

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Главный редактор:

Шубинский Игорь Борисович – доктор технических наук, профессор, Эксперт Научного совета при Совете Безопасности РФ, генеральный директор ЗАО «ИБТранс» (Москва, Россия)

Заместители главного редактора:

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

Ястребенецкий Михаил Анисимович – доктор технических наук, профессор, главный научный сотрудник Государственного научно-технического центра ядерной и радиационной безопасности (Харьков, Украина)

Ответственный секретарь:

Замышляев Алексей Михайлович – доктор технических наук, заместитель Генерального директора ОАО «НИИАС» (Москва, Россия)

Технический редактор:

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

Председатель редакционного совета:

Розенберг Игорь Наумович – доктор технических наук, профессор, Генеральный директор ОАО «НИИАС» (Москва, Россия)

Сопредседатель редакционного совета:

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

РЕДАКЦИОННЫЙ СОВЕТ:

Бочков Александр Владимирович – кандидат технических наук, заместитель директора центра анализа рисков Научно-исследовательского института экономики и организации управления в газовой промышленности, ООО «НИИгазэкономика» (Москва, Россия)

Бочков Константин Афанасьевич – доктор технических наук, профессор, проректор по научной работе УО «Белорусский государственный университет транспорта» (Гомель, Белоруссия)

Гапанович Валентин Александрович – кандидат технических наук, старший советник президента ОАО «РЖД» (Москва, Россия)

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

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

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

Лецкий Эдуард Константинович – доктор технических наук, профессор, заведующий кафедрой «Автоматизированные системы управления» ФГБОУ ВПО «Московский государственный университет путей сообщения» (Москва, Россия)

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

Папик Любиш Р. – доктор технических наук, профессор, директор Исследовательского центра по управлению качеством и надёжностью (DQM), (Приевор, Сербия)

Соколов Борис Владимирович – Заслуженный деятель науки РФ, доктор технических наук, профессор, Лауреат премии Правительства РФ в области науки и техники, заместитель директора по научной работе Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), (Санкт-Петербург, Россия)

Уткин Лев Владимирович – доктор технических наук, профессор, профессор кафедры Телематики Санкт-Петербургского политехнического университета Петра Великого (Санкт-Петербург, Россия)

Юркевич Евгений Викторович – доктор технических наук, профессор, заведующий лабораторией Института проблем управления им. В.А. Трапезникова РАН (Москва, Россия)

Язов Юрий Константинович – доктор технических наук, профессор, главный научный сотрудник Федерального автономного учреждения «Государственный научно-исследовательский испытательный институт Федеральной службы по техническому и экспортному контролю» (Воронеж, Россия)

УЧРЕДИТЕЛЬ ЖУРНАЛА:
ООО «Журнал «Надежность»

Зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций. Регистрационное свидетельство ПИ № 77-9782 от 11 сентября 2001 года.

Официальный печатный орган Российской академии надежности

Издатель журнала
ООО «Журнал «Надежность»
Генеральный директор

Дубровская А.З.
Адрес: 109029, г. Москва,
ул. Нижегородская, д. 27, стр. 1, оф. 209
ООО «Журнал «Надежность»
www.dependability.ru
Отпечатано в ОАО «Областная типография
«Печатный двор». 432049, г. Ульяновск,
ул. Пушкирева, 27.

Подписано в печать 30.03.2017
Объем , Тираж 500 экз, Заказ №
Формат 60х90/8, Бумага глянец

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

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

СОДЕРЖАНИЕ

Структурная надежность. Теория и практика

Антонов А.В., Украинцев В.Ф., Чехович В.Е., Чепурко В.А. О планировании объема испытаний образцов новой техники	3
Кирпичников А.П., Васильев С.Н. Особенности современной микроэлектроники и вопросы построения систем управления высокой надежности и безопасности	10
Похабов Ю.П. Обеспечение надежности уникальных высокоответственных систем	17
Лабутин А.Г., Филин Б.П. Использование приведенных оценок эзари-прошана для анализа надежности систем	24

Функциональная надежность. Теория и практика

Климов С.М., Поликарпов С.В., Федченко А.В. Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий	32
---	----

Функциональная безопасность. Теория и практика

Бочков А.В., Жигирев Н.Н., Ридли А.Н. Метод восстановления вектора приоритетов альтернатив в условиях неопределенности или неполноты экспертных оценок	41
Шубинский И.Б., Замышляев А.М., Игнатов А.Н., Кибзун А.И., Платонов Е.Н. Применение системы автоматической сигнализации для снижения риска транспортных происшествий на железнодорожных станциях	49
Якимов О.С., Колчин А.Ф. Состояние и перспективы развития нормативного обеспечения в области функциональной безопасности	58
Гнеденко –Форум	63
Информация по книге И.Б.Шубинского: «Надежные отказоустойчивые информационные системы». Методы синтеза	65

О планировании объема испытаний образцов новой техники

Александр В. Антонов, Обнинский институт атомной энергетики (ИАТЭ НИЯУ МИФИ), Обнинск, Россия

Валерий А. Чепурко, Обнинский институт атомной энергетики (ИАТЭ НИЯУ МИФИ), Обнинск, Россия

Владимир Е. Чехович, Акционерное общество «Государственный научный центр Российской Федерации – Физико-энергетический институт им. А.И.Лейпунского» (АО «ГНЦ РФ-ФЭИ»), Обнинск, Россия

Владимир Ф. Украинцев, Акционерное общество «Государственный научный центр Российской Федерации – Физико-энергетический институт им. А.И.Лейпунского» (АО «ГНЦ РФ-ФЭИ»), Обнинск, Россия

Резюме. Статья является логическим продолжением работы [1]. В ней рассматриваются вопросы планирования объема испытаний высоконадежных объектов. В процессе разработки и изготовления новых образцов техники возникает задача определения их показателей надежности. Наиболее объективным способом определения характеристик надежности изделий является проведение натурных испытаний по определенному плану. Одним из широко применяемых планов испытаний является план $[N, U, T]$. Это план, при котором испытывается N невосстанавливаемых образцов в течение интервала времени от 0 до некоторого T . Предполагается, что в ходе испытаний k объектов отказывает, $N-k$ объектов проходят испытания успешно. Таким образом, по результатам эксперимента мы имеем смешанную выборку, в которой присутствует k наработок до отказа и $N-k$ цензурированных справа наблюдений. Если проверяемый объект высоконадежен, вполне возможна ситуация, что на некотором промежутке времени $[0, T]$ отказы не произойдут, т.е. k будет равно 0, в силу того вероятность отказа на этом промежутке времени крайне мала, а число испытываемых объектов ограничено. Тем не менее, даже в такой ситуации хотелось бы контролировать точность оценок, получаемых в ходе такого эксперимента. Понятно, что точность этих оценок будет зависеть не только от числа испытываемых объектов N , но и от длительности проведения эксперимента. Для фиксированного N , по мере увеличения времени наблюдения T , точность оценок повышается в силу того, что увеличивается доля полных наработок до отказа, а доля цензурированных уменьшается. Заметим, что когда речь идет об определении характеристик надежности сложных, дорогостоящих объектов, нет возможности поставить на испытания партию готовой продукции большого объема. Таким образом, возникает задача определения длительности проведения натурных испытаний и объема партии изделий, подлежащих испытаниям, при условии задания требований к точности получаемых в результате испытаний оценок характеристик надежности. Планирование объема осуществляется на основании требований изготовителя о необходимости подтвердить значение нижней оценки вероятности безотказной работы P_0 с заданной доверительной вероятностью в определенной временной точке t_0 . **Цель** работы состоит в определении объема испытаний партии готовой продукции $N(T)$, для которого выполнялось бы требование заказчика о достижении значения нижней доверительной границы вероятности безотказной работы с заданной с доверительной вероятностью $1 - \alpha$. Исследуется три распределения наработки до отказа: экспоненциальный закон распределения, распределение Вейбулла и распределение с линейной функцией интенсивности. Рассмотренные виды законов распределения позволяют исследовать поведение объектов, имеющих убывающую, постоянную и возрастающую функцию интенсивности отказов. **Методы.** В работе получены формулы расчета объема испытаний для разных длительностей проведения эксперимента. Для получения оценок используется метод максимального правдоподобия, методы исследования асимптотических свойств оценок с помощью информационного количества по Фишеру. **Выводы.** Полученные результаты, позволяют обоснованно подходить к планированию объема испытаний высоконадежных объектов. Результаты исследования показали, что чем больше длительность эксперимента, тем меньше изделий требуется поставить на испытания. Зависимость нелинейная, близкая к гиперболической и обусловлена как входными параметрами, так и параметризацией функции интенсивности отказов.

Ключевые слова: планирование объема испытаний, длительность эксперимента, вероятность безотказной работы, интенсивность отказа, нижняя оценка вероятности безотказной работы, уровень доверительной вероятности.

Формат цитирования: Антонов А.В., Украинцев В.Ф., Чехович В.Е., Чепурко В.А. О планировании объема испытаний образцов новой техники // Надежность. 2017. Т. 17, № 3. С. 3-9. DOI: 10.21683/1729-2646-2017-17-3-3-9.

Введение

В процессе разработки и изготовления новых образцов техники возникает задача определения их показателей надежности. Наиболее объективным способом определения характеристик надежности изделий является проведение натурных испытаний по определенному плану. В данной работе рассматривается план испытаний $[N, U, T]$. Это план, при котором испытывается N невосстанавливаемых образцов в течение интервала времени от 0 до некоторого T . Предполагается, что в ходе испытаний k объектов отказывает, $N-k$ объектов проходят испытания успешно. Таким образом, по результатам эксперимента мы имеем смешанную выборку, в которой присутствует k наработок до отказа и $N-k$ цензурированных справа наблюдений. Понятно, что точность получаемых оценок будет зависеть не только от числа испытываемых объектов N , но и от длительности проведения эксперимента. Для фиксированного N по мере увеличения времени наблюдения T точность оценок повышается в силу того, что увеличивается доля полных наработок до отказа, а доля цензурированных уменьшается. Заметим, что когда речь идет об определении характеристик надежности сложных, дорогостоящих объектов, нет возможности поставить на испытания партию готовой продукции большого объема. Таким образом, возникает задача определения длительности проведения натурных испытаний и объема партии изделий, подлежащих испытаниям, при условии задания требований к точности получаемых в результате испытаний оценок характеристик надежности.

Постановка задачи

Эксперимент проводится по плану $[N, U, T]$. Данный план означает, что испытывается N образцов в течение заданного интервала времени от 0 до T без замены отказавших изделий [2–4]. В ходе проведения испытаний наблюдается k отказов. Обозначим зафиксированные наработки $t_1, t_2, \dots, t_k$ v изделий проходят испытания успешно $v = N-k$ (v – число не отказавших образцов,

имеющих наработку T). Не отказавшие объекты формируют выборку цензурированных справа наработок. На рисунке 1 изображен план проведения эксперимента.

Так, образец №1 проработал без отказа до момента времени T . Второй образец отказал в момент времени t_2 и т.д.

Допустим, на какой-то момент времени t_0 нижняя граница доверительного интервала с заданной доверительной вероятностью $1-\alpha_0$ для ВБР $P(t_0)$ должна быть не менее $\underline{P}_0$, т.е.

$$\Pr(P(t_0) \geq \underline{P}_0) \geq 1-\alpha_0. \quad (1)$$

Очевидно, что этого можно добиться подбором объема испытаний $N(t_0)$ только в том случае, если истинная ВБР в этой точке $P(t_0)$ будет находиться правее $\underline{P}_0$. В противном случае задача будет неразрешимой.

Логично предположить, что на некоторый момент времени T ($T \geq t_0$) для обеспечения той же точности оценивания ВБР в точке t_0 потребуется объем испытаний партии готовой продукции $N(T)$, как минимум равный объему, определенному для точки t_0 . Это обусловлено в первую очередь тем, что ВБР – невозрастающая функция. Обозначим необходимые объемы испытаний $N(t_0)$ и $N(T)$.

Цель исследования состоит в определении объема испытаний партии готовой продукции $N(T)$, для которого выполнялось бы требование заказчика о достижении значения нижней доверительной границы вероятности безотказной работы с заданной доверительной вероятностью $1-\alpha$. В ходе исследования определим, как соотносятся объемы испытаний $N(T)$ и $N(t_0)$ при условии, что заданы одинаковые требования к точности получаемого результата для разных интервалов времени проведения испытаний. В ходе исследования рассмотрим различные параметризации функции интенсивности отказов $\lambda(t)$.

При решении задачи будем предполагать, что функция интенсивности отказов задается одной из формул [1, 2]:

$$\lambda(t) = \lambda; \quad (2)$$

$$\lambda(t) = \lambda_1 + \lambda_2 t; \quad (3)$$

$$\lambda(t) = \lambda_1 t^{\lambda^2}. \quad (4)$$

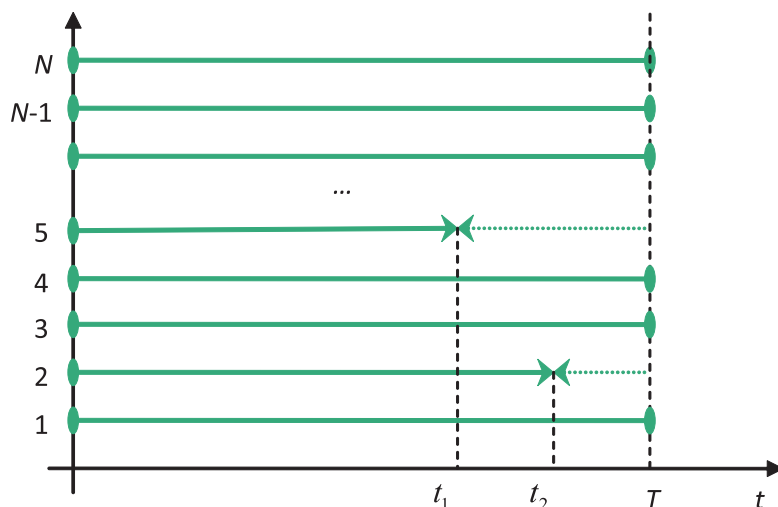


Рисунок 1 – План проведения эксперимента

Выражение (2) (интенсивность постоянна) характерно для экспоненциального распределения наработки до отказа, формула (3) – для функции распределения с линейной интенсивностью отказов и функция (4) – для закона распределения Вейбулла.

Для упрощения расчетов, как и в работе [1], приведем рассматриваемую модель к виду:

$$\lambda(t) = \lambda g(t) \quad (5)$$

где $g(t)=1$ соответствует экспоненциальному распределению,

$g(t)=a+bt$ – распределению с линейной функцией интенсивности отказов, (6)

$g(t)=t^a$ распределению Вейбулла. (7)

Функция $g(t)$ должна удовлетворять двум основным требованиям:

$$g(t) \geq 0,$$

а интегральная функция

$$G(t) = \int_0^t g(\tau) d\tau \rightarrow \infty \text{ при } t \rightarrow \infty.$$

При этом будем предполагать, что коэффициенты a , b в (6), (7) известны, неизвестным и оцениваемым по выборке является параметр λ .

В следующем разделе определим, как точность оценивания этого параметра зависит от длительности T проведения эксперимента и, в дальнейшем, выведем условие ее сохранения при данном плане эксперимента.

Оценка параметра λ и определение ее точности

Известно [2], что точность оценки, определяемой по методу максимального правдоподобия (ММП-оценки), обусловлена информационным количеством Фишера.

Вначале найдем количество информации по Фишеру, содержащееся в исходной статистике. Функция правдоподобия, соответствующая выбранному плану эксперимента $[N, U, T]$ будет выглядеть следующим образом:

$$\begin{aligned} L(\tilde{t}; T; \lambda) &= \prod_{i=1}^k f_{t_i}(t_i; \lambda) \prod_{j=1}^v P_{t_j}(T; \lambda) = \\ &= \lambda^k \cdot \prod_{i=1}^k g(t_i) \cdot \exp \left(-\lambda \left(\sum_{i=1}^k G(t_i) + vG(T) \right) \right), \end{aligned}$$

где $f_i(t, \lambda) = \lambda g(t) \exp(-\lambda G(t))$ – плотность распределения наработки до отказа.

Логарифмическая функция правдоподобия:

$$l(\tilde{t}; T; \lambda) = \ln L = k \ln \lambda + \sum_{i=1}^k g(t_i) - \lambda \left(\sum_{i=1}^k G(t_i) + vG(T) \right).$$

Определяем частную производную.

$$\frac{\partial}{\partial \lambda} l(\tilde{t}; T; \lambda) = \frac{k}{\lambda} - \left(\sum_{i=1}^k G(t_i) + vG(T) \right). \quad (8)$$

Здесь $k = \sum_{i=1}^N I\{t_i \leq T\}$ является случайной величиной

(с.в.), распределенной согласно биномиальному закону:

$$\text{Bin}(N; F_i(T)) = \text{Bin}(N; 1 - e^{-\lambda G(T)}). \quad (9)$$

Информационное количество (дисперсия правой части уравнения (8)) будет определяться суммой трех слагаемых. Найдем по отдельности каждое.

$$\text{var} \left[\frac{k}{\lambda} \right] = \frac{NP_i(T)(1 - P_i(T))}{\lambda^2} = \frac{Ne^{-\lambda G(T)}(1 - e^{-\lambda G(T)})}{\lambda^2}.$$

$$\begin{aligned} \text{var} \left[\sum_{i=1}^k G(t_i) + vG(T) \right] &= \text{var} \left[\sum_{i=1}^N G(t_i \wedge T) \right] = \\ &= \frac{N(1 - 2\lambda G(T)e^{-\lambda G(T)} - e^{-2\lambda G(T)})}{\lambda^2}. \end{aligned}$$

$$\begin{aligned} \text{cov} \left[\frac{k}{\lambda}; \sum_{i=1}^N G(t_i \wedge T) \right] &= \\ &= \frac{1}{\lambda} \text{cov} \left[\sum_{i=1}^N I\{G(t_i) \leq G(T)\}; \sum_{i=1}^N G(t_i) \wedge G(T) \right] = \\ &= \frac{1}{\lambda} \left[\sum_{i=1}^N E(G(t_i \wedge T) \cdot I\{t_i \leq T\}) - E(G(t_i \wedge T)) E I\{t_i \leq T\} \right] = \\ &= \frac{N}{\lambda^2} (e^{-\lambda G(T)} - e^{-2\lambda G(T)} - \lambda G(T) e^{-\lambda G(T)}). \end{aligned}$$

Сложив дисперсии с ковариацией, определяем информационное количество Фишера:

$$I(\tilde{t}; T; \lambda) = \frac{N}{\lambda^2} (1 - e^{-\lambda G(T)}) = \frac{N}{\lambda^2} (1 - P(T)) = \frac{NF_i(T)}{\lambda^2}, \quad (10)$$

где $F_i(T)$ – функция распределения наработки до отказа.

Теперь построим ММП-оценку (оценку по методу максимального правдоподобия) для λ :

$$\hat{\lambda}_T = \frac{k}{\sum_{i=1}^N G(t_i \wedge T)}. \quad (11)$$

Эта оценка получается приравниванием правой части уравнения (8) к нулю. Известно, что ММП-оценка асимптотически несмещенная, состоятельная, асимптотически эффективна и асимптотически нормальна. Таким образом,

$$\hat{\lambda}_T \overset{as}{\sim} \text{Norm} \left(\lambda; \frac{1}{I(\tilde{t}; T; \lambda)} \right) = \text{Norm} \left(\lambda; \frac{\lambda^2}{NF_i(T)} \right). \quad (12)$$

В следующем разделе исследуем количество информации по Фишеру.

Исследование оценки $\hat{\lambda}_T$

Введем обозначение числителя информационного количества по Фишеру (10):

$$K(T) = NF_{\lambda}(T). \quad (13)$$

Очевидно, что $K(T)$ будет зависеть и от параметра λ , поскольку от него зависит функция распределения $F_{\lambda}(T)$, однако, нас в первую очередь будет интересовать зависимость введенного показателя от времени. По смыслу $K(T)$ будет математическим ожиданием с.в. k , равной среднему числу произошедших отказов на момент времени T , которая распределена согласно закону (9).

В силу известного асимптотического свойства функции распределения

$$K(T) \xrightarrow{T \rightarrow \infty} N. \quad (14)$$

Очевидно, что рано или поздно откажут все N образцов. При этом оценка (11) будет стремиться к оценке, определяемой по полной выборке:

$$\hat{\lambda}_T = \frac{k}{\sum_{i=1}^N G(t_i \wedge T)} \xrightarrow{T \rightarrow \infty} \hat{\lambda}_{\infty} = \frac{N}{\sum_{i=1}^N G(t_i)}. \quad (15)$$

Если объем испытаний N является константой, не зависящей от времени, то функция $K(T)$, как и функция $F_{\lambda}(T)$, будет неубывающей, причем $K(0)=0$.

Рассмотрим условие, которое будет обеспечивать достижение необходимой нижней границы ВБР в точке t_0 . При выбранном способе оценки ВБР ее нижняя доверительная граница будет $\underline{P}_0$. Эта величина определяется путем вычисления верхней границы параметра λ : $\underline{P}_0 = e^{-\bar{\lambda}_{t_0} G(t_0)}$, где $\bar{\lambda}_{t_0}$ – верхняя граница показателя λ , вычисленная для случая, если бы испытания образцов заканчивались в момент времени t_0 . Определяться этот показатель будет путем решения уравнения

$$1 - \alpha_0 = P(\hat{\lambda}_{t_0} < \bar{\lambda}_{t_0}) \approx \Phi\left(\frac{\bar{\lambda}_{t_0} - \lambda}{\lambda \sqrt{K(t_0)}}\right), \quad (16)$$

где $\Phi(x)$ – функция распределения стандартного нормального закона $\text{Norm}(0,1)$. В результате решения уравнения (16) получим:

$$\bar{\lambda}_{t_0} = \lambda \left(1 + \frac{u_{1-\alpha_0}}{\sqrt{K(t_0)}}\right).$$

Если испытания будут продолжаться до момента времени T , то и верхняя граница параметра будет определяться путем решения уравнения, подобного (16), где t_0 заменяется на T . В результате получится следующее соотношение:

$$\bar{\lambda}_T = \lambda \left(1 + \frac{u_{1-\alpha_0}}{\sqrt{K(T)}}\right), \quad (17)$$

где $u_{1-\alpha_0}$ – квантиль нормального закона $\text{Norm}(0,1)$ уровня $1-\alpha_0$.

Оценка (17) будет применяться для вычисления нижней границы ВБР в точке t_0 . Согласно сформулированной цели исследования необходимо обеспечить выполнение

условия, чтобы нижняя оценка ВБР, вычисленная с доверительной вероятностью $1-\alpha_0$ была не менее $\underline{P}_0$, не зависимо от длительности проведения экспериментальных наблюдений. Так как интенсивность отказов взаимно однозначно выражается через ВБР, то аналогичное условие можно сформулировать и для интенсивности. Следовательно, для произвольного положительного момента времени T можно записать:

$$\bar{\lambda}_T = \bar{\lambda}_{t_0}. \quad (18)$$

Таким образом, необходимо подобрать такой объем партии испытываемой продукции, чтобы верхняя оценка интенсивности отказов $\bar{\lambda}_T$ не зависела от длительности наблюдений. Другими словами, точность оценивания параметра λ на момент времени t_0 должна быть такой же, как и на момент времени T . Этого можно добиться, полагая постоянной величиной количество информации Фишера. Это условие запишется как $K(T)=\text{const}$.

Условие сохранения точности оценки λ

Погрешность оценивания в моменты времени t_0 и T будет одинаковой, если будут равны информационные количества в этих точках. Равенства количеств информации будем добиваться подбором необходимого объема испытаний $N(T)$ и $N(t_0)$.

Условие равенства информационных количеств для двух произвольных моментов времени t_0 и T будет выглядеть следующим образом:

$$I(\bar{t}; t_0; \lambda) = I(\bar{t}; T; \lambda). \quad (19)$$

Это условие (19) обеспечит такую же точность оценки неизвестного параметра λ по данным эксперимента $(N(T), U, T)$, как если бы мы оценивали λ по данным опыта $(N(t_0), U, t_0)$.

Из (10), (14) и (19) следуют свойства:

$$\frac{N(T)}{N(t_0)} = \frac{F(t_0)}{F(T)} \text{ или}$$

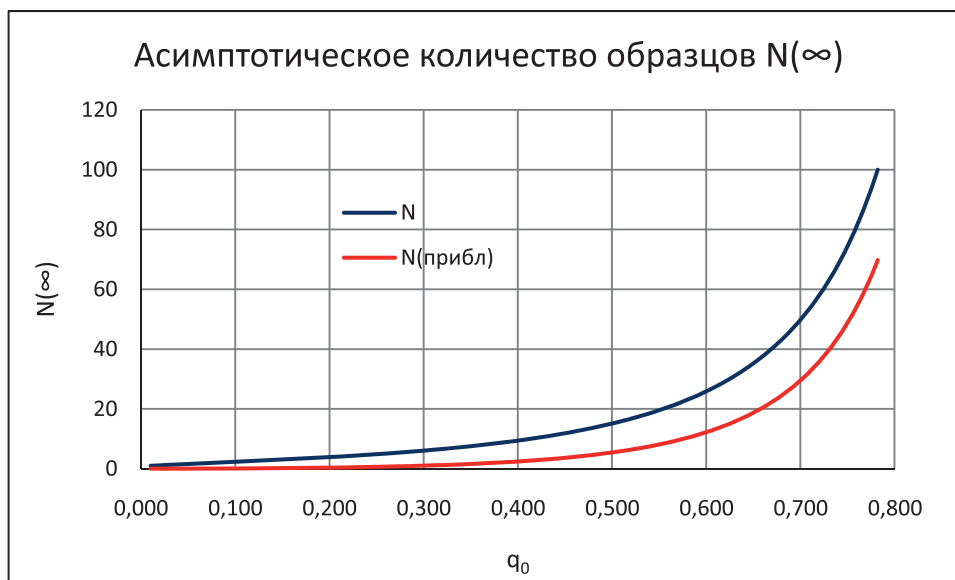
$$K(T) = \text{Const} = K(t_0) = Ek(t_0) = K(\infty) = N(\infty). \quad (20)$$

Таким образом, для любого T константа $K(T)$ будет равна как ожидаемому числу отказов на момент времени t_0 , так и количеству образцов $N(\infty)$. В следующем разделе определим константу $N(\infty)$.

Решение задачи

В выражении (15) определена оценка параметра λ при $T \rightarrow \infty$. Определим асимптотическое количество образцов $N(\infty)$ исходя из точного распределения оценки $\hat{\lambda}_{\infty}$. Известно [8], что с.в. $2\lambda G(t_i)$ будет иметь распределение хи-квадрат с двумя степенями свободы: $2\lambda G(t_i) \sim \chi_2^2$. В силу независимости слагаемых:

$$2\lambda \sum_{i=1}^N G(t_i) \sim \chi_{2N}^2. \quad (21)$$

Рисунок 2 – Точные и приближенные значения для $N(\infty)$

Утверждение (21) позволяет построить правосторонний доверительный интервал для параметра λ .

$$\Pr(\hat{\lambda}_{\infty} \leq \bar{\lambda}) = \Pr\left(2\lambda \sum_{i=1}^N G(t_i) \geq \frac{2\lambda N}{\bar{\lambda}}\right) = 1 - \alpha_0.$$

Откуда получаем трансцендентное уравнение для нахождения $N(\infty)$:

$$\frac{\chi_{\alpha_0}^2(2N)}{2N} = \frac{\lambda}{\bar{\lambda}} = \frac{\ln P_0}{\ln \underline{P}_0} = q_0, \quad (22)$$

где $\chi_{\alpha_0}^2(2N)$ – квантиль распределения хи-квадрат с $2N$ степенями свободы уровня α_0 .

В табл. 1 приведен пример расчетов асимптотических значений $N(\infty)$ для различных q_0 .

Можно воспользоваться асимптотическим распределением оценки (12) и, решая уравнение (16) относительно N получить следующий результат:

$$N(\infty) \approx \left(\frac{u_{1-\alpha_0} q_0}{1 - q_0}\right)^2. \quad (23)$$

Анализ (23) показал, что приближенный расчет обладает изрядной долей оптимистичности (см. рис. 2) и оценка необходимого объема испытаний получается существенно заниженной.

Если ВБР P_0 в точке t_0 неизвестна, то можно, по аналогии с работой [1], предположить:

$$P_0 = \frac{1 + \underline{P}_0}{2}. \quad (24)$$

Таблица 1. Асимптотические значения для числа испытаний ($\alpha_0=0,05$)

q_0	0,051	0,178	0,273	0,342	0,394	0,436	0,469	0,498	0,522	0,543
$N(\infty)$	1	2	3	4	5	6	7	8	9	10

Таблица 2 – Значения $N(\infty)$ в зависимости от α и $\underline{P}_0$.

$\alpha \backslash \underline{P}_0$	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	0,95	0,99	0,999
0,01	5,08	6,54	7,81	8,98	10,09	11,16	12,19	13,19	14,16	14,64	15,02	15,11
0,02	4,10	5,25	6,26	7,18	8,06	8,90	9,71	10,50	11,27	11,65	11,95	12,01
0,03	3,53	4,52	5,37	6,16	6,90	7,61	8,30	8,97	9,62	9,94	10,19	10,25
0,04	3,14	4,01	4,75	5,44	6,09	6,72	7,32	7,90	8,47	8,75	8,97	9,02
0,05	2,84	3,62	4,28	4,90	5,48	6,04	6,57	7,09	7,60	7,85	8,04	8,09
0,06	2,60	3,30	3,91	4,46	4,99	5,49	5,97	6,44	6,90	7,12	7,30	7,34
0,07	2,40	3,04	3,59	4,10	4,58	5,03	5,47	5,90	6,31	6,52	6,68	6,72
0,08	2,23	2,82	3,32	3,79	4,23	4,64	5,05	5,44	5,82	6,00	6,15	6,18
0,09	2,08	2,62	3,09	3,52	3,92	4,31	4,68	5,04	5,39	5,56	5,69	5,72
0,1	1,95	2,45	2,89	3,28	3,65	4,01	4,35	4,69	5,01	5,17	5,29	5,32

На самом деле, в силу сильной асимметрии биномиального распределения в случае высоконадежного оборудования будет выполняться неравенство $P_0 > \frac{1+P_0}{2}$. Поэтому $q_0 < \ln \frac{1+P_0}{2} / \ln P_0$ и оценка асимптотического значения $N(\infty)$ будет завышена, т.е. будет пессимистической оценкой.

В табл. 2 приведены рассчитанные значения $N(\infty)$ в зависимости от уровня значимости α и нижней границы ВБР P_0 .

Для оценки объема испытаний в произвольной точке t осталось применить (20).

Из (20) следует $N(T) = \frac{N(\infty)}{F(T)}$. Поскольку истинное значение параметра λ неизвестно, можно оценить его из условия $\lambda = -\frac{\ln P_0}{G(t_0)}$. Откуда

$$N(T) = \frac{N(\infty)}{1 - P_0^{G(T)/G(t_0)}}. \quad (25)$$

Зависимость от времени при малых $\lambda G(T)$ почти гиперболическая относительно $G(T)$.

$$N(T) \approx \frac{N(\infty)}{\lambda G(T)}. \quad (26)$$

На рис. 3 изображено поведение необходимого объема испытаний (25) в зависимости от T в относительной временной шкале T/t_0 . Входные параметры следующие: $P_0=0,95$; $\alpha_0=0,05$, $t_0=5$, $N(\infty)=7,85$ (см. табл. 2). Параметры распределения при проведении расчетов выбирались следующий: для распределения Вейбулла параметр $a=1,1$. Для модели с линейно-возрастающей функцией интенсивности $a=1$; $b=0,1$.

Можно заметить, что модели с возрастающей функцией интенсивности в сравнении с моделью, в которой интенсивность отказов постоянна, требуют относительно меньшего числа испытаний.

Заключение

Получены результаты, позволяющие обоснованно подходить к планированию объема испытаний высоконадежных объектов. В качестве исходной информации используется информация, предоставляемая изготовителем о необходимости подтвердить нижнюю границу ВБР изделия с заданной доверительной вероятностью. Полученные в статье формулы позволили провести исследования зависимости объема испытаний от длительности эксперимента. Результаты исследования показали, что чем больше длительность эксперимента, тем меньше изделий требуется поставить на испытания. Причем эта зависимость нелинейная, обусловлена параметризацией функции интенсивности отказа. Получены новые асимптотические результаты, позволяющие адекватно оценивать количество испытаний для заданного промежутка времени.

Библиографический список

1. Антонов А.В. К вопросу планирования объема испытаний образцов новой техники. / Антонов А.В., Чепурко В.А., Чехович В.Е., Украинцев В.Ф. *Надежность*. 2016;(3):3-7. DOI:10.21683/1729-2640-2016-16-3-3-7
2. Антонов А.В. Теория надежности. Статистические модели: Учеб. пособие/ Антонов А.В., Никулин М.С., Никулин А.М., Чепурко В.А. – М.: ИНФРА-М. 2015. – 576 с.
3. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. – М.: «НАУКА», 1965. – 524 с.

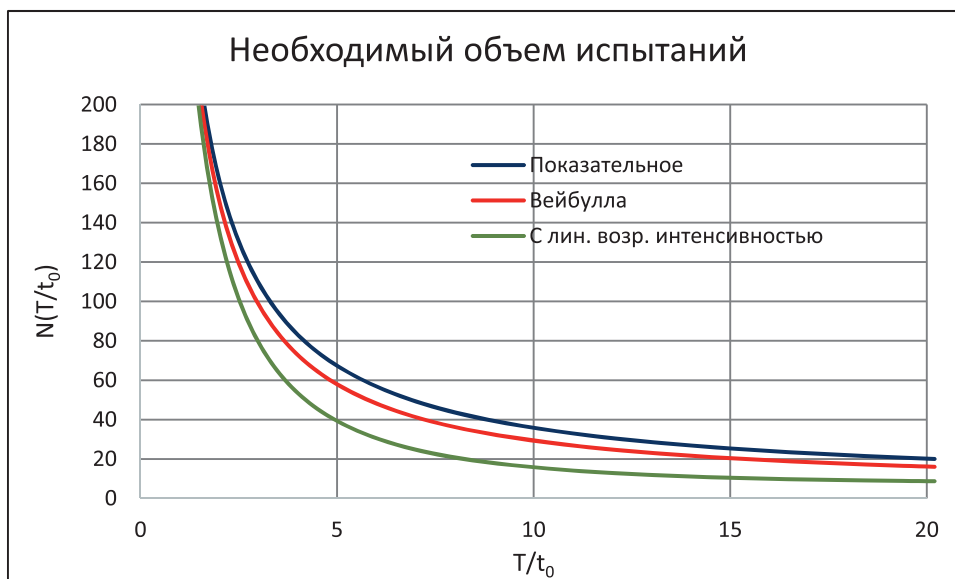


Рисунок 3 – Зависимость объема испытаний от времени при различных моделях распределения

4. Надежность технических систем: Справочник. Ю. К. Беляев. В. А. Богатырев. В. В. Болотин и др.; Под ред. И. А. Ушакова. — М.: Радио и связь, 1985. — 608 с. ил.

5. Антонов А.В. Статистические модели в теории надежности: Учеб. пособие/ Антонов А.В., Никулин М.С. — М.: Абрис. 2012. — 390 с.

6. Надежность технических систем: Справочник. Ю.К. Беляев. В.А. Богатырев. В.В. Болотин и др.; Под ред. И.А. Ушакова. — М.: Радио и связь. 1985. — 608 с. ил.

7. Определительные испытания на надежность. Ю.Г. Заренин. И.И. Стоянова. — М.: Изд-во Стандартов. 1978. — 168 с.

8. Крамер Г. Математические методы статистики. — М.: Мир. 1975. — 648 с.

9. Антонов А.В. Системный анализ: Учебник для вузов. — М.: Высш. шк. 2008. — 454 с.

10. Дейвид Г. Порядковые статистики М.: Наука. главная редакция физико-математической литературы. 1979 г. — 336 с.

