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

ISSN 1729-2646
e-ISSN 2500-3909

УЧРЕДИТЕЛЬ ЖУРНАЛА:
ООО «Журнал «Надежность»

Зарегистрирован в Министерстве Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций. Регистрационное свидетельство ПИ № 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. Пушкарева, 27.

Подписано в печать 28.05.2018
Объем , Тираж 500 экз, Заказ №
Формат 60x90/8, 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 АКЦИОНЕРНОГО ОБЩЕСТВА «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ И ПРОЕКТНО-КОНСТРУКТОРСКИЙ ИНСТИТУТ ИНФОРМАТИЗАЦИИ, АВТОМАТИЗАЦИИ И СВЯЗИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ» (АО «НИИАС») И ООО «ИЗДАТЕЛЬСКИЙ ДОМ «ТЕХНОЛОГИИ»

СОДЕРЖАНИЕ

Надежность, том 18, №4, 2018
Оригинальная статья
DOI: 10.21683/1729-2646-2018-18-4-3-9

Адаптивная гарантоспособность информационных систем управления

Игорь Б. Шубинский, *АО «НИИАС», Москва, Россия*
Алексей М. Замышляев, *АО «НИИАС», Москва, Россия*
Любиша Р. Папич, *Исследовательский центр по управлению качеством и надежностью (DQM), Приевор, Сербия*

Игорь Б. Шубинский

Алексей М. Замышляев

Любиша Р. Папич

Резюме. *В статье рассматривается надежность информационной системы управления с позиции способности предоставлять требуемые услуги, которым можно оправданно доверять, т.е. ее гарантоспособность. Предполагается, что система функционирует без участия операторов. Задача состоит в обеспечении гарантоспособности мультимодульной системы управления в условиях воздействия на результаты решения задач отказов, сбоев и ошибок в решении задач вычислительными модулями (ВМ) системы. Применение традиционных методов обеспечения отказоустойчивости не обеспечивает желаемого эффекта, поскольку даже при бесконечной структурной избыточности, но при реальных возможностях оперативного обнаружения отказов или сбоев ВМ, гарантоспособность системы значительно ниже ожидаемой. В статье предложены и оценены способы адаптивной гарантоспособности. Назначение их состоит в реализации наблюдаемости систем управления при ограниченных возможностях контроля работоспособности составных ВМ и в достижения требуемых уровней гарантоспособности информационных систем управления в условиях незначительного резерва времени и структурной избыточности. Эти цели достигаются путем активного (и автоматического) переназначения имеющихся вычислительных ресурсов для оперативной обработки информации. Способы адаптивной грантоспособности позволяют без остановки вычислительных процессов при решении реальных задач осуществлять своевременное автоматическое обнаружение и устранение отказов, сбоев ВМ и ошибок в решении предусмотренных задач путем оперативной локализации неисправных модулей и последующей автоматической реконфигурации системы с выводом из процесса функционирования отказавших модулей.*

Ключевые слова: *вычислительные модули, гарантоспособность, адаптивная защита, отказы, сбои, ошибки в решении предусмотренных задач, автоматическая реконфигурация системы, контроль, допустимое время перерыва в работе, временная избыточность, циклы и такты защиты.*

Формат цитирования: *Шубинский И.Б., Замышляев А.М., Папич Л.Р. Адаптивная гарантоспособность информационных систем управления // Надежность. 2018. Т. 18, № 4. С. 3-9. DOI: 10.21683/1729-2646-2018-18-4-3-9*

1. Введение

1.1. Гарантоспособность информационных систем управления

Обеспечение надежности информационной техники находится в центре внимания всех специалистов, кто напрямую или косвенно связан с ее разработкой, производством и эксплуатацией. За все годы развития цифровой техники интенсивность отказов элементной базы уменьшилась на шесть порядков. В составе информационной системы тысячи таких цифровых элементов, каждый из которых представляет собой программно-аппаратные устройства, выполняющее множество различных функций.

Теперь уже центральной проблемой обеспечения надежности информационной системы становится безошибочное выполнение предусмотренных в системе функциональных задач, которые технически реализуются с помощью информационных процессов. Актуальность этой проблемы обусловлена тем, что частота ошибок в работе информационной системы и связанных с ними функциональных отказов значительно превышает частоту отказов цифровой техники, а сами функциональные отказы могут быть критичными для окружающей среды и объектов управления [1, 2 и др.].

В связи с этим ряд исследователей исходят из того, что необходимо изучать надежность выполнения информационных технологий как способность информационной системы поставлять обслуживание, которому можно доверять. *Обслуживание,* поставляемое системой, представляет ее свойства или поведение в том виде, в котором это воспринимается *пользователем*. В трактовке авторов данной работы обслуживание, которому можно доверять, расценивается как *общая надежность* [3].

В указанной работе [3] применены следующие понятия:

правильное или корректное обслуживание осуществляется, когда обслуживание реализует функцию (функции) системы;

отказ системы – событие отклонения осуществляемого обслуживания от правильного обслуживания, т.е.

отказ – это переход от правильного обслуживания к *неправильному обслуживанию*, когда не осуществляется функция системы.

Развитие данного подхода нашло отражение в материалах исследований рабочей группы WG 10.4 Международной Федерации (IFIP WG-10.4) по обработке информации [4]. Однако вместо термина «общая надежность» специалисты этой рабочей группы вводят термин *«гарантоспособность»*, которая в указанной работе рассматривается как «достоверность вычислительной системы, способной предоставлять требуемые услуги, которым можно *оправданно* доверять». Услуга – вид деятельности, работ, в процессе которых не создается новый материально-вещественный продукт, но изменяется качество уже имеющегося ранее созданного продукта. Само оказание услуги создает желаемый результат [5]. В явном виде гарантоспособность – это свойство *обслуживания* и зависит от характера использования системы.

1.2. Ограниченные возможности традиционных методов обеспечения гарантоспособности систем управления

Обслуживание пользователя с заданным уровнем гарантии качества осуществляется с помощью технической системы и представляет собой действие, процесс, необходимые для реализации функции по оказанию данной услуги. Здесь подразумевается сочетание аппаратной части, программного обеспечения и человека-оператора информационной системы. В дальнейшем полагаем, что система управления автоматически без участия человека-оператора выполняет заданные функции. Следовательно, для обеспечения высокого уровня гарантоспособности системы необходимо предварительно добиться еще более высокого уровня надежности и аппаратуры (изделия) и составных программных средств. Продукция (изделие) – это предмет или набор предметов, изготовляемых на предприятии. Классическая (структурная) теория надежности исследовала процессы отказов и восстановлений *продукции* (системы, элемента). В работах [1, 6] показано, что даже при сколь угодно большой избыточности не представляется возможным достичь высокого уровня надежности изделий. Исследована модель надежности резервированного объекта с раздельным резервированием в составе одного основного и бесконечного количества резервных однотипных устройств. Приняты следующие предпосылки:

• Время жизни компонентов имеет случайный характер и описывается распределением срока службы, которое удовлетворяет условиям:

- времена выхода из строя каждого из резервированных компонентов статистически не зависят друг от друга;

- у всех резервированных компонентов одинаковое экспоненциальное распределение срока службы компонентов непрерывно, дифференцируемо, и имеет ограниченное среднее.

• Система этих случайных величин представляет собой простой процесс восстановления.

• Средства контроля и коммутации на резервные устройства идеально надежны.

• Время переключения на резерв пренебрежимо мало.

При данных предпосылках предельная вероятность безотказной работы резервированной группы определяется в виде $P_{\Pi}(t) \le \sum_{n=0}^{\infty} P(n,t) \cdot \gamma^n$, где $P(n,t)$ – распределение результирующего числа интервалов времени между заменами отказавшего устройства данного объекта, который до момента отказа выполнял функции основного элемента; $\gamma = P\{\nu \le \tau_{д}\} = \int_0^{\tau_{д}} f_{\nu}(t)dt = F_{\nu}(\tau_{д})$ – вероятность правильного и своевременного обнаружения отказа и переключения на резерв, ν – случайное время существования отказа устройства, $\tau_{д}$ – допустимое время перерыва в работе системы (для систем управления это время сопоставимо с длительностью цикла управления); $f_{\nu}(t)$ – функция плотности времени существования отказа в системе.

При указанных предпосылках в работе [7] установлено, что среднее время до отказа резервированного объекта с раздельным резервированием в составе одного основного и бесконечного количества резервных однотипных устройств не превышает уровня, определяемого формулой (1) в предположении простейшего потока отказов или сбоев устройств

$$T_{СП} \le 1/\lambda(1-\gamma) \qquad (1)$$

где λ – интенсивность отказов одного устройства.

В работе [7] установлено, что можно ожидать повышения средней наработки до отказа исходного устройства за счет многократного резервирования с восстановлением не более чем в 2…10 раз даже при очень высокой вероятности правильного и своевременного обнаружения отказа и переключения на резерв $0{,}8 < \gamma \le 0{,}9$.

Если учесть, что программное обеспечение системы управления также реализуется с отказами и чаще с ошибками [8, 9, 10 и др.], то рассчитывать на достижение высокого уровня гарантоспособности системы за счет традиционных методов не приходится даже при очень больших затратах на введение в систему избыточности.

2. Постановка задачи адаптивной гарантоспособности

Требуется обеспечить заданный высокий уровень гарантоспособности информационной системы управления ***без введения больших объемов*** структурной, временной, функциональной и т.д. избыточности, на основе:

- управления гарантоспособностью по результатам оценки ***правильности*** выполнения в системе предусмотренных задач системы, а не по частоте отказов и интенсивности восстановления после них;

- использования ***естественной*** временной избыточности, которая сохраняется во многих системах в пределах цикла управления;

- адаптации системы к ошибочным результатам выполнения предусмотренных задач с помощью динамической перестройки системы и обеспечения параллельного выполнения задач с потактным сравнением результатов;

- ***приоритетного*** обслуживания наиболее важных задач с целью обеспечения их более высокого уровня гарантоспособности.

Идеи и принципы адаптивной гарантоспособности имеют много общего с концепцией активной защиты (АЗ), которая изложена нами в работе [11]. Они кратко состоят в следующем:

- длительности всех циклов обработки информации разделяются на определенные постоянные или случайные интервалы времени, которые в дальнейшем будем называть тактами, в пределах каждого из которых реализуется предусмотренное множество программных модулей и формируются контрольные точки;

- все множество составных вычислительных модулей (ВМ) информационной системы подразделяется на два составных множества: вычислительная среда – множество, состоящее из m однотипных основных ВМ; защитная среда – множество из $k \le m$ однотипных ВМ избыточных относительно решаемых задач;

- динамическая реконфигурация модулей системы управления производится через такты для организации параллельной обработки информации;

- потактное виртуальное резервирование путем параллельного решения предусмотренных всех m задач на основных ВМ при наличии хотя бы одного исправного избыточного ВМ;

- минимальная конфигурация системы должно содержать не менее $m = 2$ основных и одного избыточного ВМ для выявления ошибочного результата в решаемой задаче, классификации неисправностей и обнаружения их местонахождения;

- синтез адаптивной гарантоспособности (АГ) основывается на выборе такого значения длительности τ такта, при котором в течение допустимого времени перерыва в работе ошибка в результате решения задачи должна с заданным уровнем гарантии быть выявлена и устранена путем локализации ВМ – источника ошибки и перекоммутации его с избыточным исправным ВМ.

3. Организация систем с адаптивной гарантоспособностью

Для практической реализации идей и способов организации АГ могут быть предложены различные дисциплины. В рамках данной статьи рассматриваются две дисциплины: ***Д1*** и ***Д2***.

Д1. Система с рестартом на один такт, содержащая m основных и один контролирующий ВМ, контроль неприоритетный, переназначение модулей не предусмотрено. В случае сбоя одного из пары ВМ выполняется повторный счет с прежними операндами. Совпадение результатов в очередном такте исключает возможность отказа модулей, сбой устранен, обновляется контрольная точка по задаче первого ВМ в i-ом цикле защиты. Если сбой ВМ обнаружен собственными средствами контроля, то естественно обновляется контрольная точка по данным первого основного ВМ. Случай отказа одного из пары ВМ обнаруживается с помощью рестарта на один такт АЗ. Если при решении одного и того же участка задачи в течение двух тактов результаты работы пары однотипных ВМ дважды не совпали, то контрольная точка не обновляется до выполнения совместной работы контролирующего ВМ с очередным основным (в данном примере третьим ВМ). В случае совпадения результатов работы этой последней пары принимается решение об отказе предыдущего основного ВМ (в данном примере второго), обновляется контрольная точка для второго ВМ по данным контролирующего модуля, который теперь выполняет функции второго основного ВМ. Если же в трех смежных тактах защиты результаты не совпали, то принимается решение об отказе контролирующего ВМ и система некоторое время в случае отсутствия исправного избыточного модуля может работать без защиты

Таким образом, относительно дисциплины ***Д1*** параметры A, b и x_y характеризуются следующим: количество тактов в цикле защиты $A = m$; количество тактов принятия решения об отказе или сбое основного ВМ $b = 2$; количество тактов, затрачиваемых на восстановление вычислительного процесса с последней контрольной точки $x_y \le m+2$.

Д2. Система с рестартом и переназначением ВМ, содержащая m основных и один контролирующий модуль. Организация обнаружения и устранения неисправностей такая же, как и в дисциплине ***Д1.*** *Переназначение ВМ* необходимо для сокращения цикла защиты в условиях, когда количество основных ВМ существенно больше числа избыточных модулей. Суть переназначения заключается в том, что в определенных тактах перераспределяются ВМ между вычислительной и защитной средами. За определенными модулями защитной среды на время такта закрепляются функции основных модулей и наоборот. В результате этого устраняется недостаток, присущий способам фиксации контролирующих ВМ, когда модули вычислительной среды контролируются значительно реже, чем модуль защитной среды. Действительно, во всех случаях фиксации модули защитной среды в пределах цикла АЗ участвуют во всех парах контролируемых ВМ, тогда как модули вычислительной среды – только в одной паре, либо несколько чаще, если в каждом такте защиты образуются две и более пары ВМ.

Таким образом, относительно дисциплины ***Д2*** параметры A, b и x_y следующие: $A = \mathrm{int}\left(\frac{m+1}{2}\right)$, $b = 2$, $x_y = \mathrm{int}\left(\frac{m+5}{2}\right)$.

Организация ***приоритетного контроля*** способности системы управления правильно решать предусмотренные задачи позволяет существенно повысить уровень ее гарантоспособности относительно приоритетных задач. Приоритетный контроль организуется на основе переназначения ВМ. Однако при этом преследуется другая цель. Если при переназначении модулей решалась задача уравнять частоту контролей основных и избыточных ВМ, то при приоритетном контроле решается задача увеличения частоты контролей наиболее значимых с точки зрения решаемых задач модулей.

Проиллюстрируем возможности построения систем с двумя отмеченными в качестве приоритетных модулями (таблица 1). Предполагается, что первый отмеченный модуль (нулевой приоритет) контролируется в цикле АЗ с заданной наибольшей частотой, второй (первый приоритет) – с повышенной частотой, но меньшей, чем модуль нулевого приоритета. Остальные ВМ в этой же системе контролируются с одинаковой, но пониженной относительно приоритетных модулей частотой. Пусть $m = 7$, $k = 1$ ($m + k = 8$), нулевой приоритет отводится модулю 2, а первый приоритет – модулю 5. Поставим условие, чтобы в цикле АГ модуль 2 контролировался в четырех тактах, модуль 5 – в двух тактах, а остальные модули 1, 3, 4, 6, 7 и 8 – в одном такте. Решение этой задачи приведено в таблице 1.

Получены следующие результаты. Цикл АГ равен $A = 6$ тактам, четыре раза переназначаются ВМ, модуль 2 контролируется в двух тактах из трех соседних, а модуль 5 контролируется через два такта. Длительность цикла АГ возросла по сравнению с равномерным переназначением ВМ в 1,5 раза, поскольку в том варианте длительность цикла равнялась бы $A = (m + k)/2k = 4$. Это естественно, так как сокращение интервалов времени между контролями одних ВМ возможно за счет увеличения времени между контролями неприоритетных ВМ. В решении таких задач АЗ должен быть применен разумный компромисс. Это в полной мере относится и к выбору способа фиксации или переназначения ВМ. В первом случае проще управление АГ, во втором случае короче цикл управления. Переназначение ВМ предпочтительнее при очень малых величинах допустимого времени перерыва в работе, хотя при этом несколько сложнее управление АГ. При менее жестких временах ограничениях следует стремиться к реализации АГ на основе фиксации контролирующих ВМ.

4. Эффективность способов адаптивной гарантоспособности систем управления

Эффективность адаптивной гарантоспособности оценивается с помощью показателя вероятности успешной адаптации информационной системы управления к отказам, сбоям, программным ошибкам. Успешная адаптация будет в том случае, если в результате действий, предусмотренных алгоритмами защиты, длительность существования указанных неисправностей меньше или равна допустимой величине, что позволяет устранить ошибочные результаты в управлении. Здесь под допустимой величиной подразумевается цикл управления, т.е. время, в течение которого обнаружение и устранение неисправности в системе не приведет к ошибочному очередному управлению. Поскольку время устранения для каждой дисциплины защиты составляет постоянное количество тактов АГ, то достаточно ограничиться сравнением длительности обнаружения неисправности с допустимым временем обнаружения.

Оценку эффективности адаптивной гарантоспособности проведем для следующих типовых условий организации защиты.

Задачи обработки информации разделены на равные части (такты) τ, причем длительность такта много меньше длительности задачи. Задачи решаются через случайные интервалы времени υ_2, однако длительности решения задач υ_1 много больше длительности пауз, т.е. $\upsilon_1 >> \upsilon_2$. Это позволяет разделить задачу на такты защиты (например, для общности – такты случайной длительности). Кроме того, учитывается, что допустимое время перерыва в работе системы – постоянная величина $\tau_д$. Предполагается, что отсутствуют одновременные отказы или сбои проверяемого в текущем такте рабочего и контролируемого ВМ. Длительность такта определяется длительностью выполнения в пределах такта группы функционально законченных программных модулей. Поскольку все ВМ, на которых выполняются программные модули, однотипны, то порядок распределения программных модулей по тактам работы ВМ является общим для всех ВМ. Это позволяет принять одинаковыми распределения $F_\upsilon(t)$ длительности тактов для всех ВМ.

Требуется установить вероятность успешной адаптации системы к отказам:

Таблица 1

Номер такта	Номера основных ВМ	Номер контролирующего ВМ	Пары контролируемых ВМ	Переназначаемые ВМ	Частота контролей ВМ		
					2	5	1, 3, 4, 6, 7, 8
1	1 8 3 4 5 6 7	2	**2**–7	8–2			
2	1 8 3 4 5 6 7	2	**2**–3	8–2			
3	1 2 3 4 5 6 7	8	8–**5**	-			
4	8 2 3 4 5 6 7	1	1–**2**	8–1	**4**	**2**	**1**
5	1 2 3 8 5 6 7	4	4–**2**	8–4			
6	1 2 3 4 8 6 7	5	**5**–6	8–5			

$$\beta = P\{\nu \le \tau_{Д} - t_{у}\} = \int_{0}^{\tau_{Д}-t_{у}} f_{\nu}(t)dt, \qquad (2)$$

где $f_{\nu}(t)$ – функция плотности времени ν существования скрытого отказа в системе.

Для нахождения функции плотности $f_{\nu}(t)$ и вероятности успешной адаптации к отказам β в целом используются следующие параметры:

• функции распределения и характеристики временных интервалов защиты – длительности тактов, допустимого времени перерыва в работе системы и времени устранения обнаруженного отказа ($\tau_{Д}$ и $t_{у}$ соответственно);

• параметры принятой дисциплины АЗ: $A, b, t, x_{у} = t_{у}/\tau$.

Время подключения контролирующего ВМ к очередному основному слагается из случайной длительности такта υ и времени ожидания ψ от момента завершения параллельной работы с предыдущим ВМ до момента начала следующего такта работы очередного ВМ. Причем, $\psi \le \upsilon$ и во время ожидания осуществляется загрузка памяти контролирующего ВМ командами и операндами очередного основного модуля.

Для нахождения функции плотности времени ν предварительно установим функцию плотности суммарного времени ψ + υ. В изображении Лапласа она имеет вид

$$f_{\xi}(s) = \phi_{\psi}(s) * f_{\upsilon}(s),$$

где $\phi_{\psi}(s)$ – изображение плотности распределения времени ожидания ψ, а $f_{\upsilon}(s)$ – изображение плотности распределения длительности такта АЗ.

Пусть от момента возникновения скрытого отказа ВМ до момента подключения к нему контролирующего ВМ прошло x тактов. Тогда условная вероятность того, что $x < X$, где $X = 0, 1, \ldots, A, \ldots$, может быть найдена с помощью соответствующего преобразования Лапласа

$$f_{x}(s) = [f_{\xi}(s)]^{x}.$$

Вследствие равновероятной возможности отказа любого из ВМ, которые не защищены в данном такте, можно полагать, что целочисленная случайная величина x равномерно распределена в диапазоне чисел 1, 2, …, A–1. Отсюда плотность распределения количества тактов существования неисправности в системе определяется с помощью выражения:

$$f(x) = \sum_{i=1}^{A-1} \frac{\delta(x-i)}{A-1}, \qquad (3)$$

где δ(x) есть дельта функция от параметра x.

Общая длительность существования отказа до его обнаружения представляет собой сумму времени x(υ+ψ) и времени b(υ+ψ) от момента обнаружения факта неисправности до локализации отказавшего ВМ в соответствии с выбранной дисциплиной АЗ.

Функция плотности случайной величины x(υ+ψ)=θ в изображении Лапласа представляется следующим образом по формуле полной вероятности:

$$f_{\theta}(s) = \sum_{i=1}^{A-1} \frac{1}{A-1} \left(f_{\xi}(s)\right)^{i}.$$

Функция плотности случайной величины $(x+b)\cdot(\upsilon+\psi)$ в изображении Лапласа вычисляется в виде

$$f_{\nu}(s) = f_{\theta}(s) * (f_{\upsilon}(s))^{b} = \frac{1}{A-1} \sum_{i=1}^{A-1} \left(f_{\xi}(s)\right)^{i+b} \qquad (4)$$

Следующий шаг в определении вероятности успешной адаптации к отказам системы с рассматриваемой организацией АЗ состоит в том, чтобы в полученном выше выражении раскрыть функцию $f_{\xi}(s)$, которая в изображении Лапласа есть функция плотности суммы длительности такта и времени задержки в подключении контролирующего ВМ к основному в пределах такта ($\xi = \upsilon + \psi \le 2\upsilon$).

Ориентируясь на экспериментальные данные [2], примем распределения случайных длительностей тактов υ в виде распределения Эрланга a-го порядка с функцией плотности $f_{\upsilon}(t) = \frac{\rho(\rho \cdot t)^{a}}{a!} e^{-\rho \cdot t}$, которые в изображении Лапласа имеют следующий вид:

$$f_{\upsilon}(s) = \left(\frac{\rho}{\rho + s}\right)^{a+1},$$

где ρ – параметр распределения Эрланга (количество событий в единицу времени).

Согласно работе [12] функция плотности времени ожидания ψ (в нашем случае время подключения контролирующего к основному) в изображении Лапласа имеет следующий вид:

$$\phi_{\psi}(s) = \frac{\rho}{(a+1)s}\left[1 - \left(\frac{\rho}{\rho + s}\right)^{a+1}\right].$$

Следовательно, в формуле (4) функция плотности $f_{\xi}(s)$ равна

$$f_{\xi}(s) = f_{\upsilon}(s) \cdot \phi_{\psi}(s) = \left(\frac{\rho}{\rho + s}\right)^{a+1} \cdot \frac{\rho}{(a+1)s}\left[1 - \left(\frac{\rho}{\rho + s}\right)^{a+1}\right].$$

Подставляя данное выражение в формулу (3.4), находим

$$f_{\nu}(s) = \frac{1}{A-1} \sum_{i=1}^{A-1} \left\{\left(\frac{\rho}{\rho + s}\right)^{a+1} \frac{\rho}{(a+1)s}\left[1 - \left(\frac{\rho}{\rho + s}\right)^{a+1}\right]\right\}^{i+b}.$$

Переходя от изображения к оригиналу при постоянной величине допустимого времени перерыва в работе и воспользовавшись формулой (3), определяем вероятность успешной адаптации системы с АГ к отказам

$$\beta = 1 - \frac{e^{-(a+1)\cdot x_{Д}^{*}}}{A-1} \sum_{i=1}^{A-1} \left(\frac{1}{a+1}\right)^{i+b} \sum_{|\bar{n}|=i+b} \frac{(i+b)!}{\bar{n}!} \cdot \sum_{k=0}^{\eta} \frac{\left((a+1)x_{Д}^{*}\right)^{k}}{k!}, \qquad (5)$$

где $\bar{n}! = n_0! n_1! \ldots \cdot n_a!$; $|\bar{n}| = n_0 + n_1 + \ldots + n_a$; $x_{Д}^{*} = \tau_{Д}^{*}/\tau$; $t_{Д}^{*} = \tau_{Д} - t_{у}$;

$$\eta = (a+2)(i+b) + \sum_{j=1}^{a} j n_j + 1.$$

В частном случае $a = 0$ (экспоненциальное распределение длительности такта) имеет место следующее выражение вероятности успешной адаптации системы к отказам $\beta = 1 - \frac{e^{-x_д^*}}{\_A-1} \sum_{i=1}^{A-1} \sum_{k=0}^{2(i+b)+1} \frac{(x_д^*)^k}{k!}$, поскольку в этом случае $\bar{n}! = 1$, а $|n| = 0$.

С помощью выражения (5) проанализируем зависимости вероятности успешной адаптации системы с АЗ от допустимого количества тактов перерыва в работе, числа m основных модулей и применительно к рассмотренным ранее дисциплинам ***Д1*** и ***Д2***.

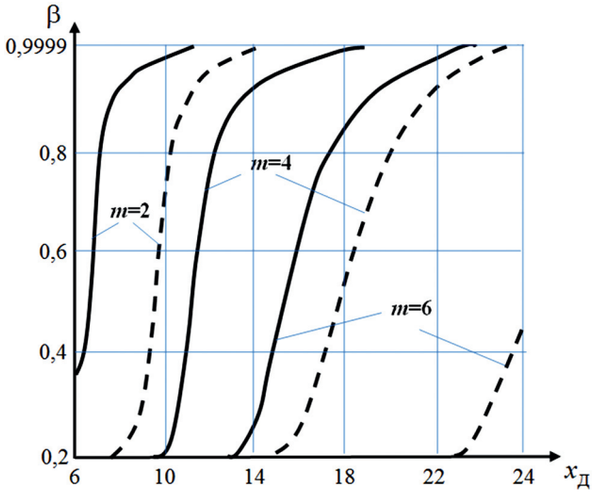


Рисунок 1 – Зависимости вероятности успешной адаптации системы со случайными тактами защиты к отказам в зависимости от допустимого количества $x_д$ тактов защиты и от числа m основных ВМ

На рисунке 1 показаны зависимости $\beta = f(x_д)$ при $a \geq 2$ применительно к дисциплинам ***Д2*** (сплошные линии) и ***Д1*** (пунктирные линии). Начиная со второго порядка распределения Эрланга длительности такта и выше результаты этих зависимостей практически совпадают. Они свидетельствуют о том, что наибольшей скоростью адаптации к отказу ВМ обладают дисциплины, аналогичные ***Д2***. Эти дисциплины примерно на несколько тактов быстрее реагируют на ошибки в результатах решения задач, чем дисциплины класса ***Д1***. Преимущества отмеченных дисциплин повышаются по мере увеличения количества основных вычислительных модулей.

Вместе с тем, АГ со случайной длительностью тактов значительно инерционнее, чем АГ с тактами постоянной длительности. Так, даже при минимальном для АГ количестве основных модулей $m = 2$ время обнаружения и устранения отказа ВМ увеличивается в 1,5–2 раза. Поскольку для многих архитектур систем управления и вычислительных процессов в них не представляется возможным организовать АГ с постоянными тактами, то целесообразно изыскивать дополнительные возможности в повышении скорости адаптации систем с АГ к отказам составных ВМ. Такая возможность, например, имеет место при применении также встроенного контроля основных ВМ, с помощью которого в системах с АГ возможно оперативнее обнаруживать и устранять неисправности ВМ.

5. Заключение

Ограниченные возможности резервирования, средств оперативного обнаружения отказов, сбоев, ошибок в выполнении информационных процессов, ограниченные возможности комплекса «аппаратура – программы» – все это вызывает необходимость в развитии нестандартных технологий обеспечения гарантоспособности информационных систем управления. Одной из них является предложенная в статье технология адаптивной гарантоспособности. Суть ее состоит в активном использовании естественной временной и структурной избыточности и в активном (и автоматическом) переназначении имеющихся вычислительных ресурсов не только для оперативной обработки информации, но и для реализации наблюдаемости системы при ограниченных средствах контроля. Адаптивная гарантоспособность предназначена для достижения требуемых уровней гарантоспособности информационных систем управления в условиях незначительного резерва времени, ограниченной эффективности средств обнаружения неисправностей составных вычислительных модулей, а также при условии, что объем избыточного оборудования не должен превышать объема основного оборудования. С помощью адаптивной защиты имеются реальные возможности добиться гораздо более высокого уровня гарантоспособности систем, чем с помощью традиционных методов резервирования. Технология адаптивной гарантоспособности позволяет в ограниченных временных условиях при решении реальных задач осуществлять своевременное автоматическое обнаружение и устранение отказов и сбойных ошибок путем оперативной локализации неисправных вычислительных модулей и последующей автоматической реконфигурации системы с выводом из процесса функционирования отказавших модулей. Вместе с тем, эта технология ориентирована на мультимодульные системы и недостаточно проработана для средств хранения и отображения информации, документирования, средств энергообеспечения информационных систем управления.

