.102	0.2	0.256	0.170	0.991
	1.1111E-01	0.364	0.6	0.910	1.023	0.729
	7.4074E-02	0.338	1.0	0.845	0.800	0.338
	1.1111E-01	0.133	1.4	0.333	0.342	0.115
	1.1111E-01	0.049	1.8	0.123	0.109	0.032
	1.1111E-01	0.006	2.2	0.015	0.029	0.008
	1.1111E-01	0.005	2.6	0.012	0.007	0.002
	1.1111E-01	0.001	3.0	0.003	0.002	0.000
	1.1111E-01	0.000	3.4	0.001	0.000	0.000
		0.000	3.8	0.001	0.000	0.000
		1.00				

Рис. 2

Из рис. 3 следует, что оценка дисперсии V материнского распределения для 9-ти групп на 3 порядка меньше оценки общей дисперсии Var, что подтверждает сделанные ранее выводы. При сравнении границ приведенного на рис. 3 90%-го интервала с результатами оценок средних групповых интенсивностей отказов в табл. 1 видно, что выпадение оценки интенсивности отказов за границы интервала наблюдается только для одной из 9-ти групп, что может объясняться статистическим разбросом.

При этом для 10-ти исходных групп значение V составляет уже около 19% дисперсии Var, а $\tau = 12{,}98$, что сравнимо с суммарной длительностью периодов наблюдений, но превышает в несколько раз длительность каждого из них. В таком случае критерий не должен давать однозначного ответа по принятию или отклонению основной гипотезы однородности, что и подтверждено результатами, представленными на рис. 1.

Если увеличить число отказов в группе 2 до 5-ти, выборочное значение критерия для 10-ти групп увеличится до 2,07, что гарантированно превышает уровень отклонения основной гипотезы. Значение τ в этом случае равно 2,22, то есть близко к групповым периодам, а V составляет уже около 57% от общей дисперсии Var. Также важно отметить, что в последнем случае значение МП-оценки $\hat{\lambda} = s / \tau = 0{,}54$, что уже заметно отличается от $r_\Sigma / T_\Sigma = 0{,}5$.

Приведенные примеры подтверждают возможность простого суммирования данных по 9-ти группам для получения более представительной статистики по расширенной группе однородности и показывают эффективность теста при анализе неоднородных данных. Применяя неинформативное распределение Джеффриса для объединенной однородной выборки по 9-ти группам получим следующие параметры байесовской оценки интенсивности отказов: $\hat{\lambda}=3{,}94\cdot10^{-7}$ 1/ч.; $\hat{\lambda}_{0,05}=2{,}01\cdot10^{-7}$ /ч.; $\hat{\lambda}_{0,5}= 3{,}78\cdot10^{-7}$ /ч.; $\hat{\lambda}_{0,95}=6{,}39\cdot10^{-7}$ /ч.

Коэффициент ошибки для данного примера равен 1,69.

Обсуждение результатов

Излагаемый здесь метод позволяет формировать группы однородности, для которых значение интенсивности отказов может считаться неизменным, что повышает представительность имеющейся эксплуатационной статистики. Если же общее число отказов в объединенной популяции остается небольшим, следует использовать дополнительную информацию по блокам-аналогам для формирования априорного распределения с последующем применением байесовской процедуры, т.е. с использованием метода [1]. Предложенный в статье C-критерий проверки гипотезы однородности сопоставим с известным D-критерием Кокса-Льюиса [3], отличаясь от последнего большим акцентом на использование результатов, полученных для групп с относительно большой наработкой. Если наработки групп равны, оба критерия можно считать эквивалентными.

4,00	3,00	2,00	3,00	3,00	3,00	3,00	3,00	3,00
1	1	2	2	0	1	0	1	0
T	LnL(T)	Lam0	LIM	Lam	Scale			
0,01	-35,96910	0,30	-10,8518076	0,30	800000,000			
0,0112982	-35,25752	TMAX	LnLMAX					
0,012765	-34,54812	2259,645	-10,8535568					
0,0144222	-33,84110	S	Vrd	V	Var			
0,0162945	-33,13671	669,583	9,88E-02	1,31E-04	9,89E-02			
0,0184099	-32,43520							
0,0207999	-31,73685							
0,0235002	-31,04195							
0,0265511	-30,35083							
0,029998	-29,66383							
0,0338925	-28,98135							
0,0382925	-28,30378							
0,0432637	-27,63155							
0,0488803	-26,96515							
0,0552261	-26,30506							
0,0623957	-25,65182							
0,0704961	-25,00599							
0,079648	-24,36818							
0,0899882	-23,73900							
0,1016707	-23,11912							
0,1148698	-22,50924							
0,1297825	-21,91006							
0,1466313	-21,32232							
0,1656673	-20,74680							
0,1871747	-20,18425							
0,2114743	-19,63547							
0,2389284	-19,10123							
0,2699467	-18,58232							
		$L_{0,05}$	$L_{0,5}$	$L_{0,95}$	Mean	EF (Mean and L0,95)	EF (Med and L0,95)	
0,304992	-18,07949							
0,3445868	-17,59348	1,38E-08	2,44E-07	1,16E-06	3,70E-07	5,11	4,74	

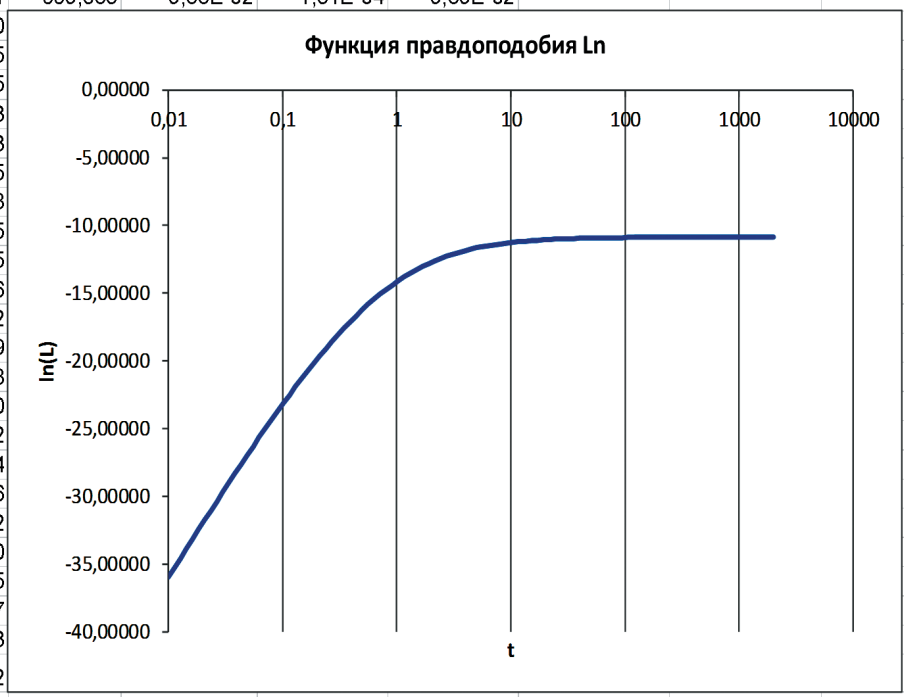


Рис. 3

Предложенный метод формирования групп в совокупности с подходом, представленным в [1], представляют две стороны единого инструмента, позволяющего обоснованно решать задачи анализа данных анализа надежности систем и ВАБ на основе имеющейся эксплуатационной статистики в рамках модели пуассоновских потоков событий.

Рассмотрим особенности применения обоих методов. Прежде всего заметим, что каждый из них предназначен для решения своей задачи: описанный в этой статье – для формирования максимально широких групп однородности в объеме эксплуатационных данных конкретного блока АЭС, а изложенный в [1, 4] – для охвата всей популяции априорных данных по блокам – аналогам при общих условиях. При этом для проектируемого блока применение [1] является единственно возможным способом получения каких-либо оценок показателей надежности.

В основе обоих подходов лежит общая цель указанных задач исследования – анализ потоков информации от близких по своим свойствам объектов, отличающиеся рядом конструктивных особенностей, проектных либо эксплуатационных характеристик, которые могут формировать различие в показателях надежности оборудования.

При их решении методы могут дополнять друг друга, обеспечивая необходимую степень уверенности в принятии статистических выводов. Пример такого использования приведен в разделе 2 статьи, где метод, описанный в [1] подтверждает вывод об однородности данных 9-ти групп на основе анализа дисперсий оценок объединенной популяции и сравнения границ 90%-го толерантного интервала с внутригрупповыми оценками.

Необходимо обратить внимание на то, что 90%-й толерантный интервал, приведенный в конце раздела 2, получен для оценки интенсивности отказов объединенной однородной группы, в то время как такой же интервал в нижней строке таблицы на рис. 3 характеризует границы отклонения частных оценок интенсивности отказов в отдельных группах от значения интенсивности отказов объединенной популяции, полученной при общих условиях, то есть указанные интервалы имеют совершенно разный смысл.

Имеется также отличие в подходах к исключению групп при анализе данных. Согласно [1], приоритет при принятии решения отводится инженерному анализу, в то время как для рассматриваемой здесь задачи – статистическому. Это напрямую связано с различием задач. В то же время, независимо от постановки задачи, при ее выполнении никогда нельзя пренебрегать инженерными аргументами в пользу применения чисто статистических выводов, поскольку последним присуща неопределенность, связанная с вероятностной природой оценок.

Заключение

В статье описан метод формирования групп однородности однотипного оборудования в системах АЭС (групп оборудования, характеризующихся в моделях надежности единым значением интенсивности отказов). Целью применения данного подхода является формирование максимально широких групп, что позволяет суммировать информацию по отказам оборудования и наработкам для повышения качества оценок параметров. Указанная задача решается на основе метода проверки гипотез. В статье предложен статистический тест проверки основной гипотезы (однородности объединяемых выборок), исследованы его свойства и приведены примеры его применения. Показано, что описанный в статье метод, в совокупности с методом, изложенным в [1], представляют единый инструмент, позволяющий обоснованно подходить к решению задачи формирования массива данных по показателям надежности элементов и интенсивностям исходных событий для ВАБ в рамках пуассоновской модели на основе метода Байеса с использованием имеющейся эксплуатационной статистики.

Библиографический список

1. Морозов В.Б., Морозова М.А. О методах оценки интенсивности отказов оборудования для вероятностного анализа безопасности проектируемой АЭС при объединении данных от различных источников // Надежность и качество сложных систем. 2024. № 1(45). С. 39-48.

2. Морозов В.Б. Совершенствование моделей и методов вероятностного анализа безопасности АЭС и их применение в практике проектирования и эксплуатации АЭС с реакторами ВВЭР: дис. … докт. техн. наук: 05.14.03 / АО ОКБ «ГИДРОПРЕСС». Москва, 2021. 283 с.

3. Кокс Д., Льюис П. Статистический анализ последовательностей событий. М.: «Мир», 1969. 312 с.

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

5. Jeffreys H. An Invariant Form for the Prior Probability in Estimation Problems // Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences. 1946. Vol. 186(1007). Pp. 453–461. DOI:10.1098/rspa.1946.0056

References

1. Morozov V.B., Morozova M.A. On methods for assessing equipment failure rates for probabilistic safety analysis of nuclear power plants at design stage when pooling data from various sources. *Reliability and Quality of Complex Systems* 2024;1(45):39-48. (in Russ.)

2. Morozov V.B. [Improving the models and methods of probabilistic analysis of NPP safety and their application in the practice of designing and operating nuclear power plants with VVER reactors: a Doctor of Engineering dissertation: 05.14.03. AO OKB GIDROPRESS]. Moscow; 2021. (in Russ.)

3. Cox D., Lewis P. The statistical analysis of series of events. Moscow: Mir; 1969.

4. Morozov V. A treatment of uncertainties for component reliability or initiator frequency estimates based on combining data sources with the potential of non-homogeneity. In: Proceedings of the International Topical Meeting on Probabilistic Safety Assessment PSA-99. Washington DC; 1999. Pp. 377-379.

5. Jeffreys H. An invariant form for the prior probability in estimation problems. In: Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences 1946;186(1007):453-461. DOI:10.1098/rspa.1946.0056.

Сведения об авторе

Морозов Владимир Борисович, Адрес: 127495, Челобитьевское ш., д.1А, 14-4, Москва, Российская федерация, АО «Атоэнергопроект», директор по ВАБ и анализу готовности, доктор технических наук, Электронная почта: Morozov_vb@aep.ru, Morozov-sloboda@mail.ru, Мобильный: +7 (909) 945 36 54

About the author

Vladimir B. Morozov, Address: 1A, 14-4 Chelobitievskoe sh., Moscow, 127495, Russian Federation, JSC Atoenergoproekt, Director on PSA and Reliability Analysis, Doctor of Engineering, E-mail: Morozov_vb@aep.ru , Morozov-sloboda@mail.ru, Mobile: +7 (909) 945 36 54.

Вклад автора в статью

Морозов В.Б. предложил статистический тест проверки основной гипотезы (однородности объединяемых выборок), исследовал его свойства и показал примеры его применения. Автором разработан общий подход к решению задач оценки надежности высоконадежных систем АЭС с использованием информации, полученной при эксплуатации как объекта анализа (конкретной АЭС), так и аналогичных объектов.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

УДК 621.019
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-12-18

Методические основы бенчмаркинга уникальных объектов электроэнергетических систем

Methodological foundations of benchmarking unique electric power facilities

Фархадзаде Э.М., Мурадалиев А.З., Ашурова У.К.
Азербайджанский научно-исследовательский и проектно-изыскательский институт энергетики, e-mail: elmeht@rambler.ru
Farhadzadeh E.M., Muradaliyev A.Z., Ashurova U.K.
Azerbaijan Scientific-Research and Design-Prospecting Institute of Energetic, e-mail: elmeht@rambler.ru


Фархадзаде Э.М.


Мурадалиев А.З.

Резюме. *Одной из основных проблем электроэнергетических систем является отсутствие нормативных документов, регламентирующих эксплуатацию, техническое обслуживание и ремонт основного оборудования, срок службы которого превышает нормативное значение. Назовем их стартехами (СТ). Трудности сводятся к отсутствию методологий количественной оценки оперативной надежности и безопасности СТ с последующим их бенчмаркингом. Наукоемкость, громоздкость и трудоемкость решения этой проблемы обусловливают необходимость разработки соответствующих автоматизированных систем. Рассмотрены некоторые особенности оценки интегрального показателя и бенчмаркинга уникальных объектов, аналоги которых по заданному сочетанию разновидностей значимых признаков отсутствуют. В рекомендуемых методах и алгоритмах использованы технико-экономические показатели энергоблоков ПГУ-400.*

Abstract. *One of the key problems faced by electric power systems is the lack of regulatory documents regarding the operation, maintenance, and repair of the main equipment whose service life is beyond the standard value. Let us call them "oldtech" (OT). The difficulties come down to the lack of a method for quantifying the operational dependability and safety of OTs with subsequent benchmarking. The research-intensive, cumbersome, and time-consuming solution to this problem requires the development of appropriate automated systems. The authors examined certain features of the process for evaluating the integrated measure and benchmarking of unique facilities that do not compare to any others in terms of a specified combination of types of significant features. The recommended methods and algorithms use the technical and economic indicators of PGU-400 power units.*

Ключевые слова: *бенчмаркинг, уникальный объект, оперативная эффективность, интегральный показатель, техническое состояние.*
Keywords: *benchmarking, unique facility, operational efficiency, integrated measure, technical condition.*

Для цитирования: *Фархадзаде Э.М., Мурадалиев А.З., Ашурова У.К. Методические основы бенчмаркинга уникальных объектов электроэнергетических систем // Надежность. 2025. №2. С. 12-18. https://doi.org/10.21683/1729-2646-2025-25-2-12-18*
For citation: *Farhadzadeh E.M., Muradaliyev A.Z., Ashurova U.K. Methodological foundations of benchmarking unique electric power facilities. Dependability 2025;2:12-18. https://doi.org/10.21683/1729-2646-2025-25-2-12-18*

Поступила: *26.05.2024* / **После доработки:** *10.10.2024* / **К печати:** *09.06.2025*
Received on: *26.05.2024* / **Revised on:** *10.10.2024* / **For printing:** *09.06.2025*

1. Актуальность проблемы

Одной из основных проблем электроэнергетических систем (ЭЭС) является повышение оперативной эффективности работы (ОЭР) основного оборудования, устройств и установок (объектов), срок службы которых приблизительно равен или превышает расчетный (номинальный, парковый). Назовем их «старой техникой» (СТ). Эта проблема не новая [1–3]. Хорошо известны недопустимые последствия системных аварий, причиной которых является СТ. Гибель и травмирование персонала ЭЭС, нарушение экологии и большие материальные затраты часто объясняются изменением климата. Несмотря на то, что наблюдается систематическое увеличение во многих ЭЭС относительного числа СТ (в настоящее время эта величина превышает 60%), проблема остается нерешенной.

Рассмотрим некоторые особенности данной проблемы:

- эффективность работы объектов ЭЭС в современном понимании – это комплексное (интегральное) понятие,

включающее наряду с экономичностью работы надежность и безопасность обслуживания. Хотя эти свойства учитывались и ранее, однако количественно оценивалась лишь экономическая составляющая ОЭР;

- количественная оценка оперативной надежности работы и опасности обслуживания не проводилась. Согласно [4] «в пределах гарантированного срока изготовитель (поставщик) несет ответственность за скрытые, а в случаях, предусмотренных договором, и за явные дефекты»;

- при завершении гарантированного срока службы объекта отношение к характеристике ОЭР не изменяется, так как отсутствует соответствующая нормативная база технического обслуживания и ремонта СТ. Обычно показатели надежности рассчитывают на этапе проектирования объектов на основе априорной информации об отказах, дефектах и длительности восстановления повреждений однотипных объектов. Теперь требуется оценить оперативную надежность работы в течение прошедшего месяца, недели, суток и даже смены. Если количественную оценку надежности работы можно оценить на стадии проектирования, то опасность обслуживания всегда, в том числе и при проектировании, оценивается только на качественном уровне;

- рассчитывать необходимо количественную оценку именно опасности обслуживания, а не безопасности, так как безопасность или есть, или ее нет. Изменяется лишь опасность;

- количественная оценка экономичности и надежности работы, как и опасности обслуживания, необходима для оперативного сравнения и ранжирования объектов ЭЭС. В экономике этот анализ принято называть бенчмаркингом, когда сопоставляются многочисленные свойства объектов и на основе этого сопоставления осуществляется повышение эффективности их работы. Число сопоставляемых показателей исчисляется десятками. Результаты ранжирования здесь во многом субъективны, а риск принятия ошибочного решения велик;

- сравнение и ранжирование ОЭР объектов ЭЭС существенно упрощается при переходе к интегральному показателю. Но снижение риска ошибочного решения достигается лишь в том случае, если интегральный показатель характеризует техническое состояние объекта;

- применение интегрального показателя Харрингтона [5] получило широкое распространение во многих отраслях материального производства и в сфере услуг, что свидетельствует об актуальности интегрального оценивания. Однако интегральный показатель Харрингтона вычисляется как среднее геометрическое вероятностей реализаций множества показателей и потому он лишен физического смысла. В работе [6] сказано: «Методика расчета становится черным ящиком, который выдает числа, лишенные физического смысла».

Одним из возможных путей частичного преодоления трудностей решения данной проблемы силами персонала ЭЭС являются рекомендации, предложенные в работе [3], суть которых сводится к организации при отраслевых научно-исследовательских институтах энергетики центров по обеспечению ОЭР объектов ЭЭС. Центр осуществляет сбор и анализ статистических данных о техническом состоянии оборудования, отказах, ремонтах; выявление факторов, влияющих на ОЭР; разработку мероприятий по повышению ОЭР; организацию повышения квалификации персонала; проведение бенчмаркинга.

Практическая реализация этих рекомендаций, несомненно, имела бы положительные результаты. Но решить проблему с их помощью невозможно по двум причинам:

1) отсутствуют методы количественной оценки интегрального показателя ОЭР объектов;

2) отсутствуют критерии проверки гипотез о характере расхождения этих показателей.

2. Методические основы синтеза интегральных показателей ОЭР и бенчмаркинг СТ

Будем различать однотипные, сходные и уникальные объекты ЭЭС. К однотипным относятся объекты, характеризуемые одной и той же совокупностью разновидностей значимых признаков. Сходными будем считать объекты, характеризуемые одними и теми же выборками разновидностей значимых признаков из их совокупности. К уникальным относятся объекты, аналоги которых по заданным разновидностям признаков отсутствуют.

Примером однотипных объектов могут быть энергоблоки электростанций, их основное оборудование, устройства и установки; примером сходных объектов –выключатели распределительных устройств (линейные, шинные, блочные), а примером уникального объекта является единственный в ЭЭС паротурбинный энергоблок 500 МВт. Такая классификация объектов свидетельствует о том, что задачи бенчмаркинга, методы и алгоритмы их решения многочисленны. И эта особенность обусловливает одну из трудностей решения проблемы совершенствования управления ОЭР ЭЭС.

Однако у этих методов и алгоритмов есть следующие общие черты.

Обеспечение безошибочности информационной базы. Это одна из важнейших задач автоматизированной системы оперативного бенчмаркинга объектов. Информация о техническом состоянии объектов ЭЭС формируется по данным ежемесячных отчетов предприятий ЭЭС (например, форма 3-ТЕХ (энерго)), протоколов испытания и ремонтов, диспетчерских журналов. Естественно, эти данные существенно отличаются от перечня используемых в бенчмаркинге расчетных показателей, а преобразование исходных данных является одним из возможных источников ошибок. Рекомендуемые методы и алгоритмы обеспечения безошибочности исходных данных, как и безошибочности базы данных в целом, приведены в работе [7], а способы контроля безошибочности расчетных технико-экономических показателей (ТЭП) – в работе [8].

Требования к оценкам интегральных показателей. Наряду с безошибочностью исходных данных метод расчета должен обеспечивать объективность, физиче-

скую суть и доступность практического использования интегрального показателя. Одной из основных причин, искажающих оценку интегрального показателя по безошибочным исходным данным, является наличие взаимосвязанных ТЭП, т.е. некоторое конкретное свойство объекта может быть представлено несколькими взаимосвязанными показателями. При этом неоправданно увеличивается значимость (относительная величина, характеризующая техническое состояние) этого свойства, что приводит к искажению интегрального показателя и бенчмаркинга. Методы решения этой задачи разработаны для одномерных случайных величин и ряда ограничений, к которым относятся соответствие распределения случайных величин нормальному закону и немалое число реализаций.

Многомерный характер реализаций ТЭП отличает их от нормального закона распределения. Если для какого-либо ТЭП статистическая функция распределения и напоминает нормальный закон распределения, то на смежном временном интервале с большой вероятностью предположение о таком соответствии будет ошибочным. Даже при наличии однотипных объектов ЭЭС число ТЭП ограничено, а при классификации интегральных показателей составляет единицы. В работе [9] предлагается преодолевать эти трудности с помощью перехода от постоянных критических значений ТЭП к «локальным», вычисляемым имитационным моделированием возможных реализаций коэффициентов корреляции по фидуциальным распределениям ТЭП.

Обеспечение физической сути интегрального показателя. Очевидно, что рекомендации бенчмаркинга объектов ЭЭС должны быть объективны и, как правило, понятны специалисту. Несоответствие рекомендаций реальным возможностям не исключается, поскольку в этой сложной системе учесть все внешние факторы практически невозможно, например отсутствие резервных узлов, необходимых для ремонта объекта, в связи со случайной задержкой их поставки. Однако при надлежащей организации технического обслуживания и ремонта это может случаться, но не ежемесячно. Поскольку по сути необходимо сопоставить степень износа объектов, для СТ наиболее важными являются показатели, характеризующие их отдельные свойства.

Реально ТЭП изменяются от номинального до предельно допустимого значения. Предлагается этот интервал представить как интервал возможности объекта ЭЭС удовлетворять предъявляемым требованиям к техническому состоянию. В результате старения происходит уменьшение этих возможностей. Изменение может быть непрерывным или дискретным. Относительная часть использованных возможностей называется износом, а оставшаяся часть – остаточным ресурсом.

Величина износа изменяется в пределах [0;1], а остаточный ресурс – в пределах [1;0]. Переход к относительным значениям ТЭП называется нормированием. Преимуществом нормирования является преодоление трудностей различия размерности и масштабов ТЭП, что не допускает возможности их совместного рассмотрения. Как случайные величины оценки износа наиболее полно характеризуются статистическими параметрами. Методология преодоления трудностей совместного рассмотрения ТЭП приведена в [10].

Разновидности интегральных показателей оперативной эффективности работы. Переход от множества ТЭП к интегральным показателям упрощает бенчмаркинг, если можно ответить на следующие вопросы: как вычисляются интегральные показатели, как выбрать интегральные показатели из множества возможных и как сопоставлять эти показатели с учетом их случайного характера.

Известно, что число показателей, характеризующих средние значения реализаций ТЭП и их разброс, превышает 10. Если учесть комплексные показатели (подобные коэффициенту вариации), то общее их число может превышать число ТЭП. Следовательно, при отказе от сравнения совокупности возможных реализаций ТЭП и переходе к интегральным показателям возникает проблема выбора из совокупности возможных типов интегральных показателей, решаемая посредством анализа возможности практического использования и взаимосвязи интегральных показателей. Результаты проведенного анализа позволили установить, что техническое состояние объекта может быть представлено двумя интегральными показателями, которые характеризуют среднюю величину износа и степень разрегулировки технического состояния объекта, а также наиболее независимы. Это среднее арифметическое нормированных значений расчетных ТЭП и их коэффициент вариации.

Поскольку рекомендуемая методология бенчмаркинга основана на сравнении и ранжировании случайных величин износа, выводы и рекомендации по повышению ОЭР объектов не могут не учитывать эту особенность. Можно сравнивать по износу как однотипные объекты, например однотипные энергоблоки электростанций, так и совершенно различные, например паровые и гидравлические турбины. В обоих случаях сравнение связано с оценкой целесообразности классификации и вполне доступно, поскольку сопоставляются величины среднего износа. Трудности решения этой задачи связаны с многомерным характером показателей и большим риском ошибочного решения при применении математического алгоритма проверки гипотез о характере расхождения статистических параметров. Этот риск обусловлен недопустимостью применения к многомерным величинам критериев, предполагающих сравнение статистических параметров одномерных случайных величин. Преодоление этих трудностей достигается сопоставлением двух фидуциальных распределений, первое из которых отражает распределение совокупности нормированных реализаций ТЭП, а второе – выборки реализаций ТЭП по заданному сочетанию разновидностей признаков. При этом предлагается считать, что если статистические функции распределения различаются случайно, то случайно различаются и их параметры распределений.

Наукоемкость, громоздкость и трудоемкость, большой риск ошибочного решения при ручном счете обусловливают необходимость перехода к автоматизированным системам синтеза интегральных ОЭР и бенчмаркинга эксплуатационных задач технического обслуживания и ремонта. Следует заметить, что перечисленные трудности и способы их преодоления относятся к категории явных. «Неявные» трудности проявляются при внедрении автоматизированной системы и обусловлены многочисленными внешними факторами, специфичными для каждой ЭЭС.

Рассмотрим особенности методологии анализа безошибочности ТЭП, оценки интегрального показателя ОЭР (синтеза ТЭП), бенчмаркинга системы технического обслуживания и ремонта, а также учет случайного характера интегральных показателей на примере ряда ТЭП парогазовой установки ПГУ-400.

3. Особенности методологии анализа, синтеза и сравнения ТЭП ПГУ-400.

В табл. 1 приведены некоторые среднемесячные показатели ТЭП, характеризующие ОЭР ПГУ-400 в анализируемом месяце t_j и предшествовавшем ему t_{j-1}. Как следует из табл. 1, отчетные показатели не всегда удобны для сравнения ОЭР ПГУ, например, не отвечают на вопрос о причинах резкого снижения суммарной выработки электроэнергии (ЭЭ) или резкого снижения расхода ЭЭ в системе собственных нужд (СН). Показатели расхода природного газа $B_г$, расход условного топлива $B_т$ и удельный расход условного топлива $b_т$ достаточно полно характеризуют экономическую эффективность, но не учитывают, что $b_т \cdot \eta_б = \text{const}$, т.е. ТЭП КПД (брутто) $\eta_б$ столь же объективно характеризует экономическую эффективность ПГУ, как и ТЭП $b_т$.

Для того, чтобы учесть это несоответствие, предлагается несколько видоизменить перечень анализируемых ТЭП, а именно:

1) ТЭП $Э_Σ$ и $Э_{ш.}$ заменить на ТЭП коэффициент использования номинальной производительности $К_п = Э_Σ / Р_н \cdot t_j$;

2) ТЭП $Э_{СН}$ представить в относительных единицах (%): $\varepsilon Э_{СН} = 100 Э_{СН} / Э_Σ$;

3) вместо ТЭП $Р_{ср}$ ввести ТЭП коэффициент использования установленной мощности $K_p = 100 Р_{ср} / Р_н$;

4) ввести ТЭП коэффициент технического использования $K_т = 100 Э_Σ / Р_{ср} \cdot t_j$.

Показатели $K_п$, $\varepsilon Э_{СН}$, $K_р$ и $K_т$ условимся называть расчетными.

Результаты автоматизированного преобразования отчетных ТЭП ПГУ-400 в расчетные ТЭП приведены в табл. 2. Нетрудно заметить, что преобразование ТЭП сводится к вводу показателей $K_п$, $K_р$ и $K_т$, хорошо известных в теории надежности. Более того, поскольку $K_п = K_р \cdot K_т$, это соотношение может быть использовано для контроля безошибочности их расчета.

Табл. 1. Реализации среднемесячных ТЭП ПГУ-400

№	ТЭП	Условное обозначение	Единицы измерения	ОЭР для месяцев	
				t_j	t_{j-1}
1	Выработка ЭЭ (всего)	$Э_Σ$	кВтч·10³	241322,8	89617,9
2	Отпуск ЭЭ с шин	$Э_ш$	кВтч·10³	235541,2	86858,1
3	Расход ЭЭ в системе СН	$Э_{СН}$	кВтч·10³	5781,6	2759,8
4	Расход природного газа	$B_г$	т·м³	45310,9	17077,5
5	Расход условного топлива	$B_т$	т.у.т	51783,8	19517,1
6	Удельный расход условного топлива	$b_т$	г/кВтч	219,85	224,7
7	Средняя мощность	$P_{ср}$	мВт	342,7	322,7
8	КПД брутто	$\eta_б$	%	55,9	51,68
9	Температура питательной воды	$T_п$	°С	150,5	151,8
10	Температура уходящих газов	$T_{у.г}$	°С	113,2	113,4
11	Вакуум	$K_у$	%	95,8	95,7

Табл. 2. Реализации рекомендуемых среднемесячных ТЭП ПГУ-400 по месяцам

№	ТЭП	Условное обозначение	Единицы измерения	t_j	t_{j-1}
1	Коэффициент использования номинальной производительности.	$K_п$	о.е.	0,84	0,30
2	Расход ЭЭ в системе СН	$\varepsilon Э_{сн}$	%	2,39	3,08
3	Коэффициент использования установленной мощности	$K_р$	о.е.	0,86	0,81
4	Коэффициент технического использования	$K_т$	о.е.	0,98	0,37
5	КПД брутто	$\eta_б$	%	55,9	54,7
6	Температура питательной воды	$T_п$	°С	150,5	151,8
7	Температура уходящих газов	$T_{у.г}$	°С	113,2	113,4
8	Вакуум	$K_у$	%	95,8	95,7

Табл. 3. Интервал изменения реализаций ТЭП ПГУ-400

№	ТЭП		Интервал изменения реализации ТЭП по годам				За четыре года
	Условное обозначение	Единицы измерения	1	2	3	4	
1	$K_{п}$	о.е.	0,232 0,699	0,179 0,747	0,450 0,787	0,210 0,875	0,179 0,875
2	$\varepsilon Э_{сн}$	%	2,60 3,23	2,40 3,15	2,31 3,71	2,32 4,68	2,31 4,68
3	$K_{р}$	о.е.	0,58 0,73	0,59 0,78	0,48 0,79	0,39 0,88	0,39 0,88
4	$K_{т}$	о.е.	0,37 1,0	0,27 1,0	0,60 1,0	0,37 1,0	0,27 1,0
5	$\eta_{б}$	%	50,8 54,3	50,0 54,6	47,0 54,3	42,7 56,8	47,0 56,8
6	$Т_{п}$	°С	152,0 155,1	153,2 158,4	156,2 158,9	149,7 158,2	149,7 158,9
7	$T_{у.г}$	°С	113,3 119,7	112,9 121,7	112,5 123,2	113,1 124,8	112,5 124,8
8	K_{v}	%	87,5 96,8	87,3 96,4	85,7 93,5	85,7 96,3	85,7 96,8

Примечание: над чертой – минимальные значения, под чертой – максимальные

Очередным этапом анализа (при вводе автоматизированной системы в работу) является определение интервала изменения возможных реализаций ТЭП. Для уникальных объектов эти интервалы устанавливаются и корректируются по среднемесячным реализациям ТЭП за несколько лет наблюдения. При этом необходимо учесть, что продолжительность интервала со временем возрастает (при неизменном числе реализаций) от исходного до предельно допустимого значения, так как реализации ТЭП изменяются от номинального до предельно допустимого значения.

В табл. 3 приведены результаты расчетов ТЭП за каждые четыре последних года и расчетный показатель за четыре года. При анализе этих данных следует учитывать направленность изменения ТЭП. Под направленностью изменения будем понимать направление изменения ТЭП при увеличении срока службы и износа объекта. Например, с увеличением износа ПГУ ТЭС величина $K_{п}$ уменьшается, а величина $\varepsilon Э_{СН}$ возрастает.

Граничные значения интервалов изменения ТЭП являются не только основой интервального метода контроля безошибочности ТЭП, но и необходимым условием перехода от фактических значений ТЭП к нормированным значениям. Для произвольного ТЭП ($П_i$, i=1, m_p) нормативные значения обозначим $Iz(П_i)$. Способов нормирования ТЭП объектов ЭЭ немало. В работе [9] предлагается проводить нормирование, в результате которого нормированная оценка ТЭП будет отражать техническое состояние ПГУ, т.е. величину износа Iz.

Рассмотрим последовательность расчетов нормированных значений ТЭП для коэффициента использования номинальной производительности $K_{п}$, который с увеличением срока службы ПГУ уменьшается. В соответствии с табл. 2 в j-м месяце $K_{п}(t_j) = 0,84$. По данным табл. 3 определяем интервал возможных реализаций: $\Delta K_{п} = (K_{п,max} - K_{п,min}) = 0,696$. Нормированное значение $K_{п}$ вычисляется по формуле

$$Iz[K_{п}(t_j)] = [K_{п,max} - K_{п,min}(t_j)]/\Delta K_{п} = 0,05.$$

Таким образом, величина износа не превышает 5%.

Теперь рассмотрим последовательность расчета нормированного значения ТЭП $\varepsilon Э_{СН}$, который с увеличением срока службы ПГУ возрастает. В соответствии с табл. 2 $\varepsilon Э_{СН}$ в j-м месяце составляет $\varepsilon Э_{СН}(t_j) = 2,39\%$. По данным табл. 3 определяем интервал возможных реализаций: $\Delta(\varepsilon Э_{СН}) = 2,37\%$. Нормированное значение $\varepsilon Э_{СН}$ вычисляем по формуле

$$Iz[\varepsilon Э_{СН}(t_j)] = [\varepsilon Э_{СН,max} - \varepsilon Э_{СН,min}(t_j)]/\Delta(\varepsilon Э_{СН}) = 0,034.$$

Результаты аналогичных расчетов приведены в табл. 4, где также приведены интегральные показатели $M^*(Iz)$ и $K_v(Iz)$, характеризующие техническое состояние ПГУ-400 за j-й и (j-1)-й месяцы по данным табл. 2 и 3.

Табл. 4. Результаты расчета нормированных значений ТЭП для двух месяцев

№	ТЭП	t_j	t_{j-1}
1	$Iz\ (K_{п})$	0,050	0,826
2	$Iz\ (\varepsilon Э_{сн})$	0,034	0,629
3	$Iz\ (K_{р})$	0,036	0,127
4	$Iz\ (K_{т})$	0,027	0,863
5	$Iz\ (\eta_{б})$	0,092	0,214
6	$Iz\ (T_{п})$	0,087	0,228
7	$Iz\ (T_{у.г})$	0,057	0,073
8	$Iz\ (V)$	0,090	0,099
$M^*(Iz)$		0,079	0,313
$K^*_v(Iz)$		0,42	1,093

Сравнение количественных оценок ТЭП ПГУ-400 в j-м и предшествовавшем ему (j-1)-м месяце позволяет сделать следующее заключение:

- шесть ТЭП – $K_{п}$, $\varepsilon Э_{Сн}$, $K_{р}$, $K_{т}$, $\eta_{б}$, $T_{р}$ – в результате среднего ремонта ПГУ-400 в (j-1)-м месяце существенно улучшили свои количественные оценки в j-м месяце;

- два ТЭП – $T_{у.г}$ и K_{ν} – практически не изменились.

Интегральные ТЭП $M^{*}(Iz)$ и $K^{*}_{\nu}(Iz)$ также свидетельствуют о существенном улучшении технического состояния ПГУ-400 после ремонта.

Поскольку учтены не все ТЭП, а ПГУ-400 не представлено совокупностью основного оборудования, устройств, установок и их узлов, кажущаяся простота синтеза и бенчмаркинга ТЭП ПГУ-400 обманчива. Есть не всегда учитываемая при расчетах особенность. Поскольку нормированные значения ТЭП, как и фактические их значения, являются случайными величинами, а число реализаций ТЭП по заданным разновидностям признаков может оказаться достаточно малым, наблюдаемое расхождение интегральных показателей может быть случайным, а риск принятия ошибочного решения – велик.