Сведения об авторах

Александр В. Антонов — доктор технических наук, профессор. Обнинский институт атомной энергетики НИЯУ МИФИ, профессор кафедры АСУ. Россия, Обнинск, e-mail: antonov@iate.obninsk.ru

Владимир Ф. Украинцев — кандидат физико-математических наук, доцент. АО «Государственный научный центр Российской Федерации — Физико — энергетический институт им. А.И. Лейпунского», ведущий специалист. Россия, Обнинск, e-mail: ukraintsev@mail.ru

Владимир Е. Чехович — АО «Государственный научный центр Российской Федерации — Физико — энергетический институт им. А.И. Лейпунского», начальник отдела. Россия, Обнинск, e-mail: 89158916216@rambler.ru

Валерий А. Чепурко — кандидат физико-математических наук, доцент. Обнинский институт атомной энергетики НИЯУ МИФИ, доцент каф. АСУ. Россия, Обнинск, e-mail: chepurko@iate.obninsk.ru

Поступила 22.03.2017

Особенности современной микроэлектроники и вопросы построения систем управления высокой надежности и безопасности

Алексей П. Кирпичников, Институт проблем управления им. В.А.Трапезникова РАН, Москва, Россия
Станислав Н. Васильев, Институт проблем управления им. В.А.Трапезникова РАН, Москва, Россия

Резюме. Цель. Обратить внимание читателей на тенденции роста количества техногенных катастроф, увеличение ущерба от них, возрастание количества человеческих жертв и связь этого феномена с микропроцессорными системами автоматики. Приводятся доводы о необходимости построения техники с повышенным функционалом безопасности в условиях воздействия многократно возросших аномальных природных и техногенных факторов. Описываются и анализируются специфика систем управления объектами критического приложения и последствия пренебрежения дополнительным контролем схемотехники и программного обеспечения. Особо отмечается возрастание риска от введения беспилотных технологий и массового их использования на железнодорожном и автомобильном транспорте. В статье рассматриваются проблемы устойчивости систем управления к сбоям и внешним воздействиям в зависимости от примененной элементной базы. Приводится статистика техногенных катастроф, рассматривается их связь с показателями неустойчивости систем управления. Отдельное внимание уделено особенностям современной микроэлектронной элементной базы и влиянию прогресса в этой области на помехоустойчивость систем и их сбойность. При этом отмечается увеличение количества опасных отказов систем, построенных на микроконтроллерах, выполненных по технологическим нормам 0,13 мкм и ниже. Значительное место отводится исследованию особенностей современных кристаллов, их топологии, в частности, главного элемента системы управления – микроконтроллера и цифрового сигнального процессора, анализируется влияние на кристалл внешних воздействий. Рассмотрены проблемы КМОП топологии в микропроцессорных узлах, показана зависимость увеличения влияния помех с переходом на новые модификации КМОП технологий. Обращается внимание на необходимость подготовки соответствующего класса специалистов для работы с этими системами, владеющих не только программированием, но обладающих глубокими знаниями в области физики, основ построения систем управления и их устойчивости. **Результаты.** Проведена сравнительная оценка устойчивости КМОП технологий с проектными нормами 0,5 мкм и 130 нм и получена разница значений пороговой мощности воздействия более 4000 раз. Отмечается, что большинство разработчиков, программирующих подобные системы, вводятся в заблуждение отсутствием у фирм-производителей электронных компонентов какой-либо открытой информации о сбойности процессорных элементов. Принимая за основной параметр цифры надежности изделия, они неверно оценивают уровень полноты безопасности, ошибочно используя вместо параметров сбойности цифры надежности микросхем, предоставляемые изготовителем. При этом стандартные методы повышения уровня безопасности, применяемые разработчиками (в частности, резервирование), часто оказываются неэффективными. **Выводы.** Для построения систем управления высокой надежности и безопасности необходимо учитывать особенность современной элементной базы, принимая во внимание факт, что новые поколения современных микросхем, ввиду своей сбойности, часто непригодны для построения высоконадежных систем. Представляется актуальным дорабатывать существующие стандарты и создавать новые механизмы повышения устойчивости и безопасности систем. Также отмечается необходимость обязательной поддержки соответствующего уровня образования и информированности широкого круга разработчиков, работающих с системами управления в областях транспорта, энергетики, систем промышленной автоматики, вооружений, и др. в части важности обеспечения необходимого уровня функциональной безопасности.

Ключевые слова: микропроцессорные системы управления, микроэлектронная элементная база, техногенные катастрофы, сбойные ошибки, УПБ, блок безопасности.

Формат цитирования: Кирпичников А.П., Васильев С.Н. Особенности современной микроэлектроники и вопросы построения систем управления высокой надежности и безопасности // Надежность. 2017. Т. 17, № 3. С. 10-16. DOI: 10.21683/1729-2646-2017-17-3-10-16

Введение

В последние десятилетия проявляется угрожающая тенденция непрерывного роста количества техногенных катастроф, сопровождающихся все большим ущербом и возрастанием количества жертв. Одной из основных причин следует полагать повсеместное внедрение микропроцессорных систем управления на замену старым релейным системам без учета особенностей современной элементной базы. Специфика систем управления объектами критического приложения предполагает очень высокий уровень безопасности, который практически недостижим на новых элементах без использования далеко не тривиальных методов. Как результат, объекты с наиболее напряженным графиком эксплуатации при модернизации систем управления неминуемо попадают в группу риска. Специалистам в области обработки сигналов и построений систем безопасности нужно обратить на это особое внимание и быть готовым к очень ответственной напряженной работе, что не всегда характерно для нового времени и даже непривычно для молодого поколения. Однако результат – сохраненные жизни – того стоит. Так что противопоставлено пускать такие работы на самотек, пренебрегать дополнительным контролем схмотехники и программного обеспечения (ПО), входным контролем элементной базы и, тем более, отдавать решения по альтернативным компонентам на откуп снабжению. Последствия могут быть непредсказуемы и даже трагичны. Авторы уже касались этих аспектов безопасности применительно к железнодорожной тематике и метрополитену [1]. Более того, причиной для разработки блока безопасности «БАРС» систем управления электропоездов московского метро 81-760 для коллективов ИПУ РАН и ООО «АВ-ТЭК» явилось именно стремление противодействовать вышеперечисленным тенденциям.

Чрезвычайно важным представляется соответствующий уровень образования и общей информированности широкого круга разработчиков в части функциональной безопасности. Необходимость получения экстремально низких вероятностей опасного отказа (например, 10^{-9} час⁻¹ для SIL 4) делает практическое подтверждение уровня безопасности натурными испытаниями аппаратуры невыполнимой задачей, что часто переносит предмет в область теоретических построений и дает почву для различных легенд и несоответствий. Так, целым рядом производителей микроконтроллеров и процессоров цифровой обработки сигналов (DSP) объявлены новые микросхемы уровня SIL 3 со специальными средствами коррекции ошибок, выполненные по технологии 90 нм и даже 65 нм. Не всем инженерам известно, что микропроцессоры, выполненные по старым, но до сих пор используемым технологиям КМОП 0,5 мкм и 0,35 мкм, при отсутствии схмотехнических и топологических ошибок де факто обеспечивали сбои на уровне SIL 4 даже при воздействии слабых электромагнитных помех. Дополнительными мерами

контроля эти цифры можно было улучшить еще на два порядка, что на практике редко требовалось, а стоял лишь вопрос отказов устройств по надежности. Тогда как современные микроконтроллеры и DSP, выполненные с технологическими нормами 0,13 мкм и ниже, даже с примененными средствами встроенной коррекции и в идеальных лабораторных условиях, не всегда могут продемонстрировать хотя бы уровень SIL 3 (10^{-7} час⁻¹) и никак не могут являться базой для построения устройств ответственного применения. Настоящая работа призвана хотя бы в некоторой степени закрыть этот информационный пробел.

Рост числа техногенных катастроф как тенденция последних десятилетий

Начнем рассмотрение с техногенных катастроф. Их количество (рисунок 1) увеличивается, и это очевидно, поскольку оно пропорционально, с одной стороны, общему количеству единиц используемой техники, а с другой – увеличению степени ее влияния на критические события. Последнее проявляется как в части разнообразия внедрений (применений на объектах), так и в вариациях масштабной шкалы последствий: как результат – получаем нелинейную (степенную) зависимость. Несмотря на ограниченность масштаба событий, влияние их велико и специфика очевидна: техника, особенно энергонасыщенная, при нарушении контроля (отсутствии надежно функционирующих систем безопасности) – это стихия. Последствия от техногенных катастроф всегда локально более разрушительны, хотя бы по той причине, что расположена техника (в отличие от вулканов) почти всегда вблизи и среди людей. Особое место при этом занимает транспорт и, в частности, системы автоматики железнодорожного транспорта и метро. Помимо обычных рисков, неумолимый прогресс (а на самом деле, непонимание истинной ситуации и подверженность популизму) диктует повсеместное внедрение автоматов, беспилотных технологий и пр., что существенно повышает требования к системам управления и узлам цифровой обработки сигналов (ЦОС). Отдельного рассмотрения заслуживают планы по массовому использованию беспилотного автомобильного и авиатранспорта (хочется надеяться, что при этом не будут забыты стандарты ГОСТ Р МЭК 61508 и ISO 26262), что существенно отразится на безопасности жизни.

Пока же статистика и без этих новых и многообещающих трендов выглядит ужасно. Обратимся к цифрам – речь идет о статистике техногенных и природных катастроф и их последствий за последние 100 лет (основываясь на материалах исследовательского центра CRED – Centre for Research on the Epidemiology of Disasters) [2]. Так, за 30 лет с 1910 г. по 1940 г. (при населении Земли ок. 2 млрд чел.) количество зарегистрированных техногенных катастроф составило лишь

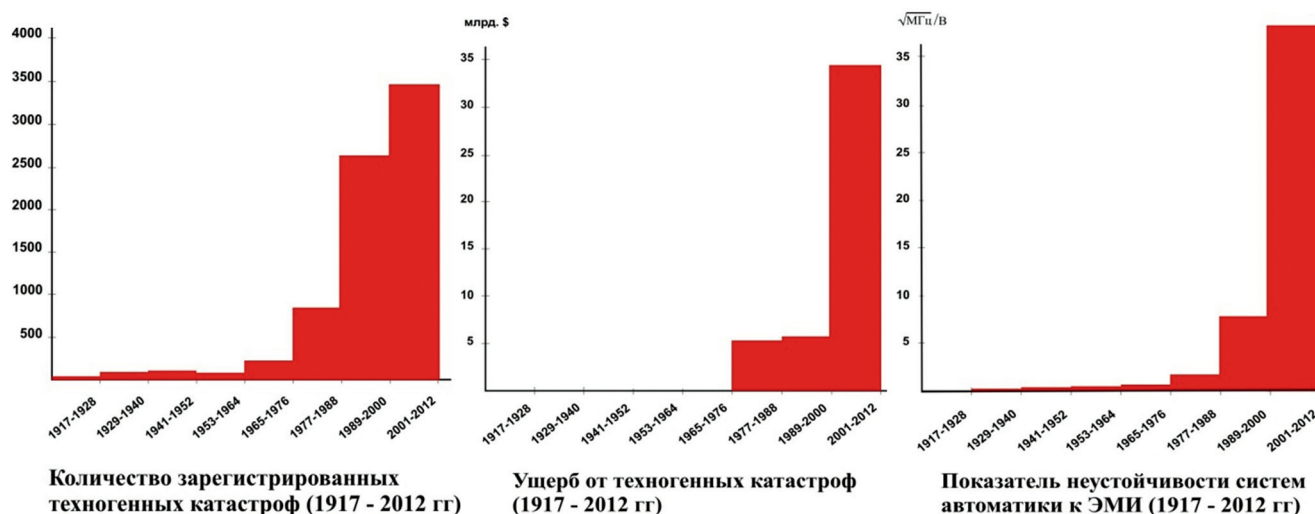


Рисунок 1 – Статистика техногенных катастроф и изменение устойчивости автоматики

162 при пострадавших и жертвах ~50 тыс. чел. с общим ущербом ~\$102,5 млн. Но за такой же период с 1982 г. по 2012 г. (при населении Земли ок. 7 млрд чел.) эти цифры составили для техногенных катастроф ~6,7 тыс. с пострадавшими и жертвами 4 млн. чел. и ущербом ~\$45,5 млрд. То есть рост по числу катастроф составил **35 раз**, а по нанесенному ими ущербу – **450 раз**! Приведенные на рисунке 1 графики говорят сами за себя (для удобства при обработке данных использованы интервалы по 12 лет, что близко, с одной стороны, к циклам солнечной активности, а с другой – к типовому времени между модернизациями капиталоемкого оборудования).

Человеческому мышлению в популяции свойственна инерционность реакции (задержка в одно поколение и более). С другой стороны, всегда присутствует «высококачественная фильтрация», когда мелкие тактические события затевают глобальные тенденции, особенно те из них, где постоянная времени – более нескольких десятилетий, и поколение привыкает. Это предполагает адекватную реакцию в реальном времени на происходящее, в лучшем случае, лишь со стороны нескольких профессиональных сообществ, при игнорировании обществом в целом.

Как и чем будет пытаться реагировать современное человечество на угрозу своей безопасности и увеличение количества катастрофических событий? Наиболее вероятно – все теми же микропроцессорными защитами, системами сбора, обработки и управления. Нас в такой ситуации должны волновать, по крайней мере, чисто профессиональные вопросы обеспечения функционала безопасности, т.е. создания техники, работоспособной в жестких условиях, когда вероятность аномальных по величине воздействующих факторов возрастает многократно. Так какова же типичная стойкость автоматики к различным воздействиям (влажность, удары, электромагнитные поля и пр.), и как она менялась на протяжении столетия? Если в части механической прочности и тщательности изготовления ответ очевиден, то в отношении электромагнитной стойкости необходимо

сделать некоторые оценки. В качестве критерия возьмем условный параметр порогового воздействия, вызывающего сбой такой системы [3, 4] и, по аналогии со спектральной плотностью шума, будем измерять его в единицах $\text{В}/\sqrt{\text{МГц}}$. Промежуточные выкладки опускаем, а результаты в виде обратных величин показаны на правом графике рисунка 1. Особое внимание следует обратить на близость характера последних двух гистограмм: ущерба и неустойчивости систем управления.

Глядя на приведенные графики, становится ясно, что необходимо переделывать стандарты и обсуждать дополнительные, нерыночные механизмы повышения устойчивости систем управления ответственных применений. В условиях нарастающего потока сбоев, приводящих к катастрофическим событиям, «прецедентное» мышление с запоздалой реакцией может не сработать. Приняв это к сведению, перейдем к рассмотрению специфики современных микроэлектронных технологий.

Общие проблемы современной микроэлектронной элементной базы

Перечень элементной базы, применяемой в системах управления и обеспечения безопасности, весьма широк и включает множество активных и пассивных компонентов: от резисторов, конденсаторов и транзисторов до больших интегральных схем и радиочастотных модулей. По каждому из разделов этого списка следовало бы рассмотреть влияние модернизированных технологий (и, прежде всего, применения нанотехнологий) на надежность элементов, их стойкость к внешним воздействиям и изменение вероятности ошибки при выполнении функций в схеме. Результатом такого рассмотрения, в частности, стало выявление нового типа дефектов компонентов поверхностного монтажа – связанных с механическими воздействиями, присутствующими в процессе производства, эксплуатации изделий и незащищенностью поверхностей модулей, на которых расположены компоненты. Для большинства электронных

модулей мы имеем ситуацию, когда правила монтажа мало изменились за десятилетия, но повысилась плотность размещения, и с компонентов исчезли корпуса (а если остались, то лишь в виде тонких слоев покрытий, не защищающих от механических воздействий), т.е. по старым стандартам большинство современных модулей рассматривались бы как микросборки и требовали соответствующей дополнительной защиты, которой теперь пренебрегают. Другим обнаруженным фактором стало изменение характера пробоя активных элементов, что связано, прежде всего, с использованием низковольтных технологий и существенно более тонких слоев в структуре полупроводника, чем в предыдущих поколениях аналогичных изделий. Отдельного упоминания заслуживает повсеместное применение силовых изделий на МОП транзисторах, что, с одной стороны, уменьшило потери мощности при коммутации, но с другой – существенно увеличило вероятность пробоя таких ключей на замыкание (в связи с упомянутыми проблемами внедрения нанотехнологий). Этот список можно было бы продолжать, обсуждая влияние каждого из факторов на безопасность и отказоустойчивость систем управления, но мы вынужденно ограничимся вышесказанным.

Рассмотрим, хотя бы кратко, главный элемент системы управления, которым, безусловно, является процессорный узел – микроконтроллер, DSP и др. – тот элемент, от которого зависит правильность выполнения алгоритма и безопасность реакций системы.

Пример такого высокотехнологичного компонента, хорошо знакомого, но едва ли узнаваемого в этом виде для IT специалиста, показан на рисунке 2.

Отметим здесь, что большинство разработчиков, связанных с программированием систем, мало понимают,

что, собственно, представляет собой та микросхема (кристалл), для которой они программируют – как объект физики и радиотехники. В качестве примера рассмотрим популярный процессор на базе ядра Cortex M3, пришедший на смену хорошо зарекомендовавшему себя ARM7. На рисунке 2 показано, что представляет собой такой процессор без корпуса и привычной матрицы выводов: прежде всего, мы видим не один, а два отдельных кристалла, смонтированных один поверх другого. Верхний представляет собой FLASH-память и соединен с нижним (вычислительное ядро) длинными петлями перемычек разварки. Анализ этих связей сразу же позволяет сделать вывод о различии помехоустойчивости режимов работы с ОЗУ и FLASH уже за счет этих контуров. А другими факторами влияния на стойкость будут разница технологии самих кристаллов, нюансы монтажа, печатных плат (PCB) и прочее. Однако в наши задачи не входит рассмотрение специфики отдельного компонента. Поэтому коснемся, хотя бы кратко, общих проблем КМОП (CMOS) технологии, по одной из модификаций которой выполнено большинство современных микропроцессорных узлов.

Проблемы КМОП технологии в современных микропроцессорных узлах

Прежде всего, обратим внимание на такой малопопулярный факт: логический вентиль КМОП, как и любой каскад, построенный на активных компонентах, в момент переключения является усилителем. Например, в случае инвертора (см. схему в левой части рисунка 3) один транзистор является нагрузкой для другого, и типовой

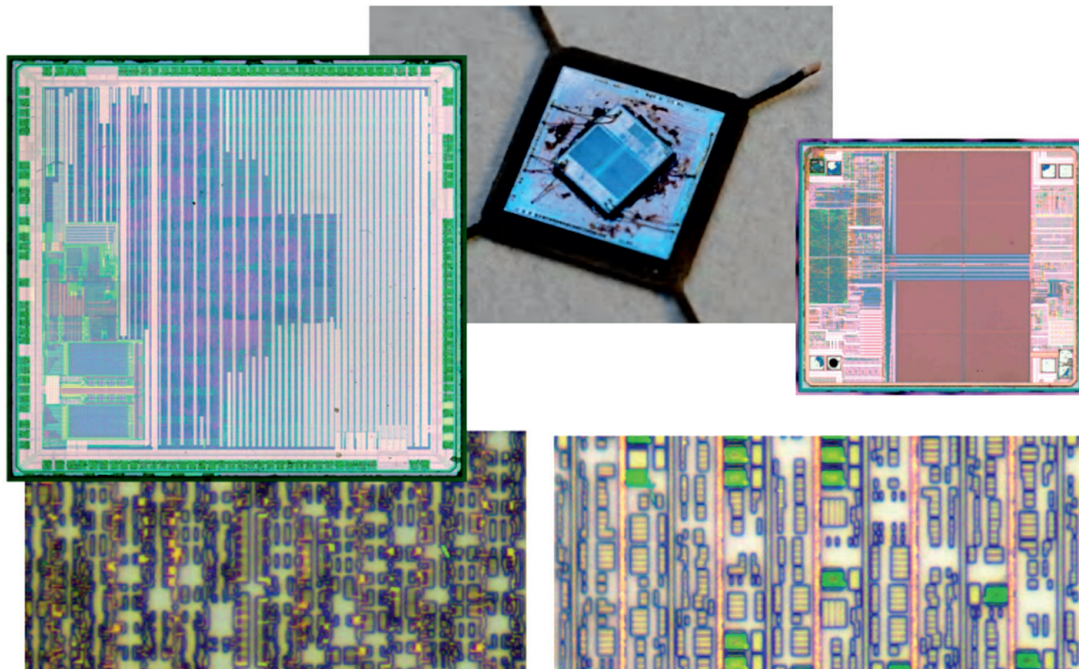


Рисунок 2 – Микроконтроллер Cortex M3 без крышки корпуса и матрицы выводов. Слева в масштабе показан кристалл процессора, справа – FLASH-память, ниже, более крупно – элементы топологии

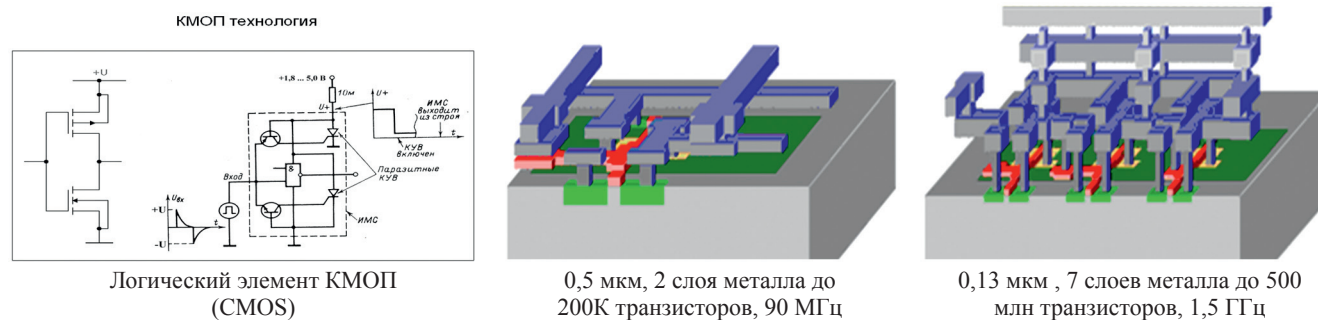


Рисунок 3 – КМОП технологии: разная плотность расположения слоев металлизации и полоса частот вентиля для 0,5 мкм и 0,13 мкм

коэффициент усиления такой пары обычно получается около 80 – 100 в широкой полосе частот. В правой части рисунка показано, что эта полоса частот изменилась с 90 МГц до 1,5 ГГц с переходом от 0,5 мкм к 0,13 мкм. При этом нужно учесть, что пороговое напряжение и питание транзисторов для новой технологии снизилось как минимум в 4 раза. Это означает, что энергию помехи схема, выполненная по технологии, показанной на рисунке 3 справа, может потребить из полосы в 16 раз более широкой, при том, что ее стойкость к амплитуде помехи как минимум в 4 раза ниже.

Опуская промежуточные выкладки, отметим, что помехоустойчивость используемых в настоящий момент модификаций КМОП технологий с различными проектными нормами к внешнему энергетическому воздействию отличается на порядки. Делая сравнительную оценку для представленных на рисунке вариантов **0,5 мкм** и **0,13 мкм**, получим значение по мощности влияющей помехи, отличающееся более чем в **4000** раз (!). Сравнение стойкости для **0,5 мкм** и **90 нм** демонстрирует нелинейность этой зависимости, и расчет дает уже более **15 000** раз – и все это не в пользу новых кристаллов, таких удобных для пользователей и программистов. Это заставляет задуматься о правомерности применения технологий с нормами менее 0,25 мкм для устройств критических приложений. Следует учитывать, что уровень электромагнитного шума в современной цивилизации очень высок в местах большого скопления людей и энергонасыщенных объектов инфраструктуры. Таким образом, эксплуатация каждого устройства безопасности, не обладающего достаточной стойкостью, превращается в игру в рулетку.

Рассмотрев коротко влияние внешних факторов, обратимся к факторам внутренним (т.е. скрытым в самих микроэлектронных изделиях). Если для предыдущих поколений микропроцессорных устройств обсуждался как значительный – фактор влияния на кристалл радиации, в частности, керамических элементов корпуса, вызывавший с конечной вероятностью сбойное переключение вентиля схемы, то теперь, безусловно, доминирующим эффектом является плохая магнитная совместимость плотно расположенных элементов и блоков самого кристалла, как видно на рисунках 2 (внизу) и 3. Фактором увеличения сбойности является близкое расположение активных элементов и плотная многослойная разводка

связей с эффектами перекрестных наводок. При этом нужно отметить, что для большинства современных процессоров максимальная длина одной связи на кристалле может достигать 1 см и более, что также в разы превышает типичный параметр длины связи для предыдущих поколений схем.

Е шума / Vdd

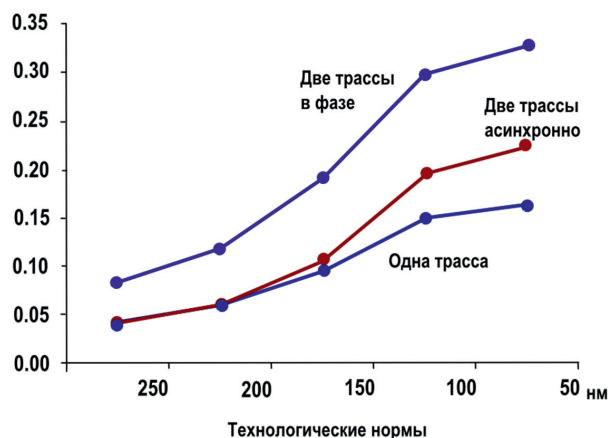


Рисунок 4 – Зависимость относительной величины напряжения помехи на шине питания от линий трассировки длиной 1 мм

На рисунке 4 показана зависимость относительной величины напряжения помехи на шине питания от фрагментов линий трассировки длиной 1 мм при топологически минимальном расстоянии между ними от проектных норм. Верхняя кривая – сигнал в источниках помех изменяется синфазно, средняя кривая – асинхронно, нижняя кривая соответствует наличию только одного проводника с помехой. Приняв во внимание реальное количество близко расположенных трасс на кристалле и их длину и посчитав вероятность пиковых значений для выбранной модели шума, получим ориентировочное количество превышений порогового уровня срабатывания вентиля и оценку сбойности конкретной архитектуры микропроцессора (разумеется, без учета схем компенсации ошибок). Даже такая грубая двумерная модель дает результаты, плохо совместимые с требованиями безопасности. Результаты 3D-моделирования конкретных фрагментов схем дают еще более удручающие результаты. Кроме того, в больших кристаллах значительно возрос ток утечки как дополнительный

дестабилизирующий фактор, также косвенно влияющий на вероятность сбоев.

Данные обстоятельства привели к тому, что помехоустойчивость упала так сильно, а сбои так возросли, что это стало заметно в простых системах реального времени (не связанных с безопасностью). Изготовители вынужденно стали применять специальные меры компенсации сбоев, а именно: встраивать в кристаллы аппаратные блоки контроля данных и коррекции ошибок, дублировать ответственные сигналы и пр. Как результат, появились кристаллы, выполненные по технологии с нормами 65 нм, для которых гарантируется уровень SIL 2 (внимание, при идеальной ЭМС в аппаратуре!). Иными словами, к функциональной безопасности это не имеет отношения, поскольку достижением таких изделий считается ситуация, когда отдельные структуры на одном кристалле не очень мешают друг другу и могут хорошо работать при сбоях на уровне 10^{-6} час⁻¹. Но этого совершенно недостаточно для построения на их основе даже систем безопасности уровня SIL 2. При этом фактором, драматически влияющим на безопасность, будет, например, любое электромагнитное воздействие, имеющее соответствующую вероятность пикового уровня на рассматриваемом временном интервале.

Практикуемое обычно резервирование как способ повышения уровня безопасности для таких узлов также оказывается малоэффективным ввиду фундаментальной причины – большинство сбойных ошибок [8] при использовании данных технологий раскрываются как отказы по общей причине (ПОП). Так, внешнее электромагнитное воздействие даже небольшой энергетики, но хорошо совпавшее по спектру частот с «антеннами» кристаллов и разводки модуля, вызывает лавинообразные сбои, которые не могут быть отработаны стандартными средствами коррекции ошибок, рассчитанными на малочисленные или одиночные события. Тогда возникнет своего рода пороговый эффект воздействия, когда поведение системы становится непредсказуемым. Для систем безопасности это следует считать абсолютно

неприемлемым, а такие компоненты – непригодными. Областью их применения должны остаться бытовые и телекоммуникационные устройства, где уровень сбоев определяет доступность сервиса и качество сигнала, но никак не связан с риском для жизни.

Как результат, имеем необычную ситуацию (рисунок 5), когда надежность микропроцессорных компонентов стала многократно лучше их сбойности. Т.е. фактически самыми ненадежными компонентами современного электронного модуля являются РСВ и разъемы; тогда как самым небезопасным – его процессорный элемент и чувствительные цифровые схемы. В пределе сбойность суперсовременной электроники достигает уровня, свойственного человеку-оператору (то есть мы достигли здесь совершенства и воспроизвели самих себя!). При этом данные о сбойности для большинства процессорных элементов практически отсутствуют в стандартной документации и доступны лишь после долгих и утомительных переговоров с изготовителем (если он вообще озабочился исследовать изделие и получить такие данные). В результате разработчики при оценке уровня полноты безопасности (УПБ) ошибочно используют вместо них цифры надежности микросхем, предоставляемые изготовителем, что абсолютно некорректно. Что же касается цифр сбойности – это является закрытой информацией, не обсуждаемой изготовителем.

У этой ситуации есть масса последствий: например, замена модификации микроконтроллера на другую, более новую и полностью совместимую по ПО, может драматически изменить УПБ изделия. Кроме того, помимо процессоров существуют дополнительные интерфейсные схемы, аналого-цифровые преобразователи (АЦП), тактовые генераторы и другие микросхемы, содержащие в себе цифровые блоки, выполненные по неизвестным разработчику технологиям и имеющие свой уровень сбойных ошибок. Некоторые из таких ошибок могут быть парированы алгоритмически тем же процессором. Но как быть, если источником сбоя становятся скачки фазы опорного сигнала – это приводит уже к абсолютно неконтролируемым последствиям для цифровых систем. Такое может возникнуть при простой замене одного компонента (генератора) в спецификации на другой, внешне и по спецификации – такой же (например, по инициативе снабжения).

На рисунке 6 в качестве примера показаны пять генераторов, выполненных по технологии поверхностного монтажа (SMD), одинакового применения, т.е. для одного и того же изделия, но от разных производителей, а рядом показаны результаты «вскрытия» после удаления резонаторов. Как видим, здесь присутствуют цифровые схемы с совершенно разными топологическими нормами, а сам монтаж кристаллов предполагает, как следствие, драматически разную помехоустойчивость.

Подытоживая вышесказанное, отметим, что создание микропроцессорных изделий для систем управления под требования SIL 3, и, тем более, SIL 4, является задачей,



Рисунок 5 – Изменение соотношения вероятностей отказа и вероятностей сбоя в поколениях микропроцессоров

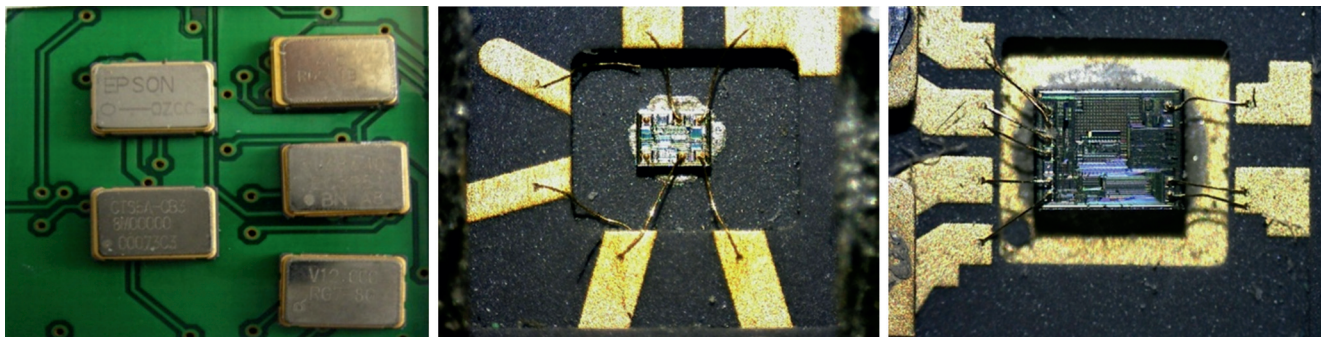


Рисунок 6 – Помехоустойчивость генераторов SMD. Слева направо: генераторы в корпусах SMD (5 типов); вариант исполнения с низкой помехоустойчивостью; приемлемый технологически и конструктивно вариант

едва ли легко выполнимой – особенно для современных коллективов разработчиков. Тем более что коллективы эти в большинстве своем состоят из IT специалистов, не видящих места для проявления физических и даже радиотехнических эффектов в своей работе. Для устройств критических приложений и безопасности это может оказаться фатальным...

Библиографический список

1. Васильев С.Н., Кирпичников А.П., Ботвинёнок А.А. Проблемы обеспечения безопасности в современных микропроцессорных системах управления подвижным составом, вызванные особенностями современной элементной базы, и их решение на примере блока безопасности «БАРС» вагонов 81–760 Московского метрополитена // Бюллетень Объединенного ученого совета ОАО «РЖД». 2016. № 5. С. 13 – 25.
2. Centre for Research on the Epidemiology of Disasters (CRED) www.emdat.be
3. Кирпичников А.П. Вопросы отказоустойчивости и безопасности в устройствах ЦОС критических приложений // Докл. 14-ой Междунар. конф. “Цифровая обработка сигналов и ее применение”. – Москва, 2012. – Т. 1. – С. III–V.
4. Кирпичников А.П. Новая роль микропроцессорных систем: обеспечение безопасности перед лицом катастроф // 16-ая Международная конференция «Цифровая

обработка сигналов и ее применение – DSPA-2014». – Москва, 2014. Т.1, С.25-29.

5. Пат. №2439666 РФ. Блок безопасности с контролем достоверности входной информации / А.П. Кирпичников // Бюл. – 2010.

6. Пат. №2449900 РФ. Блок безопасности / А.П. Кирпичников // Бюл. – 2010.

7. Кирпичников А.П., Ботвинёнок А.А., Медуницин Н.Б. Многоканальная микропроцессорная система управления со сверхвысокой безопасностью для поездов Московского метрополитена // Датчики и Системы, 2014, №9, С.38-45.

8. И.Б.Шубинский «Функциональная надежность информационных систем» – М.:Надежность, 2012, 294с.

Сведения об авторах

Алексей П. Кирпичников – начальник отдела Института проблем управления им. В. А. Трапезникова РАН (ИПУ РАН), Россия, Москва, тел. +7 (495) 334-89-10, e-mail: abramo@ipu.ru

Станислав Н. Васильев – академик РАН, доктор физ.-мат. наук, главный научный сотрудник Института проблем управления им. В. А. Трапезникова РАН (ИПУ РАН), Россия, Москва, тел. +7 (495) 334-89-10, e-mail: snv@ipu.ru

Поступила 20.03.2017

Обеспечение надежности уникальных высокоответственных систем

Юрий П. Похабов, Открытое акционерное общество «НПО ПМ – Малое Конструкторское Бюро», Россия, Красноярский край, Железногорск

Резюме. Цель. Обычно надежность изделий исследуется без учета закономерностей ее генезиса, а причины ненадежности принято рассматривать в виде обобщающих вероятностно-статистических зависимостей, учитывающих «результат взаимодействия ряда факторов: внешней среды, свойств системы, технологических, эксплуатационных и т.п. требований». Как следствие, при оценке показателей надежности исходят из предположения, что к началу эксплуатации изделие находится в работоспособном состоянии. Соответственно зависимости надежности от времени рассматриваются только за период эксплуатации изделий. Наиболее известная зависимость надежности от времени – это эмпирическая функция отказов, так называемая U-образная кривая надежности, описать которую простыми математическими формулами, пригодными для инженерных расчетов, пока никому не удалось. Наличие первого «горба» на U-образной кривой связывают с проявлением ошибок, допускаемых при проектировании, дефектов изготовления или неправильной сборки изделий, однако же, конкретные причины появления этого «горба» в публикациях не раскрываются. Определение термина «работоспособность» не исключает возможностей, а на практике нередки случаи, когда при проектировании и конструировании оказываются учтенными не все параметры, характеризующие способность изделия выполнять заданные функции, или какие-либо из требований документации не согласованы со значениями функциональных параметров, а при изготовлении значения этих параметров могут выйти за установленные пределы. В результате, на первый взгляд, работоспособная, причем даже прошедшая квалификацию по результатам экспериментальной отработки, конструкция может не соответствовать заданной надежности. **Методы.** Свойства надежности любого изделия закладываются задолго до начала эксплуатации, и получают способность проявиться в полной мере только с ее началом. В статье приведен график, отражающий условную вероятность безотказной работы по стадиям жизненного цикла изделий задолго до начала эксплуатации. Обеспечение надежности уникальных высокоответственных систем (УВС) может осуществляться уже с самых ранних стадий жизненного цикла на основе последовательного выполнения определенных конструкторских, технологических и производственных процедур и применения методов конструкторско-технологического анализа надежности. **Результаты.** Рассмотрены роль и смысл каждой из стадий жизненного цикла в обеспечении надежности УВС. Перечислены процедуры конструкторско-технологического метода обеспечения надежности и приведены принципы конструирования УВС. Даны базовые инструменты повышения и принципы оценки надежности. **Выводы.** В статье показаны возможности обеспечения надежности УВС с помощью конструкторско-технологических процедур, применяемых на каждой из стадий жизненного цикла до начала эксплуатации. Применение таких процедур способно на единой теоретической и методологической основе поднять на соответствующий уровень технологию проектирования, конструирования, подготовки производства, изготовления и на этой же основе создать методику оценки надежности УВС.

Ключевые слова: уникальная высокоответственная система, обеспечение надежности, анализ надежности, оценка надежности, стадии жизненного цикла, проектирование, конструирование.

Формат цитирования: Похабов Ю.П. Обеспечение надежности уникальных высокоответственных систем // Надежность. 2017. Т. 17, № 3. С. 17-23. DOI: 10.21683/1729-2646-2017-17-3-17-23.

Введение

Обычно надежность изделий исследуется без учета закономерностей ее генезиса, а причины ненадежности принято рассматривать в виде обобщающих вероятностно-статистических зависимостей, учитывающих «результат взаимодействия ряда факторов: внешней среды, свойств системы, технологических, эксплуатационных и т.п. требований» [1]. Как след-

ствие, при оценке показателей надежности исходят из предположения, что к началу эксплуатации (моменту начала исчисления наработки) изделие находится в работоспособном состоянии [2] и если t – общая наработка, а τ – наработка изделия до первого отказа, то вероятность безотказной работы (ВБР) изделия за время t определяется как:

$$P(t)=P(\tau>t). \quad (1)$$

Соответственно зависимости надежности от времени рассматриваются только за период эксплуатации изделий. Наиболее известная зависимость надежности от времени – это эмпирическая функция отказов, так называемая *U*-образная кривая надежности [3], описать которую простыми математическими формулами, пригодными для инженерных расчетов, пока никому не удалось. Наличие первого «горба» на *U*-образной кривой связывают с проявлением ошибок, допускаемых при проектировании, дефектов изготовления или неправильной сборки изделий, однако же, конкретные причины появления этого «горба» в публикациях не раскрываются [4].

В этой связи уместно вспомнить шутливое высказывание, которое приводит И.А. Ушаков в своей неформальной истории теории надежности: «Считают надежность те, кто ее не умеет делать» [5]. Действительно, в теоретическом аспекте надежность любой сложной технической системы представляет собой многомерную задачу, для постановки и решения которой необходимо учитывать множество взаимозависимых параметров, имеющих стохастическую природу, что практически неосуществимо. В то же время инженеры научились достигать на практике более или менее приемлемый уровень безотказности сложной техники, пользуясь качественными критериями надежности [6]. Например, разработчикам раскрывающихся конструкций космических аппаратов хорошо известно, что проектируемое изделие должно быть, во-первых, прочным, чтобы не сломаться до или в процессе раскрытия, во-вторых, работоспособным, чтобы конструктивное исполнение позволяло осуществлять процесс раскрытия после воздействия полетных нагрузок, и, в-третьих, надежным, чтобы обеспечить стабильность раскрытия от раза к разу в заданных режимах и условиях эксплуатации.