Библиографический список

1. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза [Текст] – М.: «Журнал Надежность», 2016. – 545с.

2. Кирпичников А.П., Васильев С.Н. Особенности современной микроэлектроники и вопросы построения систем управления высокой надежности и безопасности // Надежность (Dependability). – 2017. – Том 17, №3. – С. 10-16.

3. Avizienis A., Laprie J-C. and Randell B. Dependability of computer systems/ Fundamental concepts, terminology and examples. Technical report, LAAS – CNRS, October, 2000.

4. Rus I., Komi-Sirvio S., Costa P. Computer program with insurance of high reliability. Technical report, IFIP WG-10.4, March, 2008.

5. Борисов А.Б. Большой экономический словарь. – М.: Книжный мир, 2003. – 895 с.

6. Шебе Х., Шубинский И.Б. Предельная надежность структурного резервирования // Надежность (Dependability). – 2016. – Том 16, № 1. – С. 3-13.

7. Шубинский И.Б. Методы обеспечения функциональной надежности программ // Надежность (Dependability). – 2014. – № 4. – С. 87-101.

8. Потапов И.В. Проблематика в области надежности программных систем // Надежность (Dependability). – 2015. – № 1. – С. 57-61.

9. Шубинский И.Б., Шебе Х. Систематический подход к защите программного обеспечения от сбоев аппаратуры // Надежность (Dependability). – 2014. – №3. – С. 96-106.

10. Shubinsky I.B., Sheabe X. On the definition of functional reliability, Proceedings of the ESREL 2013, Safety, Reliability and Risk Analysis: Beyond the Horizon – Steenbergen et al. (Eds) 2014 Taylor & Francis Group, London, ISBN 978-1-138-00123-7, pp. 3021-3027.

11. Shubinskiy I.B. Adaptive fault tolerance in real-time information systems, Life Cycle Engineering and Management, ICDQM-2016, Prijevor, Serbia, 29-30 June 2016, pp. 3-14.

12. Гнеденко Б.В. Введение в теорию массового обслуживания [Текст] / Б.В. Гнеденко, И.Н. Коваленко. – Киев: Наука, 1963.

Сведения об авторах

Игорь Б. Шубинский – доктор технических наук, профессор, заместитель руководителя НТК АО «НИИАС», Москва, Россия, тел. +7 (495) 786-68-57, e-mail: igor-shubinsky@yandex.ru

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

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

Поступила: 26.08.2018

УДК 621.3.019.3
Оригинальная статья
Надежность, том 18, №4, 2018 DOI: 10.21683/1729-2646-2018-18-4-10-15

К вопросу об оценке коэффициента вариации наработки до отказа по квантилям малого уровня

Александр В. Федухин, *Институт проблем математических машин и систем НАН Украины, Украина*
Наталья В. Сеспедес Гарсия, *Институт проблем математических машин и систем НАН Украины, Украина*

Александр В. Федухин

Наталья В. Сеспедес Гарсия

Резюме. *При решении различных задач по оценке надежности систем вероятностно-физическими методами важнейшей априорной информацией, позволяющей эффективно их решать, является информация о коэффициенте вариации наработки до отказа. В условиях малой статистики отказов оценка коэффициента вариации наработки до отказа является сложной задачей из-за сильно цензурированных выборок. В этих случаях используют методы оценки коэффициента вариации с привлечением дополнительной априорной информации и метода квантилей. Решение ряда задач по надежности с учетом различных распределений отказов значительно упрощается, если функции этих распределений табулированы в параметрах относительная наработка и коэффициент вариации. Впервые эффективное решение задач по надежности с использованием таблиц функции DN-распределения предложено для параметризации распределения в параметрах x и v, где x – параметр масштаба, относительная наработка x = at; v – параметр формы, коэффициент вариации v = V; a – средняя скорость деградации. Это позволило при табулировании уйти от реального масштаба времени, упростить табулирование функции и ее использование при решении ряда задач по надежности методом квантилей. В работе проанализирована эффективность метода квантилей по оценке коэффициента вариации наработки до отказа, являющегося одновременно параметром формы DN-распределения, в условиях малой статистики отказов и на его основе предложен новый, более эффективный метод. Метод оценки коэффициента вариации по квантилям малого и сверхмалого уровня опирается на анализ поведения функции $a_i = f(t)$, полученной методом квантилей. Наилучшим выбором априорного значения v считается такой выбор, при котором график зависимости $a_i = f(t)$ наиболее точно описывается прямой горизонтальной линией, что полностью согласуется с гипотезой о постоянстве скорости деградации, принятой при формализации DN-распределения. В тех случаях, когда по графику зависимости $a_i = f(t)$ трудно сделать вывод о наилучшем варианте выбора априорного значения v (особенно сложно сделать выбор по статистике первых отказов), можно воспользоваться следующим формальным критерием: наиболее приемлемое априорное значение параметра формы v лежит в области значений, при которых происходит смена знака тренда средней скорости деградации (h) на графике $a_i = f(t)$. Исследованиями установлено, что наиболее значительные ошибки в оценке коэффициента вариации дают первые отказы. При обработке результатов испытаний на надежность считается, что первые отказы в выборке имеют наименьший информационный вес, так как их появление вызвано серьезными дефектами, не обнаруженными в процессе выходного контроля качества продукции. Первые отказы, как правило, «выпадают» из общей статистической закономерности и их рекомендуется исключать из последующего анализа. Предложенный метод оценки коэффициента вариации наработки до отказа по квантилям сверхмалого уровня позволяет в условиях ограниченной статистики отказов, когда другие методы не работают, довольно точно определять не только коэффициент вариации наработки до отказа и параметры DN-распределения, но и делать выводы о возможности и правомерности выравнивания (описания) исследуемой выборки с помощью данного диффузионного распределения, т.е. может использоваться в качестве своеобразного критерия согласия исследуемого эмпирического распределения отказов выбранной теоретической модели надежности. Описанный процесс нахождения наиболее истинных значений коэффициента вариации наработки до отказа с помощью формального критерия согласия может выполняться с использованием ЭВМ.*

Ключевые слова: *метод квантилей, коэффициент вариации, квантили малого и сверхмалого уровня, DN-распределение.*

Формат цитирования: *Федухин А.В., Сеспедес Гарсия Н.В. К вопросу об оценке коэффициента вариации наработки до отказа по квантилям малого уровня // Надежность. 2018. Т. 18, № 4. С. 10-15. DOI: 10.21683/1729-2646-2018-18-4-10-15*

1. Введение

При решении различных задач по оценке надежности систем вероятностно-физическими методами [1] важнейшей априорной информацией, позволяющей эффективно их решать, является информация о коэффициенте вариации наработки до отказа. В условиях малой статистики отказов оценка коэффициента вариации наработки до отказа является сложной задачей из-за сильно цензурированных выборок. В этих случаях используют методы оценки коэффициента вариации с привлечением дополнительной априорной информации [2–4] и метода квантилей [1].

В работе проанализирована эффективность метода квантилей по оценке коэффициента вариации наработки до отказа (параметра формы *DN*-распределения [5–8]) в условиях малой статистики отказов и на его основе предложен новый, более эффективный, метод.

2. Метод квантилей

Если известно априорное значение параметра формы ν, состоятельной оценкой которого является коэффициент вариации процесса деградации V, то параметр масштаба *DN*-распределения – среднюю скорость деградации a – можно определить в результате решения уравнения [1]:

$$\Phi\left(\frac{at_\gamma - 1}{\nu\sqrt{at_\gamma}}\right) + \exp(2\nu^{-2})\Phi\left(-\frac{at_\gamma + 1}{\nu\sqrt{at_\gamma}}\right) = \hat{\gamma}, \qquad (1)$$

где $\hat{\gamma} = r / N$ – квантиль, вычисляемая через отношение количества отказов r к объему выборки N, поставленной на испытания; t_γ – время появления r-го отказа.

Решение ряда задач по надежности с учетом различных распределений отказов значительно упрощается, если функции этих распределений табулированы. Впервые эффективное решение задач по надежности с использованием таблиц функции *DN*-распределения предложено в [9], где функция *DN*-распределения была параметризована и табулирована в параметрах x и ν. Использование в качестве параметра распределения относительной наработки $at = x$ позволило при табулировании уйти от реального масштаба времени, упростить табулирование функции и ее использование при решении ряда задач по надежности методом квантилей

$$\Phi\left(\frac{x_\gamma - 1}{\nu\sqrt{x_\gamma}}\right) + \exp(2\nu^{-2})\Phi\left(-\frac{x_\gamma + 1}{\nu\sqrt{x_\gamma}}\right) = \hat{\gamma}, \qquad (2)$$

где $x_\gamma = at_\gamma$.

С использованием таблиц *DN*-распределения [1] по исходным данным о $\hat{\gamma}$ и ν определяется значение x_γ, и далее по формуле $a = \dfrac{x_\gamma}{t_\gamma}$ вычисляется значение средней скорости деградации a.

Если в процессе оценки параметра масштаба *DN*-распределения a методом квантилей выбрано (исходя из самых общих рассуждений в области физики отказов [10]) априорное значение параметра формы ν, заведомо превышающее действительное значение V, то это приводит к заниженным результатам прогноза средней скорости деградации. Если априорное значение параметра формы ν заведомо меньше действительного значения V, то наоборот, это приводит к завышенным результатам прогноза. И только если выбранная априорная оценка параметра формы близка к действительному значению коэффициента вариации генеральной совокупности $\hat{V}$, то оценки a_i, полученные методом квантилей, располагаются вокруг средней оценки $\hat{a}$ с минимальной дисперсией и представляют собой график зависимости $a_i = f(t)$, максимально приближающийся к горизонтальной прямой вокруг истинного среднего значения.

Оценки a_i, полученные методом квантилей, рекомендуется усреднять, отбросив первые отказы и взяв для усреднения конечный, наиболее линеаризованный, участок зависимости $a_i = f(t)$, или воспользоваться формулой для взвешенного среднего, предложенной в [1]. Необходимо иметь в виду, что использование статистической информации о первых отказах приводит к достаточно большим погрешностям в оценке параметра масштаба *DN*-распределения. Устойчивой закономерности в этом не обнаружено, так что оценки a_i, полученные по первым отказам, могут быть как завышенными, так и заниженными по отношению к $\hat{a}$, полученной для генеральной совокупности.

Используя закономерности, описанные выше, можно сформулировать следующий метод оценки коэффициента вариации наработки до отказа по малым выборкам.

3. Метод оценки коэффициента вариации по квантилям малого уровня

Процесс деградации изделий электронной техники, наряду с монотонными реализациями (механические разрушения при термо-электроциклировании) вследствие электрических явлений, имеет и немонотонные реализации, поэтому в общем случае принято рассматривать деградацию этих изделий как процесс с немонотонными реализациями (рисунок 1). При этом тангенс угла наклона среднего значения определяющих параметров процессов деградации (наклонная сплошная линия на графике), протекающих в изделии, представляет собой постоянную величину, равную средней скорости обобщенного процесса деградации

$$tg\alpha = \hat{a} = \text{const}. \qquad (3)$$

При формализации *DN*-распределения процесс деградации для совокупности однотипных изделий предполагается однородным, то есть с постоянной средней скоростью, постоянным средним квадратическим отклонением скорости и, как следствие, постоянным коэффициентом вариации скорости (рисунок 2).

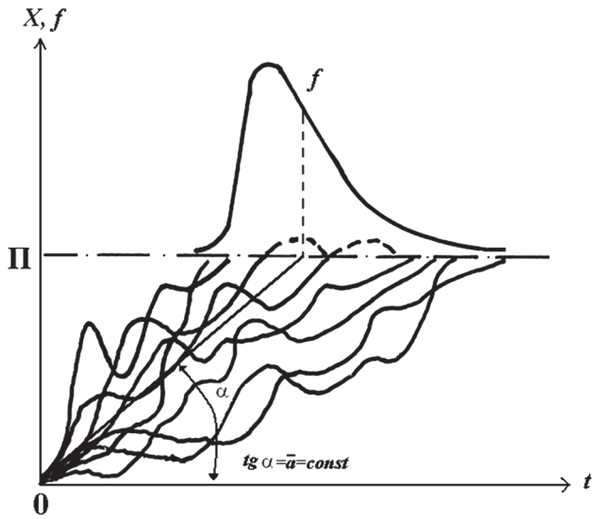


Рисунок 1 – График формирования плотности *DN*-распределения для изделия (П – уровень предельного значения определяющего параметра, при достижении (превышении) которого наступает отказ объекта)

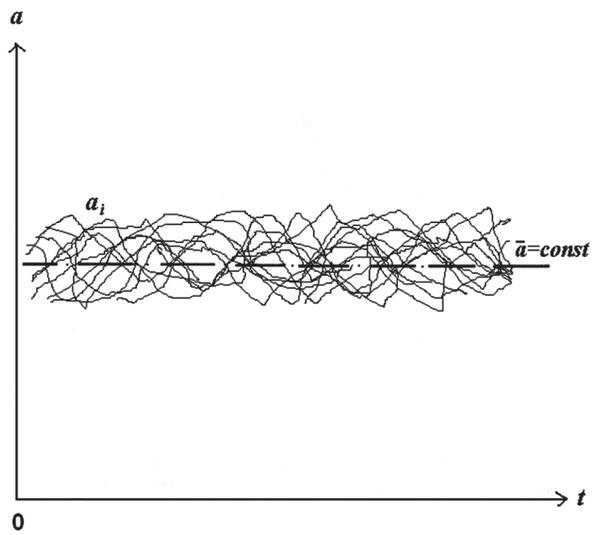


Рисунок 2 – График теоретической зависимости $a_i = f(t)$ для совокупности изделий

Метод оценки коэффициента вариации по квантилям малого уровня опирается на анализ поведения графиков зависимости $a_i = f(t)$, полученной методом квантилей. Наилучшим выбором априорного значения v считается такой выбор, при котором график зависимости $a_i = f(t)$ наиболее точно описывается прямой горизонтальной линией, что согласуется с гипотезой о постоянстве скорости деградации, принятой при формализации *DN*-распределения [4, 9] (рисунок 2).

В тех случаях, когда по графику зависимости $a_i = f(t)$ трудно сделать вывод о наилучшем варианте выбора априорного значения v (особенно сложно сделать выбор по статистике первых отказов), можно воспользоваться следующим формальным критерием.

Критерий подбора априорного значения параметра формы. Наиболее приемлемое априорное значение параметра формы v лежит в области значений, при которых происходит смена знака тренда средней скорости деградации (h) на графике $a_i = f(t)$

$$h = \frac{a_n - a_1}{\bar{a}_i}, \tag{4}$$

где a_1, a_n – оценки скорости деградации изделия, полученные по квантилям, соответственно, минимального и максимального уровней; $\bar{a}_i$ – среднее значение оценок скоростей деградации, полученных методом квантилей

$$\bar{a}_i = \frac{\sum_{i=1}^{n} a_i}{n}. \tag{5}$$

Проиллюстрируем эффективность работы данного критерия на примере натурных испытаний на долговечность образцов изделий, статистика отказов которых хорошо описывается *DN*-распределением.

Таблица 1 – Таблица данных

r	γ	t_γ, 10^3 цикл
1	0,0021	44
5	0,0107	49
10	0,0215	57
15	0,0323	59
20	0,0431	63
25	0,0539	66
30	0,0647	68
35	0,0755	73
40	0,0863	75
45	0,0971	78
50	0,1079	79
55	0,1187	82
60	0,1295	84
65	0,1403	86
70	0,1511	89
75	0,1619	91
80	0,1727	93
85	0,1835	95
90	0,1943	97
95	0,2051	99
100	0,2159	102
105	0,2267	102
110	0,2375	105
115	0,2483	106
120	0,2591	107
125	0,2699	108
130	0,2807	109
135	0,2915	111
140	0,3023	113
145	0,3131	114

Пример. Рассмотрим в качестве примера испытания образцов изделий из алюминиевого сплава В-95 на усталостную долговечность [10]. Необходимо оценить коэффициент вариации наработки до отказа предлагаемым методом по малым выборкам.

Первые элементы выборки объемом $N = 463$ с соответствующими квантилями в диапазоне от 0,0021 до 0,3131 приведены в таблице 1. В таблице 1 введены следующие обозначения: r – накопленное количество отказов на момент времени t_γ; t_γ – время испытаний, соответствующее накопленному количеству отказов; γ – эмпирическая вероятность отказа.

Проверим работу метода оценки коэффициента вариации по квантилям сверх малого уровня. В качестве исходных данных возьмем квантили уровня от 0,0021 до 0,0215. Для различных значений параметра v определим методом квантилей значения a_i по данным о γ и r и вычислим значение критерия h по формуле (4). Данные приведены в таблице 2.

График экспериментальной зависимости $a_i = f(t)$ для квантилей от 0,0021 до 0,0215 приведен на рисунке 3.

Выводы по оценкам параметров. Смена знака тренда h произошла при $0,3 < v < 0,4$, поэтому

$$\nu = \frac{0,3+0,4}{2} = 0,35;\ \overline{a}_i = 8,473\cdot10^{-6}\ \text{цикл}^{-1};$$

$$\delta_v = \frac{0,56-0,35}{0,56} = 0,375;$$

$$\delta_a = \frac{8,473\cdot10^{-6} - 5,9\cdot10^{-6}}{5,9\cdot10^{-6}} = 0,436.$$

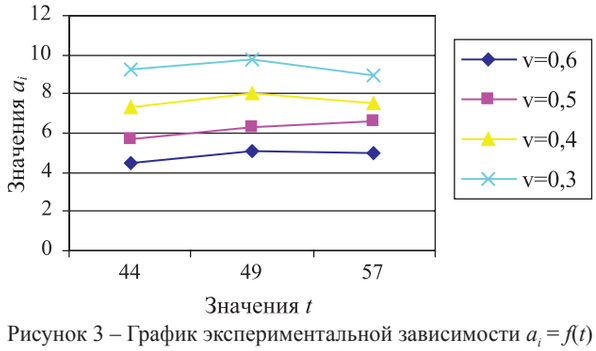


Рисунок 3 – График экспериментальной зависимости $a_i = f(t)$ для квантилей от 0,0021 до 0,0215

Ошибки в оценке как параметра формы, так и параметра масштаба, по первым отказам довольно значительные. Известно, что при обработке результатов испытаний на надежность считается, что первые отказы в выборке имеют наименьший вес, так как их появление

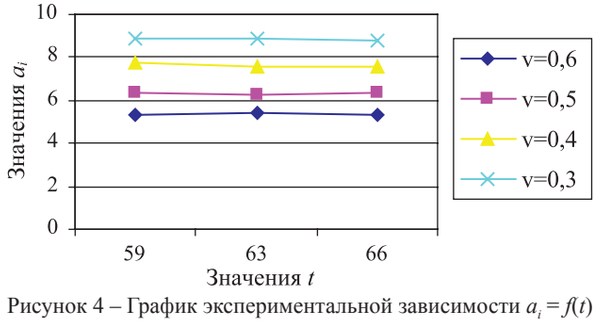


Рисунок 4 – График экспериментальной зависимости $a_i = f(t)$ для квантилей от 0,0323 до 0,0539

Таблица 2. Таблица данных

r	γ	t_γ, 10^3 цикл	$v = 0,6$		$v = 0,5$		$v = 0,4$		$v = 0,3$	
			a_i,10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h
1	0,0021	44	4,545	0,1106	5,681	0,1503	7,272	0,0358	9,318	**-0,0397**
5	0,0108	49	5,102		6,327		7,959		9,796	
10	0,0215	57	5,088		6,614		7,544		8,947	

Таблица 3. Таблица данных

r	γ	t_γ, 10^3 цикл	$v = 0,6$		$v = 0,5$		$v = 0,4$		$v = 0,3$	
			a_i, 10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h
15	0,0323	59	5,254	0,0092	6,44	**-0,0119**	7,797	**-0,0288**	8,915	**-0,0143**
20	0,0431	63	5,397		6,349		7,619		8,889	
25	0,0539	66	5,303		6,364		7,576		8,788	

Таблица 4. Таблица данных

r	γ	t_γ, 10^3 цикл	$v = 0,6$		$v = 0,5$		$v = 0,4$		$v = 0,3$	
			a_i, 10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h	a_i, 10^{-6} цикл$^{-1}$	h
15	0,0323	59	5,254	0,0148	6,44	**-0,0273**	7,797	**-0,0615**	8,915	**-0,0747**
20	0,0431	63	5,397		6,349		7,619		8,889	
25	0,0539	66	5,303		6,364		7,576		8,788	
30	0,0647	68	5,441		6,47		7,647		8,823	
35	0,0755	73	5,342		6,164		7,260		8,356	
40	0,0863	75	5,333		6,267		7,333		8,267	

вызвано серьезными дефектами, не обнаруженными в процессе выходного контроля качества продукции. Первые отказы, как правило, «выпадают» из общей статистической закономерности, поэтому для дальнейшего анализа мы их отбросим и продолжим исследование эффективности метода оценки коэффициента вариации по квантилям уровня от 0,0323 до 0,0539. Данные значений a_i и h приведены в таблице 3.

График экспериментальной зависимости $a_i = f(t)$ для квантилей от 0,0323 до 0,0539 приведен на рисунке 4.

Выводы по оценкам параметров. Последняя смена знака тренда h произошла при $0,5 < v < 0,6$, поэтому

$$\nu = \frac{0,5+0,6}{2} = 0,55;\ \overline{a}_i = 5,851\cdot10^{-6}\ \text{цикл}^{-1};$$

$$\delta_\nu = \frac{0,56-0,55}{0,56} = 0,018;$$

$$\delta_a = \frac{5,9\cdot10^{-6}-5,851\cdot10^{-6}}{5,9\cdot10^{-6}} = 0,008.$$

Анализируя абсолютные значения трендов: 0,0092 и 0,0119, можно сделать еще и дополнительный вывод о том, что истинное значение параметра формы v находится ближе к значению 0,6.

Увеличим количество статистической информации об отказах до квантилей уровня 0,0863. Данные значений a_i и h приведены в таблице 4.

График экспериментальной зависимости $a_i = f(t)$ для квантилей от 0,0323 до 0,0863 приведен на рисунке 5.

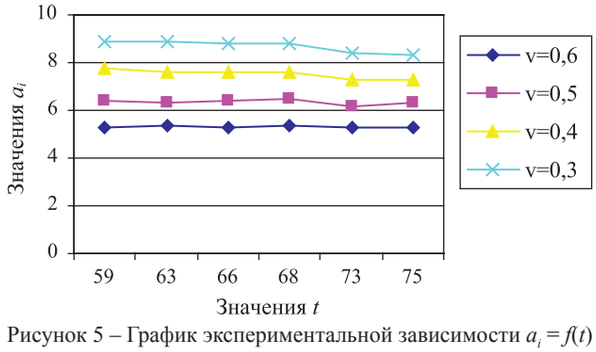


Рисунок 5 – График экспериментальной зависимости $a_i = f(t)$ для квантилей от 0,0323 до 0,0864

Выводы по оценкам параметров. Смена знака тренда h не изменилась при увеличении статистики отказов и вновь произошла при $0,5 < v < 0,6$. Поэтому

$$\nu = \frac{0,5+0,6}{2} = 0,55;\ \overline{a}_i = 5,844\cdot10^{-6}\ \text{цикл}^{-1};$$

$$\delta_\nu = \frac{0,56-0,55}{0,56} = 0,018;$$

$$\delta_a = \frac{5,9\cdot10^{-6}-5,844\cdot10^{-6}}{5,9\cdot10^{-6}} = 0,009.$$

При имеющейся дискретности изменения априорного значения v, равной 0,1, дальнейшее увеличение статистики отказов не приводит к уточнению оценки параметра формы. Если принять дискретность равной 0,05, то значение v можно было бы оценить еще более точно. Важно отметить, что описанный процесс нахождения наиболее истинного значения выборочной оценки параметра формы v с помощью формального критерия согласия достаточно алгоритмичен и может с успехом выполняться на ЭВМ.

Посмотрим, какой график изменения средней скорости деградации получается при увеличении статистической информации до квантилей малого уровня 0,3131.

В [1, 10] приведены данные, полученные в результате обработки полной выборки образцов изделий В-95: $N = 463$, $\hat{V} = 0,56$, $\hat{S} = 169\cdot10^3$ цикл, $\hat{a} = 5,9\cdot10^{-6}$ цикл$^{-1}$.

Оценки коэффициента вариации наработки до отказа по квантилям малого уровня с использованием предложенного формального критерия согласия, очень близки ($v = 0,55$; $\overline{a}_i = 5,844\cdot10^{-6}$ цикл$^{-1}$) к оценкам, полученным экспериментальным путем по полной выборке.

На рисунке 6 изображен график зависимости оценки параметра масштаба DN-распределения, полученной по квантилям от 0,0021 до 0,3131 для $v = 0,57$.

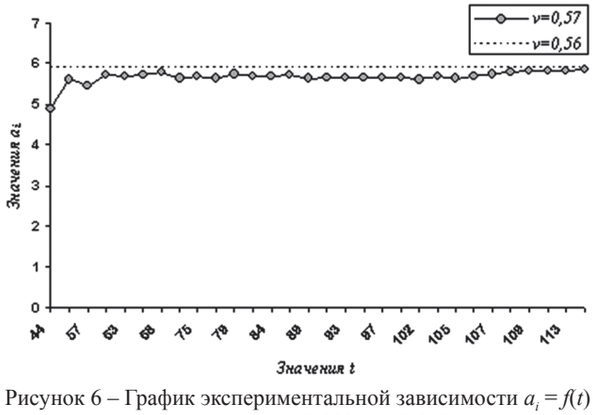


Рисунок 6 – График экспериментальной зависимости $a_i = f(t)$ для квантилей от 0,0021 до 0,3131

Нетрудно видеть, что почти при полном совпадении априорного значения параметра формы $v = 0,57$ с выборочной оценкой коэффициента вариации $\hat{V} = 0,56$, график зависимости $a_i = f(t)$ представляет собой довольно ровную прямую линию, расположенную чуть ниже оценки $\hat{a} = 5,9\cdot10^{-6}$ цикл$^{-1}$, полученной по полной выборке. Исключением, как и предполагалось, являются первые отказы, которые дают несколько заниженную оценку средней скорости деградации и выпадают из общей тенденции.

4. Выводы

Предложенный в работе метод оценки коэффициента вариации наработки до отказа по квантилям позволяет в условиях ограниченной статистики отказов по квантилям сверхмалого уровня довольно точно

определять не только коэффициент вариации наработки до отказа и параметры *DN*-распределения, но и делать выводы о возможности и правомерности выравнивания (описания) исследуемой выборки с помощью данного диффузионного распределения, т.е. может использоваться в качестве своеобразного критерия согласия исследуемого эмпирического распределения отказов выбранной теоретической модели надежности. Описанный процесс нахождения наиболее истинных значений коэффициента вариации наработки до отказа с помощью формального критерия согласия может выполняться на ЭВМ.

Библиографический список

1. Стрельников В.П. Оценка и прогнозирование надежности электронных элементов и систем / В.П. Стрельников, А.В. Федухин. – К.: Логос, 2002. – 486 с.

2. Савчук В.П. Байесовские методы статистического оценивания надёжности технических объектов. – М.: Наука, 1989. – 303 с.

3. Прохоренко В.Д. Учёт априорной информации при оценке надёжности / В.Д. Прохоренко, В.Ф Голиков. – М.: Наука и техника, 1978. – 255 с.

4. ГОСТ 27.201-81. Надёжность в технике. Оценка надёжности при малом числе наблюдений с использованием дополнительной информации. – Введ. 01.07.1981. – Москва: Издательство стандартов, 1981. – с.136.

5. Стрельников В.П. Прогнозирование ресурса изделий электронной техники // Надежность. – 2004. – №4 (12). – С.43-48;

6. Стрельников В.П. Методические погрешности расчета надежности систем // Надежность.- 2005. -№3 (12). – С.41-46.

7. Стрельников В.П. Методические погрешности оценок надежности электронных элементов и систем // Надежность.- 2009. – №2. – С. 27-32.

8. Стрельников В.П. Закономерности изменения наработки между отказами технических систем в процессе эксплуатации // Надежность, 2011. -№01 (36). – С. 17-22.

9. Погребинский С.Б. Проектирование и надежность многопроцессорных ЭВМ / С.Б. Погребинский, В.П. Стрельников. – М.: Радио и связь, 1988. – 168 с.

10. ГОСТ 27.005-97. Надежность в технике. Модели отказов. Основные положения. – Введ. 05.12.1997 . – Киев: Госстандарт Украины, 1997. – с.45.