В качестве примера решения этой задачи можно рассмотреть характер расхождения интегральных показателей в j-м и (j-1)-м месяцах. Однако, учитывая, что бенчмаркинг многомерен (множество вариантов сравнения), сравнение в рамках теории проверки статистических гипотез одномерных случайных величин связано с большим риском ошибочного решения, оценка критических значений интегральных показателей на основе имитационного моделирования специфична, сравнение случайных реализаций интегральных показателей в виду большой трудоемкости, громоздкости и наукоемкости должно осуществляться автоматически.

Выводы

1. Если замена СТ современными объектами в настоящее время невозможна, а средств на полную ее модернизацию недостаточно (и в то же время возникновение системных аварий, обусловленных СТ, недопустимо), целесообразно проведение частичной модернизации, устраняющей выявленные дефекты, с обязательным оперативным контролем технического состояния СТ и уточнением предельно допустимых значений нагрузки.

2. Центры обеспечения оперативной эффективности работы при отраслевых научно-исследовательских институтах энергетики осуществляют сбор и формализацию данных о техническом состоянии СТ, автоматизированный анализ и синтез этих данных, бенчмаркинг, подготовку оперативных рекомендаций по повышению эффективности работы, разработку соответствующих методических указаний, повышение квалификации персонала СТ в режиме on-line.

3. Разработка автоматизированных систем контроля технического состояния СТ с учетом специфических внешних факторов и повышение объективности рекомендаций по эффективности его работы требует согласования формы выходных документов с руководством.

4. Некоторые особенности формализации данных о техническом состоянии СТ, обеспечение безошибочности исходных данных, выполнение нормирования ТЭП, оценка интегральных показателей и некоторые результаты бенчмаркинга свидетельствуют о возможности объективной оценки оперативной эффективности СТ и снижении риска возникновения недопустимых последствий.

Библиографический список

1. Дьяков А.Ф., Исамухаммедов Я.Ш., Молодюк Б.Д. Проблемы и пути повышения надежности ЕЭС России // Методические вопросы исследования надежности больших систем энергетики. Вып.64. Надежность систем энергетики: достижения, проблемы, перспективы / Отв. ред. Н.И. Воропай. ИСЭМ СО РАН., М.: 2014. С. 8-16.

2. Аминов Р.З., Шкрет А.Ф., Гариевский М.В. Расчет эквивалентной выработки ресурса энергоблоков ТЭС // Электрические станции. 2014. № 8. С. 16-18.

3. Резинский В.Ф. Еще раз о резерве энергооборудования // Надежность и безопасность энергетики. 2009. № 4. С. 9-13.

4. СТО 70238424.27.040.007-2009. Паротурбинные установки. Организация эксплуатации и технического обслуживания. Нормы и требования. М.: ОРГРЭС, 2010. 165 с.

5. Зазнобина Н.И. Оценка экологической обстановки в крупном промышленном центре с помощью обобщенной функции желательности Харрингтона // Вестник Нижегородского университета. 2007. № 2. С. 115-118.

6. Лосева П. Против часовой стрелки. Что такое старение и как с ним бороться. М.: «Альпина нон-фикиш», 2020. 500 с.

7. Фархадзаде Э.М., Мурадалиев А.З., Фарзалиев Ю.З. и др. Система управления безопасностью и безошибочностью базы данных // Энергетик, 2008. № 3. С. 33-35.

8. Фархадзаде Э.М., Фарзалиев Ю.З., Мурадалиев А.З. Оценка качества восстановления износа энергоблоков ТЭС // Энергетика. 2016. № 1. С. 14-24.

9. Фархадзаде Э.М., Мурадалиев А.З., Фарзалиев Ю.З. и др. Оценка взаимосвязи технико-экономических показателей объектов ЭЭС // Электрон. моделирование. 2017. № 6. С. 93-106.

10. Фархадзаде Э.М., Фарзалиев Ю.З., Мурадалиев А.З. Метод и алгоритм ранжирования котельных установок блочных электростанций по критерию надежности и экономичности работы // Теплоэнергетика. 2015. № 10. С. 22-29.

References

1. Diakov A.F., Isamukhammedov Ya.Sh., Molodyuk B.D. [Problems and ways to improve the dependability of Russia's UES]. In: Voropay N.I., editor. [Methods of researching the dependability of large power systems. Issue 64. Dependability of power systems: achievements, problems, prospects]. ESI SB RAS; Moscow: 2014. Pp. 8-16. (in Russ.)

2. Aminov R.Z., Shkret A.F., Garievsky M.V. Calculation of service life equivalent of thermal power plant units. *Electrical stations* 2014;8:16-18. (in Russ.)

3. Rezinsky V.F. [Once again on the redundancy of power equipment]. *Safety and Reliability of Power Industry* 2009;4:9-13. (in Russ.)

4. [STO 70238424.27.040.007-2009. Steam turbine installations. Organisation of operation and maintenance. Norms and requirements]. Moscow: ORGRES; 2010. (in Russ.)

5. Zaznobina N.I. Assessing environmental situation in a large industrial center from anthropogenic load intensity by means of the generalized desirability function (Case study: Nizhni Novgorod). *Vestnik Nizhegorodskogo universiteta* 2007;2:115-118. (in Russ.)

6. Loseva P. [Counterclockwise. What is aging and how to deal with it]. Moscow: Alpina non-fiction; 2020. (in Russ.)

7. Farhadzadeh E.M., Muradaliyev A.Z., Farzaliyev Yu.Z. et al. [A system for managing the safety and faultlessness of a database]. *Energetik* 2008;3:33-35. (in Russ.)

8. Farhadzadeh E.M., Muradaliyev A.Z., Farzaliyev Yu.Z. Quality evaluation of the TPP power generating units wear reconditioning. *Energetika. Proceedings of CIS higher education institutions and power engineering associations* 2016;59(1):14-24. (in Russ.)

9. Farhadzadeh E.M., Muradaliyev A.Z., Farzaliyev Y.Z. et al. Assessment of interrelation of technical and economic indicators of EES objects. *Electronic Modeling* 2017;6:93-106. (in Russ.)

10. Farhadzadeh E.M., Farzaliyev Yu.Z., Muradaliyev A.Z. [Method and algorithm of ranking boiler plants of block-unit power stations in terms of their dependability and cost effectiveness of operation]. *Teploenergetika* 2015;10:22-29. (in Russ.)

Сведения об авторах

Фархадзаде Эльмар Мехтиевич, **д.т.н., профессор**. В 1961 году окончил энергетический факультет Азербайджанского института нефти и химии (АзИНЕФТЕХИМ) г. Баку. В 1982 году защитил докторскую диссертацию по теме «Точность и достоверность характеристик надежности электроустановок» в Новосибирском электротехническом институте (НЭТИ). Главный научный сотрудник АзНИПИИ Энергетики г. Баку. Область научных исследований – надежность и эффективность электроэнергетических систем.

E-mail: elmeht@rambler.ru. Адрес: AZ1012, г. Баку, пр. Г. Зардаби, 94.

Мурадалиев Айдын Зураб оглу, **д.т.н., доцент**. В 1982 году окончил энергетический факультет Азербайджанского института нефти и химии (АзИНЕФТЕХИМ) г. Баку. В 2013 году защитил докторскую диссертацию по теме «Разработка методов и алгоритмов расчета показателей индивидуальной надежности оборудования и устройств ЭЭС». Ведущий научный сотрудник отдела «Надежность оборудования энергосистемы» АзНИПИИ Энергетики г. Баку. Область научных исследований – количественная оценка индивидуальной надежности оборудования и устройств электроэнергетических систем.

E-mail: aydin_murad@yahoo.com. Адрес: AZ1012, г. Баку, пр. Г. Зардаби, 94.

Ашурова Ульвия Комиссар кызы, аспирантка Азербайджанского научно-исследовательского и проектно-изыскательского института энергетики (г. Баку). В 1998 г. окончила Азербайджанскую государственную нефтяную академию. Область научных исследований – количественная оценка индивидуальной надежности оборудования и устройств электроэнергетических систем.

About the authors

Elmar M. Farhadzadeh, Doctor of Engineering, Professor. In 1961, he graduated from the Energy Faculty of the Azerbaijan Institute of Oil and Chemistry (AzINEFTEKHIM) in Baku. In 1982, he defended his doctoral dissertation on the 'Accuracy and reliability characteristics of electrical installations' in the Novosibirsk Electrotechnical Institute (NETI). Chief scientific officer of AzNIPII Energetics in Baku. His field of research is dependability and efficiency of electrical power systems.

E-mail: elmeht@rambler.ru. Address: 94 G. Zardabi Ave., AZ1012, Baku.

Aydin Z. Muradaliyev, Doctor of Engineering, Associate Professor. In 1982, he graduated from the Energy Faculty of the Azerbaijan Institute of Oil and Chemistry (AzINEFTEKHIM) in Baku. In 2013, he defended his doctoral thesis titled 'Development of methods and algorithms for calculating the indicators of individual reliability of equipment and devices of EES'. Lead researcher, Reliability of Power System Equipment, AzNIPII Energetics, Baku. His field of research is quantitative estimation of individual dependability of equipment and devices of electrical power systems.

E-mail: aydin_murad@yahoo.com. Address: 94 G. Zardabi Ave., AZ1012, Baku.

Ulviya K. Ashurova, Postgraduate Student, Azerbaijan Scientific-Research and Design-Prospecting Institute of Energetic (Baku). In 1998, she graduated from the Azerbaijan State Oil and Industrial University. Her field of research is quantitative estimation of individual dependability of equipment and devices of electrical power systems.

Вклад авторов в статью

Фархадзаде Э.М. – обоснование актуальности исследования, Постановка цели решаемой задачи и разработка методики исследования.

Мурадалиев А.З. – Анализ источников информации, Разработка алгоритмов и программного обеспечения решаемой задачи. Обсуждение промежуточных результатов. Подготовка материалов к публикации.

Ашурова У.К. – Анализ источников информации. Проведение расчетов и обсуждение промежуточных результатов. Оформление целостности статьи.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Надежность, том 25, №2, 2025 / Dependability 2, 2025
Системный анализ в задачах надежности и безопасности
УДК 519.248:62-192
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-19-24

Эффективная оценка средней наработки до отказа для плана испытаний с ограниченным временем и восстановлением

Efficient Estimation of Mean Time to Failure for a Time-Limited Test Plan with Recoverability

Михайлов В.С.[1*]
Mikhailov V.S.[1*]

[1] *Федеральное государственное унитарное предприятие «Центральный научно-исследовательский институт химии и механики им. Д.И. Менделеева», Российская Федерация, Москва*
[1] *Federal State Unitary Enterprise Central Scientific Research Institute of Chemistry and Mechanics, Russian Federation, Moscow*

mvs1956@list.ru

Михайлов В.С.

Резюме. *В качестве показателя, характеризующего такое свойство надежности сложного восстанавливаемого изделия, как безотказность, выбирают в соответствии со средней наработкой до отказа (далее – t). С организационной и экономической точек зрения наиболее подходящим для испытаний восстанавливаемых (заменяемых) изделий при условии подчинения наработки до отказа экспоненциальному закону распределения вероятностей является план NBτ, где N – число испытуемых однотипных изделий; τ – наработка (одинаковая для каждого изделия); B – характеристика плана, означающая, что работоспособность изделия после каждого отказа в течение срока испытаний восстанавливается. Традиционно в качестве оценки средней наработки до отказа (СНДО) выбирается оценка $t_1 = N\tau/R$, где $R > 0$ – количество наблюдаемых отказов, которые произошли в течение времени τ. Эта оценка является смещенной и, кроме того, если за время испытаний наблюдается небольшое число отказов (порядка нескольких единиц) или не наблюдается, то эта оценка может дать значительную ошибку из-за смещения. За последнее время появились оценки СНДО лишенные указанных недостатков. Однако эти полученные оценки не являются абсолютно эффективными.* **Цель работы.** *Целью работы является построение более эффективной оценки СНДО для плана испытаний с ограниченным временем и восстановлением.* **Методы**. *При сравнении оценок СНДО на эффективность используется простой критерий эффективности смещённых оценок.* **Выводы**. *1. Получена эффективная и сбалансированная оценка СНДО. Поиск осуществлялся в классе линейных оценок в соответствии с простым критерием эффективности смещенных оценок для плана с ограниченным временем испытаний и восстановлением отказавших изделий. Полученная оценка СНДО имеет направленность практического применения при испытаниях и эксплуатации однородной продукции различного назначения, в процессе которых отказы не возникали; 2. Из оценок с одинаковой эффективностью следует выбирать оценку с минимальным смещением, а затем попытаться отбалансировать её. 3. Оценке, определенной в классе оценок $\theta = (N\tau/(R+1)) + N\tau f(R)$ с минимальным смещением, начиная с некоторой величины смещения вплоть до нуля, всегда соответствует большая дисперсия. Аналогично, оценке из этого класса с большим смещением всегда соответствует меньшая дисперсия, что не соответствует принципу минимизации функционала на смещенной оценке с уменьшением смещения при поиске эффективных смещенных оценок. Сказанное позволяет сделать более широкий вывод, что использовать дисперсию в качестве характеристики критерия эффективности смещенных оценок в принципе не имеет смысла.*

Abstract. *As an indicator characterizing such a property of reliability of a complex restored product as failure-free operation, the mean time to failure (hereinafter – t) is selected in accordance with. From the organizational and economic points of view, the most suitable for testing restored (replaceable) products, provided that the mean time to failure is subject to the exponential probability distribution law, is the NBτ plan, where N is the number of similar products being tested; τ is the operating time (the same for each product); B is the plan characteristic, meaning that the operability of the product is restored after each failure during the testing period. Traditionally, as an estimate of the mean time to failure (MTTF), the estimate $t1 = N\tau/R$ is chosen, where $R > 0$ is the number of observed failures that occurred during the time τ. This estimate is biased and, in addition, if a small number of failures (of the order of*

several units) are observed during the testing period or are not observed, then this estimate can give a significant error due to the bias. Recently, estimates of the SNDO free from the above-mentioned shortcomings have appeared. However, these estimates are not absolutely efficient. Purpose of the work. The purpose of the work is to construct a more efficient estimate of the SNDO for a time-limited test plan with recovery. Methods. A simple efficiency criterion of biased estimates is used to compare SNDO estimates for efficiency. Conclusions. 1. An efficient and balanced estimate of the SNDO has been obtained. The search was carried out in the class of linear estimates in accordance with a simple efficiency criterion of biased estimates for a plan with a time-limited test and recovery of failed products. The obtained SNDO estimate is aimed at practical application in testing and operating homogeneous products for various purposes, during which failures did not occur; 2. Of the estimates with the same efficiency, one should select the estimate with the minimum bias, and then try to balance it. 3. An estimate defined in the class of estimates $\theta = (N\tau/(R+1)) + N\tau f(R)$ *with a minimum bias, starting from a certain bias value down to zero, always corresponds to a large variance. Similarly, an estimate from this class with a large bias always corresponds to a smaller variance, which does not correspond to the principle of minimizing the functional on a biased estimate with a decrease in bias when searching for efficient biased estimates. This allows us to draw a broader conclusion that using variance as a characteristic of the efficiency criterion of biased estimates does not make sense in principle.*

Ключевые слова: *оценка, эффективная оценка, критерий эффективности, план испытаний, смещенные оценки.*
Keywords: *evaluation, effective evaluation, efficiency criterion, test plan, biased estimates.*

Для цитирования: *Михайлов В.С. Эффективная оценка средней наработки до отказа для плана испытаний с ограниченным временем и восстановлением // Надежность. 2025. №2. С. 19-24. https://doi.org/10.21683/1729-2646-2025-25-2-19-24*
For citation: *Viktor S. Mikhailov. Efficient Estimation of Mean Time to Failure for a Time-Limited Test Plan with Recoverability. Dependability 2025;2: 19-24. https://doi.org/10.21683/1729-2646-2025-25-2-19-24*

Поступила: *17.12.2024* / **После доработки:** *14.05.2025* / **К печати:** *09.06.2025*
Received on: *17.12.2024* / **Revised on:** *14.05.2025* / **Print in:** *09.06.2025*

Введение

В качестве показателя, характеризующего такое свойство надежности сложного восстанавливаемого изделия, как безотказность, выбирают в соответствии с [1] среднюю наработку до отказа (далее – *t)*. С организационной и экономической точек зрения наиболее подходящим для испытаний восстанавливаемых (заменяемых) изделий при условии подчинения наработки до отказа экспоненциальному закону распределения вероятностей является план типа $NB\tau$, где N – число испытуемых однотипных изделий; τ – наработка (одинаковая для каждого изделия); B – характеристика плана, означающая, что работоспособность изделия после каждого отказа в течение срока испытаний восстанавливается (мгновенно) [2]. Традиционно в качестве оценки средней наработки до отказа (СНДО) выбирается оценка $t_1 = N\tau/R$, где $R > 0$ – количество наблюдаемых отказов, которые произошли в течение времени τ. Эта оценка является смещенной [2] и, кроме того, если за время испытаний наблюдается небольшое число отказов (порядка нескольких единиц) или не наблюдается, то эта оценка может дать значительную ошибку из-за смещения. За последнее время появились оценки СНДО лишенные указанных недостатков [3, 4]. Однако эти полученные оценки не являются абсолютно эффективными.

Цель работы. Целью работы является построение более эффективной оценки СНДО для плана испытаний с ограниченным временем и восстановлением.

Методы. При сравнении оценок СНДО на эффективность используется простой критерий эффективности смещённых оценок [3, 4].

Понятия балансировки и абсолютного суммарного смещения [3, 4]**.** Под суммарным смещением B понимается суммирование смещений по всем возможным величинам параметра $t \in T$,

$$B\left(\theta\left(R;N,\tau\right)\right) = \int\limits_{t\in T} \left\{E\theta\left(R;N,\tau\right) - t\right\} dt = \int\limits_{t\in T} bdt.$$

где T – множество всех возможных величин параметра t.

Сформулируем понятие балансировки для оценки параметра t, а именно:

$$A\left(\theta\left(R;N,\tau\right)\right) = /B(\theta\left(R;N,\tau\right))/ =$$

$$= /\int\limits_{t\in T} \left\{E\theta\left(R;N,\tau\right) - t\right\} dt/ = /\int\limits_{t\in T} bdt/,$$

где /*/ – абсолютная величина, суммирование смещений ведется по всем возможным величинам оцениваемого параметра, которые принадлежат некоторому числовому множеству $t \in T$. Балансировка характеризует сбалансированность разностей реализаций оценки θ от оцениваe-

мого параметра t в целом по всевозможным величинам, которые может принимать этот параметр t.

Обозначим суммарное смещение одного знака через: $K_{>0} = \int\limits_{\{\}>0} \{E\theta(R;N,\tau) - t\}dt = \int\limits_{b(t)>0} bdt = B_{>0}$ – положительное суммарное смещение, где суммирование ведется по тем величинам параметра t, для которых выполняется условие $E(\theta) - t>0$;

$K_{<0} = /\int\limits_{\{\}<0} \{E\theta(R;N,\tau) - t\}dt/ = /\int\limits_{b(t)<0} bdt/ = -B_{<0} = /B_{<0}/$ – отрицательное суммарное смещение, взятое по абсолютной величине, где суммирование ведется по тем величинам параметра t, для которых выполняется условие $E(\theta) - t<0$;

$W = \int\limits_{t\in T} /E\theta(R;N,\tau) - t/dt = \int\limits_{t\in T} /b/dt$ – абсолютное суммарное смещение (разброс и точность оценки θ относительно параметра t), где суммирование смещений, взятых по абсолютной величине, ведется по всем возможным величинам оцениваемого параметра, которые принадлежат некоторому числовому множеству $t \in T$.

Тогда $A(\theta) = /K_{>0} - K_{<0}/$. Заметим, что для оценки θ балансировка, равная нулю $A = 0$ (или сбалансированность оценки θ), не означает симметрию распределения вероятностей реализаций оценки $\theta(R)$.

Т.к. величины $K_{>0} \geq 0$ и $K_{<0} \geq 0$, то для сбалансированной оценки $A = 0$ выполняется соотношение $K_{>0} = K_{<0}$.

Абсолютное суммарное смещение можно выразить через элементы разности балансировки ($K_{>0}$; $K_{<0}$) следующим образом $W = K_{>0} + K_{<0}$.

Формулировка простого критерия эффективности смещенных оценок. Выразим через характеристики A и W простой критерий эффективности смещенных оценок как некоторую характеристику $Q = (A+1) \cdot W$, минимизация которой на предложенных оценках определяет эффективную смещенную оценку [3, 4]. Компоненты построенного критерия легко вычислить через компоненты балансировки $K_{>0}$, $K_{<0}$, а именно: $Q = (/K_{>0} - K_{<0}/ + 1) \cdot (K_{>0} + K_{<0})$.

Получение эффективной смещенной оценки СНДО по результатам испытаний, проводимых в соответствии с планом испытаний типа NBτ, с использованием простого критерия эффективности смещенных оценок

Заметим, что в классе всех возможных смещенных оценок параметра t (СНДО) экспоненциального закона распределения (впрочем, как и для любого закона распределения) эффективной оценки не существует [5]! Поэтому с целью получения эффективной смещенной оценки СНДО сужают поисковый класс оценок до линейного для параметров плана испытаний N и τ (далее – линейные оценки), а именно:

$(1/t) \cdot \theta(R; N,\tau) = \theta(R;m/t)$, *где* $t > 0$ – параметр экспоненциального закона распределения наработки до отказа [3, 4].

До настоящего момента наиболее эффективной среди предложенных оценок СНДО для плана испытаний типа NBτ является смещенная и сбалансированная оценка $T_d(R = 0) = 2{,}4N\tau$, $T_d(R = 1) = 0{,}35N\tau$, $T_d(R = 2) = 0{,}3N\tau$, $T_d(R > 2) = N\tau / (R + 1)$, $A = 0$. При выборе оценки T_d в качестве эффективной кроме строгой монотонности учитывалась ее простота.

Найдем более эффективную и сбалансированную оценку параметра t для плана испытаний $NB\tau$. Для этого рассмотрим класс линейных оценок, представленных в виде $\theta = (N\tau/(R+1)) + N\tau f(R)$, тогда балансировка $A(\theta)$ для плана испытаний NBτ после подстановки оценок класса $\theta = (N\tau/(R+1)) + N\tau f(R)$ имеет вид ($\Delta = N\tau/t$ – параметр пуассоновского распределения):

$$A(\theta) = /\int_0^\infty \tfrac{1}{t}\{E\theta - t\}d\Delta/ =$$

$$= /\int_0^\infty (e^{-\Delta}\sum_{r=0}^{\infty}\frac{\Delta^{r+1}}{(r+1)!} + e^{-\Delta}\sum_{r=0}^{\infty} f(r)\frac{\Delta^{r+1}}{r!} - 1)\partial\Delta/.$$

Аналогично и для абсолютного суммарного смещения, а именно:

$$W(\theta) = \int_0^\infty \tfrac{1}{t}/E\theta - t/d\Delta =$$

$$= \int_0^\infty /e^{-\Delta}\sum_{r=0}^{\infty}\frac{\Delta^{r+1}}{(r+1)!} + e^{-\Delta}\sum_{r=0}^{\infty} f(r)\frac{\Delta^{r+1}}{r!} - 1/\partial\Delta.$$

Заметим, что первая часть суммы под интегралом для $A(\theta)$ или $W(\theta)$ равна $e^{-\Delta}\sum_{r=0}^{\infty}\frac{\Delta^{r+1}}{(r+1)!} = e^{-\Delta}(e^{\Delta} - 1) = 1 - e^{-\Delta}$. Из вида функционалов $A(\theta)$ и $W(\theta)$ следует, что для нахождения более эффективной и сбалансированной оценки $A(\theta)=0$, чем оценка T_d, необходимо действовать по схеме аналогичной в [3, 4] и рассматривать большое количество членов $f(r)$ суммы под интегралом. В такой постановке решение задачи, нахождения эффективной оценки, становится весьма затруднительным. В такой ситуации единственным способом нахождения эффективной оценки является прямое вычисление на электронной вычислительной машине. Решение получается методом спуска варьированием величинами коэффициентов линейных оценок, представленных в виде $\theta = (N\tau/(R+1)) + N\tau f(R)$.

Балансировка для плана испытаний типа NBτ на линейных оценках имеет вид $A(\theta(m,R)) = /\int_0^\infty \{E\theta(\Delta,R) - 1\}d\Delta/$, где $\Delta = m/t$, $m = N\tau$ – параметр пуассоновского потока отказов [3, 4]. Аналогично абсолютное суммарное смещение представимо в виде $W(\theta(m,R)) = \int_0^\infty /E\theta(\Delta,R) - 1/d\Delta$.

Эффективная оценка СНДО θ ищется в классе линейных оценок в соответствии с простым критерием эффективности смещенных оценок [3, 4], а именно:

$$Q = (A+1) \cdot W = (/K_{>0} - K_{<0}/ + 1) \cdot (K_{>0} + K_{<0}),$$

$$\text{где } K_{\{\}>0} = \int\limits_{\{\}>0} \left\{E\theta(\Delta, R) - 1\right\} d\Delta,$$

$$K_{\{\}<0} = / \int\limits_{\{\}<0} \left\{E\theta(\Delta, R) - 1\right\} d\Delta /.$$

На полученную оценку θ накладывается условие строгой монотонности по всем своим параметрам (N, τ, R). Кроме того, полученная эффективная оценка должна быть сбалансированной $A(\theta)=0$. Результаты расчетов приведены в табл. 1.

Из табл. 1 следует, что в соответствии с простым критерием эффективности смещенных оценок наиболее эффективной оказалась оценка θ. Остальные сбалансированные оценки приведены для сравнения [3, 4]. Результаты представлены с точностью до трёх знаков.

Проведем рассуждения о выборе эффективной оценки, основанные на выбранном классе оценок $\theta = (N\tau/(R+1)) + N\tau f(R)$. При получении двух оценок с одинаковой эффективностью следует выбирать оценку с минимальным смещением, а затем попытаться отбалансировать её. С уменьшением смещения оценок вплоть до нуля, начиная с некоторой величины, увеличивается их дисперсия D вплоть до дисперсии эффективной несмещенной оценки. Это следует непосредственно из неравенства Рао–Крамера для смещенных оценок [6]:

$D(\theta(R)) \geq [1+b'(t)]^2/i_n(t)$,

где $i_n(t) = n/t$ – количество информации Фишера для распределения Пуассона.

То есть оценке с минимальным смещением $b(\theta)$, начиная с некоторой величины вплоть до нуля, всегда соответствует большая дисперсия и эта дисперсия всегда будет меньше дисперсии эффективной несмещенной оценки (см. примеры из [3]). Поэтому делать выбор из двух смещенных оценок с одинаковой эффективностью по их дисперсии на указанном классе оценок приведет к ошибочному мнению. Сказанное позволяет сделать вывод, что использовать дисперсию в качестве характеристики критерия эффективности смещенных оценок не имеет смысла.

Докажем этот факт. Для указанного класса оценок смещение имеет вид

$$b(\theta;t) = E\theta - t = e^{-\Delta}\sum_{r=0}^{\infty}\frac{N\tau\Delta^r}{(r+1)r!} + e^{-\Delta}\sum_{r=0}^{\infty} f(r)\frac{N\tau\Delta^r}{r!} - t.$$

Построим производную по параметру t:

$$b'(\theta;t) = (e^{-N\tau/t}\sum_{r=0}^{\infty}\frac{(N\tau)^{r+1}}{t^r(r+1)!} + e^{-N\tau/t}\sum_{r=0}^{\infty} f(r)\frac{(N\tau)^{r+1}}{t^r r!} - t)' =$$

$$= (e^{-N\tau/t}\sum_{r=0}^{\infty}\frac{(N\tau)^{r+1}}{r!t^r}\left(\frac{1}{r+1} + f(r)\right) - t)'.$$

Обозначим часть рассматриваемой формулы, независящую от параметра t, через

$K = \frac{(N\tau)^{r+1}}{r!}\left(\frac{1}{r+1} + f(r)\right)$. Так как $f(R=0) > 0$ и по смыслу $f(R>0) < 1/(r+1)$, то всегда $K > 0$. Тогда

$$b'(\theta;t) = (e^{-N\tau/t}\sum_{r=0}^{\infty}\frac{K(r)}{t^{r+1}} - t)' =$$

$$= -1 + (N\tau/t^2)e^{-N\tau/t}\sum_{r=0}^{\infty}\frac{K(r)}{t^{r+1}} + e^{-N\tau/t}\sum_{r=0}^{\infty}(-1^{r+1})\frac{K(r)}{t^{2(r+1)}}.$$

Для краткости и простоты изложения рассмотрим наиболее часто встречающийся случай, когда время испытаний τ совпадает со СНДО $\tau \approx t$, тогда производная от смещения по параметру СНДО примет вид

$$b'(\theta;t) = -1 + (N/t)e^{-N}\sum_{r=0}^{\infty}\frac{N^{r+1}}{r!}(\frac{1}{r+1} + f(r)) +$$

$$+ e^{-N}\sum_{r=0}^{\infty}(-1^{r+1})\frac{N^{r+1}}{r!}(\frac{1}{r+1} + f(r))\frac{1}{t^{r+1}}.$$

Табл. 1. Результаты получения эффективной оценки СНДО

Оценка СНДО	A	W	$Q=(A+1)\cdot W$
$\theta(R=0) = 2{,}400N\tau$, $\theta(R=1) = 0{,}3799N\tau$, $\theta(R=2) = 0{,}2628N\tau$, $\theta(R=3) = 0{,}2470N\tau$, $\theta(R=4) = 0{,}2100N\tau$, $\theta(R=5) = 0{,}1710N\tau$, $\theta(R=6) = 0{,}1417N\tau$, $\theta(R=7) = 0{,}1246N\tau$, $\theta(R=8) = 0{,}1110N\tau$, $\theta(R>8) = N\tau/(R+1)$	0	0,600	0,600
$T_d(R=0) = 2{,}4N\tau$, $T_d(R=1) = 0{,}35N\tau$, $T_d(R=2) = 0{,}3N\tau$, $T_d(R>2) = N\tau/(R+1)$	0	0,624	0,624
$T_B = 2{,}3N\tau$ при $R=0$, $T_B = 0{,}35N\tau$ при $R=1$ и $T_B = N\tau/(R+1)$ при $R>1$	0	0,635	0,635
$T_C = 2{,}25N\tau$ при $R=0$, $T_C = 0{,}375N\tau$ при $R=1$ и $T_C = N\tau/(R+1)$ при $R>1$	0	0,65	0,65
$T_A = 2{,}2N\tau$ при $R=0$, $T_A = 0{,}4N\tau$ при $R=1$ и $T_A = N\tau/(R+1)$ при $R>1$	0	0,665	0,665
$T_1(R=0) = 2n\tau$, $T_1(R>0) = n\tau/(R+1)$	0	0,736	0,736

Табл. 2. Величины производной от смещения по параметру СНДО $b'(\theta;t)$ для различных вариантов оценок из указанного выше класса при $N = 5$ и для пяти различных величин параметра СНДО t, выраженных в часах

Оценка	$t=10^2$	$t=10^3$	$t=10^4$	$t=10^5$	$t=10^6$	Нормированная суммарная дисперсия D
T_1	-1	-1	-1	-1	-1	8,80
T_A	-10,2944	-1,9277	-1,0927	-1,0092	-1,0009	9,96
T_C	-117,18	-12,5971	-2,1595	-1,1159	-1,0115	10,30
T_B	-14,9416	-2,3916	-1,1391	-1,0139	-1,0013	10,65
T_D	-20,0947	-2,9069	-1,1906	-1,019	-1,0019	11,34
θ	-21,1823	-3,0162	-1,2016	-1,0201	-1,002	11,35

В табл. 2 приведены величины производной от смещения по параметру СНДО $b'(\theta;t)$ для различных вариантов оценок из указанного выше класса при $N = 5$ и для пяти различных величин параметра СНДО t.

Из табл. 2 можно сделать вывод, что производная от смещения по параметру СНДО $b'(\theta;t)$ для указанного класса оценок $\theta = (N\tau/(R+1)) + N\tau f(R)$ всегда меньше нуля. Что доказывает выше сказанное. В последней графе представлены нормированные суммарные дисперсии указанных оценок. Наибольшей дисперсией обладает наиболее эффективная оценка θ, а наименьшей дисперсией – наименее эффективная оценка T_1. Что ещё раз подтверждает сделанные выводы. Заметим, что характер изменения величин дисперсий смещенных оценок имеет тенденцию к сближению с дисперсией наиболее эффективной оценки θ ($D = 11,35$) снизу с уменьшением смещения $b(\theta)$. Что позволяет сделать вывод на основе неравенства Рао – Крамера об абсолютной эффективности оценки θ в пределах рассматриваемого класса оценок $\theta = (N\tau/(R+1)) + N\tau f(R)$.

Таким образом оценке, определенной в классе линейных оценок $\theta = (N\tau/(R+1)) + N\tau f(R)$ с минимальным смещением, начиная с некоторой величины смещения вплоть до нуля, всегда соответствует большая дисперсия. Аналогично, оценке из этого класса с большим смещением всегда соответствует меньшая дисперсия, что не соответствует принципу минимизации функционала на смещенной оценке с уменьшением смещения при поиске эффективных смещенных оценок. Сказанное позволяет сделать более широкий вывод, что использовать дисперсию в качестве характеристики критерия эффективности смещенных оценок в принципе не имеет смысла.

Тот единственный случай, когда дисперсия играет свою роль при сравнении смещенных оценок на эффективность, это когда две смещенные оценки имеют одинаковые величины эффективности и равные по величине балансировки, представляется практически не выполнимым, так как всегда можно найти более эффективную оценку в классе всех смещенных оценок.

Заметим, что минимизация функционала $Q(\theta)$ решается при строгой монотонности оценки θ по всем своим параметрам, что резко сужает поисковый класс оценок. Однако это не единственное условие, как может показаться. Формальная сторона строгой монотонности может привести к парадоксальному случаю, когда смещенная оценка лишь формально удовлетворяет этим условиям $\theta(R) > \theta(R+1)$ для всех реализаций R, а по сути своей $\theta(R) \approx \theta(R+1)$. В этих случаях оценка $\theta(R)$ должна отвергаться. И в дополнение к строгой монотонности приходит инженерный подход, когда добиваются, чтобы оценка $\theta(R)$ не противоречила здравому смыслу и была удобной в использовании, а полезность удобной оценки очевидна. Заметим, что инженерный подход еще больше сужает поисковый класс оценок.

Сказанное позволяет считать, что скорее всего полученная оценка $\theta(R)$ является предельной по своей эффективности на рассматриваемом классе оценок.

Выводы

Получена эффективная и сбалансированная оценка СНДО. Поиск осуществлялся в классе линейных оценок в соответствии с простым критерием эффективности смещенных оценок для плана с ограниченным временем испытаний и восстановлением отказавших изделий. Полученная оценка СНДО имеет направленность практического применения при испытаниях и эксплуатации однородной продукции различного назначения, в процессе которых отказы не возникали.

Из оценок с одинаковой эффективностью следует выбирать оценку с минимальным смещением, а затем попытаться отбалансировать её.

Оценке, определенной в классе линейных оценок $\theta = (N\tau/(R+1)) + N\tau f(R)$ с минимальным смещением, начиная с некоторой величины смещения вплоть до нуля, всегда соответствует большая дисперсия. Аналогично, оценке из этого класса с большим смещением всегда соответствует меньшая дисперсия, что не соответствует принципу минимизации функционала на смещенной оценке с уменьшением смещения при поиске эффективных смещенных оценок. Сказанное позволяет сделать более широкий вывод, что использовать дисперсию в качестве характеристики критерия

эффективности смещенных оценок в принципе не имеет смысла.

Список литературы

1. ГОСТ Р 27.003-2011. Надежность в технике. Управление надежностью. Руководство по заданию технических требований к надежности. М.: Стандартинформ, 2013 – 15 с.

2. Е.Ю. Барзилович, Ю.К.Беляев, В.А. Каштанов и др. Вопросы математической теории надежности.; под ред. Б.В. Гнеденко. – М.: Радио и связь, 1983. – 376 с.

3. Михайлов В.С. Критерий эффективности смещенных оценок в теории надежности. – М: Изд-во ФГУП «ЦНИИХМ», 2024. – 260 с.

4. Михайлов В.С. Простой критерий эффективности смещенных оценок. //Надежность. 2024. № 1. С. 25 – 33.

5. Ясногородский Р.М. Теория вероятностей и математическая статистика: уч. пособие. СПб.: Наукоемкие технологии, 2019. 320 с.

6. Шуленин В.П. Математическая статистика. Ч. 1. Параметрическая статистика / В.П. Шуленин. Томск: Изд-во НТЛ, 2012. 540 с.

References

1. GOST R 27.003-2011: Reliability in Engineering. Reliability Management. Guidelines for Setting Technical Requirements for Reliability.” Moscow: Standardinform, 2013. 15 p.

2. E. Yu. Barzilovich; Yu. K. Belyaev; V. A. Kashtanov, et al., “Issues of Mathematical Theory of Reliability,” ed. by B. V. Gnedenko. Moscow: Radio and Communication, 1983. 376 p.

3. Mikhailov, V. S. “Efficiency Criterion of the Shifted Estimations in the Reliability Theory.” Moscow: FGUP “TsNIIHM,” 2024. 260 pp.

4. Mikhailov, V. S. “Simple criterion of efficiency of the shifted estimations.” In Reliability. 2024. No. 1. pp. 25-33.

5. R. M. Yasnogorodskiy. Theory of Probabilities and Mathematical Statistics: Study Guide. St. Petersburg: Science-Intensive Technologies, 2019. 320 pp.