Как известно, работоспособность – это *состояние объекта, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативно-технической и (или) конструкторской (проектной) документации* [7]. Очевидно, что само определение термина «работоспособность» не исключает возможностей, а на практике нередко случаи, когда при проектировании и конструировании оказываются учтенными не все параметры, характеризующие способность изделия выполнять заданные функции, или какие-либо из требований документации не согласованы со значениями функциональных параметров, а при изготовлении значения этих параметров могут выйти за установленные пределы. В результате, на первый взгляд, работоспособная, причем даже прошедшая квалификацию по результатам экспериментальной отработки, конструкция может не соответствовать заданной надежности. Характерный пример – это повторяющееся не раскрытие панелей солнечной батареи на космических кораблях Союз ТМА-14М (2014 г.) и Союз ТМА-17М (2015 г.) из-за заклинивания элементов крепления батарей.

Роль стадий жизненного цикла, предшествующих эксплуатации, в обеспечении надежности уникальных высокоответственных систем

В работах [8–10] показано, что создание УВС с позиций обеспечения заданной надежности без учета закономерностей ее генезиса невозможно. Свойства надежности любого изделия закладываются задолго до начала эксплуатации, и получают способность проявиться в полной мере только с ее началом.

Из практики известно, что, находясь в состоянии ожидания эксплуатации, любые объекты несут в себе риски γ возникновения отказов из-за конструкторских, технологических и производственных ошибок, которые могут достигать 80% [10–11]. При этом до 80–85% затрат в машиностроении предопределяются техническими решениями, которые формируются в процессе конструирования и разработки технологии [12].

В работе [10] рассмотрено влияние конструкторской и технологической подготовки производства на надежность, в результате чего предложено оценивать ВБР УВС (1) в виде:

$$P(t) = (1 - \gamma) \cdot P(\tau > t). \quad (2)$$

Формула (2) призвана фокусировать внимание разработчика на начальных стадиях жизненного цикла (ЖЦ) – проектировании и конструировании, где только и существует возможность принять такие технические решения, которые позволят обеспечить максимально высокую надежность будущего изделия. При дальнейшем продвижении разработки по стадиям ЖЦ таких возможностей больше нет, не говоря уже о том, что «*повысить надежность техники в процессе эксплуатации нельзя*» [6].

В одном из старейших отечественных стандартов – ГОСТ 2.103 – стадии выпуска конструкторской документации (КД) разделены на разработку проектной (ПКД) и рабочей конструкторской документации (РКД), причем стадия ПКД включает три этапа: техническое предложение, эскизный и технический проекты. Каждая из стадий проектирования и конструирования выполняет строго определенные задачи и несет вполне конкретные смыслы, суть которых следует из терминологических определений, приведенных в соответствующих нормативно-технических документах:

1) Проектирование – *процесс составления описания, необходимого для создания в заданных условиях еще не существующего объекта, на основе первичного описания этого объекта и (или) алгоритма его функционирования или алгоритма процесса преобразованием (в ряде случаев неоднократного) первичного описания, оптимизацией заданных характеристик объекта и алгоритма его функционирования или алгоритма процесса, устранением некорректности первичного описания и последовательным представлением (при необходимости) описа-*

ний на различных языках. [13]. Стадия проектирования соответствует разработке технического предложения и (или) эскизного проекта, а ее результатом является ПКД технического предложения согласно ГОСТ 2.118 и (или) эскизного проекта согласно ГОСТ 2.119.

2) Разработка – стадия конструкторской подготовки производства, выполняемая при помощи САД-системы, в ходе которой разрабатывается подробная 3D-модель изделия, а также 3D-модели узлов, агрегатов и основных (базовых) деталей, на базе которых формируются 2D-проекция (чертежи), выполняются уточненные проектировочные расчеты и моделирование. Результаты работ оформляются в виде информационных объектов, помещаемых в интегрированную информационную среду. Согласно ГОСТ 2.120 эта стадия называется техническим проектированием, а ее результат – техническим проектом [14].

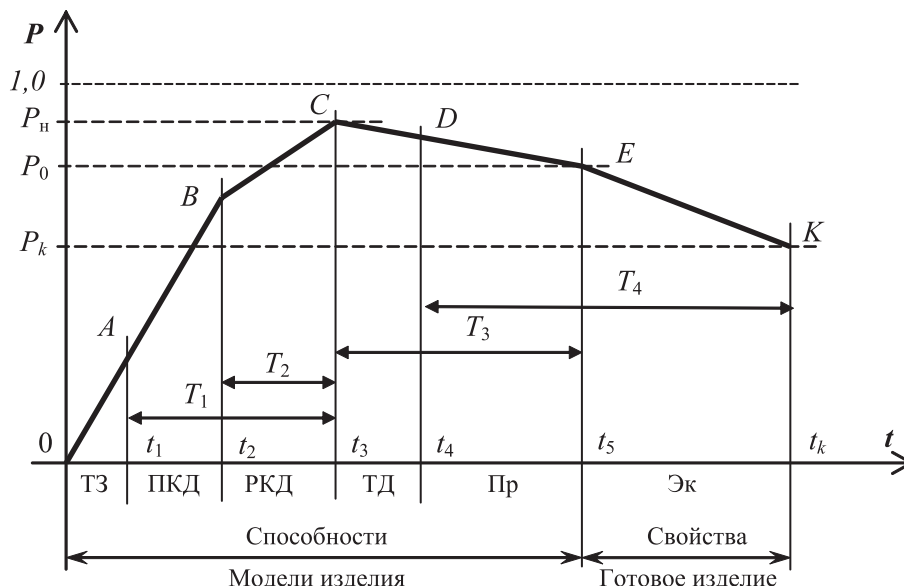
3) Конструирование – стадия конструкторской подготовки производства, выполняемая при помощи САД-системы, в ходе которой создаются 3D-модели всех оригинальных деталей и их 2D-проекция (чертежи), оформляются спецификации и ведомости материалов, комплектующих и нормализованных изделий, выполняются проверочные расчеты и моделирование. Результаты работ оформляются в виде информационных объектов, помещаемых в интегрированную информационную среду. Согласно ГОСТ 2.103 результатом этой стадии является РКД [14].

Современный «менеджерский» подход в решении производственно-технических вопросов основывается на декларативном снижении времени на разработку КД в первую очередь за счет сокращения и даже исключения стадии выпуска ПКД. В результате стадии проектирования и конструирования нередко «сваливаются в общую кучу» и представляются процессом проектирования и

разработки, как совокупностью процессов, переводящих требования в установленные характеристики или спецификации на продукцию, процесс или систему [15]. При этом сам процесс проектирования и разработки делится на этапы: проектирования, как процесса, который преобразует требования в характеристики продукции, излагаемые в проектно-конструкторской документации, и разработки, как процесса создания технической документации на продукцию для последующей подготовки производства и изготовления продукции [16]. В некоторых случаях, из-за «сжатых сроков», а иногда по недомыслию, разработанная таким куцым образом КД передается непосредственно на производство для изготовления изделий, минуя стадию технологической подготовки.

Чем способен обернуться такой «менеджерский» подход для целей достижения заданной надежности УВС, можно увидеть из рисунка, отражающего условную ВБР (УВБР) по стадиям ЖЦ [10].

Рисунок отражает общий (качественный) характер изменения УВБР по стадиям ЖЦ при условии соблюдения требований нормативно-технических документов, общепринятых правил, ЕСКД, ЕСТД и системы менеджмента качества (СМК), например, ИСО 9001. Углы наклона и формы кривой зависимости УВБР от времени в каждом конкретном случае разработки и создания изделий могут несколько отличаться от представленного графика, сохраняя при этом общую тенденцию. Положение точек A, B, C, D и E по оси ординат зависит от надлежащего выполнения процедур по обеспечению надежности, что способно не только в значительной степени нивелировать, но, в случае ненадлежащего выполнения, и существенно усугубить риски возникновения отказов из-за конструкторских, технологических и производственных ошибок.



$0-t_1$ – выпуск тактико-технического и/или технического задания на разработку (ТЗ), t_1-t_2 – проектирование и разработка изделия (ПКД), t_2-t_3 – выпуск рабочих чертежей (РКД), t_3-t_4 – технологическая подготовка производства (ТД), t_4-t_5 – изготовление изделия (Пр), t_5-t_k – эксплуатация готового изделия (Эк)

Рисунок – График изменения УВБР УВС по стадиям ЖЦ

На рисунке отражена важная особенность – здесь зримо разграничены стадии ЖЦ, когда будущее изделие существует в виде моделей и характеризуется способностью проявлять свойство надежности, а когда модель, материализуясь в готовое изделие, проявляет собственно само свойство надежности. Такое разделение позволяет:

- визуализировать скрытые причины возникновения первого «горба» на общеизвестной U -образной кривой надежности;

- получить возможность соотносить величину исходного значения УВБР P_0 к началу эксплуатации с текущими значениями УВБР в процессе разработки УВС, что создает условия для нормирования надежности по стадиям ЖЦ исходя из заданного показателя ВБР на конец эксплуатации P_k .

Смыслы процедур по обеспечению надежности на стадиях жизненного цикла

Положение точек A и B на графике отражает наличие (отсутствие) «грубых» ошибок, связанных со степенью завершенности фундаментальных исследований по изучению характеристик конструкционных материалов, получением достоверных сведений об условиях внешних воздействий и нагрузок (для точки A), рациональностью выбора конструктивно-компоновочных и конструктивно-силовых схем, соблюдением принципов и правил проектирования (для точки B) [10].

При отсутствии «грубых» ошибок в проекте, положение точки B по оси ординат может приближаться к 1, при этом не достигая ее из-за двух групп причин. Одна из группы причин связана с увязками проекта, которые могут продолжаться на протяжении всей стадии проектирования и обычно приводят к недостаточной проработке номенклатуры и содержания требований к изготовлению изделий, которые призваны обеспечить его заданную надежность [9]. Вторая группа причин подробно изложена в работе [12] – это разного рода неизбежные «мелкие» ошибки из-за несовершенств методов проектирования, нарушения предписанных положений нормативно-технической документации, недостаточно высокого уровня квалификации проектантов, их психофизиологических особенностей, связанных с невнимательностью, темпом выполнения работ, общим утомлением и т.п. проявлениями.

Недооценка значения стадии проектирования или ее игнорирование существенно повышает риск недостижения заданного уровня надежности. Если указанные «мелочи» проекта должным образом не будут устранены при конструировании, то положение на графике точки C по оси ординат может не измениться или даже оказаться ниже положения точки B . Задача стадии разработки РКД заключается в повышении надежности УВС за счет исправления ошибок проекта и установления необходимых и достаточных требований к их изготовлению. Положение точки C на графике отражает предельно возможный

уровень надежности P_n для данной разработки, который при реализации последующих стадий ЖЦ способен только снижаться.

Положение точек D и E определяется вероятностью возникновения ошибок при технологической подготовке производства и непосредственном изготовлении изделий. Важную роль здесь играет СМК, которая призвана поднять культуру производства, сократив до приемлемого уровня вероятность производственных ошибок. Важно осознавать, что действующая на производстве СМК не имеет непосредственного отношения к качеству и надежности самого изделия, как конечного продукта, являясь фактически декларацией того, что предприятие способно выпускать продукцию надлежащего качества. Без должного конструкторского и технологического обеспечения сама по себе СМК не способна решить задач надежности, но при этом и без надлежащей СМК задачи надежности решить нельзя.

Положение точки K определяется вероятностью допущения ошибок при эксплуатации изделий. Поскольку согласно ГОСТ 2.102 эксплуатационная документация является одним из видов КД, то указанные ошибки определяются, с одной стороны, установлением ясных и четких требований к исполнению правил эксплуатации, а, с другой стороны, надлежащим их исполнением.

Теоретически для УВС положение точек C , D , E и K по оси ординат может достигать своих предельно возможных значений близких к 1, при условии должного развития и реализации конструкторско-технологических методов анализа и обеспечения надежности [9]. Смыслы деятельности по стадиям ЖЦ согласно рисунку, заключаются в следующем:

- отрезок графика $0-A-B$ – это исключение «грубых» ошибок проекта;
- отрезок графика $B-C$ – исправление «мелких» ошибок проекта;
- отрезок графика $C-D$ – исключение каких-либо ошибок при технологической подготовке производства;
- отрезок графика $D-E$ – недопущение брака при производстве;
- отрезок графика $E-K$ – исключение ошибок при эксплуатации.

Базовый метод обеспечения надежности

Идея метода конструкторско-технологического обеспечения надежности заключается, с одной стороны, в реализации процедур, направленных на установление необходимых и достаточных требований в КД и гарантирующих исполнение этих требований при изготовлении. С другой стороны, в предоставлении в формализованном виде подтверждения выполнения всех конструкторских, технологических и производственных процедур путем проведения соответствующих анализов, при этом анализы надежности рассматриваются как важнейшая и неотъемлемая часть методологии обеспечения надежности УВС.

Конструкторско-технологические анализы и процедуры обеспечения надежности базируются на единой основе – это состояние и качество разработанной КД и технологической документации (ТД), и единых принципах осуществления процедур согласно логической формуле: *сделал→подтверди, что сделал→зафиксируй сделанное*. Единая основа и единые принципы осуществления конструкторско-технологических методов анализа и обеспечения надежности позволяют создать методику, которая может использоваться в трех вариантах своего применения, как дорожная карта при проектировании и конструировании, как средство верификации проекта и разработки, и в качестве инструментария для проведения внешних экспертиз. Применяя, таким образом, конструкторско-технологические методы анализа и обеспечения надежности можно повысить эффективность разработок за счет разделения полномочий и конфликтов интересов между разработчиком, который всегда думает, каким образом система будет работать, и специалистом по надежности, своего рода критичным проверяющим, который должен думать, каким образом система откажется работать [9].

Важно отметить, что конструкторско-технологический анализ надежности (КТАН) направлен на исследование человеческих решений и ошибок (конструкторов, технологов, производственников) при осуществлении последовательных стадий ЖЦ, в то время как широко используемый на западе метод FMEA и его отечественный аналог АВПКО предназначен для исследования функций изделий и процессов. В отличие от методов FMEA, привязка результатов деятельности человека к окончанию каждой из стадий ЖЦ позволяет увязывать методы КТАН и методы проектирования с учетом надежности (DFR) на основе *Stage-Gate* [17].

С позиций процедур обеспечения надежности конструкторско-технологические методы должны применяться совместно с выполнением требований СМК. Для верификации требований к надежности, КТАН должен использоваться с другими методами анализа, проводимыми в строгой последовательности: функциональный анализ (ФА), анализ худшего случая (АХС), собственно сам КТАН и анализ (оценка) надежности (АН) [9], поскольку результаты проведения каждого из предыдущих анализов служат исходными данными для проведения последующих анализов.

Процедуры конструкторско-технологического метода обеспечения надежности

Конструкторско-технологическое обеспечения надежности включает 4 процедуры, показанные на рисунке:

1) Процедура T_1 служит для обоснования нахождения в установленных пределах значений параметров и показателей, характеризующих способность выполнять требуемые функции в заданных режимах и условиях эксплуатации. Основой процедуры являются инженер-

ные расчеты, проводимые по методикам в наибольшей степени пригодными для этого (расчеты на прочность и жесткость, тепловые расчеты, расчеты размерных цепей и т.п.) любыми приемлемыми методами: детерминированными, полувероятностными или вероятностными [18]. Продолжительность процедуры T_1 включает время выполнения стадий разработки ПКД и РКД. Расчеты производятся итерационно по мере проработки и детализации конструкции, например, начиная с аналитических расчетов на прочность по балочным схемам и заканчивая численными расчетами полноразмерных 3D-моделей методами конечных элементов. Именно эту процедуру при проведении прочностных расчетов стационарных (не реконфигурируемых) конструкций принято считать расчетами на надежность, если они выполняются полувероятностными или вероятностными методами;

2) Процедура T_2 служит для установления требований в КД, выполнение которых при изготовлении обеспечивает безусловное нахождение значений показателей и параметров в заданных допусках. В результате выполнения процедуры T_2 каждому параметру (показателю) в КД должны соответствовать установленные требования в графической или текстовой форме, что в конечном итоге обеспечит безусловное выполнение изделием функциональных задач;

3) Процедура T_3 служит для обеспечения гарантированного выполнения требований КД на этапах технологической подготовки и производства изделий. Задачей данной процедуры является исключение каких-либо искажений и интерпретаций технологами и производственниками требований надежности, установленных в КД, и подтверждение того, что конструкторские, технологические и метрологические методы изготовления, сборки, монтажа и контроля выстроены на единых принципах;

4) Процедура T_4 служит для обеспечения контроля за выполнением требований КД техническими службами контроля на производстве.

Все 4 процедуры рассматриваются как единая и неделимая совокупность процессов, обеспечивающих выполнение заданных требований к надежности. Если ТД по каким-либо причинам не разрабатывается, то технологическая часть КТАН до момента разработки ТД может не проводиться, тогда все выводы о надежности изделия строятся на допущениях, что условия производства позволяют изготовить изделие в строгом соответствии с КД, т.е. технологические и производственные ошибки исключены. В таком случае формула (2) преобразуется к следующему виду:

$$P(t) = P(A|B) \cdot P(\tau > t), \quad (3)$$

где A – событие, характеризующее готовность изделия функционировать без отказов с учетом риска нарушения работоспособности из-за конструкторских ошибок; B – событие, характеризующее готовность изделия функционировать без отказов с учетом риска нарушения работоспособности из-за технологических и производственных ошибок.

При этом формулы (2) и (3) связаны следующим соотношением:

$$P(A|B) > 1 - \gamma,$$

т.е. оценка надежности на основании лишь анализа КД будет всегда завышенной.

Принципы конструирования уникальных высокоответственных систем

Конструирование рассматривается как совокупность двух равно значимых процессов, которые осуществляются с позиций единства принципов осуществления процедур T_1 и T_2 : визуализации образа будущего изделия в виде чертежей (2D-проекции) или 3D-моделей и параметрического моделирования (оцифровки) конструкции.

Оцифровка конструкции заключается в составлении вектор-столбцов параметров (показателей) X и допусков ΔX :

$$X = (X_1 \dots X_n)^T, \quad (4)$$

$$\Delta X = (\Delta X_1 \dots \Delta X_n)^T, \quad (5)$$

которые количественно характеризуют свойства будущих изделий, обеспечивающих их работоспособность. При этом процедура обоснования параметров (показателей) T_1 сводится к подтверждению того, что все параметры и показатели X (4) (область состояний E) находятся в соответствующем заданном допуске ΔX (5) (области работоспособности G):

$$E \subset G,$$

$$\text{здесь } G = \{X_i(t) | X_{\min(i)} \leq X_i(t) \leq X_{\max(i)}\}.$$

Таким образом, параметрическое моделирование при конструировании играет ключевую роль, с одной стороны, позволяет оптимизировать конструктивные схемы и избегать принципиальных конструкторских ошибок, а, с другой стороны, составление вектор-столбца параметров (показателей) (4) может служить основой составления контрольного списка (чек-листа) для критериального контроля необходимости и достаточности установленных требований в КД (выполнение процедуры T_2). В этом случае, все расчеты по обоснованию параметров (выполнение процедуры T_1), которые сопровождают процесс проектирования и конструирования, производятся для подтверждения установленных в КД требований, причем общее количество таких расчетов определяется номенклатурой указанных требований.

Базовые инструменты повышения надежности

График рисунка позволяет визуализировать инструментарию, используемые при проведении проектно-конструкторских работ.

На участке ЖЦ $0-t_1$ (отрезок графика $0-A$) закладываются основные тактико-технические характеристики будущего изделия. Достижение этих характеристик определяется использованием наиболее общих стратегических принципов, как основополагающих истин, позволяющим формировать проектные решения для осуществления

будущего изделия. Рациональные принципы работы будущего изделия – залог его надежности. Число принципов невелико, они направлены на решение целевых задач и отражают общие закономерности их решения.

На участке ЖЦ t_1-t_2 (отрезок графика $A-B$), по мере увязки проекта, выбранные принципы осуществления изделия должны быть реализованы в проектные и конструкторские решения с помощью правил проектирования [10]. Правила вытекают из принципов и ими же определяются. Число правил может быть значительным, они направлены на решения частных задач и отображают определенные закономерности причинно-следственных связей.

Принципы отражают сущность явления, а правила – его отдельные стороны. Принципы и правила проектирования являются универсальными для определенного типа изделий, поэтому могут быть сведены в нормированный свод правил проектирования.

Основой обеспечения надежности является выполнение требований как осознанной необходимости соблюдения условий, которые должны быть строго исполнены. Такие требования должны быть в обязательном порядке установлены на участке ЖЦ t_2-t_3 (отрезок графика $B-C$) и в явном виде отображены в КД. Количество требований всегда больше используемых принципов и правил, поскольку они индивидуальны для каждого разрабатываемого изделия и используются для детализации принятых конструкторских решений.

Принципы и правила, формализованные должным образом, можно применять для составления контрольных списков (чек-листов), используемых при проектировании изделий. При установлении требований в КД необходимо использовать оцифровку конструкции, на основе которой должен быть создан контрольный список, служащий для критериальной оценки полноты установленных требований при конструировании.

Принципы оценки надежности

Поскольку надежность – это свойство, то ее мерой служит численная характеристика. Требование в КД – это ожидание достижения изделием после своего изготовления таких свойств, которые безусловно обеспечивают выполнение требуемых функций в заданных условиях и режимах эксплуатации. Искомые свойства всегда могут быть установлены на основе системного анализа. Если при проведении ФА выявить все режимы и условия эксплуатации, а в результате АХС определить худшие сочетания взаимоположений, взаимосвязей и взаимодействий критичных элементов, то при КТАН всегда существует возможность обнаружить такие свойства критичных элементов, которые необходимы для достижения поставленных целей. Это достигается применением метода антитезисов [10], когда в заданных режимах и условиях эксплуатации при худшем сочетании факторов выявляются причины отказов, а искомое свойство обнаруживается в результате построения логических формул типа «для того, что исключить причину отказа

в виде... / необходимо, чтобы (такой-то) критичный элемент обладал свойством...». Далее каждое свойство выражается количественно в виде параметров (показателей) и их допустимых значений. Каждое из таких свойств характеризуется вероятностью событий, заключающихся в нахождении соответствующего параметра (показателя) в установленном пределе. При последовательном осуществлении i событий общая оценка ВБР изделия $P(t)$ в результате выполнения процедуры T_1 равна:

$$P(t) = \prod_{i=1}^n P_i(t), \quad (6)$$

здесь

$$P_i(t) = P[X_{\min(i)} \leq X_i(\tau) \leq X_{\max(i)}; 0 \leq \tau \leq t].$$

Формула (6) без учета выполнения процедур T_2 - T_4 дает завышенный результат, поскольку невыполнение или ненадлежащее выполнение любой из конструкторско-технологических процедур снижает надежность. Поэтому АН производят по результатам анализа выполнения процедур T_1 - T_4 исходя из текущего состояния КД и ТД. В случае невыполнения или ненадлежащего выполнения любой из процедур по обеспечению надежности по какому-либо параметру или показателю, в формуле (6) следует применять понижающие корректирующие коэффициенты k_i , которые определяются, например, исходя из метода балльных оценок критичности отказов по ГОСТ 27.310, в результате чего:

$$P(t) = \prod_{i=1}^n k_i P_i(t).$$

Заключение

В статье показаны возможности обеспечения надежности УВС с помощью конструкторско-технологических процедур, применяемых на каждой из стадий ЖЦ до начала эксплуатации. Применение таких процедур способно на единой теоретической и методологической основе поднять на соответствующий уровень технологию проектирования, конструирования, подготовки производства, изготовления и на этой же основе создать методику оценки надежности УВС.

Библиографический список

1. Болотин В.В. Теория надежности механических систем с конечным числом степеней свободы // Изв. АН СССР. Механика твердого тела, 1969. – № 5. – С. 74-81.
2. ГОСТ Р 56526-2015. Требования надежности и безопасности космических систем, комплексов и автоматических космических аппаратов единичного (мелкосерийного) изготовления с длительными сроками активного существования. – М.: Стандартинформ, 2015. – 49 с.
3. Барлоу З., Прошан Ф. Статистическая теория надежности и испытания на безотказность. – М.: Наука, 1984. – 328 с.

4. Тимошенков С.П., Симонов Б.М., Горошко В.Н. Основы теории надежности. – М.: Юрайт, 2015. – 445 с.
5. Ушаков И.А. Надежность – мой компас земной, а удача награда за смелость. Human factors in reliability или Неформальная история теории надёжности [Электронный ресурс] // Gnedenko e-Forum : International Group on Reliability. URL: <http://gnedenko-forum.org/history.htm> (31.08.2016).
6. Половко А.М., Гуров С.В. Основы теории надежности. – СПб.: БХВ-Петербург, 2006. – 704 с.
7. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения. М.: Изд-во стандартов, 1990. 37 с.
8. Похабов Ю.П. О философическом аспекте надежности на примерах уникальных высокоответственных систем // Надежность. – 2015. – № 3. – С. 16-27.
9. Похабов Ю.П. Подход к обеспечению надежности уникальных высокоответственных систем на примере крупногабаритных трансформируемых конструкций // Надежность. – 2016. – № 1. – С. 24-36.
10. Похабов Ю.П., Валишевский О.К. Генезис надежности уникальных высокоответственных систем // Надежность. – 2016. – №3. – С. 47-53.
11. Барт Т.В. Управление качеством. – М.: Издательство МИЭМП, 2010. – 256 с.
12. Бушуев В.В. Практика конструирования машин: справочник. – М.: Машиностроение, 2006. – 448 с.
13. ГОСТ 22487-77. Проектирование автоматизированное. Термины и определения. – М.: Изд-во стандартов, 1978. – 11 с.
14. Р 50.1.031-2001. Информационные технологии поддержки жизненного цикла продукции. Терминологический словарь. Часть 1, Стадии жизненного цикла продукции. – М.: Изд-во стандартов, 2001. – 30 с.
15. ГОСТ ISO 9000-2011. Системы менеджмента качества. Основные положения и словарь. – М.: Стандартинформ, 2012. – 43 с.
16. СТО 154-238-2014. Управление проектированием и разработкой космического аппарата с использованием требований зарубежных стандартов. – Железногорск: АО ИСС, 2014. – 60 с.
17. Design for Reliability/ Edited by Dana Crowe & Alec Feinberg. NY: CRC Press. 2001. 220 p.
18. SAMCO Final Technical Report: F08a Guideline for the assessment of existing structures / W. Rucker, F. Hille, R. Rohrmann. Berlin: Federal Institute of Materials Research and Testing (BAM), 2006. 33 p.

Сведения об авторе

Юрий П. Похабов – кандидат технических наук, Открытое акционерное общество «НПО ПМ – Малое Конструкторское Бюро», начальник центра научно-технических разработок, тел. +7 (913) 593 43 89, Россия, Красноярский край, Железногорск, e-mail: pokhabov_yury@mail.ru

Поступила 31.08.2016

Использование приведенных оценок Эзари-Прошана для анализа надежности систем

Александр Г. Лабутин, Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», Россия, Москва

Борис П. Филин, Россия, Москва

Если, изучая какое-либо явление, я умею количественно оценить хотя бы одну какую-либо его сторону, то я кое-что знаю об этом явлении. В противном случае я ничего о нём не знаю...

Уильям Томсон (лорд Кельвин)

Резюме. В работах [1–2] показано, что широко известные оценки Эзари-Прошана [3–6] (ОЭП) являются NP-полными [7]. В процессе их вычисления происходит взаимное переkreщивание этих оценок, несмотря на то, что процедура перечисления полных множеств простых цепей (ПЦ) и простых разрезов (ПР) выполняется до конца. Эта картина подтверждается и специальными исследованиями этих парадоксальных явлений в ОЭП, приведенными в работе [8], где был сделан вывод о том, что ОЭП – это никакие не оценки, поскольку оценки не могут быть NP-полными. Ведь в [7] прямо говорится о том, что в общем случае только одно лишь перечисление полного множества ПЦ (или ПР) уже есть NP-полная задача. Отсюда следует непосредственно: любой NP-полный метод не может быть оценочным. В работах [9–10] дана классификация вычислительной трудоёмкости тех или иных задач. Можно видеть, что из представленных наиболее привлекательной является интеллектуальная трудоёмкость, поскольку она позволяет управлять вычислительным процессом самым вожделенным способом, а именно – позволяет реализовать принцип принудительного прерывания (ППП) вычислительной процедуры, оцениваемой каким либо параметром. Например, параметром достигнутой относительной погрешности вычислений. Заметим, что в жизни мы чаще всего сталкиваемся с устройствами, механизмами, агрегатами и прочими системам, которые называются автоматизированными системами, поскольку в этих человеко-машинных комплексах и реализуется ППП по воле человека-оператора. С автоматическими системами мы имеем существенно меньший контакт. **Целью** данной статьи является изложение формальных правил, которые позволяют достаточно просто классические NP-полные оценки Эзари-Прошана привести к классу интеллектуальных (IN-класс) оценочных методов, реализующих ППП. Здесь не нужно перечислять полные множества ПЦ и ПР. Пополнение класса уже существующих [1–6, 8, 11–29] методов, в которых так или иначе, но реализован ППП, несомненно, является актуальной задачей для специалистов, занимающихся анализом структурной надёжности сложных систем. Это же аксиома – любой из инструментов подобного рода анализа систем, «повивальной бабкой» которых является полная группа событий (ПГС), вносит свою лепту в дело построения структурно надёжных систем, развивая, в то же время, саму систему инструментария анализа. Суть дела заключается в облачении классических ОЭП в так называемые «одежды» логики-символьного умножения (ЛСУ) логических операндов, которыми оперирует метод. **Результат** заключается в том, что мы снимаем «тяготы» NP-полноты с классических ОЭП, получая достаточно эффективный инструмент анализа.

Ключевые слова: надёжность, вероятность, двухполюсная сеть, простая цепь, простой разрез, исправное состояние, неисправное состояние.

Сокращения: ОЭП – оценки Эзари-Прошана; ПЦ – простая цепь; ПР – простой разрез; ППП – принцип принудительного прерывания; ПГС – полная группа событий; ЛСУ – логики-символьное умножение; СГ – случайный граф; ВГП – вершины граничной пары; ДС – двухполюсная сеть; ИС – исправное состояние; НС – неисправное состояние; ВС – вероятность связности; ЛАУ – логики-алгебраическое умножение; дПГСк – дополнение до ПГС конъюнкции.

Формат цитирования: Лабутин А.Г., Филин Б.П., Использование приведенных оценок эзари-прошана для анализа надежности систем // Надежность. 2017. Т. 17, № 3. С. 24–31. DOI: 10.21683/1729-2646-2017-17-3-24-31

1. Введение

В работах [9–10] приводится следующая классификация трудоёмкости вычисления задач в зависимости от их сложности: а) линейная; б) полиномиальная; в) экспоненциальная; г) N -факториальная; д) интеллектуальная (IN). Последняя среди структуристов-надёжностников зовётся проще: принцип принудительного прерывания вычислительного процесса человеком, когда он к данному моменту времени удовлетворяется достигнутой погрешностью вычислений. Поскольку в ОЭП имеет место быть логическое перемножение логических операндов, описывающих состояния ПЦ и ПР без учёта их взаимной структурной зависимости, то в данной статье вводятся разработанные правила ЛСУ таких операндов с учётом этой зависимости. В результате этого классические ОЭП по трудоёмкости вычислений переходят в IN -класс, поскольку они становятся принудительно-прерываемыми.

По сути дела в статье доказательно излагаются формальные правила перевода NP -трудных классических ОЭП в удобный и лёгкий инструментарий, не обременённый перечислением полных множеств ПЦ и ПР. Такие оценки будем называть приведенными ОЭП.

2. Постановка задачи

2.1. Предварительные сведения. Пусть задан (см. рисунок 1) простой рёберный случайный граф (СГ) [11–14, 30–31] G : простой – значит без петель, параллелей и изолированных вершин; случайный – значит его элементы либо присутствуют в графе с вероятностью p , либо отсутствуют в нём с вероятностью $q = 1 - p$ (поскольку $p + q = 1$, то присутствие вместе с отсутствием ребра в графе составляет ПГС, обозначаемую символом I [31]); рёберный – в графе ненадёжны только рёбра (это допущение не принципиальное, зато очень упрощает парадигму изложения). Граф G содержит множество вершин $V = \{v_i\}$, мощностью $m_v = |V|$, и рёбер $L = \{l_{ij}\}$, мощностью $m_L |L|$, взаимосвязь между которыми отражает функция инцидентности и смежности вида $\Phi(l_{ij}) = v_i \& v_j$;

ребро инцидентно своим вершинам граничной пары (ВГП), а ВГП – смежны друг другу по ребру l_{ij} .

Пусть на этом графе будет задана двухполюсная сеть (ДС), вершины полюса которой обозначим как s (исток) и t (сток) с параметрами: $m_v = 4$ и $m_L = 5$. Например, так, как это показано на рисунке 1, а (такую структуру специалисты часто называют «мостиком» [16]). Заметим, что в ДС появляются теперь транзитные вершины вида $V_{s,t}^T = V \setminus \{s, t\}$. В нашем случае $V_{s,t}^T = \{2, 3\}$ (см. рисунок 1).

На рисунке 1, б показан граф с перенумерованными (методом «вычёркивания дуг» [16]) рёбрами числами, начиная от $(m_v + 1)$ с шагом 1 и до $(m_v + m_L)$, а на рисунке 1, в – тот же перенумерованный СГ, но здесь символ « l » на рёбрах для чистоты рисунка опущен. К этому рисунку мы и будем чаще всего прибегать. Таким образом, на рисунке 1, в представлена «сквозная» нумерация элементов СГ. Заметим, что при формировании каких-либо конструкций на СГ (например, ПЦ или ПР) символы « v » и « l » использовать будем достаточно редко.

Сформируем в ДС (рисунок 1, в) множество её ПЦ, руководствуясь принципом: «Каждая вершина-родитель выбирает себе вершину-ребёнка из смежных с ней и не занятых ещё вершин, которая имеет наименьший номер k » [17]:

$$F_{s,t} = \left\{ \begin{aligned} f_1 &= \{5, 7, 9\}, f_2 = \{5, 8\}, \\ f_3 &= \{6, 7, 8\}, f_4 = \{6, 9\} \end{aligned} \right\} \Rightarrow (m_F = |F_{s,t}| = 4). \quad (1)$$

Из (1) видно, что каждая транзитная вершина побывала и в роли «родителя», и в роли «ребёнка», но s (исток) – только «родителем», а t (сток) – только «ребёнком».

Также сформируем и множество ПР (методом «последовательного старта» [17]):

$$R_{s,t} = \left\{ \begin{aligned} r_1 &= \{5, 6\}, r_2 = \{6, 7, 8\}, \\ r_3 &= \{5, 7, 9\}, r_4 = \{8, 9\} \end{aligned} \right\} \Rightarrow (m_R = |R_{s,t}| = 4). \quad (2)$$

ПЦ исправна, если все её рёбра в исправном состоянии (ИС): $\bar{f}_n = \forall l_k \in f_n \left[\bar{l}_k \right]$, и неисправна, если в

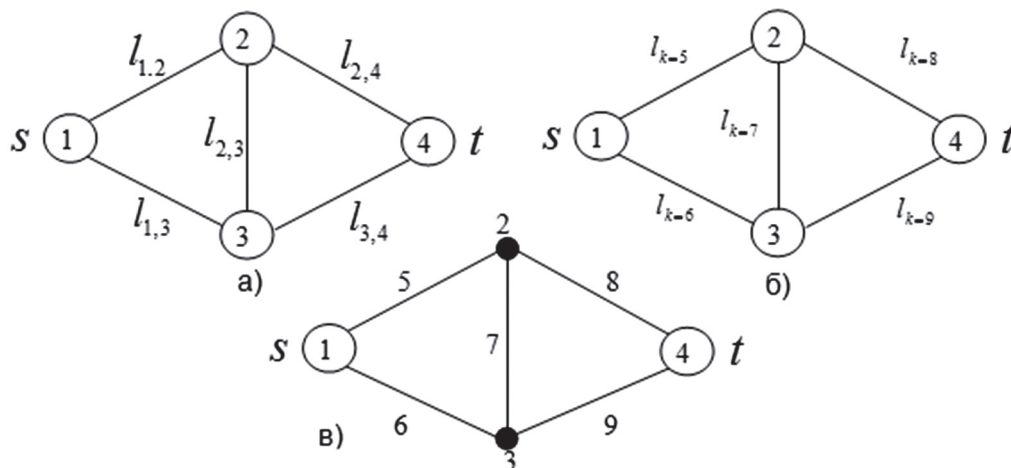


Рисунок 1 – Перенумерованный простой рёберный случайный граф

неисправном состоянии (НС) находится хотя бы одно её ребро: $\bar{f}_n = \exists l_k \in f_n [\bar{l}_k]$ (здесь $\forall$ – квантор «общности», $\exists$ – квантор «существования», $\in$ – символ «принадлежит» [30–33]). ПР исправен, если все его рёбра в НС: $\bar{r}_n = \forall l_k \in r_n [\bar{l}_k]$, и неисправен, если в ИС находится хотя бы одно его ребро: $\bar{r}_n = \exists l_k \in r_n [\bar{l}_k]$.

2.2 Поясняющий пример. Примем исходные данные по КГ рёбер СГ ДС такие:

$$(L \neq \emptyset) \Rightarrow (p_5 = 0, 5, p_6 = 0, 6, p_7 = 0, 7, p_8 = 0, 8, p_9 = 0, 9), \quad (3)$$

где $\Rightarrow$ – символ «следования» [31–33].