Сведения об авторах

Александр В. Федухин, доктор технических наук, старший научный сотрудник, заведующий лабораторией Гарантоспособных компьютерных систем для критических технологий и инфраструктур, Институт проблем математических машин и систем НАН Украины, Украина, тел. +380679898306 avfedukhin@gmail.com

Наталья В. Сеспедес Гарсия, научный сотрудник лаборатории Гарантоспособных компьютерных систем для критических технологий и инфраструктур, Институт проблем математических машин и систем НАН Украины, Украина, тел. +380932568725, nata05805@gmail.com

Поступила: 03.07.2018

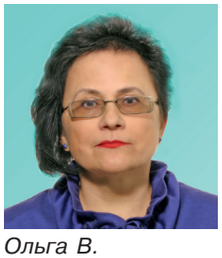
УДК 65.011.42
Оригинальная статья
Надежность, том 18, №4, 2018 DOI: 10.21683/1729-2646-2018-18-4-16-21

Комплекс показателей для оценки надежности газоперекачивающих агрегатов

Игорь Р. Байков, *ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Уфа, Россия*
Сергей В. Китаев, *ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Уфа, Россия*
Ольга В. Смородова, *ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Уфа, Россия*


Игорь Р. Байков


Сергей В. Китаев


Ольга В. Смородова

Резюме. *Работа посвящена совершенствованию методов оценки одной из важнейших эксплуатационных характеристик газоперекачивающего агрегата (ГПА) – его надежности – в условиях снижения загрузки магистральных газопроводов. В настоящее время надежность агрегатов характеризуется комплексом параметров, основанных на определении времени нахождения агрегата в том или ином эксплуатационном состоянии. Представлены основные результаты исследования коэффициентов надежности для ГПА-Ц-18 в количестве 41 агрегат, эксплуатируемых на многоцеховых компрессорных станциях (КС) одного из Дочерних Обществ ПАО «Газпром». Приведены установленные в процессе исследований коэффициенты надежности – коэффициент технического состояния, коэффициент готовности, коэффициент оперативной готовности. Выполнено структурирование ГПА по группам в зависимости от значений коэффициентов. Рассмотрена возможность применения интегральных показателей для анализа уровня надежности ГПА в группах. Предложено использованиедоверительных интервалов для идентификацииинтегрального уровня надежности эксплуатируемого парка ГПА и определения направлений для поддержания работоспособности агрегатов в условиях сниженной загрузки магистральных газопроводов. Для обобщенной оценки уровня надежности ГПА по группам предложен показатель Джини.Показано, что преимущество показателя Джини перед средним значением показателей надежности заключается в возможности учета рангов анализируемых признаков в группах. Графическая интерпретация результатов выполнена с помощью кривой Лоренца. В работе реализовано правило сигм, характеризующее вероятность попадания фактического значения коэффициента в доверительный интервал – границы прогноза (верхняя и нижняя), в которые с заданной вероятностью попадут фактические значения.Доверительные интервалы определены по виду распределения коэффициентов и σ–среднеквадратическому отклонению, в качестве примера приведена гистограммаинтервального ряда распределения коэффициента технического использования.Проверка гипотезы о виде закона распределения на уровне значимости 0,95 показала, что распределение коэффициентов является нормальным. Методом моментов было установлено математическое ожидание и среднеквадратическое отклонение для распределения значений коэффициентов надежности каждого вида.Исключение из массива первичной информации всех резко выпадающих ГПА по уровню факторного признака произведено по правилу «сигм». При этом исключены все агрегаты, у которых значение признака-фактора не попадает в интервал. По правилу «трех сигм» в доверительный интервал ($\mu \pm 3\sigma$) не попали 3 ГПА по коэффициенту технического использования, 2 ГПА по коэффициенту готовности. Проведенный анализ причин низких значений коэффициентов надежности указанных ГПАпоказал, что агрегаты длительно находились в ремонте. В работе приведены сводные данные по максимально допустимому значению показателей дифференциации Джини коэффициентов надежности ($K_{ти}$, $K_{г}$, $K_{ог}$) в зависимости от объема выборки (полная выборка агрегатов – 41 шт. и выборок с интервалом 1, 2, 3 «сигма»). При большем значении показателя Джини рекомендовано принимать меры к отдельным агрегатам для повышения уровня надежности эксплуатируемого фонда ГПА.*

Ключевые слова: *газоперекачивающий агрегат, надежность, отказ, показатель, работоспособность, правило «трех сигм».*

Формат цитирования: *Китаев С.В., Байков И.Р., Смородова О.В. Комплекс показателей для оценки надежности газоперекачивающих агрегатов// Надежность. 2018. Т. 18, № 4. С. 16-21. DOI: 10.21683/1729-2646-2018-18-4-16-21*

Введение

Одной из важнейших характеристик газоперекачивающих агрегатов (ГПА) является надежность. Надежность ГПАкак единого целого определяется надежностью его элементов, обслуживающих его систем и характером их взаимодействия [1-3].

В работе выполнено исследование комплексакоэффициентов для оценки надежности и разработка показателей дифференциации ГПА по их значению. Разрабатываемые коэффициенты могут оказаться полезными при исследовании работоспособности ГПА в компрессорных цехах или групп ГПА на многоцеховых компрессорных станциях (КС).

Анализ объема проведенного исследования

Выбор объекта исследования обоснован необходимостью обеспечения работоспособности газоперекачивающей системы при наступлении аварийного режима. Известно, что перекачка магистрального газа агрегатами средней и малой единичной мощности способствует повышению маневренности системы на основе гарантированного резервирования. При этом выход одного из агрегатов в аварийный останов сопровождается минимальным технологическим ущербом.

Гораздо большие негативные последствия могут быть вызваны аварийным отключением крупного агрегата. В Дочерних обществах ПАО «Газпром» эксплуатируются 5типоразмеров агрегатов высокой единичной мощности (таблица 1).

Из таблицы 1 видно, что максимальную суммарную мощность несут агрегаты ГПА-Ц-18 – более 27% в группе мощных агрегатов (рисунок 1). Более 77% их общего количества – 79 агрегатов – эксплуатируются в ДО «Газпром трансгаз Югорск».

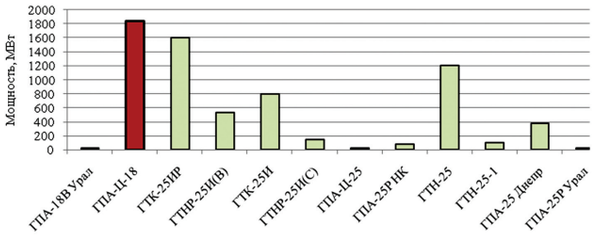


Рисунок 1 – Суммарная мощность ГПА ПАО «Газпром» по типам привода

В соответствии с выявленной структурой парка ГПА объектом исследования были определены газоперекачивающие агрегаты типа ГПА-Ц-18, установленные на многоцеховой (9 компрессорных цехов) КС в количестве 41 агрегат. Это конвертированный тип ГПА с авиационным газотурбинным двигателем. Общая наработка агрегатов на момент исследований составила от 20 тыс. ч до 136 тыс. ч (в среднем 113 тыс. ч).

Определение коэффициентов для оценки надежности ГПА

В настоящее время оценка надежности газотурбинных установок (ГТУ) осуществляется системой показателей [4, 5], основанных на определении времени нахождения агрегата в том или ином эксплуатационном состоянии: суммарном времени нахождения агрегата в работе $T_р$ за отчетный период $T_к$; времени нахождения агрегата в резерве $T_{рез}$; времени нахождения агрегата в плановом ремонте $T_{ппр}$; времени вынужденного простоя $T_в$ газоперекачивающего агрегата за отчетный период $T_к$:

- коэффициент технического использования агрегата – $K_{ти}$;
- коэффициент готовности агрегата – $K_г$;
- коэффициент оперативной готовности – $K_{ог}$;

Таблица 1. Основные сведения по газоперекачивающим агрегатам высокой единичной мощности, ПАО «Газпром»

№	Тип ГПА	Количество ГПА	Единичная мощность	Доля суммарной мощности в группе крупных агрегатов
			МВт	%
1	ГПА-18В Урал	1	18	0,3
	ГПА-Ц-18	102	18	27,3
2	ГТК-25ИР	72	22,2	23,8
	ГТНР-25И(В)	24	22,2	7,9
3	ГТК-25И	33	24	11,8
4	ГТНР-25И(С)	6	24,5	2,2
5	ГПА-Ц-25	1	25	0,4
	ГПА-25Р НК	3	25	1,1
	ГТН-25	48	25	17,8
	ГТН-25-1	4	25	1,5
	ГПА-25 Днепр	15	25	5,6
	ГПА-25Р Урал	1	25	0,4
	ИТОГО	310		

- средняя наработка агрегата на отказ в отчетном отрезке времени – T_0;

- коэффициентвремени восстановления работоспособности агрегата – $K_в$.

В работах многих авторов было показано [1, 2], что в первую очередь интенсивность отказов, определяющая надежность эксплуатации оборудования, связана с процессом старения ГПА. Вместе с тем, техническое состояние ГПА может не только поддерживаться, но и корректироваться мероприятиями предупредительных ремонтов и диагностического обслуживания. Временной режим нахождения ГПА в каждом эксплуатационном состоянии не связан напрямую с общей наработкой агрегата и является дополнительным показателем определения его надежности. Взаимная их независимость подтверждается значением коэффициента взаимной корреляции: его величина находится в диапазоне (–0,094; 0,126) для разных коэффициентов, что подтверждает отсутствие корреляционной связина значимом уровне.

На рисунке 2 приведено распределение значений показателей надежности для ГПА-Ц-18. Анализ выполнен по результатам эксплуатации агрегатов за период времени 2 года.

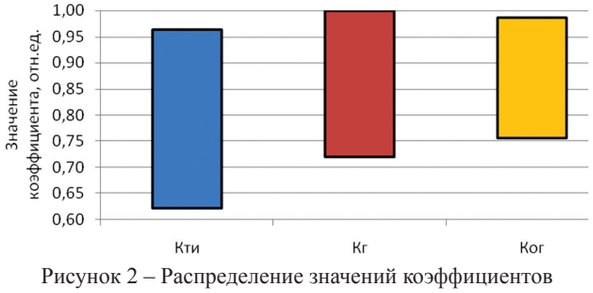


Рисунок 2 – Распределение значений коэффициентов надежности для ГПА

На рисунке 3 приведены структурные диаграммы распределения коэффициентов надежности по интервалам. Интервальная оценка коэффициентов надежности, приведенная на графиках, использовалась для разработки и обоснования показателей дифференциации.

Как показывают проведенные исследования, для агрегатов ГПА-Ц-18 коэффициент технического использования находится на уровне 0,621÷0,963; коэффициент готовности – 0,719÷1,0; коэффициент оперативной готовности – 0,755÷0,986. Наработка на отказ находится в среднем на уровне T_0 = 2900 час; коэффициент, характеризующий время восстановления, в среднем составляет $K_в$ = 70 часов.

Значения коэффициента технического использования для конвертированных ГПА должны составлять не менее 0,94, коэффициентов готовности – не менее 0,98, наработка на отказ – не менее 3500 ч [6].

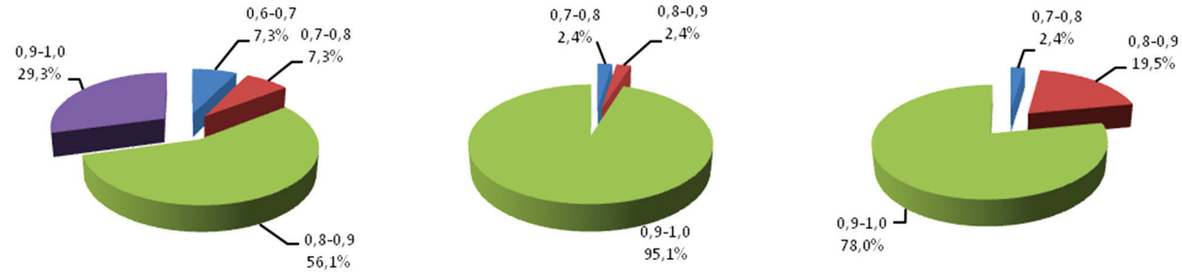
Таким образом, подавляющее количество ГПА из рассматриваемой группы имеет значения коэффициентов ниже значений, установленных ГОСТ [6]: по коэффициенту технического использования – 93% агрегатов, по коэффициенту готовности – 10%, по коэффициенту оперативной готовности – 95%, по наработке на отказ – 76%.

Определение обобщенных показателей надежности ГПА

Отклонение коэффициентов от нормативных величин связано с пониженной загрузкой магистральных газопроводовниже проектного значения и перекачкой газа меньшим количеством ГПА. В таких осложненных условиях существует потребность в дополнительных методах идентификации уровня надежности ГПА эксплуатируемого парка.

Для принятия решения о надежности ГПАобобщенно по предприятию для планирования ремонтных мероприятий разного уровня и оптимизации режимов работы выполнена интегральная оценка показателей надежности парка газоперекачивающего оборудования как единого целого. В качестве обобщенного показателя использован индекс Джини.

Первоначально коэффициент Джини был введен в экономической отрасли как индекс концентрации доходов населения [7] для оценки степени неравенства между отдельными группами общества. Применение показателя в нефтегазовой отрасли было реализовано авторами [8, 9] для дифференциации оборудования по техническому состоянию и режимным параметрам в добыче, трубопроводном транспорте и переработке углеводородов.Теоретически величина коэффициента Джини может находиться в пределах от 0 до 1. Чем ближе значение к единице, тем сильнее дифференциация оборудования по изучаемому показателю.



а – коэффициент технического использования б – коэффициент готовности в – коэффициент оперативной готовности

Рисунок 3 – Интервальная структура коэффициентов оценки надежности ГПА

Применительно к оценке различия в уровне надежности ГПА, показатель Джини будет характеризовать дифференциацию ГПА по уровню надежности, характеризуемой коэффициентами технического использования, готовности и оперативной готовности. Коэффициент Джини определяется по формуле (рисунок 4а):

$$K_L = 1 - 2\sum_i X_i \operatorname{cum} Y_i + \sum_i X_i Y_i,$$

где X_i – доля ГПА в i-ой группе; Y_i – доля i-й группы в совокупном уровне коэффициентов; $\operatorname{cum} Y_i$ – кумулятивная (вычисленная нарастающим итогом) доля коэффициентов.

Для расчета показателя Джини используются данные о распределении ГПА по уровню показателей надежности. Вся совокупность разделена на N групп с равным количеством ГПА, и определена доля каждой группы в общей сумме коэффициентов. По накопленным итогам удельных весов (частот) по численности ГПА и удельных весов в общей сумме показателей построена кривая концентрации (кривая Лоренца).

Вертикальная ось графика отражает накопление доли групп в общей сумме показателя (от 0% до 100% или от 0 до 1). Горизонтальная ось – накопленные доли групп ГПА в общем количестве (также от 0% до 100% или от 0 до 1). При равномерном распределении показателя каждая процентная группа ГПА имела бы точно такую же часть от всей суммы показателя. На графике это отображается диагональю, называемой линией равномерного распределения.

Фактическое распределение показателя отображается вогнутой вниз линией концентрации. Чем больше эта линия отклоняется от диагонали, тем сильнее неравномерность в распределении показателя (выше уровень концентрации). По результатам расчета построены графические зависимости кривых концентрации значений коэффициентов: технического использования (рисунок 4б), готовности и оперативной готовности.

Теоретически характеристика концентрации значений коэффициента может совпасть с линией равномерного распределения, в этом случае показатель дифференциации (Джини) будет равен нулю и тогда уровень надежности ГПА в группе будет равномерным.

Как видно (рисунок 4а), расчетные значения показателей дифференциации (Джини) невысоки, что свидетельствует о незначительном различии ГПА по уровню надежности. Однако для основной доли ГПА значения коэффициентов ниже нормативных величин. При этом остается неопределенность в принятии решения по выбору стратегии к способу эксплуатации фонда ГПА в условиях пониженной загрузки МГ.

Статистическая оценка уровня надежности ГПА

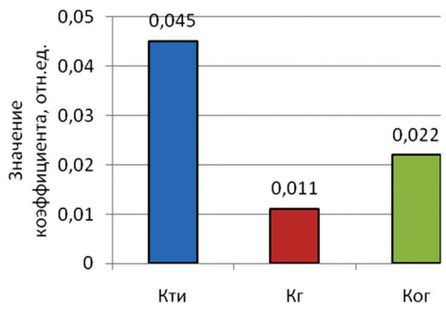
В теории надежности существует правило сигм, характеризующее вероятность попадания очередного фактического значения в доверительный интервал. С помощью доверительного интервала можно выделить направления, на которые следует обратить внимание для изменения тенденции, принять взвешенное решение (например, определить стратегию проведения ремонтно-технического обслуживания ГПА). Для коэффициентов надежности доверительный интервал – это границы прогноза (верхняя и нижняя), в рамки которых с заданной вероятностью попадут фактические значения.

Если доверительный интервал будет равен:

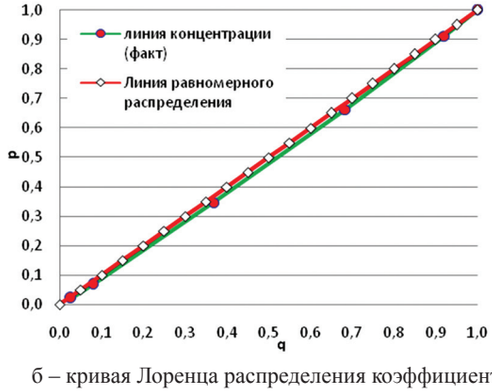
- 3 сигма – существует 0,3% вероятности выхода показателя за границы интервала;
- 2 сигма –существует 4,5% вероятности выхода показателя за границы интервала;
- 1 сигма – существует 31,7% вероятности выхода показателя за границы интервала.

Доверительный интервал определен по виду распределения коэффициента технического использования и σ – среднеквадратическому отклонению. На рисунке 5а приведена гистограмма интервального ряда распределения коэффициента технического использования.

Проверка гипотезы о виде закона распределения на уровне значимости 0,95 показала, что распределение коэффициентов является нормальным (рисунок 5). Для интервального ряда их значений методом моментовбыли

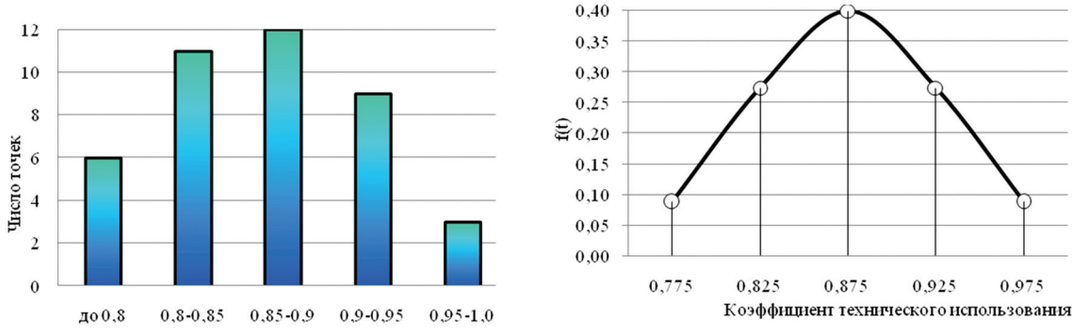


а – значения коэффициентов концентрации



б – кривая Лоренца распределения коэффициента технического использования

Рисунок 4 – Показатель дифференциации для выборки ГПА (41 шт.)



а – гистограмма распределения б – плотность нормального распределения

Рисунок 5 – Распределение коэффициента технического использования

Таблица 2 – Оценка массива данных коэффициентов $K_{ти}$, $K_{т}$, $K_{ог}$ по правилу «сигм»

Наименование коэффициента	Интервалы для массива данных коэффициентов	Интервалы значений признакафактора	Число единиц, входящих в интервал	Удельный вес единиц, входящих в интервал, в общем их числе, %
1	*2*	*3*	*4*	*5*
$K_{ти}$	$\bar{y}-\sigma \le y_i \le \bar{y}+\sigma$	$0,817 \le y_i \le 0,933$	30	73,2
	$\bar{y}-2\sigma \le y_i \le \bar{y}+2\sigma$	$0,760 \le y_i \le 0,990$	37	90,2
	$\bar{y}-3\sigma \le y_i \le \bar{y}+3\sigma$	$0,702 \le y_i \le 1,048$	38	92,7
$K_{т}$	$\bar{y}-\sigma \le y_i \le \bar{y}+\sigma$	$0,977 \le y_i \le 0,993$	12	29,3
	$\bar{y}-2\sigma \le y_i \le 2\bar{y}+2\sigma$	$0,970 \le y_i \le 1,0$	39	95,1
	$\bar{y}-3\sigma \le y_i \le \bar{y}+3\sigma$	$0,962 \le y_i \le 1,008$	39	95,1
$K_{ог}$	$\bar{y}-\sigma \le y_i \le \bar{y}+\sigma$	$0,889 \le y_i \le 0,962$	28	68,3
	$\bar{y}-2\sigma \le y_i \le 2\bar{y}+\sigma$	$0,852 \le y_i \le 0,998$	39	95,1
	$\bar{y}-3\sigma \le y_i \le \bar{y}+3\sigma$	$0,716 \le y_i \le 1,035$	41	100

установленыматематические ожиданияи среднеквадратические отклонения (рисунок 5б).

Исключение из массива первичной информации всех выпадающих ГПА по уровню факторного признака произведено по правилу «сигм» (таблица 2). При этом исключаются все агрегаты, у которых значение признака-фактора не попадает в интервал.

В таблице 3 приведены расчетные значения показателя дифференциации (Джини) для выборок с разбросом 1σ, 2σ, 3σ.

Таблица 3 – Расчетные значения показателя дифференциации (Джини) для выборок с интервалом 1σ, 2σ, 3σ

Интервал значений	Показатель дифференциации Джини		
	для $K_{ти}$	для $K_{т}$	для $K_{ог}$
1 сигма	0,016	0	0,006
2 сигма	0,029	0	0,016
3 сигма	0,032	0	0,019

В соответствии с теоремой Чебышева в технике принято придерживаться правила «трех сигм», что позволяет с достаточной степенью вероятности обеспечить надежность эксплуатации фонда оборудования. В интервал (μ±3σ) попадают не все значения– можно исключить три ГПА с наименьшими значениями коэффициента технического использования 0,621 (ГПА №3 КЦ-10), 0,663 (ГПА №1 КЦ-2) и 0,681 (ГПА №4 КЦ-7).

По правилу «трех сигм» в доверительный интервал не попали значения коэффициента готовности 0,816 (ГПА №1 КЦ-2) и 0,719 (ГПА №4 КЦ-7).

Проведенный анализ причин низких значений коэффициентов надежности выбранных ГПА, оказавшихся вне доверительного интервала, показал, что агрегаты длительно находились в ремонте по причине отказа и задержки поставки запасных частей.

На рисунке 6 приведены сводные данные по показателю дифференциации Джини коэффициентов надежности ($K_{ти}$, $K_{т}$, $K_{ог}$) в зависимости от объема выборки (полная выборка агрегатов – 41 шт. и выборок с интервалом 1σ, 2σ, 3σ).

Таким образом, в соответствии с проведенными исследованиями для конвертированных агрегатов ГПА-Ц-18 значения показателей Джини согласно правилу «трех сигм» должны составлять для коэффициента техниче-

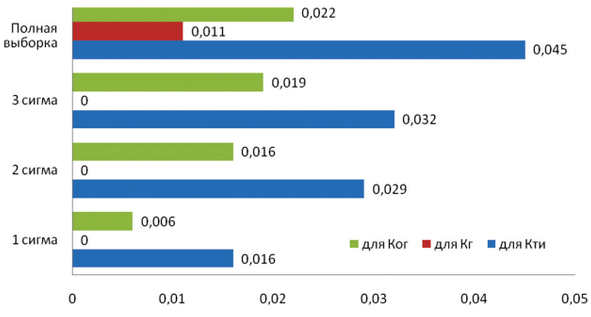


Рисунок 6 – Гистограмма распределения показателя дифференциации Джини

ского использования –не более 0,032, коэффициента готовности – не более 0, коэффициента оперативной готовности – не более 0,019.

Преимущество показателей Джини перед среднеарифметическим значением коэффициентов для анализируемых группзаключается в более адекватном расчете показателей. Достоинством индекса Джини является возможность учета рангов анализируемых признаков в группах (с исключением влияния единичных ГПА) и выявление степени дифференциации группГПА по показателям надежности.

Заключение

1. Определены значения коэффициентов надежности (на примере ГПА-Ц-18, выборка составила 41 ГПА): коэффициент технического использования – 0,621÷0,963; коэффициент готовности – 0,719÷1,0; коэффициент оперативной готовности – 0,755÷0,986. При этом преобладающее количество ГПА из рассматриваемой группы имеет значения коэффициентов ниже допустимых по ГОСТ, причиной является сниженная загрузка магистральных газопроводов.

2. Предложены показатели дифференциации групп ГПА по уровню надежности (Джини) для коэффициентов технического использования, готовности и оперативной готовности. Преимущество показателя Джини заключается в более адекватной оценке уровня различия, позволяющей учесть ранги анализируемых признаков в группах.

3. В соответствии с правилом «трех сигм» для ГПА-Ц-18 с наработкой до 136 тыс. ч значения коэффициента Джини составляют (не более) для коэффициента технического использования – 0,032, коэффициента готовности – 0, коэффициента оперативной готовности – 0,019. При большем значении показателя Джини рекомендованопредпринимать меры к отдельным агрегатам для повышения уровня надежности эксплуатируемого фонда ГПА.

4. Для других типов агрегатов, эксплуатируемых в группах на КС, необходимо проведение дополнительных исследований с учетом индивидуальных технических характеристик ГПА, технических и климатических условий эксплуатации.

Библиографический список

1. Байков И.Р., Смородова О.В., Китаев С.В. Оценка параметров надежности агрегатов перекачки магистрального газа // Электронный научный журнал Нефтегазовое дело. – 2017. – № 1. – С. 95-107. URL: http://ogbus.ru/issues/1_2017/ogbus_1_2017_p95-107_BaikovIR_ru.pdf

2. Китаев С.В., Кузнецова М.И. Статистическое моделирование показателей надежности газотурбинных установок методом «Монте-Карло» // Газовая промышленность. 2014. №5. С.101−103.

3. Смородов Е.А., Китаев С.В. Методы расчета коэффициентов технического состояния ГПА // Газовая промышленность. – 2000. – № S. – С. 29-31.

4. ГОСТ 27.002-2015. Надежность в технике. Термины и определения. – М.: Стандартинформ, 2015. – 28 с.

5. ГОСТ Р 52527-2007 (ИСО 3977-9:1999). Установки газотурбинные. Надежность, готовность, эксплуатационная технологичность и безопасность. – М.: Стандартинформ, 2006. – 32 с.

6. ГОСТ Р 54404. Агрегаты газоперекачивающие с газотурбинным приводом. Общие технические условия. – М.: Стандартинформ, 2012. – 16 с.

7. Харченко Л.П., Ионин В.Г., Глинский В.В. и др. Статистика. Под. ред. канд. эконом. наук, проф. В.Г. Ионина.-3 изд., перераб. и доп. – М.: Инфра-М, 2008. – 445 с.

8. Байков И.Р., Китаев С.В., Валиев А.Н., Зуев А.С., Старостин В.В. Энергосбережение при эксплуатации фонда центробежных электронасосов на нефтяных промыслах // Транспорт и хранение нефтепродуктов и углеводородного сырья. – 2011. – №4. – С. 23-26.

9. Смородова О.В., Китаев С.В., Сергеева К.В. Ранжирование технологических установок нефтепереработки по обобщенному критерию промышленной безопасности // Электронный научный журнал Нефтегазовое дело. – 2017. – № 4. – С. 165-179. URL: http://ogbus.ru/issues/4_2017/ogbus_4_2017_p165-179_SmorodovaOV_ru.pdf

Сведения об авторах

Игорь Р. Байков, доктор технических наук, профессор, заведующий кафедрой «Промышленная теплоэнергетика», факультет трубопроводного транспорта, Уфимский государственный нефтяной технический университет, Уфа, Россия, e-mail:pte@rusoil.net

Сергей В. Китаев, доктор технических наук, доцент, профессор кафедры «Транспорт и хранение нефти и газа», факультет трубопроводного транспорта, Уфимский государственный нефтяной технический университет, Уфа, Россия, e-mail: svkitaev@mail.ru

Ольга В. Смородова, кандидат технических наук, доцент, доцент кафедры «Промышленная теплоэнергетика», факультет трубопроводного транспорта, Уфимский государственный нефтяной технический университет, Уфа, Россия, e-mail:olga_smorodova@mail.ru

Поступила: 30.03.2018

Оригинальная статья
DOI: 10.21683/1729-2646-2018-18-4-22-27

Исследование эксплуатационной надежности автомобильных двигателей

Юрий В. Баженов, *ФГБОУ ВО «Владимирский государственный университет имени А.Г. и Н.Г. Столетовых», Владимир, Россия*
Михаил Ю. Баженов, *ФГБОУ ВО «Владимирский государственный университет имени А.Г. и Н.Г. Столетовых», Владимир, Россия*


Юрий В. Баженов


Михаил Ю. Баженов

Резюме. *Проблема повышения надежности двигателя, который является наиболее сложным и дорогостоящим агрегатом в составе автотранспортного средства, не может быть решена без объективной и достоверной информации по отказам и неисправностям его составных частей, причинам их возникновения, фактическим ресурсам, а также факторам, влияющим на эти показатели в реальных условиях эксплуатации. Заводы-изготовители не всегда имеют такую информацию, в результате чего среди причин потери двигателями работоспособного состояния нередко встречаются конструктивные отказы, связанные с несовершенством их проектирования и конструирования.* **Целью** *данной работы является исследование эксплуатационной надежности двигателя с использованием полученных результатов при организации их технического обслуживания и ремонта.* **Методы исследования** *базировались на эксплуатационных испытаниях двигателей, которые позволяют получить наиболее полную и объективную информацию об их надежности, так как проводились в типичных условиях функционирования автотранспортных предприятий в процессе проведения технического обслуживания и ремонта автомобилей. Результаты исследований, обработанные с помощью стандартной программы Statistica 6.0, представлены в виде статистических оценок надежности основных конструктивных элементов двигателя (наработок до отказа, изменение вероятностей их безотказной работы по пробегу). Анализ полученной информации позволяет оценить уровень фактической надежности двигателя, выявить слабые места в его конструкции, разработать конкретные мероприятия по повышению эксплуатационной надежности. Получаемая при таких испытаниях информация полезна не только для производителей двигателей, но и для сферы эксплуатации, так как позволяет научно обосновать нормативы обеспечения их работоспособного состояния. Для выявления и локализации конкретных неисправностей двигателей при проведении их обслуживания и ремонта обоснован комплекс диагностических параметров с их нормативными значениями.* **Выводы.** *На основе выполненных исследований сформирован комплекс диагностических параметров для оценки технического состояния основных систем двигателя (цилиндропоршневой группы, кривошипно-шатунного и газораспределительного механизмов), которые определяют и лимитируют его надежность. Внедрение результатов исследования в технологические процессы технического обслуживания и ремонта автомобилей позволяет существенно повысить эксплуатационную надежность двигателей и снизить затраты на обеспечение их работоспособного состояния.*

Ключевые слова: *двигатель, автомобиль, надежность, отказ, наработка, структурный параметр, диагностический параметр, техническое состояние.*

Формат цитирования: *Баженов Ю.В., Баженов М.Ю. Исследование эксплуатационной надежности автомобильных двигателей // Надежность. 2018. Т. 18, № 4. С. 22-27. DOI: 10.21683/1729-2646-2018-18-4-22-27*

Для решения проблемы обеспечения высокого уровня надежности и работоспособности технических систем необходимы различные сведения об условиях их работы, действующих на них нагрузках, характере и причинах возникновения отказов и неисправностей. Наличие такой информации является необходимым условием повышения надежности систем на всех стадиях их жизненного цикла и основой для разработки мероприятий по совершенствованию конструкций, технологическим процессам их изготовления и эксплуатации. Все это в полной мере относится и к двигателю внутреннего сгорания, наиболее сложному и дорогостоящему агрегату автомобиля, на который приходится до 20% всех его отказов.