6. Shulenin, V. P. Mathematical Statistics. Ch. 1. Parametric Statistics. Tomsk: NTL, 2012. 540 pp.

Сведения об авторе

Виктор Сергеевич Михайлов – ведущий инженер, Федеральное государственное унитарное предприятие «Центральный научно-исследовательский институт химии и механики им. Д.И. Менделеева» (ФГУП «ЦНИИХМ»). Адрес: ул. Нагатинская, д. 16а, Москва, Российская Федерация, 115487, e-mail: Mvs1956@list.ru

About the author

Viktor S. Mikhailov, Lead Engineer, Federal State Unitary Enterprise Central Research Institute of Chemistry and Mechanics (CNIIHM). Address: 16a Nagatinskaya St., Moscow, 115487, Russian Federation, e-mail: Mvs1956@list.ru.

Вклад автора в статью:

Получена эффективная и сбалансированная оценка СНДО. Поиск осуществлялся в классе линейных оценок в соответствии с простым критерием эффективности смещенных оценок для плана с ограниченным временем испытаний и восстановлением отказавших изделий. Сделаны выводы.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

УДК 621.879.3:658.5
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-25-32

Экспертная оценка влияния стажа работы оператора на риск повреждения оборудования

Expert assessment of the effect of an operator's work experience on the risk of equipment damage

Доронин С.В.[1], Альшанская А.А.[1]*
Doronin S.V.[1], Alshanskaya A.A.[1]*

[1] *Сибирский федеральный университет, Красноярск, Российская Федерация*
[1] *Siberian Federal University, Krasnoyarsk, Russian Federation.*
**alshanskaya_anna@inbox.ru*

Доронин С.В.

Альшанская А.А.

Резюме. Цель. *Целью является разработка и практическая апробация методики количественной оценки риска повреждения оборудования вследствие ошибок оператора, частота которых обусловлена стажем его работы.* **Методы.** *Используются прикладные методы социологии (анкетирование, экспертная оценка) и анализа рисков для получения количественных зависимостей риска повреждения от стажа работы оператора. Использование этих методов предполагает систематизацию возможных ошибок оператора в виде нарушений правил технической эксплуатации оборудования, экспертную оценку частоты этих нарушений в зависимости от стажа оператора. В результате декомпозиции оборудования определяется множество составных частей, для которых получаются экспертные оценки опасности повреждений для систематизированных нарушений правил технической эксплуатации. В конечном итоге риск оценивается как произведение частоты ошибок оператора (систематизированных нарушений правил) на опасность повреждения составных частей оборудования.* **Результаты.** *Методика апробирована на примере сбора экспертной информации и количественной оценки риска повреждения составных частей силовых конструкций рабочего оборудования карьерных экскаваторов при нарушениях машинистом правил технической эксплуатации.* **Выводы.** *Предложено использование экспертных оценок влияния опыта работы оператора на риск повреждения оборудования для решения ряда прикладных задач: обоснования периодичности и объема плановой и неплановой технической диагностики и ремонта, установления ошибок оператора, которые в первую очередь должны быть исключены за счет повышения качества профессиональной подготовки.*

Abstract. Aim. *The paper aims to develop and test a methodology for quantifying the risk of equipment damage due to operator errors whose frequency depends on their work experience.* **Methods.** *The authors use applied methods of sociology (questionnaires, expert assessment) and risk analysis to obtain quantitative dependences of the risk of damage on the work experience. The above methods involve classifying the possible operator errors in the form of equipment operation violations, an expert assessment of the frequency of such violations depending on the operator's work experience. By decomposing the equipment we define a set of components, for which expert assessments are obtained of the risk of damage for classified operation violations. Ultimately, the risk is assessed as the product of the frequency of operator errors (classified violations of the rules) and the probability of damage to the equipment components.* **Results.** *The method was tested by collecting expert information and quantifying the risk of damage to the components of the power structures of working equipment of mining excavators in case of violations by the operator of the rules of operation.* **Conclusions.** *It is proposed to use expert assessments of the effect of an operator's work experience on the risk of equipment damage to solve a number of applied problems, i.e., substantiation of the frequency and scope of scheduled and emergency diagnostics and maintenance operations, identification of the operator errors to be – above all else – eliminated by improving the quality of professional training.*

Ключевые слова: *экспертные оценки, ошибки оператора, риск повреждения*
Keywords: *expert assessment, operator errors, risk of damage*

Для цитирования: *Доронин С.В., Альшанская А.А. Экспертная оценка влияния стажа работы оператора на риск повреждения оборудования // Надежность. 2025. №2. С. 25-32. https://doi.org/10.21683/1729-2646-2025-25-2-25-32*

For citation: *Doronin S.V., Alshanskaya A.A. Expert assessment of the effect of an operator's work experience on the risk of equipment damage. Dependability 2025;2: 25-32. https://doi.org/10.21683/1729-2646-2025-25-2-25-32*

Поступила: *08.06.2024* / **После доработки:** *25.12.2024* / **К печати:** *09.06.2025*
Received on: *08.06.2024* / **Revised on:** *25.12.2024* / **For printing:** *09.06.2025*

Введение

Известна роль оператора в формировании надежности управляемых человеком технических систем [1]. По данным разных источников, учитывающих специфику отраслей и типов систем, отказы, обусловленные ошибками человека-оператора, составляют от 30 до 94 % всех отказов [1–5]. Анализ причин и условий возникновения этих ошибок затруднен вследствие весьма сложной структуры человеческого фактора, подверженного влиянию явлений, процессов и событий разной природы [1, 2, 5–7]. Большим разнообразием отличается также степень влияния ошибок оператора на работу технической системы – это касается как характера нарушений работоспособности, так и их отражения в изменении количественных характеристик надежности [4, 8]. Формализация анализа количественного влияния ошибок оператора на тяжесть их последствий значительно осложняется разнообразием проявлений, возможностью в некоторых случаях только качественного описания как ошибок, так и последствий. С позиций системного анализа исследование взаимосвязи ошибок оператора и надежности технической системы представляет собой слабоструктурированную задачу. В связи с этим обоснование универсального подхода представляется малопродуктивным для практических целей. По-видимому, целесообразны разработка и апробация частных методик формализации проблемы количественного анализа влияния ошибок человека-оператора на надежность технических систем. Представляется целесообразным выстраивать такие методики на основании экспертных знаний в терминах риска, учитывающего опасность возникновения ошибок оператора. Они могут рассматриваться в качестве вклада в решение проблемы «человеческого фактора» в надежности – по мнению проф. И.А. Ушакова [9] – одной из проблем, ожидающих решения.

Концепция экспертной оценки риска повреждения оборудования

Основным содержанием понятия «риск» являются вероятностные характеристики нежелательных событий, процессов, явлений [10, 11]. В качестве универсальной общепринятой меры риска рассматривается произведение вероятности и последствий наступления неблагоприятных событий. Полагаем, что вероятность этих событий зависит от инициирующего их оператора, а последствия определяются преимущественно свойствами технической системы.

При разработке варианта одной из возможных частных методик формализации влияния ошибок оператора на надежность оборудования исходили из следующих концептуальных положений.

Рассматриваемые технические системы ограничиваются отдельным классом (типом) технологического оборудования, ошибки оператора которого приводят к повреждениям некоторых конструктивных элементов (подсистем, составных частей) этого оборудования.

Последствия ошибок оператора выражаются в изменении состояния оборудования и безотносительно к классу технической системы в общем виде могут соответствовать состояниям, принятым в теории надежности: исправное, неисправное, работоспособное, неработоспособное, предельное. Поскольку в сложных системах возможно множество неработоспособных состояний, и их дифференциация необходима для обоснования решений по восстановлению работоспособности, целесообразна систематизация и конкретизация этих состояний и соответствующих им повреждений.

Ошибки оператора заключаются в нарушении правил технической эксплуатации (ПТЭ) оборудования. Предполагается, что эти нарушения не обусловливают друг друга, т.е. являются независимыми событиями. Это предположение вытекает из логики создания ПТЭ, каждое положение которых обычно сформулировано как самостоятельное требование к отдельным аспектам процесса эксплуатации. Проанализированные ПТЭ некоторых классов технических систем (в частности, технологического оборудования горнодобывающих предприятий открытого способа разработки) подтверждают это предположение. Это существенно уменьшает потенциальный перечень рассматриваемых ошибок и облегчает их формализацию: ошибкой считаются только действия, явно противоречащие тому или иному требованию ПТЭ. Тогда систематизация возможных ошибок оператора заключается в формировании перечня нарушений ПТЭ оборудования.

Вероятность ошибок оператора (нарушений ПТЭ) является производной всего комплекса его психо-физиологических характеристик. Достоверное определение как перечня этих характеристик, так и их количественных значений является чрезвычайно сложной проблемой. Эту вероятность целесообразно оценивать экспертными методами, ориентируясь на некоторую качественную шкалу оценки вероятности. Примером такой шкалы может служить следующая градация качественных значений вероятности: почти наверняка; высоковероятно; вероятно; маловероятно; почти наверняка нет. Более детальная градация, сопровождаемая количественными значениями вероятности, предложена в [12]: шкала содержит 19 позиций, начиная от *certain* (вероятность 1)

и заканчивая *impossible* (вероятность 0) с дискретным шагом значения вероятности 0,05. Однако такая детальная градация требует от эксперта способности различать вероятности событий, отличающиеся на 5%, как и вообще навыков вероятностного мышления. Во многих случаях экспертам, работающим в реальном секторе экономики, целесообразно использовать частотную трактовку вероятности нежелательных событий, например: почти наверняка – очень часто; высоковероятно – часто; вероятно – умеренно часто; маловероятно – редко; почти наверняка нет – крайне редко.

Принято упрощающее допущение: частота ошибок оператора обусловлена (скорее всего, нелинейно) стажем его работы с рассматриваемым оборудованием. Поскольку стаж оператора определяется достоверно, допущение связи стажа и частоты ошибок значительно облегчает получение экспертных оценок этой частоты.

При получении экспертных оценок в каждом конкретном случае привлекаются специалисты высокой квалификации в области эксплуатации конкретного класса оборудования, входящие в достаточно узкую профессиональную группу. Это способствует высокой однородности и воспроизводимости их мнений.

Таким образом, в качестве интегральной характеристики тяжести ошибок оператора рассматривается риск повреждения оборудования, оцениваемый как произведение экспертных оценок частоты нарушений ПТЭ на степень повреждения оборудования, что не противоречит общепринятому пониманию риска. В этом случае неблагоприятными событием является нарушение ПТЭ вследствие ошибки оператора, аналогом вероятности служит экспертная оценка его частоты, а степень повреждения оборудования рассматривается в качестве последствий.

Методика оценки риска повреждения оборудования в связи со стажем оператора

Для количественного анализа риска повреждения оборудования в связи с ошибками оператора необходимо получить экспертные оценки вероятности ошибок и тяжести их последствий в форме, допускающей количественную интерпретацию. Это предполагает использование процедуры приписывания количественной меры качественным понятиям (квантификации). Такая процедура должна быть максимально прозрачной, понятной и обоснованной, чтобы избежать превращения в свою противоположность («квантофрению») [13]. Рассмотрим примеры квантификации качественных величин применительно к задачам надежности и безопасности.

Оценка критичности отказов осуществляется с учетом трех характеристик: тяжести последствий отказа единицы оборудования, вероятности отказа этого оборудования и вероятности необнаружения этого отказа до проявления его последствий. Первая характеристика по своей природе качественная, остальные – количественные, но получаемые методом экспертных оценок в качественной форме. Для квантификации всем трем величинам ставятся в соответствие целочисленные шкалы в интервале от 1 до 10 со следующими значениями крайних значений [14]. Ранг тяжести последствий изменяется от 1 (агрегат полностью работоспособен, но его целостность, шумность и вибрация не соответствуют требованиям, и это замечают менее 25% эксплуатационного персонала) до 10 (отказ создает угрозу здоровью и жизни людей, причинения существенного вреда окружающей среде). Ранг вероятности отказа равен 1 для «невероятного» отказа (один раз в 1001 сутки и реже) и 10 для частого отказа (один раз в сутки и чаще). Ранг вероятности необнаружения отказа составляет 1, если автоматика предотвращает причины всех потенциальных отказов, и 10, если контроль не предусмотрен, не производится или не позволяет обнаружить отказ, результаты контроля не регистрируются и не анализируются.

Аналогичные характеристики используются в [15] для балльной оценки травмирующих факторов: тяжесть последствий от возникновения опасности, вероятность возникновения опасности, относительная частота обнаружения опасности. Каждая характеристика оценивается по относительной шкале от 1 до 10. Так, последствие опасности оценивается в 1 в при возможности боли, но невозможности повреждений и ухудшения состояния здоровья; 10 – при групповом смертельном случае со смертельным исходом. Относительная частота обнаружения оценивается по обратной 10-балльной шкале – чем проще своевременно обнаружить и избежать последствий, тем меньше оценка.

При категорировании объектов по уязвимости с помощью выполняемых экспертами парных сравнений и анализе иерархий шкала квантификации смысла экспертных оценок содержит значения от 1 (равная важность) до 9 (очень сильное превосходство одного над другим) [16].

Лингвистические оценки силы влияния друг на друга концептов в когнитивных картах анализа надежности квантифицируются с помощью нецелочисленной шкалы в интервале от -1 до 1: -1 – отрицательное максимальное, -0,75 – отрицательное выше среднего,…, 0,75 – положительное выше среднего, 1 – положительное максимальное влияние [17].

В [18] предложены балльно-факторные функции при анализе безопасности эксплуатации подземного газопровода. Так в общем случае глубине прокладки стального газопровода более 0,8 м соответствует балл 0, равной 0,8 м – 2, менее 0,8 м – 10; на пахотных и орошаемых землях глубине более 1,0 м приписывается балл 3, равной 1,0 м – 5, менее 1,0 м – 10. Аналогичные распределения приведены и для других факторов. Здесь используются шкалы с непостоянным шагом и не интуитивно ожидаемыми крайними значениями.

Таким образом, встречаются целочисленные и нецелочисленные шкалы квантификации с постоянным и

произвольным шагом дискретизации, положительными и отрицательными значениями на шкале, «круглыми» и «некруглыми» границами интервалов. Практически всегда эти шкалы постулируются авторами без логического обоснования и объяснения. Очевидно, квантификация по своей природе оказывается субъективной, как и сами экспертные оценки. Поэтому мы ориентируемся на наиболее простой и «прозрачный» вариант с целочисленными шкалами, положительными значениями рангов, минимальным числом постоянных шагов дискретизации. Для более сложных вариантов просто не находится логических оснований.

На основании предложенной концепции сформулирована следующая методика экспертной оценки влияния стажа работы оператора на риск повреждения технологического оборудования, представляющая собой один из вариантов формализации влияния ошибок оператора на его надежность.

Для количественной оценки частоты нарушений ПТЭ вводится пятибалльная шкала, определяемая следующим образом: 1 – крайне редко; 2 – редко; 3 – умеренно часто; 4 – часто; 5 – очень часто. Увеличение балла (то есть, «чаще») соответствует росту риска повреждения оборудования. Очевидно, возможны и другие варианты вербальной характеристики частоты.

Стаж работы оператора с рассматриваемым оборудованием является непрерывной величиной на шкале времени, которую предлагается разбить на m интервалов в предположении качественного изменения опыта работы оператора при переходе из одного интервала в другой. Очевидно, это условность, необходимая для ограничения количества альтернативных вариантов экспертных оценок влияния стажа на частоту нарушений ПТЭ.

Далее осуществляется сбор экспертной информации (анкетирование и статистическая обработка результатов) о частоте систематизированных нарушений ПТЭ в связи со стажем оператора. Возможная форма вопроса анкеты: «Оцените частоту *конкретного нарушения ПТЭ* в зависимости от стажа оператора». Ответы экспертов получаются в виде процентного распределения частот нарушения ПТЭ для каждого интервала стажа работы $E_{i,j}$, i=1, …, m; j=1, …, 5, где i – порядковый номер интервала стажа, j – балл качественной оценки частоты нарушения ПТЭ.

Суммарная балльная оценка влияния стажа для его i-го интервала определяется суммой произведений процентной доли качественной характеристики E на соответствующий балл b по формуле

$$B_{fi} = \sum_{j=1}^{n} E_{i,j} b_j, \quad i = 1,...,m. \tag{1}$$

Исходя из предположения (подтверждающегося данными опроса экспертов), что наименьшему стажу соответствует максимальная частота нарушений ПТЭ, снижающаяся с накоплением опыта, относительный коэффициент количественного влияния равен

$$K_i = \frac{B_{fi}}{B_{f1}}, \quad i = 1,...,m. \tag{2}$$

Таким образом, влияние стажа на частоту нарушения ПТЭ выражается относительной безразмерной величиной в интервале от 0 до 1. В этом случае минимальному стажу соответствует величина относительного коэффициента $K_1 = 1$, а с увеличением стажа значение коэффициента падает.

Для каждого систематизированного нарушения ПТЭ результаты анкетирования и соответствующей статистической обработки организовываются в виде сводной таблицы (табл. 1).

Далее осуществляется декомпозиция оборудования – выделение n составных частей (подсистем, узлов, агрегатов…), для которых предполагается оценивать опасность (степень) повреждений при нарушении ПТЭ.

Для количественной оценки опасности повреждения оборудования вследствие ошибки оператора также вводится пятибалльная шкала:

0 – опасность отсутствует (повреждений нет);

1 – незначительная опасность (возможны незначительные, визуально необнаруживаемые повреждения, не снижающие работоспособность во всем спектре эксплуатационных нагрузок);

2 – умеренная опасность (повреждения, не снижающие работоспособность при номинальных нагрузках);

3 – высокая опасность (серьезные повреждения, ограниченная работоспособность при пониженных нагрузках);

4 – неприемлемо высокая опасность (разрушения, неработоспособное состояние).

Табл. 1. Формализация и квантификация экспертных оценок влияния стажа на частоту нарушения ПТЭ

Качественная экспертная оценка частоты нарушения ПТЭ	**Балльная оценка b**	**Значение фактора E, %, при стаже**						
		E_1	E_2	….	E_i	….	E_{m-1}	E_m
Крайне редко	1	$E_{1,1}$	$E_{2,1}$	….	$E_{i,1}$	….	$E_{m-1,1}$	$E_{m,1}$
Редко	2	$E_{1,2}$	$E_{2,2}$	….	$E_{i,2}$	….	$E_{m-1,2}$	$E_{m,2}$
Умеренно часто	3	$E_{1,3}$	$E_{2,3}$	….	$E_{i,3}$	….	$E_{m-1,3}$	$E_{m,3}$
Часто	4	$E_{1,4}$	$E_{2,4}$	….	$E_{i,4}$	….	$E_{m-1,4}$	$E_{m,4}$
Очень часто	5	$E_{1,5}$	$E_{2,5}$	….	$E_{i,5}$	….	$E_{m-1,5}$	$E_{m,5}$
Балльная оценка влияния B_f		B_{f1}	B_{f2}	….	B_{fi}	….	B_{fm-1}	B_{fm}
Коэффициент количественного влияния K		K_1	K_2	….	K_i	….	K_{m-1}	K_m

Как и в случае оценки частоты, увеличение балла (то есть, «опаснее») соответствует росту риска повреждения оборудования.

Далее осуществляется опрос экспертов об опасности повреждения декомпозированных составных частей (СЧ) оборудования при всех систематизированных нарушениях ПТЭ. Возможная форма вопроса анкеты: «Оцените опасность повреждения *конкретной составной части оборудования* вследствие *конкретного нарушения ПТЭ*». Ответы экспертов получаются в виде процентного распределения мнений относительно опасности повреждения СЧ D_l, l=0, …, 4, где l – балльная оценка опасности повреждения. Безразмерная интегральная оценка опасности повреждения каждой СЧ оборудования при каждом нарушении ПТЭ определяется суммированием произведений экспертной оценки процентного распределения степени опасности повреждения на соответствующие балльные оценки

$$B_d = \sum_{l=1}^{4} lD_l. \qquad (3)$$

Суммирование выполняется начиная с l=1, поскольку при l=0 повреждения отсутствуют.

Для каждого систематизированного нарушения ПТЭ сводная таблица результатов оценки опасности повреждений СЧ выглядит следующим образом (табл. 2).

Табл. 2. Формализация и квантификация экспертных оценок опасности повреждений при нарушении ПТЭ

Составная часть	Значение фактора D, %					Интегральная оценка опасности
	$l=0$	$l=1$	$l=2$	$l=3$	$l=4$	
СЧ$_1$	$D_{0,1}$	$D_{1,1}$	$D_{2,1}$	$D_{3,1}$	$D_{4,1}$	B_{d1}
СЧ$_2$	$D_{0,2}$	$D_{1,2}$	$D_{2,2}$	$D_{3,2}$	$D_{4,2}$	B_{d2}
…	…	…	…	…	…	…
СЧ$_n$	$D_{0,n}$	$D_{1,n}$	$D_{2,n}$	$D_{3,n}$	$D_{4,n}$	B_{dn}

В конечном итоге для каждой СЧ рассматриваемого оборудования определяется риск ее повреждения при всех нарушениях ПТЭ в зависимости от опыта работы оператора как

$$R = K_i B_d, \quad i = 1,...m. \qquad (4)$$

Экспертная оценка риска повреждения силовых конструкций рабочего оборудования карьерного экскаватора в связи со стажем работы машиниста

Апробация методики выполнена на примере экспертной оценки влияния стажа работы машиниста на риск повреждения силовых конструкций карьерных гусеничных экскаваторов ЭКГ. Экспертные мнения получены путем анкетирования нескольких десятков специалистов угольных разрезов и рудных карьеров Сибири и Дальнего Востока, входящих в узкую профессиональную группу эксплуатационников карьерных экскаваторов [19]. При определении числа анкетируемых ориентировались на следующие оценки [20]: эмпирическим путем установлено, что эксперты в количестве 13–15 человек могут рассматриваться как достаточно представительная группа для проведения экспертизы сложных технических систем. Значительное увеличение числа экспертов потенциально опасно снижением уровня их компетентности (число экспертов в достаточно узкой профессиональной группе по умолчанию не может быть очень большим). Число экспертов от 30 до 40 человек нам представляется разумным компромиссом между точностью и стоимостью получаемых оценок.

Перечень нарушений ПТЭ сформулирован на основании технической документации (преимущественно инструкций по эксплуатации). В качестве основных нарушений ПТЭ рассматриваются:

- удар ковшом о забой в начале цикла экскавации;
- удар ковшом о транспортное средство при разгрузке ковша;
- удар ковшом по гусеницам;
- удар рукоятью по стреле;
- удар упорами рукояти об упоры седлового подшипника;
- удар обоймой блока ковша по головным блокам стрелы;
- допущение режима стопорения ковша в забое;
- совмещение работы напорного и поворотного механизмов;
- совмещение работы подъемного и поворотного механизмов;
- работа при наклоне площадки забоя свыше 5°;
- глубокое врезание ковша в грунт;
- копание тяжелых грунтов при полностью выдвинутой рукояти.

Эти нарушения являются независимыми друг от друга событиями: каждое из них является следствием самостоятельной, отдельной ошибки машиниста экскаватора.

Далее рассмотрим применение методики на примере первого нарушения из представленного списка.

Рассматривается m = 5 интервалов стажа: до одного года, от одного до трех лет, от трех до пяти лет, от пяти до десяти лет, свыше десяти лет. Результаты ответов анкетируемых на вопрос «Оцените частоту удара ковшом о забой в начале цикла экскавации в зависимости от стажа машиниста экскаватора» представлены в табл. 3. В соответствии с (1) балльные оценки влияния для рассматриваемых интервалов стажа определены, например, для первого интервала стажа (до одного года) следующим образом: B_{f1} = 4·1+15·2+22·3+26·4+33·5 = 369. Соответственно коэффициент количественного влияния (2) для этого подинтервала равен K_1 = 369/369 = 1,00. Результаты расчета балльных оценок и коэффициентов влияния для всех подинтервалов стажа содержатся в табл. 3.

Табл. 3. Экспертная оценка частоты удара ковшом о забой в связи со стажем машиниста

Качественная экспертная оценка частоты удара ковшом о забой	Балльная оценка b	Частота нарушения ПТЭ, %, при стаже машиниста, лет				
		< 1	1–3	3–5	5–10	> 10
Крайне редко	1	4	15	56	63	78
Редко	2	15	22	22	33	22
Умеренно часто	3	22	37	18	4	
Часто	4	26	22	4		
Очень часто	5	33	4			
Балльная оценка влияния B_f		369	278	170	141	122
Коэффициент количественного влияния K		1,00	0,75	0,46	0,38	0,33

В результате декомпозиции выделены шесть СЧ силовых конструкций рабочего оборудования: ковш, рукоять, стрела, двуногая стойка, седловой подшипник, подкосы. Результаты ответов анкетируемых на вопрос «Оцените опасность повреждения составных частей оборудования вследствие удара ковшом о забой в начале цикла экскавации» содержатся в табл. 4. Интегральная оценка опасности повреждения (3) для экспертных мнений, выраженных в долях единицы, определяется, например, для первой СЧ (ковш) следующим образом: $B_{d1} = 0{,}21 \cdot 1 + 0{,}24 \cdot 2 + 0{,}45 \cdot 3 + 0 \cdot 4 = 2{,}04$. Результаты вычисления интегральной оценки опасности для всех СЧ содержатся в табл. 4.

Оценка риска осуществляется по формуле (4) с учетом данных табл. 3 и 4. Так, например, риск повреждения ковша при работе машиниста со стажем до одного года оценивается как $R = 1{,}00 \cdot 2{,}04 = 2{,}04$, а со стажем от одного до трех лет – $R_1 = 0{,}75 \cdot 2{,}04 = 1{,}53$. Результаты оценки риска повреждения всех составных частей оборудования при рассматриваемом нарушении ПТЭ машинистом экскаватора с разным стажем работы приведены в табл. 5.

Аналогичные оценки получены для всех систематизированных нарушений ПТЭ.

Заключение

Получаемые таким образом количественные оценки риска применимы для сравнительного анализа повреждаемости оборудования при решении следующих практических задач:

- для составных частей оборудования с наибольшими рисками повреждения осуществляется повышение периодичности и объема неразрушающего контроля, диагностики и плановых ремонтов;
- в случае установления факта конкретного нарушения ПТЭ устанавливаются приоритеты планового визуального и измерительного контроля;
- организовывается повышение качества профессиональной подготовки операторов в части отработки приемов работы, снижающих (в пределе – исключающих) условия и причины возникновения нарушений ПТЭ, характеризующихся наибольшими рисками повреждения оборудования.

Благодарности

Авторы выражают признательность д.т.н. А.В. Бочкову за ценные советы и замечания по существу проблемы

Табл. 4. Экспертная оценка опасности повреждения составных частей оборудовании при ударе ковшом о забой

Составная часть	Распределение D, %, опасности повреждения l					Интегральная оценка опасности B_d
	0	1	2	3	4	
Ковш	10	21	24	45	0	2,04
Рукоять	7	24	21	45	3	2,13
Стрела	10	28	34	28	0	1,80
Двуногая стойка	21	34	21	24	0	1,48
Седловой подшипник	7	24	41	21	7	1,97
Подкосы	17	42	24	17	0	1,41

Табл. 5. Оценка риска повреждения составных частей силовых конструкций рабочего оборудования экскаваторов

Составная часть	Риск повреждения R в связи со стажем машиниста				
	< 1	1–3	3–5	5–10	> 10
Ковш	2,04	1,53	0,94	0,78	0,67
Рукоять	2,13	1,60	0,98	0,81	0,70
Стрела	1,80	1,35	0,83	0,68	0,59
Двуногая стойка	1,48	1,11	0,68	0,56	0,49
Седловой подшипник	1,97	1,48	0,91	0,75	0,65
Подкосы	1,41	1,06	0,65	0,54	0,47

экспертной оценки риска повреждения оборудования при обсуждении настоящей статьи.

Библиографический список

1. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. М.: ООО «Журнал Надежность», 2012. 296 с.

2. Артемов А.Д., Лысаков Н.Д., Лысакова Е.Н. Человеческий фактор в эксплуатации авиационной техники. М.: МАИ, 2018. 156 с.

3. Ганнесен В.В., Соловьева Е.Е. Человеческий фактор как одна из основных причин аварийности // Научные труды Дальрыбвтуза. 2022. Т. 61. № 3. С. 64-69.

4. Николайкин Н.И., Шаров В.Д., Андрусов В.Э. Эволюция учета влияния ошибок человека на особенности и результаты коллективной работы // Crede experto: транспорт, общество, образование, язык. 2019. № 1. С. 8-40.

5. Котик М.А. О преднамеренных и непреднамеренных ошибках человека-оператора // Психологический журнал. 1993. Т. 14. № 5. С. 34-41.

6. Ллойд Д., Липов М. Надежность. Организация исследования, методы, математический аппарат. М.: Советское радио, 1964. 687 с.

7. Скоробогатов С.М. Место человеческого фактора в классификации техногенных катастроф железобетонных сооружений // Академический вестник УралНИИпроект РААСН. 2008. № 1. С. 91-94.

8. Репина И.Б. Учет влияния человеческого фактора на организационно-технологическую надежность производственных процессов инфраструктуры железных дорог: дис. … канд. техн. наук: 05.02.22 / СибГУПС; науч. рук. В.Д. Верескун. Новосибирск, 2015. 211 с.

9. Ушаков И. Надежность: прошлое, настоящее, будущее // Reliability: Theory & Applications. 2006. No. 1. Pp. 17-27.

10. Соколов Ю.И. Проблемы рисков современного общества // Проблемы анализа рисков. 2016. Т. 13. № 2. С. 6-23.

11. Бочков А.В. Проблемы оценки опасностей и управления риском объектов критически важной инфраструктуры Группы «Газпром»: аналитический обзор // Научно-технический сборник «Вести газовой науки». 2018. № 2(34). С. 51-87.

12. Sileo D., Moens M.-F. Probing neural language models for understanding of words of estimative probability / Proceedings of the The 12th Joint Conference on Lexical and Computational Semantics (*SEM 2023). Pp. 469-476.

13. Кравченко А.И. Квантификация и квантофрения: углубление познания или эскалация ошибок // Социология. 2018. № 4. С. 23-38.

14. Антоненко И.Н. Методика приоритизации объектов обслуживания на основе оценки критичности отказов // В мире НК. 2018. Т. 21, № 3. С. 68-72.

15. Мазаник Е.В., Гендлер С.Г., Истомин Р.С. и др. Ранжирование шахт ОАО «СУЭК-Кузбасс» на основе балльной оценки травмирующих факторов // Горный информационно-аналитический бюллетень. 2012. № S2-5. С. 21-26.

16. Бочков А. Категорирование критически важных объектов по уязвимости к возможным противоправным действиям. Экспертный подход // Безопасность. Достоверность. Информация. 2009. № 1(82). С. 22-24.

17. Ротштейн А.Н. Нечеткие когнитивные карты в анализе надежности // Надежность. 2019. № 4. С. 24-31.

18. Ямаева Э.Г., Фомина Е.Е. Разработка балльной оценки факторов влияния на безопасную эксплуатацию объектов газораспределения на этапе проектирования // Безопасность жизнедеятельности. 2016. № 1. С. 18-23.

19. Альшанская А.А., Доронин С.В., Тюменцев В.А. Экспертное оценивание факторов повышения надежности механического оборудования карьерных экскаваторов // Транспортное, горное и строительное машиностроение: наука и производство. 2023. № 19. С. 155-160.

20. Крянев А.В., Семенов С.С. К вопросу о качестве и надежности экспертных оценок при определении технического уровня сложных систем // Надежность. 2013. № 4. С. 90-109.

References

1. Shubinsky I.B. [Functional dependability of information systems. Analysis methods]. Moscow: Dependability Journal; 2012. (in Russ.)

2. Artiomov A.D., Lysakov N.D., Lysakova E.N. [Human factor in the operation of aviation equipment]. Moscow: MAI; 2018. (in Russ.)

3. Gannesen V.V., Soloveva E.E. The human factor as one of the main causes of accidents. *Scientific Journal of the Far Eastern State Technical Fisheries University* 2022;61(3):64-69. (in Russ.)

4. Nikolajkin N.I., Sharov V.D., Andrusov V.E. Evolution of account for human errors influence on collective work features and results. *International informational and analytical journal «Crede Experto: transport, society, education, language»* 2019;1:8-40. (in Russ.)

5. Kotik M. On undeliberate and deliberate errors of man-operator. *Psychological Journal* 1993;14(5):34-41. (in Russ.)

6. Lloyd D., Lipov M. Reliability: Management, Methods and Mathematics. Moscow: Sovietskoye radio; 1964.

7. Skorobogatov S.M. Place of the human factor in classification of the technologic accidents of ferro-concrete construction. *Akademicheskij vestnik UralNIIproekt RAASN* 2008;1:91-94. (in Russ.)

8. Repina I.B. [Accounting for the effect of the human factor on the organisational and process-related reliability of railway infrastructure processes: a Candidate of Engineering dissertation: 02.05.12. SibGUPS; scientific supervisor V.D. Vereskun]. Novosibirsk; 2015. (in Russ.)

9. Ushakov I. [Reliability: past, present, future]. *Reliability: Theory & Applications* 2006;1:17-25. (in Russ.)

10. Sokolov Yu.I. Problems of the risks of modern society. *Issues of Risk Analysis* 2016;13(2):6-23. (in Russ.)

11. Bochkov A.V. [Problems of hazard estimation and risk management of critical infrastructure facilities of the Gazprom Group: an analytical review]. *Vesti gazovoy Nauki* 2018;2(34):51-87. (in Russ.)

12. Sileo D., Moens M.-F. Probing neural language models for understanding of words of estimative probability. In: Proceedings of the The 12th Joint Conference on Lexical and Computational Semantics (*SEM 2023). Pp. 469-476.

13. Kravchenko A.I. Quantification and Quantophrenia: from the real world into the scientific world and vice versa. *Sociology* 2018;4:23-38. (in Russ.)

14. Antonenko I.N. Risk based prioritization technique of maintenance objects. *NDT World* 2018;21(3):68-72. (in Russ.)

15. Mazanik E.B., Gendler S.G., Istomin R.S., et al. Ranking the mines of JSC SUEK-Kuzbass based on a point assessment of injury risk factors. *Mining informational and analytical bulletin* 2012;S2-5: 21-26.

16. Bochkov A. [Categorisation of critical facilities in terms of their vulnerability to possible illegal actions. An expert approach]. *Bezopasnost. Dostovernost. Informatsiya* 2009;1(82):22-24. (in Russ.)

17. Rotshtein A.P. Fuzzy cognitive maps in the dependability analysis of systems. *Dependability* 2019;19(4):24-31.

18. Yamaeva E.G., Fomina E.E. Development of Scoring Factors Influencing the Safe Operation of the Gas Distribution in the Design Phase. *Bezopasnost' zhiznedeatel'nosti* 2016;1:18-23. (in Russ.)

19. Alshanskaya A.A., Doronin S.V., Tyumencev V.A. Expert evaluation of the factors of increasing the reliability of the mechanical equipment of mining excavators. *Transport, mining and construction engineering: science and production* 2023;19:155-160. (in Russ.)

20. Kryanev A.V., Semenov S.S. On the issue of quality and reliability of expert judgments in determining the engineering level of complex systems. *Dependability* 2013;(4):90-109.

Сведения об авторах

Доронин Сергей Владимирович – кандидат технических наук, доцент кафедры «Горные машины и комплексы», ФГАОУ ВО Сибирский федеральный университет (СФУ), пр-т Красноярский рабочий, д. 95, Красноярск, Российская Федерация, 660025, e-mail: mr.svdoronin@yandex.ru

Альшанская Анна Александровна – кандидат технических наук, старший преподаватель кафедры «Горные машины и комплексы», ФГАОУ ВО Сибирский федеральный университет (СФУ), пр-т Красноярский рабочий, д. 95, Красноярск, Российская Федерация, 660025, e-mail: alshanskaya_anna@inbox.ru

About the authors

Sergey V. Doronin, Candidate of Engineering, Senior Lecturer, Department of Mining Machines and Systems, Federal State Autonomous Educational Institution of Higher Education Siberian Federal University (SibFU), 95 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660025, Russian Federation, e-mail: mr.svdoronin@yandex.ru.

Anna A. Alshanskaya, Candidate of Engineering, Senior Teacher, Department of Mining Machines and Systems, Federal State Autonomous Institution of Higher Education Siberian Federal University (SibFU), 95 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660025, Russian Federation, e-mail: alshanskaya_anna@inbox.ru.

Вклад авторов в статью

Доронин С.В. – идея статьи, концепция и некоторые положения методики экспертной оценки риска повреждения оборудования в связи со стажем работы оператора.

Альшанская А.А. – разработка методики экспертной оценки, сбор и обработка экспертной информации, практическое получение количественных оценок риска повреждения оборудования.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

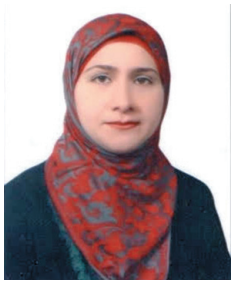
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-33-38

Анализ динамики пандемии с помощью бегущих волн: математическая модель

Running waves analysis of pandemic dynamics: a mathematical model

Таха Асраа[1], Игорь С. Константинов[2], Денис Н. Старченко[2]
Taha Asraa[1], Igor S. Konstantinov[2], Denis N. Starchenko[2]

[1] Белгородский национальный исследовательский университет, Ул. Победы, 85, Белгород, 308015, Россия
[2] Белгородский государственный технологический университет, ул.Костюкова, Белгород, 308012, Россия
[1] Belgorod State National Research University, 85 Pobedy st., Belgorod, 308015, Russia
[2] Belgorod State Technological University, Kostyukova st., Belgorod, 308012, Russia
1591248@bsu.edu.ru.