Вычислим точное значение вероятности связности (ВС) нашей ДС. Сначала, опираясь на (1), опишем полное событие связности (СоС) ДС (когда вершины-полюса ДС связаны хотя бы одной исправной ПЦ), обозначаемое символом $E_{s,t}$:

$$E_{s,t} = 5 \cdot 7 \cdot 9 + 5 \cdot 8 \cdot \overline{7 \cdot 9} + 6 \cdot 7 \cdot 8 \cdot \bar{5} + 6 \cdot 9 \cdot (\bar{5} \cdot \overline{7 \cdot 8} + 5 \cdot \bar{7} \cdot \bar{8}), \quad (4)$$

где $\cdot$ – символ логико-алгебраического умножения (ЛАУ) (* – символ ЛСУ, при котором, в отличие от ЛАУ, учитывается структурная зависимость перемножаемых логических операндов).

Заметим, что здесь (и далее) мы ИС рёбер «не нагружали» двойной чертой над элементами операндов, поскольку она гласила о том, что ребро «не неисправно». Двойное отрицание и есть ИС (черта черту уничтожает) ребра, т.е. «не неисправен» и «исправен» – это синонимы. Запишем расчётную формулу для $P_{s,t}$, опираясь из результат (4):

$$P_{s,t} = p_5 \cdot p_7 \cdot p_9 + p_5 \cdot \overline{p_8 \cdot p_7 \cdot p_9} + p_6 \cdot p_7 \cdot p_8 \cdot q_5 + p_6 \cdot p_9 \cdot (\overline{q_5 \cdot p_7 \cdot p_8} + p_5 \cdot q_7 \cdot q_8). \quad (5)$$

Подставим в (5) наши исходные данные (3) и получим, что точное (в рамках точности исходных данных (3)) значение ВС нашей ДС равно:

$$P_{s,t} = 0,315 + 0,148 + 0,168 + 0,136 = \underline{0,766}. \quad (6)$$

Теперь у нас есть некоторое «мерило» в виде $P_{s,t} = 0,766$, позволяющее проводить некоторое сравнение между «старым» и «новым», т.е. предлагаемым.

2.3. Собственно постановка задачи. Прежде всего, запишем согласно [3] для общего случая формальное представление ОЭП таким образом:

$$\left. \begin{aligned} E_{s,t}^B &= I - \prod_{n=1}^{m_F} \cdot \bar{f}_n = I - \prod_{n=1}^{m_F} \left(I - \prod_{e=1}^{m_n} \cdot \bar{l}_{k_e} \right) = \\ E_{s,t}^H &= \prod_{n=1}^{m_R} \cdot \bar{r}_n = \prod_{n=1}^{m_R} \left(I - \prod_{e=1}^{m_n} \cdot \bar{l}_{k_e} \right) = \prod_{n=1}^{m_R} \left(\prod_{e=1}^{m_n} \cdot \bar{l}_{k_e} \right) \end{aligned} \right\} \quad (7)$$

Здесь: $\prod$ – конъюнкция (логическое (или арифметическое) произведение); $\prod$ – дополнение до ПГС (или до 1) конъюнкции (логической или арифметической) (дПГСк).

Если без промежуточных преобразований, то ОЭП можно записать так:

$$\left. \begin{aligned} E_{s,t}^B &= I - \prod_{n=1}^{m_F} \cdot \bar{f}_n = \prod_{n=1}^{m_F} \left(\prod_{e=1}^{m_n} \cdot \bar{l}_{k_e} \right) \\ E_{s,t}^H &= \prod_{n=1}^{m_R} \cdot \bar{r}_n = \prod_{n=1}^{m_R} \left(\prod_{e=1}^{m_n} \cdot \bar{l}_{k_e} \right) \end{aligned} \right\} \quad (8)$$

Применительно к нашему примеру СГ (см. рисунок 1) эти события (согласно (1), (2) и (8)) графически можно представить так, как это показано на рисунке 2.

Можно видеть, что избыточное СоС ДС по ПЦ читается так: «Дополнение до ПГС конъюнкции дополнений до ПГС конъюнкций ИС рёбер, входящих в n -ые ПЦ». В то же время, ущербное описание СоС ДС по ПР читается несколько иначе: «Конъюнкция дополнений до ПГС конъюнкций ИС рёбер, входящих в n -ые ПР».

Если ДСО ВС ДС вычислены, то расчёт приближённой оценки $P_{s,t}^{\approx}$ относительной погрешности $\Delta_{s,t}$ (априори) и абсолютной погрешности $W_{s,t}$ (апостериори) прост:

$$P_{s,t}^{\approx} = \frac{P_{s,t}^B + P_{s,t}^H}{2}, \quad \Delta_{s,t} = \frac{|P_{s,t}^B - P_{s,t}^H|}{2},$$

$$W_{s,t} = |P_{s,t} - P_{s,t}^{\approx}| \text{ и } W_{s,t} < \Delta_{s,t}. \quad (9)$$

1. Требуется доказать (см. первое в (8)), что игнорирование структурной зависимости логических операндов конъюнкции приводит к избыточности в описании СоС ДС.

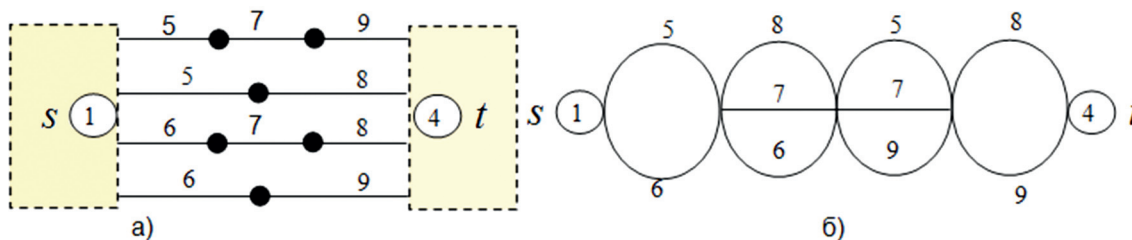


Рисунок 2 – «Мостик» в терминах элементарных событий ОЭП

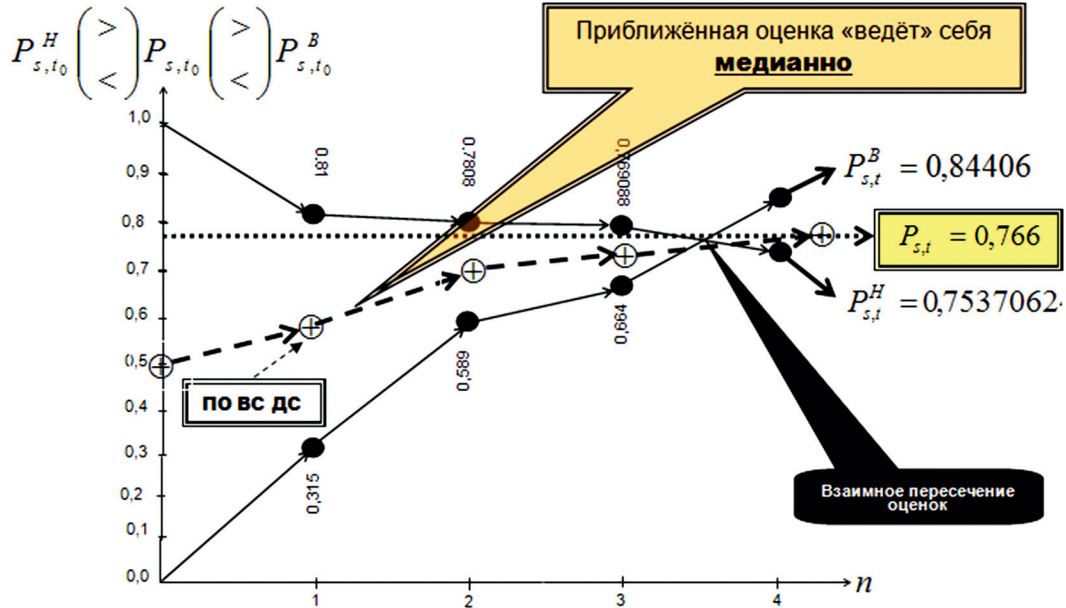


Рисунок 3 – График двойного изображения «поведения» ДСО ВС для «мостика» при принятых исходных данных

$$\forall l_{(5 \leq v \leq 9)} \in L \left[p_{(5 \leq v \leq 9)} = 0, (5 \leq v \leq 9) \right]$$

2. Требуется доказать (см. второе в (8)), что игнорирование структурной зависимости логических операндов дПГСк приводит к ущербности в описании СоС ДС.

3. Доказанное проиллюстрировать графически и числовым примером.

3. Решение задачи

Руководствуясь правилами (7-8) и множествами ПЦ (1) и ПР (2), можно записать, что применительно к «мосту» (рис.1,в и рис. 2) ОЭП запишем следующим образом:

$$\left. \begin{aligned} E_{s,t}^B &= \overline{5 \cdot 7 \cdot 9 \cdot 5 \cdot 8 \cdot 6 \cdot 7 \cdot 8 \cdot 6 \cdot 9} \\ E_{s,t}^H &= \overline{5 \cdot 6 \cdot 6 \cdot 7 \cdot 8 \cdot 5 \cdot 7 \cdot 9 \cdot 8 \cdot 9} \end{aligned} \right\} \quad (10)$$

На основе (10) получим следующие расчётные формулы для ДСО ВС ДС (для ВО и для НО ВС ДС):

$$\left. \begin{aligned} P_{s,t}^B &= \overline{p_5 \cdot p_7 \cdot p_9 \cdot p_5 \cdot p_8 \cdot p_6 \cdot p_7 \cdot p_8 \cdot p_6 \cdot p_9} \\ P_{s,t}^H &= \overline{q_5 \cdot q_6 \cdot q_6 \cdot q_7 \cdot q_8 \cdot q_5 \cdot q_7 \cdot q_9 \cdot q_8 \cdot q_9} \end{aligned} \right\} \quad (11)$$

Поскольку здесь мы имеем дело с пошаговым «накоплением» некоторого численного значения, как результата перемножения (а не аддитивности), то мы эту «пошаговость» будем отображать просто переходными стрелочками. Воспользуемся нашими исходными данными (3) и вычислим по ОЭП ДСО ВС ДС: ВО $P_{s,t}^B$ и НО $P_{s,t}^H$, помня о том (см. (6)), что $P_{s,t} = 0,766$:

$$\left. \begin{aligned} P_{s,t}^B &= 0,315 \rightarrow 0,589 \rightarrow 0,664 \rightarrow 0,84406 = P_{s,t}^B \\ P_{s,t}^H &= 0,81 \rightarrow 0,7808 \rightarrow 0,769088 \rightarrow 0,75370624 = P_{s,t}^H \end{aligned} \right\} \quad (12)$$

Воспользуемся полученным и построим график двойного отображения [17, 20] «поведения» ДСО ВС нашей ДС (см. рисунки 1,в, 2 и 3).

Анализируя полученное, можно видеть, что парадоксальные явления классических ОЭП налицо: а) ВО ВС ДС начинает накапливаться от 0, а НО – от 1; б) ДСО ВС ДС взаимно пересекаются; в) после пересечения ДСО ВС ДС начинают расходиться.

На рисунке 4 приведена ось вероятностей, её области и интервалы, которые должны нам помочь при ниже следующих рассуждениях.

Рассуждая о конъюнкциях и их дополнениях (7) и (8), поневоле приходишь к пониманию их «неравно-весности» в ряде случаев и важных, и не столь важных. Например, арифметическое произведение вида $\prod$ в исходном состоянии мысленно «объединчивают» (как сумму «обнуляют» в исходном положении):

$$\left. \begin{aligned} n &= \overline{1, N} \\ n &:= 0 \end{aligned} \right\} \Rightarrow \prod := 1. \quad (13)$$

Конъюнкцию в исходном состоянии также необходимо «обПолноГруппно-Событийствовать» таким образом:

$$\left. \begin{aligned} n &= \overline{1, N} \\ n &:= 0 \end{aligned} \right\} \Rightarrow \prod := I. \quad (14)$$

Тогда дПГСк в исходном состоянии необходимо «обНевозможноСобытийствовать» таким образом:

$$\left. \begin{aligned} n &= \overline{1, N} \\ n &:= 0 \end{aligned} \right\} \Rightarrow \prod = I - \prod = I - I = \otimes, \quad (15)$$

где $\otimes$ – символ невозможного события.

Дополнение арифметического произведения до 1 «обнуляем», поскольку мы находимся в диапазоне числовых значений от «нуля» и до «единицы»:

$$\left. \begin{aligned} n &= \overline{1, N} \\ n &:= 0 \end{aligned} \right\} \Rightarrow \prod = 1 - \prod = 1 - 1 = 0. \quad (16)$$

Мы исходим из того, что $I * I = I$, $I + I = I$, $\otimes * \otimes = \otimes$, $\otimes + \otimes = \otimes$, но $I + \otimes = \otimes$, $I \otimes = I$.

Поясним только две аббревиатуры на рисунке 4: СВН – события вероятности ноль; СВЕ – события вероятности единица [9–10]. Учитывая, что в теории комбинаторной надёжности наши расчёты зиждутся на числовых значениях в интервале от 0 до 1 (включая эти границы), то сформулируем некоторые утверждения и теоремы.

Утверждение 1 (см. рисунок 4). С увеличением числа сомножителей в виде вероятностных числовых значений численное значение их произведения резко уменьшается и устремляется в область СВН (это остаётся справедливым, если операнды поменять ролями).

Утверждение 2 (см. рисунок 3). С увеличением числа логических сомножителей высказываемая ими логическая фраза становится менее достоверной.

И ещё одно... В работе [16] записано: «*При раскрытии скобок не забывай выполнять простое правило $p \cdot p = p$* ». Используя его, мы это правило называем именем автора этой работы: «**Правило Богатырёва**».

Теорема 1. Событие связности ДС, описываемое дПГСк, каждая из которых, в свою очередь, представляет собой дПГСк, сомножителями которой являются ИС рёбер СГ, несомненно, является избыточным, т.е.:

$$\begin{aligned} f_1 = \{a, b\} &\Rightarrow \left[\left(\overline{a \cdot b \cdot a \cdot c} \right) > \left(\overline{a \cdot b \cdot a \cdot c} = a \cdot \overline{b \cdot c} \right) \right] \\ f_2 = \{a, c\} &\Rightarrow \left[\left(\overline{a \cdot b \cdot a \cdot c} \right) > \left(\overline{a \cdot b \cdot a \cdot c} = a \cdot \overline{b \cdot c} \right) \right]. \end{aligned} \quad (17)$$

Доказательство:

$$\begin{aligned} &\left(\left(\overline{a \cdot b \cdot a \cdot c} \right) \Leftrightarrow \left(a \cdot \overline{b \cdot c} \right) \right) \Rightarrow \\ &\Rightarrow \left(\left((I - (I - a \cdot b) \cdot (I - a \cdot c)) \Leftrightarrow (a \cdot (I - (I - b) \cdot (I - c))) \right) \right) \Rightarrow \\ &\Rightarrow \left(\left(I - (I - a \cdot b - a \cdot c + a^2 \cdot b \cdot c) \right) \Leftrightarrow \left(a \cdot (I - (I - b - c + b \cdot c)) \right) \right) \Rightarrow \\ &\Rightarrow \left(\left(I - I + a \cdot b + a \cdot c - a^2 \cdot b \cdot c \right) \Leftrightarrow \left(a \cdot (I - I + b + c - b \cdot c) \right) \right) \Rightarrow \\ &\Rightarrow \left((a \cdot b + a \cdot c - a^2 \cdot b \cdot c) \Leftrightarrow (a \cdot b + a \cdot c - a \cdot b \cdot c) \right) \Rightarrow \\ &\Rightarrow \left(\underline{\underline{(-a) \Leftrightarrow (-I)}} \right). \end{aligned}$$

Переходя к стохастической стороне «эндшпиля» и помятуя о том, что $(0 < p_{(a,b,c)} < 1)$, легко видеть, что итог сравнения выполняется именно так $((-p_a) > -1)$, ч.т.д. ($\Leftrightarrow$ – знак «сравнить»)

Следствие 1.1. Поскольку в ОЭП используется только ЛАУ, то согласно (17) в ОЭП (см. первое из (8)) всегда описывается только избыточное СоС ДС, что и

приводит к пересечению ВО снизу точного значения ВС ДС, вследствие чего эта ВО и является ложной оценкой.

Следствие 1.2. Для устранения этого недостатка необходимо при описании ВО ВС ДС ОЭП вместо ЛАУ использовать давно известные правила ЛСУ [17, 20]. Тогда избыточного описания СоС ДС не будет, а ложная ВО ВС ДС по ОЭП обратится в истинную, т.е. в нижнюю НО ВС ДС. Правила ЛСУ для ПЦ в НС (см. первое из (8) и [17, 20]) таковы:

$$\left. \begin{aligned} \overline{a} * \overline{a \cdot b} &= \overline{a} \\ \overline{a \cdot b} * \overline{a \cdot c} &= \overline{a \cdot \overline{b \cdot c}} \\ \overline{a \cdot \overline{b \cdot c}} * \overline{b \cdot d} &= \overline{a \cdot \overline{b \cdot d}} + \overline{a \cdot \overline{b \cdot c}} \\ \overline{a} * \overline{b} &= \overline{a \cdot b} \end{aligned} \right\} \quad (18)$$

Теорема 2. Событие связности ДС, описываемое конъюнкцией дПГСк, сомножителями которых являются НС рёбер СГ, несомненно, является избыточным, т.е.:

$$\begin{aligned} r_1 = \{a, b\} &\Rightarrow \left[\left(\overline{a \cdot b \cdot a \cdot c} \right) > \left(\overline{a \cdot b \cdot a \cdot c} = a \cdot \overline{b \cdot c} \right) \right] \\ r_2 = \{a, c\} &\Rightarrow \left[\left(\overline{a \cdot b \cdot a \cdot c} \right) > \left(\overline{a \cdot b \cdot a \cdot c} = a \cdot \overline{b \cdot c} \right) \right]. \end{aligned} \quad (19)$$

Доказательство: Также переведём сравнение в «эндшпиль», для чего выполним следующее:

$$\begin{aligned} &\left(\left(\overline{a \cdot b \cdot a \cdot c} \right) \Leftrightarrow \left(a \cdot \overline{b \cdot c} \right) \right) \Rightarrow \left(\left((I - \overline{a \cdot b}) \cdot (I - \overline{a \cdot c}) \right) \Leftrightarrow \right. \\ &\Leftrightarrow \left[(I - \overline{a \cdot b \cdot c}) \right] = (I - \overline{a \cdot b \cdot c}) \cdot (I - \overline{a \cdot c}) = \\ &= (I - \overline{a \cdot b \cdot c}) \cdot (I - \overline{a \cdot c}) = (I - \overline{a \cdot b \cdot c}) \cdot (I - \overline{a \cdot c}) = \\ &= (I - \overline{a \cdot b \cdot c}) \cdot (I - \overline{a \cdot c}) = (I - \overline{a \cdot b \cdot c}) \cdot (I - \overline{a \cdot c}) = \\ &= (I - \overline{a \cdot b \cdot c}) \cdot (I - \overline{a \cdot c}) = (I - \overline{a \cdot b \cdot c}) \cdot (I - \overline{a \cdot c}) = \\ &\Rightarrow \left[\left(I - \overline{a \cdot b \cdot c} - \overline{a \cdot c} + \overline{a \cdot b \cdot c} \cdot \overline{a \cdot c} \right) \Leftrightarrow \left(I - \overline{a \cdot b \cdot c} - \overline{a \cdot c} + \overline{a \cdot b \cdot c} \cdot \overline{a \cdot c} \right) \right] \Rightarrow \left(\overline{a} \Leftrightarrow \otimes \right). \end{aligned}$$

Переходя к стохастической стороне «эндшпиля» и помятуя о том, что $(0 < p_{(a,b,c)} < 1)$, что всегда будет справедливым неравенство вида $q_a > 0$. Из этого следует, что исходное (19) верно, ч.т.д.

Следствие 2.1. Поскольку в ОЭП используется только ЛАУ, то согласно (19) в ОЭП (см. второе из (8)) всегда описывается только избыточное СоС ДС, что и приводит к пересечению сверху НО точного значения ВС ДС, вследствие чего эта НО также является ложной оценкой (заметим, что при этих рассуждениях не следует забывать, что здесь мы используем ГДИ [17, 20]).

Следствие 2.2. Для устранения этого недостатка необходимо при описании НО ВС ДС в ОЭП вместо ЛАУ

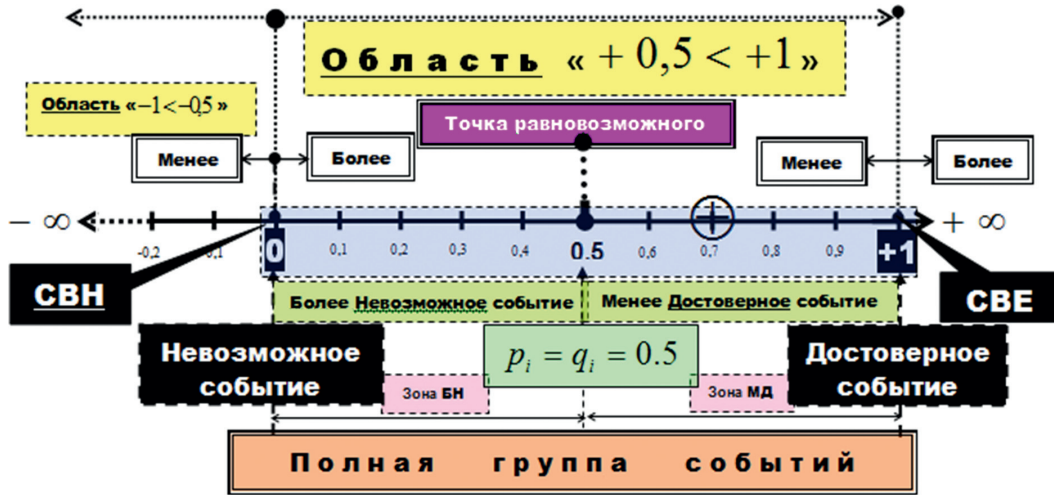


Рисунок 4 – Ось вероятностей

использовать известные правила ЛСУ [17, 20]. Тогда избыточного описания СоС ДС не будет иметь место, а ложная НО ВС ДС по ОЭП обратится в истинную, но в верхнюю ВО ВС ДС. Правила ЛСУ для ПР в НС (см. второе из (8) и [17, 20]) таковы:

$$\left. \begin{aligned} a * \overline{a} * \overline{b} &= a \\ \overline{a} * \overline{b} * \overline{a} * \overline{c} &= \overline{a} * \overline{b} * \overline{c} \\ \overline{a} * \overline{b} * \overline{c} * \overline{b} * \overline{d} &= \overline{a} * \overline{b} * \overline{d} + \overline{a} * \overline{b} * \overline{c} \\ a * b &= a * b \end{aligned} \right\} \quad (20)$$

На рисунке 5 представлена графическая интерпретация изложенного в теоремах 1 и 2.

Таким образом, окончательно правила ЛСУ и ОЛФ будут выглядеть следующими:

Нижняя оценка (по ПЦ):

$$\left. \begin{aligned} \overline{a} * \overline{a} * \overline{b} &= \overline{a} \\ \overline{a} * \overline{b} * \overline{a} * \overline{c} &= \overline{a} * \overline{b} * \overline{c} \\ \overline{a} * \overline{b} * \overline{c} * \overline{b} * \overline{d} &= \overline{a} * \overline{b} * \overline{d} + \overline{a} * \overline{b} * \overline{c} \\ \overline{a} * \overline{b} &= \overline{a} * \overline{b} \end{aligned} \right\} \Rightarrow \left(E_{s,t}^H = \prod_{e=1}^{m_F} \overline{f}_e \mid (e=0) \Rightarrow \prod_{e=0}^{m_F} \overline{I} \right) \leq E_{s,t} \quad (21)$$

где $\overline{}$ – «при условии», а

Верхняя оценка (по ПР):

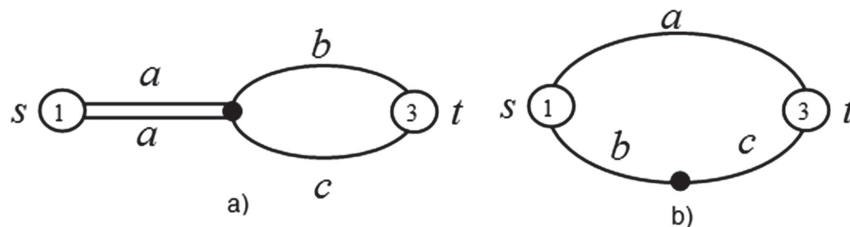


Рисунок 5 – Графическая интерпретация

$$\left. \begin{aligned} a * \overline{a} * \overline{b} &= a \\ \overline{a} * \overline{b} * \overline{a} * \overline{c} &= \overline{a} * \overline{b} * \overline{c} \\ \overline{a} * \overline{b} * \overline{c} * \overline{b} * \overline{d} &= \overline{a} * \overline{b} * \overline{d} + \overline{a} * \overline{b} * \overline{c} \\ a * b &= a * b \end{aligned} \right\} \Rightarrow \left(E_{s,t}^B = \prod_{e=1}^{m_R} \overline{r}_e \mid (e=0) \Rightarrow \prod_{e=0}^{m_R} \overline{I} \right) \geq E_{s,t} \quad (22)$$

На этом описание основного результата закончено.

4. Пример

Поскольку лимит на листы очень исчерпан, то обойдёмся «мостиком» (см. рисунок 1,в), множества ПЦ и ПР которого размещены соответственно в (1) и (2), а исходные данные по КГ рёбер – в (3). Итак, вычислим «поведение» НО ВС ДС, опираясь на формальные правила ОЛФ (19):

$$\begin{aligned} E_{s,t}^H &= I * \overline{5} * \overline{7} * \overline{9} = \overline{5} * \overline{7} * \overline{9} \rightarrow \overline{5} * \overline{7} * \overline{9} * \overline{5} * \overline{8} = \\ &= \overline{5} * \overline{7} * \overline{9} * \overline{8} = \overline{5} * \overline{7} * \overline{9} * \overline{8} \rightarrow \overline{5} * \overline{7} * \overline{9} * \overline{8} * \overline{6} * \overline{7} * \overline{8} = \dots \\ &\dots = \left(\overline{5} * \overline{6} * \overline{7} * \overline{8} + \overline{5} * \overline{7} * \overline{9} * \overline{8} \right) \rightarrow \\ &\rightarrow \left(\overline{5} * \overline{6} * \overline{7} * \overline{8} + \overline{5} * \overline{7} * \overline{9} * \overline{8} \right) * \overline{6} * \overline{9} = \dots \\ &\dots = \left(\overline{5} * \overline{6} * \overline{7} * \overline{8} * \overline{9} + \overline{5} * \overline{7} * \overline{6} * \overline{9} * \overline{8} \right) \end{aligned} \quad (23)$$

Подчёркнутый снизу двойной чертой есть окончательный результата на соответствующем шаге после ЛСУ операндов. Если из (21) убрать все промежуточные логические операции, то тогда мы получим короткую запись следующего вида:

$$\begin{aligned} E_{s,t}^H &= 5 \cdot 7 \cdot 9_1 \rightarrow 5 \cdot \overline{7 \cdot 9 \cdot 8_2} \rightarrow \\ &\rightarrow \left(\overline{5 \cdot 6 \cdot 7 \cdot 8 + 5 \cdot 7 \cdot 9 \cdot 8} \right)_3 \rightarrow \\ &\rightarrow \left(\overline{5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 + 5 \cdot 7 \cdot 6 \cdot 9 \cdot 8} \right)_4. \end{aligned} \quad (24)$$

Воспользуемся нашими исходными данными (3) и покажем динамику «нормального» поведения НО ВС ДС, получаемой по изложенным в статье правилам ОЛФ (19), позволившим, наконец-таки, оценкам прекратить их взаимное перекрещивание и внезапно из НО превращаться в ВО ВС ДС, что было отличительнейшей чертой «классических» ОЭП. Восходящие НО ВС ДС таковы:

$$P_{s,t}^H = 0,315_1 \rightarrow 0,463_2 \rightarrow 0,631_3 \rightarrow \underline{\underline{0,766}}_4 = P_{s,t}. \quad (25)$$

Можно видеть, что на последнем 4-м шаге НО ВС ДС точно равна точному значению ВС ДС, вычисленному в (6).

Теперь, воспользовавшись правилами (22) опишем динамику «нормального» поведения ВО ВС ДС методом ОЛФ:

$$\begin{aligned} E_{s,t}^B &= I \cdot \overline{5 \cdot 6} = \underline{\underline{5 \cdot 6}} \rightarrow \left(\overline{5 \cdot 6 \cdot 7 \cdot 8} = \underline{\underline{6 \cdot 5 \cdot 7 \cdot 8}} \right)_2 \rightarrow \\ &\rightarrow \left(\overline{6 \cdot 5 \cdot 7 \cdot 8 \cdot 9} = \underline{\underline{6 \cdot 5 \cdot 7 \cdot 9 \dots + 6 \cdot 5 \cdot 7 \cdot 8}} \right)_3 \rightarrow \\ &\rightarrow \left(\overline{6 \cdot 5 \cdot 7 \cdot 9 + 6 \cdot 5 \cdot 7 \cdot 8} \cdot 8 \cdot 9 = \underline{\underline{6 \cdot 9 \cdot 5 \cdot 7 \cdot 8 + 6 \cdot 5 \cdot 8 \cdot 7 \cdot 9}} \right)_4. \end{aligned} \quad (26)$$

Воспользовавшись нашими исходными данными (3) легко получаем численные значения нисходящих ВО ВС ДС к точному значению ВС ДС:

$$P_{s,t}^B = 0,8 \rightarrow 0,788 \rightarrow 0,779 \rightarrow \underline{\underline{0,766}} = P_{s,t}. \quad (27)$$

Видно, что и ВО ВС ДС в итоге также стала равной точному значению ВС ДС, вычисленному в (6).

На базе полученных в (25) и (27) результатов вычислений можно легко построить график двойного изображения [17, 20] динамики восхождения НО и нисхождения ВО ВС ДС к точному значению ВС ДС. Этот график представлен на рисунке 6. Здесь же, на рисунке 6, показано, что на 2-м шаге вычислений был реализован ППП процедуры вычислений, вычислены оценочные параметры расчётов, руководствуясь которыми оператор должен решить, будет ли он (или не будет) продолжать вычисления.

5. Заключение

Мы полагаем, что постановка задачи реализована нами (соавторами) вполне достаточно и полно. Видно, что приведенные ОЭП не относятся к *NP*-классу. Эти новые оценки истинно *IN*-класса, базирующиеся на интеллект вычислителя-человека. Такой подход очень популярен среди структуристов-надёжностников.

Библиографический список

1. Кривулец В.Г. Об оценке оценок Эзари-Прошана в задачах анализа структурной надежности сетей связи // Труды 55-й Научной сессии, посвященной дню Радио / РНТОРЭС им. А.С.Попова, 2000.
2. Филин Б.П. О предельном развязывании клаттеров в оценках Полесского границ комбинаторной надёж-

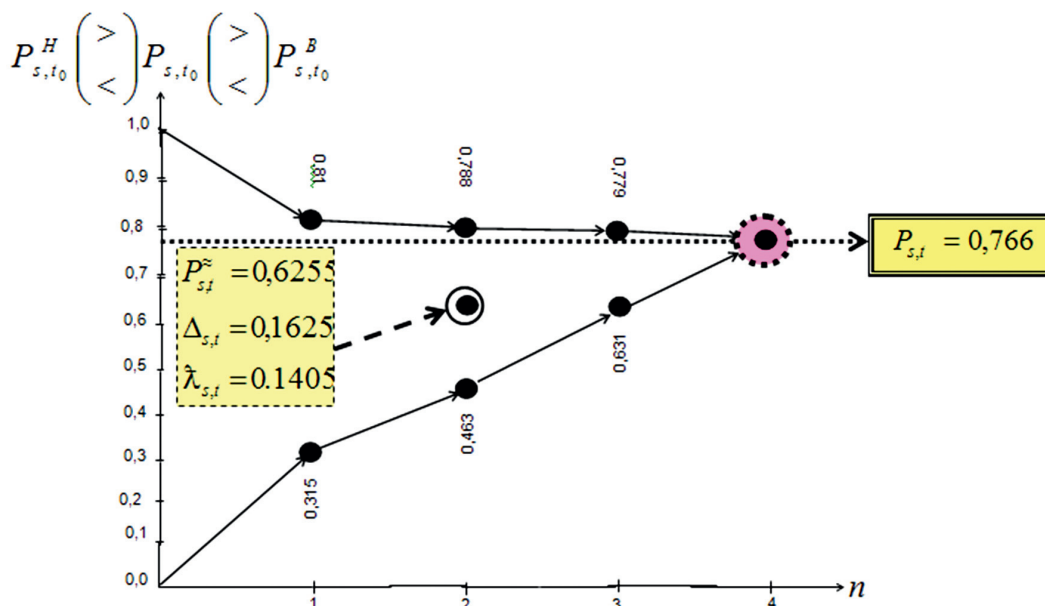


Рисунок 6 – График двойного изображения «поведения» ДСО ВС для «мостика» при принятых исходных данных

$$\forall l_{(5 \leq v \leq 9)} \in L[p_{(5 \leq v \leq 9)} = 0, (5 \leq v \leq 9)]$$

ности случайных бинарных систем // Автоматика и телемеханика. – 2005. – № 9. – С. 149-189.

3. Esary J., Proshan F. Coherent Structures of Non-Identical Components // Technometrics. 1963. V. 5. № 2. P. 191-209.

4. Эзари Дж., Прошан Ф. Надёжность связанных систем // Методы введения избыточности для вычислительных систем: Сб. М.: Радио и связь, 1966.

5. Барлоу Р., Прошан Ф. Математическая теория надёжности: Пер. с англ. / Под ред. Б.В. Гнеденко Б.В. М.: Сов. радио, 1969.

6. Барлоу Р., Прошан Ф. Статистическая теория надёжности и испытания на безотказность: Пер. с англ. / Под ред. Б.В. Гнеденко Б.В. М.: Наука, 1969.

7. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

8. Лабути А.Г., Филин Б.П. Об уклонении от NP-полноты в оценках Эзари-Прошана // Автоматика и телемеханика. – 2017 (в печати).

9. Гадасин В.А. Триада субстанций в микромире «Корпускула – Случайность – Волна». Сборник статей ВНИИ ПВТИ, 2005.

10. Гадасин В.А. Аксиоматика концепции триад – трёхмерная группа // Труды XV-й международной конференции «Проблема безопасности сложных систем». М.: ИПУ РАН. 2007. С. 64-70.

11. Половко А.М., Гурович Б.И. : Техническая кибернетика, 1971, № 4, 78 с.

12. Пантелей В.Г., Шубинский И.Б. Расчётные методы оценки надёжности приборов. М.: Машиностроение, 1974. – 55 с.

13. Шубинский И.Б. Топологический метод и алгоритм определения стационарных показателей надёжности технических систем // Надёжность и качество. – 1984. – № 5. – С. 3-10.

14. Шубинский И.Б. Структурная надёжность информационных систем. Методы анализа. М.: Журнал Надёжность, 2012, 295 с.

15. Полесский В.П. Развязывания клаттеров, корреляционные неравенства и границы комбинаторной надёжности // Проблемы передачи информации. 1997. Т. 33. Вып.3. С. 50-70.

16. Носов М.В. Метод полного разложения мостиковых соединений в задачах анализа связности структурно-сложных двухполюсных сетей // Надёжность. 2015. № 4. С. 68-74.

17. Филин Б.П. Методы анализа структурной надёжности сетей связи. М.: Радио и связь, 1988.

18. Филин Б.П. Метод последовательного старта в определении простых сечений (печ.) / Деп. в ЦИВТИ, 07.07.1977г., № Д 2908 Н.

19. Богатырев В.А. К расчету надёжности сетей связи по совокупности путей // Электросвязь. 1981. № 2. С. 42-44.

20. Филин Б.П. О принципе дуальности в задачах анализа структурной надёжности сложных систем // Автоматика и телемеханика. – 1989. – № 6. – С. 158-172.

21. Иваницкая Л.Г. О функциях надёжности устройств релейного действия / Тез. Докладов научно-технической конференции профессорско-преподавательского состава ВЗЭИС под председательством ректора ВЗЭИС д.т.н. проф. Варакина Л.Е. М.: ВЗЭИС. 1967. Вып. 1. С. 111-132.

22. Hansler E. A fast recursive to calculate the reliability of a communication network // IEEE Trans. Commun. 1972. Com-20. № 3. P. 637-642.

23. Богатырев В.А. К расчету надёжности сети по совокупности путей // Электросвязь. –1981. – № 5. – С. 42-44.

24. Рябинин И.А., Черкесов Г.Н. Логико-вероятностные методы исследования надёжности структурно-сложных систем. М.: Радио и связь, 1981.

25. Ушаков И.А., Литвак Е.И. Верхняя и нижняя оценки параметров двухполюсной сети: Пер. с англ. // Изв. АН СССР, Техн. кибернетика, 1977.

26. Handbook of Reliability Engineering / Editor I.A. Ushakov, co-editor R. Harrison. N-Y.: John Wiley and Sons inc., 1994.

27. Филин Б.П. О методе экспресс-оценки и коэффициенте потенциальной структурной неуязвимости связей в сложных системах // Автоматика и телемеханика. – 1994. – № 5. – С. 158-182.

28. Victor A. Netes, Boris P. Filin. Consideration of Node Failures in Network-Reliability Calculation // IEEE Transactions on Reliability. – 1996. – Vol. 49. – № 1. P. 67-68.

29. Филин Б.П., Шапарев А.В. Об одном подходе к расчету вероятности сохранения максимального потока // Автоматика и телемеханика. – 2001. – № 1. – С. 102-117.

30. Басакер Р., Саати Т. Конечные графы и сети. М.: Наука, 1974.