Заводы-изготовители двигателей не всегда имеют достоверную информацию о неисправностях, возникающих в процессе эксплуатации, причинах нарушения работоспособности, наработках до предельного состояния и других показателях, характеризующих эксплуатационную надежность выпускаемой ими продукции. В результате в реальных условиях эксплуатации среди причин отказов двигателей нередко встречаются конструктивные отказы, связанные с несовершенством их проектирования и конструирования.

Источником достоверных сведений о надежности двигателей, как и любого механизма и системы автомобиля, являются испытания (доводочные, исследовательские, приемочные, квалификационные и др.). Наиболее объективную и исчерпывающую информацию о надежности двигателей дают эксплуатационные испытания, которые проводят в типичных условиях эксплуатации автомобилей с выполнением присущей им транспортной

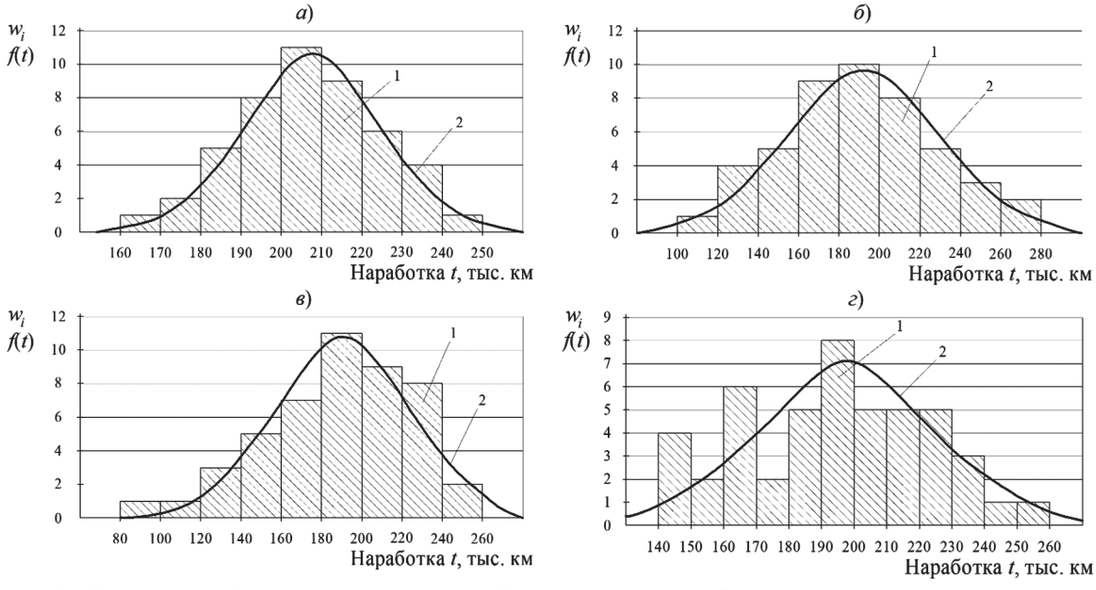


Рисунок 1 – Гистограммы (1) и теоретические кривые (2) распределения наработок до отказа конструктивных элементов двигателя: *а* – блок цилиндров; *б* – головка блока; *в* – поршневая группа; *г* – коленчатый вал

Таблица 1 – Статистические оценки числовых характеристик надежности двигателей

№ п/п	Наименование конструктивных элементов двигателя	Средний ресурс $t_{ср}$, тыс. км	Среднее квадратическое отклонение σ, тыс. км	Коэффициент вариации ν
1	Блок цилиндров	203,7	34,5	0,169
2	Вал коленчатый	198,4	39,2	0,198
3	Промежуточный вал	141,8	41,7	0,294
4	Вал распределительный	194,6	26,8	0,138
5	Поршневая группа	191,6	35,3	0,184
6	Кольца поршневые	148,2	45,2	0,304
7	Вкладыши нижних головок шатунов	164,0	41,4	0,254
8	Вкладыши подшипников коленчатого вала	166,0	40,6	0,245
9	Втулка верхней головки шатуна	195,9	52,9	0,270
10	Поршневой палец	186,2	37,2	0,200
11	Направляющая втулка клапана	154,6	34,0	0,220
12	Клапан выпускной	169,0	34,8	0,206
13	Толкатель гидравлический	131,8	39,8	0,302
14	Головка блока цилиндров	193,6	39,0	0,201

работы. Получаемая при таких испытаниях информация полезна не только для производителей двигателей, но и для сферы эксплуатации, так как позволяет научно обосновать нормативы обеспечения их работоспособного состояния.

В данной работе исследования надежности двигателей проводились в реальных условиях эксплуатации с регистрацией данных об их состоянии в процессе проведения технического обслуживания и ремонта автомобилей. В качестве объекта исследования был принят двигатель ЗМЗ-4063.10 Заволжского моторного завода, устанавливаемый на автомобили семейства «Газель». По результатам исследований собран большой массив информации по возникающим в процессе эксплуатации автомобилей неисправностям и отказам двигателей.

Результаты исследований эксплуатационной надежности основных конструктивных элементов двигателей, обработанные с помощью компьютерной программы Statistica 6.0, представлены в табл. 1 и частично, в виде гистограмм и сглаживающих их теоретических кривых распределения наработок до отказа, на рис. 1.

Вид кривых, а также рассчитанные значения коэффициентов вариации ν показывают, что распределения наработок до отказа деталей двигателя хорошо описываются нормальным законом. Проверка гипотезы о принадлежности опытных данных нормальному распределению с помощью критерия согласия χ^2 Пирсона подтвердила её правомерность.

Одним из основных показателей, оценивающих надежность конструктивных элементов двигателя, служит вероятность их безотказной работы $P(t)$ или отказа $F(t)$ в пределах заданной наработки. В табл. 2 приведены результаты обработки статистических данных по эксплуатационной надежности основных деталей исследуемых двигателей, которые наглядно показывают изменение вероятности их отказов по наработке t.

Анализируя приведенные в таблице данные, можно сделать некоторые выводы по эксплуатационной надежности деталей исследуемых двигателей. Для начальных интервалов наработки от 0 до 90 тыс. км вероятность безотказной работы деталей находится на достаточно высоком уровне. В этот период эксплуатации с невысокой долей вероятности могут потерять свою работоспособность выпускные клапана и гидравлические толкатели газораспределительного механизма, которые подвергаются большим механическим и тепловым нагрузкам при работе двигателя. К наработке 154 тыс. км существенно снижается вероятность безотказной работы промежуточного вала, прокладок головок блока цилиндров, поршневых колец, вкладышей нижних головок шатуна и направляющих втулок клапана. В интервале наработки от 154 до 218 тыс. км наблюдается резкое увеличение вероятности отказов двигателя, которая для разных деталей колеблется от $F(t) = 0{,}620$ (втулка верхней головки шатуна) до $F(t) = 0{,}995$ (выпускной клапан). Практически все детали двигателя полностью реализуют свой ресурс к наработке 250 тыс. км. Вероятность отказа базовой детали двигателя, блока цилиндров, достигает к этой наработке значения $F(t) = 0{,}911$, что указывает на необходимость проведения капитального ремонта двигателя или его списания.

Среди причин такого уровня эксплуатационной надежности двигателя, кроме факторов конструирования и производства, следует отметить и влияние условий его эксплуатации: состояние дорог, хранение, природно-климатические условия, производственно-техническая база и др. К условиям эксплуатации относится и система ТО, включающая в себя комплекс контрольно-диагностических, профилактических и ремонтных мероприятий, направленных на обеспечение работоспособности двигателей.

Для обеспечения надежной работы двигателя и снижения затрат на проведение ремонтных операций

Таблица 2 – Вероятности отказов основных деталей двигателя ЗМЗ-4063 по наработке

№ п/п	Наименование деталей	Вероятность отказа $F(t)$ на наработке, тыс. км						
		58	90	122	154	186	218	250
1	Блок цилиндров	0	0,001	0,009	0,075	0,304	0,661	0,911
2	Вал коленчатый	0	0	0,004	0,065	0,336	0,749	0,961
3	Вал промежуточный	0,022	0,107	0,317	0,615	0,856	0,966	0,995
4	Вал распределительный	0	0	0,003	0,065	0,375	0,810	0,981
5	Поршневая группа	0	0,002	0,024	0,143	0,437	0,773	0,951
6	Кольца поршневые	0,023	0,099	0,281	0,551	0,799	0,939	0,988
7	Вкладыши нижних головок шатунов	0,005	0,037	0,161	0,405	0,702	0,904	0,981
8	Вкладыши подшипников коленчатого вала	0,004	0,030	0,139	0,384	0,689	0,901	0,981
9	Втулка верхней головки шатуна	0,005	0,023	0,081	0,214	0,426	0,620	0,847
10	Поршневой палец	0	0,005	0,042	0,194	0,438	0,804	0,957
11	Направляющая втулка клапана	0,002	0,031	0,169	0,493	0,807	0,969	0,997
12	Клапан выпускной	0,053	0,221	0,5314	0,827	0,962	0,995	0,999
13	Толкатель гидравлический	0,071	0,229	0,493	0,759	0,923	0,984	0,998
14	Головка блока цилиндров	0	0,001	0,033	0,155	0,423	0,735	0,926
15	Прокладка головки блока цилиндров	0,006	0,069	0,332	0,729	0,951	0,996	0,999

после отказов необходимо, чтобы большая их часть была предупреждена при выполнении регламентных ТО. Поэтому при проведении ТО весьма важно иметь индивидуальную информацию о техническом состоянии двигателя, скрытых и назревающих в нем отказов, причинах нарушения работоспособности и т.д. Такая информация может быть получена при диагностировании двигателя путем измерения параметров, характеризующих его состояние и сопоставления их с нормативными значениями.

Разнообразие и значительное число диагностических параметров, оценивающих состояние ДВС, вызывает необходимость выбора из них наиболее информативных, которые характеризуются чувствительностью изменения их значений с изменением структурных параметров и однозначностью в постановке диагноза. Обоснование комплекса диагностических параметров для оценки технического состояния двигателя осуществлялось на основе анализа статистических данных по отказам и неисправностям его конструктивных элементов, закономерностей изменения технического состояния механизмов и узлов, разработанных схем структурно-следственных связей для основных систем двигателя, которые определяют и лимитируют его ресурс (цилиндропоршневой группы, кривошипно-шатунного механизма, механизма газораспределения). Не менее важным условием выбора диагностических параметров является возможность по их текущим значениям оценивать остаточный ресурс двигателя (запас его исправной работы).

Поэтому такие параметры, как анализ качественного и количественного состава продуктов износа в масле, расход масла на угар, разряжение в камере сгорания, массовый расход топлива, содержание вредных выбросов в отработавших газах и некоторые другие мало информативны или требуют больших затрат времени на постановку диагноза. В табл. 3 приведены диагностические параметры, отвечающие предъявляемым к ним требованиям, а также перечень структурных параметров, которые они оценивают.

Нормативные значения номинальных и предельных значений диагностических параметров, установленные заводом-изготовителем для двигателей ЗМЗ-4061.10, 4063.10, 40637.10, приведены в табл. 4.

В процессе эксплуатационных испытаний надежности двигателей исследовалось влияние значений приведенных в табл. 3 зазоров в сопряжениях на оценивающие их диагностические параметры. С этой целью перед выполнением ТО-2 контролировалось техническое состояние механических систем ДВС. В случае, когда значения диагностических параметров превышали предельно допустимые, двигатели направлялись на участок ремонта, где подвергались частичной или, при необходимости, полной разборке и измерению соответствующих зазоров. По мере накопления данных о результатах измерений была сформирована база данных, по результатам обработки которой построены регрессионные модели, характеризующие влияние структурных параметров

Таблица 3 – Структурные и оценивающие их диагностические параметры двигателя ЗМЗ-4063

№ п/п	Диагностический параметр	Структурный параметр
1	Давление в конце такта сжатия – S_1	• Зазор между поршнем и 1-м компрессионным кольцом по высоте канавки – Y_1 • Зазор в стыке 1-го компрессионного кольца – Y_2 • Зазор между поршнем и 2-м компрессионным кольцом по высоте канавки – Y_3 • Зазор в стыке 2-го компрессионного кольца – Y_4 • Зазор между поршнем и блоком цилиндров – Y_5 • Зазор «стержень клапана – направляющая втулка» – Y_6 • Зазор «клапан-седло клапана» – Y_7
2	Значение относительной утечки воздуха при положении поршня в ВМТ – S_2	• Зазор между поршнем и 1-м компрессионным кольцом по высоте канавки – Y_1 • Зазор в стыке 1-го компрессионного кольца – Y_2 • Зазор между поршнем и 2-м компрессионным кольцом по высоте канавки – Y_3 • Зазор в стыке 2-го компрессионного кольца – Y_4 • Зазор между поршнем и блоком цилиндров – Y_5 • Зазор «стержень клапана – направляющая втулка» – Y_6 • Зазор «клапан – седло клапана» – Y_7
3	Расход картерных газов – S_3	• Зазор между поршнем и 1-м компрессионным кольцом по высоте канавки – Y_1 • Зазор в стыке 1-го компрессионного кольца – Y_2 • Зазор между поршнем и 2-м компрессионным кольцом по высоте канавки – Y_3 • Зазор в стыке 2-го компрессионного кольца – Y_4 • Зазор между поршнем и блоком цилиндров – Y_5
4	Давление в главной масляной магистрали – S_4	• Зазор «шатунная шейка – вкладыш» – Y_8 • Зазор «коренная шейка – вкладыш» – Y_9 • Зазор «втулка промежуточного вала – шейка вала» – Y_{10} • Зазор «опора распределительного вала – шейка вала» – Y_{11}

Таблица 4 – Нормативные значения диагностических параметров, оценивающих состояние двигателя

№ п/п	Диагностический параметр	Номинальное	Предельное
1	Давление в конце такта сжатия, кгс/см^2	12	9,6
2	Значение относительных утечек воздуха при положении поршня в ВМТ, кгс/см^2 в течении не менее 5 с	снижение с 1,5 до 1	снижение с 1,5 до 0,75
3	Расход картерных газов при 4000 мин$^{-1}$, л/мин не более	22	62
4	Значение давления в главной масляной магистрали, кгс/см^2: при 2500 мин$^{-1}$ при 700-800 мин$^{-1}$	5,0 –	3,0 1,1

Y систем двигателя на выбранные для их оценки диагностические параметры S:

$S_1 = 0{,}355\ Y_1 + 0{,}054\ Y_2 + 0{,}073\ Y_3 + 0{,}031\ Y_4 + 0{,}16\ Y_5 + 0{,}105\ Y_6 + 0{,}223\ Y_7$;

$S_2 = 0{,}298\ Y_1 + 0{,}037\ Y_2 + 0{,}033\ Y_3 + 0{,}015\ Y_4 + 0{,}104\ Y_5 + 0{,}077\ Y_6 + 0{,}436\ Y_7$;

$S_3 = 0{,}434\ Y_1 + 0{,}078\ Y_2 + 0{,}103\ Y_3 + 0{,}035\ Y_4 + 0{,}350\ Y_5$;

$S_4 = 0{,}294\ Y_8 + 0{,}372\ Y_9 + 0{,}148\ Y_{10} + 0{,}186\ Y_{11}$.

Результаты исследований показали, что степень влияния одних и тех же структурных параметров на выбранные для оценки технического состояния ДВС диагностические параметры имеют разное значение. Зазор, например, между поршнем и 1-м компрессионным кольцом по высоте канавки (Y_1) оказывает доминирующее влияние на диагностические параметры S_1 – давление в конце такта сжатия (35,5%) и S_3 – расход картерных газов (43,4%). На относительную утечку сжатого воздуха S_2 наибольшее влияние оказывает структурный параметр Y_7 – зазор «клапан – седло клапана» (43,6%). На величину диагностического параметра S_4 – давление в главной масляной магистрали основное влияние оказывают зазоры «коренная шейка – вкладыш Y_9» (37,2%) и «шатунная шейка – вкладыш Y_8» (29,4%). Графическая интерпретация степени влияния зазоров на диагностические параметры (в процентах) представлена на рис. 2.

Полученные зависимости диагностических параметров от формирующих их структурных позволяют определить наиболее вероятные отказы механических систем двигателя и сформировать необходимый перечень и алгоритм технических воздействий для восстановления их работоспособности. Например, выход за допустимые пределы параметра S_2 (относительная утечка сжатого воздуха при положении поршня в ВМТ) с большой долей вероятности свидетельствует об увеличенных износах выпускных клапанов, поршней и компрессионных колец и в меньшей степени – об изменениях в остальных элементах двигателя.

Наиболее вероятными неисправностями при отклонении от нормативных значений диагностического параметра S_1 (давление в конце такта сжатия) являются

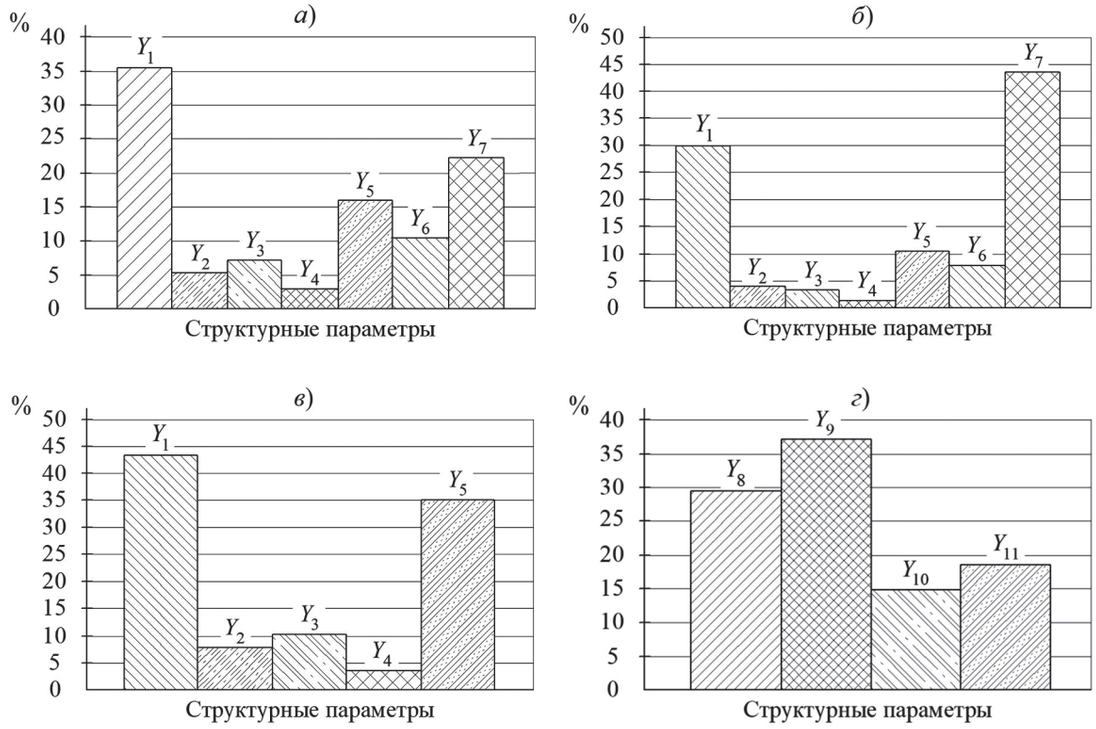


Рисунок 2 – Степень влияния структурных параметров на диагностические: а – давление в конце сжатия; б – относительная утечка воздуха; в – расход картерных газов; г – давление в главной масляной магистрали

износы в сопряжениях «поршень – компрессионное кольцо», «клапан – седло клапана», а также «поршень – блок цилиндров». Выход за допустимое значение диагностического параметра S_4 (давление масла в главной масляной магистрали) свидетельствует об износах в сопряжениях «коренные шейки коленчатого вала – вкладыши подшипников», «шатунные шейки – вкладыши нижних головок шатунов», а также износах шеек промежуточного и распределительного валов.

Результаты выполненных исследований эксплуатационной надежности двигателей позволяют оптимизировать систему их технического обслуживания и ремонта, разработать алгоритмы поиска и устранения возникающих в них неисправностей. Например, до наработки 90 тыс. км нет необходимости контролировать состояние механических систем двигателя, так как вероятности их безотказной работы находятся на достаточно высоком уровне. В интервале наработки 90–122 тыс. км рекомендуется выполнять углубленное диагностирование сопряжений газораспределительного механизма, так как в этом интервале наблюдается существенное увеличение вероятностей отказов их деталей (выпускного клапана, толкателя гидравлического, прокладки головки блока цилиндров). Начиная с наработки 122 тыс. км необходимо контролировать техническое состояние всех структурных параметров двигателя.

Внедрение результатов исследований в технологические процессы ТО и ремонта автомобилей позволяет существенно повысить эксплуатационную надежность двигателей и снизить затраты на обеспечение их работоспособного состояния.

Библиографический список

1. Баженов Ю.В. Основы теории надежности машин: учеб. пособие для вузов. – М.: Форум, 2017. – 320 с.

2. Баженов Ю.В., Баженов М.Ю. Прогнозирование остаточного ресурса конструктивных элементов автомобилей в условиях эксплуатации // Фундаментальные исследования. – 2014. – № 8, ч. 1. – С. 18-23.

3. Баженов Ю.В., Каленов В.П. Обеспечение работоспособного состояния электронных систем управления двигателем в эксплуатации // Автомобильная промышленность. – 2015. – № 12. – С. 23-27.

4. Денисов А.С. Обеспечение надежности автотракторных двигателей / А.С. Денисов, А.Т. Кулаков. – Саратов: Издательство СГТУ, 2007. – 422 с.

5. Денисов И.В. Исследование эксплуатационной надежности систем автомобиля *Lada Kalina*, влияющих на безопасность дорожного движения [Текст] / И.В. Денисов, А.А. Смирнов // Надежность. – 2017. – Том 17, № 4. – С. 31-35.

6. ГОСТ 27578–87. Техническая диагностика. Диагностирование изделий. Общие требования [Текст]. – М.: Изд-во стандартов, 1988. – 20 с.

7. Методические указания. Надежность в технике. Методы оценки показателей надежности по экспериментальным данным. РД 50-690-89. – М.: Издательство стандартов, 1990.

Сведения об авторах

Юрий В. Баженов – кандидат технических наук, профессор кафедры «Автомобильный транспорт», ФГБОУ ВО «Владимирский государственный университет имени А.Г. и Н.Г. Столетовых», Владимир, Россия

Михаил Ю. Баженов – кандидат технических наук, доцент кафедры «Автомобильный транспорт», ФГБОУ ВО «Владимирский государственный университет имени А.Г. и Н.Г. Столетовых», Владимир, Россия, e-mail: bagenovyv@mail.ru

Поступила: 30.03.2018

Оригинальная статья
DOI: 10.21683/1729-2646-2018-18-4-28-35

Что понимать под расчётом надёжности уникальных высокоответственных систем применительно к механизмам одноразового срабатывания космических аппаратов

Юрий П. Похабов, *Акционерное общество «НПО ПМ – Малое Конструкторское Бюро» (АО «НПО ПМ МКБ»), Железногорск, Красноярский край, Россия_*

Юрий П. Похабов

Резюме. Цель. *Расчёты являются неотъемлемой частью разработки любого сложного технического объекта. Обычно они подразделяются на расчёты, подтверждающие работоспособность изделия (кинематические, электрические, тепловые, прочностные, расчёты гидравлических и пневматических систем и пр.), и расчёты, подтверждающие его надёжность (расчёты показателей безотказности, долговечности, ремонтопригодности, сохраняемости и пр.). При этом под расчётами надёжности понимаются и нормативно закреплены процедуры определения значений показателей надёжности объекта с использованием методов, основанных на их вычислении по справочным данным о надёжности элементов объекта, по данным о надёжности объектов-аналогов, данным о свойствах материалов и другой информации, имеющейся к моменту расчёта. Однако в случае разработки уникальных высокоответственных систем получить статистические данные для расчёта надёжности не представляется возможным из-за двух взаимоисключающих условий: ограниченного числа создаваемых объектов и высокой точности требуемой исходной информации. Тем не менее, по мнению автора, расчёты надёжности должны проводиться, вопрос заключается только в том, как считать надёжность и что под таким расчётом понимать.* **Методы**. *В классической теории надёжности под вероятностью безотказной работы принято понимать частоту наступления отказов во времени, но для уникальных высокоответственных систем частота отказов должна стремиться к нулю за весь срок эксплуатации (желательно чтобы отказов вообще не было). По этой причине к понятию «отказ» для уникальных высокоответственных систем разумнее относиться не как к событию – всякому факту, который в результате опыта может произойти или не произойти, а как к возможному риску – нежелательной ситуации или обстоятельству, характеризующемуся вероятностью возникновения и потенциально негативными последствиями. Тогда событию в виде реального или потенциального отказа при эксплуатации можно сопоставить риск в виде вероятности возникновения отказа с негативными последствиями, что с позиций последствий отказов для уникальных высокоответственных систем одинаково недопустимо. В этом случае расчёт надёжности без потери смыслов может быть заменён оценкой риска – процессом, охватывающим идентификацию риска, анализ риска и сравнительную оценку риска. Таким образом, с помощью оценки рисков появляется возможность достигать заданной надёжности напрямую путём обоснования стабильности проявления свойств конкретного изделия, а не опосредованно через ненадёжность, как следствие отказов объектов-аналогов.* **Результаты.** *Приведена последовательность проведения оценки риска для уникальных высокоответственных систем. На примере механической системы с подвижными узлами в виде однозвенной поворотной штанги космического аппарата показаны процедуры проведения оценки риска. Представлена возможность проведения оценки риска с применением конструкторско-технологического анализа надёжности.* **Выводы**. *Показано, что отсутствие статистических данных о надёжности образцов-аналогов уникальных высокоответственных систем не является препятствием для проведения расчётов надёжности в виде оценки риска. Более того, результаты таких расчётов могут быть источником и руководством для принятия конструкторских и технологических решений при разработке и создании изделий с заданной надёжностью. Однако для легализации методики проведения таких расчётов необходима корректировка нормативно-технической документации, позволяющая производить расчёты надёжности иными методами, нежели с использованием статистических данных об отказах образцов-аналогов.*

Ключевые слова: *уникальная высокоответственная система, расчёт, расчёт надежности, оценка риска, конструкторско-технологический анализ надёжности.*

Формат цитирования: *Похабов Ю.П. Что понимать под расчётом надёжности уникальных высокоответственных систем применительно к механизмам одноразового срабатывания космических аппаратов // Надёжность. 2018. Т. 18, № 4. С. 28-35. DOI: 10.21683/1729-2646-2018-18-4-28-35*

Введение

Разработка любых сложных технических изделий невозможна без проведения расчётов – *установления и подсчёта необходимых данных* [1]. Расчёты в виде ***документов**, содержащих расчёт параметров и величин, например, расчёт размерных цепей, расчёт на прочность и др*., входят в номенклатуру конструкторской документации по ГОСТ 2.102. Коды и виды расчётов для изделий машиностроения определены в отраслевом стандарте ОСТ 92-0290. В общем виде, например, согласно ГОСТ 2.119, расчёты разделяются на расчёты, подтверждающие работоспособность изделия (кинематические, электрические, тепловые, прочностные, расчёты гидравлических и пневматических систем и пр.) и расчёты, подтверждающие его надёжность (расчёты показателей безотказности, долговечности, ремонтопригодности, сохраняемости и пр.). Причём в нормативно-технической документации (ГОСТ 27.301 и ГОСТ 27.410) под расчётами надёжности понимаются только *процедуры определения значений показателей надёжности объекта с использованием методов, основанных на их вычислении по справочным данным о надёжности элементов объекта, по данным о надёжности объектов-аналогов, данным о свойствах материалов и другой информации, имеющейся к моменту расчёта*. Что немаловажно, наличие расчётов надёжности на основании справочных данных о надёжности объектов-аналогов несёт юридические и финансовые последствия при страховании рисков утраты объектов [2]. Однако в случае разработки уникальных высокоответственных систем (УВС) получить статистические данные для расчёта надёжности не представляется возможным из-за двух взаимоисключающих условий: ограниченного числа создаваемых объектов и высокой точности требуемой исходной информации. Несмотря на существующее мнение о том, что для абсолютно надёжных систем не имеет смысла делать расчёты надёжности и их следует заменить выполнением качественных критериев надёжности [3], по мнению автора, нет альтернативы, делать или не делать расчёты надёжности при разработке УВС. Существует лишь вопрос, как считать надёжность и что под таким расчётом понимать.