Таха Асраа

Игорь С. Константинов

Денис Н. Старченко

Резюме. *В этой статье исследуется динамика пандемий через призму решений, основанных на бегущей волне, в рамках математических моделей. Расширяя классическую модель SIR (Восприимчивый-Инфекционный-Выздоровевший), включив в нее пространственную зависимость, мы исследуем, как волны заболеваний распространяются среди населения. Посредством математического анализа и вывода мы выводим уравнения для скорости распространения волн и оцениваем серьезность эпидемий. Наши результаты подчеркивают решающую роль снижения коэффициента контакта в замедлении распространения болезни и минимизации ее последствий. Исследование подчеркивает силу математического моделирования в понимании пандемий и борьбе с ними, предлагая понимание стратегий эффективного вмешательства.*

Abstract. *This paper examines pandemic dynamics using running-wave-based tools and mathematical models. By extending the classic SIR (Susceptible-Infected-Removed) model to include spatial dependence, we explore how disease waves spread across a population. Through mathematical analysis and inference, we derive equations for the wave velocity and assess the severity of epidemics. Our findings emphasise the crucial role of reducing the contact factor in slowing the spread of a disease and minimising its consequences. The study highlights the power of mathematical modelling in understanding and responding to pandemics, suggesting insights into effective intervention strategies.*

Ключевые слова: *динамика пандемии, бегущие волны, математическое моделирование, модель SIR, пространственная зависимость, скорость волны, тяжесть эпидемии, коэффициент контактности, распространение болезни, стратегии вмешательства*
Keywords: *pandemic dynamics, running waves, mathematical modelling, SIR model, spatial dependence, wave velocity, epidemic severity, contact rate, disease spread, intervention strategies*

Для цитирования: *Таха Асраа, Константинов И.С., Старченко Д.Н. Анализ динамики пандемии с помощью бегущих волн: математическая модель // Надежность. 2025. №2. С. 33-38. https://doi.org/10.21683/1729-2646-2025-25-2-33-38*
For citation: *Taha Asraa, Konstantinov I.S., Starchenko D.N. Running wave analysis of pandemic dynamics: a mathematical model. Dependability 2025;2:33-38. https://doi.org/10.21683/1729-2646-2025-25-2-33-38*

Поступила: *29.07.2024* / **После доработки:** *29.12.2024* / **К печати:** *09.06.2025*
Received on: *29.07.2024* / **Revised on:** *29.12.2024* / **For printing:** *09.06.2025*

Введение

Волны в контексте пандемии представляют собой одну из волн распространения болезней среди населения. Математически волна – это нечто, что распространяется с постоянной формой и движется с постоянной скоростью. Решение этой формы называется решением бегущей волны. Это решение бегущей волны появляется в наших моделях путем добавления пространственной зависимости. Другими словами, мы хотим позволить людям передвигаться в рамках нашей модели и нашего эпидемического сценария. В модели SIR у нас есть зависимость только от времени для наших трех переменных S, I и R, мы можем видеть это, потому что у нас была только производная по времени. Итак, когда мы смотрим на то, как эти популяции менялись с течением времени, мы хотим, чтобы популяции также менялись в пространстве, потому что люди могут перемещаться. То, что мы делаем – создаем немного более реалистичную модель.

1. Обзор литературы

Пандемии были определяющими моментами на протяжении всей истории, формируя человеческую цивилизацию и оставляя неизгладимые следы в обществах, экономике и системах здравоохранения [1]. Эти глобальные вспышки инфекционных заболеваний выходят за рамки границ государств и оказывают массовое воздействие на население [2]. Динамика пандемий сложна, на нее влияют такие факторы, как вирулентность патогена, скорость передачи, плотность населения, инфраструктура здравоохранения и социальное поведение. Инфекционные заболевания могут быстро распространяться среди населения, чему способствуют глобальные путешествия, урбанизация и взаимосвязанность [3].

Математические модели широко использовались для изучения эпидемий, включая основополагающие работы, такие как модель SIR, представленная Кермаком и Маккендриком. Эти модели учитывают ключевые концепции, такие как восприимчивость, инфекционность и темпы выздоровления, для понимания динамики [4]. Они были применены к реальным сценариям для составления прогнозов и обоснования мер общественного здравоохранения. Например, математическое моделирование использовалось для контроля распространения заболеваний, управления ресурсами и принятия решений в спорте [5]. Использовались детерминированные и случайные модели, при этом компьютерные имитационные модели использовались для более сложных сценариев [6]. Системы математического моделирования предназначены для оценки эффективности мер по борьбе с эпидемией, анализа рисков и оценки экономического ущерба [7].

Решения в области пространственной зависимости и бегущей волны были изучены в нескольких исследованиях для расширения классических моделей эпидемий и понимания пространственного распространения болезней среди населения. В этих исследованиях были изучены теоретические основы моделей бегущих волн и их значимость для описания динамики эпидемий. Например, в [8] исследована модель эпидемии нелокального распространения с множественными нелокально распределенными задержками и нелинейными эффектами распространения, определена минимальная скорость волны и базовое число воспроизведения для определения существования решений для бегущих волн. Аналогично, в [9] использовали метод решения бегущей волны для преобразования дифференциальных уравнений в частных производных в обыкновенные дифференциальные уравнения и получили решения для скорости инфекционной волны и гипергеометрической функции в пространственной модели SIR.

Математические модели, в том числе те, которые включают бегущие волны, использовались в исследованиях общественного здравоохранения и при разработке политики. Эти модели были применены для обоснования мер вмешательства, стратегий вакцинации и обеспечения готовности к пандемии. Например, в [4] обсуждаются основы и перспективы, принятые для моделирования инфекционных заболеваний с использованием математического моделирования. Они освещают методологию, тактику и взаимосвязи этих подходов. Рассматриваются эпидемиологические сетевые модели, которые использовались для объяснения COVID-19 и обеспечивают достаточно точное приближение для директивных органов для определения действий, необходимых для ограничения спроблем и ограничений, связанных с математическим моделированием эпидемий, включая неопределенности в оценке параметров, упрощающие допущения и потребность в данных в реальном времени для точных прогнозов. Будущие направления исследований и разработок в области динамики пандемии и математического моделирования включают изучение новейших технологий, междисциплинарных подходов и новых методологий для улучшения нашего понимания распространения болезней и информирования общественного здравоохранения об ответных действиях [10]. Многочисленные лекции, организованные Департаментом непрерывного образования Оксфордского университета, изучали динамику модели SIR, которую исследователи использовали в этой статье [11].

2. Модель D-развития

Отправной точкой является та же самая модель SIR. Есть класс S для восприимчивых, тех, кто пока не заражен этой болезнью, но потенциально может заболеть. Класс I включает инфицированных, которые в настоящее время имеют болезнь и распространяют ее среди населения, и класс R – для категории выздоровевших, то есть тех, кто был заражен и либо умер, либо выздоровел и теперь обладает иммунитетом. Модель включает три

дифференциальных уравнения для каждой из трех частей совокупности части:

$$\frac{dS}{dt} = -rSI, \quad (1)$$

$$\frac{dI}{dt} = rSI - aI, \quad (2)$$

$$\frac{dR}{dt} = aI, \quad (3)$$

где a, r – параметры.

Поскольку мы вводим пространственную зависимость в нашу первоначальную модель SIR, нам нужны дополнительные предположения, объясняющие, как люди взаимодействуют с окружающим их пространством. Наше первое предположение заключается в том, что эти восприимчивые группы населения не собираются переезжать, а это означает, что в контексте текущей вспышки COVID-19 мы можем считать, что люди, восприимчивые к этому заболеванию, остаются дома. Вторым предположением является то, что инфекционная миграция происходит с постоянной скоростью. Третье предположение заключается в том, что, как только люди оказываются в отдаленном населенном пункте, они больше не переезжают. Подводя итог, можно сказать, что пространственная зависимость сосредоточена на зараженных, поскольку подозреваемые не перемещаются, и удаленное население также не перемещается, поэтому нас интересует, как болезнь может заразить других, которые собираются мигрировать и могут распространить болезнь среди населения. Важно, что у нас есть дополнительный член dI/dt в уравнении (2) исходной модели SIR. Теперь мы добавляем член D, который является постоянной скоростью диффузии, а затем математически моделируем диффузию, используя производную, чтобы получить вторую производную. Таким образом, уравнение (2) принимает вид

$$\frac{dI}{dt} = rSI - aI + D\frac{\partial^2 I}{\partial x^2}. \quad (4)$$

Поскольку наша популяция зависит как от времени, так и от пространства, получаем уравнения в частных производных

$$\frac{\partial S}{\partial t} = -rSI, \quad (5)$$

$$\frac{\partial I}{\partial t} = rSI - aI + D\frac{\partial^2 I}{\partial x^2}, \quad (6)$$

$$\frac{\partial R}{\partial t} = aI. \quad (7)$$

Частные производные функций переменных S, I и R теперь зависят как от времени, так и от пространства. Что касается анализа, то важно отметить, что переход к безразмерной модели заключается в том, чтобы взять все константы, которые есть в уравнениях (5)–(7), и объединить их таким образом, чтобы получить один ключевой параметр. Базовый репродуктивный показатель R_o показывает количество вторичных инфекций, которые, как ожидается, произойдут в среднем среди населения в результате одной первичной инфекции. Другими словами, – это количество людей, которым, как мы ожидаем, один инфицированный человек передаст болезнь, и мы определяем это математически как $R_o = S_o q$, $q = r/a$, S_o – количество восприимчивых в начале эпидемии, q – доля населения, которая контактирует с инфицированным человеком в период его зараженности. Помимо безразмерности мы можем использовать второй математический трюк, который заключается в изменении переменных. На данный момент у нас есть S, I и R, которые зависят от времени t и пространства x. Если бы мы ввели новую переменную с именем y, то мы преобразовали бы уравнения (5), (6) и (7) в дифференциальные уравнения, включающие только одну новую переменную, которая зависит от x и t:

$$y = x - ct, \quad (8)$$

где c – константа.

Это изменение действительно упростило бы наш набор уравнений

$$0 = c\frac{DS}{dy} - SI, \quad (9)$$

$$0 = \frac{d^2 I}{dy^2} + c\frac{dI}{dy} + I\left(S - \frac{1}{R_o}\right). \quad (10)$$

Уравнения изменились довольно кардинально, поэтому у нас больше нет производных по x и t с частными производными. Мы вернулись к полным производным по одной переменной y. Поскольку теперь нам нужно решить дифференциальные уравнения, нам нужны некоторые граничные или начальные условия. Целесообразно вернуться во времени к началу вспышки. Итак, мы предполагаем, что время в уравнении (8) равно (-∞), что означает возвращение в прошлое, тогда y в том же уравнении будет стремиться к плюс бесконечности из-за знака минус между x и t.

Число случаев заражения должно снизиться до нуля, потому что это было до того, как болезнь появилась среди населения. Кроме того, восприимчивость должна вернуться к своему первоначальному значению – с учетом того, что модель безразмерная, S должно быть равно 1:

$$\begin{aligned} &\textit{Поскольку } t \to -\infty \,(\text{прошлое}), \\ &\text{то } y \to +\infty \text{ тогда } I \to 0,\ S \to 1. \end{aligned} \quad (11)$$

Мы также можем подумать о том, что по нашим ожиданиям произойдет в будущем. Итак, будущее – это когда мы позволим времени t уйти в бесконечность, и это приведет к тому, что y перейдет в минус бесконечность; если y перейдет в (+∞), тогда вспышка, должно быть, прошла так далеко в будущем, что болезнь начала свое

распространение среди населения, и теперь I снова исчезнет, так что зараженность должна снизиться до нуля:

$$\begin{aligned} &\textit{Поскольку } t \to +\infty \,(\text{будущее}), \\ &\text{то } y \to -\infty, \text{ тогда } I \to 0. \quad . \end{aligned} \tag{12}$$

Здесь мы пока не знаем значение S в будущем.

Первый вопрос, на который мы хотим получить ответ – насколько быстро болезнь будет распространяться среди населения. Потому что сейчас мы представляем болезнь как волну, распространяющуюся по населению. Мы можем рассчитать скорость распространения болезни при нашей вспышке. Вопрос в следующем: какова скорость волны? Чтобы ответить на вопрос, мы используем математический инструмент, называемый линеаризацией, в котором мы применим значение S в прошлом в качестве приближения так, что S=1–P, где P – малое значение (приближение), а затем, поскольку мы линеаризуем, подставим S=1–P в уравнения (9) и (10), игнорируя любой член, который равен P в степени 2 и выше, в результате получим следующий набор уравнений:

$$0 = -c\frac{dp}{dy} - I, \tag{13}$$

$$0 = \frac{d^2 I}{dy^2} + c\frac{dI}{dy} + I\left(1 - \frac{1}{R_o}\right). \tag{14}$$

Уравнения (13) и (14) имеют форму, позволяющую нам использовать другой математический инструмент, называемый анализом фазовой плоскости. А применение анализа фазовой плоскости к уравнениям (13) и (14) говорит нам, что решение для бегущей волны существует, тогда

$$c \geq 2\sqrt{1 - \frac{1}{R_o}}. \tag{15}$$

Выражение (15) определяет минимально возможную скорость волны, , для которой существует решение. Обычно скорость волны принимается равной минимальному значению и задается через равенство

$$c = 2\sqrt{1 - \frac{1}{R_o}}. \tag{16}$$

Итак, значение c в формуле замены переменной (8) на самом деле представляет собой скорость бегущей волны и, следовательно, скорость распространения болезни среди населения.

При любой эпидемии, в частности при современной COVID-19, мы хотим снизить скорость c распространения болезни настолько, насколько это возможно; мы хотим замедлить распространение болезни, и, исходя из формулы (16), мы можем уменьшить c, сделав R_o также малым. При $R_o < 1$ c становится отрицательным, но на самом деле этого не может произойти, потому что согласно базовой модели SIR эпидемия возникнет тогда и только тогда, когда R_o будет больше 1. Таким образом, абсолютное меньшее значение, которое может принимать R_o, равно единице, и при подстановке $R_o = 1$ в уравнение (16) получится $c = 0$. Следовательно, мы должны поддерживать R_o на как можно более низком уровне, чтобы снизить скорость распространения болезни. Минимальное значение, к которому мы можем его свести – немногим более единицы, для этого мы смотрим на формулу $R_o = S_o/q$ и видим, что единственное, что мы можем контролировать, – это коэффициент контакта q, поскольку количество зависимых объектов S_o фиксировано. Чтобы снизить количество контактов, нам нужно постоянно мыть руки и как можно больше времени проводить дома, а если нам приходится выходить на улицу, мы должны свести к минимуму количество контактов с помощью социального дистанцирования.

Другой вопрос, на который следовало бы ответить, заключается в том, какова серьезность эпидемии или каково значение количества восприимчивых людей S_{end}, оставшихся в конце вспышки; последнее можно определить из граничных условий в уравнении (9): $SI = c \cdot dS/dy$, и подставить его в уравнение (10). Поскольку члены – производные по dy, то возможно проинтегрировать все уравнение, тогда полученное выражение будет включать только I и S

$$\frac{dI}{dy} + cI + c\left(S - \frac{1}{R_o}\ln S\right) = \text{const}. \tag{17}$$

Чтобы вычислить значение константы, мы должны использовать наши начальные граничные условия в (11). Чтобы найти количество восприимчивых S_{end} на момент окончания вспышки, зная серьезность эпидемии, нам нужно продлить время до бесконечности и, следовательно, устремиться в будущее (12), в результате

$$S_{end} - \frac{1}{R_o}\ln\left(S_{end}\right) = 1. \tag{18}$$

Самый простой и лучший способ справиться с уравнением (18) – это построить график. Сначала мы должны подумать о диапазоне значений, которые могут принимать S_{end} и R_o. Итак, поскольку мы рассматривали

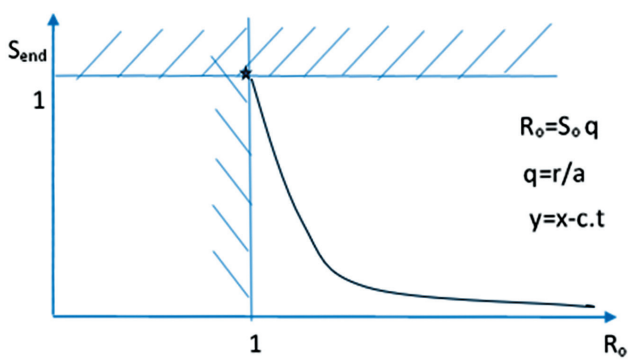


Рис. 1

безразмерную модель, это означает, что S – доля от первоначальной восприимчивой популяции, и поэтому она может варьироваться только от нуля до единицы. В то время как R_o в соответствии с уравнением (16) задает скорость бегущей волны, в первую очередь R_o должно быть больше единицы, чтобы эпидемия возникла, и поскольку мы моделируем распространение эпидемии, это означает, что R_o также должно быть ограничено единицей снизу.

При построении графика для уравнения (18), мы видим быстро уменьшающуюся кривую, поэтому максимальное значение достигается при (S_{end}, R_o) равном (1; 1). Когда значение S_{end} равно единице, это означает, что никто не заразился болезнью, мы можем полагать, что значение S_{end} будет уменьшаться по мере того, как R_o увеличивается.

Итак, возвращаясь к нашему вопросу, какова серьезность эпидемии – в лучшем случае общее число людей, заразившихся этой болезнью, было бы ниже, чем число людей, незатронутых, или количество восприимчивых. Для этого мы хотим сделать S_{end} как можно больше, изменяя $R_{o,}$ что означает, что R_o будет максимально приближено к единице, чего можно добиться, уменьшив коэффициент контакта q.

Заключение

Используя модель бегущей волны для распространения болезни, мы смогли вывести уравнение для скорости волны c в уравнении (16), которое представляет собой скорость, с которой болезнь распространялась бы среди населения. Кроме того, нам удалось получить выражение в уравнении (18), которое определяет количество восприимчивых людей, оставшихся в конце вспышки. Чтобы свести к минимуму тяжесть и последствия такой вспышки, как COVID-19, нам необходимо максимально снизить скорость распространения, чтобы болезнь распространялась как можно медленнее и у нас было больше времени для принятия мер по борьбе с ней, таких как вакцинация. Чтобы сделать это, мы должны сделать R_o как можно меньше, где нижняя граница для R_o равна 1; чтобы приблизить R_o к единице, зная, что R_o пропорционально q, нужно минимизировать q, что снизит скорость распространения болезни. А что касается второго вопроса о степени эпидемической тяжести – уравнения (18) для количества восприимчивых в конце эпидемии – то мы хотим сделать его наибольшим, потому что количество восприимчивых, оставшихся после вспышки, – это количество людей, которые не были затронуты болезнью, и поэтому они не пострадали. Это можно сделать в соответствии с рис. 1, сократив репродуктивный показатель до единицы.

Все ответы говорят нам, что мы должны снизить коэффициент контакта q. Это дает нам один конкретный параметр, который мы хотим сделать как можно меньше. В этом сила математического моделирования, потому что когда мы ввели пространственную зависимость в модель SIR, мы получили различные решения, которые выглядят как бегущие волны. Но все то, чего мы хотим добиться (замедление распространения болезни, уменьшение числа заболевших), имеет одну общую черту: всего этого можно достигнуть, сделав число контактов как можно меньше.

Библиографический список

1. Emerging Pandemics: Connections with Environment and Climate Change (1st ed.) / S. Nazneen, A.L. King Abia, S. Madhav (Eds.). CRC Press, 2023. 180 p.

2. Schulz S., Pastor R., Koyuncuoglu C. et al. Real-time Dissection and Forecast of Infection Dynamics during a Pandemic. 2023. URL: https://www.researchgate.net/publication/369095299_Real-time_Dissection_and_Forecast_of_Infection_Dynamics_during_a_Pandemic (дата обращения 31.03.2025).

3. Frutos R. Chapter 15 – Emergence and dynamics of COVID-19 and future pandemics / In : Omics approaches and technologies in COVID-19. Debmalya Barh (ed.). Academic Press, 2023. Pp. 245-254.

4. Abiodun O., Olukayode A., Ndako J. Mathematical Modeling and Its Methodological Approach: Application to Infectious Disease // 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG), Omu-Aran, Nigeria. 2023. Pp. 1-14.

5. Богданов А.И., Монгуш Б.С., Кузьмин В.А. и др. (2023). Анализ моделей математической теории эпидемий и рекомендации по использованию детерминированных и стохастических моделей // Нормативно-правовое регулирование в ветеринарии. 2023. № 4. С. 37-42.

6. Piqueira J. R. C. Editorial: Epidemic models on networks // Frontiers in Physics. Sec. Social Physics. 2022. Vol. 10. P. 1122070.

7. Cifuentes-Faura J., Faura-Martínez U., Lafuente-Lechuga M. Mathematical Modeling and the Use of Network Models as Epidemiological Tools // Mathematics. 2022. Vol. 10(18). P. 3347. DOI: 10.3390/math10183347

8. Alam N. An analytical technique to obtain traveling wave solutions to nonlinear models of fractional order // Partial Differential Equations in Applied Mathematics. 2023. Vol. 8. P. 100533.

9. Zhang Q., Wu S.-L. Wave propagation of a discrete SIR epidemic model with a saturated incidence rate // Int. J. Biomath. 2019. Vol. 12. P. 1950029. DOI: 10.1142/S1793524519500293

10. Yin Zhang Y., Xiong J., Mao N. Epidemic model of Covid-19 with public health interventions consideration: a review // Authorea. 2023. DOI: 10.22541/au.168539048.84429551/v1

11. Факультет непрерывного образования Оксфордского университета. 2021. «Серия «Динамика пандемии»: доктор Том Кроуфорд». URL: https://www.conted.ox.ac.uk/profiles/tom-crawford (дата обращения 31.03.2025).

References

1. Nazneen S., King Abia A.L., Madhav S, editors. Emerging Pandemics: Connections with Environment and Climate Change (1st ed.). CRC Press; 2023.

2. Schulz S., Pastor R., Koyuncuoglu C. et al. Real-time Dissection and Forecast of Infection Dynamics during a Pandemic. 2023. (accessed 31.03.2025). Available at: https://www.researchgate.net/publication/369095299_Real-time_Dissection_and_Forecast_of_Infection_Dynamics_during_a_Pandemic.

3. Frutos R. Chapter 15 – Emergence and dynamics of COVID-19 and future pandemics. In: Barh D., editor. Omics approaches and technologies in COVID-19. Academic Press; 2023. Pp. 245-254.

4. Abiodun O., Olukayode A., Ndako J. Mathematical Modeling and Its Methodological Approach: Application to Infectious Disease. In: 2023 International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG). Omu-Aran; Nigeria. 2023. Pp. 1-14.

5. Bogdanov A.I., Mongush B.S., Kuzmin V.A., Orekhov D.A., Nikitin G.S., Baryshev A.N., Aidiev A.B., Gulyukin E.A. Analysis of models of the mathematical theory of epidemics and recommendations on the use of deterministic and stochastic models. *Legal regulation in veterinary medicine* 2022;(4):37-42. (in Russ.)

6. Piqueira J. R. C. Editorial: Epidemic models on networks. *Frontiers in Physics. Sec. Social Physics* 2022;10:1122070.

7. Cifuentes-Faura J., Faura-Martínez U., Lafuente-Lechuga M. Mathematical Modeling and the Use of Network Models as Epidemiological Tools. *Mathematics* 2022;10(18):3347. DOI: 10.3390/math10183347.

8. Alam N. An analytical technique to obtain traveling wave solutions to nonlinear models of fractional order. *Partial Differential Equations in Applied Mathematics* 2023;8:100533.

9. Zhang Q., Wu S.-L. Wave propagation of a discrete SIR epidemic model with a saturated incidence rate. *Int. J. Biomath* 2019;12:1950029. DOI: 10.1142/S1793524519500293.

10. Yin Zhang Y., Xiong J., Mao N. Epidemic model of Covid-19 with public health interventions consideration: a review. *Authorea* 2023. DOI: 10.22541/au.168539048.84429551/v1.

11. Department of Continuing Education, University of Oxford. 2021. The Pandemic Dynamics Series: Dr. Tom Crawford. (accessed 03/31/2025). Available at: https://www.conted.ox.ac.uk/profiles/tom-crawford.

Сведения об авторах

Таха Асраа, аспирант кафедры математического и программного обеспечения информационных систем Белгородского государственного национального исследовательского университета, Белгород, Россия

Константинов Игорь Сергеевич, кандидат технических наук, профессор института энергетики, информатики и систем управления, Белгородский государственный технологический университет, Белгород, Россия

Старченко Денис Николаевич, кандидат технических наук, доцент института энергетики, информатики и систем управления, Белгородский государственный технологический университет, Белгород, Россия

About the authors

Taha Asraa, Postgraduate Student, Department of Mathematics and Software in Information Systems, Belgorod State National Research University, Belgorod, Russia

Igor S. Konstantinov, Candidate of Engineering, Professor, Institute of Energy, Computer Science, and Control Systems, Belgorod State Technological University, Belgorod, Russia

Denis N. Starchenko, Candidate of Engineering, Associate Professor, Institute of Energy, Computer Science, and Control Systems, Belgorod State Technological University, Belgorod, Russia

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Проблемы создания доверенной среды разработки и реализации интеллектуальных систем водного транспорта

Matters of trusted development framework creation and implementation of intelligent water transportation systems

Михалевич И.Ф.
Mikhalevich I.F.

Российский университет транспорта (МИИТ), Российская Федерация, Москва
Russian University of Transport (MIIT), Russian Federation, Moscow
mif-orel@mail.ru

Михалевич И.Ф.

Резюме. Цель. *На безопасность интеллектуальных транспортных систем (ИТС) существенное влияние оказывают угрозы нефизической природы. Они могут осуществляться незаконным вмешательством в разработку и реализацию ИТС. Создание доверенной среды разработки и реализации ИТС рассмотрено на примере интеллектуальных систем водного транспорта (ИСВТ).* **Проблемы.** *Указом Президента Российской Федерации ИТС, телекоммуникации и безопасность обработки информации включены в число приоритетных направлений научно-технологического развития. Технологии ИТС и технологии создания доверенного и защищенного системного и прикладного программного обеспечения отнесены к важнейшим наукоемким технологиям критического уровня. Функционирование ИТС связано с масштабным использованием компьютеризированных систем, реализующих новейшие информационные и телекоммуникационные технологии, технологии автоматизированного и автоматического управления, искусственного интеллекта, которые могут нести угрозы безопасности. Создание и функционирование ИТС должны осуществляться в условиях обеспечения доверенной среды их разработки и реализации.* **Методы.** *В работе были использованы методология обеспечения безопасности ИСВТ, разработки безопасных аппаратно-программных платформ автоматизированных систем в защищенном исполнении, методы системного анализа, теории надежности, защиты информации, права.* **Результаты.** *Сформулирована проблема создания доверенной среды разработки и реализации ИСВТ, разработана применимая к ней терминология. Исследовано влияние ИСВТ на безопасность критической информационной инфраструктуры (КИИ) и национальную безопасность, разработана модель отношений областей безопасности ИСВТ, учитывающая угрозы физического и нефизического происхождения. Приведены примеры компьютерных инцидентов в ИСВТ, повлекших последствия национального и межнационального уровня. Определен состав объектов ИСВТ, относимых к КИИ, приведены критические процессы, осуществляемые типовыми объектами КИИ в составе ИСВТ. Сформирован перечень концептуальных проблем обеспечения безопасности ИСВТ и сформулированы принципы создания доверенной среды разработки и реализации ИСВТ.* **Заключение.** *Обеспечение безопасности ИСВТ в условиях современных угроз требует решения проблем создания доверенной среды разработки и реализации ИСВТ. Для повышения оперативности и качества их решения предложена интуитивно понятная терминология, отражающая предметную область и позволяющая повысить уровень взаимопонимания проблем безопасности специалистов из различных сфер деятельности. Объекты ИСВТ оказывают влияние на безопасность КИИ и национальную безопасность в целом. Это учтено в модели отношений областей безопасности ИСВТ, показано на примерах компьютерных инцидентов в ИСВТ, повлекших последствия национального и межнационального уровня. С учетом вышеизложенного сформирован состав объектов ИСВТ, относимых к КИИ, и приведены примеры критических процессов, осуществляемых типовыми объектами КИИ в составе ИСВТ. Расширение ландшафта угроз безопасности ИСВТ небезопасными программным обеспечением, аппаратно-программными платформами, программно-аппаратными комплексами и новейшими технологиями учитывает сформированный перечень концептуальных проблем обеспечения безопасности ИСВТ При разработке принципов создания доверенной среды разработки и реализации ИСВТ учтен опыт успешного внедрения методологии создания национальных защищенных аппаратно-программных платформам объектов КИИ, обеспечившей создание автоматизированных систем в защищенном исполнении различного назначения на основе отечественных решений. Рассмотренные проблемы носят системный характер, что позволяет использо-*

вать полученные результаты при разработке и реализации ИТС других видов транспорта.
Abstract. Aim. *Threats of a non-physical nature have a significant effect on the security of intelligent transportation systems (ITS). They may have the form of unlawful interference in the development and implementation of ITS. The creation of a trusted framework for the development and implementation of ITS is examined as in the case of intelligent water transportation systems (IWTS).* **Problems.** *By decree of the President of the Russian Federation, ITS, telecommunications and security of information processing are among the priority areas of scientific and technological development. ITS technologies, as well as those involved in the creation of trusted, secure system and application software are among the most important critical high technologies. The operation of ITS involves wide use of computerised systems that implement the latest information and telecommunication technologies, automated and automatic control technologies, artificial intelligence that can pose security threats. ITS are to be developed and operated in a trusted environment.* **Methods.** *The paper used the methodology for ensuring the security of IWTS, development of secure hardware and software platforms for secure automated systems, methods of system analysis, dependability theory, information protection, and law.* **Results.** *The paper defines the problem of creating a trusted framework for the development and implementation of IWTS, the applicable terminology is developed. The author examined the effect of IWTS on the security of critical information infrastructure (CII) and national security, developed a model of relationships between the IWTS security domains taking into account threats of physical and non-physical origin. Examples of computer incidents within IWTS that caused consequences at the national and international levels are given. The composition of the IWTS facilities attributed to CII is defined, critical processes implemented by standard CII facilities as part of the IWTS are set forth. The author lists conceptual problems of IWTS security, defines the principles of creating a trusted framework for the development and implementation of IWTS.* **Conclusion.** *Ensuring the security of IWTS against modern threats requires solving a number of problems associated with the creation of a trusted framework for the development and implementation of IWTS. For the purpose of improving the timeliness and quality of their solution, the paper proposes an intuitive terminology that reflects the subject area and helps finding a common understanding of the security domain by experts from various industries. IWTS facilities have an effect on CII security and national security in general. That is taken into account in the model of relationships between IWTS security domains, demonstrated using cases of computer incidents within IWTS that caused consequences at the national and international level. Given the above, the paper lists IWTS facilities attributed to CII and sets forth examples of critical processes implemented by standard CII facilities as part of the IWTS. The defined list of conceptual IWTS security problems take into account the growing landscape of IWTS security threats that includes insecure software, hardware and software platforms, software and hardware systems and emerging technologies. When developing the principles for the creation of a trusted IWTS development and implementation framework, the author took into account the best practice of implementing the methodology for creating national secure hardware and software platforms of CII facilities that enables the creation of secure automated systems for various applications that are based on domestically-developed solutions. The examined matters are of a systemic nature, which allows using the findings in the development and implementation of ITS in other modes of transportation.*

Ключевые слова: *безэкипажное (автономное) судно, искусственный интеллект, компьютерная атака, компьютерный инцидент, угроза.*
Keywords: *unmanned (autonomous) vessel, artificial intelligence, computer attack, computer incident, threat.*

Для цитирования: *Михалевич И.Ф. О Проблемы создания доверенной среды разработки и реализации интеллектуальных систем водного транспорта // Надежность. 2025. №2. С. 39-47. https://doi.org/10.21683/1729-2646-2025-25-2-39-47*
For citation: *Mikhalevich I.F. Matters of trusted development framework creation and implementation of intelligent water transportation systems. Dependability 2025;2:39-47. https://doi.org/10.21683/1729-2646-2025-25-2-39-47*

Поступила: *24.11.2024* / **После доработки:** *10.12.2024* / **К печати:** *09.06.2025*
Received on: *24.11.2024* / **Revised on:** *10.12.2024* / **For printing:** *09.06.2025*

Введение

Указом Президента Российской Федерации от 18 июня 2024 года № 529[1] утверждены приоритетные направления научно-технологического развития страны и перечни важнейших наукоемких технологий. Интеллектуальные транспортные системы (ИТС) и телекоммуникации, безопасность получения, хранения, передачи и обработки информации включены в число приоритетных направлений научно-технологического развития. Транспортные технологии для различных сфер применения (море, земля, воздух), в том числе беспилотные и автономные системы, отнесены к важнейшим наукоемким технологиям критического уровня. К критическим наукоемким технологиям отнесены также технологии создания доверенного и защищенного системного и прикладного программного обеспечения (ПО).

Функционирование ИТС связано с масштабным использованием компьютеризированных систем, реализующих новейшие информационные и телекоммуникационные технологии, технологии автоматизированного и автоматического управления, искусственного интеллекта (ИИ) (далее – новейшие технологии), которые могут нести угрозы безопасности. В связи с этим создание и функционирование ИТС должны осуществляться в условиях обеспечения доверенной среды их разработки и реализации.

Проблемы создания доверенной среды разработки и реализации ИТС рассмотрим на примере интеллектуальных систем водного транспорта (ИСВТ).

[1] Указ Президента РФ от 18.06.2024 № 529 «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоемких технологий».

1. Терминология в области проблем создания доверенной среды разработки и реализации ИСВТ

Под ИСВТ (рис. 1) будем понимать систему управления, интегрирующую современные информационные, телематические, телекоммуникационные технологии, ИИ и предназначенную для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления водным транспортным комплексом, конкретным судном или группой судов, объектами водной инфраструктуры с целью обеспечения заданной мобильности населения, максимизации показателей использования водных путей, повышения безопасности и эффективности транспортного процесса, комфортности для судоводителей и пользователей водного транспорта (с учетом[2,3]).

При решении задач создания доверенной среды разработки и реализации ИСВТ предлагается использовать следующие определения терминов:

• обработка информации – любые действия по сбору, накоплению, вводу, выводу, приему, передаче, записи, хранению, регистрации, преобразованию, отображению информации, совершаемые с заданной целью (с учетом[4,5]). Отметим, что в определенных случаях

[2] ГОСТ Р 56829-2015. Интеллектуальные транспортные системы. Термины и определения.

[3] ПНСТ 555-2021. Интеллектуальные транспортные системы. Системы искусственного интеллекта для автоматизации управления автомобильными транспортными средствами. Классификация и общие технические требования.

[4] ГОСТ Р 51624-2000. Автоматизированные информационные системы в защищенном исполнении. Общие положения.

[5] ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

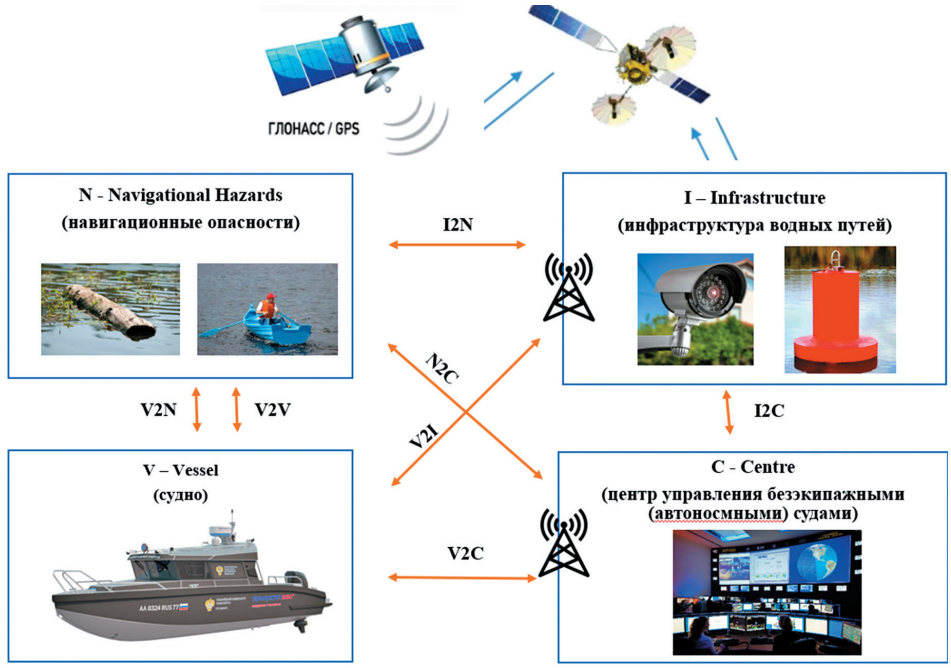


Рис. 1. Базовая конфигурация ИСВТ

Рис. 2. Связь областей безопасности компьютеризированных систем ИСВТ

целью таких действий или бездействия может быть нарушение безопасности ИСВТ;

• безопасность ИСВТ – состояние защищенности объектов инфраструктуры водных путей и судов, процессов их проектирования, производства, строительства и эксплуатации от актов незаконного вмешательства (АНВ) (с учетом[6,7]);

• акт незаконного вмешательства в ИСВТ – любое противоправное действие или бездействие, в том числе компьютерная атака, угрожающие безопасности ИСВТ, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшие угрозу наступления таких последствий (с учетом[3,4]);

• компьютерная атака в ИСВТ – целенаправленное воздействие программных и (или) программно-аппаратных средств на информационные системы (ИС), автоматизированные системы управления (АСУ), системы автоматического управления (САУ), системы ИИ (СИИ), информационно-телекоммуникационные сети (ИТКС), сети электросвязи морских и речных судов, портов и иных объектов ИСВТ в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, обрабатываемой указанными объектами (с учетом[8]);

• компьютерный инцидент в ИСВТ – факт нарушения и (или) прекращения функционирования ИС, АСУ, САУ, СИИ, ИТКС, сети электросвязи морских и речных судов, портов и иных объектов ИСВТ и (или) нарушения безопасности информации, обрабатываемой объектом ИСВТ, в том числе произошедший в результате компьютерной атаки (с учетом[7]);

• доверие к ИСВТ – степень уверенности граждан, бизнеса, органов власти и других заинтересованных лиц в том, что ИСВТ будет выполнять свои функции так, как это предполагалось (с учетом[9]);

• доверенные ПО, аппаратно-программные платформы (АПП), программно-аппаратные комплексы (ПАК), технологии ИСВТ – ПО, АПП, ПАК, технологии ИСВТ, отвечающие стандартам безопасности ИСВТ, разработанные с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку и нарушения его основополагающих прав и свобод, нанесение ущерба интересам общества и государства (с учетом[8]);

• доверие к безопасности ИСВТ – степень уверенности граждан, бизнеса, органов власти и других заинтересованных лиц в том, что безопасность ИСВТ будет обеспечена на заявленном уровне;

• доверенная среда разработки и реализации ИСВТ – среда, отвечающая принципам доверия к безопасности ИСВТ, требованиям по разработке безопасных ПО, АПП, ПАК, технологий ИСВТ (с учетом[10]).