31. Вентцель Е.С. Теория вероятностей. М.: Наука, 1964.

32. Бураченко В.А., Колесников А.Н., Коржик В.И., Финк Л.М. Общая теория связи. Л.: Военная Краснознаменная Академия связи им. Маршала Советского Союза С.М. Будённого, 1970.

33. Давыденко В.П., Лоскутов Н.Г., Иванов Л.Т. Основы военной кибернетики. Л.: Военная Краснознаменная Академия связи им. Маршала Советского Союза С.М. Будённого, 1971.

Сведения об авторах

Александр Г. Лабути, Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», магистрант (1-й курс); ООО «Прогресс», инженер 2-ой категории, e-mail: aglabutin@gmail.com, Россия, Москва

Борис П. Филин, доктор технических наук, e-mail: filinbp41@mail.ru, Россия, Москва

Поступила 24.04.2017

Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий

Сергей М. Климов, 4 ЦНИИ Минобороны России, Россия, Королёв

Сергей В. Поликарпов, 4 ЦНИИ Минобороны России, Россия, Королёв

Андрей В. Федченко, 4 ЦНИИ Минобороны России, Россия, Королёв

Резюме. Цель. Целью статьи является разработка методики, позволяющей комплексно экспериментальным, расчетно-аналитическим и экспертным путем оценить уязвимость сетей спутниковой связи, реализуемость информационно-технических воздействий нарушителя на эти уязвимости и вероятность отказоустойчивости при выбранных вариантах средств защиты информации, доверенных информационных технологий и сенсоров отказоустойчивости. В статье показана актуальность и важность методики для повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий на технологические каналы управления и данные спутникового оборудования. Рассмотрены целенаправленные и массированные информационно-технические воздействия, приводящие к нарушению функционирования спутниковых модемов, управляющих станций и подключенных вычислительных сетей потребителей. Показаны особенности функционирования сетей спутниковой связи, связанные с глобальностью зоны обслуживания потребителей на поверхности Земли, доступностью широкополосных радиосигналов от космических аппаратов связи и ретрансляции для технического анализа и обработки в зоне обслуживания потребителей, потенциальной возможностью несанкционированного подключения к услугам связи. Определены основные перспективные направления развития методического и технологического обеспечения защищенности и отказоустойчивости сетей спутниковой связи. **Методы.** Разработана методика, основанная на трех компонентах: модели экспериментального выявления уязвимостей сетей спутниковой связи; имитационной, расчетно-аналитической модели обнаружения и идентификации угроз информационно-технических воздействий; алгоритме принятия решения по повышению отказоустойчивости сети спутниковой связи в условиях информационно-технических воздействий. Модель экспериментального выявления уязвимостей сетей спутниковой связи позволяет в ходе стендовых испытаний установить взаимосвязь между существующими уязвимостями аппаратно-программного обеспечения спутниковых модемов, управляющих станций, сетей потребителей услуг связи и потенциальными информационно-техническими воздействиями на них нарушителя. В рамках модели уязвимостей описаны паспорта уязвимых радиотехнических и информационных параметров сигналов сетей спутниковой связи, а также предложено аналитическое выражение для расчета вероятности выявления уязвимостей этих сетей. Представлена расчетно-аналитическая модель обнаружения и идентификации угроз информационно-технических воздействий в виде структуры перспективных средств обнаружения, предупреждения и ликвидации последствий информационно-технических воздействий на сеть спутниковой связи и математическое выражение для определения условной вероятности реализации угроз информационно-технических воздействий на сеть спутниковой связи. Рассмотрен алгоритм повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий, включающий подготовку параметров и проведение оценки отказоустойчивости сети спутниковой связи, регулирование параметров сети спутниковой связи и параметров средств защиты информации и сенсоров обеспечения отказоустойчивости, ситуационное регулирование вариантов отказоустойчивых сетей спутниковой связи. **Выводы.** Отмечается, что разработанная методика позволяет повысить отказоустойчивость сети спутниковой связи в условиях информационно-технических воздействий на основе совокупности взаимосвязанных процедур модели экспериментального выявления уязвимостей сети спутниковой связи на стендовом полигоне; имитационной, расчетно-аналитической моделей обнаружения и идентификации угроз информационно-технических воздействий; применения алгоритма принятия решения по повышению отказоустойчивости сети спутниковой связи.

Ключевые слова: сети спутниковой связи, уязвимости, информационно-технические воздействия, повышение отказоустойчивости, средства защиты информации, доверенные информационные технологии и сенсоры отказоустойчивости.

Формат цитирования: Климов С.М., Поликарпов С.В., Федченко А.В. Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий // Надежность. 2017. № 3. С. 32-40. DOI: 10.21683/1729-2646-2017-17-3-32-40.

Введение

В соответствии с Доктриной информационной безопасности Российской Федерации от 5 декабря 2016 года одним из важнейших направлений обеспечения информационной безопасности в области государственной и общественной безопасности является повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления.

К одним из сложнейших и развивающихся объектов современной критической информационной инфраструктуры, для которых необходимо обеспечить повышенные требования к защищенности и устойчивости от информационно-технических воздействий (ИТВ), относятся сети спутниковой связи (ССС). Например, активно развиваются информационно-телекоммуникационные системы на базе сервисов и услуг интерактивных сетей спутникового Интернета для передачи больших массивов данных на базе открытого стандарта DVB-RCS [1].

При разработке современных моделей и методов обеспечения устойчивости (живучести) информационных сетей в условиях разрушающих информационных воздействий [2] особенности взаимосвязанной оценки реальной защищенности и отказоустойчивости СССР могут быть учтены в форме предлагаемой методики повышения отказоустойчивости СССР в условиях ИТВ.

Целенаправленные и массированные ИТВ на протоколы передачи данных являются угрозой для нарушения защищенности и устойчивости функционирования СССР, что обуславливает необходимость разработки методик и средств обнаружения, предупреждения и ликвидации последствий этих информационных угроз на основе повышения отказоустойчивости этих сетей [3, 5].

В настоящее время наиболее опасны ИТВ, которые скрытно проникают, распространяются, вызывают сбои (отказы) и наносят ущерб информационным ресурсам СССР.

Особенностями функционирования СССР, прежде всего, на базе космических аппаратов (КА), находящихся на геостационарной орбите, являются:

- глобальность зоны обслуживания потребителей на поверхности Земли (например, КА «Ямал 401», обслуживающий территорию Российской Федерации в целом и сопредельные территории);
- доступность широкополосных радиосигналов от КА связи и ретрансляции для технического анализа и обработки в зоне обслуживания потребителей;
- потенциальная возможность несанкционированного подключения к услугам связи на расстоянии до 10 тысяч километров между абонентами, как с территории Российской Федерации, так и сопредельных государств;
- сетевая иерархическая инфраструктура СССР с территориально распределенными абонентами, взаимодействующими через разнородные КА связи и ретрансляции и наземные сети по стандартизированным протоколам передачи данных.

В статье используются следующие основные термины:

- уязвимости СССР – программные, архитектурные или логические недостатки в СССР, используя которые возможно получить несанкционированный доступ к защищаемой информации, нарушить ее целостность и доступность, а также вызвать нештатное функционирование СССР;

- информационно-техническое воздействие (компьютерная атака) – целенаправленное воздействие на автоматизированные, информационные и информационно-телекоммуникационные системы программно-техническими средствами, осуществляемое в целях нарушения функционирования и безопасности информации в СССР;

- методика повышения отказоустойчивости СССР – совокупность моделей и алгоритмов анализа, выявления уязвимых мест СССР, обнаружения угроз ИТВ, экспериментальной, расчетно-аналитической и экспертной оценки реальной отказоустойчивости СССР в условиях ИТВ.

Основные перспективные направления развития методического и технологического обеспечения защищенности и отказоустойчивости СССР включают в свой состав разработку:

- имитаторов угроз целенаправленных и массированных ИТВ для проверки СССР;
- методик, алгоритмов и средств обнаружения, предупреждения и ликвидации последствий ИТВ на СССР;
- стендовых полигонов испытаний СССР в условиях ИТВ;
- учебно-тренировочных средств на базе технологий виртуализации, облачных вычислений и сетевых компьютерных игр по противодействию ИТВ на СССР;
- проведение компьютерных учений по отработке действий операторов СССР в условиях чрезвычайных угроз целенаправленных и массированных ИТВ.

Постановка задачи

Предлагаемая в статье методика базируется на взаимосвязанной совокупности экспериментальных оценок реальной отказоустойчивости СССР в условиях имитации ИТВ нарушителя, расчетно-аналитических и экспертных оценок достигаемой отказоустойчивости СССР при выбранных вариантах, доверенных информационных технологий (ДИТ), средств защиты информации (СЗИ) и сенсоров отказоустойчивости (обнаружения, предупреждения и ликвидации последствий ИТВ).

Методика повышения отказоустойчивости СССР состоит из следующих моделей и алгоритма:

1. Модели экспериментального выявления уязвимостей СССР.
2. Имитационной, расчетно-аналитической моделей обнаружения и идентификации угроз ИТВ.
3. Алгоритма принятия решения по повышению отказоустойчивости СССР в условиях ИТВ.

На рисунке 1 приведена схема модели экспериментального выявления уязвимостей СССР. Она представ-

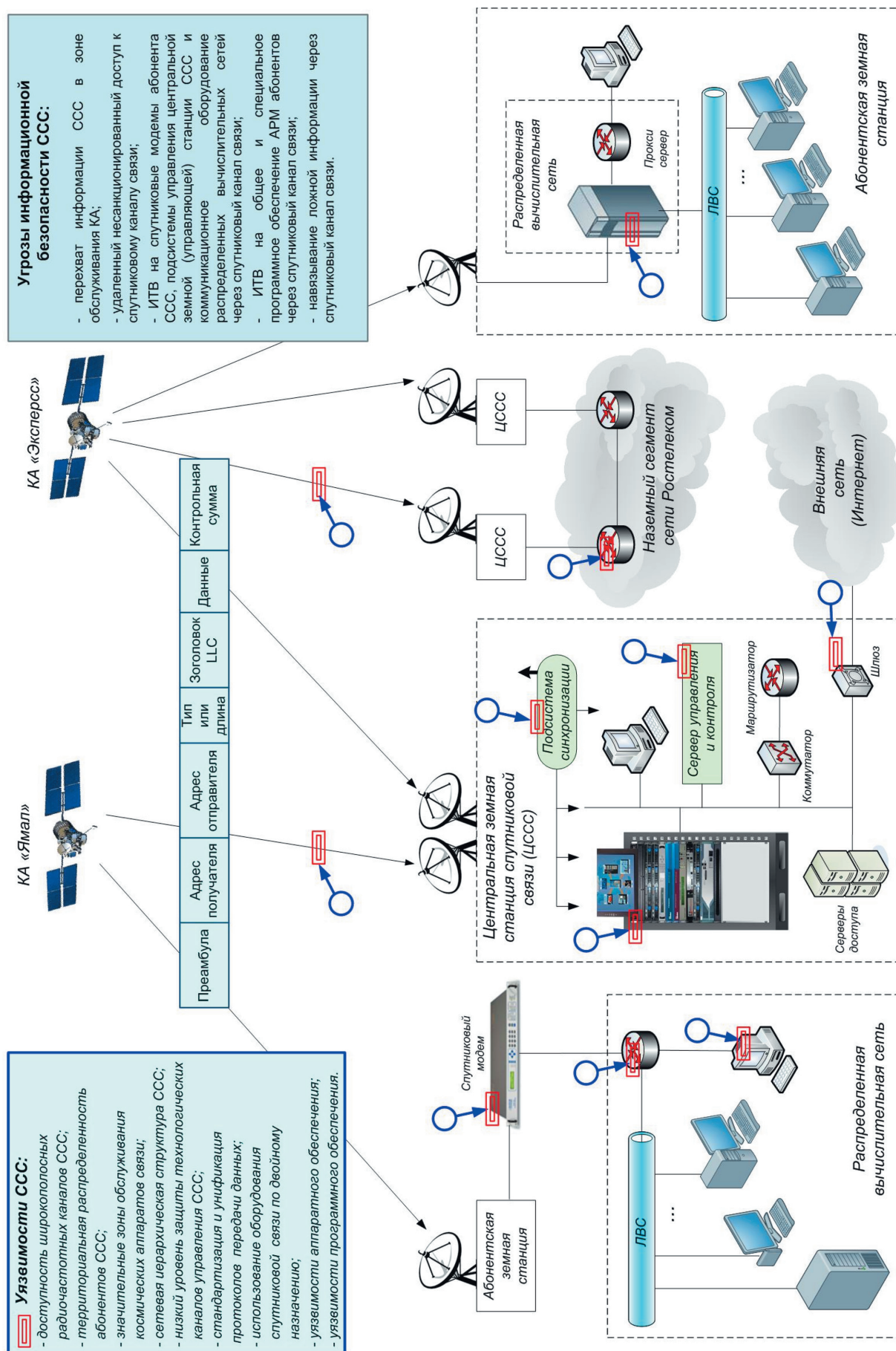


Рисунок 1 – Модель экспериментального выявления уязвимостей ССС

ляет собой типовую критическую информационную инфраструктуру ССС с характерными уязвимостями территориально распределенных объектов, которые взаимодействуют между собой через КА связи и ретрансляции, а также наземные магистральные сети. Уязвимостям ставятся в соответствие потенциальные ИТВ.

Главной уязвимостью являются стандартные и открытые протоколы передачи данных ССС, которые недостаточно защищены в технологических каналах управления и синхронизации. Высокая связность разнородных сегментов нескольких ССС создает возможность несанкционированного доступа к объектам воздействия, не являющихся элементом отдельной ССС.

Экспериментальное выявление уязвимостей ССС осуществляется путем практической проверки (тестирования) доступности протоколов управления и информационного обмена для технического анализа радиотехнических параметров и вскрытия информационных параметров широкополосных сигналов каналов передачи данных в ходе пассивного и активного сканирования.

На схеме двойной, красный прямоугольник обозначает уязвимость, а синяя стрелка с кругом – ИТВ. Рассматриваемая модель экспериментального выявления уязвимостей ССС, позволяет предварительно оценить доступность ССС с используемыми информационными технологиями и СЗИ для потенциальных ИТВ. Экспериментальные исследования проводятся на реальных каналах передачи данных ССС с использо-

ванием частотных ресурсов КА связи и ретрансляции, оборудования имитации спутниковых каналов связи между управляющей станцией и абонентами с учетом особенностей технологического цикла управления, а также с привлечением стендовой базы.

В рамках моделирования комплекс технических и программных средств стендовой базы позволяет проводить технический анализ радиотехнических и информационных параметров ССС, имитировать ИТВ, помеховую обстановку в соответствии с разработанными сценариями и исходными данными. Стенд для экспериментальной оценки защищенности ССС в условиях ИТВ должен содержать антенные системы различных диапазонов частот, приемо-передающие устройства, демодуляторы, программно-алгоритмическое обеспечение, реализующие технологию реальной работы ССС в условиях ИТВ.

В итоге модель обеспечивает формирование перечня выявленных уязвимостей ССС.

Паспорт уязвимых радиотехнических параметров сигналов ССС, доступных для технического анализа нарушителем, представлен в таблице 1.

Аналитическое выражение для расчета вероятности выявления уязвимостей ССС по результатам экспериментальных исследований с использованием [3–5] имеет вид:

$$P_{\text{уяз}}^{\text{ССС}}(t_{\text{ск}}) = P_{\text{НСД}}^{\text{ССС}}(t_{\text{ск}}) + (1 + P_{\text{НСД}}(t_{\text{ск}})) \cdot P_{\text{ПСК}}(t_{\text{ск}}) + (1 - P_{\text{НСД}}(t_{\text{ск}})) \cdot P_{\text{АСК}}(t_{\text{ск}}), \quad (1)$$

где $P_{\text{НСД}}(t_{\text{ск}})$ – вероятность наличия точек несанкционированного доступа в каналах передачи данных между абонентами ССС в направлениях «борт КА – Земля» (обратный уязвимый канал с доступными широкополосными сигналами) и «Земля – борт КА»;

$P_{\text{ПСК}}(t_{\text{ск}})$ – вероятность пассивного сканирования каналов передачи данных между абонентами ССС за время $t_{\text{ск}}$;

$P_{\text{АСК}}(t_{\text{ск}})$ – вероятность активного сканирования каналов передачи данных между абонентами ССС за время $t_{\text{ск}}$.

Паспорт уязвимых информационных параметров каналов передачи данных ССС представим с использованием ГОСТ Р 56546-2015 (таблица 2).

Имитационная, расчетно-аналитическая модели обнаружения и идентификации угроз ИТВ на ССС определяют перечень угроз информационной безопасности ССС, который соответствуют структуре протокола передачи данных между управляющей станцией и абонентским сегментом, а также элементам ССС. Имитационная модель угроз ИТВ позволяет вскрыть уязвимости протоколов, возможные способы реализации угроз ИТВ на них и последствия от нарушения безопасности информации ССС.

Наличие потенциальных уязвимостей и угроз реализации ИТВ на ССС обуславливает возможность несанкционированного подключения к сети и перехвата информации.

Таблица 1 – Пример паспорта уязвимых радиотехнических параметров сигналов ССС

Элементы описания уязвимых радиотехнических параметров	Описание уязвимых радиотехнических параметров ССС
Идентификатор сигнала	алфавитно-цифровая последовательность, идентифицирующая радиочастотный сигнал в базе данных
Наименование космического аппарата связи и ретрансляции	Ямал-401
Орбитальная позиция	90 в.д.
Значение частоты переноса	3050 МГц
Уровень сигнала	-34 дБм
Центральная частота	11245 МГц
Частотная полоса	20 МГц
Вид поляризации	горизонтальная (линейная)
Вид модуляции	QPSK
Тип многостанционного доступа	MF-TDMA
Тип помехоустойчивого кодера	5/6
Тип турбокодера	Рида-Соломона
Скремблирование	не используется
Мультиплексирование	Да

Таблица 2 – Пример паспорта уязвимых информационных параметров ССС

Элементы описания уязвимых информационных параметров ССС	Описание уязвимых информационных параметров ССС
1. Наименование уязвимости	Уязвимость протокола управления спутникового модема
2. Идентификатор уязвимости	УСМ-2017-00002
3. Краткое описание уязвимости	Уязвимость допускает перехват канала управления программным обеспечением спутникового модема
4. Класс уязвимости	Уязвимость программного обеспечения спутникового модема
5. Наименование уязвимого элемента и его версия	Программное обеспечение спутникового модема версии 7.34
6. Протокол передачи данных	Протокол управления telnet, прямой доступ к средствам управления спутникового модема
7. Особенности аппаратной и программной реализации	Аппаратно-программная платформа основана на технологиях клиент-сервер, протокол передачи данных ТСР/IP версии v.4.0
8. Тип недостатка	Недостатки, связанные с аутентификацией администратора
9. Место возникновения (проявления) уязвимости	Уязвимость существует из-за отсутствия проверки легитимности источника команд управления спутниковым модемом
10. Идентификатор типа недостатка	Нет данных
11. Дата выявления уязвимости	1.03.2017
12. Автор, опубликовавший информацию о выявленной уязвимости	Подразделение информационной безопасности
13. Способ (правило) обнаружения уязвимости	Выполнение пошаговой инструкции
14. Критерии опасности уязвимости	Превышение установленного значения вероятности риска
15. Степень опасности уязвимости	Высокая
16. Возможные меры по устранению уязвимости	Доработка средств защиты информации и протоколов управления спутниковым модемом
17. Дополнительные сведения	В сети используется спутниковые модемы, допускающие удаленную перезагрузку программного обеспечения через ССС

Схема модели обнаружения и идентификации угроз ИТВ на ССС создается в форме структуры оперативного реагирования на ИТВ и повышения отказоустойчивости, состоит из трех контуров (рисунок 2):

- первый – ДИТ ССС;
- второй – управления защитой информации и повышением отказоустойчивости на основе информации от сенсоров средств обнаружения и идентификации ИТВ;
- третий – оповещения о нарушении информационной безопасности по типовой форме описания компьютерных инцидентов.

Элементы ДИТ ССС представляют собой защищенные аппаратно-программные платформы, включающие операционные системы (ОС), системы управления базами данных (СУБД), трансляторы с языков программирования высокого уровня и другое общее программное обеспечение. Аппаратная составляющая ДИТ ССС включает защищенные процессоры, модули памяти, интерфейсные шины, спутниковые модемы, управляющие станции, доверенное коммуникационное оборудование наземных распределенных сетей, которые в совокупности должны позволить сформировать неуязвимое спутниковое и коммуникационное оборудование в условиях ИТВ.

В модели обнаружения и идентификации угроз ИТВ, с одной стороны, к средствам защиты информации (СЗИ) относятся известные СЗИ, такие как автоматизированные модули доверенной загрузки (АМДЗ), межсетевые экраны (МЭ), ложные сетевые информационные

объекты (ЛСИО), а с другой стороны – совокупность сенсоров, которые реализуют функции обнаружения, предупреждения и ликвидации последствий ИТВ. Для повышения отказоустойчивости ССС в условиях ИТВ совокупность сенсоров регистрируют и идентифицируют факты воздействий и формируют исходные данные для восстановления работоспособности ССС.

Элементы СЗИ ССС целесообразно реализовать на основе аппаратно-программных средств пункта мониторинга ИТВ и управления защитой информации.

В рамках повышения отказоустойчивости ССС анализируются потенциальные угрозы нарушения защищенности и отказоустойчивости ССС, потенциальные объекты поражения, ДИТ ССС, комплекс СЗИ и необходимый стендовый полигон испытаний ССС в условиях ИТВ.

Особенности повышения отказоустойчивости ССС в условиях ИТВ состоят в том, что требуемый ее уровень необходимо обеспечить в течение длительного периода эксплуатации при совершенствующихся угрозах нарушителей, в технологических трактах систем управления с различными протоколами передачи данных.

Порядок обнаружения и идентификации угроз ИТВ на ССС следующий:

1. Устанавливается сервер обнаружения ИТВ на центральной управляющей (земной) станции, размещаются сенсоры отказоустойчивости на подключенных абонентских управляющих станциях (терминалах) и осуществляется мониторинг защищенности ССС.

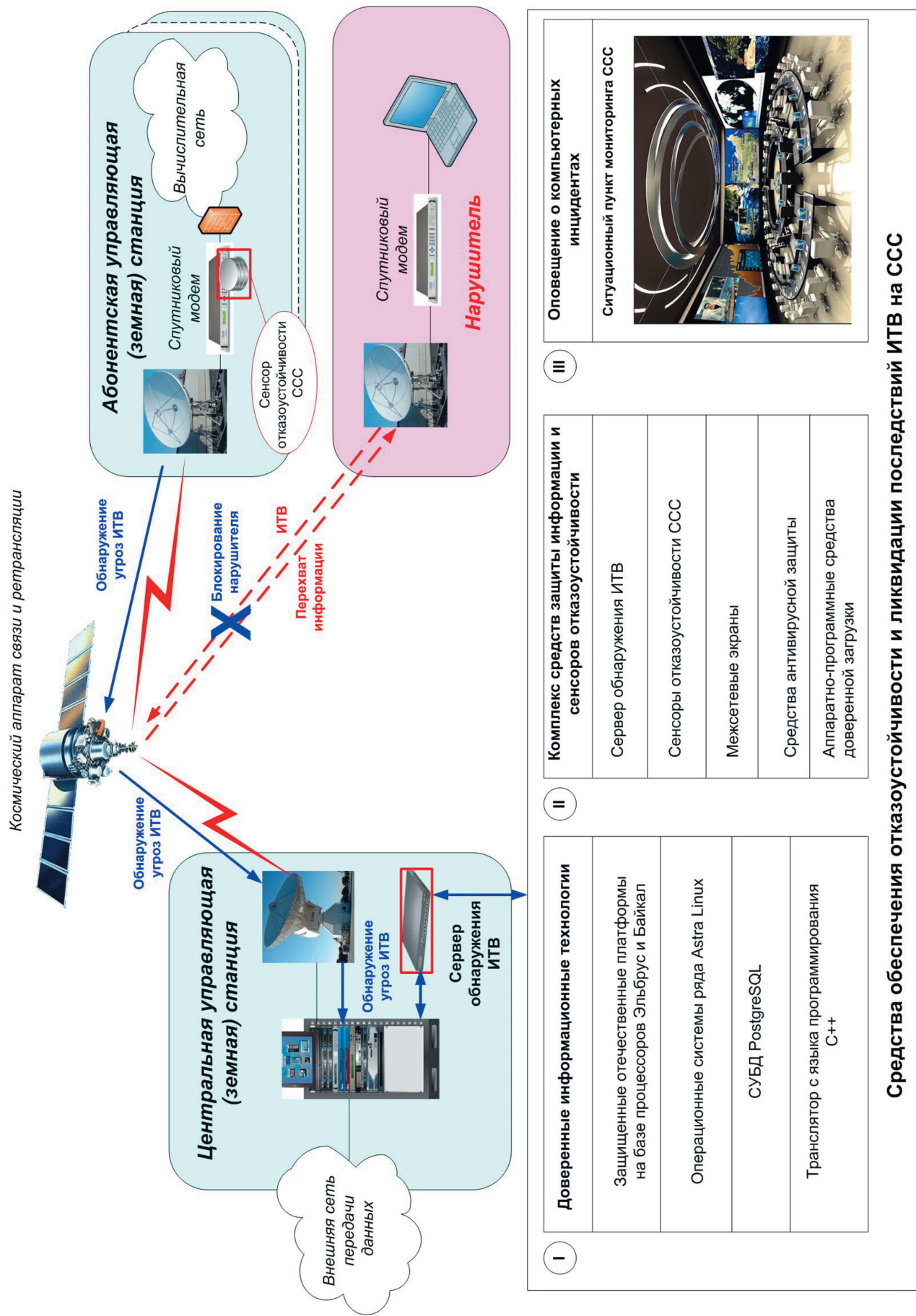


Рисунок 2 – Схема модели обнаружения и идентификации угроз ИТВ

2. Производится первоначальное извещение о появлении незарегистрированного абонента в случае несанкционированного подключения нарушителя к ССС с активным использованием нештатного спутникового модема.

3. Осуществляется извещение о компьютерном инциденте при реализации ИТВ на абонентов и управляющую станцию ССС сенсорами отказоустойчивости на основе использования встроенных сигнатурных и эвристических методов.

4. Выполняется анализ целенаправленных и массированных ИТВ, идентификация их типа и обновление баз данных сигнатур ИТВ.

5. Принимаются решения о ликвидации последствий ИТВ путем блокирования спутникового модема нарушителя на основе контроля параметров прямого и обратного спутниковых каналов, информации от сенсоров отказоустойчивости.

Мониторинг защищенности ССС с целью обнаружения и идентификации ИТВ осуществляется следующими проверочными мероприятиями:

- контроль радиотехнических параметров;
- контроль каналов управления ССС;
- контроль параметров подключения и функционирования абонентов ССС;
- контроль информационных потоков в ССС;
- обнаружение открытых каналов управления и передачи данных;
- обнаружение ИТВ в прямом и обратном каналах ССС;
- локализация нарушителя (идентификация источника ИТВ и определение предполагаемого местоположения);
- блокирование нарушителя (отключение от ССС);
- технический анализ и выявление уязвимостей ССС;
- контроль параметров функционирования спутникового оборудования центральной и абонентских станций, коммуникационного оборудования, аппаратно-программного обеспечения, средств защиты информации и повышения отказоустойчивости.

Расчетно-аналитическая модель основана на математическом выражении для определения условной вероятности реализации угроз ИТВ на ССС (с использованием [3–5]):

$$P(S_p/Y_{ИТВ}) = \frac{P(S_{pi}) \cdot P(Y_{ИТВ_i}/S_{pi})}{P(S_{pj}) \cdot P(Y_{ИТВ_i}/S_{pj}) + P(S_{hk}) \cdot P(Y_{ИТВ_i}/S_{hk})}, \quad (2)$$

где $P(S_p)$ – вероятность нахождения ССС в работоспособном состоянии в условиях ИТВ;

$P(Y_{ИТВ_i}/S_{pj})$ – условная вероятность реализации i -й угрозы ИТВ на j -й работоспособный элемент ССС;

$P(S_{hk})$ – вероятность нахождения k -го элемента ССС в неработоспособном состоянии при реализации ИТВ;

$P(Y_{ИТВ_i}/S_{hk})$ – условная вероятность реализации i -й угрозы ИТВ на k -й элемент ССС, приводящей к нарушению его отказоустойчивости.

На рисунке 3 представлен алгоритм повышения отказоустойчивости ССС в условиях ИТВ.

Алгоритм обеспечения отказоустойчивости ССС основан на совокупности экспериментальных, расчетно-аналитических и экспертных оценках параметров ССС в условиях ИТВ для выбора вариантов отказоустойчивых ССС путем их ситуационного регулирования.

Сущность алгоритма обеспечения отказоустойчивости ССС в условиях ИТВ заключается в реализации пяти этапов:

1. Подготовка параметров (исходных данных) для оценки отказоустойчивости ССС в условиях ИТВ.
2. Проведение оценки реальной защищенности ИТВ.
3. Регулирование параметров ССС.
4. Регулирование параметров СЗИ и средств обеспечения отказоустойчивости.
5. Ситуационное регулирование вариантов отказоустойчивых ССС.

Алгоритм обеспечения отказоустойчивости ССС в условиях ИТВ, по сути, определяет схему поэтапного управления отказоустойчивостью сети, выбора наименее уязвимого и наиболее защищенного варианта ССС с возможностью ликвидации последствий ИТВ.

Технологический цикл управления (ТЦУ) ССС характеризуется реальным масштабом времени, динамически изменяющимися условиями ИТВ, использованием значительного числа ДИТ, что требует ситуационного регулирования параметров отказоустойчивости ССС адекватно складывающейся обстановке.

Предполагается, что в начальной стадии работы алгоритма существует неопределенность исходных данных об ИТВ, уязвимостях ССС, ДИТ, СЗИ и сенсорах отказоустойчивости, что обуславливает необходимость проведения экспериментальных и аналитических исследований по обеспечению отказоустойчивости ССС в условиях ИТВ.

Применение алгоритма предполагается как на этапах проектирования и разработки ССС в защищенном исполнении, так и регулирования параметров и средств обеспечения отказоустойчивости ССС в условиях эксплуатации.

Выполнение этапов алгоритма по управлению отказоустойчивостью ССС в условиях ИТВ позволяет осуществить:

- подготовку входных данных и учет факторов для оценки отказоустойчивости ССС в условиях ИТВ;
- имитационное моделирование реальных процессов функционирования ССС на стендовом полигоне;
- инструментальный контроль потенциальных возможностей нарушителя по проведению пассивного и активного сканирования уязвимостей ССС;
- регулирование параметров ССС, СЗИ, ДИТ и сенсоров отказоустойчивости по результатам расчетно-аналитических и экспертных оценок;
- ситуационное регулирование вариантов отказоустойчивых ССС при динамически изменяющихся ИТВ на основе устранения уязвимостей в аппаратно-программных средствах, выбора вариантов отказоустойчивых элементов ССС, СЗИ и сенсоров отказоустойчивости;

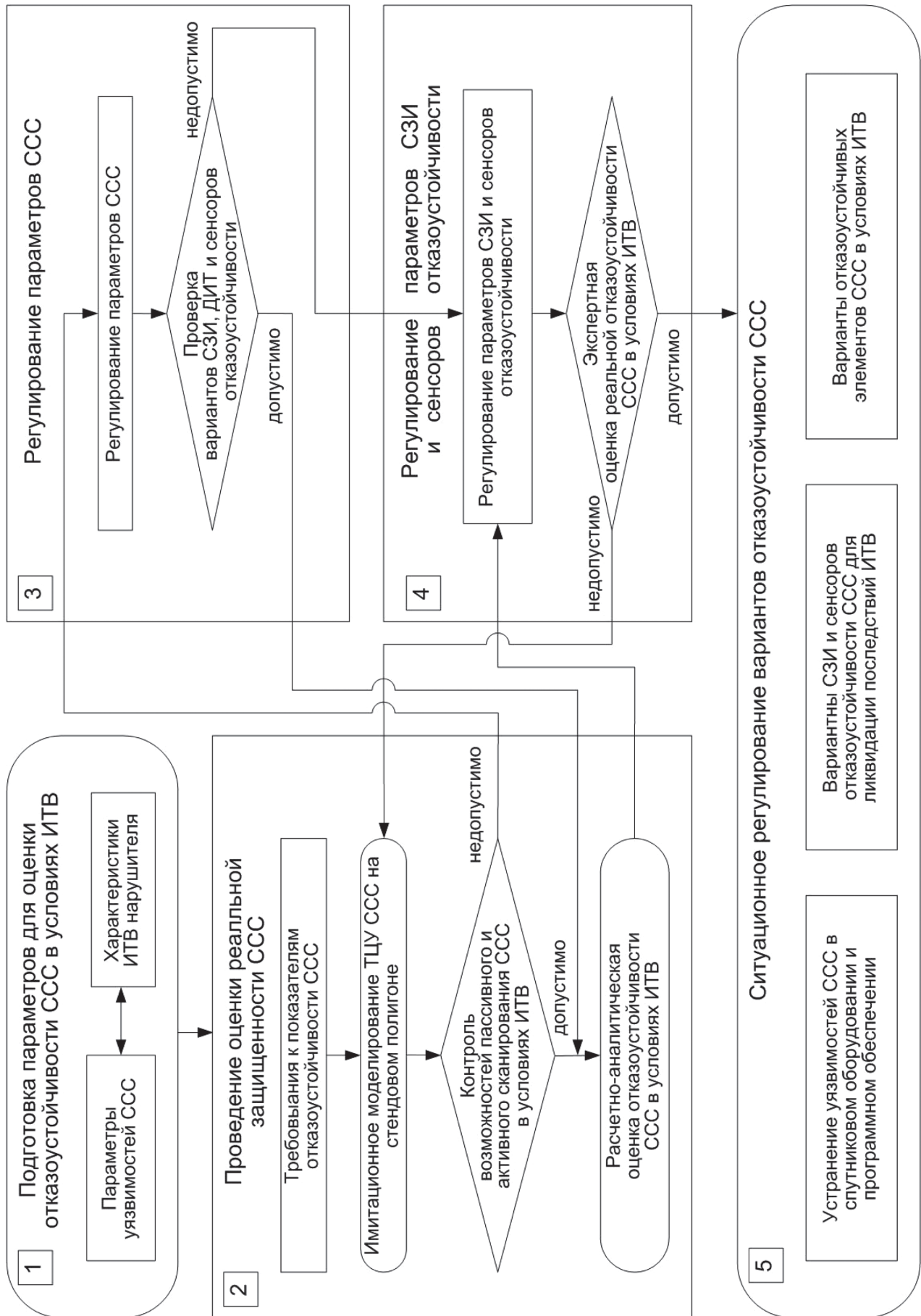


Рисунок 3 – Алгоритм обеспечения отказоустойчивости ССС в условиях ИТВ

- выбор моделей ССС, ИТВ, СЗИ, ДИТ, сенсоров отказоустойчивости для определения мер по повышению (обеспечению) функциональной устойчивости ССС;

- комплексную экспериментальную, расчетную и экспертную оценку отказоустойчивости ССС в условиях ИТВ;

- подготовку к ликвидации последствий ИТВ на ССС;
- эффективное управление отказоустойчивостью ССС в условиях неопределенности ИТВ и внесения различных замедлений в процесс выполнения ТЦУ по предоставлению услуг спутниковой связи и передачи данных;

- оценку выполнения предъявляемых требований к показателям отказоустойчивости ССС в условиях ИТВ и выдать практические рекомендации по ее обеспечению.

Множество различных параметров ССС, СЗИ, ДИТ, сенсоров отказоустойчивости и факторов ИТВ приводит к множеству возможных текущих состояний отказоустойчивости ССС. Количество вариантов регулирования (управляющих решений) по повышению отказоустойчивости ССС на практике ограничено. В этих условиях рассмотренный алгоритм на основе ситуационного регулирования вариантов отказоустойчивости ССС позволяет обеспечить выполнение требований к отказоустойчивости ССС.

Под ситуацией понимается совокупность уязвимостей и состояний ССС, СЗИ, ДИТ и сенсоров отказоустойчивости на определенный момент функционирования для определения необходимости вмешательства в процесс управления ССС.

При выполнении процедур контроля, проверки и экспертной оценки параметров отказоустойчивости ССС в условиях ИТВ, предполагается, что с использованием базы данных испытаний стендового полигона в ходе принятия решений на этапах выполнения алгоритма устанавливаются факты допустимого и недопустимого отклонения параметров текущего состояния ССС от требуемого значения.

Интервал регулирования состояния отказоустойчивости ССС выбирается исходя из значимости абонентов и узлов (управляющих станций) ССС и наиболее вероятной реализацией ИТВ.

Если состояние ССС в условиях ИТВ требует ситуационного регулирования, то ее описание классифицируется на основе паспортов радиотехнических и информационных параметров ССС, профиля нормального поведения и результатов расследования компьютерных инцидентов. Каждое текущее состояние ССС в условиях ИТВ можно отнести к определенному классу, которому соответствует некоторое множество регулируемых параметров ССС.

Ситуационное регулирование отказоустойчивости ССС характеризуется следующей последовательностью: описание состояния ССС в условиях ИТВ – подготовки регулируемых параметров ССС, СЗИ, ДИТ, сенсоров отказоустойчивости – реализация управляющих воздействий по противодействию ИТВ и восстановлению работоспособности (переходу на резервные сегменты) ССС.

Расчетное соотношение для вероятности отказоустойчивости ССС в условиях ИТВ с использованием [3–5] имеет вид:

$$P_{\text{отк}}(t) = \prod_{i=1}^k \left[1 - \left(1 - \prod_{j=1}^r P_{\text{БОТ}i}(S_{pj}) \right) \right], \quad (3)$$

где $P_{\text{БОТ}i}(S_{pj})$ – вероятность безотказной работы j -го элемент ССС при i -й угрозе ИТВ;

k – общее количество элементов СЗИ (сенсоров), размещенных в ССС;

r – общее количество резервных элементов ССС.