Актуальность проведения расчёта надёжности УВС видна на примере срабатывания одноразовых механизмов космических аппаратов. Эффективность функционирования космических аппаратов на орбите целиком зависит от успешности раскрытия панелей солнечных батарей и космических антенн (рефлекторов), стоимость которых составляет ничтожную долю от суммарных затрат на космический аппарат и средства его выведения. Экспериментальное подтверждение надёжности раскрытия конструкций невозможно из-за высоких требований к безотказности (на уровне 0,9995 и выше) и уникальных внешних условий раскрытия на орбите, которые невозможно в точности воспроизвести при проведении наземной экспериментальной отработки. В то же время практически любая ошибка при конструировании и изготовлении механизмов раскрытия способна привести к отказу, что может закончиться гибелью космического аппарата. Поэтому надёжность в данном случае во многом определяется именно расчётами.

Подходы к проведению расчётов надёжности

Поскольку отказы УВС приводят к потерям несоизмеримо большим, чем затраты на их создание [4], надёжность характеризуется безотказностью и определяется показателем вероятности безотказной работы (ВБР), т.е. *вероятностью того, что в пределах заданной наработки отказ объекта не возникнет* [5, 6]. В классической теории надёжности под ВБР принято понимать частоту наступления отказов во времени, но для УВС частота отказов в теории должна стремиться к нулю за весь срок эксплуатации (желательно чтобы отказов вообще не было). По этой причине к понятию «отказ» для УВС разумнее относиться не как к **событию** – *всякому факту, который в результате опыта может произойти или не произойти* [7], а как к возможному **риску** – *нежелательной ситуации или обстоятельству, характеризующимися вероятностью возникновения и потенциально негативными последствиями* [8]. Причём для механизмов одноразового срабатывания космических аппаратов имеет смысл говорить о риске как *влиянии неопределённости на цели*, где под неопределённостью понимается *«состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей»* [9]. Тогда **событие** в виде реального или потенциального отказа при эксплуатации можно рассматривать как **риск** (вероятность возникновения отказа с негативными последствиями), что с позиций последствий отказов для УВС одинаково недопустимо. В этом случае **расчёт надёжности** без потери смыслов может быть заменён **оценкой риска** – *процессом, охватывающим идентификацию риска, анализ риска и сравнительную оценку риска* [10]. Важно отметить, что риски отказов не несут в себе частотного смысла, но оценка риска позволяет прогнозировать сценарии развития нежелательных ситуаций, способных привести к отказам, и на основании таких оценок принимать технические решения при разработке УВС. Таким образом, с помощью оценки рисков появляется возможность достигать заданной надёжности напрямую путём обоснования стабильности проявления свойств конкретного изделия [11], а не опосредованно через ненадёжность, как следствие отказов объектов-аналогов [12].

Отход от понятия «событие» как факта *нарушения работоспособного состояния объекта* [5, 6] при расчёте надёжности делает чувствительным понимание сущности понятия «надёжность» к её терминологическому определению. По мнению автора, смещение нормативного определения термина «надёжность» в сторону

функционального толкования уводит от возможности понимать надёжность иначе, чем принято в рамках существующего математического аппарата теории надёжности. Употребление понятия «функция» в терминологическом определении надёжности как требований, *установленных в нормативной, конструкторской, проектной, контрактной и* ***иной документации*** *на объект* [6], приводит к абстрагированию физических процессов, происходящих в конструкции изделий, и как следствие не создаёт предпосылок для проведения анализа рисков. Например, раскрытие складных космических аппаратов на орбите в организационно-технической документации рассматривается как функция, обеспечивающая подготовку аппарата к работе в течение заданного срока активного существования, но на физическом уровне достигается спланированной и последовательной работой множества конструктивных элементов, обеспечивающих выполнение данной функции. Функциональное определение надёжности фактически делает «невидимой» работу конструктивных элементов, обеспечивающих в конечном итоге надёжность при выполнении функции раскрытия складных конструкций космического аппарата.

По мнению автора, определение надёжности как *свойства системы сохранять во времени в установленных пределах значения всех параметров* ***и/или показателей****, характеризующих способность системы выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования* [13], даёт единое понимание (непротиворечивость) параметрического и функционального определения надёжности [14] и позволяет производить оценку надёжности как с позиций классической теории надёжности, так и с позиций анализа рисков возникновения отказов. Это становится осуществимым благодаря тому, что появляется возможность рассматривать надёжность как физическую величину с присущими ей простыми и/или существенными свойствами, которые могут быть выражены с помощью параметрических или непараметрических моделей через параметры и/или показатели [11].

В основе методики проведения анализа риска, связанного с возникновением отказов УВС лежат принципы физичности (закономерности причинно-следственных связей) и физической необходимости (непротиворечия законам природы) причин отказов. Задачей анализа рисков при использовании указанных принципов становится анализ и синтез простых свойств, составляющих (существенное) свойство надёжности, что становится возможным благодаря парадигме А.И. Уёмова о триединстве вещей, их свойств и отношений [15], и расширенному толкованию понятия «отношение» как взаиморасположения, взаимосвязи и взаимодействия вещей (предметов, объектов и пр.) [11]. Связь между параметрической и непараметрической природой проявления функций в объектах обнаруживается, если использовать термин «функционирование» из некогда аннулированного стандарта ГОСТ 22487 в значении *«выполнение в объекте (системе) процесса (процессов), соответствующего (соответствующих) заданному алгоритму и (или) проявление объектом заданных свойств»*. В этом случае предписанные организационно-технической документацией функции [6] на физическом уровне могут быть представлены в виде проявления объектом заданных свойств в соответствие с заданным алгоритмом выполняемого процесса. Данное обстоятельство чрезвычайно важно для сложных технических систем, где при функционировании могут одновременно или последовательно проявляться множество свойств, приводящих к выполнению или невыполнению функций, заданных в организационно-технической документации.

Такой подход расширяет возможности классической теории надёжности, применяемой при прочностных расчётах надёжности, позволяя дополнительно производить оценку функционирования изделий по механическим, кинематическим, энергетическим, электрическим и иным параметрам [16]. Причём поскольку на уровне определённой иерархии физические свойства являются независимыми (например, свойства прочности и электропроводности), то в рамках рассмотрения любого из свойств, выявленных в ходе анализа рисков, становится возможным как детерминированный, так и стохастический подход при количественной оценке конкретного рассматриваемого свойства надёжности.

При оценке рисков, в отличие от классических расчётов надёжности, становится возможным исключать неопределённости при разработке изделия, т.е. принимать во внимание то обстоятельство, что задумка конструктора должна быть отражена в конструкторской документации так, чтобы его мысль была понятна лицам, не участвовавшим в разработке и не знакомым с исходными идеями без дополнительных разъяснений и комментариев и, тем более, без утраты смыслов. Чаще всего неопределённости могут быть скрыты в восприятии термина «работоспособное состояние», который определяется как *состояние объекта, в котором он способен выполнять требуемые функции* [6]. С учётом пояснения того, что понимается под функцией в термине «надёжность», данном в Государственном стандарте, невозможно квалифицировать работоспособное состояние как достаточное для выполнения служебного назначения изделия. Ситуацию в каком-то степени проясняет пояснение к термину «работоспособное состояние», согласно которому оно может быть определено как *состояние объекта, в котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствует требованиям, установленным в документации на этот объект* [6]. Это, безусловно, более конкретное определение работоспособного состояния для сложного технического объекта, но и оно грешит серьёзными неточностями. Во-первых, для УВС требования в документации должны быть необходимыми и достаточными, но каким образом этого достичь,

Государственный стандарт не поясняет, что, безусловно, повышает роль человеческого фактора при разработке (кому-то кажется, что требования достаточны для достижения работоспособного состояния изделия, а кому-то – нет). Во-вторых, первичным документом для изготовления изделия является конструкторская документация, а не какая-нибудь *иная документация*, как это трактует всё тот же стандарт. В этом смысле отказ от прежнего определения термина «работоспособное состояние» [5], где чётко фигурирует конструкторская документация, никак не способствует снижению роли того же человеческого фактора (из-за размывания понятий).

Пример и последовательность проведения оценки риска

Рассмотрим пример проведения оценки риска в общем виде. В соответствии с определением термина «оценка риска» [10] на первом этапе проводится *идентификация риска*, которая заключается в выявлении источника риска и возможных причин отказов. На данном этапе определяется функциональность изделия на физическом уровне согласно ГОСТ 28806 в виде *наличия и конкретных особенностей набора функций, способных удовлетворить заданные или подразумеваемые потребности*. Целью данной процедуры является словесное описание отказов как гипотетических ситуаций, препятствующих выполнению конкретных рассматриваемых функций. Предполагается, что каждый из потенциальных отказов происходит из-за причин, непосредственно их порождающих, которые возникают, существуют и развиваются в условиях окружающей действительности как совокупности факторов внешней среды и режимов работы с учётом худших возможных сочетаний. Очевидно, что каждому виду отказов может соответствовать одновременно несколько причин. Выявленные возможные причины отказов в своей совокупности являются базой для составления контрольного списка (чек-листа) при идентификации рисков. Здесь важно понимать, что процедуры идентификации риска определяют полноту выявленной функциональности объекта и должны выполняться специалистами с соответствующей квалификацией, поскольку результаты выполнения этих процедур используются для наполнения чек-листа и служат в конечном итоге критериями для установления необходимых и достаточных требований в конструкторской документации.

На последующем этапе оценки рисков проводится анализ, который подготавливает информационную базу для сравнительной оценки рисков и принятия решения по воздействию на их источники. Процедуры проведения анализа риска подчинены следованию заданному алгоритму в строгом соответствии с общей логикой действий согласно чек-листу (в данном случае выявленные причины отказов являются отправной точной для всех дальнейших действий при анализе и оценки рисков):

- определяются свойства критичных элементов конструкции, наличие которых делает невозможной каждую из причин отказов;
- каждое из свойств критичных элементов определяется количественно с помощью параметров (показателей);
- каждому параметру (показателю) определяется диапазон допустимых значений исходя из требований технического задания на разработку (представления изделия с точки зрения заказчика) и конструктивному исполнению изделия (представления конструкции изделия с точки зрения разработчика);
- значение каждого параметра внутри допустимого диапазона обосновывается расчётно-экспериментальными методами с позиций работоспособности и надёжности;
- производится оценка надёжности с применением метода структурной схемы надёжности для подтверждения того, что выбранные значения параметров (показателей) соответствуют требованиям технического задания;
- осуществляется проверка условий работоспособности на соответствие значений параметров требованиям нормативно-технической и конструкторской документации (для каждого параметра должно быть предусмотрено соответствующее требование для изготовления и/или эксплуатации, выполнение которого может быть проверено средствами технического контроля);
- выявляются риски, связанные с возникновением отказов вследствие не установления требований в рабочей конструкторской и технологической документации в состоянии «как она есть»;
- делается анализ вероятности возникновения отказов, связанных с недооценкой конструкторских и/или технологических ошибок при разработке рабочей документации для принятия окончательного решения о соответствии конструкции и рабочей документации заданным требованиям надёжности.

На завершающем этапе оценки риска производится сравнение значения выявленной вероятности отказов с заданными требованиями безотказности и, в случае необходимости, предпринимаются действия, связанные с пересмотром технических решений и/или установлением дополнительных требований в рабочей документации.

Пример оценки риска

В качестве конкретного примера оценки риска рассмотрим механическую систему с подвижными узлами в виде однозвенной поворотной штанги космического аппарата, которая какое-то время закреплена на опорной поверхности с помощью замка зачековки, затем производится снятие механических связей в замке, штанга под действием приводов раскрывается на заданный угол, фиксируется в конечном положении и начинает работать

как консоль с заданными параметрами работоспособности [4]. Безотказность работы штанги обеспечивается за счёт последовательного выполнения её конструктивными элементами заданных функций, заключающихся в проявлении прочности штанги от нагрузок в зачекованном положении, недопущении несанкционированного снятия механических связей в замке, прохождении электрического сигнала на электрозапалы пиропатронов по заданной команде, срабатывании пироустройства, разделении механических связей в замке, отделении штанги от опорного основания, поворота штанги на заданный угол, фиксации и обеспечении заданных параметров штанги в рабочем положении. Конструктивные элементы поворотной штанги при раскрытии должны последовательно выполнить все указанные функции в заданных условиях и режимах эксплуатации. Нераскрытие штанги может быть обусловлено отказом при выполнении любой из функций, причём одновременно несколькими причинами, которые могут определяться не столько самими условиями и режимами эксплуатации, сколько сочетанием неблагоприятных факторов.

Рассмотрим в качестве примера функцию поворота штанги на заданный угол с помощью раскрывающего привода. Причинами отказа при выполнении рассматриваемой функции могут быть следующие условия: невключение или поломка привода (невключение), отсутствие необходимых запасов движущего момента (торможение), пропадание радиального зазора в шарнире вращения (запрессовка), исчезновение осевого зазора в шарнирном узле (заклинивание), возникновение внезапных препятствий на пути движения штанги (зацепление).

Очевидно, что каждая из причин отказов может быть парирована решениями и/или действиями разработчика штанги путём придания её конструкции таких свойств критичных элементов, которые позволят безусловно выполнить заданные функции. Например, для исключения или смягчения последствий:

- невключения привода – необходимо обеспечить предельную вероятность его безотказной работы за счёт резервирования критичных элементов конструкции;
- торможения штанги – создать требуемый запас движущего момента относительно момента сил сопротивления на пути её движения за счёт выбора энергетических характеристик привода;
- запрессовки шарнира – выбрать такие радиальные зазоры в подшипнике, чтобы при возможных изменениях толщины слоя твёрдого смазывающего покрытия и температурных деформациях была бы обеспечена свобода вращения;
- заклинивания в шарнирном узле – предусмотреть тепловую развязку в направлении оси вращения шарнира;
- зацепления – исключить все возможные помехи на пути движения штанги, вызванные условиями невесомости, кинематикой движения или компоновкой смежных конструкций.

Для количественной оценки условий обеспечения работоспособности по каждому из выявленных свойств критичных элементов необходимо выбрать параметр (показатель), который в полной мере характеризует рассматриваемое свойство, и соответствующую ему допустимую область отклонений [16]. Причём область допустимых отклонений параметров (показателей) будет определяться требованиями технического задания на разработку (внешними параметрами) или внутренними параметрами конструирования (выбранными материалами, компоновочными и силовыми схемами, технологиями изготовлениями и т. п.) [17].

Приведём параметры (показатели) и их допустимые области, которые соответствуют безусловному выполнению функции поворота штанги на заданный угол в виде условий, исключающих или смягчающих последствия причин отказов для следующих рассматриваемых рисков:

1) невключения привода

$$P_d \geq P_{lim}, \quad (1)$$

где P_d – вероятность включения (работы) привода; P_{lim} – вероятность безотказной работы привода в соответствии с распределением заданного требования показателя надёжности штанги по элементам конструкции;

2) торможения штанги

$$M_d > M_c, \quad (2)$$

где M_d – движущий момент, развиваемый приводом раскрытия штанги; M_c – момент сил сопротивления на пути движения штанги;

3) запрессовки шарнира

$$\Delta_r = \delta - 2\delta_n - \delta_{pr} > 0, \quad (3)$$

где Δ_r – радиальный зазор в шарнире; δ – минимальный зазор в сопряжении между охватываемой и охватывающей деталями шарнира без учёта слоя смазки; δ_n – максимальная толщина твёрдой смазки с учётом её возможных изменений в процессе эксплуатации; δ_{pr} – предельное значение тепловых деформаций в радиальном зазоре при объёмном расширении (сжатии) охватываемой (охватывающей) деталей шарнира;

4) заклинивания в шарнирном узле

$$\Delta_{sh} > \Delta l, \quad (4)$$

где Δ_{sh} – осевой зазор в шарнирном узле; Δl – тепловая деформация, способная вызвать распорные усилия в конструкции шарнирного узла;

5) зацеплений штанги

$$Q_{st} \to 0, \quad (5)$$

где Q_{st} – вероятность зацепления штанги.

Выполнение каждого из условий (1)–(5) в процессе эксплуатации при заданных условиях и режимах может быть выражено в виде вероятностей того, что значения параметров (показателей) не превысят пределы допустимых ограничений за интервал наблюдения t и будут равны

$$P_1(t) = P(P_d \geq P_{lim}), \quad (6)$$
$$P_2(t) = P(M_d > M_s), \quad (7)$$
$$P_3(t) = P(\Delta_r > 0), \quad (8)$$
$$P_4(t) = P(\Delta_{sh} > \Delta l), \quad (9)$$

$$P_5(t) = 1 - Q_{st}. \quad (10)$$

Определение вероятностей (6)–(10) может быть произведено стохастическими или детерминированными методами. В первом случае производят вычисления вероятностей нахождения параметров в допустимой области методами теории надёжности, например методом индивидуальной надёжности [18] (что в конечном итоге не исключает возможность отказов, но способно дать представление о частоте их возможного проявления). Во втором случае обосновывают нахождение параметров в заданном допуске (принимают необходимые меры для исключения отказов) за счёт обеспечения конструктивных запасов (резервирования, запасов прочности и движущих моментов, параметрической избыточности, силовых и температурных развязок, процедур получения гарантированных результатов, в т. ч. с применением минимаксных критериев).

При детерминированном подходе для достижения вероятностей $P_i(t) \approx 1$, где $i = 1, 2, \ldots, 5$, в выражении (1) необходимо обеспечить резервирование актуатора привода, например, для электромеханического привода – введение резервного электропитания мотора, а для механического привода – применение структурного резервирования; в выражении (2) – запасы движущих моментов, как правило, не менее 200 % для худшего сочетания условий применения при нулевой кинетической энергии штанги [19]; в выражении (3) – минимаксные критерии, основанные на ограничениях диапазонов реализации случайных параметров для худших условий их реализации [20]; в выражении (4) – тепловые развязки [21]; в выражении (5) – процедуры получения гарантированного результата, например с применением компьютерной симуляции [22].

В случае использования любого из методов (стохастического или детерминированного) вычисления вероятностей (6)–(10) надёжность успешного выполнения функции поворота штанги на заданный угол определяется по формуле

$$P(t) = \prod_{i=1}^{n} P_i(t), \quad (11)$$

где n – количество показателей, обеспечивающих безусловное выполнение функции поворота штанги на заданный угол; $P_i(t)$ – вероятность того, что i-й параметр ($i = 1, 2, \ldots, 5$) не выйдет за пределы допустимых ограничений; t – интервал наблюдения.

Вычисленное значение (11) даёт теоретический показатель надёжности, который может отличаться от действительного, если в конструкторской и/или технологической документации будут отсутствовать какие-либо требования к изготовлению или они будут заданы некорректно для однозначного выполнения условий (1)–(5). К отсутствию, нечёткости или ненадлежащему исполнению требований в технической документации могут привести события, связанные с непроведением необходимых расчётов и испытаний, невнимательностью конструкторов при разработке чертежей, ограничением сроков сдачи конструкторской документации в производство, несогласованностью действий между конструкторами и технологами и т. п.

Для снижения рисков, связанных с возникновением отказов из-за недостаточного объёма и нечёткости требований, необходимо проводить анализ конструкторской и технологической документации на соответствие полноты параметров (показателей), описывающих выполнение определённых функций, например (1)–(5), и требований, установленных для их реализации.

Нерелевантность параметров и требований конструкторской и/или технологической документации, риски невыполнения или ненадлежащего выполнения требований при изготовлении рассматриваются как события C_i, где индекс i соответствует i-му элементу рассматриваемой системы. Вероятность совершения каждого из таких событий может быть определена формулой:

$$P(C_i) = \alpha_i \cdot P_i(t), \quad (12)$$

здесь α_i – корректирующие коэффициенты, которые могут быть получены экспертным путём, например с использованием балльных оценок критичности отказов:

$$\alpha_i = 1 - Q_i,$$

где Q_i – ожидаемая вероятность отказа i-го элемента согласно шкале балльных оценок критичности отказов по ГОСТ 27.310.

Для вычисления окончательной вероятности выполнения функции поворота штанги на заданный угол с учётом состояния конструкторской и технологической документации (12) используют формулу

$$P(C) = \prod_{i=1}^{n} P_i(C_i). \quad (13)$$

Представленные процедуры для оценки вероятности осуществления функции поворота штанги на заданный угол могут быть применены при анализе каждой из указанных функций штанги при раскрытии, а вероятность их выполнения и общая вероятность безотказной работы штанги – оценена с помощью формул (11) и/или (13). Целесообразность применение указанных формул определяется требуемой точностью оценки надёжности [16]. Для оценки безотказности ниже трёх девяток вполне приемлемой может оказаться формула (11), а при требованиях к безотказности на уровне трёх девяток и выше необходимо применять формулу (13).

Оценка риска с применением конструкторско-технологического анализа надёжности

Методика анализа и оценки риска с учётом конструкторских и технологических решений (1)–(13) получила название методики конструкторско-технологического анализа надёжности (КТАН), основы которой приведены в работах [23, 24]. Наиболее полное представление о данной методике сводится к последовательному осуществлению определённых методов:

- Метод функционального анализа предназначен для выявления основных функций, обеспечивающих выполнение служебного назначения изделий, и определения возможных отказов, как следствий нарушения условий функционирования;
- Метод проведения анализа худшего случая – для выявления причин возможных отказов, включая худшие сочетания факторов технического состояния изделия, режимов и условий его эксплуатации;
- Метод парирования отказов – для выявления свойств критичных элементов изделия, при реализации которых причины отказов становятся невозможными;
- Метод параметризации конструкции изделия – для количественной характеристики свойств критичных элементов и определения областей допустимых значений, например (1)–(5);
- Метод обоснования параметров – для оценки вероятностей нахождения параметров функционирования в допустимой области, например (6)–(10);
- Метод оценки надёжности с использованием метода структурной схемы надёжности (11) – для принятия решения о соответствии выбранных параметров конструкции заданным требованиям надёжности;
- Метод установления необходимых и достаточных требований путём сплошного анализа конструкторской и технологической документации – для установления степени соответствия параметров функционирования установленным требованиям;
- Метод выявления рисков отказов вследствие не установления требований в конструкторской и/или технологической документации (12) – для выявления и оценки возможных отказов вследствие выполнения требований рабочей документации в состоянии «как она есть»;
- Метод оценки надёжности с учётом рисков, связанных с недооценкой конструкторских и/или технологических ошибок (если они обнаружатся), например, с использованием балльных оценок критичности отказов (13), – для принятия окончательного решения о соответствии конструкции заданным требованиям надёжности.

В зависимости от требуемой точности оценки надёжности, полученные значения вероятностей (11) или (13) сравнивают с заданными требованиями надёжности P_{pr} для выполнения условия

$$\forall P = [P(t) \vee P(C)] > P_{pr}. \qquad (14)$$

В случае невыполнения условия (14) необходимо повторить итерацию проведения процедур КТАН и сделать новые расчёты с уточнёнными исходными данными.

Следует отметить, что приведённый подход к расчёту надёжности (11)–(14) был разработан целенаправленно для раскрывающихся конструкций космических аппаратов и применительно к другим техническим объектам пока не применялся. Тем не менее, если сравнивать указанный подход с методикой расчёта надёжности механических частей поворотных конструкций летательных аппаратов, основанной на классических подходах теории надёжности [25, 26], то он позволяет существенно расширить возможность учёта факторов неопределённости. Например, из пяти рассмотренных в статье причин отказов, в известных работах рассматривается лишь одна – «торможение штанги» (2), что вполне объяснимо – там не учитывались конструкторские и технологические решения как факторы неопределённости.

Заключение

Показано, что отсутствие статистических данных о надёжности образцов-аналогов УВС не является препятствием для проведения расчётов надёжности в виде оценки риска. Более того, результаты таких расчётов могут быть источником и руководством для принятия конструкторских и технологических решений при разработке и создании изделий с заданной надёжностью. Однако для легализации методики проведения таких расчётов необходима корректировка нормативно-технической документации, позволяющая производить расчёты надёжности иными методами, нежели с использованием статистических данных об отказах образцов-аналогов.

Библиографический список

1. Толковый словарь русского языка: в 4 т. Т. 3 / под ред. Д. Ушакова. – М.: ТЕРРА, 1996. – 712 с.

2. Термины космического страхования [Электронный ресурс] // Космическое страхование (страхование космических рисков: информационно-аналитический сайт. – Режим доступа: http://www.space-ins.ru/index.php/kategoria8/8-terms.html.

3. Половко А.М., Гуров С.В. Основы теории надёжности. – СПб.: БХВ-Петербург, 2006. – 704 с.

4. Похабов Ю.П., Ушаков И.А. О безаварийности функционирования уникальных высокоответственных систем // Методы менеджмента качества. – 2014. – №11. – С. 50–56.

5. ГОСТ 27.002–89. Надёжность в технике. Основные понятия. Термины и определения. – М.: Изд-во стандартов, 1990. – 37 с.

6. ГОСТ 27.002–2015. Надёжность в технике. Термины и определения. – М.: Стандартинформ, 2016. – 28 с.

7. Вентцель Е.С. Теория вероятностей. – М.: Наука, 1969. – 576 с.

8. ГОСТ Р ЕН 9100–2011. Системы менеджмента качества организаций авиационной, космической и оборонных отраслей промышленности. Требования. – М.: Стандартинформ, 2012. – 23 с.

9. ГОСТ Р ИСО 31000–2010. Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2012. – 26 с.

10. ГОСТ Р 51897–2011. Менеджмент риска. Термины и определения. – М.: Стандартинформ, 2012. – 16 с.

11. Похабов Ю.П. О философическом аспекте надёжности на примерах уникальных высокоответственных систем // Надёжность. – 2015. – № 3. – С. 16–27.

12. Ван-Желен В. Физическая теория надёжности. – Симферополь: Крым, 1998. – 318 с.

13. Похабов Ю.П. О дефиниции термина «надёжность» // Надёжность. – 2017. – Т. 17, № 1. – С. 4–10.

14. Нетес В.А., Тарасьев Ю.И., Шпер В.Л. Как нам определить что такое «надёжность» // Надежность. – 2014. – № 4. – С. 3-14.

15. Уёмов А.И. Вещи, свойства и отношения. – М.: Изд-во АН СССР, 1963. – 184 с.

16. Похабов Ю.П. Теория и практика обеспечения надёжности механических устройств одноразового срабатывания. – Красноярск: СФУ, 2018. – 340 с.

17. Чеботарёв В.Е. Проектирование космических аппаратов систем информационного обеспечения: в 2-х кн. Кн. 2. Внутреннее проектирование космического аппарата. – Красноярск: СибГАУ, 2005. – 168 с.

18. Тимашев С.А., Похабов Ю.П. Проблемы комплексного анализа и оценки индивидуальной конструкционной надёжности космических аппаратов (на примере поворотных конструкций): препринт / С.А. Тимашев, Ю.П. Похабов. – Екатеринбург: АМБ, 2018. – 38 с.

19. NASA Standard. Design and Development Requirements for Mechanisms (13 June 2006). NASA-STD-5017. – 30 p.

20. Основы проектирования космических аппаратов информационного обеспечения / В.Е. Чеботарёв, В.Е. Косенко. – Красноярск: СибГАУ, 2011. – 488 с.

21. Пат. 2230945 Российская Федерация. МПК F16B 1/00. Способ закрепления изделий / Ю.П. Похабов, В.В. Гриневич. – № 2002113143/11; заявл. 18.05.2002; опубл. 20.06.2004. Бюл. № 17.

22. Емельянов А.А. Путь от аналоговых моделей к симулятору на цифровом компьютере // Прикладная информатика. – 2007. – № 5. – С. 41–53.

23. Похабов Ю.П. Подход к обеспечению надёжности уникальных высокоответственных систем на примере крупногабаритных трансформируемых конструкций // Надёжность. – 2016. – № 1. – С. 24–36.

24. Похабов Ю.П. Обеспечение надёжности уникальных высокоответственных систем // Надёжность. – 2017. – Т. 17, № 3. – С. 17–23.

25. Кузнецов А.А. Надёжность конструкции баллистических ракет. – М.: Машиностроение, 1978. – 256 с.

26. Кузнецов А.А., Золотов А.А., Комягин В.А. и др. Надёжность механических частей конструкции летательных аппаратов. – М.: Машиностроение, 1979. – 144 с.