[6] Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности».

[7] ГОСТ Р 56461-2015 «Безопасность транспортная. Общие требования».

[8] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[9] ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии (ИТ). Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов

[10] ГОСТ Р 56939-2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования

Табл. 1. Компьютерные инциденты на объектах ИСВТ (примеры, по сводкам [6])

Порт/ страна	Роль порта в экономике	Дата (период) / способ / цель атаки	Последствия	Сумма ущерба
Нагоя / Япония	10% от общего объема торговли Японии, в среднем 10 000 единиц грузов в день	05.07.2023 / шифрование информации АСУ грузовыми операциями / получение выкупа	2 суток простоя грузовых терминалов	Сведения отсутствуют, признается национальный уровень инцидента
Сидней, Мельбурн, Брисбен, Фримантле / Австралия	40% общего объема грузов Австралии	10.11.2023 / шифрование информации АСУ грузовыми операциями / получение выкупа	3 суток простоя грузовых терминалов	Сведения отсутствуют, признается национальный уровень инцидента
Дурбане/ ЮАР	более 60% грузооборота ЮАР, второй по величине контейнерный порт в южной Африке	22.07.2021 / шифрование информации АСУ грузовыми операциями / получение выкупа	7 суток простоя грузовых терминалов	Выкуп более 200 000 долларов США, признается межнациональный уровень инцидента
Роттердам / Нидерланды	Первое и второе место среди портов Европы по грузообороту в 2023г.	2011-2013 / подмена данных о контейнерах с наркотиками и оружием / контрабанда	Изменение местоположения и времени доставки контейнеров	200 000 евро на контрмеры
Антверпен / Бельгия				

2. Влияние ИСВТ на безопасность критической информационной инфраструктуры и национальную безопасность

В соответствии с федеральным законом о безопасности критической информационной инфраструктуры[8] (КИИ), ИСВТ входят в состав КИИ. В ИСВТ, следуя закону, объектами КИИ являются ИС, АСУ, САУ, СИИ, ИТКС, сети электросвязи, созданные (создаваемые) в целях обеспечения функционирования морских и речных судов, портов, пристаней, иных объектов инфраструктуры водных путей, технологических и административных центров управления и иных объектов ИСВТ, использующих компьютеризированные системы.

Модель отношений областей безопасности ИСВТ приведена на рис. 2.

В [1, 2] рассмотрены концептуальные проблемы обеспечения безопасности ИСВТ, состав которых представим следующим перечнем:

• расширение ландшафта угроз безопасности ИСВТ за счет АНВ нефизического характера [3–5]. Невыявленные (или) неустраненные уязвимости ИСВТ приводят к компьютерным инцидентам, последствия которых могут достигать национальных и межнациональных масштабов (табл. 1) [6];

• несовершенство нормативной правовой базы обеспечения безопасности ИСВТ, создающее правовой разрыв между физическими и нефизическими областями регулирования, вследствие чего в планах обеспечения безопасности объектов ИСВТ могут быть пропущены актуальные угрозы [7];

• наличие противоречий в международных документах по обеспечению безопасности морского транспорта с российским законодательством о безопасности КИИ, что затрудняет процессы исполнения;

• запутанность кибертерминологии, затрудняющая понимание причин компьютерных инцидентов в ИСВТ [8];

• низкий уровень публичного раскрытия информации о имевших место компьютерных инцидентах в ИСВТ [9–11];

• несоблюдение на объектах ИСВТ цифровой гигиены;

• цифровое неравенство в защищенности автоматизированных систем технологического и корпоративного управления ИСВТ, повышающее в интегрированных системах управления риски реализации угроз комплексного характера, в том числе со стороны ИИ [12-14].

Критические процессы, осуществляемые типовыми объектами КИИ в составе ИСВТ, приведены в табл. 2 (с учетом[11,12]).

В связи с вышеизложенным перечень концептуальных проблем обеспечения безопасности ИСВТ дополняет проблемы создания доверенной среды разработки и реализации ИСВТ. Для их решения сформулированы приведенные ниже принципы.

3. Принципы создания доверенной среды разработки и реализации ИСВТ

В соответствии с ГОСТ Р 51624-2000[13] объекты ИСВТ относятся к автоматизированным системам в защищенном исполнении (АСЗИ) и должны создаваться в

[11] Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утв. Минтрансом России 15.05.2024).

[12] Методические рекомендации по категорированию объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утв. Минтрансом России 24.01.2024). URL: https://mintrans.gov.ru/documents/10/13201?ysclid=lu2cx9gfse525544140. (дата обращения 10.03.2024).

[13] ГОСТ Р 51624-2000. Автоматизированные информационные системы в защищенном исполнении. Общие положения.

Табл. 2. Типовые объекты КИИ в составе ИСВТ

№ п/п	Типовые объекты КИИ в составе ИСВТ	Критические процессы, осуществляемые типовым объектом КИИ в составе ИСВТ
1	Информационные системы, предназначенные для контроля деятельности морского пассажирского транспорта.	Контроль за деятельностью морского и внутреннего водного пассажирского транспорта. Контроль перевозки пассажиров в морских и прибрежных водах, осуществляемой по расписанию либо вне расписания. Контроль за деятельностью экскурсионных, круизных или прогулочных судов. Контроль за перевозкой пассажиров на паромах, водных такси. Контроль за перевозкой пассажиров по морским трассам на судах смешанного (река – море) плавания.
2	Информационные системы, обеспечивающие контроль деятельности морского и внутреннего грузового транспорта	Контроль за деятельностью морского и внутреннего грузового транспорта. Контроль за перевозкой грузов в морских и прибрежных водах, осуществляемой по расписанию либо не по расписанию. Контроль за деятельностью судов заграничного плавания. Контроль за деятельностью судов каботажного плавания. Контроль за деятельностью судов речного плавания.
3	Информационные системы, предназначенные для обеспечения судоходства в морских и прибрежных водах, включая лоцманскую проводку судов	Обеспечение безопасного судоходства в морских и прибрежных водах. Обеспечение лоцманской проводки судов.
4	Автоматизированные системы, предназначенные для управления деятельностью по навигационному обеспечению судоходства на морском и внутреннем водном транспорте	Предоставление картографической информации. Определение местоположения судов морского и внутреннего водного плавания. Контроль маршрута вне зоны покрытия GSM-связи.
5	Автоматизированные системы, обеспечивающие управление погрузочными станциями в портах	Сбор и обработка информации о состоянии технологических параметров. Обнаружение, сигнализация и регистрация аварийных ситуаций. Контроль доступа в основные складские помещения. Архивирование истории изменения параметров. Формирование и выдача оперативных и архивных данных персоналу. Дистанционное управление запорно-регулирующей арматурой (задвижки). Дистанционное управление насосными агрегатами. Управление процессом слива/налива нефтепродуктов: автоматическое открытие/закрытие задвижек с целью обеспечения требуемого маршрута слива/налива. Диагностика состояния программно-технических средств управления.
6	Автоматизированные системы, предназначенные для управления аварийно-спасательной и судоподъемной деятельностью на морском транспорте	Контроль сигналов о бедствии от судов морского и внутреннего водного плавания. Автоматизация управления аварийно-спасательной деятельности. Осуществление работ по подъему судов морского плавания.
7	Автоматизированные системы, обеспечивающие управление ледокольными судами	Контроль параметров ледокольных судов. Отображение информации о контролируемых параметров ледокольных судов операторам. Обеспечение проводки судов во льдах. Обеспечение прокладки маршрутов во льдах. Обеспечение спасательных работ во льдах. Управление распределением электроэнергии между потребителями. Управление техническими средствами и системами обитаемости и жизнеобеспечения. Управление техническими средствами и системами борьбы с пожарами. Управление техническими средствами и системами грузовых и балластных систем.

Табл. 2. Типовые объекты КИИ в составе ИСВТ (окончание)

№ п/п	Типовые объекты КИИ в составе ИСВТ	Критические процессы, осуществляемые типовым объектом КИИ в составе ИСВТ
8	Интегрированные системы, обеспечивающие комплексную автоматизацию судна	Обеспечение безопасного судовождения речных и морских судов. Управление динамическим позиционированием речных и морских судов. Управление дизельными и электрическими установками речных и морских судов. Управление распределением электроэнергии между потребителями. Управление техническими средствами и системами обитаемости и жизнеобеспечения. Управление техническими средствами и системами борьбы с пожарами. Управление техническими средствами и системами грузовых и балластных систем. Управление техническими средствами и системами обеспечения экологической чистоты и экологической безопасности судна.

Табл. 3. Принципы создания доверенной среды разработки и реализации ИСВТ

Наименование	Описание
Безопасность	недопустимость использования АПП, создающих угрозы безопасности информации ИСВТ или угрозы нарушения (прекращения) функционирования ИСВТ вследствие применения информации, безопасность которой была нарушена
Защищенность	безопасность и правовая охрана решений в области АПП для ИСВТ, разграничение ответственности организаций – разработчиков АПП и пользователей АПП, а также защита указанных пользователей от негативного влияния АПП на функционирование и безопасность ИСВТ и взаимодействующих с ними иных объектов КИИ
Контролируемость	наличие полного комплекта документации на АПП, в том числе о соответствии всех компонентов АПП и процессов достижения результатов их работы по отдельности и совместно в составе вычислительных систем (ПАК) требованиям по безопасности
Технологический суверенитет	преимущественное использование отечественных решений в области АПП, независимость от импорта и технологическая независимость: обеспечение полноценности, способности сохранять заявленные характеристики, развиваться и поддерживаться независимо от внешнеполитических и внешнеэкономических факторов, без применения импортных компонентов, без иностранного участия, принудительного обновления компонентов и управления из-за рубежа, передачи информации, в том числе технологической, за пределы РФ
Полноценность	обеспечение полноты состава АПП, необходимого для функционирования ИСВТ различного назначения, разных классов защищенности, уровней топологической и архитектурной сложности
Промышленный уровень	обеспечение необходимого уровня производительности, отказоустойчивости и других заявленных характеристик ИСВТ сложных топологии и архитектуры, при высоких нагрузках и больших объемах данных в течение всего срока эксплуатации
Универсальность	обеспечение на основе собственных базовых компонентов создание (модернизацию) ИСВТ различного назначения, разных классов защиты и уровней топологической и архитектурной сложности
Гарантии развития и поддержки	обеспечение развития, эксплуатации, обслуживания и модернизации ИСВТ, созданных на основе АПП
Совместимость	обеспечение необходимого уровня аппаратной и программной совместимости компонентов АПП, включенных в вычислительную систему (ПАК), возможность создания на их основе интегрированной программной среды (экосистемы)
Гибкость	обеспечение возможности создания разнообразных архитектур вычислительных систем (ПАК) на основе компонентов АПП
Оперативность	обеспечение сокращения сроков перехода от научного или прикладного исследования к созданию вычислительных систем (ПАК)
Преемственность (наследование)	обеспечение постепенного перехода на отечественное специальное программное обеспечение (СПО) путем последовательного замещения СПО, функционирующего под управлением операционных систем (ОС) из недружественных стран (унаследованное ПО)
Целостность инновационного цикла	обеспечение тесного взаимодействия научных исследований и разработок в области АПП с реальными потребностями ИСВТ
Поддержка конкуренции	развитие рыночных отношений и недопустимость действий, направленных на монополизацию и ограничение конкуренции между российскими организациями, осуществляющими деятельность в области АПП

порядке, установленном ГОСТ Р 51583-2014[14], с учетом ГОСТ 56939-2024.

В [15] приведена методология создания национальных защищенных аппаратно-программных платформ объектов КИИ, основанная на Концепции создания доверенной среды функционирования АСЗИ [16], реализованной с учетом [17, 18] при создании и внедрении АПП типовых технических решений построения АСЗИ. Концепция и методология были успешно реализованы при создании АСЗИ различного назначения. На их основе разработаны принципы создания доверенной среды разработки и реализации ИСВТ, описание которых приведено в табл. 3.

Заключение

Обеспечение безопасности ИСВТ в условиях современных угроз требует решения проблем создания доверенной среды разработки и реализации ИСВТ. Для повышения оперативности и качества их решения предложена интуитивно понятная терминология, отражающая предметную область и позволяющая повысить уровень взаимопонимания проблем безопасности специалистов из различных сфер деятельности.

Объекты ИСВТ оказывают влияние на безопасность КИИ и национальную безопасность в целом. Это учтено в модели отношений областей безопасности ИСВТ, показано на примерах компьютерных инцидентов в ИСВТ, повлекших последствия национального и межнационального уровня. С учетом вышеизложенного сформирован состав объектов ИСВТ, относимых к КИИ, и приведены примеры критических процессов, осуществляемых типовыми объектами КИИ в составе ИСВТ.

Расширение ландшафта угроз безопасности ИСВТ небезопасными ПО, АПП, ПАК и новейшими технологиями учитывает сформированный перечень концептуальных проблем обеспечения безопасности ИСВТ.

При разработке принципов создания доверенной среды разработки и реализации ИСВТ учтен опыт успешного внедрения методологии создания национальных защищенных АПП объектов КИИ, обеспечившей создание АСЗИ различного назначения на основе отечественных решений.

Рассмотренные проблемы носят системный характер, что позволяет использовать полученные результаты при разработке и реализации ИТС других видов транспорта.

Библиографический список

1. Михалевич И.Ф. Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем // Надежность. 2024. № 2. С. 72-87. DOI: 10.21683/1729-2646-2024-24-2-72-87

2. Михалевич И.Ф. Проблемы обеспечения безопасности автономного судоходства на внутренних водных путях. М.: Горячая линия – Телеком, 2024. 336 с.

3. 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

4. Шубинский И.Б. Надежность, риски, безопасность систем управления на железнодорожном транспорте / И.Б. Шубинский, Е.Н. Розенберг, А.В. Бочков. М.; Вологда: Инфра-Инженерия, 2024. 416 с.

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

6. Maritime Cyber Attack Database (MCAD). URL: https://maritimecybersecurity.nl/ (дата обращения 30.03.2025).

7. Семенов С.А. Кибербезопасность морского и речного транспорта // Транспорт Российской Федерации. 2018. № 1(74). С. 43-46.

8. 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.

9. Annual Threat Assessment 2024. The Nordic Maritime Cyber Resilience Centre. URL: https://static1.squarespace.com/static/5fae4682cc2b52123f436f99/t/6614e6a60fbde93c9dfdc4e3/1712645824622/Norma+Cyber+Annual+Threat+Assessment+-+Spreads.pdf (дата обращения 30.03.2025).

10. Q2 2024 – a brief overview of the main incidents in industrial cybersecurity. Kaspersky ICS CERT Analytical Report/. URL: https://ics-cert.kaspersky.com/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/ (дата обращения 30.03.2025).

11. Threat landscape for industrial automation systems. Q2 2024. Kaspersky ICS CERT Analytical Report/ URL: https://ics-cert.kaspersky.com/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024/ (дата обращения 30.03.2025).

12. Намиот Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность // International Journal of Open Information Technologies. 2022. Vol. 10. No. 9. Pp. 135-147.

13. Yamin M.M. et al. Weaponized AI for cyber attacks // Journal of Information Security and Applications. 2021. Vol. 57. P. 102722. DOI: 10.1016/j.jisa.2020.102722

14. Nwakanma C.I., Ahakonye L.A.C., Njoku J.N. et al. Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review // Appl. Sci. 2023. Vol. 13. P. 1252. DOI: 10.3390/app13031252

15. 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.

16. Михалевич И.Ф. Проблемы создания доверенной среды функционирования автоматизированных систем управления в защищенном исполнении /В сб.: Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). М.: Институт проблем управления им. В.А. Трапезникова РАН, 2014. С. 9201-9207.

17. Зегжда Д.П., Ивашко А.М. К созданию защищенных систем обработки информации // Проблемы информаци-

[14] ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

онной безопасности. Компьютерные системы. 1999. № 1. С. 99-107.

18. Зегжда Д.П., Ивашко А.М. Технология создания безопасных систем обработки информации на основе отечественной защищенной операционной системы // Проблемы информационной безопасности. Компьютерные системы. 1999. № 2. С. 59-66.

References

1. Mikhalevich I.F. Conceptual problems of transportation security of intelligent water transportation systems. *Dependability* 2024;24(2):72-87. (in Russ.) DOI: 10.21683/1729-2646-2024-24-2-72-87.

2. Mikhalevich I.F. [Challenges in ensuring safe autonomous navigation on inland waterways]. Moscow: Goriachaya liniya – Telekom; 2024. (in Russ.)

3. 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. (in Russ.) DOI: 10.21683/1729-2646-2023-23-3-38-45.

4. Shubinsky I.B., Rozenberg E.N, Bochkov A.V. [Dependability, risks, safety of control systems in railway transportation]. Moscow; Vologda: Infra-Engineering; 2024. (in Russ.)

5. Shubinsky I.B., Rozenberg E.N. [Functional safety of control systems in railway transportation]. Moscow; Vologda: Infra-Inzheneria; 2023. (in Russ.)

6. Maritime Cyber Attack Database (MCAD). (accessed 30.03.2025). Available at: https://maritimecybersecurity.nl/.

7. Semenov S.A. [Cybersecurity of sea and river transport]. *Transport Rossiuskoy Federatsii* 2018;1(74):43-46. (in Russ)

8. 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).

9. Annual Threat Assessment 2024. The Nordic Maritime Cyber Resilience Centre. (accessed 30.03.2025). Available at: https://static1.squarespace.com/static/5fae4682cc2b52123f436f99/t/6614e6a60fbde93c9dfdc4e3/1712645824622/Norma+Cyber+Annual+Threat+Assessment+-+Spreads.pdf.

10. Q2 2024 – a brief overview of the main incidents in industrial cybersecurity. Kaspersky ICS CERT Analytical Report. (accessed 30.03.2025). Available at: https://ics-cert.kaspersky.com/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity.

11. Threat landscape for industrial automation systems. Q2 2024. Kaspersky ICS CERT Analytical Report/ (accessed 30.03.2025). Available at: https://ics-cert.kaspersky.com/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024.

12. Namiot D., Ilyushin E., Chizov I. Artificial intelligence and cybersecurity. *International Journal of Open Information Technologies* 2022;10(9):135-147. (in Russ.)

13. Yamin M.M. et al. Weaponized AI for cyber attacks. *Journal of Information Security and Applications* 2021;57:102722. DOI: 10.1016/j.jisa.2020.102722.

14. Nwakanma C.I., Ahakonye L.A.C., Njoku J.N. et al. Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review. *Appl. Sci.* 2023;13:1252. DOI: 10.3390/app13031252.

15. 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.).

16. Mikhalevich I.F. [Challenges in creating a trusted environment for the operation of secure automated control systems]. In: Proceedings of the XII All-Russian Meeting on Management Problems (VSPU-2014, Moscow). Moscow: V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences; 2014. Pp. 9201-9207. (in Russ.)

17. Zegzhda D.P., Ivashko A.M. [Towards the creation of secure information processing systems]. *Information Security Problems. Computer Systems* 1999;1:99-107. (in Russ.)

18. Zegzhda D.P., Ivashko A.M. [Process of creating secure information processing systems using a domestically-developed secure operating system]. *Information Security Problems. Computer Systems* 1999;2:59-66. (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, 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, bldg. 9 Obraztsova str., Moscow, Russian Federation, e-mail: mif-orel@mail.ru

Вклад автора в статью

Автором сформулирована проблема создания доверенной среды разработки и реализации ИСВТ и разработана применимая к ней терминология. Исследовано влияние ИСВТ на безопасность критической информационной инфраструктуры и национальную безопасность, разработана модель отношений областей безопасности ИСВТ, учитывающая угрозы физического и нефизического происхождения. Приведены примеры компьютерных инцидентов в ИСВТ, повлекших последствия национального и межнационального уровня. Определен состав объектов ИСВТ, относимых к критической информационной инфраструктуре, приведены критические процессы, осуществляемые типовыми объектами КИИ в составе ИСВТ. Сформирован перечень концептуальных проблем обеспечения безопасности ИСВТ и сформулированы принципы создания доверенной среды разработки и реализации ИСВТ. Предложено распространить полученные результаты на ИТС других видов транспорта.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

1980

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

1990

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

1960

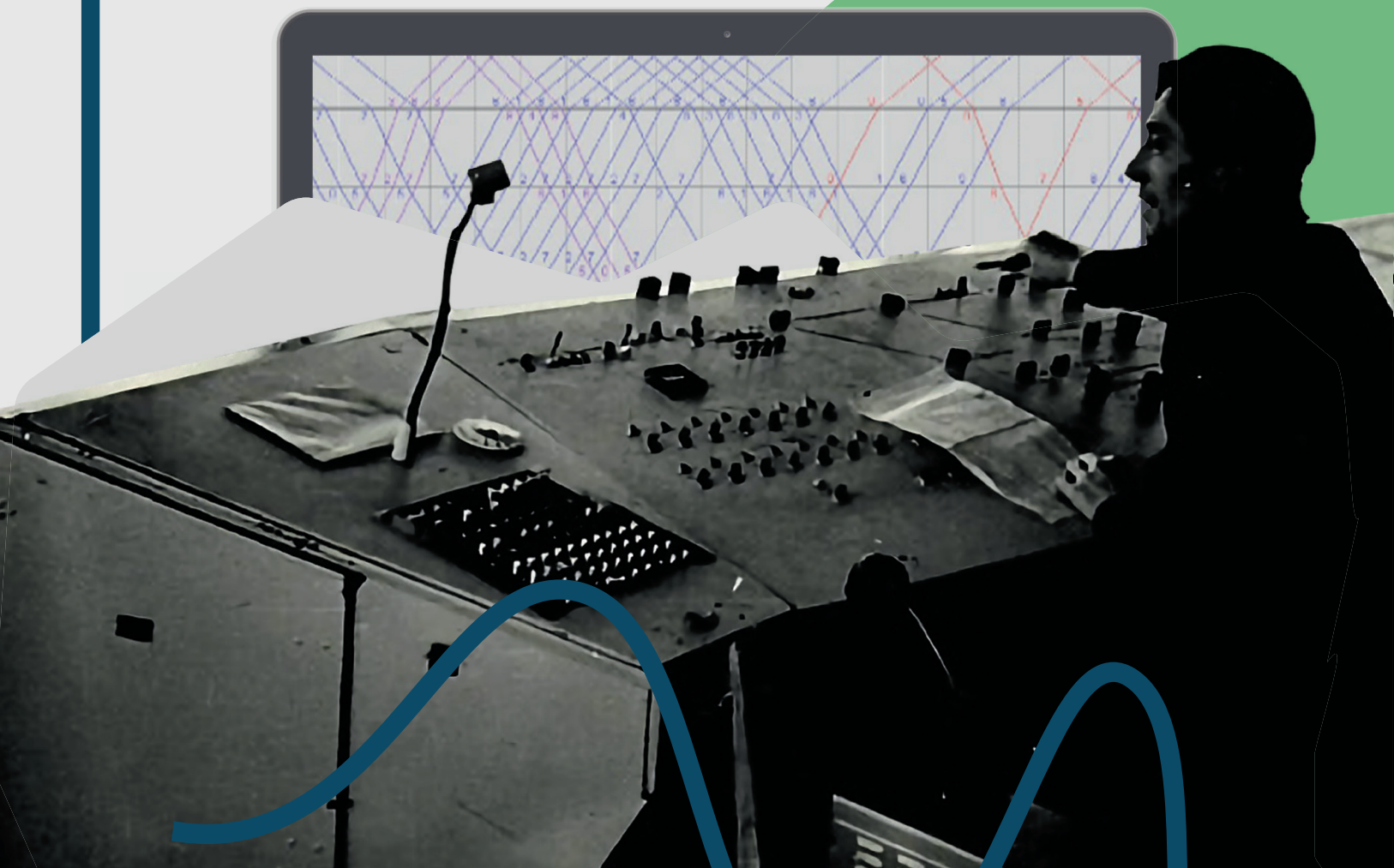
Разработаны и внедрены отечественные системы автоматической локомотивной сигнализации.

1956

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

1970

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



2000

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

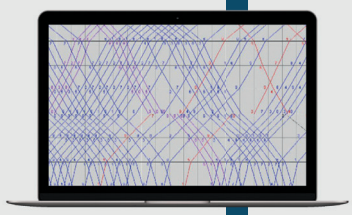
НИИАС

2010

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

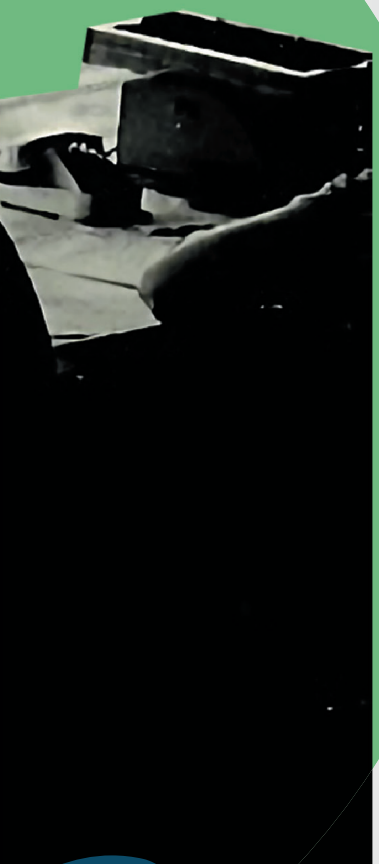
2020

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



2025

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



niias.ru

vniias_official

УДК 004.891.2
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-50-58

Теория игр для автономных систем искусственного интеллекта при управлении корпорациями

Game theory for autonomous AI systems in corporate governance

Романова А.С.[1]
Romanova A.S.[1]

[1] *Московский физико-технический институт (национальный исследовательский университет), аспирант, г. Москва, Российская Федерация, romanova.as@phystech.edu, ORCID 0009-0004-4649-6037*
[1] *Moscow Institute of Physics and Technology (National Research University), Postgraduate Student, Moscow, Russian Federation, romanova.as@phystech.edu, ORCID 0009-0004-4649-6037*
romanova.as@phystech.edu

Романова А.С.

Резюме. *Несмотря на то, что современные технологии искусственного интеллекта в значительной степени основаны на машинном обучении, сами по себе алгоритмы машинного обучения стратегией не являются. Стратегией мы будем называть полное описание того, как система будет себя вести при всех возможных обстоятельствах. Наиболее перспективным инструментом, позволяющим автономным системам принимать эффективные решения при управлении корпорациями, представляется теория игр. Учитывая разнообразие проблем, с которыми приходится сталкиваться советам директоров, теория игр, нашедшая свое применение в экономике, политологии, чистой математике, психологии, социологии, маркетинге и финансах, предоставляет возможность обеспечивать автономность системы искусственного интеллекта на основе моделирования эффективной стратегии. Обязательное требование о разработке этичных и легитимных автономных систем искусственного интеллекта может привести к тому, что некоторые дилеммы самой теории игр для автономных систем или не существуют, или изменяют свой смысл.*
Abstract. *Despite the fact that modern artificial intelligence technologies are largely based on machine learning, machine learning algorithms themselves are not a strategy. We will define a strategy as a complete description of how a system will behave under all possible circumstances. Game theory appears to be the most promising tool that allows autonomous systems to make effective decisions when managing corporations. Given the variety of problems faced by boards of directors, game theory that has found application in economics, political science, pure mathematics, psychology, sociology, marketing and finance, potentially enables an autonomous artificial intelligence system based on effective strategy simulation. If the development of ethical and legitimate autonomous AI systems is mandatory, some dilemmas of game theory itself either become nonexistent or change their meaning in the context of game theory.*

Ключевые слова: *теория игр, искусственный интеллект, алгоритмические решения, корпоративное управление, андроиды.*
Keywords: *game theory, artificial intelligence, algorithmic solutions, corporate governance, androids.*

Для цитирования: *Романова А.С. Теория игр для автономных систем искусственного интеллекта при управлении корпорациями // Надежность. 2025. №2. С. 50-58. https://doi.org/10.21683/1729-2646-2025-25-2-50-58*
For citation: *Romanova A.S. Game theory for autonomous AI systems in corporate governance. Dependability 2025;2:50-58. https://doi.org/10.21683/1729-2646-2025-25-2-50-58*

Поступила: *11.11.2024* / **После доработки:** *16.12.2024* / **К печати:** *09.06.2025*
Received on: *11.11.2024* / **Revised on:** *16.12.2024* / **For printing:** *09.06.2025*

Введение

Современные технологии искусственного интеллекта (далее – ИИ) в значительной степени основываются на алгоритмах машинного обучения, однако алгоритмы машинного обучения нельзя назвать стратегией. Стратегией называется полное описание того, как система будет себя вести при всех возможных обстоятельствах [1]. Теория игр предоставляет математический аппарат, который позволит автономным системам принимать эффективные решения при управлении корпорациями. Несмотря на то, что многие задачи теории игр можно решать с помощью алгоритмов машинного обучения (впрочем, как и задачи машинного обучения можно формализовать с помощью теории игр), базовые алгоритмы машинного обучения являются скорее сенсорами, способными сказать нам, что именно мы видим в определенном наборе данных, но не могут решить за нас, что нам с этим знанием делать. Теория игр, нашедшая свое применение в экономике, политологии, чистой математике, психологии, социологии, маркетинге и финансах [1], предоставляет возможность системе ИИ работать автономно и принимать управленческие решения на основе моделирования эффективной стратегии. В силу того, что автономные системы искусственного интеллекта являются техническими системами, теория игр, основанная на математических методах анализа принятия управленческих решений, является понятным инструментом для автономных систем ИИ при управлении корпорациями. Предлагаемая модель разработки и внедрения автономных систем ИИ для управления корпорациями (рис. 1) основана на синтезе вычислительного права, выделенного операционного контекста, контролируемой генерации синтетических данных, алгоритмов машинного обучения, определения оптимальной стратегии с использованием теории игр, и технологий объяснимого ИИ.

Концепция закона как вычисления (называемая «вычислительным правом») направлена на то, чтобы свести закон к набору алгоритмов, которые могут автоматически выполняться на компьютере, преобразуя необработанные входные данные в юридические выводы [2]. С целью создания специального операционного контекста для автономных систем ИИ формулировки локальных нормативных документов могут быть одновременно представлены в двух вариантах: для использования людьми и для использования автономными системами [3]. Таким образом, физические лица действуют в рамках кодексов, политик, и процедур, предназначенных для людей, а автономные системы ИИ действуют в рамках кодексов, политик, и процедур, предназначенных для систем ИИ. Обучение систем ИИ на синтетических данных позволяют разрабатывать автономные системы, которые могут действовать более легитимно и этично, чем обычные топ-менеджеры [4]. На основании теории игр компания может определить оптимальные (с точки зрения компании) стратегии для системы ИИ и контролировать их выполнение. Для взаимодействия с заинтересованными сторонами автономная система ИИ должна иметь удобный интерфейс, который позволит осуществлять эффективную коммуникацию, представлять аргументацию и данные, используем системой.

1. Основные типы автономных систем ИИ для управления корпорациями

Основные типы современных автономных систем ИИ для корпоративного управления представлены рис. 2. Цифровые командные центры в настоящее время внедряются многими транснациональными корпорациями, но техническая информация о них в основном является коммерческой тайной. Персонализированные виртуальные системы и гуманоидные роботы являются двумя основными типами интерфейсов, которые позволяют автономным системам ИИ социально взаимодействовать с людьми. С одной стороны, внедрение автономных персонализированных систем управления может существенно изменить концепцию корпоративного лидерства. Цифровые командные центры в настоящее время не имеют возможности социально и эмоционально взаимодействовать с людьми. С другой стороны, ожидаемым шагом в развитии автономных

Рис. 1. Модель разработки автономных систем ИИ для управления компаниями

Рис. 2. Основные типы автономных систем ИИ для управления корпорациями

систем ИИ для корпоративного управления является появление гибридных систем путем объединения многофункциональных цифровых центров и интерфейса в виде персонализированных виртуальных систем и/или гуманоидных роботов.

Отдельные, персонифицированные системы не смогут обрабатывать тот же объем информации, что и многофункциональные цифровые фабрики, и будут периодически или постоянно подключаться к более мощным цифровым фабрикам (рис. 3). Современные цифровые командные центры используя интернет вещей и технологии цифровых двойников собирают данные с производственных площадок, заводов и фабрик. Затем данные записываются (например, используя технологию блокчейн) и обрабатываются алгоритмами машинного обучения, а результаты представляются либо в бумажном виде, либо в электронном. Гибридные же системы смогут передавать полученные результаты также виртуальным агентам или гуманоидным роботам для дальнейшей коммуникации с людьми.

Ниже мы покажем, почему гибридные системы скорее всего станут доминирующей формой автономных систем для управления корпорациями.

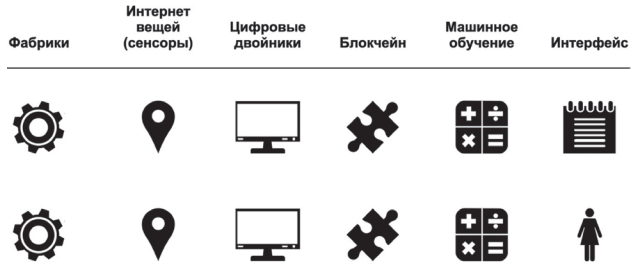


Рис. 3. Возникновение гибридных систем на базе цифровых фабрик

2. Преимущество стратегии над отдельными алгоритмами

Как отмечено в отчете Европейской Комиссии по Этике подключенных и автоматизированных транспортных средств, одного только технологического прогресса недостаточно для эффективного внедрения автономных систем. Будущее развитие автономных систем ИИ должно включать широкий набор этических, правовых и социальных положений, учитываемых при разработке, развертывании и использовании автономных систем [12]. Эксперты Европейской Комиссии по этике беспилотных автомобилей предлагают считать

поведение автономных систем этичным, если оно органически вытекает из непрерывного статистического распределения риска в целях повышения безопасности дорожного движения и равенства между категориями участников дорожного движения [12]. Исследователи в области безопасности беспилотных автомобилей также предлагают различные алгоритмы этичного планирования траектории со структурой, направленной на справедливое распределение рисков среди участников дорожного движения [13].

Однако просто мониторинга уровня риска недостаточно. Существует значительная разница между просто управлением рисками и стратегией, направленной на достижение цели. Автономным системам ИИ нужна эффективная стратегия, благодаря которой они смогут достигать заявленных целей и необходимого уровня безопасности при всех возможных обстоятельствах. Рассмотрим, какие особенности автономных систем гражданского и коммерческого назначения необходимо учитывать при моделировании стратегий для автономных систем ИИ при управлении корпорациями.

3. Основной вопрос теории игр для автономных систем ИИ

В своем труде «Теория игр и экономическое поведение» Джон фон Нейман и Оскар Моргенштерн сформулировали фундаментальные вопросы экономической теории, которые они предлагали решать с помощью теории игр. В частности, описание попыток индивидуума к извлечению максимальной пользы или в случае предпринимателя – к получению максимальной прибыли [14]. Очевидно, что мы не планируем проектировать автономные системы, которые будут стремиться к извлечению максимальной пользы для себя. Нас интересуют автономные системы ИИ, которые будут стремиться к извлечению максимальной пользы для своих создателей. Это основополагающее ограничение ничуть не мешает нам использовать математические модели исследуемые в теории игр.

При формализации ситуации для целей анализа с использованием теории игр рассматриваются, как минимум, несколько базовых вопросов, которые позволяют классифицировать игры тем или иным способом [1]. Однако основным вопросом для автономных систем ИИ гражданского и коммерческого назначения является вопрос: в какую именно игру играет система в данный момент? От корректного определения игры зависит определение оптимальной стратегии.

Во многих источниках по этике автономных систем ИИ игры смешиваются, что затрудняет анализ ситуации и поиск эффективной стратегии. Например, рассматривается вопрос: должен ли беспилотный автомобиль более бережно относиться к мотоциклистам, которые не носят шлем? Таким образом, может показаться, что мотоциклисты, которые носят шлемы, по сути, подвергаются наказанию и дискриминации за свое ответственное решение надеть шлем [15]. С точки зрения теории игр, беспилотные автомобили без специального обучения не участвуют в игре по изучению мотоциклистами правил дорожного движения, т.е. для автономного автомобиля такой вопрос даже не возникнет, в лучшем случае он просто передаст сведения о нарушителе дорожной полиции. Описанная выше ситуация является одним из примеров, когда гипотетические дилеммы ИИ с точки зрения теории игр или не возникают, или имеют совершенно другой смысл.