Заключение

На базе системного анализа потенциальных уязвимостей и особенностей функционирования ССС в статье предложена методика повышения отказоустойчивости ССС в условиях возможных ИТВ. Методика основана на совокупности взаимосвязанных процедур модели экспериментального выявления уязвимостей ССС на стендовом полигоне, формирования имитационной, расчетно-аналитической моделей обнаружения и идентификации угроз ИТВ и применения алгоритма принятия решения по повышению отказоустойчивости ССС в условиях ИТВ.

Библиографический список

1. Воронин А.В, Иванов В.Н., Сотов А.М, Цифровое телевизионное вещание/ Под редакцией доктора технических наук, профессора А.М. Сомова – М.: Горячая линия – Телеком, 2017. – 240 с.: ил. – Серия «Цифровое телевизионное и радиовещание. Выпуск 1».
2. Величко В.В., Попков Г.В., Попков В.К. Модели и методы повышения живучести современных систем связи. – М.: Горячая линия – Телеком, 2016. – 270 с.: ил.
3. Климов С.М., Астрахов А.В., Сычев М.П. Экспериментальная оценка противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 116 с, 2013.
4. К. Капур, Л. Ламберсон. Надежность и проектирование систем. Под ред. И.А. Ушакова. Пер. с англ. – М.: «Мир», 1980. – 604 с., ил.
5. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза/ И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2016. – 544 с., ил. – («Журнал надежность»).

Сведения об авторах

Сергей М. Климов – доктор технических наук, профессор, начальник управления 4 ЦНИИ Минобороны России. Россия, Королёв, тел. +7 (985)928-13-55, e-mail: klimov.serg2012@yandex.ru.

Сергей В. Поликарпов – заместитель начальника отдела 4 ЦНИИ Минобороны России. Россия, Королёв, тел. +7 (916)332-60-66, e-mail: polikarpov.s.v@yandex.ru.

Андрей В. Федченко – начальник отдела 4 ЦНИИ Минобороны России. Россия, Королёв, тел. +7 (916)334-87-89, e-mail: fedchandr@yandex.ru

Поступила 15.05.2017

Метод восстановления вектора приоритетов альтернатив в условиях неопределенности или неполноты экспертных оценок

Александр В. Бочков, Научно-исследовательский институт экономики и организации управления в газовой промышленности, Москва, Россия

Николай Н. Жигирев, Научно-исследовательский институт экономики и организации управления в газовой промышленности, Москва, Россия

Александра Н. Ридли, аспирант МАИ (НИУ), Москва, Россия

Резюме. Цель. Одной из наиболее популярных процедур принятия решений за счёт своей эффективности, гибкости и простоты является т.н. метод попарных сравнений. Основным недостатком этого метода при проведении экспертиз большого количества альтернатив или в довольно широкой области знаний является невозможность сравнения каждого элемента с каждым, как по причине большого количества таких сравнений, случайных пропусков, так и по причине затруднений у эксперта при сравнении некоторых альтернатив. В оценках возникают пропущенные данные, затрудняющие принятие решения, т.к. большинство статистических методов не применимо к неполному набору данных. Не может работать с матрицей, содержащей преимущественно нулевые элементы и достаточно популярный алгоритм обработки матриц попарных сравнений (алгоритм Саати). Цель статьи заключается в разработке метода обработки неполных матриц сравнений с целью получения весовых коэффициентов (весов) рассматриваемых альтернатив, позволяющих количественно сравнить их между собой. **Методы.** На практике встречается несколько подходов к работе с массивами данных, содержащих пропущенные значения. Первый подход, наиболее простой в реализации, – это удаление экземпляров, содержащих пропущенные значения, из массива и работа только с полными данными. Использование данного подхода целесообразно, если пропуски данных носят единичный характер. Но даже в этом случае имеется серьезная опасность при удалении данных «потерять» важные закономерности. Вторым подходом является использование специальных модификаций методов обработки данных, допускающих наличие пропусков в массиве. И, наконец, используют различные методы оценки значений пропущенных элементов. Данные методы помогают заполнить пропуски в массивах, основываясь на некоторых предположениях о значении отсутствующих данных. Принципиальная применимость и эффективность того или иного подхода зависит от количества пропусков в данных и причин, по которым они образовались. В статье матрица попарных сравнений рассматривается в формате нагруженного графа, причём альтернативы являются вершинами, а сравнения между ними – рёбрами графа. Соответственно, если возникает пара альтернатив, для которой эксперт не смог задать предпочтение, то соответствующее ей ребро отсутствует. Рассмотрен способ удаления рёбер, соответствующих наиболее противоречивым оценкам, т.е. алгоритм разрыва циклов, приводящий к преобразованию исходного графа к остовному дереву, позволяющему однозначно сравнить любые две альтернативы. Алгоритм совместного согласования и верхних, и нижних границ экспертных оценок в данной статье не рассматривается. **Результаты.** В статье приведён пример практического применения разработанного алгоритма для обработки неполной матрицы попарных сравнений десяти объектов, полученной в ходе некоторой экспертизы. Показана работоспособность предложенного подхода к задачам восстановления приоритетов сравнимых альтернатив, намечены пути автоматизации расчётов и направления дальнейших исследований. **Выводы.** Предложенный метод может быть применён для широкого круга задач анализа и количественной оценки рисков, управления безопасностью сложных систем и объектов, а также задач, связанных с контролем выполнения требований к таким высоконадежным элементам, как элементы ядерных реакторов, авиационной и ракетно-космической техники, газового оборудования и т.п., т.е. там, где требуется оценивать малые (менее 0,01) вероятности отказа на заданную наработку, а статистика отказов таких элементов в эксплуатации практически отсутствует. Предложенный алгоритм может найти применение при экспертной оценке для установления вида и параметров распределения наработки на отказ таких высоконадежных элементов, что в свою очередь позволит оценивать с приемлемой точностью показатели надёжности.

Ключевые слова: пропущенные данные, экспертиза, нагруженный граф, остовное дерево, матрица попарных сравнений, критерий связности.

Формат цитирования: Бочков А.В., Жигирев Н.Н., Ридли А.Н. Метод восстановления вектора приоритетов альтернатив в условиях неопределенности или неполноты экспертных оценок // Надежность. 2017. Т. 17, № 3. С. 41-48. DOI: 10.21683/1729-2646-2017-17-3-41-48

Введение

Процедуры принятия решений, в которых экспертам предлагается выбрать наилучший вариант(ы) из допустимого множества, достаточно часто используются в самых различных областях для проведения оценки, отбора и определения приоритетности целей и т.п. Очевидно, что сравнение различных альтернатив в соответствии с их предпочтительностью в задачах принятия решений, во многих случаях, не может быть выполнено с помощью одного критерия или одного эксперта. Как следствие, в большинстве задач принятия решений, существуют процедуры, позволяющие объединять мнения разных экспертов по поводу предлагаемых им альтернатив [1, 2]. Чаще всего эти процедуры используют т.н. метод попарных сравнений, предполагающих, что эксперт может выставить предпочтение одной альтернативы над другой при их сравнении.

Поскольку каждый эксперт имеет отличный от других опыт решения подобных задач, мнения различных экспертов могут существенно отличаться (действительно, существует множество факторов, которые влияют на предпочтения эксперта). Такое разнообразие экспертных оценок может привести к ситуациям, когда некоторые из них не смогут эффективно выразить любые степени предпочтения, сравнивая две или более доступных альтернатив. Это может быть следствием недостаточного уровня компетентности эксперта в какой-то области знаний, касающейся решаемой проблемы, или потому, что эксперт не в состоянии однозначно определить степень предпочтения некоторых из предложенных ему для сравнения вариантов над другими. В таких ситуациях такой эксперт вынужден обеспечить неполное нечеткое отношение предпочтения [3] или отказаться от оценивания предложенной пары альтернатив. Возникает нетривиальная задача восстановления пропущенных данных для получения приемлемого результата экспертизы.

На практике встречается несколько подходов к работе с массивами данных, содержащих пропущенные значения. Первый подход, наиболее простой в реализации, – это удаление экземпляров, содержащих пропущенные значения, из массива и работа только с полными данными [4]. Использование данного подхода выглядит целесообразным, если пропуски данных носят единичный характер. Но даже в этом случае имеется серьезная опасность при удалении данных «потерять» важные закономерности. В том же случае, когда количество пропусков велико, удаление соответствующих экземпляров может привести к дефициту данных и даже невозможности дальнейшей обработки. Вторым подходом является использование специальных модификаций методов обработки данных, допускающих наличие пропусков в массиве. В исследовании [5] приведен ряд модификаций методов классификации и кластеризации для работы с данными, содержащими пропущенные значения. И, наконец, третьим подходом, наиболее распространенным, является использование методов оценки значений про-

пущенных элементов. Данные методы помогают заполнить пропуски в массивах, основываясь на некоторых предположениях о значении отсутствующих данных. Принципиальная применимость и эффективность того или иного подхода зависит от количества пропусков в данных и причин, по которым они образовались. С точки зрения природы возникновения данных традиционно выделяют категории пропусков [6].

Довольно часто в эмпирических исследованиях приходится отвергать результаты экспертных опросов, когда отсутствуют некоторые данные [7].

В работе [8] исследовано влияние приведенных наборов попарных сравнений. Сравнивались результаты, полученные для полной матрицы попарного сравнения и неполной, полученной путём исключения известных элементов полной. Результат исследования [8] показал, что «случайное удаление до 50% от сравнений дает хорошие результаты без потери точности». Тем не менее, поскольку этот процесс опирается на априорное знание полной матрицы попарного сравнения, поэтому неприменим в реальной практике. Поэтому в [8] предложено при наличии неполной матрицы попарных сравнений использовать методы, позволяющие «достроить» матрицу до полной. Сильный аргумент в пользу этого подхода дан в [9]: «сценарий с пропущенными значениями, как правило, нарушает рейтинг более сильно, чем тот же сценарий со значением при условии». Система, которая помогает построить нечёткие отношения предпочтений в решении была предложена в [10]. В группе принятия решений, процедур, исправляющих отсутствие знаний конкретного эксперта, используя информацию, предоставленную остальными экспертами, вместе с некоторыми процедурами агрегации, можно найти в работах [11] и [12]. Эти подходы имеют ряд недостатков, некоторые из которых отмечают авторы [13].

В отечественной литературе также есть работы, связанные с поиском ответов на обозначенные нами проблемы, например, [14], однако используемые ими подходы не дают однозначного решения.

1. Постановка задачи

В классической постановке Саати [15] мы имеем некоторую совокупность объектов $O_1, O_2, \dots, O_M$ (возможных действий, параметров, альтернатив решений и т.п.) некоторой иерархии. Количественные суждения эксперта о паре объектов (O_i, O_j) представляются матрицей размера $n \times n$: $A = (a_{ij})$, $(i, j = 1, 2, \dots, n)$, причём числа a_{ij} , из которых состоит матрица, соответствуют значимости объекта O_i по сравнению с O_j и неотрицательны. Для выявления количественных показателей относительной значимости сравниваемых объектов, в методе предложена шкала относительных сравнений, выраженная в целых числах от 1 до 9. При этом объекты, имеющие одинаковую важность, получают оценку «1». Также «1» равны оценки, стоящие на главной диагонали матрицы (объекты сравниваются сами с собой), т.е. $a_{ii} = 1$. Матрица

Саати обратно-симметрична относительно главной диагонали, т.е. $a_{ij}=1/a_{ji}$.

Далее в [15], после построения количественных суждений о парах (O_i, O_j) в числовом выражении через a_{ij} задача сводится к тому, чтобы поставить в соответствие каждому из сравниваемых объектов числовые веса, которые в наилучшей степени соответствовали бы зафиксированным суждениям экспертов. Для нахождения вектора приоритетов необходимо найти вектор ω , который удовлетворяет $A\omega=\lambda_{\max}\omega$. Согласно теореме о существовании и единственности при решении задачи о собственном значении для неотрицательной матрицы по [15, 16] находят главный собственный вектор, который после нормализации и становится вектором приоритетов сравниваемых объектов.

Мы ищем решение для случая, когда в матрице A некоторые оценки не определены, т.е. $\exists a_{ij}; a_{ji}=NA$ (здесь NA – англ., Not Available).

2. Описание метода

Матрица попарных неполных сравнений $\bar{A}$ легко преобразуется в кососимметричную матрицу $\bar{A}$ путём логарифмирования элементов матрицы коэффициентов.

Веса W_i преобразуются в $V_i=\ln(W_i)$, матрица коэффициентов попарных сравнений $\bar{S}_{ij}=\ln(S_{ij})$, а матрица

невязки $F_{ij}=\left(\frac{S_{ij}\times W_j}{W_i}-1\right)$ – в матрицу функционалов $\bar{F}_{ij}=(\bar{S}_{ij}+V_j-V_i)$ приобретает кососимметричный вид.

$$W_i, S_{ij}, F_{ij}=\left(\frac{S_{ij}\times W_j}{W_i}-1\right)\rightarrow V_i=\ln(W_i),$$

$$\bar{S}_{ij}=\ln(S_{ij}), \bar{F}_{ij}=(\bar{S}_{ij}+V_j-V_i) \quad (1)$$

Определив величины V_i , проводим обратное преобразование:

$$V_i\rightarrow W_i=\frac{\exp(V_i)}{\sum_{j=1}^N \exp(V_j)} \quad (2)$$

для того чтобы удовлетворить условию нормировки весов Саати, т.е.

$$\sum_{i=1}^N W_i=1, W_i>0 (i=1, \dots, N).$$

Можно провести диагонализацию матрицы, чтобы она приобрела положительный вид над основной диагональю. Однако, следует отметить, что такая диагонализация не всегда возможна даже в случае одного эксперта, и, впрочем, необязательна – важна только связность графа матрицы. Для группы же экспертов диагонализация необходима, так как в зависимости от порядка вершин происходит перестановка верхних и нижних оценок. Предполагается, что для группы экспертов полное согласие не достижимо, а их коэффициенты предпочтения $\bar{S}_{ij}$ находятся в некотором диапазоне:

$$B_{ij}\leq \bar{S}_{ij}\leq T_{ij} \quad (3)$$

Нижняя граница B_{ij} (англ., Bottom) соответствуют минимальному значению, а верхняя граница T_{ij} (англ., Top) – максимальному. В данной статье мы рассматриваем реализацию алгоритма для верхних оценок T_{ij} или одного эксперта $\bar{S}_{i,j}$.

В силу особенностей матрицы T_{ij} начальное значение весов может быть произвольной постоянной величиной, чтобы не путаться в знаках приращений весов. Величина изменений зависит от типа строки-столбца. Тип равен «-1», когда в j -ой строке матрицы $(E_1-\dots-N_1;\dots;E_n-\dots-N_n)$ выше основной диагонали присутствуют только неопределенные значения (NA). Тип равен «1», когда в i -ом столбце матрицы $(E_1-\dots-N_1;\dots;E_n-\dots-N_n)$ выше основной диагонали присутствуют только неопределенные значения (NA). В тех случаях, когда реальные данные присутствуют и в j -ой строке, и в i -ом столбце, очевидно, что тип первого объекта всегда равен «1», а тип последнего объекта равен «-1».

Первоначально матрица $\|\bar{F}_{ij}\|$ равна матрице $\|\bar{S}_{ij}\|$. Произвольный выбор весов вызван тем фактом, что результат не зависит от выбора начального приближения

$$\bar{F}_{ij}=(\bar{S}_{ij}+[V_j+const]-[V_i+const])=(\bar{S}_{ij}+[V_j]-[V_i]). \quad (4)$$

Первый важный этап: поиск самого жёсткого противоречия. Для всех строк ищется оптимальное смещение весов за счёт оптимизации веса V_i , которое затрагивает и j -ую строку и i -ый столбец. Выбираем строки по убыванию $(i=N, \dots, 1)$ до тех пор, пока все смещения не обратятся в нуль¹.

Далее, принимаем

$$|\Delta V_i|\leq \varepsilon C=1,0e^{-7}. \quad (5)$$

Изменение весов происходит шаг за шагом по закономерностям

$$V_i=V_i+\Delta V_i. \quad (6)$$

После выполнения очередного шага ΔV_i обращается в ноль.

Величина ΔV_i выбирается по алгоритму, в основе которого лежит оптимизация модуля значений в матрице $\|\bar{F}_{ij}\|$, но только в той части, которая касается i -го шага (i -строки).

Мы минимизируем максимум из модулей следующих величин

$$\max_{\square}\{|R_{\max}^i-\Delta^i|, |R_{\min}^i-\Delta^i|, |C_{\max}^i+\Delta^i|, |C_{\min}^i+\Delta^i|\}\rightarrow \min_{\Delta} \square \quad (7)$$

для всех $i=1, \dots, N$, где N – размерность задачи; $R_{\max}^i$ – максимальное значение над диагональю в i -ой строке; $R_{\min}^i$ – минимальное значение над диагональю в i -ой

¹ Например, для матрицы размерности 10 потребуется порядка 15 итераций.

Таблица 1

Тип	Условие	Формула расчёта
0	Есть элементы в строке и есть элементы в примыкающем столбце	
	если $R_{\max} > \max\{ R_{\min} , C_{\min} , C_{\max}\}$, то	$\Delta^{(I)} = \frac{1}{2} \cdot \min\{R_{\max} + R_{\min}; R_{\max} - C_{\max}\}$
	если $C_{\max} > \max\{ R_{\min} , C_{\min} , R_{\max}\}$, то	$\Delta^{(II)} = \frac{1}{2} \cdot \min\{-C_{\max} - C_{\min}; R_{\max} - C_{\max}\}$
	если $-R_{\max} > \max\{ C_{\min} , C_{\max}, R_{\max}\}$, то	$\Delta^{(III)} = \frac{1}{2} \cdot \min\{R_{\max} + R_{\min}; R_{\min} - C_{\min}\}$
	если $-C_{\max} > \max\{ R_{\min} , C_{\max}, R_{\max}\}$, то	$\Delta^{(IV)} = \frac{1}{2} \cdot \min\{-C_{\max} - C_{\min}; R_{\min} - C_{\min}\}$
	в других случаях	$\Delta^{(V)} = 0$
1	Все компоненты столбца равны NA	$\Delta V_i = \frac{(R_{\max}^i + R_{\min}^i)}{2}$
-1	Все компоненты строки равны NA	$\Delta V_i = \frac{-(C_{\max}^i + C_{\min}^i)}{2}$

строке; $C_{\max}^i$ – максимальное значение над диагональю в i -ом столбце; $C_{\min}^i$ – минимальное значение над диагональю в i -ом столбце.

Изменённый вес рассчитывается по формулам:

$$W^i = W^i + \Delta^i. \quad (8)$$

Соответствующие решения для любой строки определяются по формулам, приведённым в таблице 1.

Следующий шаг: удаление ячеек. Если это допустимо по критерию связности¹, удаляется первое по порядку ребро принадлежащее правому концу «поплавка» напротив которого в строке имеется ребро из «левого» конца «поплавка», когда ребро (i, j) является единственным ребром, соединяющим непересекающиеся подмножества вершин (объектов).

После удаления ребра решение возобновляется с начальных условий.

Стоит отметить, что важно следить за возможным изменением типа «строки-столбца». Обычно изменения происходят в сторону от «0» до «1», то есть тогда, когда исчезает последний значимый элемент в соответствующем столбце.

Следующий этап: процедура, состоящая из двух вложенных циклов. Внешний цикл – поиск очередного «предельного цикла» в оставшейся матрице. Внутренний цикл – поиск рёбер, составляющих «предельный цикл».

Окончанием внешнего цикла является условие:

$$\|sup\|F_{ij}\| < \varepsilon_F = 1,0 \cdot e^{-5} \quad (9)$$

Полученное решение и будет являться решением задачи для случая одного эксперта. Для случая группы экспертов это решение – всего лишь опорное ($V_i^{опор}$).

¹ Критерий связности важен в тех случаях, когда возможен разрыв остова графа.

Требуется учёт отдалённости нижних границ, задаваемой матрицей $\|B_{ij}\|$. Для этого восстановим первоначальную конфигурацию графа.

Рассчитаем результирующую матрицу $\|R_{ij}\|$:

$$R_{ij} = -(B_{ij} + V_j - V_i) \quad (10)$$

и удалим в ней все отрицательные элементы.

Некоторые ребра могут дополнить опорную конфигурацию.

Далее осуществляем следующую процедуру, которая имеет также два цикла.

Во внешнем цикле мы определяем наиболее критическое ребро, которое можно отбросить. Для этого изме-

Таблица 2 – Исходные значения коэффициентов

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
O1	1	$\frac{1}{3}$	$\frac{1}{5}$	$\frac{1}{3}$	$\frac{1}{7}$	$\frac{1}{3}$	NA	NA	NA	$\frac{1}{4}$
O2	$\frac{3}{1}$	1	$\frac{1}{5}$	NA	$\frac{1}{5}$	$\frac{1}{4}$	NA	NA	NA	$\frac{1}{3}$
O3	$\frac{5}{1}$	$\frac{5}{1}$	1	$\frac{3}{1}$	NA	$\frac{3}{1}$	$\frac{3}{1}$	$\frac{5}{1}$	$\frac{5}{1}$	$\frac{3}{1}$
O4	$\frac{3}{1}$	NA	$\frac{1}{3}$	1	$\frac{1}{3}$	NA	NA	NA	NA	$\frac{1}{3}$
O5	$\frac{7}{1}$	$\frac{5}{1}$	NA	$\frac{3}{1}$	1	$\frac{3}{1}$	$\frac{5}{1}$	$\frac{5}{1}$	$\frac{5}{1}$	$\frac{3}{1}$
O6	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{1}{3}$	NA	$\frac{1}{3}$	1	NA	NA	NA	$\frac{1}{4}$
O7	NA	NA	$\frac{1}{3}$	NA	$\frac{1}{5}$	NA	1	NA	NA	$\frac{1}{5}$
O8	NA	NA	$\frac{1}{5}$	NA	$\frac{1}{5}$	NA	NA	1	NA	$\frac{1}{5}$
O9	NA	NA	$\frac{1}{5}$	NA	$\frac{1}{5}$	NA	NA	NA	1	$\frac{1}{5}$
O10	$\frac{4}{1}$	$\frac{3}{1}$	$\frac{1}{3}$	$\frac{3}{1}$	$\frac{1}{3}$	$\frac{4}{1}$	$\frac{5}{1}$	$\frac{5}{1}$	$\frac{5}{1}$	1

Таблица 3 – Логарифмы от значения коэффициентов

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
O1	0	-1,09861	-1,60944	-1,09861	-1,94591	-1,09861	NA	NA	NA	-1,38629
O2	1,098612	0	-1,60944	NA	-1,60944	-1,38629	NA	NA	NA	-1,09861
O3	1,609438	1,609438	0	1,098612	NA	1,098612	1,098612	1,609438	1,609438	1,098612
O4	1,098612	NA	-1,09861	0	-1,09861	NA	NA	NA	NA	-1,09861
O5	1,94591	1,609438	NA	1,098612	0	1,098612	1,609438	1,609438	1,609438	1,098612
O6	1,098612	1,386294	-1,09861	NA	-1,09861	0	NA	NA	NA	-1,38629
O7	NA	NA	-1,09861	NA	-1,60944	NA	0	NA	NA	-1,60944
O8	NA	NA	-1,60944	NA	-1,60944	NA	NA	0	NA	-1,60944
O9	NA	NA	-1,60944	NA	-1,60944	NA	NA	NA	0	10,65705
O10	1,386294	1,098612	-1,09861	1,098612	-1,09861	1,386294	1,609438	1,609438	1,609438	0

Таблица 4 – Перестановка порядка объектов

	O5	O3	O10	O6	O2	O4	O1	O7	O8	O9
O5	0	NA	1,0986	1,0986	1,7041	1,0986	1,9459	1,7041	1,7041	1,7041
O3	NA	0	1,0986	1,0986	1,7041	1,0986	1,7041	1,0986	1,7041	1,7041
O10	-1,0986	-1,0986	0	1,3863	1,0986	1,0986	1,3863	1,7041	1,7041	1,7041
O6	-1,0986	-1,0986	-1,3863	0	1,3863	NA	1,0986	NA	NA	NA
O2	-1,7041	-1,7041	-1,0986	-1,3863	0	NA	1,0986	NA	NA	NA
O4	-1,0986	-1,0986	-1,0986	NA	NA	0	1,0986	NA	NA	NA
O1	-1,9459	-1,7041	-1,3863	-1,0986	-1,0986	-1,0986	0	NA	NA	NA
O7	-1,7041	-1,0986	-1,7041	NA	NA	NA	NA	0	NA	NA
O8	-1,7041	-1,7041	-1,7041	NA	NA	NA	NA	NA	0	NA
O9	-1,7041	-1,7041	-1,7041	NA	NA	NA	NA	NA	NA	0

ряется масштаб единичного смещения для каждого веса U_i , определяется размер единичного шага смещения для каждого ребра (i, j) D_{ij} , и величина шага h по формуле

$$h = \min_{i,j} \left(\frac{R_{ij}}{D_{ij}} \right). \quad (11)$$

Формулы для D_{ij} и U_i в этой статье опускаем.

Далее во внутреннем цикле определяем виртуальное оптимальное решение по формулам:

$$V_i^{omm} = V_i^{опор} - h \times U_i, (i = 1, \dots, N) \quad (12)$$

$$R_{ij}^{omm} = R_{ij}^{опор} - h \times D_{ij}, (i = 1, \dots, N-1; j = i+1, \dots, N) \quad (13)$$

Если появившиеся нулевые элементы R_{ij}^{omm} не приводят к потере связности графа, ребро первого из них может быть отброшено. Если, напротив, происходит потеря связности матрицы результатов, то происходит запоминание «последней» удачной попытки в качестве уже реального оптимального значения для весов R_{ij}^{omm} .

Если матрица R_{ij}^{omm} совпадает с матрицей инцидентности матрицы $R_{ij}^{опор}$, единичное смещение $U_i=1$ (тип $i=1$); $U_i=0$ (тип $i=-1$).

После выброса вершин в R_{ij}^{omm} оптимальное решение приобретает окончательный вид. Оно примыкает к нижней границе, и является оптимальным решением,

полученным на данных о верхней границе. Предполагается, что конфликт интересов находится на верхней границе, где каждый их экспертов стремится обозначить собственные приоритеты.

3. Пример практического применения метода

Пусть задана матрица попарных сравнений, заполненная экспертами по методу Саати (таблица 2).

Матрица заполнена не полностью (отсутствующие оценки обозначены NA), поскольку эксперты не смогли высказать своих предпочтений при сравнении некоторых пар объектов (например, O_1 и O_7 , O_2 и O_4 , и др.).

Преобразуем матрицу неполных попарных сравнений в кососимметричную матрицу путём логарифмирования элементов матрицы коэффициентов (таблица 3).

Матрица после диагонализации, которую мы проводим для того, чтобы матрица приобрела положительный вид над основной диагональю, представлена в таблице 4.

Рассмотрим реализацию алгоритма¹ для верхних оценок T_{ij} или одного эксперта $\bar{S}_{i,j}$.

¹ В силу того, что матрица является кососимметричной, опустим при её изображении её часть ниже главной диагонали

Таблица 5 – Исходные данные

A	B	C	D	E	F	G	H	I	J	K	L	M	N
i	V_j	V_j	Тип	1	2	3	4	5	6	7	8	9	10
1	10,00000	1,70280	1	0	NA	1,2528	1,3863	1,7918	1,2528	2,1528	1,7118	1,7918	1,6247
2	10,00000	1,48430	1		0	1,3863	1,3863	1,7047	1,0968	1,8718	1,2528	1,7047	1,8718
3	10,00000	0,24275	0			0	1,5041	1,2528	1,3863	1,5041	1,7918	1,8718	1,7047
4	10,00000	0,05265	0				0	1,6094	NA	1,2528	NA	NA	NA
5	10,00000	-0,20275	0					0	NA	1,3863	NA	NA	NA
6	10,00000	-0,06675	0						0	1,2528	NA	NA	NA
7	10,00000	-1,70280	-1							0	NA	NA	NA
8	10,00000	-1,52230	-1								0	NA	NA
9	10,00000	-1,78825	-1									0	NA
10	10,00000	-1,74825	-1										0

Таблица 6

A	B	C	D	E	F	G	H	I	J	K	L	M	N
i	V_j	V_j	Тип	1	2	3	4	5	6	7	8	9	10
1	10,81469	0,00	1	0	0	0,5956	0,0279	-0,373	-0,354	-0,5956	-0,176	-0,3619	-0,3686
2	10,74094	0,00	1		0	0,8029	0,1016	-0,387	-0,436	-0,8029	-0,5612	-0,3753	-0,0477
3	10,15750	0,00	0			0	0,8029	-0,255	0,4365	-0,5871	0,5612	0,3753	0,3686
4	9,45626	0,00	0				0	0,8029	0	-0,1372	0	0	0
5	8,64972	0,00	0					0	0	0,8029	0	0	0
6	9,20767	0,00	0						0	0,1114	0	0	0
7	8,06628	0,00	-1							0	0	0	0
8	8,92692	0,00	-1								0	0	0
9	8,66097	0,00	-1									0	0
10	8,82140	0,00	-1										0

Таблица 7

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	V_i	ΔV_j	W_i	Тип V_i	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
v_1	2,688766	0,00000	0,162651	1	0	0	0	0	0	0	0	0	$-1e^{-16}$	$-2e^{-16}$
v_2	2,229765	0,00000	0,102782	1		0	0	0	0	0	0	$-1e^{-16}$	0	0
v_3	2,768765	0,00000	0,176197	1			0	0	0	0	$-2e^{-16}$	$-1e^{-16}$	$1e^{-6}$	$1e^{-6}$
v_4	2,517465	0,00000	0,137044	1				0	0	0	$-2e^{-16}$	0	0	0
v_5	2,650965	0,00000	0,156618	1					0	0	$2e^{-16}$	0	0	0
v_6	2,517465	0,00000	0,137044	1						0	$-2e^{-16}$	0	0	0
v_7	1,264665	0,00000	0,039154	-1							0	0	0	0
v_8	0,976965	0,00000	0,029365	-1								0	0	0
v_9	0,896966	0,00000	0,027107	-1									0	0
v_{10}	1,064066	0,00000	0,032038	-1										0

В силу особенностей матрицы T_{ij} начальное значение весов (столбец B, табл. 5) может быть произвольной постоянной величиной, чтобы не путаться в знаках приращений весов. Величина изменений (столбец C, табл. 5), как мы говорили выше, зависит от типа строки-столбца.

Для поиска самого жёсткого противоречия, для всех строк ищем оптимальное смещение весов за счёт оптимизации веса V_j , которое затрагивает и j -ую строку и i -ый столбец. Выбирая строки по убыванию ($i=N, \dots, 1$) до тех пор, пока **все смещения** в столбце C (табл. 5) не обратятся в нуль.

В соответствии вышеизложенным алгоритмом ищем предельный по модулю цикл для начальных стартовых условий. Результат приведён в таблице 6.

Какая ячейка должна быть удалена? На правом конце «поплавок» – (2,3), (3,4), (4,5), (5,7), на левом конце только одно ребро (2,7). Ребра на правом конце сообщают, что 2-й объект лучше 3-го, 3-й объект лучше 4-го, 4-й лучше 5-го, 5-й лучше 7-го в $e^{0,8029}=2,3632$ раз.

Итого получается, что 2-й объект лучше 7-го объекта в $(2,3632)^4=31,1890$ раз. Но в ячейке (2,7) стоит обратное – объект 2-й хуже 7-го объекта в 2,3632 раза. И тем

Таблица 8

	w_{cp}			w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
w_1	2,688766			0	0	-0,773	-0,745	-1,3485	-0,745	-0,3677	0,2077	0,1824	0,1206
w_2	2,229765				0	-1,232	-0,981	-1,8075	-1,204	-0,539	0,3365	-0,1713	-0,2206
w_3	2,768765					0	-1,002	-0,5754	-0,665	0,4073	0,4055	0,3677	0,4519
w_4	2,517465						0	-1,3863	0	0,5596	0	0	0
w_5	2,650965							0	0	0,47	0	0	0
w_6	2,517465								0	0,5596	0	0	0
w_7	1,264665									0	0	0	0
w_8	0,976965										0	0	0
w_9	0,896966											0	0
w_{10}	1,064066												0

Таблица 9

	w_{cp}			w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
w_1	2,688766			0	0	0	0	0	0	0	0,2077	0,1824	0,1206
w_2	2,229765				0	0	0	0	0	0	0,3365	0	0
w_3	2,768765					0	0	0	0	0,4073	0,4055	0,3677	0,4519
w_4	2,517465						0	0	0	0,5596	0	0	0
w_5	2,650965							0	0	0,47	0	0	0
w_6	2,517465								0	0,5596	0	0	0
w_7	1,264665									0	0	0	0
w_8	0,976965										0	0	0
w_9	0,896966											0	0
w_{10}	1,064066												0

Таблица 10

	V_i	W_i		w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}
w_1	2,48106	0,1611740		0	0	0	0	0	0	0	$1e^{-6}$	0	0
w_2	2,02867	0,1025226			0	0	0	0	0	0	0,1354	0	0
w_3	2,56767	0,1757537				0	0	0	0	0,2062	0,2044	0,1666	0,2508
w_4	2,31637	0,1366993					0	0	0	0,3585	0	0	0
w_5	2,44987	0,1562230						0	0	0,2689	0	0	0
w_6	2,11637	0,1119200							0	0,1585	0	0	0
w_7	1,26467	0,0477550								0	0	0	0
w_8	0,97697	0,0358156									0	0	0
w_9	0,89697	0,0330620										0	0
w_{10}	1,06407	0,0390751											0

самым возникает противоречие. С одной стороны, 2-й лучше в 31,1890 раз объекта 7, с другой стороны хуже его в 2,3632 раза. Но самое важное, что цикл не может быть улучшен. Попытка изменить веса объектов в цикле приводит к автоматическому росту модуля.

Следовательно, должно быть удалено ребро (2,3). Поскольку 0,8029 до 0,1016 (ребро (2,4)) имеет наибольшее сокращение.

Следуя по алгоритму далее, осуществляем процедуру двух вложенных циклов (внешнего и внутреннего). Полученное решение (столбец «В», таблица 7) является решением задачи для случая «одного эксперта».

Для учёта отдалённости нижних границ, задаваемой матрицей $\|B_{ij}\|$ восстановим первоначальную конфигурацию графа (таблица 8).

И далее рассчитаем по (10) результирующую матрицу R_{ij} и удалим в ней все отрицательные элементы (таблица 9).

Некоторые ребра, например, (1,8), могут дополнить опорную конфигурацию. Далее во внешнем цикле мы определяем наиболее критическое ребро, которое можно отбросить. Для этого измеряется масштаб единичного смещения для каждого веса U_i , определяется размер единичного шага смещения для каждого ребра (i, j) D_{ij} , и величина шага h по формуле (11), во внутреннем цикле определяем виртуальное оптимальное решение по формулам (12) и (13).

В рассматриваемом примере матрица R_{ij}^{omm} совпадает с матрицей инцидентности матрицы R_{ij}^{onop} , единичное смещение $U_i=1$ (тип $i=1$); $U_i=0$ (тип $i=-1$).

После выброса вершин (1,10) и (1,9) в R_{ij}^{omm} оптимальное решение приобретает окончательный вид (таблица 10).

Решение примыкает ребром (1,8) к нижней границе, и является оптимальным решением, полученным на данных о верхней границе. Предполагается, что конфликт интересов находится на верхней границе, где каждый их экспертов стремится обозначить собственные приоритеты.

Библиографический список

1. Evangelos, T.: Multi-criteria decision making methods: a comparative study. (Kluwer Academic Publishers, Dordrecht, 2000)
2. Fodor, J., Roubens, M.: Fuzzy preference modelling and multicriteria decision support. (Kluwer Academic Publishers, Dordrecht, 1994)
3. Xu, Z.S.: Goal programming models for obtaining the priority vector of incomplete fuzzy preference relation. *International Journal of Approximate Reasoning*, 36:3 (2004) 261–270
4. Литтл Р. Дж. А., Рубин Д. Б. Статистический анализ данных с пропусками. – М.: Финансы и статистика, 1991. – 336 с.
5. Garcia-Laencina P.J., Sancho-Gomez J.-L., Figueiras-Vidal A.R. Pattern classification with missing data: a review. – London: Springer-Verlag Limited, 2009.
6. Schafer J.L., Graham J.W. Missing data: Our view to the state of the art // *Psychological methods*. – 2002. – Vol. 7. – № 2. – С. 147–177.
7. Millet I., “The effectiveness of alternative preference elicitation methods in the analytic hierarchy process,” *J. Multi-Criteria Decis. Anal.*, vol. 6, no. 1, pp. 41–51, 1997.
8. Carmone F. J., Kara Jr., A., Zanakos S. H. “A Monte Carlo investigation of incomplete pairwise comparison matrices in AHP,” *Eur. J. Oper. Res.*, vol. 102, no. 3, pp. 533–553, Nov. 1997.
9. Ebenbach D.H., Moore C.F. “Incomplete information, inferences, and individual differences: The case of environmental judgements,” *Org. Behav. Human Decis. Process.*, vol. 81, no. 1, pp. 1–27, Jan. 2000.
10. S. Alonso, F. J. Cabrerizo, F. Chiclana, F. Herrera, and E. Herrera-Viedma, “An interactive decision support system based on consistency criteria,” *J. Mult.-Valued Log. Soft Comput.*, vol. 14, no. 3–5, pp. 371–386, 2008.
11. J. K. Kim and S. H. Choi, “A utility range-based interactive group support system for multiattribute decision making,” *Comput. Oper. Res.*, vol. 28, no. 5, pp. 485–503, Apr. 2001.
12. J. K. Kim, S. H. Choi, C. H. Han, and S. H. Kim, “An interactive procedure for multiple criteria group decision making with incomplete information,” *Comput. Ind. Eng.*, vol. 35, no. 1/2, pp. 295–298, Oct. 1998.
13. Chiclana F., Herrera-Viedma E., Alonso S. A Note on Two Methods for Estimating Missing Pairwise Preference Values. *IEEE Transactions On Systems, MAN, and Cybernetics – Part B: Cybernetics*, Vol. 39, No. 6, December 2009. 1628- 1633.
14. Карлов И.А. Восстановление пропущенных данных при численном моделировании сложных динамических систем, Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление, 2013, выпуск 6(186), с. 137–144. (I. A. Karlov, “The missing value estimation in numerical modeling of complex dynamic systems”, *SPbSPU Journal. Computer Science. Telecommunication and Control Systems*, 2013, no. 6(186), 137–144).
15. Саати Т. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993. – 278 с.
16. Ашманов С.А. Математические модели и методы. М.: Изд-во Моск. Ун-та, 1980. – 199 с.