Сведения об авторе

Юрий П. Похабов – кандидат технических наук, Акционерное общество «НПО ПМ – Малое Конструкторское Бюро» (АО «НПО ПМ МКБ»), начальник центра научно-технических разработок, Россия, Красноярский край, Железногорск, e-mail: pokhabov_yury@mail.ru

Поступила: 16.04.2018

УДК: 004.056.53
Оригинальная статья
Надежность, том 18, №4, 2018 DOI: 10.21683/1729-2646-2018-18-4-36-44

Методика оценки защищенности микропроцессорных систем управления в условиях информационно-технических воздействий

Сергей М. Климов, *4 ЦНИИ Минобороны России, Королёв, Россия*
Юрий В. Сосновский, *Физико-технический институт Крымского федерального университета им. В.И. Вернадского, Симферополь, Россия*

Сергей М. Климов

Юрий В. Сосновский

Резюме. *Целью статьи является разработка моделей, позволяющих дать типовое представление структуры, функций микропроцессорных систем управления (МСУ) и получить количественную оценку рисков (отказоустойчивости) автоматизированных систем управления и их основных компонент – МСУ в условиях информационно-технических воздействий (ИТВ). В статье показана актуальность и важность моделей МСУ и оценки рисков функционирования автоматизированных систем управления технологическими процессами (АСУ ТП) при осуществлении на них различных ИТВ (компьютерных атак). В качестве ИТВ нарушителя рассматриваются аппаратные, аппаратно-программные и программные воздействия, обладающие свойствами блокирования коммуникационных каналов, нарушения доступности и целостности информации, а также целенаправленного и продолжительного информационно-технического воздействия на автоматизированную систему, в том числе, вредоносными программами. Разработанная в статье структурно-функциональная модель микропроцессорной системы управления как основной компоненты системы более высокого уровня – АСУ ТП, образована совокупностью схем и описаний функций. Структурно-функциональная модель включает в свой состав: структуры каналов основного цикла системы управления (считывание данных, обработка, запись выходных значений, а также работа с коммуникационной подсистемой), структурно-функциональную схему МСУ различного типа в зависимости от наличия и уровня использования телекоммуникационного канала в структуре цикла управления, типового паспорта уязвимости МСУ. В схемах подробно описаны типовые функции, порядок работы и информационного взаимодействия модулей МСУ с внешней средой через каналы передачи данных. Модель рисков АСУ ТП и МСУ, как ее части, в условиях воздействий ИТВ описывается показателями, характеризующими условный ущерб и состояние системы управления, при котором она может восстановить свою работоспособность или потребуется внешнее вмешательство, затрагивающее не только саму систему управления, но контролируемый технологический процесс. В качестве показателей, рассмотрены следующие: характеристические точки и параметры функции риска, основанной на распределении Вейбулла-Гнеденко, статистическая оценка защищенности МСУ, функция риска, динамическая оценка риска успешной реализации ИТВ на МСУ. Предполагается, что значения параметров, необходимых для расчета показателей риска и защищенности МСУ получены:*
- эмпирически, на основе структурно-параметрического анализа особенностей построения, динамики функционирования и уязвимостей МСУ;
- в рамках имитационного моделирования МСУ как абонентов вычислительных сетей в условиях ИТВ на стендовом полигоне;
- экспериментально на основании частоты успешно реализованных угроз ИТВ,
а также показатели защищенности экстраполируются на весь жизненный цикл МСУ посредством введения динамической поправки, основанной на функции риска с использованием распределения Вейбулла-Гнеденко.
В выводе отмечается, что разработанная методика оценки защищенности МСУ в условиях ИТВ позволяет оценить риски успешной реализации нарушителем вредоносного воздействия на МСУ и АСУ ТП в целом, что создает предпосылки для своевременного устранения уязвимостей в МСУ и принятия дополнительных организационно-технических мер по повышению уровня информационной безопасности автоматизированных систем управления.

Ключевые слова: *информационно-технические воздействия, микропроцессорные системы управления, средства защиты информации, отказоустойчивость.*

Формат цитирования: Климов С.М., Сосновский Ю.В. Методика оценки защищенности микропроцессорных систем управления в условиях информационно-технических воздействий // Надежность. 2018. № 4. С. 36-44. DOI: 10.21683/1729-2646-2018-18-4-36-44

Введение

Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 2016 года, определены современные угрозы информационно-технических воздействий на критическую информационную инфраструктуру страны.

В настоящее время необходимость развития цифровой экономики страны обусловливает активное внедрение информационных и коммуникационных технологий в автоматизированных системах управления технологическими процессами (АСУ ТП). За рубежом АСУ ТП классифицируются как SCADA-системы для управления энергетикой, транспортом и промышленными системами. На практике внедрение информационных и коммуникационных технологий приводит к появлению дополнительных уязвимостей в программном обеспечении, что повышает вероятность реализации на них нарушителем угроз информационно-технических воздействий (ИТВ).

Современные средства реализации ИТВ вредоносными программами [1], например, Stuxnet, Flame, miniFlame, Duqu, Gauss, Reign, Wiper, Shamoon, Careto используют уязвимости программного кода АСУ ТП для скрытного внедрения, самораспространения и целенаправленного нарушения функционирования системы. Развитие средств ИТВ и их функциональных возможностей значительно опережает разработку соответствующих средств обнаружения предупреждения компьютерных атак (СОПКА), особенно в форме вредоносных программ.

Ключевым элементом СОПКА для АСУ ТП является сенсор (индикаторный программно-аппаратный или программный модуль) регистрирующий факт компьютерного инцидента – успешной реализации ИТВ нарушителем.

Базовым элементом АСУ ТП являются микропроцессорные системы управления (МСУ) [2], программное обеспечение которых выполняет функции сбора, обработки и передачи информации для управления в реальном масштабе времени критически важными объектами. Если ранее программируемые производственные микропроцессоры управлялись набором специальных команд, то на современном уровне они функционируют под управлением операционных систем (ОС) общего применения (например, ОС Windows или Linux) и доступны как абоненты вычислительной сети с протоколами передачи данных типа TCP/IP или с характерным для SCADA-систем протоколом Modbus.

Для оценки и обеспечения защиты информации в МСУ в условиях реализации угроз ИТВ нарушителем необходим комплекс методик и средств для обнаружения, идентификации вредоносных воздействий и ликвидации их последствий [9-14].

Таким образом, задача разработки методики оценки защищенности МСУ в условиях ИТВ с целью априорной количественной оценки рисков нарушения функционирования МСУ критически важных объектов является актуальной и представляет практический интерес.

Постановка задачи

При проведении исследований были приняты следующие допущения:

- оценка рисков успешных ИТВ нарушителя должна выполняться на стендовом полигоне, позволяющем создать требуемые тестовые условия для работы функциональных аналогов МСУ, элементов СОПКА и имитации ИТВ;

- выделенные группы рисков нарушения функционирования МСУ возможно оценивать непосредственно на объекте с помощью мобильного тестового комплекса;

- предварительная оценка уязвимостей МСУ и угроз ИТВ нарушителя позволяет сформировать возможные варианты средств защиты информации (СЗИ) и выбрать наиболее эффективный из них.

Параметры защищенности МСУ определяются:

- эмпирически, на основе структурно-параметрического анализа особенностей построения, динамики функционирования и уязвимостей МСУ;

- экспериментально на основании частоты успешно реализованных угроз ИТВ нарушителя,

при этом установленные показатели защищенности экстраполируются на весь жизненный цикл МСУ посредством введения динамической поправки, основанной на функции риска с использованием распределения Вейбулла-Гнеденко [3-4].

Основой для разработки методики оценки защищенности МСУ в условиях ИТВ является модель функционирования МСУ в условиях ИТВ, которая позволяет проводить комплексный анализ взаимосвязанных процессов функционирования МСУ, реализации ИТВ и ликвидации их последствий.

В разработанной модели предполагается, что МСУ оснащена коммуникационной подсистемой. Коммуникационная подсистема выполняет такие функции, как взаимодействие с промышленными системами более высокого уровня, удаленное считывание данных с датчиков и запись их значений в исполнительные устройства посредством сетевых интерфейсов.

Коммуникационная подсистема МСУ, которая напрямую включена в контур управления технологическим процессом, и является основной уязвимостью для реализации нарушителем угроз ИТВ на ее протоколы передачи данных. Предполагается, что при реализации ИТВ нарушителем могут быть использованы недекларированные возможности как в аппаратно-программных средствах МСУ, так и в программируемых маршрутизаторах сети передачи данных на различных уровнях АСУ ТП. Кроме того, нарушитель может быть не только внешний, но и внутренний, который знаком со спецификой и временными ограничениями технологического процесса (условиями срабатывания автоматических и автоматизированных

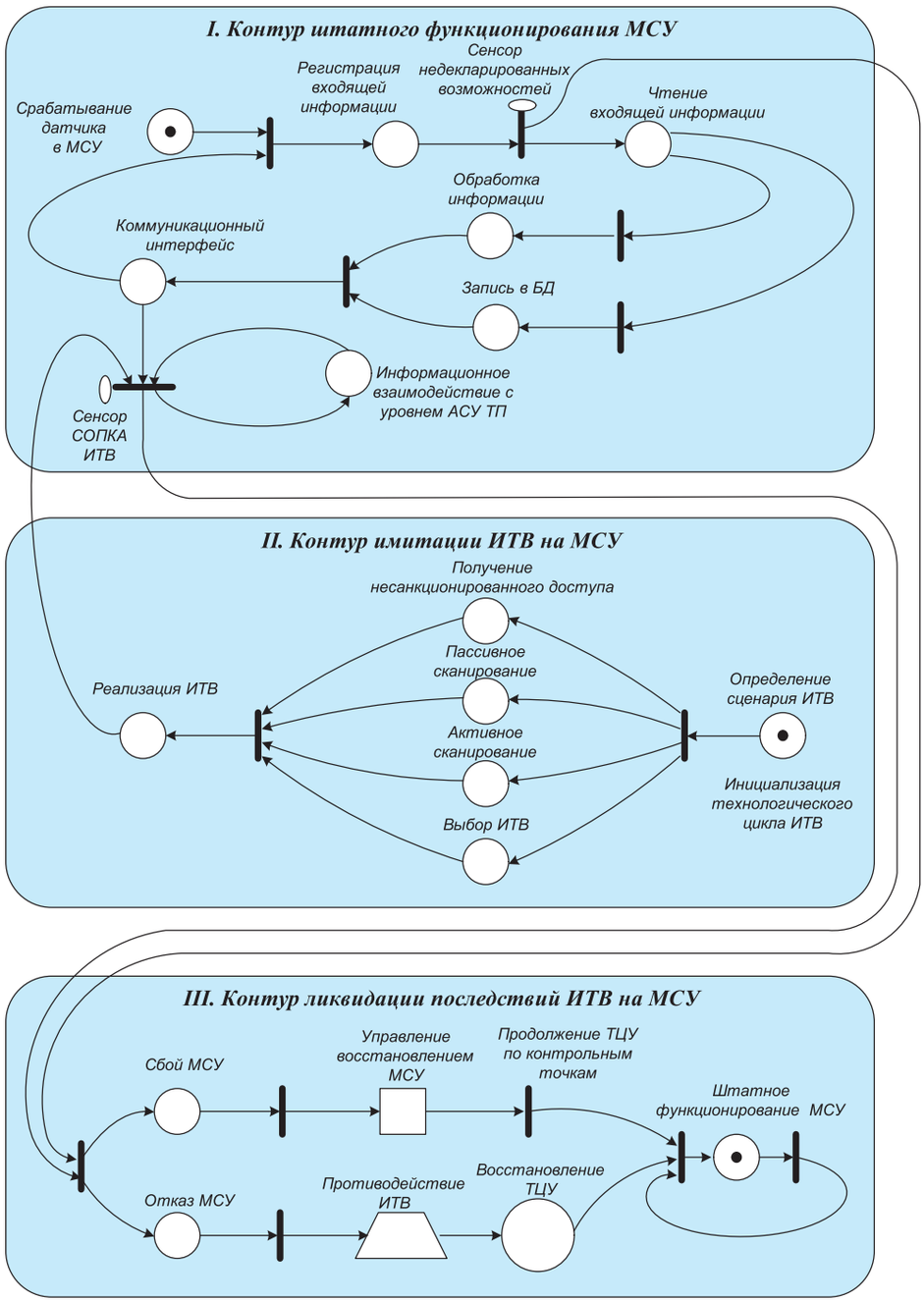


Рисунок 1 – Схема модели функционирования МСУ в условиях ИТВ и терминах РСП

исполнительных устройств), и способен реализовать неизвестное воздействие «нулевого» дня.

Схема модели функционирования МСУ в условиях ИТВ и терминах расширенной сети Петри (РСП) [5] представлена на рисунке 1.

Модель функционирования МСУ в условиях ИТВ включает в свой состав три контура:

1. Контур штатного функционирования МСУ, позволяющий осуществить имитационное моделирование и структурно-параметрический анализ технологического цикла управления (ТЦУ) МСУ.

2. Контур имитации ИТВ, предназначенный для моделирования действий нарушителя по получению несанкционированного доступа к МСУ, пассивного и активного сканирования уязвимостей, выбора и запуска ИТВ. В качестве исходных данных о современных угрозах ИТВ нарушителя вредоносными программами в статье использованы материалы статьи [1].

3. Контур ликвидации последствий ИТВ, обеспечивающий моделирование процессов предупреждения, обнаружения и ликвидации последствий ИТВ на основе использования сенсоров (индикаторных модулей) обна-

ружения и идентификации воздействий.

На рисунке 1 в блоке III показаны две альтернативы ликвидации последствий ИТВ на МСУ в случае их успешной реализации нарушителем.

Ветвь I (верхняя) отражает ситуацию, при которой МСУ обладает свойством восстановления в случае сбоя (относительно кратковременной ТЦУ – от нескольких секунд до нескольких минут). Под сбоем понимается кратковременное нарушение ТЦУ, вызванное ИТВ, но не приводящее к срыву работы МСУ. В этом случае при идентификации сбоя в системе запускается алгоритм восстановления ТЦУ, после выполнения которого МСУ переходит в состояние нормального функционирования.

Ветвь II (нижняя) иллюстрирует такой исход реализации ИТВ нарушителем, при котором МСУ переходит в состояние отказа, характеризующегося длительным нарушением процессов управления в МСУ (от 30 минут до нескольких часов).

Специфика МСУ такова, что восстановление ТЦУ после длительного отказа зачастую требует вмешательства оператора и (или) технического персонала и не может быть выполнено перезапуском или внедрением заведомо работоспособной МСУ.

Для предотвращения сбоев и отказов в МСУ в условиях ИТВ необходимо оперативное обнаружение, локализация воздействия и восстановление ТЦУ на основе внедренных избыточных сенсоров (индикаторных программно-аппаратных средств) СОПКА [5-6].

Формализация модели функционирования МСУ в условиях ИТВ и терминах РСП [5]:

$$S_{МСУ} = \{(P,V),T,D,M,Q,I_p,Y\}, \quad (1)$$

где $P = p_1, p_2, ..., p_i$ – непустое конечное множество позиций, характеризующих штатный режим функционирования МСУ;

$V = v_1, v_2, ..., v_i$ – множество позиций восстановления, отражающие процедуры восстановления после успешных ИТВ нарушителя (графически представляется □);

$T = t_1, t_2, ..., t_i$ – непустое множество переходов, при этом в соответствии с РСП каждому переходу t_i может быть поставлен в соответствии алгоритм его срабатывания $a \vee g_i$ (при наличии алгоритма над переходом делается пометка $a \vee g_i$);

D – непустое конечное множество дуг сети, причем $D = (D_1 \cup D)$, $D_1 = (P \times T) \cup (V \times T)$ – непустое множество входных дуг, соединяющих позиции и переходы, $D_2 = (T \times P) \cup (T \times V)$ – непустое множество выходных дуг, ориентированных от переходам к позициям;

M – множество маркировок сети Петри;

$F_p : (M_p : P \to N), F_v : (M_v : V \to N)$ – функции начальной маркировки позиций штатного функционирования и восстановления, соответственно, N={0,1,2,…} – множество натуральных чисел (помечается точкой внутри позиции ⊙);

Q – множество вероятностей запусков переходов, отражающее вероятности нахождения МСУ в режиме штатного функционирования, моменты реализации ИТВ и срабатывания датчиков СОПКА, процессы восстановления;

$Z_{АПДi}$ – множество позиций противодействия ИТВ ( );

$I_p = i_{p1}, i_{p2}, ..., i_{pm}$ – множество приоритетов для дуг;

$Y = y_1, y_2, ..., y_k$ – множество временных параметров ИТВ.

Функции описания структуры РСП в виде отображения множеств выглядят как

$$F_{d1} : P \times T \bigcup V \times T \to N, \text{ или } F(p_i, v_j, t_n), \quad (2)$$

$$F_{d2} : T \times P \bigcup T \times V \to N, \text{ или } F(t_n, p_i, v_j),$$

где F_{d1} – функция входных позиций, ставящая в соответствие позициям и переходам количество маркеров, необходимых для запуска перехода («входа»);

F_{d2} – функция выходных позиций, ставящая в соответствие позициям и переходам количество маркеров, необходимых для изменения маркировки (корректировки «выхода»);

N={0,1,2,…} – множество натуральных чисел.

С учетом вышесказанного, правило запуска переходов имеет общий вид:

$$\forall (p_i \in P \wedge v_j \in V) \to \exists (M(p_i) \geq F_{d1}(p_i, v_j, t_n)). \quad (3)$$

Если сработал переход t_n, то из каждой его входной позиции p_i и v_j удаляется количество маркеров $m(p_i)$ и $m(v_j)$, равное числу входных дуг, а в выходные позиции p_{i+1} и v_{j+1} добавляется число маркеров, равное числу выходных дуг. При этом происходит срабатывание перехода, которому соответствует наибольшее значение вероятности его запуска (q_w) и предшествует дуга с более высоким приоритетом (i_{pm}). Задержка на время срабатывания перехода определяется параметрами ИТВ (y_k) в позициях сети, из которых выходят дуги к этому переходу. С учетом этого, правило изменения маркировки РСП имеет вид:

$$\forall (M_p \wedge M_v) : (p_i \in P \wedge v_j \in V) \to \exists (M'_p \wedge M'_v) =$$
$$= F_p(Mp) + F_v(Mv) - F_{d1}(p_i, v_j, t_n) + F_{d2}(t_n, p_i, v_j). \quad (4)$$

Описание начальной маркировки (M_i) в РСП для отображения и анализа причинно-следственных связей между процессами в МСУ и системы СОПКА при воздействии ИТВ. Условие достижимости РСП:

$$\forall (p_i \in P \wedge V_r \in V \wedge Z_j \in Z_{АПД}) \to \exists M'(p_i, v_r, z_j) =$$
$$= M(p_i, v_r, z_j) - [F_p(M_p) + F_v(M_v) + F_z(M_z)] -$$
$$- [F_{ud1}(p_i, v_r, z_j, t_n) + F_{ud2}(t_n, p_i, v_r, z_j)]. \quad (5)$$

Определение логических условий для срабатывания переходов РСП (T_i) при маркировке $M(p_i, v_r, z_j)$:

$$\forall\left(p_i \in P \wedge V_r \in V \wedge Z_j \in Z_{АПД}\right) \rightarrow$$
$$\rightarrow \exists\left[M\left(p_{i1}, v_{r1}, z_{j1}\right) \geq F_{ud1}\left(p_i, v_r, z_j, t_n\right)\right],$$
$$\Psi_t\left[\left(p_{i1}, v_{r1}, z_{j1}\right),...,\left(p_{in}, v_{rn}, z_{jn}\right)\right] = 1, \quad (6)$$

где Ψ_t – функция распределения маркировки по входным позициям РСП.

Определение соотношения для позиции РСП – «подсобытий» $P_i, V_r, Z_{АПДi}$ предупреждения, обнаружения, анализа ИТВ, активного противодействия им, а также восстановления МСУ:

$$\forall\left(p_i \in P, e_i \in E_{ki}, n_i \in N_{ki}, b_i \in B_{ki}\right) \rightarrow$$
$$\rightarrow \exists \min\left(p_i, V_r, Z_j, E_{ki+1}, N_{ki+1}, B_{ki+1},\right) \rightarrow$$
$$\rightarrow Z^*_{\text{ПД}} \rightarrow, \Psi_{tn} = \left\{\left(p_{i1}, V_{r1}, Z_{j1}\right),...,\left(p_{in}, V_{rn}, Z_{jn}\right)\right\}. \quad (7)$$

Функция начального входного распределения маркировки Ψ_t по позициям РПС принимает значения (8), которое определяет порядок начального размещения маркеров по позициям РСП

$$\Psi_{tn}\left(p_i, V_r, Z_j\right) = \left\{1, \textit{если } m_{pi} \in M_p, m_{vr} \in M_v, m_{zj} \in M_z. \right. \quad (8)$$

Задание условия срабатывания сенсоров СОПКА (Q_i):

$$\forall t_i \in T, Q_{ki} \in Q, \exists Q_{i+1} \neq 0,$$
$$\phi_q\left(t_i, Q_{ki}\right) = \left\{1, \textit{если } mp_i \in M_p, y_i \in Y, a \vee g_i = \right.$$
$$= 1, \left\{\frac{1}{R}, \textit{если } mp_i \in M_p, y_i \notin Y, a \vee g_i = 1, \right. \quad (9)$$

где $a \vee g_i$ – алгоритм срабатывания сенсора. Условия срабатывания сенсора выглядят следующим образом:

$\phi_q\left(t_i, Q_{ki}\right) = 1$ – сенсор сработал, атака обнаружена;

$\phi_q\left(t_i, Q_{ki}\right) = \frac{1}{R}$ – ложное срабатывание сенсора при R-ном срабатывании перехода;

$\phi_q\left(t_i, Q_{ki}\right) = 0$ – сенсор не сработал, неизвестная атака не обнаружена.

С учетом современных методов защиты информационных систем и управления рисками [1, 5, 7, 9, 13, 14] методика оценки защищенности МСУ в условиях ИТВ представлена в виде последовательности шагов:

1. Определение способа мониторинга МСУ с учетом особенностей функционирования (контролируемых процессов и типов протоколов передачи данных).

2. Анализ уязвимостей и формирование паспорта уязвимостей МСУ.

3. Разработка модели угроз ИТВ.

4. Разработка имитационной модели контролируемого ТЦУ в МСУ с учетом коммуникационных интерфейсов АСУ ТП.

5. Проведение экспериментальных исследований МСУ в условиях ИТВ на основе имитационного моделирования на стендовом полигоне.

6. Оценка показателей защищенности МСУ по результатам моделирования.

7. Оценка рисков нарушения защищенности МСУ в условиях ИТВ.

Шаг 1. Способ мониторинга МСУ основывается на классификации МСУ. Классификация МСУ выполняется по признакам, включающим в себя определение наличия проводных и беспроводных коммуникационных каналов, интерфейсов (однонаправленность, двунаправленность, «многоточка»), возможности удаленной «перепрошивки» программного обеспечения и удаленного администрирования МСУ. По указанным признакам, выделим базовые типы МСУ:

МСУ 1-го типа – система с локальным контроллером, осуществляющая локальное чтение входных сигналов, обработку данных и выработку выходных управляющих сигналов с помощью локальных модулей вывода;

МСУ 2-го типа – система, использующая интерфейсы передачи данных в качестве информационной среды между удаленными модулями ввода-вывода и процессорными блоками;

МСУ 3-го типа – системы, использующие протоколы передачи данных, функционирующие в двунаправленном варианте для передачи данных на системы более высокого уровня и прием данных от них;

МСУ 4-го типа – системы, обладающие перечисленными особенностями 3-го типа но, кроме этого, допускающие возможность удаленного (с использованием общей среды передачи данных) администрирования, в том числе – корректировки и смены управляющей программы («перепрошивки»).

К контролируемым процессам относится внутренний и внешний обмен данными через интерфейсы МСУ, параметры сетевого трафика с элементами АСУ ТП. Мониторинг обмена в МСУ разделен по типам протоколов передачи данных и осуществляется сенсорами СОПКА сигнатурным анализом и функциональным анализом аномального поведения МСУ, выявлением искажений структуры протоколов, параметров сигнализации и синхронизации, преамбулы пакетов данных и различных служебных параметров оборудования МСУ.

Шаг 2. Уязвимости программного обеспечения МСУ определим с использованием ГОСТ Р 56546-2015 [8] и формализуем в виде типового паспорта уязвимостей программного обеспечения МСУ в условиях ИТВ (таблица 1). За основу взят паспорт уязвимостей базы данных ФАУ «ГНИИИ ПТЗИ ФСТЭК России» BDU:2018-00543. В качестве дополнения к типовому паспорту уязвимостей требуется введение следующих характеристик:

1. Тип промышленного протокола передачи данных (ввиду потенциально возможных уникальных атак на промышленные протоколы с учетом их аппаратной и программной специфики).

2. В вектор уязвимости ввести данные, касающиеся контролируемого технологического процесса (обычный, важный, критически важный), так как информационно-

Таблица 1 – Типовой паспорт уязвимости (на примере BDU:2018-00543)

Описание уязвимости	Уязвимость сценария track_import_export.php системы управления производственными и жилыми объектами U.motion builder связана с непринятием мер по защите структуры SQL-запроса
Вендор	Schneider Electric
Наименование ПО	U.motion Builder
Версия ПО	до 1.3.4
Тип ПО	Программное средство АСУ ТП
ОС и аппаратные платформы	Данные уточняются
Тип ошибки	Непринятие мер по защите структуры запроса SQL (атаки типа \»внедрение SQL\»)
Идентификатор типа ошибки	CWE-89
Класс уязвимости	Уязвимость кода
Дата выявления	02.03.2018
Базовый вектор уязвимости	AV:N/AC:L/Au:N/C:C/I:C/A:C
Уровень опасности уязвимости	Критический уровень (базовая оценка CVSS 2.0 составляет 10) Высокий уровень (базовая оценка CVSS 3.0 составляет 8,8)
Возможные меры по устранению уязвимости	Использование рекомендаций: https://www.schneider- electric.com/en/download/document/SE_UMOTION_BUILDER/
Статус уязвимости	Подтверждена производителем
Наличие эксплойта	Данные уточняются
Способ эксплуатации	Инъекция
Способ устранения	Обновление программного обеспечения
Информация об устранении	Уязвимость устранена
Ссылка на источники	https://www.schneider-electric.com/en/download/document/SE_UMOTION_BUILDER/
Идентификаторы других систем описания уязвимостей	CVE: CVE-2018-7765
Прочая информация	

техническое воздействие на МСУ, АСУ ТП приводит не только к сбою или отказу данной системы, а влечет за собой сбой или отказ контролируемого технологического процесса.

3. Показатель «Уровень опасности уязвимости» зависит как от уровня угрозы уязвимости, так и от типа контролируемого технологического процесса (обычный, критически важный).

Шаг 3. Разработка модели угроз ИТВ основана на анализе потенциальных угроз, зависящих от типа МСУ (по классификации), а также используемых протоколов и контролируемых технологических циклов управления (ТЦУ).

Ввиду того, что рассматривается безопасность информации уровня МСУ, можно выделить следующие основные пути реализации угроз ИТВ нарушителя:

- угрозы информационного воздействия, приходящие с более высокого уровня АСУ ТП (такими угрозами могут быть некорректные значения уставок для данного технологического процесса, принудительная их фиксация, иные попытки нарушить работу МСУ посредством искажения информации и управляющих параметров);

- угрозы воздействия на протоколы ввода и вывода информации в МСУ (в случае отнесения последней к МСУ 2-4 типов), приводящие к блокировке протоколов или нарушения целостности передаваемых данных;

- угрозы воздействия на программную составляющую МСУ (при наличии возможности удаленной «перепрошивки» контроллеров).

Возможности реализации угроз ИТВ нарушителя непосредственно связаны с характеристиками используемого оборудования, протоколов, контролируемых технологических процессов в МСУ и не могут рассматриваться вне данного контекста.

Шаг 4. Разработка имитационной модели контролируемого ТЦУ в МСУ (объекта исследований) с учетом коммуникационных интерфейсов АСУ ТП заключается в разработке так называемого «информационного окружения» и базовых функций для МСУ. В ходе экспериментальных исследований на стенде модель ТЦУ может быть представлена отдельной группой программируемых устройств, например программируемыми логическими коммутаторами, программы которых позволяют моделировать ТЦУ в МСУ при изменении преднамеренных и непреднамеренных управляющих и информационных воздействий. При имитационном моделировании роль «информационного окружения» играют независимые программные блоки модели, а при натурном моделировании – реальное оборудование, за-

Таблица 2 – Дополненные показатели, характеризующие проектную защищенность МСУ

Структурно-функциональные характеристики МСУ	Уровень проектной защищенности МСУ		
	Высокий	Средний	Низкий
По типу взаимодействия между уровнями МСУ: - автономная, нет межуровневого взаимодействия, есть однонаправленное (на верхний уровень); - есть двунаправленное взаимодействие.	3	2	-
По организации интерфейсов ввода-вывода: - локальные физические (электрические) подключения; - используются коммуникационные интерфейсы, они физически отделены от иных сегментов сети; - общая коммуникационная среда.	3	2	1
Наличие средств «перепрошивки» программного обеспечения МСУ: - отсутствует; - имеется, требует локального подключения; - возможность удаленного управления.	3	2	1
По встроенным средствам контроля МСУ и самодиагностики: - отсутствуют; - имеется идентификация сбоя (отказа); - имеется идентификация сбоя (отказа), средства восстановления работоспособности и резервирования функций.	3	2	1

действованное в контроле ТЦУ. В рамках моделирования сам реальный ТЦУ в МСУ может быть не запущен (ввиду сложности полного воспроизведения функций АСУ ТП), а моделирование его реакции на те или иные воздействия может осуществляться добавлением независимых программных модулей в специальное программное обеспечение коммуникационного оборудования.

Шаг 5. Проведение экспериментальных исследований МСУ в условиях ИТВ на основе имитационного моделирования на стендовом полигоне основано на выполнении трех основных процессов:

- моделирование штатного функционирования МСУ;

- имитация ИТВ на МСУ из базы данных моделей воздействий;

- моделирование СЗИ, в качестве которых в статье рассматриваются сенсоры СОПКА, настроенные на мониторинг ТЦУ с учетом предложенной классификации МСУ.

Программный код и сценарий для имитации ИТВ хранится в базе данных и разрабатывается с учетом используемых протоколов, типов и потенциальных уязвимостей МСУ (согласно классификации). Ряд ИТВ может быть представлен стандартными компьютерными атаками, например ARP-спуфинг, DDoS-атаки, другие же являются специфическими для применяемых в АСУ ТП протоколов. Примерами специальных ИТВ могут являться компьютерные атаки на протокол синхронизации времени PTP (IEEE 1588), протокол Modbus, встроенное программное обеспечение контроллера МСУ.

Шаг 6. Статистическая оценка защищенности МСУ состоит в проведении оценки защищенности МСУ по результатам имитационного и натурного моделирования. Оценка защищенности МСУ строится на контроле корректности функционирования системы управления по уровням эталонной модели взаимодействия открытых систем.

Для расчета показателей статистической оценки защищенности МСУ используется принцип ALARP и четыре установленные категории риска: от недопустимого до не принимаемого в расчет [13, 14]. Соответственно, для каждого типа ИТВ и заданного (эмпирически или полученного путем моделирования) выбирается уровень допустимого риска и коэффициент относительного шага шкалы риска, позволяющий формализовать отнесения последствий реализации ИТВ к одной из четырех категорий риска, принятых согласно принципу ALARP, также индивидуально для каждого типа ИТВ выбираются значения функции значимости.