4. Участники игр

В процессе своей деятельности автономная система ИИ может играть с социальными системами (человеком или человеческим коллективом), с техническими системами (другой системой ИИ), со смешанными системами (например, человек при поддержке системы ИИ) и с природой. Очевидно, что без специального обучения для системы ИИ и живые, и неживые организмы изначально равнозначны. Существенным для нас является вопрос, должны ли системы ИИ одинаково бережно относиться и к людям, и к другим автономным системам? Аргументом «за» может служить то, что любая техническая система – это своеобразное «прокси» какой-то социальной системы (т. е. человека или человеческого коллектива).

5. Классификация игр

Профессор математики Мортон Дэвис подразделяет конечные игры для двух игроков на три категории: игры с нулевой суммой и полной информацией, общие игры с нулевой суммой, игры с ненулевой суммой [1]. Можно отметить, что игры с нулевой суммой не должны являться приоритетными при проектировании автономных систем ИИ. В отчете Европейской Комиссии по этике беспилотных автомобилей указывается, что автономные автомобили должны быть разработаны и эксплуатироваться таким образом, чтобы вносить позитивный вклад в благосостояние людей, включая будущие поколения и других живых существ [12]. Как указывает Дэвис, игра является игрой с нулевой суммой, если она удовлетворяет определенному закону сохранения: игра является игрой с нулевой суммой, если в ходе игры богатство не создается и не уничтожается [1]. Но зачем нам проектировать автономные системы ИИ, которые не приумножают благосостояние человечества? Таким образом, автономные системы в общем случае в первую очередь должны рассчитывать игры с ненулевой суммой.

Учитывая доступность больших данных для автономных систем ИИ понятие полной и неполной информации меняет свой смысл. С одной стороны, информация уже никогда не будет полной, потому что всегда найдется очередной набор данных. С другой стороны, при использовании больших данных точность прогноза значительно повышается.

6. Понятие полезности для автономных систем ИИ

Поскольку решения, принимаемые автономными системами ИИ, напрямую могут влиять на жизнь отдельного человека, человеческого коллектива или общества, то для моделирования таких игр необходим измеритель полезности. Несмотря на многочисленные заявления о том, что ценность человеческой жизни измерить нельзя, на практике такие измерения уже применяются, например, в медицине. При распределении дефицитных медицинских лекарств, а также донорских органов современное общество уже использует разнообразные подходы, которые считаются морально приемлемыми: равное отношение к людям, предпочтение наиболее больным, максимизация общей выгоды, поощрение и вознаграждение социальной полезности [16]. Для повышения справедливости также используются комбинации возможных подходов: система баллов Объединенной сети по обмену органами, годы жизни с поправкой на качество и годы жизни с поправкой на инвалидность, система полных жизней (которая отдает приоритет молодым людям), принципы прогнозирования, принципы спасения наибольшего количества жизней, лотереи и инструментальные ценности [16]. Приведенные выше примеры позволяют численно измерять полезность для каждого отдельно взятого человека.

С точки зрения общества также существует система мониторинга экологического, социального и корпоративного управления (ESG). Принципы ESG называют также «моральными деньгами» (“moral money”) [17]. Исследователи из MIT и Цюрихского университета насчитывают более 700 индикаторов, которые ведущие рейтинговые агентства используют для составления ESG рейтингов [18]. Таким образом, и с точки зрения отдельно взятого человека, и с точки зрения компании и общества, уже существуют общепризнанные модели измерителей, которые можно использовать для определения полезности при расчете стратегий для автономных систем ИИ при управлении корпорациями.

7. Сигнализация

Автономные системы ИИ имеют намного больше возможностей установить рациональность другой системы. Более того, они имеют возможность установить даже уровень рациональности другой системы. Даже если в сигналах одной системы ИИ присутствует шум и она не передает полностью прозрачные сигналы, другая система ИИ имеет возможность вычислить уровень правдоподобности.

Нас же интересует вопрос прозрачности намерений автономной системы ИИ при игре с человеком: должны ли сигналы системы ИИ быть полностью прозрачными или система ИИ имеет право хитрить? И должно ли это быть законодательно закреплено: по требованию человека автономная система ИИ должна отвечать только правду и ничего кроме правды?

8. Этичность и легитимность как основные правила теории игр для автономных систем ИИ

Исходя из предпосылки, что автономные системы ИИ для коммерческих и гражданских целей должны быть спроектированы с учетом соблюдения правовых и этических норм, этичность и легитимность должны являться стандартным ограничивающим правилом при анализе стратегий автономными системами ИИ. Обязательное требование о разработке этичных и легитимных автономных систем ИИ может привести к тому, что некоторые дилеммы самой теории игр для автономных систем ИИ или не существуют, или изменяют свой смысл. Например, знаменитая дилемма двух заключенных для этичных и легитимных систем ИИ будет означать, что если нанесен непреднамеренный ущерб (так как автономные системы гражданского и коммерческого назначения не могут проектироваться для нанесения преднамеренного ущерба), то его нужно как можно быстрее исправить, а не замалчивать. В то время как математическая модель ситуации может оставаться той же самой, содержательное описание должно измениться, чтобы отражать возможности и ограничения автономных систем ИИ.

В общем случае требования легитимности и этичности будут затрагивать практически все базовые вопросы теории игр:

1) ограничивать или увеличивать количество игр, которые может или должна рассматривать система ИИ;

2) ограничивать или увеличивать количество стратегий;

3) ограничивать или увеличивать количество игроков и т.д.

Обязательное требование легитимности и этичности изначально возможно реализовать через ранжирование игр: обязательные требования должны рассчитываться в играх более высокого уровня (приоритета). В некоторой степени можно сказать, что знаменитые три закона робототехники представляют собой зачатки вычислительного права для автономных систем ИИ. Например, нулевой закон робототехники: «Робот не может нанести вред человечеству или своим бездействием допустить, чтобы человечеству был нанесен вред» [19] – отражает проблему соотношения частных и публичных интересов. Таким образом, если при анализе игр для социальных систем (человека и человеческих коллективов) можно рассматривать возможность нелегитимного и неэтичного поведения, то стратегии для автономных систем ИИ сразу должны исключать нелегитимность и неэтичность.

9. Коалиционные и бескоалиционные игры для автономных систем ИИ

Требования этичности и легитимности для автономных систем ИИ в значительной степени предопределяют, в каких случаях игры могут или должны быть коалици-

онными, а в каких – нет. В случае игры по спасению жизни человека для автономной системы ИИ целесообразно иметь возможность вступать в коалиции с другими системами. В тех случаях, когда коалиции запрещены (например, законодательством о свободе конкуренции) требования легитимности ограничат вступление автономных систем ИИ в такую игру. Учитывая способность автономных систем вычислять и скрывать паттерны, обычный человек не сможет определить, вступили ли системы ИИ в коалицию.

Поскольку автономные системы могут существенно различаться по вычислительной мощности, их понимание рациональности и эффективность также могут быть разными. В отчете Европейской Комиссии по этике беспилотных автомобилей указывается, что в соответствии с принципом справедливости автономные автомобили могут быть обязаны вести себя по-другому в отношении некоторых категорий участников дорожного движения, например, пешеходов или велосипедистов, чтобы предоставить им тот же уровень защиты, что и другим участникам дорожного движения [12]. В частности, автономные автомобили должны, помимо прочего, адаптировать свое поведение в отношении уязвимых участников дорожного движения вместо того, чтобы ожидать, что эти пользователи приспособятся к опасностям дороги [12]. Таким образом, с точки зрения этичности и легитимности более мощная автономная система ИИ должна иметь возможность рассчитывать и сообщать стратегию для всех участников игры (если только такие действия прямо не запрещены законодательно).

10. Базовая игра для автономных систем ИИ

При создании своей теории Джон фон Нейман и Оскар Моргенштерн предположили, что целью всех участников экономической системы являются деньги или некоторый единый монетарный товар [14]. Мы же приходим к тому, что целью проектируемых автономных систем ИИ должна быть человеческая жизнь, ее сохранение и защита. Тем не менее, чтобы использовать методологию теории игр необходимо ввести универсальный измеритель полезности для автономных систем ИИ (например, с использованием примеров определения ценности, описанных выше).

Если мы примем, что основной целью для любой гражданской или коммерческой автономной системы ИИ прежде всего является сохранение жизни человека (или человечества), то система будет действовать «рациональным образом», если она будет нацелена на то, чтобы получить соответствующие максимумы по сохранению жизни. Таким образом, у любой автономной системы ИИ всегда будет базовая игра, направленная на сохранение жизни идентифицированных такой системой людей. Игры для автономных систем ИИ возможно разделить на несколько уровней в зависимости от приоритета выполняемой задачи. При этом базовая игра должна иметь высший приоритет, и либо может быть бесконечной, либо может быть разделена на несколько партий или подигр, сменяющих друг друга. Также базовая игра не может формулироваться как игра с нулевой суммой, так как изначально мы не хотим проектировать систему, которая будет проигрывать человеческие жизни.

В некоторых играх похожее правило просто включено в состав общей игры: например, в шахматах правила игры запрещают ставить короля под шах [14]. Разница заключается в том, что в шахматах цель игры более общая, чем просто избежать положения шаха для своего короля. Если же мы говорим, что цель игры – именно сохранение жизни человека, значит это отдельная стратегия и отдельная игра.

Правила базовой игры могут формулироваться под влиянием социальных норм общества, в котором предстоит работать автономной системе ИИ. Как показал эксперимент MIT «Моральная машина» – моральная приемлемость жертв и ценность человеческой жизни различаются в зависимости от принятых в стране социальных и культурных норм [20].

11. Дизайн базовой игры для мониторинга защиты одного человека

Для упрощения и прозрачности модели базовой игры будем рассматривать игру с природой, где природа представляет собой игрока, использующего случайную стратегию. Возможным примером может служить вопрос для руководства компании о закупке дорогостоящего защитного оборудования, которое может никогда не пригодиться.

Игра определяется следующей матрицей:

- (1) – человек защищен полностью;
- (-1) – человек не защищен (полностью или частично).

Данную матрицу можно представить в виде стратегий (табл. 1):

- $S_1 = (1, 1, 1)$;
- $S_2 = (–1, 1, 1)$;
- $S_3 = (–1, –1, 1)$;

Табл. 1. Платежная матрица игры для защиты одного человека

Класс защитного оборудования	Регулярные стихийные бедствия	Средний уровень погодной опасности	Хорошая погода
Высокий	1	1	1
Средний	-1	1	1
Низкий	-1	-1	1

Наиболее очевидным критерием с точки зрения защищаемого человека является критерий Вальда. По критерию Вальда оптимальной является стратегия,

Табл. 2. Расчет стратегии по критерию Вальда

Класс защитного оборудования	Регулярные стихийные бедствия	Средний уровень погодной опасности	Хорошая погода	Худший результат	Лучший худший результат
Высокий	1	1	1	1	1
Средний	-1	1	1	-1	-
Низкий	-1	-1	1	-1	-

которая при наихудших действиях природы гарантирует максимальный выигрыш [21] (табл. 2). Более того, может существовать общество, которое может принять критерий Вальда в качестве обязательного для автономных систем ИИ.

Рассмотрим несколько других, часто применяемых, но менее приемлемых с точки зрения защищаемого человека критериев принятия решения в условиях неопределенности. Например, критерий Гурвица пытается найти золотую середину между крайностями, заданными оптимистическим и пессимистическим критериями [22]. Однако человека, которого автономная система ИИ должна защищать, нацеленность автономной системы на оптимистичные прогнозы скорее всего не устроит (если только он сам не исключительный оптимист). Критерий минимаксного сожаления Сэвиджа рассматривает сожаление, альтернативные издержки или потери, возникающие в случае, когда возникает конкретная ситуация, а выигрыш от выбранной альтернативы меньше выигрыша, который мог бы быть получен в этой конкретной ситуации [22]. Сожаление также не подходит в качестве эффективного критерия – автономная система должна добиваться выигрыша (сохранения жизни человека, непричинения ему вреда), а не фокусироваться на возможном проигрыше.

12. Дизайн базовой игры для мониторинга защиты социального (человеческого) коллектива

Приведенный выше дизайн базовой игры не является оптимальным с точки зрения человеческого коллектива, поскольку не учитывает множество факторов:

• отвлечение ресурсов компании на приобретение ненужного дорогостоящего оборудования означает, что ресурсов может не хватить на приобретение действительно жизненно необходимых вещей;

• производство дорогостоящего оборудования может наносить непоправимый вред окружающей среде и т.д.

Для всесторонней оценки принимаемого решения и расчета полезности с точки зрения общества для автономных систем ИИ возможно адаптировать или уже существующие системы ESG метрик, или разработать собственную систему метрик на основе уже существующих международных норм. Примером для создания системы метрик могут использоваться Цели в области устойчивого развития (далее – ЦУР), разработанные и принятые всеми государствами-членами Организации Объединенных Наций в 2015 году, как общий план мира и процветания для людей и планеты сейчас и в будущем [23]. В основе лежат 17 целей и 169 показателей в области устойчивого развития, которые включают: ликвидацию нищеты и голода, обеспечение качественного образования, рациональное использование водных ресурсов, принятие срочных мер по борьбе с изменением климата, рациональное управление лесами и т. д. [23].

При оценке легитимности и этичности принимаемого решения автономная система ИИ может использовать указанные выше показатели для расчета показателей полезности при различных стратегиях. Для полноценного расчета данной модели требуется значительное количество данных и вычислительных мощностей. Поэтому многофункциональные цифровые фабрики или гибридные системы смогут решить эту задачу значительно лучше, чем менее мощные отдельные, персонифицированные системы.

Заключение

Теория игр предоставляет широкие возможности для моделирования решений, принимаемых автономными системами ИИ при управлении корпорациями. Учитывая чрезвычайно большой объем данных, необходимых для принятия качественных управленческих решений, на современном уровне развития технологий только мощные цифровые фабрики смогут рассчитывать обоснованные и качественные решения.

Отдельные, персонифицированные автономные системы ИИ самостоятельно пока что не могут проводить необходимый объем вычислений. Поэтому такие системы могут применяться либо как интерфейсы многофункциональных цифровых командных центров (цифровых фабрик), либо будут являться просто «говорящими головами» без объективной возможности принимать ответственные управленческие решения.

Библиографический список

1. Davis M.D. Game Theory: A Nontechnical Introduction. Dover Publications, 1997. 208 p.

2. Романова А.С. Основы моделирования алгоритмических решений при управлении корпорациями // Искусственные общества. 2024. Т. 19. Вып. 3. URL: https://artsoc.jes.su/s207751800032184-1-1/ (дата обращения 30.03.2025). DOI: 10.18254/S207751800032184-1

3. Романова А.С. Начала законодательства для автономных систем искусственного интеллекта // Надежность. 2024. № 24(3) С. 10-17. DOI: 10.21683/1729-2646-2024-24-3-10-17

4. Романова А.С. Моделирование автономных систем управления корпорациями на основе синтетических данных // В сб.: XXXVI Международная научно-техническая конференция «НЕЙРОИНФОРМАТИКА-2024». М.: МФТИ, Физтех, 2024. С. 193-203.

5. ADNOC, ADNOC Wins Industry Technology Award for its Panorama Digital Command Center // URL: https://adnoc.ae/news-and-media/press-releases/2021/adnoc-wins-industry-technology-award-for-its-panorama-digital-command-center (дата обращения 30.03.2025).

6. Businesswire. Tieto the First Nordic Company to Appoint Artificial Intelligence to the Leadership Team of the New Data-Driven Businesses Unit // URL: https://www.businesswire.com/news/home/20161016005092/en/Tieto-the-First-Nordic-Company-to-Appoint-Artificial-Intelligence-to-the-Leadership-Team-of-the-New-Data-Driven-Businesses-Unit (дата обращения 30.03.2025).

7. Deep Knowledge Ventures // URL: https://deepknowledgeventures.com/ (дата обращения 30.03.2025).

8. IHC. IHC's Aiden Insight sets a new benchmark for the integration of artificial intelligence in high-level corporate strategy // URL: https://www.ihcuae.com/photo/plugin/article/2024/1715086662_file_1.pdf (дата обращения 30.03.2025).

9. NetDragon. NetDragon's AI Leader Tang Yu Named China's Best Virtual Employee of 2024, 2024 // URL: https://www.netdragon.com/content/2024-04-28/20240428231345555.shtml (дата обращения 30.03.2025).

10. Business Standard. Mika becomes world's first robot CEO, thinks she's better than Musk // URL: https://www.business-standard.com/world-news/mika-becomes-world-s-first-robot-ceo-thinks-she-s-better-than-musk-123110901563_1.htm (дата обращения 30.03.2025).

11. Hanson Robotics // URL: https://www.hansonrobotics.com/sophia/ (дата обращения 30.03.2025).

12. Ethics of Connected and Automated Vehicles. Recommendations on road safety, privacy, fairness, explainability and responsibility. Luxembourg: Publications Office of the European Union, 2020. URL: https://data.europa.eu/doi/10.2777/93984 (дата обращения 30.03.2025).

13. Geisslinger M., Poszler F., Lienkamp M. An ethical trajectory planning algorithm for autonomous vehicles // Nature Machine Intelligence. 2023. Vol. 5. Pp. 137-144.

14. Neumann J.V., Morgenstern O. The Theory of Games and Economic Behaviour. Princeton University Press, 1944.

15. Lin P. Why Ethics Matters for Autonomous Cars //In: Autonomes Fahren. Technische, rechtliche und gesellschaftliche Aspekte / Eds: Markus Maurer, J. Christian Gerdes, Barbara Lenz, Hermann Winner. Springer Vieweg Berlin, Heidelberg, 2015. Pp. 69-75.

16. Persad G., Wertheimer A., Emanuel E.J. Principles for allocation of scarce medical interventions // The Lancet. 2009. Vol. 373 (9661). Pp. 423-431.

17. Financial Times. A new revolution in finance: introducing Moral Money, the latest FT newsletter. URL: https://professional.ft.com/en-gb/blog/new-revolution-finance-introducing-moral-money-latest-ft-newsletter/ (дата обращения 30.03.2025).

18. Berg, F., Kölbel, J.F., & Rigobón, R. Aggregate Confusion: The Divergence of ESG Ratings // Review of Finance. 2022. Vol. 26. Issue 6. Pp. 1315–1344. DOI: 10.1093/rof/rfac033

19. Asimov I. Foundation and Earth. Harper Voyager, 2016.

20. Awad E., Dsouza S., Shariff A.F. et al. Universals and variations in moral decisions made in 42 countries by 70,000 participants // In: Proceedings of the National Academy of Sciences of the United States of America. 2020. Vol. 117. Pp. 2332-2337. DOI: 10.1073/pnas.1911517117

21. Sniedovich M. Wald's maximin model: a treasure in disguise! // The Journal of Risk Finance. 2020. Vol. 9. No. 3. Pp. 287-291. DOI: 10.1108/15265940810875603

22. Thapaswini P.S. Savage Minimax Regret Criterion Method to Find Optimal Decision // International Journal of Science and Research (IJSR). 2020. Vol. 9. Issue 2. DOI: 10.21275/ART20204447

23. United Nations. Sustainable development goals // URL: https://sdgs.un.org/goals (дата обращения 30.03.2025).

References

1. Davis M.D. Game Theory: A Nontechnical Introduction. Dover Publications; 1997.

2. Romanova A. Fundamentals of Modeling Algorithmic Decisions in Corporate Management. *Artificial societies* 2024;19(3). Available at: https://artsoc.jes.su/s207751800032184-1-1/. DOI: 10.18254/S207751800032184-1. (in Russ.)

3. Romanova A.S. Fundamentals of legislation in autonomous artificial intelligence systems. *Dependability* 2024;24(3):10-17. (in Russ.) DOI: 10.21683/1729-2646-2024-24-3-10-17.

4. Romanova A.S. [Simulating autonomous corporate management systems based on synthetic data]. In: Proceedings of the XXXVI International Science and Technology Conference NEUROINFORMATICS-2024. Moscow: MIPT, Phystech; 2024. Pp. 193-203. (in Russ.)

5. ADNOC Wins Industry Technology Award for its Panorama Digital Command Center. (accessed 30.03.2025). Available at: https://adnoc.ae/news-and-media/press-releases/2021/adnoc-wins-industry-technology-award-for-its-panorama-digital-command-center.

6. Tieto the First Nordic Company to Appoint Artificial Intelligence to the Leadership Team of the New Data-Driven Businesses Unit. (accessed 30.03.2025). Available at: https://www.businesswire.com/news/home/20161016005092/en/Tieto-the-First-Nordic-Company-to-Appoint-Artificial-Intelligence-to-the-Leadership-Team-of-the-New-Data-Driven-Businesses-Unit.

7. Deep Knowledge Ventures. (accessed 30.03.2025). Available at: https://deepknowledgeventures.com/.

8. IHC. IHC's Aiden Insight sets a new benchmark for the integration of artificial intelligence in high-level corporate strategy. (accessed 30.03.2025). Available at: https://www.ihcuae.com/photo/plugin/article/2024/1715086662_file_1.pdf.

9. NetDragon. NetDragon's AI Leader Tang Yu Named China's Best Virtual Employee of 2024. (accessed 30.03.2025). Available at: https://www.netdragon.com/content/2024-04-28/20240428231345555.shtml.

10. Business Standard. Mika becomes world's first robot CEO, thinks she's better than Musk. (accessed 30.03.2025). (accessed 15.08.2019). Available at: https://www.business-standard.com/world-news/mika-becomes-world-s-first-robot-ceo-thinks-she-s-better-than-musk-123110901563_1.htm.

11. Hanson Robotics. (accessed 30.03.2025). Available at: https://www.hansonrobotics.com/sophia.

12. Ethics of Connected and Automated Vehicles. Recommendations on road safety, privacy, fairness, explainability and responsibility. Luxembourg: Publications Office of the European Union; 2020. (accessed 24.06.2024). Available at:// doi: 10.21683/ 2777/ 93984.

13. Geisslinger M., Poszler F., Lienkamp M. An ethical trajectory planning algorithm for autonomous vehicles. *Nature Machine Intelligence* 2023;5:137- 144.

14. Neumann J.V., Morgenstern O. The Theory of Games and Economic Behaviour. Princeton University Press; 1944.

15. Lin P. Why Ethics Matters for Autonomous Cars. In: Maurer M., Gerdes J.C., Lenz B., Winner H., editors. Autonomes Fahren. Technische, rechtliche und gesellschaftliche Aspekte. Springer Vieweg Berlin: Heidelberg; 2015. Pp. 69- 75.

16. Persad G., Wertheimer A., Emanuel E.J. Principles for allocation of scarce medical interventions. *The Lancet* 2009;373(9661):423-431.

17. A new revolution in finance: introducing Moral Money, the latest FT newsletter. (accessed 30.03.2025). Available at: https://professional.ft.com/en-gb/blog/new-revolution-finance-introducing-moral-money-latest-ft-newsletter.

18. Berg F., Kölbel J.F., Rigobón R. Aggregate Confusion: The Divergence of ESG Ratings. *Review of Finance* 2022;26(6):1315-1344. DOI: 10.1093/rof/rfac033.

19. Asimov I. Foundation and Earth. Harper Voyager; 2016.

20. Awad E., Dsouza S., Shariff A.F. et al. Universals and variations in moral decisions made in 42 countries by 70,000 participants. In: Proceedings of the National Academy of Sciences of the United States of America 2020;117:2332-2337. DOI: 10.1073/pnas.1911517117.

21. Sniedovich M. Wald's maximin model: a treasure in disguise! *The Journal of Risk Finance* 2020;9(3):287-291. DOI: 10.1108/15265940810875603.

22. Thapaswini P.S. Savage Minimax Regret Criterion Method to Find Optimal Decision. *International Journal of Science and Research (IJSR)* 2020;9(2). DOI: 10.21275/ART20204447.

23. United Nations. Sustainable development goals. (accessed 30.03.2025). Available at: https://sdgs.un.org/goals.

Сведения об авторе

Романова Анна Сергеевна – эксперт в области цифровой трансформации, к.э.н., MBA, LL.M, ALM, FCCA, свыше 15 лет опыта работы в крупнейших российских и международных компаниях. Аспирант МФТИ по направлению «Искусственный интеллект и машинное обучение», Москва, Российская Федерация, e-mail: romanova.as@phystech.edu.

About the author

Anna S. Romanova, an expert in digital transformation, Candidate of Economics, MBA, LL.M, ALM, FCCA, over 15 years of experience in the largest Russian and international companies. Postgraduate student, Artificial Intelligence and Machine Learning, MIPT, Moscow, Russian Federation, e-mail: romanova.as@phystech.edu.

Вклад автора в статью

Романовой А. С. разработана таксономия автономных систем искусственного интеллекта для управления корпорациями. Также предложены базовые принципы, позволяющие автономным системам искусственного интеллекта рассчитывать этичную и легитимную стратегию при принятии ответственных управленческих решений.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Надежность, том 25, №2, 2025 / Dependability 2, 2025
Защита информации

УДК 681.32
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-59-66

Методология глубокого анализа пакетов данных как средства обеспечения адекватности спецификаций, передаваемых в промышленных сетях

A method for deep packet inspection as means of ensuring the adequacy of specifications transmitted in industrial networks

Чаус Е.А.[1]*, Юркевич Е.В.[2]
Chaus E.A.[1]*, Yurkevich E.V.[2]

[1] *ПАО «Группа Черкизово», Российская Федерация, Москва*
[2] *ФГБУН Институт проблем управления им. В. А. Трапезникова Российской академии наук, Российская Федерация, Москва*
[1] *Cherkizovo Group, Russian Federation, Moscow*
[2] *V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Russian Federation, Moscow*
** zc86@mail.ru*

Чаус Е.А.

Юркевич Е.В.

Резюме. Цель. *Повышение адекватности спецификаций, передаваемых в системах автоматизации производственных процессов, связанных с безопасностью.* **Методы.** *Интеграция технологии глубокого контроля пакетов данных в работу открытой платформы коммуникаций с унифицированной архитектурой. Применение такой платформы в промышленных сетях определяется нормами реализации трафика сообщений в соответствии с российскими стандартами. На основании статистического анализа существующих угроз применению программных технологий использован подход, основанный на применении единого интерфейса в средствах управления объектами автоматизации технологических процессов. Применение технологии глубокой проверки сетевых пакетов по их содержимому позволило разработать алгоритм накопления статистических данных, определяющих эффективность регулирования и фильтрации трафика. На базе использования такой технологии предлагаемые методологические положения расчета рисков в работе систем автоматизации направлены на учет технических и операционных аспектов угроз влияния внешних факторов.* **Результаты.** *Показано, что соблюдение требований, предлагаемых для введения в нормативные документы, и положений, определяющих устойчивость транзакций, позволяет интернет-провайдерам визуализировать существующий трафик, определять его узкие места, вводить алгоритмизацию в использование сетевых ресурсов включая ее влияние на производительность сети и совместимость с различными протоколами. На основе результатов глубокого контроля пакетов данных рассмотрены возможности проведения эффективного анализа содержимого пакетов и их метаданных. Разработан алгоритм глубокого контроля пакетов данных, который демонстрирует этапы захвата, анализа и обработки сетевого трафика, а также структурная схема размещения средств реализации этого алгоритма в сети открытых распределенных систем, включающая точки интеграции между промышленными контроллерами, серверами и клиентами, а также облачными сервисами. Данная схема помогает визуализировать, интеграцию технологии глубокого контроля пакетов данных на все уровни взаимодействия элементов систем автоматизации производственных процессов. Для контроля динамики рисков предложен алгоритм, основанный на учете развития угроз работе каждого элемента, а также для построения контрмер в системах автоматизации производственных процессов. Характеристики средств, являющихся такими контрмерами угрозам внешних воздействий, определяются соответствием пакетов передаваемых данных нормам, определяющим спецификации протокола сервера открытой платформы. Получаемая информация помогает администраторам контролировать трафик, выявлять аномалии и планировать пропускную способность каналов связи в рассматриваемых системах автоматизации технологических процессов. Описанный подход к построению схемы обнаружения киберугроз является стратегической основой для обеспечения безопасности использования критически важных приложений.* **Заключение.** *Для обеспечения безопасности промышленных систем автоматизации технологических процессов введение норм, определяющих технологию глубокого контроля пакетов данных, в российские стандарты на цифровое производство является существенным шагом к повышению адекватности спецификаций, передаваемых в промышленных сетях, в условиях растущих киберугроз.*

Abstract. Aim. *To improve the adequacy of specifications transmitted within safety-critical process automation systems.* **Methods.** *Integration of deep packet inspection technology into the operation of an open communications platform with a uniform architecture. The application of such a platform in industrial networks is defined by the requirements of the Russian standards as regards the implementation of messaging traffic. The paper employed an approach that is based on the statistical analysis of existing threats to the use of software technologies and single interfaces as part of process automation tools. Content-based deep packet inspection allowed developing an algorithm for accumulating statistical data that define the efficiency of traffic regulation and filtering. Using the above technology along with the proposed method for calculating risks affecting automation systems would allow taking into account the technological and operational aspects of the external factors.* **Results.** *It was shown that compliance with the proposed regulatory requirements, as well as provisions defining the stability of transactions will allow Internet providers visualising existing traffic, identifying its bottlenecks, algorithmising the use of network resources, including its effect on network performance and compatibility with various protocols. Based on the results of deep packet inspection, the paper examined the feasibility of effective analysis of packet content and metadata. An algorithm was developed for deep packet inspection that demonstrates capturing, analysis, and processing of network traffic along with a diagram of the allocation of the means and facilities implementing the algorithm in a network of open distributed systems that includes integration points between industrial controllers, servers, and clients, as well as cloud services. The diagram helps visualising the integration of deep packet inspection technology at all levels of interaction between the elements of process automation systems. To control the risk dynamics, an algorithm was proposed that takes into account the evolution of threats to each of the elements, as well as building countermeasures within process automation systems. The characteristics of the facilities that represent such countermeasures to external threats are defined by the compliance of the transmitted data packets with the requirements that define the protocol specifications of an open platform server. The obtained information helps administrators inspect traffic, identify anomalies and plan the capacity of communication channels within the examined process automation systems. The above approach to building a cyber threat detection framework is a strategic basis for ensuring the security of critical applications.* **Conclusions.** *Given the demand for ensuring the safety of process automation systems, the introduction of requirements defining the deep packet inspection process into Russian digital manufacturing standards would be a significant step towards improving the adequacy of specifications transmitted within industrial networks in the face of growing cyber threats.*

Ключевые слова: *технология глубокого анализа пакетов данных, адекватность спецификаций, открытая распределенная система, промышленные сети, унифицированная архитектура, кибератаки, безопасность промышленных систем, защита данных, аутентификация, анализ пакетов.*
Keywords: *deep packet inspection process, adequacy of specifications, open distributed system, industrial networks, uniform architecture, cyber attacks, security of industrial systems, data protection, authentication, packet analysis.*

Для цитирования: *Чаус Е.А., Юркевич Е.В. Методология глубокого анализа пакетов данных как средства обеспечения адекватности спецификаций, передаваемых в промышленных сетях // Надежность. 2025. №2. С. 59-66. https://doi.org/10.21683/1729-2646-2025-25-2-59-66*
For citation: *Chaus E.A., Yurkevich E.V. Method for deep packet inspection as means of ensuring the adequacy of specifications transmitted in industrial networks. Dependability 2025;2:59-66. https://doi.org/10.21683/1729-2646-2025-25-2-59-66*

Поступила: *11.11.2024* / **После доработки:** *10.01.2025* / **К печати:** *09.06.2025*
Received on: *11.11.2024* / **Revised on:** *10.01.2025* / **For printing:** *09.06.2025*

Введение

Технология глубокой проверки пакетов данных (*Deep Packet Inspection* (*DPI*)) представляет собой важный инструмент анализа сетевого трафика, позволяющий отслеживать и фильтровать информацию об элементах рассматриваемых систем в реализации конкретного технологического процесса, а также в режиме реального времени контролировать адекватность содержимого пакетов сообщений, передаваемых между элементами системы. Данная технология обеспечивает возможность подробного анализа и мониторинга транзакций, определяющих базу для обеспечения безопасности, качества обслуживания (*QoS*) в управлении сетевым трафиком [1, 2].

В 2023 году объем мирового рынка DPI оценивался в 24,19 млрд долларов США. По прогнозам международной компании *Fortune Business Insights*, этот рынок вырастет с 30,38 млрд долларов США в 2024 году до 202,94 млрд долларов США к 2032 году, при этом среднегодовой темп роста составит 26,8% в течение прогнозируемого периода [3].

По мере развития цифровой трансформации средств связи проверка элементов сообщений, составляющая глубокий анализ содержания пакетов данных, начинает играть решающую роль в обеспечении безопасности транзакций и оптимизации сетевой среды. Сегодня *DPI* применяется в широком классе секторов систем связи, например, телекоммуникации, средства обеспечения кибербезопасности, оптимизация работы сети. Ключевые элементы таких систем включают в себя передовые аппаратные и программные решения, предназначенные для анализа сетевых пакетов в реальном масштабе времени, помогая организациям повышать безопасность и эффективность работу сети [42].

По мере увеличения сложности и масштабов промышленных систем автоматизации возрастает и уровень потенциальных угроз, делая критически важной адекватность передаваемого контента. Всемирно признанным стандартом, регламентирующим обеспечение надежной и безопасной передачи данных в системах автоматизации технологических процессов, является нормативное обеспечение открытой платформы коммуникаций с унифицированной архитектурой (*Open Platform Communications Unified Architecture* (*OPC UA*)) [5].

В ориентации на нормы *OPC UA*, применение *DPI* может значительно повысить эффективность систем защиты, предоставляя новые возможности для управления промышленными сетями. Основные положения, определяющие работу систем, связанных с безопасностью, определены в ГОСТ Р МЭК 61508. Важной характеристикой этих систем является то, что их работа сама по себе не опасна, но нештатный результат их работы может быть опасен.

На примере таких систем предлагается рассмотрение методологических положений глубокого контроля пакетов данных, направленных на обеспечение адекватности спецификаций, передаваемых в промышленных сетях.

1. Открытые распределенные системы и их применение

Внешние воздействия на системы управления производственными процессами, влияющими на способность платформы коммуникаций передавать и получать информацию, порождают неопределенности, в отношении достижимости целей, поставленных перед разработчиками систем автоматизации (АСУ). Фактически вся деятельность, связанная с эксплуатацией АСУ, содержит риски, учитывающие влияние этих неопределенностей. Ставится задача оценки рисков на каждом из этапов жизненного цикла АСУ от приемных испытаний разработки до выведения ее из эксплуатации.

Построение унифицированной архитектуры (*UA*) открытых распределенных систем (OPC), регламентируется российскими стандартами, определяющими механизмы передачи данных и взаимодействия устройств в промышленных сетях. Данные стандарты являются универсальной системой нормативных документов, регламентирующих всесторонние аспекты кроссплатформенного обмена данными в системах автоматизации производственных процессов. Нормы OPC *UA* обеспечивают высокую надежность и безопасность передачи сообщений, они ориентированы на поддержание эффективной реализации широкого класса промышленных сценариев, от операций на производственных линиях до управления энергетическими системами [4].

Структура OPC *UA* основывается на взаимодействии серверов, предоставляющими данные, и клиентов, обменивающихся данными с серверами. Применение

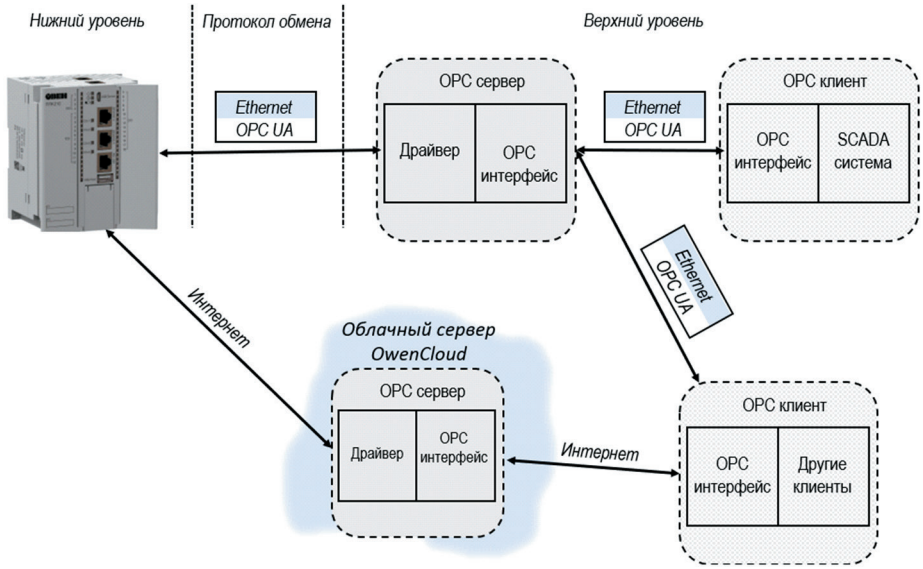


Рис.1. Структурная схема взаимодействия клиентов и серверов *OPC UA*

программного обеспечения спецификаций OPC *UA*, определяет независимость потребителей от наличия или отсутствия драйверов или протоколов. Широкая возможность выбора оборудования и программного обеспечения позволяет поддерживать соответствие характеристик систем и реальных потребностей заказчиков разработок. Схема взаимодействия клиентов и серверов OPC *UA* представлена на схеме (рис. 1).

На нижнем уровне промышленный контроллер собирает данные с датчиков и других источников информации. Контроллер подключен к серверу через протокол *Ethernet* и для передачи данных использует стандарты OPC *UA*. На верхнем уровне OPC сервер принимает данные от контроллера через драйвер и обеспечивает их обработку и хранение. Сервер предоставляет интерфейс OPC для взаимодействия с клиентами. Это могут быть системы *SCADA* или другие клиентские приложения и системы управления. Они используют данные, предоставленные сервером, для мониторинга и управления производственными процессами.