Сведения об авторах

Александр В. Бочков – кандидат технических наук, заместитель директора центра анализа рисков, Научно-исследовательский институт экономики и организации управления в газовой промышленности, Москва, Россия, тел. +7 (916) 234-40-32 e-mail: a.bochkov@gmail.com

Николай Н. Жигирев – кандидат технических наук, главный научный сотрудник, Научно-исследовательский институт экономики и организации управления в газовой промышленности, Москва, Россия, тел. +7 (985) 782-47-16, e-mail: nnzhigirev@mail.ru

Александра Н. Ридли – аспирант МАИ (НИУ), Москва, Россия, тел. +7 (929) 970-59-69, e-mail: alexandra.ridley@yandex.ru

Поступила 18.01.2017

Применение системы автоматической сигнализации для снижения риска транспортных происшествий на железнодорожных станциях¹

Игорь Б. Шубинский, ЗАО «ИБТранс», Москва, Россия

Алексей М. Замышляев, ОАО «НИИАС», Москва, Россия

Алексей Н. Игнатов, Московский Авиационный институт, Москва, Россия

Андрей И. Кибзун, Московский Авиационный институт, Москва, Россия

Евгений Н. Платонов, Московский Авиационный институт, Москва, Россия

Резюме. Цель. Оценить риск столкновения составов при проведении маневровых работ на железнодорожной станции. Риск – сочетание вероятности события и его последствий. Наиболее сложной задачей при расчёте риска является выбор модели оценки вероятности появления нежелательного события. Модель должна обеспечивать практическую применимость результатов. Для объектов железнодорожного транспорта наибольший интерес представляет построение аналитической модели оценки вероятности в виду возможности наглядной демонстрации учитываемых в модели факторов. Основной целью данной работы является исследование степени влияния системы маневровой автоматической локомотивной сигнализации (МАЛС) на вероятность бокового столкновения составов с участием маневровых локомотивов на железнодорожной станции. Основной функцией системы маневровой автоматической локомотивной сигнализации является обеспечение непроезда маневровыми локомотивами светофоров с запрещающими показаниями на станции. **Методы.** Используются методы теории вероятностей и теории случайных процессов, формулы сложения, умножения, полной вероятности, свойства пуассоновских потоков. В статье [2] предложена методика расчета вероятности столкновения вследствие проезда маневровым или поездным локомотивом запрещающего сигнала светофора. Основным предположением при разработке методики является предположение о том, что поток маневровых составов для каждого стрелочного перевода является пуассоновским. В настоящей работе предлагается модификация данной методики с учётом возможности использования системы МАЛС на локомотивах маневровых составов. Исходными данными для реализации алгоритма вычисления вероятности столкновения служат топология станции, расписание движения пассажирских поездов и возможные маршруты их следования через станцию, средние значения длин составов и скоростей их движения, а также интенсивности движения маневровых составов через стрелочные переводы. **Результаты.** Получен алгоритм вычисления вероятности столкновения составов с участием маневровых локомотивов для произвольного промежутка времени. Для различных режимов движения маневрового состава: подтягивания, сцепки – приводятся расчетные формулы для вычисления вероятности столкновения с пассажирским или грузовым поездом на произвольной стрелке. Алгоритм состоит в следующем: 1) задается промежуток времени, для которого необходимо провести расчет вероятности столкновения; 2) формируется расписание следования пассажирских поездов из АСУ «Экспресс»; 3) вычисляется общее количество пассажирских поездов, проезжающих через станцию в течение заданного промежутка времени; 4) пассажирские поезда перенумеровываются согласно порядку их прибытия на станцию; 5) вычисляется вероятность проезда машинистом маневрового локомотива светофора с запрещающим показанием; 6) вычисляется вероятность нарушения машинистом маневрового локомотива безопасности движения в режиме «подтягивание»; 7) вычисляется вероятность нарушения машинистом маневрового локомотива безопасности движения после сцепки с отключенным режимом «сцепка»; 8) вычисляется общее число возможных маршрутов для каждого поезда; 9) для каждого поезда определяется частота использования того или иного маршрута; 10) для всех стрелок на каждом маршруте присваиваются номера в порядке их появления; 11) вычисляется вероятность того, что с каждым пассажирским поездом на каждом маршруте произойдет хотя бы одно столкновение; 12) вычисляется вероятность того, что произойдет хотя бы одно столкновение каждого пассажирского поезда при движении через станцию; 13) рассчитывается вероятность того, что за заданный промежуток времени произойдет хотя бы одно столкновение на станции. Рассмотрен пример расчёта вероятности столкновения для отдельного маршрута поезда и для всей железнодорожной станции в целом в течение месяца и года. В работе показано, что применение системы МАЛС позволяет существенно уменьшить вероятность боковых столкновений на железнодорожной станции.

¹ Работа выполнена при поддержке Российского научного фонда (проект № 16-11-00062).

Ключевые слова: железнодорожный транспорт, безопасность движения, маневровые работы, вероятность столкновения.

Формат цитирования: Шубинский И.Б., Замышляев А.М., Игнатов А.Н., Кибзун А.И., Платонов Е.Н. Применение системы автоматической сигнализации для снижения риска транспортных происшествий на железнодорожных станциях // Надежность. 2017. Т. 17, № 3. С. 49-57. DOI: 10.21683/1729-2646-2017-17-3-49-57

1. Введение

При проведении как пассажирских, так и грузовых перевозок с определенной интенсивностью могут возникать различные неблагоприятные события, которые могут привести как к репутационным, так и материальным издержкам ОАО «РЖД», связанным, например, с ущербом инфраструктуре и/или подвижному составу. Поэтому для определения количественной характеристики опасности того или иного события вводят понятие риска, который согласно [1] является функционалом от вероятности и ущерба от неблагоприятного события.

Как отмечено в [2], при проведении маневровых работ на станции вследствие проезда запрещающего сигнала одним из участников движения возможны столкновения не только двух маневровых составов, но и, в частности, пассажирского поезда и маневрового состава, что, как выяснено в [3], может привести к гибели людей и, соответственно, большому ущербу. При этом, несмотря на то, что при проезде одного пассажирского поезда вероятность его столкновения с маневровым составом довольно мала, вероятность хотя бы одного столкновения за год по всем поездам, проезжающим через станцию, составляет довольно-таки существенную величину, особенно если на станции проводятся интенсивные маневровые работы. Для уменьшения вероятности столкновения поездов можно установить и использовать систему МАЛС.

При установке системы МАЛС на маневровые локомотивы возможны несколько режимов движения локомотива. Первый режим – «типичный», когда система МАЛС работает в штатном режиме. Второй режим – режим «подтягивание», когда система МАЛС отключена и машинист маневрового локомотива может подъехать к запрещающему сигналу светофора на расстояние ближе 20 метров и, следовательно, может проехать запрещающий сигнал, вследствие чего возможно столкновение между маневровым составом и пассажирским или грузовым поездом. Третий режим – режим «движение после сцепки с отключенным режимом «сцепка», когда при движении вагонами вперед система МАЛС некорректно определяет положение начала или конца состава, вследствие чего также возможен проезд запрещающего сигнала. Второй и третий режим являются нештатными режимами движения. Очевидно, что в «типичном» режиме маневровый локомотив находится большую часть времени, однако в двух других режимах вероятность проезда запрещающего сигнала существенно выше, поэтому каждый из этих случаев характеризуется своей вероятностью столкновения ма-

неврового состава с пассажирским/грузовым поездом и отдельно рассматривается в статье.

2. Алгоритм вычисления вероятности столкновения за произвольный промежуток времени при использовании системы МАЛС

Введем следующие обозначения:

- N – общее количество стрелок на станции;
- L – количество маневровых локомотивов;
- N_l – количество проезжаемых стрелок маневровой группой в час, $l=1, \dots, L$;
- r_l – количество полурейсов, $l=1, \dots, L$;
- s_l – количество сцепок с отключенным режимом сцепки, $l=1, \dots, L$;
- T_l – количество подтягиваний, $l=1, \dots, L$;
- l_m – средняя длина маневровой группы;
- l_n – средняя длина пассажирского поезда;
- v_n – средняя скорость движения пассажирского поезда по станции;
- v_m – средняя скорость движения маневровой группы по станции;
- v_t – средняя скорость движения маневровой группы по станции в режиме «подтягивание»;
- P_n – вероятность проезда запрещающего сигнала пассажирским поездом;
- $P_{m(один)}$ – вероятность проезда машинистом маневрового локомотива светофора с запрещающим показанием при работе без помощника машиниста;
- $P_{m(двое)}$ – вероятность проезда машинистом маневрового локомотива светофора с запрещающим показанием при работе с помощником машиниста;
- $P_{двое}$ – вероятность комплектования локомотивной бригады маневрового локомотива машинистом и его помощником;
- $P_{вм}$ – вероятность сцепки с последующим движением маневрового локомотива вместе с вагонами;
- $P_d(s)$ – вероятность непредотвращения дежурным по станции проследования машинистом маневрового локомотива запрещающего сигнала светофора в режиме «подтягивание»;
- $P_{тп}$ – вероятность проезда запрещающего сигнала машинистом маневрового локомотива в режиме «подтягивание», когда маневровый локомотив находится в голове поезда;
- $P_{тх}$ – вероятность проезда запрещающего сигнала машинистом маневрового локомотива в режиме «под-

тягивание», когда маневровый локомотив находится в хвосте поезда;

$P_{\text{сцх}}$ – вероятность нарушения безопасности движения составителем;

λ_c^i – интенсивность останавливающихся на стрелочных переводах маневровых групп, не нарушивших при пересечении стрелки безопасности движения, $i=1, \dots, N$;

τ_c^i – среднее время нахождения на стрелочном переводе маневровой группы, не нарушившей при пересечении стрелки безопасности движения, при условии остановки на стрелочном переводе, $i=1, \dots, N$;

τ_t – среднее время освобождения маневровой группой стрелочного перевода при попадании на него в режиме «подтягивание» после остановки на этом переводе.

1. Задается промежуток времени T , для которого необходимо провести расчет вероятности столкновения, получение расписания следования пассажирских поездов из АСУ «Экспресс». Согласно расписанию определяются все пассажирские поезда, следующие через станцию в течение времени T .

2. Определяется I – общее количество пассажирских поездов, проезжающих через станцию в течение времени T .

3. Присваиваются номера пассажирским поездам, следующим через станцию за рассматриваемый промежуток времени, по времени прибытия на станцию. Пассажирские поезда перенумеровываются согласно порядку их прибытия на станцию, то есть первый прибывший поезд, получает номер 1, второй – номер 2 и так далее.

4. Вероятность проезда машинистом маневрового локомотива светофора с запрещающим показанием вычисляется по формуле

$$P_m = P_{\text{двос}} \cdot P_{\text{м(двос)}} + (1 - P_{\text{двос}}) \cdot P_{\text{м(один)}}$$

вероятность нарушения машинистом маневрового локомотива безопасности движения в режиме «подтягивание» определяется по формуле

$$P_t = \frac{1}{2} P_d(s)(P_{\text{тл}} + P_{\text{тх}}),$$

вероятность нарушения машинистом маневрового локомотива безопасности движения после сцепки с отключенным режимом «сцепка» определяется по формуле

$$P_{\text{сц}} = \left(1 - \frac{1}{2} P_{\text{вм}}\right) P_m + \frac{1}{2} P_{\text{вм}} P_{\text{сцх}}.$$

Для каждой стрелки вычисляется

$\tilde{\lambda}_t$ – интенсивность нахождения маневровой группы в режиме «подтягивание» перед стрелкой

$$\tilde{\lambda}_t = \sum_{l=1}^L \frac{1}{N} \cdot \frac{T_l}{24},$$

$\tilde{\lambda}_{\text{сц}}$ – интенсивность пересечения стрелки маневровой группой после сцепки с отключенным режимом «сцепка»

$$\tilde{\lambda}_{\text{сц}} = \sum_{l=1}^L \frac{N_l}{N} \cdot \frac{S_l}{r_l},$$

$\tilde{\lambda}_m$ – интенсивность пересечения стрелки маневровой группой в «обычном» режиме

$$\tilde{\lambda}_m = \sum_{l=1}^L \frac{N_l}{N} - \tilde{\lambda}_t P_t - \tilde{\lambda}_{\text{сц}}.$$

Интенсивность¹ λ_t^1 возможного пересечения стрелки маневровой группой в режиме «подтягивание» в некотором направлении l вычисляется по формуле $\lambda_t^1 = \tilde{\lambda}_t / 4$.

Интенсивность $\lambda_{\text{сц}}^1$ пересечения стрелки маневровой группой после сцепки с отключенным режимом «сцепка» в некотором направлении l вычисляется по формуле $\lambda_{\text{сц}}^1 = \tilde{\lambda}_{\text{сц}} / 4$.

Интенсивность λ_m^1 пересечения стрелки маневровой группой в «обычном» режиме в некотором направлении l вычисляется по формуле $\lambda_m^1 = \tilde{\lambda}_m / 4$.

5. Величина i полагается равной единице.

6. Вычисляется K – общее число возможных маршрутов для i -го поезда.

7. Величина k полагается равной единице.

8. Для i -го поезда определяется частота использования того или иного маршрута²

$$P(R_k) = \frac{m_{R_k}}{n},$$

где m_{R_k} – число проехавших пассажирских поездов с номером i по маршруту R_k , а n – общее число пассажирских поездов с номером i , проехавших через станцию за время наблюдения.

9. При обработке маршрута R_k присваиваются номера стрелкам, входящим в этот маршрут, согласно следованию через этот маршрут i -го поезда, то есть первая стрелка, которую пересекает пассажирский поезд, получает номер 1, вторая стрелка, которую пересекает пассажирский поезд, получает номер 2 и так далее. Пусть m – общее число стрелок, которые i -ый поезд, пересекает на маршруте R_k .

10. Величина j полагается равной единице.

11. В случае неизолированности³ j -ой стрелки маршрута R_k i -го пассажирского поезда определяются:

λ_m – интенсивность пересечения маневровой группой стрелочного перевода в «обычном» режиме в направлении

¹ Интенсивности могут быть уточнены при непосредственном сборе данных для каждого стрелочного перевода на рассматриваемой железнодорожной станции.

² Если отсутствуют данные о прошлых проездах поезда через станцию, то все маршруты полагаются равновероятными, то есть для любого k вероятность $P(R_k)$ использования маршрута R_k вычисляется по формуле $P(R_k) = 1/K$.

³ Изолированным стрелочным переводом называется тот, на котором столкновение, вызванное проездом светофора с запрещающим показанием, невозможно, неизолированным стрелочным переводом называется тот, на котором столкновение возможно.

нии, при котором возможно столкновение (выбирается из λ_m^1 , полученных на шаге 4, см. рисунок 1);

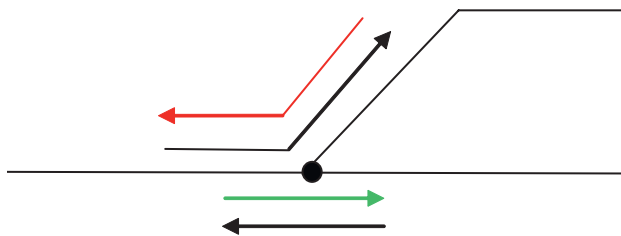


Рисунок 1 – Направление следования (отмечено красной стрелочкой) маневровой группы через стрелочный перевод (отмечен кружком), при котором возможно столкновение с пассажирским составом, следующим в направлении, показанном зеленой стрелочкой

λ_{cu} – интенсивность пересечения маневровой группой с маневровым локомотивом, проводившим сцепку с отключенным режимом «сцепка», стрелочного перевода в направлении, при котором возможно столкновение (выбирается из λ_{cu}^1 , полученных на шаге 4, см. рисунок 1);

λ_t – интенсивность возможного пересечения маневровой группой с маневровым локомотивом, находившемся перед стрелочным переводом в режиме «подтягивание», стрелочного перевода в направлении, при котором возможно столкновение (выбирается из λ_t^1 , полученных на шаге 4, см. рисунок 1);

λ_c – интенсивность останавливающихся на j -ой стрелке маневровых групп;

τ_c – среднее время нахождения маневровой группы на j -ой стрелке при условии остановки на ней;

P_{nc} – вероятность остановки i -го пассажирского поезда на j -ой стрелке;

τ_{nc} – среднее время стоянки i -го пассажирского поезда на j -ой стрелке;

вероятность столкновения, произошедшего по вине машиниста маневрового локомотива (при отказе системы МАЛС), проехавшего светофор с запрещающим показанием

$$P_M(A_m) = \lambda_m P_m \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} + P_{nc} \tau_{nc} \right);$$

вероятность столкновения, произошедшего по вине машиниста пассажирского поезда, проехавшего запрещающий сигнал

$$P_M(A_n) = P_n \lambda_m \left(\frac{l_m}{v_m} + \frac{l_n}{v_n} \right) + P_n \lambda_{cu} \left(\frac{l_m}{v_m} + \frac{l_n}{v_n} \right);$$

вероятность столкновения, произошедшего по вине машиниста пассажирского поезда, проехавшего запрещающий сигнал и столкнувшегося с вагонами, стоящими на стрелочном переводе

$$P_M(A_c) = P_n \lambda_c \tau_c;$$

вероятность столкновения, произошедшего по вине машиниста маневрового локомотива, проехавшего запрещающий сигнал в режиме «подтягивание»

$$P_M(A_t) = \lambda_t P_t \left(\frac{l_n}{v_n} + \frac{l_t}{v_t} + P_{nc} \tau_{nc} + \tau_t \right);$$

вероятность столкновения при проезде светофора с запрещающим показанием и машинистом маневрового локомотива, и машинистом пассажирского поезда

$$P_M(A_{tn}) = \lambda_t P_t P_n \left(\frac{l_t}{v_t} + \frac{l_n}{v_n} \right) + \lambda_m P_m P_n \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} \right) + \lambda_{cu} P_{cu} P_n \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} \right);$$

вероятность столкновения, произошедшего по вине машиниста маневрового локомотива, после сцепки с отключенным режимом «сцепка»

$$P_M(A_{cu}) = \lambda_{cu} P_{cu} \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} + P_{nc} \tau_{nc} \right).$$

Результирующая вероятность столкновения на j -ой стрелке вычисляется по формуле

$$P_M(A_{k;j}) = \left(\lambda_m \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} \right) (P_m (1 + P_n) + P_n) + \lambda_{cu} \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} \right) (P_{cu} (1 + P_n) + P_n) + \lambda_t \left(\frac{l_t}{v_t} + \frac{l_n}{v_n} + \tau_t \right) \cdot P_t (1 + P_n) + \lambda_c P_n \tau_c + (\lambda_m P_m + \lambda_t P_t + \lambda_{cu} P_{cu}) P_{nc} \tau_{nc} \right) \cdot k_c,$$

где k_c принимает значение 1, если стрелочный перевод неизолированный, и 0, если изолированный, а остальные переменные, входящие в эту формулу, определены на шаге 1 и 4.

12. Если $j=m$, то переход к шагу 14, иначе переход к шагу 13.

13. $j:=j+1$, переход к шагу 11.

14. Вычисляется вероятность того, что с i -ым пассажирским поездом на маршруте R_k произойдет хотя бы одно столкновение, которая составляет

$$P_M(A_i | R_k) = 1 - \prod_{j=1}^m (1 - P_M(A_{k;j})),$$

где вероятности $P_M(A_{k;j})$ вычислены на шаге 11, величина m – на шаге 9.

15. Если $k=K$, то переход к шагу 17, иначе переход к шагу 16.

16. $k:=k+1$, переход к шагу 8.

17. Вычисляется вероятность того, что произойдет хотя бы одно столкновение пассажирского поезда с номером i при движении через станцию

$$P_M(A_i) = \sum_{k=1}^K P_M(A_i | R_k) P(R_k),$$

где вероятности $P_M(A_i | R_k)$ вычислены на шаге 14, а вероятности $P(R_k)$ – на шаге 8, величина K – на шаге 6.

18. Если $i=I$, то переход к шагу 20, иначе переход к шагу 19.

19. $i:=i+1$, переход к шагу 6.

20. Рассчитывается вероятность того, что за промежуток времени T произойдет хотя бы одно столкновение

$$P_M(A_T) = P_M(A_1 + A_2 + \dots + A_I) = 1 - \prod_{i=1}^I (1 - P_M(A_i)).$$

3. Пример расчета вероятности столкновения пассажирского состава с маневровой группой для некоторой станции с установленной системой МАЛС

Пусть имеется 4 направления следования от и к станции (схема станции приведена рисунке 2): северо-восточное, юго-восточное, северо-западное, юго-западное. С северо-восточного направления поезда следуют на станцию через путь F , с юго-восточного поезда следуют на станцию через путь D , с северо-западного поезда следуют на станцию через путь B , с юго-западного через путь B или путь C . Со станции на северо-восточное направление можно попасть по пути F , на юго-восточное направление можно попасть по пути E , на северо-западное направление можно попасть с пути A , на юго-западное направление можно попасть с пути B или C . Пусть пригородные поезда могут останавливаться только на 1, 3, 7, 8, 11, 12, 13 путях, а поезда дальнего следования и грузовые поезда могут останавливаться или проезжать через вокзал только по путям 1, 3, 4, 5, 6, 7, 8. Пусть имеется расписание движения поездов за май и август. Заполним таблицы с данными,

необходимыми для применения алгоритма вычисления вероятности.

Рассмотрим пассажирский поезд 255Н, проследующий станцию без остановки, с северо-восточного направления на северо-западное, причем известно, что этот поезд будут пропускать только по первому пути. В этом случае у него имеется только 6 маршрутов передвижения через станцию.

Вычислим вероятность проезда запрещающего сигнала маневровой группой, которая зависит от вероятности $P_{\text{двое}}$ того, что в локомотиве находится машинист и его помощник, а также от вероятностей $P_{\text{м(двое)}}$ и $P_{\text{м(один)}}$ того, что маневровая группа пересечет стрелочный перевод на запрещающий сигнал светофора, когда в кабине локомотива находится машинист и его помощник и когда в кабине находится только один машинист (см. пункт 4 алгоритма)

$$P_M = P_{\text{двое}} \cdot P_{\text{м(двое)}} + (1 - P_{\text{двое}}) \cdot P_{\text{м(один)}} = 0,8 \cdot 7 \cdot 10^{-9} + (1 - 0,8) \cdot 2,1 \cdot 10^{-8} \approx 10^{-8}.$$

Вероятность нарушения безопасности движения машинистом маневрового локомотива в режиме «подтягивание» равна (см. пункт 4 алгоритма)

$$P_T = \frac{1}{2} P_d(s)(P_{\text{тл}} + P_{\text{тх}}) = \frac{1}{2} \cdot 10^{-2} \cdot (10^{-4} + 10^{-3}) = 5,5 \cdot 10^{-6},$$

вероятность нарушения безопасности движения машинистом маневрового локомотива после сцепки с

Таблица 1. Блок данных, описывающий топологию станции и маневровые работы на ней

Наименование	Обозначение	Количество	Единицы измерения
Общее количество стрелок на станции	N	102	шт
Количество маневровых локомотивов	L	2	шт
Количество проезжаемых стрелок маневровой группой в час с локомотивом №1	N_1	36	шт,
Количество проезжаемых стрелок маневровой группой в час с локомотивом №2	N_2	36	шт
Средняя длина маневровой группы	l_m	0,2	км
Средняя скорость движения маневровой группы по станции	v_m	4,2	км/ч
Вероятность проезда машинистом маневрового локомотива светофора с запрещающим показанием при работе без помощника машиниста	$P_{\text{м(один)}}$	$2,1 \cdot 10^{-8}$	
Вероятность проезда машинистом маневрового локомотива светофора с запрещающим показанием при работе с помощником машиниста	$P_{\text{м(двое)}}$	$7 \cdot 10^{-9}$	
Вероятность комплектования локомотивной бригады маневрового локомотива машинистом и его помощником	$P_{\text{двое}}$	0,8	
Интенсивность останавливающихся на стрелочных переводах маневровых групп, не нарушивших при пересечении стрелки безопасности движения	$\lambda_{\text{с}}^1$..., $\lambda_{\text{с}}^{102}$	0, ..., 0	1/ч, ..., 1/ч
Среднее время нахождения на стрелочном переводе маневровой группы, не нарушившей при пересечении стрелки безопасности движения, при условии остановки на стрелочном переводе	$\tau_{\text{с}}^1$..., $\tau_{\text{с}}^{102}$	0, ..., 0	ч, ..., ч

отключенным режимом «сцепка» равна (см. пункт 4 алгоритма)

$$P_{\text{сц}} = \left(1 - \frac{1}{2} P_{\text{вм}}\right) P_{\text{м}} + \frac{1}{2} P_{\text{вм}} P_{\text{сцх}} =$$

$$= \left(1 - \frac{1}{2} \cdot \frac{1}{4}\right) \cdot 10^{-8} + \frac{1}{2} \cdot \frac{1}{4} \cdot 10^{-3} \approx 1,25 \cdot 10^{-4}.$$

Интенсивность нахождения маневровой группы в режиме «подтягивание» перед произвольной стрелкой равна (см. пункт 4 алгоритма)

$$\tilde{\lambda}_t = \sum_{l=1}^L \frac{1}{N} \cdot \frac{T_l}{24} = \frac{1}{102} \cdot \frac{3}{24} + \frac{1}{102} \cdot \frac{3}{24} = 0,0025 \text{ (1/ч)},$$

интенсивность пересечения произвольной стрелки маневровой группой после сцепки с отключенным режимом «сцепка» равна (см. пункт 4 алгоритма)

$$\tilde{\lambda}_{\text{сц}} = \sum_{l=1}^L \frac{N_l}{N} \cdot \frac{s_l}{r_l} = \frac{36}{102} \cdot \frac{2}{20} + \frac{36}{102} \cdot \frac{0}{22} = 0,035,$$

интенсивность пересечения стрелки маневровой группой в «обычном» режиме равна (см. пункт 4 алгоритма)

$$\tilde{\lambda}_m = \sum_{l=1}^L \frac{N_l}{N} - \tilde{\lambda}_t P_t - \tilde{\lambda}_{\text{сц}} = \frac{36}{102} + \frac{36}{102} -$$

$$- 0,0025 \cdot 5,5 \cdot 10^{-6} - 0,035 = 0,671.$$

Вычислим вероятность хотя бы одного столкновения на маршруте R_1 . Вероятность $P(R_1)$ использования маршрута R_1 равна (см. пункт 8 алгоритма)

$$P(R_1) = \frac{2}{2+1+0+0+0+0} = \frac{2}{3}.$$

Присвоим номера стрелкам согласно порядку их прохождения поездом (см. пункт 9 алгоритма): 115→1, 121→2, 151-147→3, 149-161→4, 244→5, 238→6, 236→7, 174→8, 164→9, 154→10, 144→11, 138→12.

Для стрелок №144, 236, 149-161, 151-147 имеем $\lambda_m = \tilde{\lambda}_m / 4 \approx 0,168$, $\lambda_t = \tilde{\lambda}_t / 4 \approx 0,0006$, $\lambda_{\text{сц}} = \tilde{\lambda}_{\text{сц}} / 4 \approx 0,009$ где деление на 4 проводится, так как у каждой маневровой группы есть 4 возможных направления для пересечения стрелочного перевода (см. рисунок 1).

Вероятность столкновения на неизолированных стрелках №144, 236, 149-161, 151-147 вычисляется по формулам (см. пункт 11 алгоритма)

Таблица 2. Блок дополнительных данных, описывающих топологию станции и маневровые работы на ней

Наименование	Обозначение	Количество	Единицы измерения
Количество полурейсов, совершенных локомотивом №1	r_1	20	шт
Количество полурейсов, совершенных локомотивом №2	r_2	22	шт
Количество сцепок с отключенным режимом сцепка, совершенных локомотивом №1	s_1	2	шт
Количество сцепок с отключенным режимом сцепка, совершенных локомотивом №2	s_2	0	шт
Количество подтягиваний, совершенных локомотивом №1	T_1	3	шт
Количество подтягиваний, совершенных локомотивом №2	T_2	3	шт
Длина маневрового локомотива (вагона)	l_t	0,2	км
Средняя скорость движения маневровой группы по станции в режиме «подтягивание»	v_t	2	км/ч
Среднее время освобождения маневровой группой стрелочного перевода при попадании на него в режиме «подтягивание» после остановки на этом переводе	τ_t	0,01	ч
Вероятность сцепки с последующим движением маневрового локомотива вместе с вагонами	$P_{\text{вм}}$	0,25	
Вероятность непредотвращения дежурным по станции проследования машинистом маневрового локомотива запрещающего сигнала светофора в режиме «подтягивание»	$P_d^1(s)$	10^{-2}	
Вероятность проезда запрещающего сигнала машинистом маневрового локомотива в режиме «подтягивание», когда маневровый локомотив находится в голове поезда	$P_{\text{тл}}$	10^{-4}	
Вероятность проезда запрещающего сигнала машинистом маневрового локомотива в режиме «подтягивание», когда маневровый локомотив находится в хвосте поезда	$P_{\text{тх}}$	10^{-3}	
Вероятность нарушения безопасности движения составителем	$P_{\text{сцх}}$	10^{-3}	

$$\begin{aligned}
 P_M(A_{1:3}) &= \lambda_m \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} \right) (P_m(1 + P_n) + P_n) + \\
 &+ \lambda_{cu} \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} \right) (P_{cu}(1 + P_n) + P_n) + \lambda_t \left(\frac{l_n}{v_n} + \frac{l_t}{v_t} + \tau_t \right) \cdot \\
 &\cdot P_t(1 + P_n) + \lambda_c P_n \tau_c + (\lambda_m P_m + \lambda_t P_t + \lambda_{cu} P_{cu}) P_{nc} \tau_{nc} = \\
 &= 0,168 \cdot \left(\frac{0,48}{42} + \frac{0,2}{4,2} \right) \cdot (10^{-8} \cdot (1 + 10^{-7}) + 10^{-7}) + \\
 &+ 0,009 \cdot \left(\frac{0,48}{42} + \frac{0,2}{4,2} \right) \cdot (1,25 \cdot 10^{-4} \cdot (1 + 10^{-7}) + 10^{-7}) + \\
 &+ 0,0006 \cdot \left(\frac{0,48}{42} + \frac{0,02}{2} + 0,01 \right) \cdot 5,5 \cdot 10^{-6} \cdot (1 + 10^{-7}) = 6,8 \cdot 10^{-8}.
 \end{aligned}$$

$$\begin{aligned}
 P_M(A_{1:4}) &= P_M(A_{1:7}) = P_M(A_{1:11}) = 0,168 \cdot \left(\frac{0,48}{42} + \frac{0,2}{4,2} \right) \cdot \\
 &\cdot (10^{-8} \cdot (1 + 10^{-7}) + 10^{-7}) + 0,009 \cdot \left(\frac{0,48}{42} + \frac{0,2}{4,2} \right) \cdot \\
 &\cdot (1,25 \cdot 10^{-4} \cdot (1 + 10^{-7}) + 10^{-7}) + 0,0006 \cdot \\
 &\cdot \left(\frac{0,48}{42} + \frac{0,02}{2} + 0,01 \right) \cdot 5,5 \cdot 10^{-6} \cdot (1 + 10^{-7}) = 6,8 \cdot 10^{-8}.
 \end{aligned}$$

Для изолированных стрелок 138, 154, 164, 174, 238, 244, 121, 115 вероятность столкновения на них равна нулю, то есть

$$\begin{aligned}
 P_M(A_{1:1}) &= P_M(A_{1:2}) = P_M(A_{1:5}) = P_M(A_{1:6}) = \\
 &= P_M(A_{1:8}) = P_M(A_{1:9}) = P_M(A_{1:10}) = P_M(A_{1:12}) = 0.
 \end{aligned}$$

Вероятность хотя бы одного столкновения пассажирского поезда №255Н на маршруте R_1 равна (см. пункт 14 алгоритма)

$$\begin{aligned}
 P_M(A_1 | R_1) &= 1 - 1 \cdot 1 \cdot (1 - 6,8 \cdot 10^{-8}) \cdot (1 - 6,8 \cdot 10^{-8}) \cdot \\
 &\cdot 1 \cdot 1 \cdot (1 - 6,8 \cdot 10^{-8}) \cdot 1 \cdot 1 \cdot (1 - 6,8 \cdot 10^{-8}) \cdot 1 = 2,7 \cdot 10^{-7}.
 \end{aligned}$$

Вычислим вероятность хотя бы одного столкновения на маршруте R_2 . Вероятность $P(R_2)$ использования маршрута R_2 равна (см. пункт 8 алгоритма)

$$P(R_2) = \frac{1}{2 + 1 + 0 + 0 + 0 + 0} = \frac{1}{3},$$

Для стрелок №144, 236, 149-161, 151-147 имеем $\lambda_m = \tilde{\lambda}_m / 4 \approx 0,168$, $\lambda_t = \tilde{\lambda}_t / 4 \approx 0,0006$, $\lambda_{cu} = \tilde{\lambda}_{cu} / 4 \approx 0,009$.

Присвоим номера стрелкам согласно порядку их прохождения поездом (см. пункт 9 алгоритма): 115→1, 121→2, 151-147→3, 149-161→4, 244→5, 238→6, 236→7, 176→8, 144→9, 138→10.

Вероятность столкновения на неизолированных стрелках №144, 236, 149-161, 151-147 вычисляется по формулам (см. пункт 11 алгоритма)

$$\begin{aligned}
 P_M(A_{2:3}) &= \lambda_m \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} \right) (P_m(1 + P_n) + P_n) + \lambda_{cu} \left(\frac{l_n}{v_n} + \frac{l_m}{v_m} \right) \cdot \\
 &\cdot (P_{cu}(1 + P_n) + P_n) + \lambda_t \left(\frac{l_n}{v_n} + \frac{l_t}{v_t} + \tau_t \right) P_t(1 + P_n) + \lambda_c P_n \tau_c + \\
 &+ (\lambda_m P_m + \lambda_t P_t + \lambda_{cu} P_{cu}) P_{nc} \tau_{nc} = 0,168 \cdot \left(\frac{0,48}{42} + \frac{0,2}{4,2} \right) \cdot \\
 &\cdot (10^{-8} \cdot (1 + 10^{-7}) + 10^{-7}) + 0,009 \cdot \left(\frac{0,48}{42} + \frac{0,2}{4,2} \right) \cdot \\
 &\cdot (1,25 \cdot 10^{-4} \cdot (1 + 10^{-7}) + 10^{-7}) + 0,0006 \cdot \left(\frac{0,48}{42} + \frac{0,02}{2} + 0,01 \right) \cdot \\
 &\cdot 5,5 \cdot 10^{-6} \cdot (1 + 10^{-7}) = 6,8 \cdot 10^{-8}.
 \end{aligned}$$

$$\begin{aligned}
 P_M(A_{2:4}) &= P_M(A_{2:7}) = P_M(A_{2:9}) = 0,168 \cdot \left(\frac{0,48}{42} + \frac{0,2}{4,2} \right) \cdot \\
 &\cdot (10^{-8} \cdot (1 + 10^{-7}) + 10^{-7}) + 0,009 \cdot \left(\frac{0,48}{42} + \frac{0,2}{4,2} \right) \cdot \\
 &\cdot (1,25 \cdot 10^{-4} \cdot (1 + 10^{-7}) + 10^{-7}) + 0,0006 \cdot \\
 &\cdot \left(\frac{0,48}{42} + \frac{0,02}{2} + 0,01 \right) \cdot 5,5 \cdot 10^{-6} \cdot (1 + 10^{-7}) = 6,8 \cdot 10^{-8}.
 \end{aligned}$$

Для изолированных стрелок 138, 176, 238, 244, 121, 115 вероятность столкновения на них равна нулю, то есть

$$\begin{aligned}
 P_M(A_{2:1}) &= P_M(A_{2:2}) = P_M(A_{2:5}) = P_M(A_{2:6}) = \\
 &= P_M(A_{2:8}) = P_M(A_{2:10}) = 0.
 \end{aligned}$$

Вероятность хотя бы одного столкновения пассажирского поезда №255Н равна (см. пункт 14 алгоритма)

$$\begin{aligned}
 P_M(A_1 | R_2) &= 1 - 1 \cdot 1 \cdot (1 - 6,8 \cdot 10^{-8}) \cdot (1 - 6,8 \cdot 10^{-8}) \cdot \\
 &\cdot 1 \cdot 1 \cdot (1 - 6,8 \cdot 10^{-8}) \cdot 1 \cdot (1 - 6,8 \cdot 10^{-8}) \cdot 1 = 2,7 \cdot 10^{-7}.
 \end{aligned}$$

Вероятность использования маршрутов R_3 , R_4 , R_5 , R_6 равна нулю (см. пункт 8 алгоритма), поскольку

$$P(R_3) = P(R_4) = P(R_5) = P(R_6) = \frac{0}{2 + 1 + 0 + 0 + 0 + 0} = 0.$$

Поэтому вероятности $P_M(A_1 | R_3)$, $P_M(A_1 | R_4)$, $P_M(A_1 | R_5)$, $P_M(A_1 | R_6)$ хотя бы одного столкновения на этих маршрутах можно не считать.