С учетом изложенного, итоговая интегральная оценка риска системы может рассчитываться по формуле

$$R_{МСУ} = \frac{\sum_{j=0}^{3} k_j z_j w_j}{RS}, \qquad (10)$$

где k_j – количество ИТВ с уровнем риска j;

z_j – значение функции значимости соответствующего риска;

w_j – условный вес соответствующего уровня риска;

$RS = N \cdot k_3 \cdot w_3$, N – число типов реализуемых ИТВ согласно модели угроз.

Кроме того, в методике предлагается учитывать уровень проектной защищенности МСУ, соответствующий ее структурным построением и функциональным возможностям, определяемый дополнительными показателями таблицы 2.

Шаг 7. Оценка динамики рисков нарушения защищенности МСУ в условиях ИТВ состоит в перерасчете функции риска, в которую вводится дополнительный

коэффициент, основанный на распределении Вейбулла-Гнеденко и, в результате, получении динамической оценки защищенности МСУ.

Динамика рисков нарушения защищенности МСУ в условиях ИТВ описывается функцией интенсивности сбоев (отказов), базирующейся на функции распределения Вейбулла-Гнеденко. Функция плотности распределения определена формулой (11), где α – параметр формы распределения, задающий характер динамики риска во время всех стадий жизненного цикла модели (рисунок 2), $R_{БАЗ}$ – параметр, определяющий уровень значения коэффициента базового риска функции распределения

$$f\left(t_{ЖЦ}\right)=\frac{at^{a-1}e^{-\left(\frac{t_{ЖЦ}}{R_{БАЗ}}\right)^{a}}}{R_{БАЗ}}. \qquad (11)$$

Значения функции распределения Вейбулла-Гнеденко сосредоточены на полуоси от 0 до бесконечности. Для экспериментальных исследований динамики рисков нарушения защищенности МСУ в условиях разнотипных и массированных ИТВ и минимизации испытаний введем сдвиговый коэффициент и используем гипотезу о трехпараметрическом распределении Вейбулла-Гнеденко, а также понятие функции риска [4].

Функция динамики оценки рисков нарушения защищенности МСУ выводится из трехпараметрического распределения, результат преобразований приведен в (12). Для получения функции динамики риска нарушения защищенности МСУ $R_{ДИН}(t_{ЖД})$ требуется учет параметра сдвига, определяемого по результатам моделирования и позволяющего построить корректную форму динамики риска для каждого типа МСУ, при этом характер поведения функции определяется (14)

$$R_{\text{ДИН}}\left(t_{\text{ЖЦ}}\right)=\frac{a_k\left(t_{\text{ЖЦ}}-t_k\right)^{(a_k-1)}}{\left(\frac{1}{R_{\text{БАЗ}}}\right)^{a_k}},\ k\in[1,2,3]. \qquad (12)$$

Значения индекса t_k являются различными для разных этапов жизненного цикла модели (рисунок 2), более подробно их формирование описывается в [3]. Общий вид кривой динамики риска будет определяться тремя составляющими модели, для каждой из которых на основе моделирования подбираются свои значения коэффициентов. Базовые условия приведены в (13)

$$a_k:\{k=1:0<a_k<1\{k=2:a_k=1,$$
$$t_k:\{k=1:t_k=0\{k=2:t_k=0, \qquad (13)$$

$$R_{ДИН}\left(t_{ЖЦ}\right):\{a=1:R_{ДИН}(t)=Const\{a>1:R_{ДИН}(t)\uparrow. \qquad (14)$$

Графическое оценивание и прогнозирование изменения функции динамики оценки рисков нарушения защищенности МСУ в условиях ИТВ на основе распределения Вейбула-Гнеденко представлено на рисунке 2.

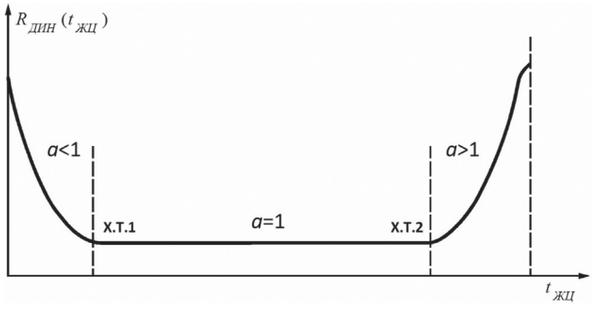


Рисунок 2 – Общий вид функции динамики риска

Динамика риска (первый этап, до характеристической точки х.т.1) определяется повышенным уровнем риска, обусловленным началом эксплуатации системы и следующими потенциальными угрозами:

- сбой (отказ) в работе новой версии программного обеспечения;
- внесенные потенциальные уязвимости в новую версию программного и аппаратного обеспечения;
- недостаточный уровень отладки информационного взаимодействия программных и аппаратных средств МСУ в ходе выполнения ТЦУ.

В то же время уровень риска нарушения защищенности МСУ со временем снижается за счет выпуска и внедрения обновлений программ («патчей») в МСУ, а также доработки алгоритмов управляющих программ с учетом изменений модели угроз ИТВ нарушителя.

На рисунке 2 динамика риска $R_{ДИН}(t_{ЖД})$ на участке между двумя характеристическими точками х.т.1 и х.т.2 (второй этап) является линейной и соответствует базовому уровню риска, полученному на основе статистической оценки (10-12). Этот участок соответствует штатному функционированию отлаженной системы, когда периодичность выхода «патчей» является установившейся величиной и алгоритмы управления МСУ отлажены.

На участке после характеристической точки х.т. 2 (третий этап) $R_{ДИН}(t_{ЖД})$ показывает плавное увеличение уровня риска, что связано как с возможным снижением надежности аппаратных средств, так и появлением со временем не устраненных ошибок в программных средствах, обусловленных ИТВ нулевого дня. Динамическая поправка риска $R_{ДИН}(t_{ЖД})$ (выражение (14)) сформирована таким образом, что на этапе между точками х.т.1 и х.т.2 (второй этап) она имеет значение, равное единице.

Для реальной МСУ требуется уточнение параметров $R_{ДИН}(t_{ЖД})$ с учетом тех особенностей, которыми обладает система и контролируемый сенсорами СОПКА технологический цикл управления. В случае, когда максимально выполнены требования к проектной защищенности МСУ, риск нарушения защищенности будет минимален.

Уточнение значения риска нарушения защищенности будет уточняться по результатам экспериментальных исследований на стендовом полигоне в условиях различных ИТВ, а также с учетом динамики риска на протяжении жизненного цикла системы управления на основе функции риска.

Вывод. Предлагаемая методика оценки защищенности МСУ критически важными информационными объектами позволяет получить числовую статистическую и динамическую оценку риска нарушения защищенности рассматриваемой системы в условиях ИТВ нарушителя. Научная новизна предложенной методики заключается в разработке модели функционирования МСУ в условиях ИТВ на основе расширенных сетей Петри и математических соотношений для определения функции риска нарушения защищенности МСУ с использованием распределения Вейбулла-Гнеденко.

Авторы выражают признательность проф. И.Б. Шубинскому за помощь в оценке интегрального риска нарушения информационной защищенности системы управления.

Библиографический список

1. Климов С.М., Купин С.В., Купин Д.С. Модели вредоносных программ и отказоустойчивости информационно-телекоммуникационных сетей // Надежность. – 2017. – Том 17, № 4. – С. 36-43. DOI: 10.21683/1729-2640-2017-17-4

2. «Умные» среды, «умные» системы, «умные» производства: серия докладов (серия зеленых книг) в рамках проекта «Промышленный и технологический форсайт Российской Федерации» / Коллектив авторов; Фонд «Центр стратегических разработок «Северо-Запад». – СПб, 2012. – Вып. 4. – 62 с.

3. ГОСТ Р 50779.27-2017 Статистические методы. Распределение Вейбулла. Анализ данных.

4. К. Капур, Л. Ламберсон. Надежность и проектирование систем. Под ред. И.А. Ушакова. Пер. с англ. – М.: «Мир», 1980. – 604 с., ил.

5. Климов С.М., Астрахов А.В., Сычев М.П. Методические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 110 с, 2013.

6. Климов С.М., Астрахов А.В., Сычев М.П. Технологические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 71 с, 2013.

7. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза / И.Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2016. – 544 с.

8. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

9. Климов С.М., Котяшев Н.Н. Метод регулирования рисков комплексов средств автоматизации в условиях компьютерных атак // Надежность. – 2013. – №2. – С. 93-107.

10. Антонов С.Г., Климов С.М. Методика оценки рисков нарушения устойчивости функционирования программно-аппаратных комплексов в условиях информационно-технических воздействий // Надежность. – 2017. – Том 17. – №1. – С.32-39.

11. Климов С.М., Половников А.Ю., Сергеев А.П. Модель функциональной отказоустойчивости процессов обеспечения потребителей навигационными сигналами в сложных условиях // Надежность. – 2017. – Том 17, № 2. – С.41-47.

12. Климов С.М., Поликарпов С.В., Федченко А.В. Методика повышения отказоустойчивости сетей спутниковой связи в условиях информационно-технических воздействий. // Надежность. – 2017. – Том 17, №3. – С. 32-40.

13. Гапанович В.А., Шубинский И.Б., Замышляев А.М. Метод оценки рисков системы из разнотипных элементов // Надежность. – 2016. – Том 16, № 2. – С.49-53.

14. Гапанович В.А., Розенберг Е.Н., Шубинский И.Б. Некоторые положения отказобезопасности и киберзащищенности систем управления // Надежность. – 2014. – №2. – С.88-100.

Сведения об авторах

Сергей М. Климов – доктор технических наук, профессор, начальник управления 4 ЦНИИ Минобороны России, Королев, Россия, e-mail: klimov.serg2012@yandex.ru

Юрий В. Сосновский – кандидат технических наук, доцент кафедры компьютерной инженерии и моделирования Физико-технического института Крымского федерального университета им. В.И. Вернадского, Симферополь, Россия, e-mail:yuri.sosnovskij@yandex.ru

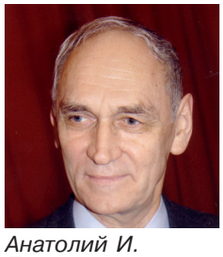
Поступила 23.08.2018

Оригинальная статья
Надежность, том 18, №4, 2018 DOI: 10.21683/1729-2646-2018-18-4-45-50

Риск как одно из свойств качества решений, принимаемых в условиях неопределенности

Владимир И. Звягин, *Военно-космическая академия имени А.Ф.Можайского, Санкт-Петербург, Россия*
Анатолий И. Птушкин, *Военно-космическая академия имени А.Ф.Можайского, Санкт-Петербург, Россия*
Алексей В. Трудов, *Военно-космическая академия имени А.Ф.Можайского, Санкт-Петербург, Россия*

Владимир И. Звягин



Анатолий И. Птушкин

Алексей В. Трудов

Резюме. Цель. *Широчайшая распространённость различных видов деятельности и соответствующих им возможных неблагоприятных исходов породила необычайное многообразие трактовок всего понятийного фонда, связанного с риском, в том числе в нормативных документах. Это обстоятельство входит в противоречие с основной целью стандартизации научно-технической терминологии – установление однозначно понимаемой и непротиворечивой терминологии во всех видах документации, входящей в сферу работ по стандартизации или использующей результаты этих работ. В связи с этим целью статьи является оценка соответствия определений понятия «риск» в комплексе стандартов по менеджменту риска требованиям нормативных документов системы стандартизации РФ и разработка предложений по новой трактовке этого понятия.* **Методы.** *Для обоснования необходимости корректировки существующих определений риска и выработки определения, отвечающего всем требованиям нормативных документов системы стандартизации РФ, использовались методы терминологического, логикосемантического и системного анализа.* **Результаты.** *Проведен анализ соответствия существующих определений термина «риск» требованиям системы стандартизации РФ, который показал, что они далеко не в полной мере соответствуют этим требованиям, а поэтому трактовка понятия «риск» нуждается в пересмотре. Обоснована целесообразность трактовки риска как одного из свойств качества решения, принимаемого в ситуации с неопределёнными исходами. Это свойство характеризует возможность и последствия недостижения целей человеческой деятельности в ситуации принятия решения о выборе дальнейших действий в условиях неопределённости. Исходя из этого дано следующее новое определение термина риск: риск (рискованность) – это одно из свойств качества решения, принимаемого в ситуации с неопределёнными исходами, характеризующее возможность и последствия недостижения поставленных целей. Рассмотрены преимущества предложенной трактовки риска перед существующими определениями.* **Выводы.** *Предложено и обосновано новое определение термина «риск», которое может рассматриваться как предпочтительное по отношению к существующим вариантам. Предложенное определение базируется на важнейших для теории и практики управления понятиях «свойство», «качество», «решение», «ситуация», «цели», которые входят в число базовых категорий человеческого познания. На этой основе возникает возможность использования как уже существующих количественных характеристик риска, так и расширения аппарата обоснованных характеристик риска, в том числе заимствованных из арсенала средств оценки интенсивности проявления свойств различных объектов, принятых в других областях науки. Показаны такие особенности предложенной трактовки риска как комплексность, ситуативность и целевая ориентация. Комплексность и целевой характер риска обусловливают необходимость рассмотрения реальных возможностей достижения требуемых характеристик безопасности, результативности, ресурсоемкости и своевременности достижения поставленных целей деятельности. Ситуативный характер риска как свойства решения в конкретной ситуации влечет за собой необходимость рассмотрения всего множества соответствующих атрибутов ситуации, от которых они зависят: состава объектов и субъектов человеческой деятельности, а также условий и обстоятельств, создающих определенные отношения между ними. Подобный подход существенно повышает достоверность выявления перечня и природы факторов, влияющих на риск и, следовательно, расширяет возможности выбора средств и методов управления им.*

Ключевые слова: *термин, риск, свойство, качество, ситуация, неопределенность исхода, управленческое решение, недостижение цели, характеристики, показатели.*

Формат цитирования: *Звягин В.И., Птушкин А.И., Трудов А.В. Риск как одно из свойств качества решений, принимаемых в условиях неопределенности // Надежность. 2018. Т. 18, № 4. С. 45-50. DOI: 10.21683/1729-2646-2018-18-4-45-50*

Введение

Понятие риска издавна связано с возможностью возникновения какого-либо неблагоприятного (нежелательного) результата некой деятельности в условиях неполной информации о ее дальнейшем протекании. Таким результатом может быть ущерб или конфликт того или иного вида (материальный или экономический ущерб, причинение вреда жизни или здоровью людей и животных, экологический ущерб, политический конфликт и т.д.). Учет риска является обязательным при обосновании практически всех важных решений.

Широчайшая распространённость различных видов деятельности и соответствующих им возможных неблагоприятных исходов породила необычайное многообразие трактовок всего понятийного фонда, связанного с риском, в том числе в нормативных документах (НД). Это обстоятельство входит в противоречие с основной целью стандартизации научно-технической терминологии [1] – установление однозначно понимаемой и непротиворечивой терминологии во всех видах документации и литературы, входящих в сферу работ по стандартизации или использующих результаты этих работ.

Отсюда логически вытекает и одна из основных задач стандартизации научно-технической терминологии – анализ, выявление и исправление недостатков терминологии, в первую очередь – в национальных стандартах. Важность этого направления исследований уже давно подчеркивалась в трудах видных специалистов в таких наукоемких, энергоемких и риско-чувствительных областях как ядерная и радиационная безопасность [2], надежность и безопасность структурно-сложных систем [3, 4], надежность и безопасность пневмогидравлических систем ракетно-космических комплексов [5] и др. С особой силой значимость данной проблемы выражена в [2]: «…от четкости нормативных документов во многом зависит вся наша жизнь… Четкость терминологии лежит в основе как постановки научных задач, так и принятия регулирующих законов». Актуальность этой задачи в плане исследования содержательной трактовки таких важнейших понятий как надежность, безопасность и риск подтверждается в последние годы целым рядом публикаций терминологического характера, например, [6, 7, 8].

Целью настоящей статьи является оценка соответствия определений понятия «риск» в комплексе стандартов по менеджменту риска требованиям НД системы стандартизации РФ и разработка предложений по новой трактовке этого понятия.

1. Объект и цель проводимого анализа требований системы стандартизации РФ

Для придания конструктивности и конкретности излагаемых далее положений сузим объект рассмотрения, ограничив его следующими двумя условиями:

- анализу будут подвергаться не разрозненные ГОСТы, а комплекс действующих стандартов «Менеджмент риска» с практически одинаковыми объектами стандартизации и областями применения. Названный комплекс включает в настоящее время более 25 стандартов! Однако не все стандарты этой серии содержат определения риска, поэтому подвергнем анализу лишь те НД, где такие определения приведены [10-24];

- анализ будет проводиться с целью оценки соответствия терминологических положений, формулируемых в рассматриваемом комплексе стандартов, требованиям действующей в РФ системы стандартизации. Для достижения этой цели необходимо найти ответы на следующие три вопроса.

Во-первых, насколько оправдано вышеупомянутое многообразие воззрений на сущность понятия «риск»? Наиболее логичным объяснением этому могла бы быть лишь существенная зависимость приведенных определений от особенностей соответствующих видов деятельности. Поэтому первое, что необходимо выяснить, – это присутствует ли в существующих определениях риска их зависимость от специфики той или иной деятельности?

Во-вторых, если при анализе первого вопроса выяснится, что существующие определения риска инвариантны к особенностям той или иной деятельности, то возникает следующий вопрос – имеется ли среди множества существующих определений такое, которое в наибольшей мере отвечает требованиям НД системы стандартизации и, следовательно, может быть использовано (рекомендовано) в качестве универсального, общепринятого определения риска?

И, в-третьих, при отрицательных ответах на оба предыдущих вопроса возникает последний – какое определение риска может быть предложено в качестве приемлемого в плане его соответствия требованиям НД системы стандартизации?

Поиску ответов на эти вопросы и соответствующим предложениям посвящены последующие подразделы статьи.

2. Обзор существующих определений термина «риск» в действующих стандартах.

Проведенный анализ вышеназванной группы документов [10-24] показал, что в них определение риска встречается, главным образом, в виде трех вариантов формулировок:

- риск – вероятность причинения вреда жизни или здоровью граждан, имуществу, окружающей среде и т.д. с учетом тяжести этого вреда [10]. Примерно такая же формулировка содержится и в [11] с тем отличием, что помимо количественной предлагается и качественная мера значимости возможного ущерба;

- риск – сочетание вероятности появления опасного события и его последствий [12-21];

- риск – следствие влияния неопределенности на достижение поставленных целей [22-24].

К этим определениям риска, содержащимся в НД, могут быть добавлены определения риска, встречаю-

щиеся в научно-технических публикациях, в которых, например, риск трактуется как опасное (нежелательное) событие, мера опасности, действие наудачу, упущенная выгода и т.п. Эти и другие виды определений сопровождаются пространными классификациями рисков по множеству самых разнообразных признаков, например, по роду опасности (риски техногенные, природные и т.д.), по сфере проявления (риски финансовые, экономические, экологические и т.д.), по масштабам последствий (большие, средние, малые, критические, катастрофические и т.д.) К сожалению, ни эти определения и классификации, ни перечисляемые в них наименования, функции и свойства рисков никак не проясняют суть самого понятия и оставляют вопрос открытым.

Из приведенных определений риска следует ответ на первый из выше сформулированных вопросов, а именно – *существующие определения рисков в НД и научно-технической литературе носят достаточно общий характер и не связаны с особенностями той или иной деятельности.* В силу сказанного существующее в НД многообразие этих определений вряд ли можно признать полезным для теории и практики.

3. Анализ соответствия существующих определений термина «риск» требованиям системы стандартизации РФ

Главным, ведущим принципом НД системы стандартизации РФ [25-29] является однозначность понимания требований, включаемых в документы в области стандартизации [26]. Для реализации данного принципа необходимо выполнение группы основных требований этой системы, сводка которых приведена в таблице 1.

Заметим, что в таблице 1 требования 4-6 относятся не только к терминам, но и к их определениям. Первое, что можно сказать, анализируя перечисленные требования, это что в вышеприведенных формулировках риска даны разные по содержанию понятия для одного и того же термина, что противоречит требованиям 1-2. Более того, имеет место противоречие между первыми двумя и третьей трактовкой риска. Действительно, в первом случае риск выступает как мера, а во втором – как некое следствие влияния неопределенности, которое можно трактовать как угодно: численно, качественно, какими-то вербальными конструкциями и т.д., что не соответствует требованию 3.

Если говорить о каждом определении риска по отдельности, то труднее всего согласиться с третьей трактовкой, т.к. она хоть и содержится в терминологических гармонизированных стандартах [22, 23], но не отвечает требованиям 4-6.

Последнее требование, приведенное в этой таблице, может наилучшим образом выполняться при использовании интенсиональных определений [29]. В интенсиональном определении базовая часть определяет превосходящее по классу понятие, к которому рассматриваемое понятие принадлежит, а вторая часть перечисляет ограничивающие характеристики, которые устанавливают отличие этого по-

Таблица 1 – Требования нормативных документов системы стандартизации к формированию терминов и их определений

№	Содержание требования
1	Одно обозначение (т. е. термин, символ или название) должно соответствовать одному понятию, и только одно понятие соответствовать одному обозначению
2	Недопустимо использование одного термина для многих понятий и многих терминов для одного понятия
3	Терминологические статьи в тесно связанных стандартах не должны содержать противоречий
4	Термин должен показывать ограничивающие характеристики выражаемого понятия
5	Термин должен поддерживать привычную устоявшуюся выразительную форму в языковом сообществе
6	Термин должен соответствовать морфологическим, морфосинтаксическим и фонологическим обычаям языка
7	Родной язык должен быть предпочтительным
8	Определение термина должно состоять из одной фразы, определяющей понятие и, по возможности, отражающей его положение в системе понятий

нятия от его равноправных понятий. И вот тут приходится сказать о недостатках наиболее распространенных определений понятия «риск» в виде первых двух трактовок. В них, к сожалению, используется не интенсиональное определение с соответствующей базовой частью и ограничивающими характеристиками, а просто дано отождествление риска с его мерой (о чем уже выше было сказано), т.е. одной из возможных числовых характеристик, что является смешением различных смысловых категорий и не соответствует требованию 8. Помимо этого замена смысловой трактовки числовой характеристикой (показателем) входит в противоречие с другими стандартами комплекса «менеджмент риска» (см. например, [20, 21]), где фигурируют такие показатели как индекс риска и индекс серьезности риска, по смыслу аналогичные упомянутым трактовкам риска, но описывающие уровень риска, а не сам риск.

Таким образом, *проведенный анализ существующих определений риска показал, что они далеко не в полной мере соответствуют основным принципам и требованиям системы стандартизации РФ. Отсюда следует вывод, что понятие «риск» требует переосмысления,* чему и посвящен следующий подраздел статьи.

4. Предложения по трактовке понятия «риск», удовлетворяющей требованиям системы стандартизации РФ

Для начала следует отметить, что в существующих научно-технических публикациях, а тем более – в НД обнаружить какие-либо обоснования вышеприведенных определений риска не удается. Практически во всех слу-

чаях они просто постулируются, причем часто с многочисленными примечаниями, дополняющими предлагаемое определение возможными вариантами его интерпретации (см., например, [22-24]). Нежелательность подобного подхода, собственно, и проиллюстрирована выше.

Обоснование трактовки термина «риск» может быть выполнено на основе применения методов терминологического, логикосемантического и системного анализа и состоит в следующем.

Человеческий опыт неопровержимо свидетельствует о том, что понятие «риск» при любом его понимании практически всегда связано с ситуацией принятия решения о предстоящих действиях в условиях неопределенности. Суть такой ситуации заключается в каком-то выборе из множества альтернатив при недостатке информации, необходимой для достоверного прогноза возможности и характера последствий принимаемого решения. С наибольшей остротой подобная ситуация характерна для управленческих решений, принимаемых в условиях неполноты исходной информации. Такая тесная связь риска с управленческими решениями позволяет воспользоваться некоторыми результатами теории управления, широко освещаемой в литературе по менеджменту.

Одним из центральных понятий этой теории является качество управленческого решения, под которым по аналогии с получившей широкое распространение трактовкой качества продукции в [32]) понимают (см., например, [30, 31]) совокупность свойств (характеристик, параметров) принимаемого решения, выполняющих определенную роль в процессе управления и удовлетворяющих конкретного потребителя. Непременными атрибутами решения, принимаемого в условиях неопределенности, являются возможность и последствия недостижения предусмотренных этим решением целей.

К сказанному остается добавить, что качество управленческого решения необходимо уметь измерять, а поэтому вряд ли имеет смысл отходить в концептуальном плане от рекомендаций науки о методологии и проблематике измерения качества объектов любой природы – квалиметрии, согласно которой качество – это совокупность свойств объекта, с которыми человек сталкивается в своей практической деятельности.

Исходя из изложенных соображений, представляется вполне логичным и уместным включить в комплекс таких свойств рискованность (риск) принимаемого решения. Именно это свойство характеризует возможность и последствия недостижения целей человеческой деятельности в ситуации принятия решения о выборе дальнейших действий в условиях неопределенности. Тогда можно дать следующее итоговое определение термина риск:

Риск (рискованность) – это одно из свойств качества решения, принимаемого в ситуации с неопределёнными исходами, характеризующее возможность и последствия недостижения поставленных целей.

При этом заметим, что при проведении сценарного анализа указанной ситуации должна быть отражена вся потенциальная семантика множества возможных исходов: позитивных, негативных, нейтральных и др.

Кратко прокомментируем основные системные особенности предложенного определения. Во-первых, его особенностью является интерпретация риска не как меры, а как некоего атрибута принимаемого решения, а именно – его свойства. Во-вторых – риск как свойство является компонентом качества этого решения как некоего управленческого акта. Третья особенность состоит в комплексности риска как свойства принимаемого решения в целенаправленных процессах. Действительно, любая деятельность человека связана с необходимостью достижения, по крайней мере, четырех целей: обеспечение требуемых характеристик безопасности, результативности, ресурсоемкости и своевременности ее выполнения. Многоцелевой характер этой деятельности обусловливает необходимость рассмотрения риска как комплексного свойства, включающего в себя свойства, характеризующие возможность и последствия несоответствия требуемым значениям реальных показателей степени достижения целей. Примеры недостижения этих целей в технических областях приведены в таблице 2.

И, наконец, четвертая особенность приведенного определения риска состоит в его ситуативном характере, зависимости от ситуации принятия решения, т.е. от состава объектов и субъектов человеческой деятельности, условий и обстоятельств, создающих определенные отношения между ними.

Следует подчеркнуть, что принятию решения должен предшествовать целый комплекс подготовительных процедур, в том числе, например, прогнозирование возможных последствий катастрофических природно-климатических явлений. На основании результатов выполнения таких процедур должно быть сформировано решение о характере и последовательности последующих действий для достижения поставленной цели.

Таблица 2. Примеры недостижения целей деятельности

Цели	Примеры
Обеспечение безопасности	Гибель персонала или населения, причинение вреда здоровью персоналу или населению, оборудованию или собственности населения, окружающей природной среде
Обеспечение результативности	Недостижение требуемых значений показателей качества спроектированного изделия, невыполнение поставленной задачи
Достижение ребуемого результата выделенными средствами	Превышение объемов выделенных ресурсов (материальных, финансовых и других)
Своевременное достижение требуемого результата	Задержки в окончании работ, выполняемых на различных этапах достижения результата

Заключение

Приведенные выше обоснование и особенности предложенной трактовки риска позволяют выделить следующие ее преимущества перед существующими определениями.

1. Прежде всего, данное определение свободно от недостатков существующих определений и отвечает всем требованиям системы стандартизации РФ. По этой причине предложенное определение риска может рассматриваться как предпочтительное по отношению ко всем остальным существующим вариантам, не отвечающим, как показано в статье, требованиям этой системы.

2. Предложенное определение базируется на важнейших для теории и практики управления понятиях «решение», «свойство», «качество», «цель», «ситуация», которые входят в число базовых категорий человеческого познания и во многом определяют дифференциацию наук. Риск как свойство, как сторона качества обладает интенсивностью проявления, т.е. может быть «большим» или «меньшим», «высоким» или «низким», «приемлемым» или «неприемлемым» и т.д. Отсюда возникает возможность расширения аппарата обоснованных характеристик риска, как качественных, так и, что особенно ценно – количественных. В частности, трактовка риска как одного из свойств качества позволяет использовать методологию оценки интенсивности проявления свойств различных объектов, принятую в других областях науки, в том числе – в квалиметрии, в теории надежности, теории игр, исследовании операций и др. Так, например, следуя достаточно хорошо разработанному понятийному фонду такого важнейшего для науки свойства техники, как надежность [33], представляется возможным заимствование наиболее устоявшихся в этой области и апробированных терминов и понятий. В частности, вполне возможна дифференциация риска как комплексного свойства на ряд частных его свойств. При этом подчеркнем, что риск как свойство принимаемого человеком решения имеет объективную природу, хотя его оценочные характеристики могут иметь и признаки субъективизма, что вполне естественно.

3. Предложенная трактовка риска никак не отменяет, а вполне допускает и использование бытующих в настоящее время в литературе характеристик риска, таких, например, как вероятность того или иного сценария реализации риска, размер ущерба (убытка), их сочетание, уровень риска, индекс риска [20, 21] и др. Остаются в силе и многочисленные классификации риска по видам деятельности и другим признакам, рассмотрение стадий и этапов разработки требований к риску, его анализа и управления и т.д. – в общем, весь арсенал средств исследования риска как полноценной научной категории.

4. Фигурирующая в определении риска понятие «ситуации принятия решения» влечет за собой необходимость при выборе и исследовании характеристик риска рассмотрения всего множества соответствующих атрибутов этой ситуации, влияющих на величину риска. Поэтому непременным компонентом оценки риска должен быть анализ всех сценариев (сценарный анализ) возникновения нежелательных событий, вытекающих из этой и других потенциальных ситуаций, которые могут возникнуть в процессе реализации принятого решения. Подобный подход существенно повышает достоверность выявления перечня и природы факторов, влияющих на риск и, следовательно, расширяет возможности выбора средств и методов управления им.