Стандарты OPC *UA* позволяют использовать облачные технологии (например, облачный сервер *OwenCloud*). Данный сервер взаимодействует с локальным OPC сервером и предоставляет возможность удаленного доступа клиентам через Интернет. Клиенты могут быть расположены в разных географических зонах и получать данные через интерфейс *OPC*.

Глубокая проверка пакетов данных (*Deep Packet Inspection* (*DPI*)) – это технология, которая позволяет анализировать как заголовки, так и содержимое пакетов данных, проходящих через точку инспекции. В отличии от традиционного метода инспекции пакетов, который фокусирует только заголовки пакетов, *DPI* обеспечивает анализ элементов передаваемых сообщений, позволяя идентифицировать, контролировать и фильтровать данные, а также проводить их детальную обработку, например, приоритизацию трафика, блокировку вредоносного контента, управление сетевыми ресурсами и обеспечение соблюдения политик безопасности [5].

Рис. 2. Алгоритм реализации принципов работы *DPI*

В структуре модели *Open System Interconnection* (*OSI*) технология *DPI* применима начиная с 2 по 7 уровень (уровень приложений), проводя анализ данных в пакетах, которые перемещаются по сетевой инфраструктуре [2]. Технологию *DPI* предлагается реализовывать с помощью аппаратных средств ОРС или в виде программного обеспечения, внедренного в такие устройства как маршрутизаторы, брандмауэры или независимые системы, в частности серверы ОРС. Принципы работы *DPI* предлагается рассматривать на примере алгоритма, представленного на рис. 2.

Предлагаемый алгоритм построения *DPI* включает ряд последовательных этапов.

На первом этапе инициализируется захват пакетов на сетевом уровне, после чего проводится анализ заголовков пакетов с целью определения адресов источника и приемника, а также других параметров. Далее следует этап анализа содержимого пакетов, на котором осуществляется сканирование конкретных данных для выявления вредоносных компонентов. На основании полученной информации принимаются решения о дальнейших действиях в отношении пакетов (блокировка, перенаправление или приоритизация). Завершающим этапом является применение политик безопасности, согласно результатам проведенного анализа.

В целом технология *DPI* позволяет визуализировать трафик, определять узкие места и оптимизировать сетевые ресурсы. Анализ содержимого и метаданных пакетов помогает администраторам контролировать трафик, выявлять аномалии и планировать пропускную способность каналов связи. *DPI* также используется Интернет-провайдерами для соблюдения нормативных требований и регулирования трафика. В результате обнаружение киберугроз повышает врзможность обеспечения безопасности критически важных приложений и качества их использования.

2. Особенности применения DPI в работе OPC UA и методика расчета рисков ИБ

Важность системы стандартов ОРС *UA* определяется регламентацией условий для обеспечения надежной и безопасной передачи данных в промышленных автоматизированных системах. На каждом из этапов жизненного цикла АСУ оценка живучести этой системы управления осуществляется посредством идентификации рисков и оценки параметров ее работы на соответствие нормативным критериям. Далее ставится задача минимизации рисков с помощью введения контрмер, устраняющих уязвимости, связанные с воздействиями внешних факторов. Для контроля динамики рисков в данной работе предлагается алгоритм, основанный на учете развития угроз, а также для оценки действенности контрмер по каждому элементу АСУ.

В соответствии методологическими нормами ИСО/МЭК 15408-1 предлагаются этапы расчета рисков при внешних воздействиях на систему автоматизации:

Первый этап – рассчитывается уровень угроз (R) по уязвимостям (U) на основе критичности и вероятности реализации угрозы внешних воздействий через данные уязвимости. Уровень угроз показывает, насколько критичным является воздействие каждой угрозы на объект защиты с учетом вероятности ее реализации.

Уязвимость при режиме работы с одной базовой угрозой: $U = \frac{E_R}{100} \times \frac{p(V)}{100}$, где *:* E_R – критичность реализации угрозы R (%); $P(U)$ – вероятность реализации R при уязвимости U (%).

Значения уровня R находятся в интервале от 0 до 1.

Второй этап – рассчитываются уровни угроз при всех уязвимостях U, через которые возможна реализация R на данном объекте, Итоговые уровни угроз через конкретные уязвимости вычисляются по формуле:

Уязвимость для режима с одной базовой угрозой (r):

$$U_r = 1 - \prod_{i=1}^{n} \left(1 - U_r^i\right),$$

где U_r^i – уровень r по уязвимостям $i = 1, 2..., n$. Значения уровней угроз при всех уязвимостях также получается в интервале от 0 до 1.

Аналогично рассчитывается общий уровень уязвимостей U, учитывающий все угрозы, действующие на объект, по формуле:

$$U = 1 - \prod_{r=1}^{R} \left(1 - U_r\right),$$

где U – уровень уязвимостей для всех угроз.

В рассмотрении функциональной надежности систем автоматизации важным параметром, значение которого зависит от эффективности применения технологии *DPI*, является ресурс системы (G). В данной работе примем, что для системы, имеющей ресурс G, риск Q рассчитывается как $Q = CU_G \times D$, где G – оценка ресурса системы ($G = 1 - P(G)$), где $P(G)$ – вероятность сбоев в передаче сообщений между ее элементами с адекватностью не ниже нормативной; D – критичность ресурса (безразмерный экспертный коэффициент задается количественно или качественно, исходя из цели применения объекта); U_G – общий уровень угроз по ресурсу G.

Если риск задается качественно, то для значения критичности берется оценка уровня. Например, для трех равномерных уровней:

Название уровня	Оценка уровня, %
1	33,33
2	66,66
3	100

Для угрозы доступность (отказ в обслуживании) критичность ресурса в год назначается, исходя из следующих оценок: $D_{а/год} = D_{а/час} \times T_{max}$, где $D_{а/год}$ – критичность ресурса в год*;* $D_{а/час}$ – критичность ресурса в час; T_{max} – максимальное критичное время проведения транзакций в год.

Риск по АСУ R_S рассчитывается по формулам:

Для количественного расчета риска: $R_S = \sum_i^n R_S^i$, где: R_S – риск по ресурсу. Для качественного расчета риска:

$$R_C = \left[1 - \prod_{i=1}^{n}\left(1 - \frac{R_c^i}{100}\right)\right] \times 100,$$

где R_c – риск по составу АСУ.

Однако с расширением цифровизации промышленных систем и повсеместным подключением их к Интернету возрастают и потенциальные угрозы безопасности [3, 6]. К наиболее существенным угрозам в области информационной безопасности можно отнести:

• кибератаки, целью которых является изменение нормального хода производственных процессов за счет внедрения вредоносного ПО системы управления и мониторинга;

• несанкционированный доступ к защищенной информации в сети предприятия, что может привести к утечке коммерческой тайны или другой важной информации;

• атаки на такие компоненты сети как DDoS-атаки, которые могут вывести из строя элементы инфраструктуры, вызывая остановку технологического процесса или другие сбои в работе систем управления [5];

• неустраненные ошибки в системах аутентификации и авторизации, которые могут быть использованы для несанкционированного доступа к системам управления и мониторинга.

Примерами кибератак в сетях OPC *UA* являются: кибератака *Stuxnet* [87], нацеленная на программируемые логические контроллеры, вредоносное программное обеспечение *Havex* [8], которое было использовано для сбора данных и саботажа в промышленных системах, кибератака *BlackEnergy* на крупные энергосистемы в том числе через протоколы OPC *UA* [9]. Такие инциденты подчеркивают необходимость укрепления защиты информации. Технологии *DPI* в промышленных автоматизированных системах на основе OPC *UA* помогают обнаруживать и предотвращать такие атаки, благодаря наличию функций детального анализа сетевого трафика в промышленных сетях [10].

3. Особенности размещения *DPI* в промышленной сети OPC *UA*

В качестве одного из комплексных решений организации применения технологии глубокой проверки пакетов информации в открытой распределенной системе данных на рис. 3 представлена структурная схема размещения *DPI* в промышленной сети взаимодействия клиентов и серверов OPC *UA*. Выделены 3 наиболее уязвимые точки:

1) *DPI* задействована для анализа всего трафика, передаваемого от контроллера к серверу OPC. Точка дает возможность выявления аномалий или злонамеренного трафика, исходящего из нижележащих слоев сети.

2) *DPI* применяется для мониторинга обмена данными между сервером и клиентами, включая системы *SCADA*. Точка позволяет противодействовать атакам на уровне передачи данных между сервером и клиентскими приложениями.

3) *DPI* предназначена для анализа коммуникаций между облачным сервером и другими элементами сети, что критически важно для предотвращения атак, направленных на облачные ресурсы, а также для защиты данных, транслируемых через Интернет в закрытый сегмент сети.

Предлагаемое расположение аппаратно-программных комплексов *DPI* обеспечивает возможность контроля и защиты критически важных точек передачи данных в системе, гарантируя комплексную безопасность сетевой архитектуры на основе OPC *UA*.

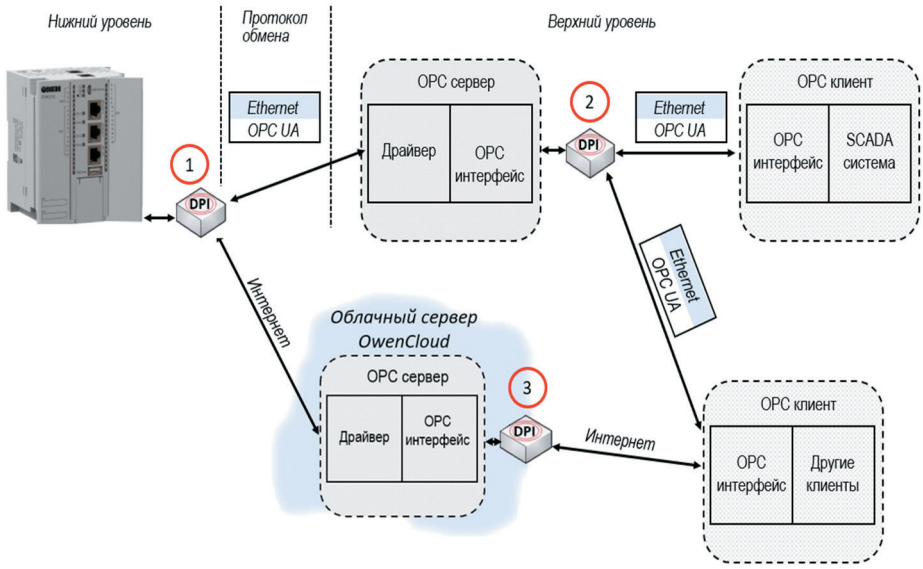


Рис. 3. Место DPI в схеме взаимодействия клиентов и серверов OPC UA

Заключение

Проведенный анализ показал, что существующие системы OPC *UA* подвержены таким угрозам, как кибератаки на уровне управления и мониторинга, утечки конфиденциальных данных и *DDoS*-атаки. Сложности и ограничения, которые возникают в процессе интеграции технологии *DPI* в архитектуру OPC *UA*, предлагается классифицировать по двум категориям.

Во-первых, технические и эксплуатационные аспекты. Внедрение *DPI* требует глубоких изменений в структуре и настройках сетевых устройств и программного обеспечения. Это сложные и трудоемкие задачи, выходящие за рамки компетенции персонала. Использование *DPI* повышает нагрузку на сетевые ресурсы за счет необходимости тщательной обработки каждого передаваемого пакета данных, что приводит к снижению производительности сети и увеличению времени задержки передаваемого сообщения. Интеграция *DPI* с существующими системами OPC *UA* может потребовать модернизации или замены некоторых компонентов системы, что также влечет за собой дополнительные расходы и временные затраты.

Во-вторых, при обеспечении совместимости и производительности технология *DPI* должна быть адаптирована к использованию с различными протоколами OPC *UA*. Для достижения эффективного уровня анализа и защиты данных может потребоваться индивидуальная настройка для каждого конкретного протокола. Повышенная нагрузка на устройства *DPI* может сказаться на их производительности и удлинить процесс анализа данных, потому важно найти баланс между глубиной анализа данных и производительностью системы. Кроме того, необходимость в регулярном обновлении базы сигнатур и правил фильтрации данных требует постоянного внимания и поддержки со стороны специалистов в области информационной безопасности.

Опыт применения разработанной схема интеграции программно-аппаратных комплексов *DPI* в промышленную сеть на основе стандартов OPC *UA* с учетом возникающих сложностей позволяет: выявлять скрытые угрозы при детальном анализе содержимого пакетов; блокировать вредоносный трафик при обнаружении атак по сигнатурам; идентифицировать аномалии, указывающие на вторжение злоумышленника, путем применения поведенческого анализа трафика; фильтровать и блокировать нежелательный трафик с высокой точностью.

Внедрение технологии *DPI* и инструментов, предоставляемых ею в инфраструктуру OPC *UA*, позволяет повысить уровень безопасности и надежности промышленных автоматизированных систем. *DPI* позволяет улучшить анализ сетевого трафика, за счет учета аномалии трафика в рамках конкретного протокола. Применение данной технологии в промышленных сетях позволяет выявлять основные факторы, требующие дополнительного изучения при внедрении *DPI*: сложность интеграции, большая нагрузка на сеть и необходимость обновления отдельных элементов системы, в ряде случаев необходимость реализации аппаратно-программных компонентов со стороны производителя систем промышленной автоматизации. Важно учитывать необходимость регулярного обновления баз данных сигнатур и правил фильтрации. Разработанная схема размещения *DPI* в сети OPC *UA* показывает, как этот программно-аппаратный комплекс применяется для обеспечения безопасности на всех уровнях взаимодействия.

В целом, можно сделать вывод, что интеграция *DPI* в OPC *U*A является действенной стратегией при повышении уровня безопасности и надежности промышленных автоматизированных систем в современных условиях интеграции сети Интернет в промышленных решениях при растущем числе киберугроз.

Библиографический список

1. Чаус Е.А. Концепция и базовый подход к построению системы защиты информации в многоуровневой интеллектуальной системе управления предприятием // Евразийское объединение. Оригинальная статья https://doi.org/10.21683/1729-2646-2024-24-3-52-60. 2020, 10-2 (68), с. 157-159.

2. Романенко О.А. Глубокая инспекция пакетов как средство анализа и контроля трафика. Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных. // В сб.: Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы Междун. науч.-технич. семинара, Минск, ноябрь-декабрь 2018 г. / Редкол.: М. Н. Бобов [и др.]. Минск: БГУИР, 2018. С. 90–93.

3. Панин Д.Н., Бобков Е.О., Балашова Е.А. Анализ кибератак на критическую информационную инфраструктуру с IOT технологиями // Автономия личности. 2020. № 2(22). С. 55-64.

4. Юркевич Е.В., Крюкова Л.Н. Проблемы нормативного обеспечения функциональной надежности цифрового производства // Надежность. 2024. Т. 24. № 3. С. 52-60. DOI: 10.21683/1729-2646-2024-24-3-52-60

5. Вейбер В.В., Кудинов А.В., Марков Н.Г. Задача сбора и передачи технологической информации распределенного промышленного предприятия // Известия ТПУ. 2011. № 5. С. 69-74.

6. Камышев С.В., Карманов И.Н. Проблемы DDoS-атак в современной IT-индустрии и методы защиты от них // Интерэкспо Гео-Сибирь. 2018. № 9. С. 121-125.

7. Langner R. Stuxnet: Dissecting a cyberwarfare weapon // IEEE Security & Privacy. 2011. Vol. 6. Iss. 3. Pp. 49–51. DOI: 10.1109/MSP.2011.67

8. Takagi H., Morita T., Matta M. et al. Strategic security protection for industrial control systems // In: Society of Instrument and Control Engineers of Japan (SICE), 2015 54th Annual Conference. IEEE, 2015. Pp. 986-992.

9. Khan R., Maynard P., Mclaughlin K. et al. Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid // In: 4th

International Symposium for ICS & SCADA Cyber Security Research 2016. DOI: 10.14236/ewic/ICS2016.7

10. Кузьмин В.Н., Менисов А.Б. Исследование путей и способов повышения результативности выявления компьютерных атак на объекты критической информационной инфраструктуры // Информационно-управляющие системы. 2022. № 4. С. 29–43. DOI: 10.31799/1684-8853-2022-4-29-43

References

1. Chaus E.A. [Concept and basic approach to building an information protection system in a multilevel intelligent enterprise management system]. *Eurasian Scientific Association* 2020;10-2(68):157-159. (in Russ.)

2. Romanenko O.A. [Deep packet inspection as a means of traffic analysis and control]. In: Telecommunications: networks and technologies, algebraic coding, and data security]. (accessed 30.06.2024). Available at: https HYPERLINK "https://libeldoc.bsuir.by/bitstream/123456789/36300/1/Romanenko_Glubokaya.pdf.

3. Panin D.N., Bobkov E.O., Balashova E.A. Analysis of cyber-attacks on critical information infrastructure with IoT technologies. *The Autonomy of Personality* 2020;2(22):55-64. (in Russ.)

4. Yurkevich E.V., Kryukova L.N. Matters of assuring functional dependability compliance of digital manufacturing. *Dependability* 2024;24(3):52-60. (in Russ.) DOI: 10.21683/1729-2646-2024-24-3-52-60.

5. Weiber V.V., Kudinov A.V., Markov N.G. [The task of collecting and transmitting technological information of a distributed industrial enterprise]. *TPU News* 2011;5. (accessed 29.06.2024). Available at: https://cyberleninka.ru/article/n/zadacha-sbora-i-peredachi-tehnologicheskoy-informatsii-raspredelennogo-promyshlennogo-predpriyatiya. (in Russ.)

6. Kamyshev S.V., Karmanov I.N. Problem of DDoS attacks in modern IT-industry and methods of protection against them. *Interexpo GEO-Siberia* 2018;9:121-125. (in Russ.)

7. Langner R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy* 2011;6(3):49-51. DOI: 10.1109/MSP.2011.67.

8. Takagi H., Morita T., Matta M. et al. Strategic security protection for industrial control systems. In: Society of Instrument and Control Engineers of Japan (SICE), 2015 54th Annual Conference. IEEE; 2015. Pp. 986-992.

9. Khan R., Maynard P., McLaughlin K. et al. Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. In: 4th International Symposium for ICS & SCADA Cyber Security Research; 2016. DOI: 10.14236/ewic/ICS2016.7.

10. Kuzmin V.N., Menisov A.B. A study of ways and solutions to increase the efficiency of detecting computer attacks on the objects of critical information infrastructure. I*nformatsionno-upravliaiushchie sistemy* 2022;4:29-43. (in Russ.). DOI:10.31799/1684-8853-2022-4-29-43.

Сведения об авторах

Чаус Евгений Александрович – ведущий инженер по автоматизированным системам управления производством, специалист в области стандартизации средств и систем автоматизации технологических процессов. ПАО «Группа Черкизово», Российская Федерация, Москва, e-mail: zc86@mail.ru

Юркевич Евгений Владимирович – д.т.н., профессор, главный научный сотрудник ИПУ РАН специалист в области функциональной надежности и системного анализа. Институт проблем управления имени В.А.Трапезникова Российской академии наук, Российская Федерация, Москва, e-mail: 79163188677@yandex.ru

About the authors

Evgeny A. Chaus, Lead Engineer, Automated Production Control Systems, expert in standardisation of process automation equipment and systems. Cherkizovo Group, Russian Federation, Moscow, e-mail: zc86@mail.ru

Evgeny V. Yurkevich, Doctor of Engineering, Professor, Head Researcher, ICS RAS, expert in functional dependability and systems analysis. V.A. Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Russian Federation, Moscow, e-mail: 79163188677@yandex.ru

Вклад авторов в статью

Чаус Е.А. разработал алгоритм реализации принципов работы DPI в сегменте промышленного протокола OPC UA. Показал особенности размещения узлов DPI в промышленной сети OPC UA.

Юркевич Е.В. предложил методику расчета рисков при внешних воздействиях на систему автоматизации в рамках использования механизмов DPI в промышленной сети OPC UA.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

История и перспективы развития теории надежности и безопасности технических систем: взгляд сквозь время

Время создания научных школ

В современном мире, где технические системы становятся все сложнее, а требования к их безотказности и безопасности — все строже, теория надежности остается одной из ключевых научных дисциплин. Ее развитие — это не только история математических моделей и инженерных решений, но и история людей, которые стояли у истоков, преодолевали вызовы и закладывали основы для будущих поколений.

Фундамент этой науки был заложен десятилетия назад, в том числе благодаря выдающимся советским ученым и инженерам. Их работы не только определили развитие теории надежности в XX веке, но и продолжают влиять на современные подходы к проектированию безотказных технических систем. В этом разделе мы обращаемся к истории возникновения и развития теории надежности и безопасности технических систем через призму воспоминаний специалистов, стоявших у истоков формирования ключевых школ надежности в СССР, которые славились своей глубиной и практической направленностью: от расчетов надежности космических аппаратов и ядерных реакторов до создания методов прогнозирования отказов в промышленности. Каждая из этих школ имела свою специфику, методологию и область применения, но все они внесли неоценимый вклад в мировую науку. Советские школы надежности оставили в наследство не только теоретические наработки, но и культуру системного подхода к обеспечению безотказности. Сегодня, когда на первый план выходят задачи кибербезопасности, искусственного интеллекта и интернета вещей (IoT), многие принципы, сформулированные десятилетия назад, обретают новое звучание. Вспомним для начала тех, кто представлял три столичные школы: московскую, ленинградскую, киевскую:

• Московская школа (МГУ, МАИ, МЭИ) – связана с именами Б.В. Гнеденко, Ю.К. Беляева, А.Д. Соловьева, И.А. Ушакова, В.В. Болотина, Е.Ю. Барзиловича, В.А. Каштанова, В.В. Рыкова и других ученых, разрабатывавших вероятностные методы анализа надежности, статистические модели отказов, теория резервирования, методы повышения долговечности сложных систем.

• Ленинградская школа (ЛТА, ЛЭТИ, ЛКВВИА, Политехнический институт) – развивала теорию живучести и безопасности систем (И.А. Рябинин, Г.Н. Черкесов), прикладные аспекты надежности под руководством А.М. Половко, методы анализа и синтеза отказоустойчивых систем (И.Б. Шубинский), надежность эргатических систем (А.И. Губинский), надежность автоматизированных систем управления (О.В. Щербаков) методологию диагностирования дискретных систем (А.В. Мозгалевский) и др.

• Киевская школа (Институт математики НАНУ, КВИРТУ, КПИ) вела основные исследования в области высоконадежных систем (И.Н. Коваленко), полумарковских методов анализа надежности (В.С. Королюк, А.Ф. Турбин), прикладных методов анализа надежности радиоэлектронной аппаратуры (Н.А. Шишонок), надежности автоматизированных систем управления (Ю.Г. Заренин), теории ускоренных испытаний (А.И. Перроте) и т.д.

Мы на примере трех школ надежности коснулись громадного пласта научных и практических работников, специалистов, которые создавали и развивали фундамент надежности в СССР и России. Через личные истории ветеранов науки мы проследим, как развивалась теория надежности, какие задачи казались неразрешимыми тогда и какие решения нашли свое применение в современных технологиях. Мы также обсудим, какие уроки прошлого могут помочь в решении новых вызовов — цифровизации, кибербезопасности и создания "умных" систем с искусственным интеллектом. Поговорим и об удивительных людях, которые создавали эту науку, будучи сами «надёжными» в высшем человеческом смысле этого слова.

Этот раздел — не только дань уважения пионерам теории надежности и безопасности технических систем, но и мост между прошлым и будущим. Мы приглашаем читателей погрузиться в историю, чтобы лучше понять, куда движется теория надежности сегодня и какие перспективы ее ждут завтра.

Редакция журнала

Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-2-66-71

Краткий очерк жизни и творческого пути Бориса Владимировича Гнеденко

Д.Б. Гнеденко

Борис Владимирович Гнеденко родился в Симбирске (ныне Ульяновск) 1 января 1912 года.

Его дед Василий Ксенофонтович Гнеденко и бабушка Анастасья Изотовна (оба по отцовской линии) – крестьяне Полтавской губернии, перебравшиеся в семидесятых годах XIX века в Казанскую губернию, где они получили землю в деревне Базарные Матаки.

Отец Бориса Владимировича – Владимир Васильевич Гнеденко – окончил землеустроительное училище и работал землемером. Мама – Мария Степановна (1886–1961) – родилась в Костроме, окончила прогимназию (семилетнее училище), в которой получила музыкальную специализацию (игра на фортепьяно), дававшую право преподавать музыку. Брат – Глеб Владимирович – родился 1 ноября 1909 года, физик, закончил отделение физики Саратовского пединститута, аспирантуру пединститута им. Либкнехта в Москве, работал в Саратове, погиб 27 октября 1943 года при форсировании Днепра в районе Днепропетровска.

Борис Владимирович Гнеденко, весна 1941 г.

В 1915 году семья переехала в Казань, где одновременно с работой землемера Владимир Васильевич с осени 1916 года стал студентом физико-математического факультета университета. Весной 1918 года по ложному доносу одного из коллег Владимир Васильевич был арестован и более полугода провел в концлагере под Казанью. Его здоровье было сильно подорвано, и по возвращении домой он был вынужден оставить студенческую скамью.

Этой же осенью 1918 года Борис Владимирович (Б.В.) поступил в школу. Как он сам пишет в своих воспоминаниях: «Все бы хорошо, если бы не было арифметики. Я действительно не любил арифметику, хотя складывал, вычитал, умножал и делил совсем неплохо. Я увлекался поэзией».

4 апреля 1922 года Владимира Васильевича вновь арестовывают, и он более трех месяцев проводит в тюрьме ГПУ. Его выпускают 12 июля. Оставаться в Казани было опасно, и семья в сентябре переезжает в Галич, где Владимир Васильевич начинает работать старшим землеустроителем. К приезду семьи в Галич набор в школы был закончен, и этот год с Борисом и его братом Глебом занимается мама. «Мама узнала программу и начала заниматься с нами, чтобы мы не отстали. Достали учебник грамматики, арифметику Киселева, учебник географии Иванова. Я с особым удовольствием читал учебник географии и учил правила грамматики русского языка. <…> Летом мы были зачислены с братом в школу в один и тот же шестой класс».

В апреле 1925 года семья переезжает в Саратов. Это было связано с тем, что родители начали беспокоиться о дальнейшем образовании своих детей, которые через два года должны были окончить школу (в то время среднее образование было девятилетним).

В Саратове братья были зачислены в школу № 3, бывшее реальное училище. Выяснилось, что они серьезно отстали по химии и математике. На осень им были назначены переэкзаменовки по этим предметам. Это оказалось очень полезным. «Мы сумели продумать весь материал по математике и по химии, прорешать по многу десятков задач, и осенью, благодаря этому, переэкзаменовка прошла благополучно. Более того, химия и математика стали восприниматься совершенно свободно, задачи не вызывали никаких трудностей, и я начал решать задачи сразу в уме, как только узнавал условие. По математике и химии я выдвинулся в число первых учеников класса. Одноклассники стали обращаться ко мне за помощью.

Математика стала мне нравиться... Мне нравилось учиться, дополнительно читать книги, решать нестандартные задачи... Я достал сборник конкурсных задач, предлагавшихся на вступительных экзаменах в Петроградский институт инженеров путей сообщения. Ни одна задача из этого сборника не вызвала у меня затруднений... Я отдавал себе отчет в том, что хочу учиться дальше и буду добиваться этого права. Я тщательно изучил правила приема в вузы страны и повсюду наталкивался на одно требование, которому я не удовлетворял, – поступающему должно исполниться 17 лет, мне же было только 15... Брат хотел стать или инженером, или физиком, а я мечтал о кораблестроении. Я даже послал в Ленинградский кораблестроительный институт письмо с просьбой допустить меня к вступительным экзаменам в мои пятнадцать лет».

Из города на Неве на это письмо Б.В. получил отказ. Тогда он посылает письмо народному комиссару просвещения А.В. Луначарскому с просьбой разрешить ему поступать в Саратовский университет. К началу вступительных экзаменов разрешение было получено.

С осени 1927 года Б.В. – студент физико-математического факультета Саратовского университета. «В мае 1930 года нам объявили, что мы будем заниматься все лето, с тем чтобы в сентябре разъехаться по местам работы. Было решено организовать ускоренный выпуск... Экзамены были сданы, и в середине августа нам были выданы документы об окончании Саратовского университета. Я не испытывал от этого ни радости, ни удовлетворения. Я понимал, что получено ущербное образование и нужно приложить много собственных усилий, чтобы исправить положение дел».

Один из университетских преподавателей Б.В. – профессор Георгий Петрович Боев – в это время был приглашен заведовать кафедрой математики в организуемый в Иваново-Вознесенске Текстильный институт и, в свою очередь, пригласил Б.В. на должность ассистента этой кафедры.

В Иваново-Вознесенске Б.В. преподавал и занимался вопросами применения математических методов в текстильном деле. Здесь им были написаны его первые работы по теории массового обслуживания, здесь Б.В. увлекся теорией вероятностей. Этот период деятельности сыграл огромную роль в его формировании как ученого и педагога.

Понимая необходимость углубления своих математических знаний, Б.В. в 1934 году поступает в аспирантуру механико-математического факультета МГУ. Его научными руководителями становятся А.Я. Хинчин и А.Н. Колмогоров.

В аспирантуре Б.В. увлекся предельными теоремами для сумм независимых случайных величин. 16 июня 1937 года он защитил кандидатскую диссертацию на тему «О некоторых результатах по теории безгранично делимых распределений», и с 1 сентября этого же года он – младший научный сотрудник Института математики МГУ.

В работах А.Я. Хинчина и Г.М. Бавли было установлено, что класс возможных предельных распределений для сумм независимых случайных величин совпадает с классом безгранично делимых распределений. Оставалось выяснить условия существования предельных распределений и условия сходимости к каждому возможному предельному распределению. Заслуга постановки и решения этих задач принадлежит Б.В. Гнеденко. Для решения возникших проблем Б.В. предложил оригинальный метод, получивший название метода сопровождающих безгранично делимых законов (идея метода появилась в октябре 1937 года и опубликована в «Докладах АН СССР» в 1938 году[1]). Он позволил единым приемом получить все ранее найденные в этой области результаты, а также и ряд новых.

В ночь с 5-го на 6-ое декабря 1937 года Борис Владимирович был арестован. Ему предъявили надуманное обвинение в контрреволюционной деятельности и участии в контрреволюционной группе, возглавляемой профессором А.Н. Колмогоровым. Его водили на допросы, во время одного из которых ему не давали спать в течение восьми суток. Требовали подписать бумаги, подтверждающие обвинения. Борис Владимирович не подписал ничего, что могло бы быть поставлено в вину ему, А.Н. Колмогорову или кому-либо другому. В конце мая 1938 года его освободили.

Слева направо: Александр Александрович Бобров, Александр Яковлевич Хинчин, Борис Владимирович Гнеденко

С осени 1938 года Б.В. – доцент кафедры теории вероятностей механико-математического факультета МГУ, ученый секретарь Института математики МГУ. К этому периоду относятся работы Б.В. Гнеденко, в которых дано решение двух важных задач. Первая из них касалась построения асимптотических распределений максимального члена вариационного ряда, выяснения природы предельных распределений и условий сходимости к ним[2]. Вторая задача касалась построения теории поправок к показаниям счетчиков Гейгера-Мюллера, применяемых во многих областях физики и техники[3].

В начале июня 1941 года Б.В. защитил докторскую диссертацию, состоящую из двух частей: теории суммирования и теории максимального члена вариационного ряда.

[1] Гнеденко Б.В. О сходимости законов распределения сумм независимых слагаемых (Доклады АН СССР, т. 18, № 4–5, 231 – 234).

[2] Гнеденко Б.В. Предельные теоремы для максимального члена вариационного ряда («Доклады АН СССР», т. 32, № 1, 7-9)

[3] Гнеденко Б.В. К теории счетчиков Гейгер-Мюллера («Журнал экспериментальной и теоретической физики», т. 11, вып. 1, 101 – 106).

Борис Владимирович Гнеденко, 1948 г.

В годы Великой Отечественной войны Б.В. принимал активное участие в решении многочисленных задач, связанных с обороной страны.

В феврале 1945 года Борис Владимирович избирается членом-корреспондентом АН УССР и направляется Президиумом АН УССР во Львов для восстановления работы Львовского университета.

Во Львове Б.В. читает разнообразные курсы лекций: математический анализ, вариационное исчисление, теорию аналитических функций, теорию вероятностей, математическую статистику и др., в окончательной формулировке доказывает локальную предельную теорему для независимых, одинаково распределенных решетчатых слагаемых (1948 г.), начинает исследования по непараметрическим методам статистики. Во Львове им были воспитаны талантливые ученики – Е.Л. Рвачева (Ющенко), Ю.П. Студнев, И.Д. Квит и др.

Курс лекций по теории вероятностей послужил Борису Владимировичу основой для написания учебника «Курс теории вероятностей» (1949 г.). Эта книга многократно издавалась в разных странах и является одним из основных учебников по теории вероятностей и в наши дни. В эти же годы им совместно с А.Н. Колмогоровым написана монография «Предельные распределения для сумм независимых случайных величин» (1949 г.), за которую авторы были удостоены премии АН СССР им. П.Л. Чебышева (1951 г.). Совместно с А.Я. Хинчиным Б.В. пишет «Элементарное введение в теорию вероятностей» (1946 г.), которое, в свою очередь, выдержало множество изданий в СССР и за рубежом. Кроме этого Борисом Владимировичем была написана замечательная книга «Очерки по истории математики в России» (1946 г.).

В 1948 году Б.В. избирается академиком АН УССР, и в 1950 году Президиум АН УССР переводит его в Киев. Здесь он возглавляет только что созданный в Институте математики АН УССР отдел теории вероятностей и одновременно начинает заведовать кафедрой теории вероятностей и алгебры в Киевском университете. Очень скоро около него образовалась группа молодежи, заинтересовавшейся теорией вероятностей и математической статистикой. Первыми киевскими учениками Б.В. были В.С. Королюк, В.С. Михалевич и А.В. Скороход.

В это время Б.В. увлекся сам и увлек многих своих учеников и коллег задачами, связанными с проверкой однородности двух выборок. В.С. Королюк, В.С. Михалевич, Е.Л. Рвачева (Ющенко), Ю.П. Студнев и др. получили серьезные результаты в этой области.

Борис Владимирович участвует в проведении 2-го тура математической олимпиады, 1952 г.

В конце 1953 года Б.В. Гнеденко был направлен в ГДР для чтения лекций в университете им. Гумбольдта (Берлин). Он провел там весь 1954 год. За это время Б.В. сумел заинтересовать большую группу молодых немецких математиков (И. Керстан, К. Маттес, Д. Кёниг, Г.- И. Россберг, В. Рихтер и др.) задачами теории вероятностей и математической статистики. Правительство ГДР наградило Бориса Владимировича серебряным орденом «За заслуги перед Отечеством», а университет им. Гумбольдта избрал его почетным доктором.

Вернувшись в конце 1954 года в Киев, Б.В. по поручению Президиума АН УССР возглавил работу по организации Вычислительного центра. Был создан коллектив, в который вошли сотрудники лаборатории академика С.А. Лебедева, автора первой в континентальной Европе ЭВМ, получившей название МЭСМ (малая электронная счетная машина). Лаборатория к этому времени возглавлялась её старейшими сотрудниками – Е.А. Шкабарой и Л.Н. Дашевским, т.к. сам С.А. Лебедев уже переехал в Москву, где ему была поручена организация Института точной механики и вычислительной техники. В этот коллектив вошли и математики, среди

которых в первую очередь надо назвать В.С. Королюка, Е.Л. Ющенко и И.Б. Погребысского. Началась работа по проектированию универсальной машины «Киев» и специализированной машины для решения систем линейных алгебраических уравнений.

Слева направо: Я.М. Сорин, Б.В. Гнеденко, Я.Б. Шор (Рыбинск, 11.05.1960)

Одновременно Б.В. начал читать в университете курс программирования для ЭВМ и возглавил работу по написанию учебника по программированию. Этот курс (первая в СССР книга по программированию в открытой печати) был издан в Москве в 1961 году (авторы – Б.В. Гнеденко, В.С. Королюк, Е.Л. Ющенко)[4]. В это же время (1955 г.) Президиум АН УССР возложил на Б.В. Гнеденко обязанности директора Института математики АН УССР и председателя бюро физико-математического отделения АН У ССР.

Б.В. Гнеденко и Дитер Кёниг (конец 70-х, начало 80-х годов)

В этот период Борис Владимирович начинает разрабатывать два новых направления прикладных научных исследований – теорию массового обслуживания (ТМО) и применение математических методов в медицине.

К первому он привлек И.Н. Коваленко, Т.П. Марьяновича, Н.В. Яровицкого, С.М. Броди и др. Б.В. применил методы ТМО к расчету электрических сетей промышленных предприятий. В 1959 году были изданы «Лекции по теории массового обслуживания» (выпуск 1), прочитанные Б.В. в КВИРТУ[5] в 1956-57 годах. Затем последовали выпуски 1-2 (1960 г.), выпуски 1-3 (1963 г., совместно с И.Н. Коваленко). Эти книги послужили основой для монографии «Введение в теорию массового обслуживания» (1966 г.), написанную Б.В. Гнеденко и И.Н. Коваленко.

Второе направление связано с разработкой электронного диагноста сердечных заболеваний. Над этой проблемой работали Б.В. Гнеденко, Н.М. Амосов, Е.А. Шкабара и М.А. Куликов. В начале 1960 года была завершена сборка первого в мире диагноста.

Переехав в июле 1960 года в Москву, Борис Владимирович возобновляет работу на механико-математическом факультете МГУ. Работа вновь полностью захватила его: чтение разнообразных лекционных курсов, новые ученики, новые обязанности.