Вероятность хотя бы одного столкновения пассажирского поезда 255Н при проезде через станцию составляет (см. пункт 17 алгоритма)

$$\begin{aligned}
 P_M(A_1) &= \sum_{k=1}^K P_M(A_1 | R_k) P(R_k) = \sum_{k=1}^6 P_M(A_1 | R_k) P(R_k) = \\
 &= 2,7 \cdot 10^{-7} \cdot \frac{2}{3} + 2,7 \cdot 10^{-7} \cdot \frac{1}{3} = 2,7 \cdot 10^{-7}.
 \end{aligned}$$

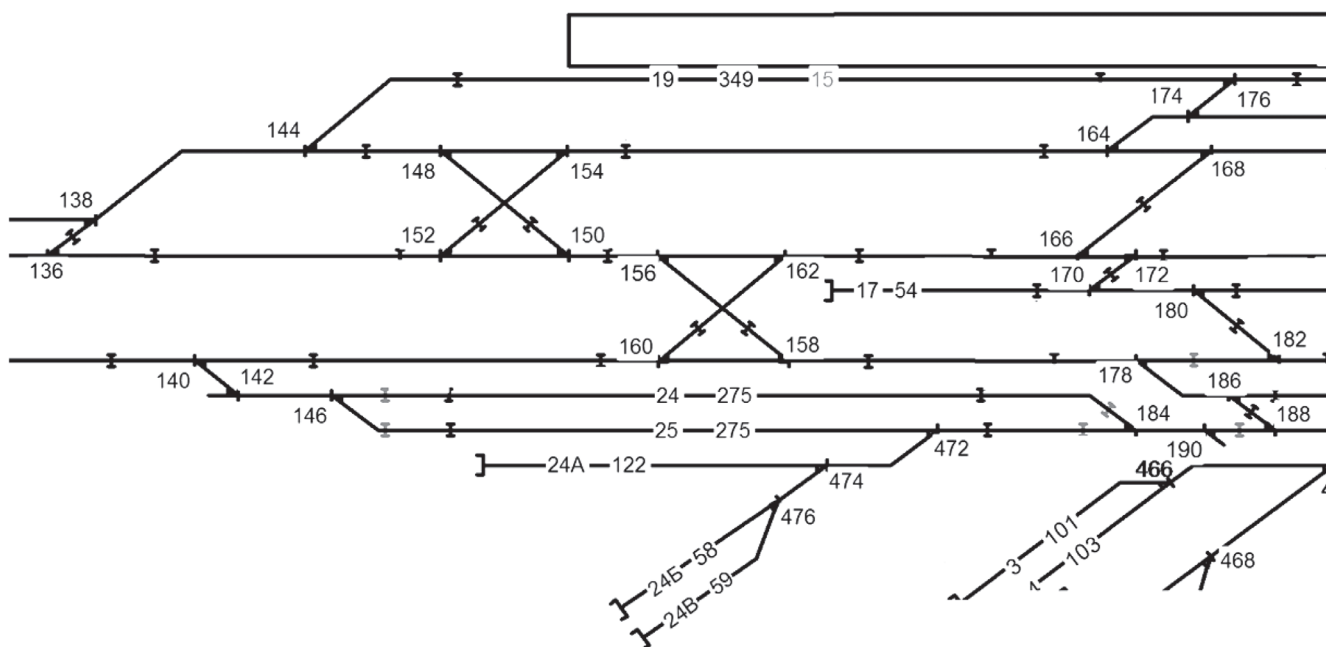


Рисунок 2 – Схема станции, для которой производится расчет вероятности столкновения

Вычислим теперь вероятность хотя бы одного столкновения для некоторой станции с установленной системой МАЛС за год.

Пусть для всех поездов, неизвестны прошлые проезды через станцию. Тогда вероятность хотя бы одного столкновения пассажирских поездов, проследующих станцию без остановки, с маневровой группой за май составляет

$$P_M(A_{\text{май}}) = 0,00002.$$

Вероятность хотя бы одного столкновения пассажирских поездов, проследующих станцию без остановки, с маневровой группой за август составляет

$$P_M(A_{\text{август}}) = 0,00008.$$

Интенсивность движения поездов в августе является пиковой, т.е. в остальные месяцы вероятность хотя бы одного столкновения будет меньше. Это предположение подтверждается анализом расписания движения. Отсюда получаем, что вероятность хотя бы одного столкновения за год оценивается величиной

$$P_M(A_{\text{год}}) = 1 - (1 - 0,00008)^{12} = 0,00096$$

В случае использования системы МАЛС на станции наибольшее влияние на вероятность хотя бы одного столкновения пассажирского поезда, проезжающего через станцию, оказывает слагаемое, связанное со сцепкой. Это объясняется тем, что вероятность проезда маневровой группой светофора с запрещающим показанием при сцепке с отключенным режимом

«сцепка» оказывается больше, нежели чем в режиме «подтягивание» или при проведении остальных маневровых работ. Если же рассматривается грузовой поезд, то на вероятность его столкновения с маневровой группой наибольшее влияние оказывает слагаемое, не связанное со сцепкой или подтягиванием. Это связано с высокой вероятностью проезда запрещающего сигнала машинистом грузового состава. При этом вероятность хотя бы одного столкновения пассажирского поезда ожидаемо меньше, чем вероятность хотя бы одного столкновения грузового поезда. Это связано и с тем, что вероятность проезда запрещающего сигнала машинистом грузового поезда на два порядка выше, чем вероятность проезда запрещающего сигнала машинистом маневрового поезда, и с тем, что грузовые поезда длиннее пассажирских, а значит, большее время будут находиться на стрелочном переводе, следовательно, большее время будет возможность столкновения.

Если сравнить полученную вероятность хотя бы одного столкновения в течение года с аналогичной вероятностью, полученной в [2] для маневровых локомотивов без использования системы МАЛС, то эта вероятность оказывается на порядок меньше.

6. Заключение

В статье рассмотрены вопросы оценки рисков столкновения на железнодорожной станции, на которой маневровые локомотивы могут быть оборудованы системой МАЛС. Основное внимание уделено методике расчёта вероятности столкновения пассажирских поездов с маневровыми составами на железнодорожной

станции, основанной на интенсивностях движения маневровых составов и конкретного расписания движения пассажирских поездов. Использование системы МАЛС для железнодорожной станции позволяет существенно уменьшить вероятность столкновения в течение года.

Библиографический список

1. ГОСТ Р 33433–2015 «Безопасность функциональная. Управление рисками на железнодорожном транспорте».
2. Игнатов А.Н., Кибзун А.И., Платонов Е.Н. Оценка вероятности столкновения железнодорожных составов // *Автоматика и телемеханика*, №11. 2016. С. 43—59.
3. Шубинский И.Б., Замышляев А.М., Игнатов А.Н., Кан Ю.С., Кибзун А.И., Платонов Е.Н. Оценка рисков, связанных с проездом запрещающего сигнала светофора маневровым составом или пассажирским поездом // *Надежность*. 2016. № 3. С. 39-46.
4. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа, Ульяновск: Областная типография «Печатный двор», 2012.

Сведения об авторах

Игорь Б. Шубинский – доктор технических наук, профессор, директор ЗАО «ИБ Транс», Москва, Россия, тел. +7 (495) 786-68-57, e-mail: igor-shubinsky@yandex.ru

Алексей М. Замышляев – доктор технических наук, заместитель Генерального директора ОАО «НИИ-АС», Москва, Россия, тел. +7 (495) 967-77-02, e-mail: A.Zamyshlaev@gismps.ru

Алексей Н. Игнатов – Московский Авиационный институт, аспирант, Москва, Россия, тел. +7 (906) 059 50 00, alexei.ignatov1@gmail.com

Андрей И. Кибзун – доктор физико-математических наук, профессор, Московский Авиационный институт, заведующий кафедрой, Москва, Россия, тел. +7 (499) 158-45-60, e-mail: kibzun@mail.ru

Евгений Н. Платонов – кандидат физико-математических наук, доцент, Московский Авиационный институт, факультет «Прикладной математики и физики», доцент, Москва, Россия, тел. +7 (499) 158-45-60, e-mail: en.platonov@gmail.com

Поступила 17.03.2017

Состояние и перспективы развития нормативного обеспечения в области функциональной безопасности

Александр Ф. Колчин, ООО «Корпоративные электронные системы», Россия, Москва

Олег С. Якимов, ФБУ «КВФ «Интерстандарт», Россия, Москва

Резюме. Цель. Познакомить читателя с состоянием и перспективами развития нормативного обеспечения в области функциональной безопасности в Российской Федерации. Так как второй по важности характеристикой любой продукции, услуги или процесса после характеристики назначения является характеристика ее безопасности, то для достижения безопасности объектов промышленности, транспорта, энергетики, связи, критически важных объектов, зданий и сооружений, объектов городской инфраструктуры, а также машин и оборудования, транспортных средств, повсеместно применяют связанные с безопасностью системы (СБ-системы). К сожалению, технологии создания СБ-систем после 80-х годов прошлого столетия пока еще не получили в Российской Федерации должного развития. В результате применяется консервативный подход, в котором часто используются избыточные требования, что увеличивает стоимость создаваемых систем обеспечения безопасности, но который, как правило, не гарантирует предъявляемые к ним требования. В настоящее время в мире главной характеристикой СБ-систем признана функциональная безопасность (ФБ) – вероятность успешного выполнения для этой системы функции или функций безопасности при заданных условиях в заданных интервалах времени. **Методы.** Реализация, дальнейшее развитие и практическое использование методологии ФБ в мире основано на разработке и применении большого количества нормативных документов на международном, региональном и национальном уровнях, которые позволяют организовать и выполнять работы по оценке и подтверждению соответствия требованиям ФБ для широкой номенклатуры СБ-систем. С целью научнометодологической поддержки и координации работ по формированию нормативной базы в области ФБ в Российской Федерации в соответствии с национальным стандартом ГОСТ Р 1.1-2013 «Стандартизация в Российской Федерации. Технические комитеты по стандартизации. Правила создания и деятельности» создан и активно работает технический комитет по стандартизации ТК 058 «Функциональная безопасность», в рамках которого разработано около 50 стандартов в области ФБ. Деятельность по стандартизации ТК 058 проводится в рамках реализации Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». **Выводы.** Так как в Российской Федерации определенная нормативная база в области ФБ уже сформирована, а на рынке появился спрос на услуги по оценке и подтверждению соответствия систем требованиям ФБ, то основной задачей сегодня является разработка на основе национальных и международных требований организационной и нормативно-методической документации, обеспечивающей в стране функционирование полноценной инфраструктуры, реализующей национальный институт подтверждения соответствия систем требованиям ФБ. Это позволит не только резко снизить риск катастроф и аварий, но и существенным образом повысить конкурентоспособность российской продукции на отечественном и зарубежном рынках.

Ключевые слова: функциональная безопасность, нормативное обеспечение, стандартизация, уровень полноты безопасности, сертификация, оценка соответствия

Формат цитирования: Колчин А.Ф., Якимов О.С. Состояние и перспективы развития нормативного обеспечения в области функциональной безопасности // Надежность. 2017. №3. С. 58-62. DOI: 10.21683/1729-2646-2017-17-3-58-62

Введение

Все, что создает человек для удовлетворения своих потребностей, в принципе ОПАСНО (для человека и окружающей среды). Поэтому создание любого объекта должно включать в себя выявление и анализ опасностей, которые связаны с этим объектом. Таким образом, вместе с обеспечением наличия требуемых функций у создаваемого объекта человек должен на всех этапах жизненного цикла этого объекта решать задачу обеспечения правильного безопасного функциониро-

вания (поведения) этого создаваемого объекта с учетом взаимосвязей различных систем объекта между собой и окружением.

По этой причине второй по важности характеристикой любой продукции, услуги или процесса после характеристики назначения является характеристика ее безопасности.

Для достижения безопасности объектов промышленности, транспорта, энергетики, связи, критически важных объектов, зданий и сооружений, объектов городской инфраструктуры, а также машин и оборудования, транс-

портных средств, повсеместно применяют связанные с безопасностью системы (СБ-системы).

К сожалению, технологии создания СБ-систем после 80-х годов прошлого столетия пока еще не получили в Российской Федерации должного развития. Их основные недостатки следующие:

1. Отечественные разработчики и производители СБ-систем, проектные и строительные организации, за редким исключением, предпочитают использовать в своей работе прежние устаревшие нормативные документы, основанные на предписывающем подходе, выполнение требований которых не гарантирует работоспособность этих систем в период их эксплуатации и, соответственно, не гарантирует безопасность объектов, на которых эти системы установлены.

2. СБ-системы и их подсистемы рассматриваются как автономные независимые единицы продукции (вещь в себе), а их опасность/безопасность оценивается без учета взаимосвязей их составляющих между собой и окружением.

В результате применяется консервативный подход, в котором часто используются избыточные требования, что увеличивает стоимость создаваемых систем обеспечения безопасности, но который, как правило, не гарантирует предъявляемые к ним требования.

В настоящее время в мире главной характеристикой СБ-систем признана функциональная безопасность (ФБ) – вероятность успешного выполнения для этой системы функции или функций безопасности при заданных условиях в заданных интервалах времени.

Представленная в комплексе стандартов ГОСТ Р МЭК 61508 методология ФБ:

1. Использует единый (независимый от отрасли) системный комплексный процессный подход и направлена на выявление, предотвращение и ослабление последствий всех безопасных отказов, опасных выявляемых событий, а также разумно предсказуемых опасных событий и редко встречающихся опасных событий, которые могут привести к катастрофическим последствиям, в сложных технических системах.

2. Вводит единую меру оценки безопасности – уровень полноты безопасности (Safety Integrity Level, SIL), который представляется и оценивается в величинах неприемлемого риска причинения вреда людям, имуществу, окружающей среде. В методологии ФБ предусмотрен регулярный итерационный процесс анализа опасностей и риска, общей оценки риска и принятия мер по снижению риска, который осуществляется на всех стадиях жизненного цикла СБ-систем, а также прописываются действия всех лиц, влияющих на безопасность на этих стадиях.

3. Распространена по всему миру, активно используется в промышленно развитых странах, и ее применение регламентируют уже более 200 международных, региональных и межгосударственных стандартов в различных отраслях промышленности.

Дальнейшее развитие и практическое использование методологии ФБ в мире сопровождается разработкой

и применением большого количества нормативных документов на международном, региональном и национальном уровнях, которые позволяют организовать и выполнять работы по оценке и подтверждению соответствия требованиям ФБ для широкой номенклатуры СБ-систем.

Хотя в Российской Федерации ряд исследователей проблемами ФБ занимается уже более 20 лет, широкий круг инженерно-технических специалистов познакомился с практическим применением методологии ФБ после издания в Российской Федерации уже хорошо известных работ Дэвида Дж. Смита и Кеннета Дж. Л. Симпсона [1, 2] и выпуска в 2007 г. первой редакции базового стандарта по ФБ ГОСТ Р МЭК 61508–2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Части 1–7».

С целью научно-методологической поддержки и координации работ по формированию в Российской Федерации нормативной базы в области ФБ в соответствии с национальным стандартом ГОСТ Р 1.1-2013 «Стандартизация в Российской Федерации. Технические комитеты по стандартизации. Правила создания и деятельности» был создан и в дальнейшем реструктурирован технический комитет по стандартизации ТК 058 «Функциональная безопасность». Кроме этого, в настоящее время в работе по созданию отечественной нормативной базы в области ФБ принимают участие также несколько других смежных национальных технических комитетов по стандартизации ведущих отраслей промышленности.

Деятельность по стандартизации ТК 058 проводится в рамках реализации Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации».

ТК 058 создан на основе принципа добровольности участия.

ТК создан для сотрудничества заинтересованных организаций и органов власти при проведении работ по национальной, межгосударственной и международной стандартизации в области ФБ.

Основными задачами ТК в области стандартизации в сфере ФБ являются:

- формирование ежегодных программ национальной стандартизации и контроль за реализацией этих программ;

- рассмотрение предложений по применению международных и региональных стандартов на национальном и межгосударственном уровнях;

- проведение научно-технической, правовой и нормативной экспертиз проектов национальных и межгосударственных стандартов и проектов изменений к действующим стандартам, также представление их для принятия в федеральный орган исполнительной власти в сфере стандартизации;

Далее кратко рассмотрены полученные за последние 10 лет результаты этой деятельности.

Действующие в РФ стандарты в области ФБ

Особое внимание в работе ТК 058 было уделено подготовке 2-й редакции базового стандарта МЭК 61508–2010, а также основополагающих стандартов по ФБ для различных отраслей. В результате в 2012 году был подготовлен комплекс стандартов ГОСТ Р МЭК 61508–2010 [3–9].

В настоящее время на ряде предприятий нефтехимической и газовой отраслей, а также электроэнергетики, которые для обеспечения безопасности различных промышленных процессов применяют приборные системы безопасности, активно используется комплекс МЭК 61511 [10–12].

Для строительной отрасли были введены прямым применением несколько международных стандартов, а также на базе МЭК 61508 были разработаны национальные стандарты по ФБ [13–19]. На основе этих нормативных документов уже разработано несколько стандартов организаций для строительной отрасли.

Большое внимание в Российской Федерации уделяется реализации методологии ФБ на железнодорожном транспорте. В ОАО «РЖД» разработано и применяется достаточно большое количество стандартов организаций для обеспечения гарантированной безопасности и надежности перевозочного процесса в холдинге «РЖД». В настоящее время в железнодорожной отрасли действует большое число национальных и межгосударственных стандартов в области ФБ, некоторые из которых представлены в [20–23].

В области атомного энергомашиностроения подготовлено несколько стандартов, посвященных созданию систем контроля и управления для различных разрабатываемых в отрасли изделий, удовлетворяющих требованиям ФБ [24–32].

Проблемы ФБ машин и механизмов рассмотрены в нормативных документах [33–36].

Реализация методологии ФБ для систем управления дорожно-транспортных средств представлена в [37–47].

Общие принципы реализации требований серии стандартов МЭК 61508 к передаче данных, связанных с безопасностью, включая возможные сбои передачи данных, меры по устранению неисправности и сообщения, влияющие на целостность данных, в промышленных сетях связи можно найти в [48–53].

Требования помехоустойчивости для систем безопасности и оборудования, предназначенного для выполнения функций, связанных с безопасностью, представлены в [54, 55].

В [56] рассмотрены требования ФБ к программируемым контроллерам.

В настоящее время ТК 058 разработаны и готовятся к утверждению еще 4 стандарта по ФБ, в том числе подготавливается 2-я редакция МЭК 61511–2016.

От стандартизации к оценке соответствия

Сегодня поставить за рубеж сложную техническую систему либо ее компоненты без подтвержденной оценки соответствия заданному для нее уровню полноты безопасности практически невозможно. Да и почти любые поставляемые в Российской Федерации сложные системы маркируются этим параметром, однозначно характеризующим их безопасность.

Поэтому в большинстве экономически развитых государств действуют органы по подтверждению соответствия (сертификации) сложного оборудования, промышленных объектов, систем и их компонентов требованиям ФБ с соответствующими структурами (испытательными лабораториями, центрами), обеспечивающими измерения, испытания, расчеты по оценке соответствия этим требованиям.

В России национальный институт подтверждения соответствия систем требованиям ФБ пока отсутствует, что не только резко увеличивает риск катастроф и аварий, но и существенным образом снижает конкурентоспособность российской продукции на отечественном и зарубежном рынках. Между тем все необходимые условия для создания такого института есть. Нормативная база существует и востребована, а также на рынке появился спрос на услуги по оценке и подтверждению соответствия систем требованиям ФБ.

Поэтому основной задачей сегодня является разработка на основе национальных и международных требований организационной и нормативно-методической документации, обеспечивающей в Российской Федерации функционирование инфраструктуры, реализующей национальный институт подтверждения соответствия систем требованиям ФБ.

В марте 2016 г. в едином реестре добровольных систем сертификации в Федеральном агентстве по техническому регулированию и метрологии зарегистрирована Система добровольной сертификации в области функциональной безопасности (регистрационный номер РОСС RU.31461.04ИДД0). Объектами сертификации в ней являются: системы, связанные с безопасностью (ССБ), их составные части, изделия для них, системы менеджмента функциональной безопасности организаций и/или их подразделений, осуществляющих разработку, производство и применение ССБ: анализ опасностей и рисков, проектирование, изготовление, установку и ввод в эксплуатацию, техническое обслуживание и ремонт, модернизацию, вывод из эксплуатации ССБ, инструментальные средства для разработки, производства и применения систем, связанных с безопасностью. Предполагается также аккредитация органа по сертификации в области ФБ и в Национальной системе добровольной сертификации Российской Федерации.

Библиографический список

1. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов / Дэвид Дж. Смит, Кеннет Дж. Л. Симпсон; [пер. с англ. Хвилевичкого Л. О., Серебрянского А. Я.]. – М.: Технологии, 2004 – 207с.
2. Безотказность, ремонтпригодность и риск. Практические методы для инженеров, включая вопросы оптимизации надежности и систем, связанных с безопасностью / Дэвид Дж. Смит; [пер. с англ. Хвилевичкого Л. О.]. – Москва: Группа ИДТ, 2007. – 431с.
3. ГОСТ Р МЭК 61508-1–2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования
4. ГОСТ Р МЭК 61508-2–2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам
5. ГОСТ Р МЭК 61508-3–2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению
6. ГОСТ Р МЭК 61508-4–2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения
7. ГОСТ Р МЭК 61508-5–2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности
8. ГОСТ Р МЭК 61508-6–2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3
9. ГОСТ Р МЭК 61508-7–2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства
10. ГОСТ Р МЭК 61511-1–2011 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования
11. ГОСТ Р МЭК 61511-2–2011 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1
12. ГОСТ Р МЭК 61511-3–2011 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности
13. ГОСТ Р ИСО/МЭК 14762–2013 Информационные технологии. Требования к функциональной безопасности электронных систем домов и зданий (ЭСДЗ)
14. ГОСТ Р 53195.1–2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения
15. ГОСТ Р 53195.2–2008 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 2. Общие требования
16. ГОСТ Р 53195.3–2015 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 3. Требования к системам
17. ГОСТ Р 53195.4–2010 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 4. Требования к программному обеспечению
18. ГОСТ Р 53195.5–2010 Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 5. Меры по снижению риска, методы оценки
19. ГОСТ Р ЕН 50491-4-1–2014 Общие требования к электронным системам жилых домов и общественных зданий (ЭСДЗ) и системам управления и автоматизации общественных зданий (СУАЗ). Часть 4-1. Общие требования к функциональной безопасности изделий, предназначенных для включения в ЭСДЗ и СУАЗ
20. ГОСТ Р 55980–2014 Управление рисками на железнодорожном транспорте. Классификация опасных событий
21. ГОСТ 33432–2015 Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта
22. ГОСТ 33433–2015 Безопасность функциональная. Управление рисками на железнодорожном транспорте
23. ГОСТ Р МЭК 62279–2016 Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах
24. ГОСТ Р МЭК 60880–2010 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А
25. ГОСТ Р МЭК 62138–2010 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С
26. ГОСТ Р МЭК 60987–2011 Атомные станции. Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения компьютеризованных систем
27. ГОСТ Р МЭК 61513–2011 Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования
28. ГОСТ Р МЭК 61225–2011 Атомные станции. Системы контроля и управления, важные для безопасности. Требования к электроснабжению
29. ГОСТ Р МЭК 61226–2011 Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления

30. ГОСТ Р МЭК 60709–2011 Атомные станции. Системы контроля и управления, важные для безопасности. Разделение.

31. ГОСТ Р МЭК 62340–2011 Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине

32. ГОСТ Р МЭК 61500–2012 Атомные станции. Системы контроля и управления, важные для безопасности. Передача данных в системах, выполняющих функции категории А.

33. ГОСТ Р МЭК 62061–2013 Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью

34. ГОСТ Р МЭК 61800-5-2–2015 Системы силовых электроприводов с регулируемой скоростью. Часть 5-2. Требования функциональной безопасности.

35. ГОСТ Р 60.1.2.1-2016 Роботы и робототехнические устройства. Требования по безопасности для промышленных роботов. Часть 1. Роботы

36. ГОСТ Р 60.1.2.2-2016 Роботы и робототехнические устройства. Требования по безопасности для промышленных роботов. Часть 2. Робототехнические системы и их интеграция

37. ГОСТ Р ИСО 26262-1–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 1. Термины и определения

38. ГОСТ Р ИСО 26262-2–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 2. Менеджмент функциональной безопасности

39. ГОСТ Р ИСО 26262-3–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 3. Стадия формирования концепции

40. ГОСТ Р ИСО 26262-4–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 4. Разработка изделия на уровне системы

41. ГОСТ Р ИСО 26262-5–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 5. Разработка аппаратных средств изделия

42. ГОСТ Р ИСО 26262-6–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 6. Разработка программного обеспечения изделия

43. ГОСТ Р ИСО 26262-7–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 7. Производство и эксплуатация

44. ГОСТ Р ИСО 26262-8–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 8. Вспомогательные процессы

45. ГОСТ Р ИСО 26262-9–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 9. Анализ уровня полноты безопасности автомобиля и анализ безопасности автомобиля

46. ГОСТ Р ИСО 26262-10–2014 Дорожные транспортные средства. Функциональная безопасность. Часть 10. Руководящие указания по ИСО 26262

47. ГОСТ Р 57300–2016/ISO/TS 15998-2:2012 Машины землеройные. Системы управления с использованием электронных компонентов. Часть 2. Применение ИСО 15998.

48. ГОСТ Р МЭК 61784-1-2016 Промышленные сети. Профили. Часть 1. Профили полевых шин

49. ГОСТ Р МЭК 61784-3-2015 Промышленные сети. Профили. Часть 3. Функциональная безопасность полевых шин. Общие правила и определения профилей

50. ГОСТ Р МЭК 61784-3-1-2016 Промышленные сети. Профили. Часть 3-1. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 1

51. ГОСТ Р МЭК 61784-3-3-2016 Промышленные сети. Профили. Часть 3-3. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 3

52. ГОСТ Р МЭК 61784-3-8-2016 Промышленные сети. Профили. Часть 3-8. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 8

53. ГОСТ Р МЭК 61784-3-12-2016 Промышленные сети. Профили. Часть 3-12. Функциональная безопасность полевых шин. Дополнительные спецификации для CPF 12

54. ГОСТ ИЕС 61326-3-1-2015 Электрическое оборудование для измерения, управления и лабораторного применения. Требования ЭМС. Часть 3-1. Требования помехоустойчивости для систем, связанных с безопасностью, и оборудования, предназначенного для выполнения функций, связанных с безопасностью (функциональная безопасность). Общие промышленные применения

55. ГОСТ ИЕС 61326-3-2-2015 Электрическое оборудование для измерения, управления и лабораторного применения. Требования ЭМС. Часть 3-2. Требования помехоустойчивости для систем, связанных с безопасностью, и оборудования, предназначенного для выполнения функций, связанных с безопасностью (функциональная безопасность). Промышленные применения с учетом определенной электромагнитной обстановки

56. ГОСТ Р МЭК 61131-6-2015 Программируемые контроллеры. Часть 6. Безопасность функциональная.

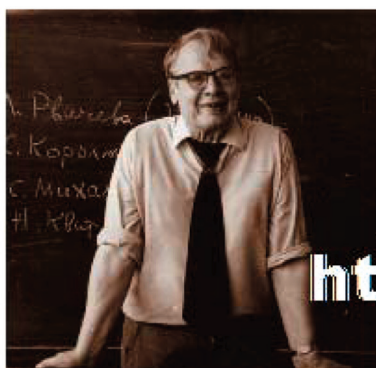
Сведения об авторах

Александр Ф. Колчин – заместитель генерального директора ООО «Корпоративные электронные системы», Россия, Москва, e-mail: kolchin@calscenter.ru

Олег С. Якимов – директор Департамента нормативного обеспечения ФБУ

«КВФ «Интерстандарт», председатель ТК 058 «Функциональная безопасность», Россия, Москва

Поступила 30.06.2017



<http://Gnedenko-Forum.org/>

Дорогие коллеги!

В 2005 году была основана неформальная Ассоциация специалистов по надежности, прикладной вероятности и статистике (I.G.O.R.), которая имеет свой сайт в Интернете GNEDENKO FORUM. Сайт назван в честь выдающегося математика Бориса Владимировича Гнеденко (1912-1995). Целью Форума является улучшение профессиональных и персональных контактов специалистов по математической статистике, теории вероятностей и их важных ветвей, как Теория надежности и контроля качества, Теория массового обслуживания, Теории управления запасами и т.п.

Начиная с января 2006 года Форум издает ежеквартальный Международный электронный журнал

«Надежность: Теория и приложения» (“Reliability: Theory & Applications”).

Журнал зарегистрирован в Библиотеке Конгресса США (ISSN 1932-2321). Все права сохраняются за авторами, так что статьи затем могут быть свободно опубликованы в любых других изданиях или представлены на конференции.



Вступайте в Форум
Гнеденко!

Добро

пожаловать!

В наших рядах уже более

500 специалистов

из **44** стран мира.

Для вступления в
Форум присылайте
фото и краткое резюме
по адресу:

к.т.н. Александр Бочков,
a.bochkov@gmail.com

Membership is free.

ТРЕБОВАНИЯ РЕДАКЦИИ ПО ОФОРМЛЕНИЮ СТАТЕЙ В ЖУРНАЛАХ ИЗДАТЕЛЬСКОЙ ГРУППЫ IDT PUBLISHERS

Письмо от организации, где работает автор(ы), либо лично от автора(ов) с предложением о публикации статьи направляется в редакцию журнала по фактическому адресу: 107078, г.Москва, Орликов переулок, д.5, офис 755 ООО «ЖУРНАЛ «НАДЕЖНОСТЬ» или по адресу e-mail: E.Patrikeeva@gismps.ru (в отсканированном виде).

К письму прилагается в электронном виде (на CD или по приведенному выше E-mail) текст статьи с аннотацией и ключевыми словами, информацией об авторах, с приставным библиографическим списком, предоставляется с одним комплектом рисунков

Внимание! Названия статьи, ФИО авторов, аннотация и ключевые слова обязательно представляются в соответствии с требованиями ВАК на русском и английском языках. Аннотация не менее 350 слов.

Информация о каждом авторе должна содержать следующие стандартные сведения:

- Фамилия, имя, отчество;
- Ученая степень, ученое звание, почетное звание;
- Членство в общественных союзах и т.д.;
- Место работы, должность;
- Перечень и номера журналов IDT Publishers, в которых ранее публиковались статьи автора;
- Сведения для контактов;
- Фотографии всех авторов статьи.

Текст необходимо набирать в редакторе Word 97-2003 шрифтом № 12; текст не форматируется. Абзацы организуются путем нажатия клавиши Enter. Текст статьи набирается через полтора интервала на странице формата A4; слева должно быть поле 2 см; страницы нумеруются, «красная строка» обязательна.

Все буквенные обозначения, приведенные на рисунках, необходимо пояснять в основном или подрисункном тексте. Недопустимы отличия в обо-

значениях на рисунках и в тексте. Нумеровать следует только те формулы и уравнения, на которые есть ссылка в тексте.

Непосредственно в тексте набираются простые формулы (например, m^2 ; n^2t , $C = 1 + DDF - A_2$), греческие буквы и символы, например, β , $\odot$ — шрифтом Symbol. То, что невозможно набрать непосредственно в текстовом редакторе, — с использованием редактора формул Microsoft Equation (входящего в комплект поставки Microsoft Office) или редактора формул MathType.

Не допускается представление текста, в котором формулы представлены в виде изображения.

Фотографии и рисунки к статьям предоставляются отдельными файлами с расширением TIF, или EPS или JPEG с разрешением не менее 300 dpi.

Список использованной литературы составляется в порядке цитирования и дается в конце статьи.

Ссылки на литературу в тексте отмечаются порядковыми цифрами в квадратных скобках.

Вниманию авторов, публикующихся в журналах IDT Publishers.

Представленная информация о каждом авторе помимо журнала будет размещаться на сайте techizdat.ru в разделе «Авторы» на отдельной интернет-странице.

Авторам также предоставляется возможность при публикации своих статей направить в редакцию свою электронную фотографию и дополнительные материалы для размещения их на этой индивидуальной Интернет-визитке. По своему усмотрению автор может рассказать более подробно о себе, об интересных примерах и историях решения технических проблем, о современных задачах - в соответствии с тематикой соответствующего журнала - и т.п. Желательный объем этого материала — не более 1000 знаков с пробелами.

ПОДПИСКА НА ЖУРНАЛ «НАДЕЖНОСТЬ»

Подписаться на журнал можно:

- Через агентство «Роспечать» — индекс 81733;

- По каталогу «Пресса России» агентства «Книга-Сервис» — индекс 11804;

- Через редакцию на любой срок
тел.: 8-916-105-81-31
e-mail: E.Patrikeeva@gismps.ru

НАДЁЖНОСТЬ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

ПРЕДСТАВЛЯЕТ

И.Б. ШУБИНСКИЙ

Надежные отказоустойчивые информационные системы

Методы синтеза



Приобрести издание можно через редакцию ООО «Журнал «Надежность»

8 (495) 967-77-05, доб.186
8-916-105-81-31
(Патрикеева Евгения)

E.Patrikeeva@gismps.ru,
www.dependability.pro

Шубинский Игорь Борисович

НАДЕЖНЫЕ ОТКАЗООУСТОЙЧИВЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ Методы синтеза

Подписано в печать 12.02.2016. Формат издания 70х100/16.
Печать офсетная. Бумага офсетная. Усл. печ. л. 17,55.
Тираж 700 экз. Заказ № 1452.

ООО «Журнал «Надежность»,
109029, г. Москва,
ул. Нижегородская, д.27, стр.1, офис 209
Тел./факс: +7 499 262 53 20
E-mail: E.Patrikeeva@gismps.ru

И.Б.Шубинский «Надежные отказоустойчивые информационные системы» 2016 г.

В книге приведены концептуальные положения обеспечения структурной и функциональной надежности информационных систем на всех этапах их жизненного цикла. Различные виды структурного резервирования рассмотрены с учетом ограничений в обнаружении отказов. При этих условиях оценена их эффективность и установлены предельные возможности структурного резервирования в предположении бесконечного количества резервных устройств. Рассмотрены способы обеспечения функциональной надежности программных средств, в том числе приведены рекомендации по разработке спецификации требований к программам, описана технология разработки архитектуры надежной программы, приведены хорошо апробированные правила и рекомендации по проектированию надежного программного обеспечения и его реализации, а также интеграции с аппаратными средствами системы.

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, а также результаты исследования надежности информационных систем с различными дисциплинами активной защиты. Оценена ее эффективность по отношению к традиционным методам структурного резервирования.

Рассмотрены принципы обеспечения функциональной безопасности информационных систем, обоснована возможность перезапуска независимых каналов в двухканальных безопасных системах, разработаны правила определения допустимого времени гарантированного обнаружения одиночных и двойных отказов, одиночных и двойных отказов, разработан метод синтеза комбинированной двухуровневой информационной системы, к которой предъявлены повышенные требования по функциональной безопасности.

Для подтверждения соответствия надежности и функциональной безопасности разработан метод ускоренных натурных испытаний информационной системы и приведен пример его практической реализации, развиты методики сертификационных испытаний по требованиям безопасности информации и декларирования соответствия программных средств.

В конце каждой главы содержатся контрольные вопросы по наиболее сложному и значимому материалу главы. Книга рассчитана, в первую очередь, на специалистов, занимающихся практической работой по разработке, производству, эксплуатации и модификации информационных систем. Она предназначена научным работникам в области структурной надежности различных дискретных систем, преподавательскому составу, аспирантам и студентам, специализирующимся в области информационных систем, а также в области автоматизированных систем управления.

Приобрести издание можно через редакцию журнала «Надежность»
по тел.: 8 (495) 967-77-05, доб.186; 8-916-105-81-31 (Патрикеева Евгения),
e-mail: E.Patrikeeva@gismps.ru, www.dependability.pro

ЗАЯВКА НА ПОДПИСКУ НА ЖУРНАЛ «НАДЕЖНОСТЬ»

с № _____ 20__ г. по № _____ 20__ г., количество экз. _____

Полное наименование организации	
Юридический адрес предприятия (индекс, страна, адрес)	
Почтовый адрес предприятия (индекс, страна, адрес)	
ИНН/КПП	
Расчетный счет	
Банк	
Корреспондентский счет	
БИК	
Контактное лицо: Ф.И.О., должность	
Телефон/факс, e-mail	

Реквизиты: ООО «Журнал «Надежность»

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

Тел./факс: (495) 967-77-02 , e-mail: E.Patrikeeva@gismps.ru

ИНН 7709868505 КПП 770901001

р/с 40702810100430000017

к/с 30101810100000000787

Адрес доставки:

Кому: _____

Куда: _____

Для оформления подписки на журнал «Надежность» заполните заявку и отправьте ее по факсу или электронной почте.

По всем вопросам, связанным с подпиской, обращайтесь в редакцию журнала.

Стоимость годовой подписки 4180-00 руб, в т.ч. НДС 10%.

Периодичность – 4 номера в год.

ЖУРНАЛ ИЗДАЕТСЯ ПРИ УЧАСТИИ И ПОДДЕРЖКЕ

ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ И ПРОЕКТНО-КОНСТРУКТОРСКИЙ ИНСТИТУТ ИНФОРМАТИЗАЦИИ, АВТОМАТИЗАЦИИ И СВЯЗИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ»
(ОАО «НИИАС»)



ОАО «НИИАС» – ведущее предприятие ОАО «РЖД» в области создания комплексов и систем обеспечения безопасности движения, управления движением, геоинформационного обеспечения, мониторинга состояния подвижного состава и инфраструктуры железных дорог



Цели:

- ☐ эффективность,
- ☐ безопасность
- ☐ надежность перевозок



Основные направления деятельности

- Интеллектуальные системы управления
- Технологии управления перевозками и транспортного обслуживания
- Системы автоматики и телемеханики
- Центры автоматизированного управления
- Информационные системы
- Геоинформационные системы и спутниковые технологии
- Системы транспортной безопасности
- Системы управления инфраструктурой
- Системы управления топливно-энергетическими ресурсами
- Испытания, сертификация и экспертиза
- Информационная безопасность
- Нормативно-правовое обеспечение



www.vniias.ru