Слева направо: Н.Х. Розов, Б.В. Гнеденко, А.Д. Соловьев

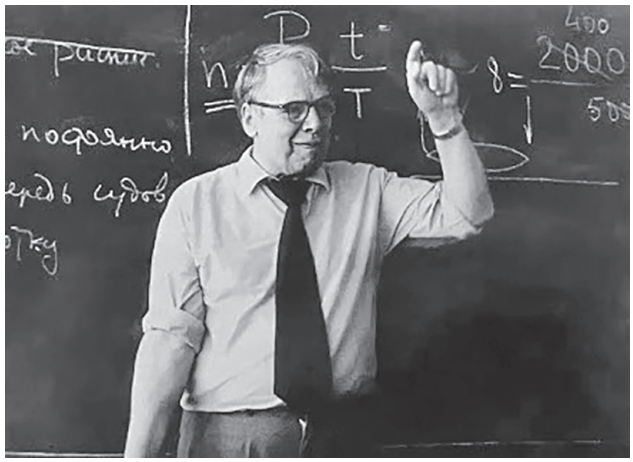
В 1961 году группа в составе Я.М. Сорин, Ю.К. Беляев, А.Д. Соловьев, Я.Б. Шор и И.А. Ушаков во главе с Б.В. становится коллективным консультантом при Госстандарте СССР, в котором возникает Методический совет по надежности и качеству. Затем Б.В. и Я.М. Сорин организуют семинар по надежности при Политехническом музее, который эффективно работал в течение многих лет. Параллельно они же создают журнал Госстандарта «Надежность и качество». Вскоре появляется необходимость организации отдельного семинара специально по математическим методам теории надежности. Этот семинар начинает работать

[4] Б.В. Гнеденко, В.С. Королюк, Е.Л. Ющенко. Элементы программирования. Москва, Физматгиз. 3-348.

[5] Киевское высшее инженерное радиотехническое училище.

на механико-математическом факультете МГУ под руководством Б.В. Гнеденко, А.Д. Соловьева, Ю.К. Беляева и И.Н. Коваленко, который в это время работал в Москве. Семинар по математическим методам в теории надежности регулярно работал до конца восьмидесятых годов. Он помог в научном отношении встать на ноги многим своим участникам, теперь широко известным специалистам в области надежности, таким как В.А. Гадасин, В.А. Каштанов, Г.Д. Карташов, Б.А. Козлов, И.В. Павлов, Г.Б. Рубальский, Р.С. Судаков, О.И. Тескин, И.А. Ушаков, В.Л. Шпер и др. Этот семинар повлиял, в свою очередь, и на своих руководителей и подтолкнул Б.В. Гнеденко, Ю.К. Беляева и А.Д. Соловьева к написанию широко известной у нас и за рубежом монографии «Математические методы в теории надежности» (1965 г.). За цикл работ в области надежности Б.В. вместе с ближайшими сподвижниками был удостоен в 1979 году Государственной премии СССР. В 1983 г. Б.В. с группой соавторов был удостоен Премии Минвуза за коллективную монографию «Вопросы математической теории надежности».

В связи с задачами надежности Б.В. вновь вернулся к исследованию предельных теорем для сумм независимых случайных величин, но уже в случайном числе. К этому направлению исследований Б.В. привлекает многих своих учеников. За эти работы в 1982 году ему присуждается премия им. М.В. Ломоносова первой степени, а в 1986 году – премия Минвуза СССР.



Болгария, Шумен (1972)

Б.В. не переставал интересоваться вопросами истории математики, подключив своих учеников и к этому направлению работ. В различных отечественных и зарубежных журналах печатались его статьи по этому направлению исследований, а его «Очерк по истории теории вероятностей» дает наиболее полное представление о его взглядах на историю этой науки.

Совместно с А.И. Маркушевичем Б.В. руководил работой семинара по вопросам преподавания в средней школе. Он тесно сотрудничал с редакциями журналов «Вестник высшей школы» и «Математика в школе». В этих и многих зарубежных журналах, в сборниках научно-методического совета Минвуза СССР им было опубликовано большое число статей по различным аспектам преподавания.

Б.В. Гнеденко на праздновании юбилея (80 лет)

По этим же вопросам Б.В. написал в эти годы и несколько книг.

В январе 1966 года А.Н. Колмогоров передал Б.В. Гнеденко руководство кафедрой теории вероятностей механико-математического факультета МГУ, которой Б.В. заведовал до последних дней своей жизни.

Еще работая во Львове, Б.В. много времени и сил отдавал работе в обществе «Знание». С 1949 года он последовательно избирался председателем областного правления общества, возглавлял республиканскую физико-математическую секцию общества, являлся членом Президиума правления Всесоюзного общества «Знание», председателем общества «Знание» Московского университета.

Б.В. был членом редколлегий ряда отечественных и зарубежных журналов, являлся почетным членом Королевского Статистического Общества (Великобритания), был избран почетным доктором Берлинского университета, почетным доктором Афинского университета.

В последние годы жизни, зная суровый приговор врачей, Б.В. продолжает руководить кафедрой, выдвигает и осуществляет идею создания на механико-математическом факультете экономической специализации и подготовки в ее рамках специалистов в области актуарной и финансовой математики. Кроме этого он намечает список книг, которые надо успеть написать за оставшееся время. И он пишет.

Окончательно ослепнув, диктует, но выполняет намеченное.

27 декабря 1995 года Бориса Владимировича не стало. Он похоронен на Кунцевском кладбище в Москве. Дэвид Кендалл и Ю. М. Сухов в некрологе «Boris Vladimirovitch Gnedenko» («Bernoulli», 1997, 3(1), 121–122) написали: «Его смерть означает конец великолепной и плодотворной эры, которая навсегда преобразовала теорию

вероятностей и значительно расширила ее кругозор и число ее приложений».

Ульф Гренандер – шведский статистик и профессор прикладной математики в Университете Брауна – писал, что монография «Предельные распределения для сумм независимых случайных величин» «…представляет собой неразрушимый вечный памятник в литературе по теории вероятностей».

Б.В. Гнеденко оставил много учеников. Среди них – академики и члены-корреспонденты различных академий, профессора и доценты. В их памяти сохраняются незабываемые дни приобщения к науке и самостоятельному творчеству под руководством большого ученого и педагога, часы непосредственного общения с Человеком большой эрудиции и высокой культуры.

Мемориальную доску, посвященную выдающемуся математику, академику АН УССР Борису Владимировичу Гнеденко (1912–1995), открыли в Киеве 5 декабря 2017 года на здании по адресу улица Прорезная, 10, где в 1950-х годах жил Борис Владимирович с женой и двумя сыновьями. В то время Б.В. Гнеденко был директором Института математики Академии наук УССР.

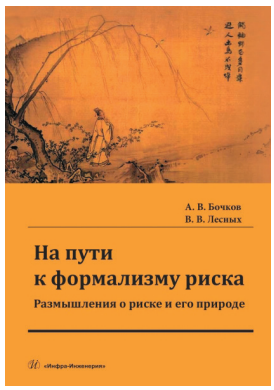
Об авторе:

Дмитрий Борисович Гнеденко, окончил Механико-математический факультет Московского университета в 1965 году и до 1996 года работал на кафедре теории чисел, сначала в должности ассистента, а после защиты в 1975 году кандидатской диссертации (научный руководитель А.Д. Соловьев) – доцента кафедры. С 1996 года Д.Б. Гнеденко – доцент кафедры теории вероятностей. С этого же года – заместитель заведующего кафедрой.

От редакции: больше информации о Борисе Владимировиче Гнеденко вы можете найти на сайте «Гнеденко-Форума»: https://www.gnedenko.net/Memorial/Gnedenko/biograph2.htm . Там же размещена наиболее полная на настоящий момент времени и постоянно пополняемая библиография работ Б.В.: https://www.gnedenko.net/Memorial/Gnedenko/biograph_rus.htm

Редакция рекомендует

На пути к формализму риска. Размышления о риске и его природе



ISBN 978-5-9729-2146-1
Авторы: Бочков А.В., Лесных В.В.
Издательство: Инфра-Инженерия
Объем 296 с.
Год: 2024

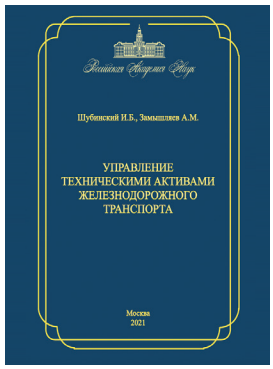
Кажется, мы знаем о риске почти всё и в то же время ничего. Сконцентриро¬вавшись на этимологии слова «риск», исследователи часто упускают из виду его природу, причины и характерис¬тики. В то же время в разных ситуациях риск проявляется по-разному и может быть как характеристикой случайного события, так и характеристикой и мерой качества процесса, протека¬ющего во времени. В последнем случае риску присущи свойства волнового процесса, что требует поиска иных мер, кроме вероятностных, для его измерения и оценки. В данной работе сделана попытка обобщить наиболее характерные различные проявления риска и предложить способы оценки риска, учитывающие эти различия. Книга может рассматриваться как приглашение к дискуссии о природе риска и о том, как может быть построен его формализм. Для широкого круга научных работников и специалистов в области анализа, оценки и управления рисками.

На пути к формализму риска. Безопасность и устойчивость функционирования умных экспансивных систем

ISBN 978-5-9729-2373-1
Автор: Бочков А.В.
Издательство: Инфра-Инженерия
Объем 348 с.
Год: 2025

Представлена методология обеспечения безопасности и устойчивости функционирования особого класса структурно-сложных систем – умных экспансивных систем, направленная на прогнозирование и снижение риска возникновения чрезвычайных ситуаций, нарушающих условия жизнедеятельности людей. Методология оперирует пятью ключевыми, неразрывно связанными между собой методами, решающими задачи, возникающие при построении подсистем, обеспечивающих безопасность и устойчивость рассматриваемого класса структурно сложных систем в условиях возникновения нештатных и чрезвычайных ситуаций природного, техногенного и антропогенного характера. В отличие от существующих подходов рассматривается невероятностная постановка, что оправдано для редких событий, какими являются чрезвычайные ситуации и противоправные акции. Разработан метод, обеспечивающий поддержку принятия решения в так называемой задаче группового выбора объектов критически важной инфраструктуры, требующих повышенного внимания службы безопасности и затрат ресурсов государства и собственника системы на обеспечение их защищённости, безопасности и устойчивости функционирования. Разработан и теоретически обоснован метод построения интегрального показателя безопасности, позволившего решить задачу построения оптимальных процессов дискретной обработки непрерывных данных, поступающих от системы, снизить размерность её описания с целью повышения оперативности принятия управляющих решений, обеспечивающих её устойчивое функционирование при наличии внешних негативных воздействий различной природы. Для широкого круга научных работников и специалистов в области анализа, оценки и управления рисками.

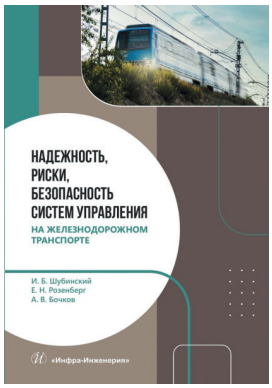
Управление техническими активами железнодорожного транспорта



ISBN 975-5-902928-89-8
Авторы: Шубинский И.Б., Замышляев А.М.
Издательство: М.: ВИНИТИ РАН
Объем 248с.
Год: 2021

В книге изложены ключевые положения системы управления техническими активами на основе УРРАН- методологии управления ресурсами, рисками путем анализа и обеспечения требуемых уровней надежности и безопасности объектов железнодорожного транспорта. Приведены базовые понятия и показатели надежности и функциональной безопасности объектов, эталонирование этих объектов транспорта и нормирование показателей их надежности. Приведены основы управления техническими, технологическими и техногенными рисками на железнодорожном транспорте, представлены основы управления ресурсами, а также методики оценки деятельности структурных подразделений инфраструктуры и подвижного состава. Представлена архитектура единой корпоративной платформы информационной системы УРРАН (ЕКП УРРАН) и ее подсистем для комплексов объектов транспорта. Показаны перспективы развития ЕКП УРРАН, особенно в части применения искусственного интеллекта для прогнозирования опасных событий в работе инфраструктуры. Книга рассчитана, в первую очередь, на специалистов, занимающихся практической работой по техническому содержанию объектов железнодорожного транспорта. Она предназначена студентам, аспирантам железнодорожных вузов и может быть также полезна специалистам, студентам и преподавателям других отраслей.

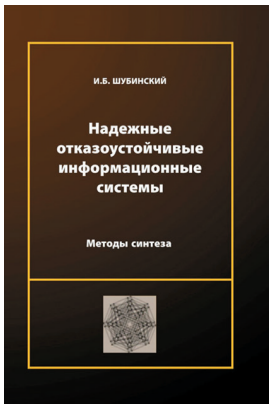
Надежность, риски, безопасность систем управления на железнодорожном транспорте



ISBN 978-5-9729-1992-5
Авторы: Шубинский И.Б., Розенберг Е.Н., Бочков А.В.
Издательство: Инфра-Инженерия
Объем: 416 с.
Год: 2024

Центральное внимание уделено вопросам обеспечения структурной и особенно функциональной надежности. Обсуждается специфика терминологии в данной области. Представлена методологическая основа прогнозирования редких опасных событий (отказов). Рассмотрен комплекс математических моделей и методов, различных метрик для проверки качества построенных моделей. Большое внимание уделено вопросам нормирования показателей надёжности. Представлены результаты современных исследований авторов в области безопасности движения поездов, включая информационную безопасность. Для широкого круга научных работников, специалистов железнодорожной отрасли, связанных с процессами управления, а также для профессорско-преподавательского состава, аспирантов и студентов вузов железнодорожного транспорта.

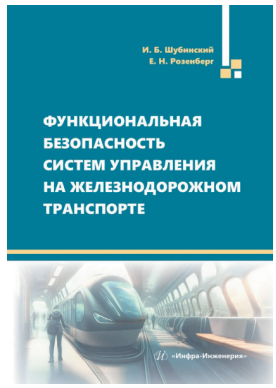
Надежные отказоустойчивые информационные системы. Методы синтеза



ISBN 978-5-7572-0399-7
Автор: Шубинский И.Б.
Издательство: Ульяновск: Печатный двор; М.: Надежность
Объем: 546 с.
Год: 2016

В книге приведены концептуальные положения обеспечения структурной и функциональной надежности информационных систем на всех стадиях их жизненного цикла. Различные виды структурного резервирования рассмотрены с учетом ограничений в обнаружении отказов. При этих условиях установлены предельные возможности структурного резервирования в предположении бесконечного количества резервных устройств. . Представлены теоретические и практические положения адаптивной отказоустойчивости (активной защиты) информационных систем, в том числе методы и дисциплины активной защиты, способы ее практической реализации. Предложен метод синтеза активной защиты. Оценена эффективность активной защиты по отношению к традиционным методам структурного резервирования. Для широкого круга научных работников и специалистов в области информационной техники.

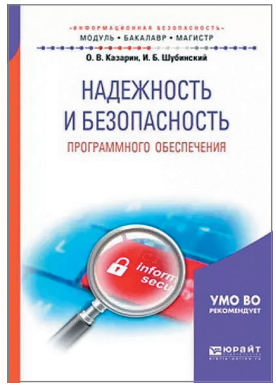
Функциональная безопасность систем управления на железнодорожном транспорте



ISBN 978-5-9729-1553-8
Авторы: Шубинский И.Б., Розенберг Е.Н.
Издательство: Инфра-Инженерия
Объем: 360 с.
Год: 2023

Представлен широкий спектр вопросов функциональной безопасности – от научных основ (понятий, постулатов, принципов) до методов и способов обеспечения безопасности технических средств и программного обеспечения систем управления на железнодорожном транспорте, включая прогрессивные методы обеспечения безопасности с помощью виртуальных каналов и цифровых двойников. Значительное внимание уделено методологии подтверждения соответствия требованиям функциональной безопасности. Для широкого круга научных работников, специалистов железнодорожной отрасли, связанных с процессами управления, профессорско-преподавательского состава, аспирантов и студентов вузов железнодорожного транспорта. Может представлять интерес специалистам, студентам и преподавателям других отраслей.

Надежность и безопасность программного обеспечения

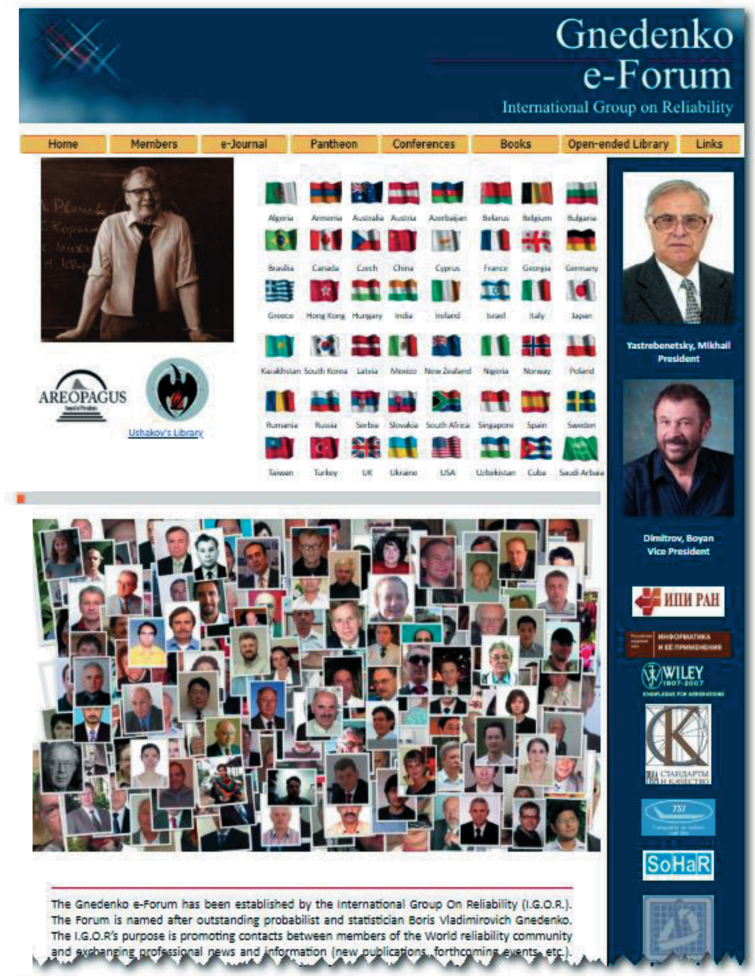


ISBN 978-5-534-05142-1
Авторы: Казарин, О.В., Шубинский И.Б.
Издательство: Москва, Издательство Юрайт
Объем: 342 с.
Год: 2024

В курсе изложены теоретические и практические основы создания надежного и безопасного программного обеспечения информационных систем. Приведены правила, этапы и технологии построения надежного программного обеспечения. Рассмотрены требования к функциональной надежности и архитектуре программного обеспечения критически важных систем, методы защиты программного обеспечения от вредоносных программ, методы обеспечения безопасности программ, реализуемые на этапах испытания программных комплексов, методы и средства тестирования и защиты программ от исследования недобросовестными конкурентами и злоумышленниками. Представлены нормативные документы, регулирующие деятельность в данной сфере, а также процедуры подтверждения соответствия надежности и безопасности программного обеспечения современных информационных систем требованиям российских регуляторов.

GNEDENKO FORUM

INTERNATIONAL GROUP ON RELIABILITY



Gnedenko Forum основан в 2004 году неофициальной международной группой экспертов в области теории надёжности для профессиональной поддержки исследователей всего мира, заинтересованных в изучении и развитии научных, технических и пр. аспектов теории надёжности, анализа рисков и безопасности в теоретической и прикладной областях.

Форум создан в сети Интернет как некоммерческая организация. Его цель – привлечь к совместному обсуждению и общению технических специалистов, заинтересованных в развитии теории надёжности, безопасности и анализа рисков, независимо от места их проживания и принадлежности к тем или иным организациям.

Форум выступает в качестве объективного и нейтрального лица, распространяющего научную информацию для прессы и общественности по вопросам, касающимся безопасности, анализа риска и надёжности сложных технических систем. Он опубликует обзоры, технические документы, технические отчеты и научные эссе для распространения знаний и информации.

Форум назван в честь Бориса Владимировича Гнеденко, выдающегося советского математика, специалиста в области теории вероятностей и её приложений, академика Украинской академии наук. Форум является площадкой для распространения информации о стипендиях, академических и профессиональных позициях, открывающихся в профессиональной области надёжности, безопасности и анализа рисков по всему миру.

В настоящее время в Форуме состоят 500 участников из 47 стран мира.

Начиная с января 2006 года, Форум выпускает свой ежеквартальный журнал Reliability: Theory & Applications (www.gnedenko.net/RTA). Журнал зарегистрирован в Библиотеке Конгресса США (ISSN 1932-2321) и публикует статьи, критические обзоры, воспоминания, информацию и библиографии на теоретические и прикладные аспекты надёжности, безопасности, живучести, технического обслуживания и методы анализа и управления рисками.

С 2017 года журнал индексируется в международной базе Scopus.

Членство в GNEDENKO FORUM не подразумевает никаких обязательств. Достаточно прислать по адресу a.bochkov@gmail.com свою фотографию и краткую профессиональную биографию (резюме). Образцы можно найти на http://www.gnedenko.net/personalities.htm

www.gnedenko.net

ТРЕБОВАНИЯ РЕДАКЦИИ ПО ОФОРМЛЕНИЮ СТАТЕЙ В ЖУРНАЛАХ ИЗДАТЕЛЬСКОЙ ГРУППЫ IDT PUBLISHERS

Требования к формату статьи

Статья представляется в редакцию в электронном формате, в виде файла, созданного в текстовом редакторе MS Word из пакета Microsoft Office (файл с расширением *.doc или *.docx). Текст набирается черным шрифтом на листе формата А4 с полями: левое, верхнее, нижнее – 2 см; правое – 1,5 или 2 см. Минимальный объем статьи – 5 страниц, максимальный (может быть увеличен по согласованию с редакцией) – 12 страниц. При этом статья включает структурные элементы, описание которых представлено ниже.

Структура материала статьи

Представленные ниже структурные элементы статьи отделяются друг от друга *пустой строкой*. Отдельные примеры оформления, как это должно выглядеть в тексте, выделены *синим шрифтом*.

1) Название статьи

Название статьи представляется на русском и английском языках. Название статьи на русском языке должно соответствовать содержанию статьи. Англоязычное название должно быть грамотно с точки зрения английского языка, при этом по смыслу полностью соответствовать русскоязычному названию.

Оформление: Текст названия набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «полужирный». Точка в конце не ставится.

Пример:

Повышение надежности электронных компонентов
The Increasing of dependability of electronic components

2) Фамилия И.О. автора (авторов)

Данный структурный элемент для каждого автора включает:

- на русском языке – его фамилию и инициалы, после которых указывается сноска в виде цифры, набранной верхним индексом (надстрочным), которая ссылается на указание места работы автора. У фамилии автора, который будет контактировать с редакцией, также верхним индексом (после цифры) указывается символ «*»;

- на английском языке – его фамилию, имя и отчество в формате «Имя, инициал отчества, фамилия» (Ivan I. Ivanov). Фамилию на английском языке необходимо указывать в соответствии с заграничным паспортом или так, как она была указана в ранее опубликованных статьях. Если автор не имеет заграничного паспорта и/или публикаций, для транслитерации фамилии и имени необходимо использовать стандарт BSI.

Оформление: Текст ФИО набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «полужирный». ФИО разделяются запятой, точка в конце не ставится.

Пример:

Иванова А.А.[1], Петров В.В.[2*]
Anna A. Ivanova, Victor V. Petrov

3) Место работы автора (авторов)

Место работы авторов приводится на русском языке, перед указанием места набирается верхним индексом (надстрочным) соответствующая цифра сноски, указывающая на имя автора.

Оформление: Текст места работы набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный». Каждое место работы – с новой строки, точки в конце не ставятся.

Пример:

[1]Московский государственный университет, Российская Федерация, Москва
[2]Санкт-Петербургский институт теплоэнергетики, Российская Федерация, Санкт-Петербург

4) Адрес электронной почты автора, который будет вести переписку с редакцией

Оформление: Текст адреса набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный», все символы – строчные. Перед адресом набирается символ сноски «*». Точка в конце не ставится.

Пример:

*petrov_vv@aaa.ru

5) Резюме статьи

Данный структурный элемент включает структурированную аннотацию статьи объемом не менее 350 слов и не более 400 слов. Резюме представляется на русском и английском языках. Резюме должно содержать (желательно в явной форме) следующие разделы: Цель; Методы; Результаты; Выводы (на англ. яз.: Objective, Methods, Results, Conclusion). В резюме статьи не следует включать впервые введенные термины, аббревиатуры (за исключением общеизвестных), ссылки на литературу.

Оформление: Текст резюме набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный», кроме слов «**Резюме.**», «**Цель.**», «**Методы.**», «**Выводы.**» («**Objective.**», «**Methods.**», «**Results.**», «**Conclusion.**»), которые (вместе с точкой) должны иметь начертание шрифта «полужирный». Текст резюме на отдельные абзацы не разделяется (набирается в один абзац).

Пример (на рус. яз.):

Резюме. Цель. Предложить подход … с учетом современных методик. **Методы.** В статье применяются методы математического анализа,…, теории вероятностей. **Результаты.** С использованием предложенного метода получено… **Заключение.** Предлагаемый в статье подход позволяет…

6) Ключевые слова

Указывается 5-7 слов по теме статьи. Желательно, чтобы ключевые слова дополняли резюме (аннотацию) и название статьи. Ключевые слова указываются на русском и английском языках.

Оформление: Текст набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный», кроме слов «**Ключевые слова:**» («**Keywords:**») которые (вместе с двоеточием) должны иметь начертание «полужирный». Текст на отдельные абзацы не разделяется (набирается в один абзац). В конце ставится точка.

Пример (на рус. яз.):

Ключевые слова: надежность, функциональная безопасность, технические системы, управление рисками, техническая эффективность.

7) Текст статьи

Рекомендуется структурировать текст статьи в виде следующих разделов: Введение, Обзор источников, Методы, Результаты, Обсуждение, Заключение (или выводы). Рисунки и таблицы включаются в текст статьи (положение рисунков должно быть «в тексте», а не «за текстом» или «перед текстом»; без «обтекания текстом»).

Оформление:

Заголовки разделов набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, с абзацным отступом слева 1,25 см. Начертание шрифта «полужирный». Заголовки разделов (кроме введения и заключения (выводов)) могут иметь нумерацию арабскими цифрами с точкой после номера раздела. Номер с точкой отделяются от заголовка неразрывным пробелом (Ctrl+Shift+Spacebar).

Текст разделов набирается шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, с абзацным отступом слева 1,25 см. Начертание шрифта «обычный» Текст разделов разделяется на отдельные абзацы. Абзацный отступ не применяется для абзаца, следующего за формулой и содержащего пояснения к формуле, например:

где n – количество изделий.

Пример:

1. Состояние вопроса повышения надежности электронных компонентов

Проведенный анализ отечественной и зарубежной литературы по теме исследования показал, что…

Рисунки (фотографии, скриншоты) должны быть хорошего качества, пригодные для печати. Разрешение рисунка – не хуже 300 dpi. Если рисунок представляет собой схему, диаграмму, чертеж и т.п., то желательно вставлять такой рисунок в текст в редактируемом формате (MS Visio). Все рисунки должны иметь подрисуночные подписи. Рисунки нумеруются арабскими цифрами, по порядку следования в тексте. Если рисунок в тексте один, то он не нумеруется. Отсылки на рисунки оформляются следующим образом: «На рис. 3 указано, что …» или «Указано, что … (см. рис. 3)». Сокращение «рис.» и номер рисунка (если он есть) всегда разделяются неразрывным пробелом (Ctrl+Shift+Spacebar). Подрисуночная подпись включает порядковый номер рисунка и его название. Располагается на следующей строке после рисунка и выравнивается по центру:

Рис. 2. Описание жизненно важных процессов

Точка после подрисуночной подписи не ставится. *При выравнивании по центру абзацный отступ всегда должен отсутствовать!* Все обозначения, приведенные на рисунках, необходимо пояснять в основном или подрисуночном тексте. Недопустимы отличия в обозначениях на рисунках и в тексте (включая различие прямых/наклонных символов). *При проблемах с верстkой рисунков, вставленных в текст, авторы должны по запросу редакции предоставить данные рисунки в графическом формате, в виде файлов с расширениями* *.tiff, *.png, *.gif, *.jpg, *.eps.

Таблицы должны быть хорошего качества, пригодные для печати. Таблицы должны быть пригодны для редактирования (а не отсканированные или в виде рисунков). Все таблицы должны иметь заголовки. Таблицы нумеруются арабскими цифрами, по порядку следования в тексте. Если таблица в тексте одна, то она не нумеруется. Отсылки на таблицы оформляются следующим образом: «В табл. 3 указано, что …» или «Указано, что … (см. табл. 3)». Сокращение «табл.» и номер таблицы (если он есть) всегда разделяются неразрывным пробелом (Ctrl+Shift+Spacebar). Заголовок таблицы включает порядковый номер таблицы и ее название. Располагается на строке, предшествующей таблице и выравнивается по центру:

Табл. 2. Описание жизненно важных процессов

Точка после заголовка таблицы не ставится. *При выравнивании по центру абзацный отступ всегда должен отсутствовать!* Все обозначения (символы), приведен-

ные в таблицах, необходимо пояснять в основном тексте. Недопустимы отличия в обозначениях в таблице и в тексте (включая различие прямых/наклонных символов).

Математические обозначения в тексте набираются заглавными и строчными буквами латинского, греческого и русского алфавитов. Латинские символы всегда набираются наклонным шрифтом (курсивом), кроме обозначений функций, таких как sin, cos, max, min и т.п., которые набираются прямым шрифтом. Греческие и русские символы всегда набираются прямым шрифтом. Размер шрифта основного текста и математических обозначений (включая формулы) должен быть одинаков; верхние и нижние индексы масштабируются в MS Word автоматически.

Формулы могут быть включены непосредственно в текст, например:

Пусть $y = a \cdot x + b$, тогда…,

либо набираться в отдельной строке, с выравниванием по центру, например:

$$y = a \cdot x + b.$$

При наборе формул как в тексте, так и в отдельной строке, знаки препинания должны ставиться по обычным правилам – точка, если формулой заканчивается предложение; запятая (или отсутствие знака препинания), если предложение после формулы продолжается. Для разделения формулы и текста рекомендуется для строки с формулой устанавливать вертикальные отступы (6 пт перед, 6 пт после). Если в тексте статьи делается отсылка на формулу, то такая формула обязательно набирается отдельной строкой, по правому краю которой указывается номер формулы в круглых скобках, например:

$$y = a \cdot x + b. \qquad (1)$$

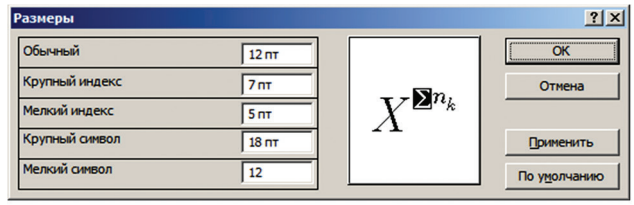
Если формула набирается в отдельной строке и имеет номер, то данная строка выравнивается по правому краю, а формула и номер разделяются знаком табуляции; позиция табуляции (в см) выбирается таким образом, чтобы формула располагалась примерно по центру. Формулы, на которые в тексте делаются отсылки, нумеруются арабскими цифрами, по порядку следования в тексте.

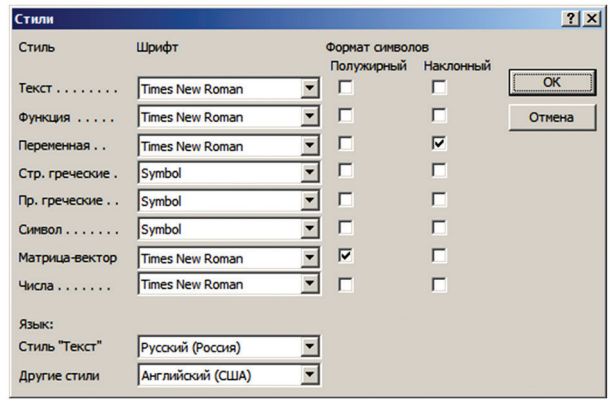
Простые формулы следует набирать без применения формульного редактора (использовать в MS Word русские и латинские буквы, а также меню «Вставка» + «Символ», если требуются греческие буквы и математические операторы), с соблюдением требуемого наклона для латинских символов, например:

$$\Omega = a + b \cdot \theta.$$

Если формула набирается без применения редактора формул, то между буквами и знаками «+», «–», «=» должны быть набраны неразрывные пробелы (Ctrl+Shift+Spacebar).

Сложные формулы набираются с применением редактора формул. Для отсутствия проблем с редактированием формул и их верстской настоятельно рекомендуется использовать редакторы Microsoft Equation 3.0 или MathType 6.x. Для обеспечения корректного ввода формул (размер символов, их наклон и т.д.) рекомендуемые настройки редактора приведены на рисунках ниже.





При наборе формул в редакторе формул, если требуются скобки, то следует использовать скобки из формульного редактора, а не набирать их на клавиатуре (для корректной высоты скобок в зависимости от содержимого формулы), например (Equation 3.0):

$$Z = \frac{a \cdot \left(\sum_{i=1}^{n} x_i + \sum_{j=1}^{m} y_i \right)}{n + m}. \qquad (2)$$

Сноски в тексте нумеруются арабскими цифрами, размещаются постранично. В сносках могут быть размещены: ссылки на анонимные источники в сети Интернет, ссылки на учебники, учебные пособия, ГОСТы, статистические отчеты, статьи в общественно-политических газетах и журналах, авторефераты, диссертации (если нет возможности процитировать статьи, опубликованные по результатам диссертационного исследования), комментарии автора.

Отсылка на библиографический источник указывается в тексте статьи в квадратных скобках, а источники приводятся в библиографическом списке в порядке их упоминания в тексте (затекстовые ссылки). Страница указывается внутри скобок, через запятую и пробел после номера источника: [6, с. 8]

8) Благодарности

В этом разделе указываются все источники финансирования исследования, а также благодарности людям, которые участвовали в работе над статьей, но не

являются ее авторами. Участие в работе над статьей подразумевает: рекомендации по совершенствованию исследования, предоставление пространства для исследования, ведомственный контроль, получение финансовой поддержки, одиночные виды анализа, предоставление реагентов/пациентов/животных/прочих материалов для исследования.

Оформление:

Сведения набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».

9) Библиографический список

В библиографический список включаются только рецензируемые источники (статьи из научных журналов и монографии), упоминающиеся в тексте статьи. Нежелательно включать в библиографический список авторефераты, диссертации, учебники, учебные пособия, ГОСТы, информацию с сайтов, статистические отчеты, статьи в общественно-политических газетах, на сайтах и в блогах. Если необходимо сослаться на такую информацию, следует поместить информацию об источнике в сноску.

При описании источника следует указывать его DOI, если удается его найти (для зарубежных источников удается это сделать в 95% случаев).

Ссылки на принятые к публикации, но еще не опубликованные статьи должны быть помечены словами «в печати»; авторы должны получить письменное разрешение для ссылки на такие документы и подтверждение того, что они приняты к печати. Информация из неопубликованных источников должна быть отмечена словами «неопубликованные данные/документы», авторы также должны получить письменное подтверждение на использование таких материалов.

В ссылках на статьи из журналов должны быть обязательно указаны год выхода публикации, том и номер журнала, номера страниц.

В описании каждого источника должны быть представлены все авторы.

Ссылки должны быть верифицированы, выходные данные проверены на официальном сайте журналов и/или издательств.

Оформление:

Оформление ссылок (в русскоязычной версии журнала) должно выполняться по ГОСТ Р 7.0.5-2008. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления.

Библиографические ссылки набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, с абзацным отступом слева 1,25 см. Начертание шрифта «обычный» (см. примеры оформления в ГОСТ Р 7.0.5). Каждая запись имеет нумерацию арабскими цифрами с точкой после номера раздела. Номер с точкой отделяются от записи неразрывным пробелом (Ctrl+Shift+Spacebar).

10) Сведения об авторах

Фамилия, имя, отчество полностью (на русском и английском языках); полный почтовый адрес (включая индекс, город и страну); полное наименование места работы, занимаемая должность; ученая степень, ученое звание, почетные звания; членство в общественных союзах, организациях, ассоциациях и т.д.; официальное англоязычное название учреждения (для версии на английском языке); адрес электронной почты; перечень и номера журналов, в которых ранее публиковались статьи автора; фото авторов для публикации в журнале.

Оформление:

Сведения набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».

11) Вклад авторов в статью

Следует указать подробно, каким из авторов что сделано в статье. Например: Автором А. выполнен анализ литературы по теме исследования, автором Б. разработана модель объекта в реальных условиях эксплуатации, выполнен расчет примера и т.д. Даже если у статьи один автор, то требуется указание его вклада.

Оформление:

Сведения набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».

12) Конфликт интересов

Конфликт интересов – это условия, при которых у людей возникают вступающие в конфликт или конкурирующие интересы, способные повлиять на принятие редакторского решения. Конфликты интересов могут быть потенциальными или осознанными, а также реально существующими. На объективность могут повлиять личные, политические, финансовые, научные или религиозные факторы.

Автор обязан уведомить редакцию о реальном или потенциальном конфликте интересов, включив информацию о конфликте интересов в статью.

Если конфликта интересов нет, автор должен также сообщить об этом. Пример формулировки: «Автор заявляет об отсутствии конфликта интересов».

Оформление:

Текст набираются шрифтом Times New Roman, 12 пт, междустрочный интервал 1,5 строки, выравнивание по ширине, без абзацного отступа слева. Начертание шрифта «обычный».