5. Из целевой ориентации данной трактовки риска непосредственно вытекает ряд важных требований к организации управленческой деятельности, к числу которых относятся:

- любое управляющее решение должно быть риск-ориентированным, т.е. непременно содержать оценку характеристик возможности и последствий недостижения целей, предусмотренных этим решением;
- при формировании решения необходимо совместное рассмотрение взаимного влияния компонент риска, связанных со всеми предусмотренными в нем целями;
- для улучшения качества согласования интересов участников выполнения решения и использования выделенных ресурсов необходимо учитывать весь комплекс институциональных отношений между ними;
- с целью повышения достоверности выявления перечня и природы факторов, влияющих на риск, и расширения возможности выбора средств и методов управления им необходимо при формировании альтернативных решений рассмотрение как можно более полного множества ситуационных характеристик.

Завершая статью, хочется еще раз отметить, что понятие риска является широко употребляемым в самых разнообразных областях деятельности и поэтому требует пристального внимания всех заинтересованных сторон. Авторы убеждены, что предложенная интерпретация риска как свойства качества решений, принимаемых в условиях неопределённости, является плодотворной с точки зрения развития теории управления риском. Однако они отдают себе отчет в том, что предложенное определение и его аргументация не являются свободными от недостатков, а поэтому их конструктивная критика в рамках соответствующей дискуссии могла бы быть полезной.

Библиографический список

1. Р 50.1.075-2011 Рекомендации по стандартизации. Разработка стандартов на термины и определения. Утверждены и введены в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2011 г. № 35-ст.

2. Гордон Б.Г. Об использовании понятия риска в различных отраслях промышленности // Вестник Госатомнадзора России. – 2003. – № 1. – С-3-7.

3. Рябинин И.А. Надежность и безопасность структурно-сложных систем. СПб.: Изд-во С.-Петерб. ун-та, 2007. – 276с.

4. Шубинский И. Б. Структурная надежность информационных систем: методы анализа / И. Б. Шубинский. – Ульяновск: Печатный двор, 2012. – 216 с.

5. Голиков И.О., Гранкин Б.К. О состоянии нормативного обеспечения сложных технических комплексов // Стандарты и качество. – 2016. – № 5(947). – С. 76-80.

6. Голиков И.О, Гранкин Б.К., Звягин В.И. Обучение качеству по стандартам // Стандарты и качество. – 2017. – № 2(956). – С. 29-33.

7. Похабов Ю.П. О дефиниции термина «надежность» // Надежность. – 2017. – Том 17, №1. – С. 4-10.

8. Струков А.В. Анализ международных и российских стандартов в области надежности, риска и безопасности [электронный ресурс] URL: https://szma.com/standarts_analysis.pdf Дата обращения 07.06.2018.

9. ГОСТ 1.1-2002. Межгосударственная система стандартизации. Термины и определения. – М: ИПК Изд-во стандартов, 2003.

10. Федеральный закон от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании» (с изменениями на 29 июля 2017 года).

11. ГОСТ Р ИСО 11231-2013 Менеджмент риска. Вероятностная оценка риска на примере космических систем. – М: Стандартинформ, 2014.

12. ГОСТ Р ИСО 12100-1-2007 Безопасность машин. Общие принципы конструирования. Часть 1. Основные термины, методология. – М: Стандартинформ, 2008.

13. ГОСТ Р ИСО 17666 – 2006 Менеджмент риска. Космические системы. – М: Стандартинформ, 2006.

14. ГОСТ Р ИСО-МЭК 31010-2011. Менеджмент риска. Методы оценки риска. – М: Стандартинформ, 2012.

15. ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем. – М: ИПК Издательство стандартов, 2002.

16. ГОСТ Р 51901.4-2005 Менеджмент риска. Руководство по применению при проектировании. – М: Стандартинформ, 2005.

17. ГОСТ Р 51901.11-2005 Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство. – М: Стандартинформ, 2006.

18. ГОСТ Р ИСО- МЭК 16085- 2007 Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения. – М: Стандартинформ, 2008.

19. ГОСТ Р 56255-2014 Термины и определения в области обеспечения безопасности жизни и здоровья. – М: Стандартинформ, 2015.

20. ГОСТ Р 54144-2010 Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Идентификация инцидентов. – М: Стандартинформ, 2012.

21. ГОСТ Р 54145-2010 Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Общая методология. – М: Стандартинформ, 2012.

22. ГОСТ Р 51897-2011 Менеджмент риска. Термины и определения. – М: Стандартинформ, 2012.

23. ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь. – М: Стандартинформ, 2015.

24. ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство. – М: Стандартинформ, 2012.

25. Федеральный закон от 29.06. 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации» (с изменениями на 3 июля 2016 года).

26. ГОСТ Р 1.0-2012 Стандартизация в Российской Федерации. Основные положения. (с изменениями от 01.07.2014 г.). – М: Стандартинформ, 2013.

27. ГОСТ Р 1.2-2016 Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила разработки, утверждения, обновления, внесения поправок, приостановки действия и отмены. – М: Стандартинформ, 2016.

28. ГОСТ Р 1.5-2012 Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения. – М: Стандартинформ, 2013.

29. ГОСТ Р ИСО 10241-1-2013 Терминологические статьи в стандартах. Часть 1. Общие требования и примеры представления. – М: Стандартинформ, 2015.

30. А.Г. Поршнев, М.Л. Разу, А.В. Тихомирова. Менеджмент: теория и практика в России: Учебник / Под ред. А.Г. Поршнева, М.Л. Разу, А.В. Тихомировой. – М: ИД ФБК-ПРЕСС, 2003, 528 с.

31. Прохоров Ю.К., Фролов В. В. Управленческие решения: Учебное пособие. – 2-е изд., испр. и доп. СПб: СПбГУ ИТМО, 2011. – 138 с.

32. ГОСТ 15467-79 Управление качеством продукции. Основные понятия, термины и определения. – М: Стандартинформ, 2009.

33. ГОСТ 27.002-2015 Надежность в технике. Термины и определения. – М: Стандартинформ, 2016.

Сведения об авторах

Владимир И. Звягин – кандидат технических наук, профессор, профессор кафедры организации эксплуатации и технического обеспечения вооружения, военной и специальной техники Военно-космической академии имени А.Ф.Можайского, Санкт-Петербург, Россия, e-mail: v.zvyagin@mail.ru

Анатолий И. Птушкин – кандидат технических наук, профессор, профессор кафедры организации эксплуатации и технического обеспечения вооружения, военной и специальной техники Военно-космической академии имени А.Ф.Можайского, Санкт-Петербург, Россия, e-mail: anatoly.ptushkin2011@yandex.ru

Алексей В. Трудов – кандидат технических наук, доцент кафедры организации эксплуатации и технического обеспечения вооружения, военной и специальной техники Военно-космической академии имени А.Ф.Можайского, Санкт-Петербург, Россия, e-mail: trudovalex2016@yandex.ru

Поступила: 28.06.2018

УДК 656.2-027.45:343.326
Оригинальная статья
Надежность, том 18, №4, 2018 DOI: 10.21683/1729-2646-2018-18-4-51-55

Обеспечение эффективной системы безопасности объектов транспортной инфраструктуры посредством систем, позволяющих зафиксировать факт проникновения посторонних лиц в охраняемую зону

Наталья А. Кузьмина, *Дальневосточный государственный университет путей сообщения, Хабаровск, Россия*

Наталья А. Кузьмина

Резюме. *Ввиду специфики работы транспорт сам по себе является потенциальным источником опасности. А если вторгнуться в его сферу незаконными, агрессивными действиями, опасность становится реальной, грозящей тяжелейшими последствиями. Статистика последних 10–15 лет показывает, что от 50 до 70% совершаемых террористических актов связано с транспортом. Какими–то отдельными мерами обеспечить транспортную безопасность невозможно. К этой проблеме надо подходить комплексно и системно. От обеспечения транспортной безопасности существенно зависит национальная безопасность Российской Федерации. Федеральный закон «О транспортной безопасности» от 9 февраля 2007 г. № 16-ФЗ впервые в отечественной практике поставил вопрос об обеспечении безопасности всей транспортной отрасли Российской Федерации, установил правовые основы деятельности по обеспечению безопасности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства, в том числе террористической направленности. Впервые предусматривается единый для всех видов транспорта системный подход к антитеррористической защите. Транспорт – весьма уязвимый объект для террористических атак. Имеются в виду сами транспортные средства, транспортные коммуникации, помещения вокзалов, транспортные средства с опасными грузами. Уязвимость транспорта связана с возможностью повреждения средств сигнализации, устройств автоматики и связи, охрана которых с учетом масштабов и протяженности, железных дорог РФ затруднена. Несмотря на проблемные вопросы и объективные трудности в законодательных вопросах при реализации мер по обеспечению транспортной безопасности, работники железных дорог РФ прилагают усилия для обеспечения защищенности объектов транспортной инфраструктуры (ОТИ) и транспортных средств (ТС) от актов незаконного вмешательства. Незамедлительно реагируя на другие вызовы и угрозы, обеспечивают надежное функционирование работы транспортного комплекса, сохраняя тем самым спокойствие и безопасность наших граждан. В данной статье рассмотрены вопросы эффективной системы безопасности ОТИ. Большая роль отводится системам, позволяющим зафиксировать факт проникновения посторонних лиц в охраняемую зону объекта.*

Ключевые слова: *транспортная безопасность, акт незаконного вмешательства, объект транспортной инфраструктуры, система безопасности, охрана объекта, нарушитель, датчики, извещатели.*

Формат цитирования: *Кузьмина Н.А., Обеспечение эффективной системы безопасности объектов транспортной инфраструктуры посредством систем, позволяющих зафиксировать факт проникновения посторонних лиц в охраняемую зону // Надежность. 2018. Т. 18, № 4. С. 51-55. DOI: 10.21683/1729-2646-2018-18-4-51-55*

Несмотря на принимаемые меры субъектами транспортной инфраструктуры и перевозчиками по повышению уровня защищенности транспортного комплекса, угроза совершения актов незаконного вмешательства (АНВ) остается. Сухая статистика констатирует, что к сожалению, пока полностью исключить возможность совершения АНВ не предоставляется возможным. В этой связи первоочередной задачей является максимально затруднить попытки совершения АНВ в деятельность объектов транспортной инфраструктуры (ОТИ) и транспортных средств (ТС) и нарушить коварные планы нарушителей.

Это возможно лишь при консолидированном подходе государства и общества к вопросам обеспечения безопасности [1].

Федеральный закон № 16-ФЗ «О транспортной безопасности» обязывает защищать ОТИ от актов незаконного вмешательства [2].

Под защищенностью, как правило понимают наличие соответствия технических средств защиты, которые соответствуют категории объекта.

Такой подход не предусматривает оценку эффективности принятых мер и способности всей системы противостоять реальным угрозам. И нет никакой гарантии того, что в нештатной ситуации реагирование на нее будет своевременным и корректным.

Какой должны быть эффективная система безопасности объекта и как обеспечить его защищенность? Этот вопрос актуален сегодня для многих субъектов транспорт-

ной инфраструктуры, перед которыми стоит непростая задача обеспечения транспортной безопасности.

В начале 2014 г. в силу вступил федеральный закон № 15-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам обеспечения транспортной безопасности». При помощи этого документа были устранены пробелы Федерального закона № 16-ФЗ «О транспортной безопасности», действовавшего еще с 2007 года. Данный закон, являясь по своей сути базовым актом, имел чрезвычайно широкое толкование, не содержал конкретных требований к силам и средствам обеспечения транспортной безопасности, а по отдельным направлениям лишь формализовал процесс [3].

При комплексном подходе к обеспечению безопасности на ОТИ причины, повлекшие возможность совершения террористического акта, должны рассматриваться как симптомы неудовлетворительной организации эксплуатации данных объектов, на совершенствование которой требуется направлять основные усилия, людские и материальные ресурсы. Согласно предложенной профессором Колорадского университета (США) Д. Питерсоном теории множественности причин возникновения любой нештатной ситуации, можно не только спрогнозировать возможность ее возникновения, но и выявить обстоятельства, сделавшие возможным ее появление. Следовательно, безопасностью, в том числе и транспортной, не только можно, но и необходимо управлять так же, как и любой другой областью транспортной системы. Обеспечение транспортной безопасности должно представлять собой одну из неотъемлемых, ежедневных функций руководящих и оперативно-управленческих работников различного уровня, такую же, как снижение стоимости, обеспечение требуемого объема и качества перевозок грузов и пассажиров.

При решении задачи обеспечения безопасности на объектах транспортной инфраструктуры большая роль отводится системам, позволяющим зафиксировать факт проникновения посторонних лиц в охраняемую зону объекта. Для этой цели используются различные системы пультовой охраны, решающие задачи оповещения о факте проникновения на объект с указанием места и времени нарушения границы объекта. Данные системы обеспечивают сбор информации с датчиков, контролирующих места возможного проникновения на объект, фиксацию факта несанкционированного проникновения и передачу сигнала тревоги на пульт управления системой. Системы пультовой охраны часто интегрируются с системами пожарной сигнализации и имеют во многом схожую с ними архитектуру.

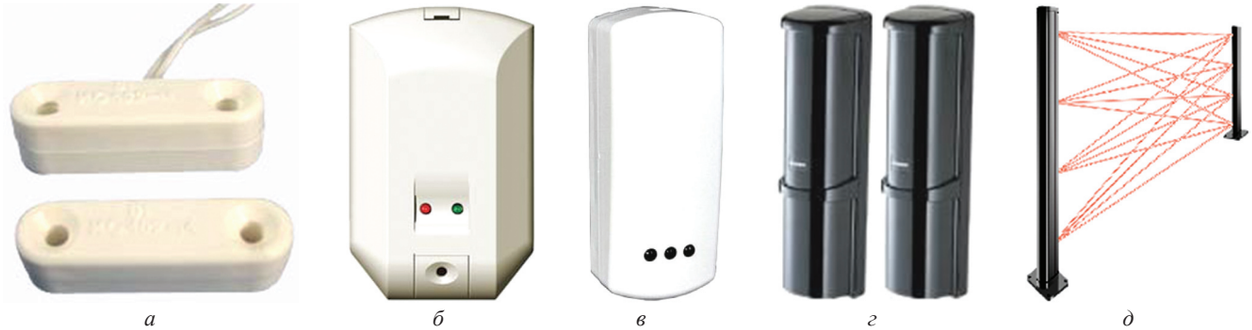
В состав системы охраны объекта входит оборудование централизованного управления, приемно-контрольные приборы (ПКП) или панели (ПКН) и датчики контроля охраняемого объекта. Централизованное управление системой обеспечивает компьютер или заменяющая его в небольших системах специальная панель управления. Приемно-контрольные приборы осуществляют питание шлейфов с устанавливаемыми на объекте датчиками, принимают и анализируют передаваемые датчиками сообщения, формируют и передают сигнал тревоги на пункт централизованного управления, управляют оповестительными устройствами и другими системами обеспечения безопасности объекта. На небольших объектах управление всеми системами может осуществляться непосредственно ПКП без передачи информации на пункт централизованного управления.

В системах пультовой охраны для контроля возможных мест проникновения на охраняемый объект используются различные, отличающиеся по типу и принципу действия и решаемой задаче, датчики-извещатели, такие как: магнитные, вибрационные, фотоэлектрические, микроволновые, ультразвуковые датчики, шлейфы, датчики разбития стекла, датчики движения.

Наиболее простыми, дешевыми и широко используемыми являются *магнитоконтактные датчики*, устанавливаемые на окна, двери охраняемого объекта. Данные датчики состоят из закрепляемого на подвижной части окна или двери магнитоуправляемого контакта – геркона и постоянного магнита, закрепляемого на раме окна или дверной коробке.

Примером такого датчика может служить накладной малогабаритный магнитоконтактный охранный извещатель ИО-102-14 (СМК-14, геркон), используемый для защиты дверей и окон (рисунок 1, *а*).

Датчики разбития стекла (рисунок 1, *б*) реагируют на звук бьющегося стекла и предназначены для защиты



а *б* *в* *г* *д*

Рисунок 1 – Охранные извещатели: а – извещатель охранный магнитоконтактный ИО-102-14 (СМК-14, геркон); б – датчик разбиения стекол ИО329-3 Арфа; в – извещатель охранный поверхностный вибрационный «Шорох-2» (ИО-313-5/1); г – четырехлучевой датчик-барьер инфракрасных лучей NR110QS; д – схема использования лучевых датчиков

окон охраняемого объекта. Принцип работы датчика основан на анализе спектра фиксируемого шума и его сравнении с записанными в память датчика эталонными звуковыми сигналами. Наиболее совершенные типы датчиков формируют сигнал тревоги при наличии двух факторов: удара по стеклу и звука бьющегося стекла.

Вибрационные датчики (рисунок 1, *в*) фиксируют наличие вибрации и ударов, возникающих при попытке разрушения защищаемого объекта. Принцип действия таких датчиков основан на использовании пьезоэлектрического эффекта или электромагнитной индукции для преобразования сигналов вибрации, подвергающихся разрушению, в анализируемые электрические сигналы.

Фотоэлектрические (лучевые) датчики инфракрасного (ИК) излучения (рисунок 1, *г*, *д*) используют для защиты коридоров, лестничных пролетов, ворот и входных дверей, а также в системе периметральной охраны объекта.

Действие датчиков основано на образовании барьера из формируемых специальными излучателями для защиты охраняемой зоны объекта системы модулированных инфракрасных лучей. При попадании нарушителя в зону действия барьера выдается сигнал тревоги.

Шлейфы систем охранной сигнализации представляют собой наклеиваемую на защищаемый элемент конструкции (стекло, дверь и т. п.) ленту из алюминиевой фольги, включенную в цепь охранной сигнализации. При разрушении конструкции вместе с лентой разрывается цепь охранной сигнализации и формируется сигнал тревоги.

Датчики движения позволяют распознать движение в охраняемой зоне по изменению уровня инфракрасного излучения при перемещении излучающего тепло объекта в зоне чувствительности датчика. По мере движения объекта ИК-излучение попадает на разные сегменты оптической системы, что приводит к формированию ряда импульсных сигналов, фиксируемых электронной системой датчика. Для защиты от ложных срабатываний в современных датчиках движения используется микропроцессорная обработка фиксируемых сигналов. В качестве примера датчиков движения представлены два типа инфракрасных пассивных извещателя семейства «Фотон» (рисунок 2).

Наряду с рассмотренными выше типами извещателей для охранной сигнализации также могут использоваться радиоволновые, ультразвуковые, микроволновые, емкостные и другие датчики, принцип действия которых основан на анализе отраженного от объекта сигнала или изменения поля и емкости охраняемого объекта. Однако означенные датчики получили гораздо меньшее распространение, так как весьма критичны к влиянию изменений окружающей среды, типу охраняемого объекта и наличию различных дестабилизирующих факторов.

От извещателей информация передается в другую обязательную структурную составляющую любой охранной системы, роль которой выполняют ПКП, а на небольших объектах – ПКН. Задачей ПКП является проверка исправной работы оборудования, сбор и анализ поступающей от извещателей информации, передача

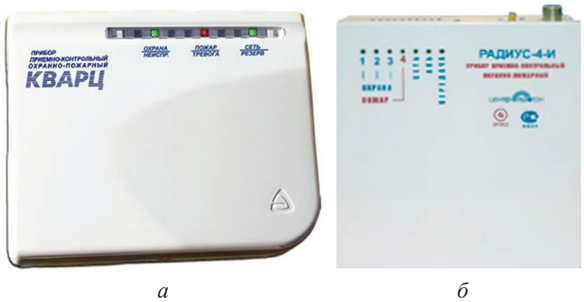
а *б*

Рисунок 2 – Датчики движения: а – извещатель инфракрасный пассивный «Фотон-9»; б – охранный оптико-электронный извещатель потолочной установки «Фотон-21»

сигнала тревоги на пульт охраны, управление световой и звуковой оповестительной и пожарной сигнализацией, а также другими техническими устройствами и системами обеспечения безопасности объекта. В ПКП обычно совмещаются функции охранной и пожарной сигнализации. Примером ПКП могут служить приемно-контрольные охранно-пожарные приборы «Кварц», «Радиус», «Сигнал», «Риф» и т. п.

Прибор «Кварц» (рисунок 3, *а*) является довольно простым ПКП и позволяет обеспечить питание и контроль одного шлейфа с включенными в него охранными или пожарными извещателями.

Прибор также управляет оповещателями и передает на пульт центрального наблюдения сигнал тревоги.



а *б*

Рисунок 3 – Приемно-контрольные приборы: а – «Кварц», б – «Радиус-4И»

Применяемые на железнодорожном транспорте приемно-контрольные охранно-пожарные приборы «Радиус-4И» (рисунок 3, *б*) и «Радиус-6И» могут использоваться как при централизованной, так и при автономной охране объектов от несанкционированного доступа и пожаров.

Прибор «Радиус-4И» обеспечивает возможность контроля четырех, а «Радиус-6И» шести шлейфов с включенными в них охранными и пожарными извещателями. При получении сигнала от любого из извещателей устройство по каналам связи передает сигнал тревоги,

а также сигнализирует о проникновении на объект или пожаре световыми и звуковыми сигналами. В обоих приборах предусмотрена индикация состояния шлейфов с использованием светодиодов. Диапазон рабочих температур прибора составляет от минус 10 до плюс 50°С, что обеспечивает возможность его широкого использования при охране различных объектов.

Для охраны распределенных по территории стационарных объектов используют системы радиоохраны с передачей извещения о проникновении на объект или пожаре по радиоканалу. Одним из примеров такой системы является «Риф Стринг-202». Данная система включает в себя размещаемую в центре охраны базовую станцию, пульт наблюдения и компьютер, а также размещаемые на объектах приемно-контрольные приборы с передающим устройством. Система позволяет контролировать с одного пульта до 600 устанавливаемых на объектах передающих устройств мощностью 10 мВт. В зависимости от местности система обеспечивает дальность связи от 25 до 50 и более километров, что достигается использованием сверхузкополосных каналов связи и помехоустойчивого кодирования. В системе применена цифровая фильтрация и одновременная, параллельная обработка всех принятых по различным каналам связи сигналов от контролируемых объектов. Передача каждого нового сообщения с объектного приемно-контрольного прибора осуществляется на новой частоте, случайным образом выбираемой из 1024 заранее запрограммированных частот связи. Для проверки исправности оборудования каждый объектный передатчик один раз в минуту передает на базовую станцию контрольные сигналы. Благодаря использованию лицензируемых частот и передатчиков малой мощности эксплуатация системы «Риф Стринг-202» не предусматривает получения разрешительных документов.

Для полного контроля больших территорий используют системы радиоохраны, также обеспечивающие сбор информации с распределенных по территории объекта датчиков с радиоизвещением. Датчики в данном случае располагаются по всей территории охраняемого объекта таким образом, чтобы расстояние между ними не превышало радиуса действия датчика, при котором обеспечивается обнаружение постороннего объекта и не образуются так называемые мертвые зоны. При попадании в зону действия датчика человека или постороннего предмета датчик фиксирует факт возникновения нештатной ситуации и посылает по радиоканалу на пульт управления системой сигнал тревоги.

Во многих случаях для обеспечения безопасности любой территории достаточно надежно контролировать только ее периметральные границы, чтобы полностью исключить факт несанкционированного проникновения на данную территорию. Такие системы получили название периметральных. Данные системы просто незаменимы при охране объектов с большими защищаемыми территориями, таких как аэродромы, базы, транспортные логистические терминалы, а также объектов с большой протяженностью, таких как железные и автомобильные дороги, трубопроводы и т. п.

Периметральные системы позволяют зафиксировать нарушение границы охраняемой территории и выдать сигнал тревоги намного раньше, чем нарушитель попадет на расположенные на данной территории особо важные объекты. Данные системы довольно часто конструктивно связаны с физическим ограждением охраняемого объекта, поэтому их работа напрямую зависит от физических характеристик ограждения, его параметров, наличия вибраций, используемого материала, а также от выбора места установки оборудования, качества выполнения монтажных работ и ряда других факторов.

Для надежной охраны объекта периметральные системы должны отвечать определенным требованиям, таким как:

- полный контроль всего периметра охраняемого объекта и отсутствие «мертвых зон»;
- высокая чувствительность обнаружения нарушителя;
- низкая вероятность ложных срабатываний;
- надежная работа в условиях электромагнитных помех от работающего оборудования и расположенных вблизи индустриальных объектов;
- надежная работа в различных климатических условиях.

В настоящее время для обеспечения безопасности объектов наиболее часто используются лучевые, радиоволновые и емкостные периметральные системы. Данные системы имеют высокую эффективность обнаружения и позволяют надежно защитить охраняемую территорию. Однако лучевые системы, например, инфракрасные барьеры, могут эффективно контролировать только прямолинейные участки периметра. Радиоволновые системы критичны к рельефу местности и плохо работают при наличии в охраняемой зоне деревьев или кустарников, что часто имеет место вблизи железных и автомобильных дорог. Емкостные системы требуют наличия физического ограждения объекта, так как фиксируют изменение электрического поля и емкости при приближении или прикосновении нарушителя к данному ограждению.

Для охраны протяженных объектов также могут использоваться проводно-радиоволновые системы, представляющие собой два расположенных по охраняемому периметру параллельных фидера. Один фидер выполняет роль приемной, а другой передающей антенны. При попадании в зону действия поля данных фидеров постороннего предмета происходит возмущение поля, сопровождающееся изменением параметров принимаемого сигнала, постоянно фиксируемых соответствующим оборудованием.

Рассматриваемые системы радиоохраны обычно интегрируются с системами видеонаблюдения, так как требуют идентификации нарушителя, пытающегося проникнуть на охраняемый объект.

Конечно только человек остается центром принятия решения в системе безопасности. Он следит за состоянием технических средств, получает тревожные сигналы,

управляет силами реагирования. Несмотря на четкий и понятный алгоритм действий, неукоснительное соблюдение требований по обеспечению транспортной безопасности на ОТИ и ТС железнодорожного транспорта, в нестандартной ситуации может сработать естественный человеческий фактор: утомляемость, усталость, растерянность и даже халатность. И тогда ценой ошибки или промедления в реагировании на угрозы может стать человеческая жизнь [4].

За последние годы немалое количество террористических актов было совершено на объектах транспорта или с использованием транспортных средств. Сухая статистка неумолима, о чем свидетельствуют отечественные и международные источники. Вот почему защита ОТИ и ТС от актов незаконного вмешательства, особенно совершенных умышленно, в форме террористических актов и диверсий, в последние годы вошла в число самых актуальных проблем во всем мире [5].

По итогам 2017 года на сети железных дорог России зарегистрировано 670 АНВ в деятельность железнодорожного транспорта. Среди них отмечены случаи с признаками террористического характера, в том числе 68 сообщений об угрозах совершения террористических актов. Также произошло 142 наложения посторонних предметов на рельсы, 79 случаев разоборудования железнодорожных путей и 269 случаев разукомплектования средств сигнализации, централизации и блокировки (СЦБ).

В течение 2017 года на объектах железнодорожного транспорта зафиксировано 5 случаев обнаружения взрывчатых веществ, 665 бесхозных подозрительных предметов. Изъято 20 единиц огнестрельного оружия, 1292 патрона различного калибра, 49 взрывоопасных предметов [6].

Между тем, опыт США, Канады и ряда европейских стран говорит о том, что забота об укреплении транспортной безопасности находится в центре внимания не только государства. Этой проблеме уделено огромное внимание и в ее разрешении активно участвуют общественные организации. Так, например, в США сотни частных компаний и фирм, под эгидой соответствующих общественных фондов, систематически выделяют в рамках своих годовых бюджетов огромные средства на исследования и разработки проблем обеспечения транспортной безопасности. Отмеченное выше свидетельствует в пользу того, что забота о кардинальном и неотложном повышении уровня безопасности на транспорте не может быть лишь уделом государства, равно как и не должны только государством изыскиваться необходимые для решения этой задачи финансовые, организационные и кадровые ресурсы. Кроме того, даже самая хорошо отлаженная система транспортной безопасности не может эффективно функционировать без широкой опоры на понимание и поддержку всех структур гражданского общества.

Подводя итог, хотелось бы напомнить, что одна из основных задач субъекта транспортной инфраструктуры или перевозчика – это безопасность человека. Безопасность – одно из важнейших условий развития личности, общества, государства. Это всегда требовало и требует от людей компетентности в мире опасностей и способах защиты от них.

Применение средств физической защиты в сочетании с организационными мероприятиями и действиями подразделений транспортной безопасности является важнейшим фактором, обеспечивающим обнаружение и противодействие попыткам совершения АНВ в отношении имущества, груза и физических лиц на объектах железнодорожного транспорта.

Эффективная система управления безопасностью – как хороший солдат: и в мирное, и в боевое время отвечает за точное и своевременное исполнение возложенных обязанностей и задач. При этом позволяет видеть ситуацию цельно и максимально снижает вероятность ошибки [7].

Библиографический список

1. Старовойтов А.С. Защищенность объектов транспорта необходимо поддерживать // Транспортная и технологическая безопасность. – 2017. – № 2. – С. 100-101.

2. Федеральный закон от 09.02.2007 г. № 16-ФЗ «О транспортной безопасности».

3. Федеральный закон от 03.02.2014 № 15-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам обеспечения транспортной безопасности».

4. Постановление правительства РФ от 26.04.2017 г. № 495 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств железнодорожного транспорта».

5. Natalia Kuzmina. Ensuring transport security in the transport infrastructure and means of transport railway transport facilities. / Natalia Kuzmina, Tatyana Odudenko // Proceedings of the XV International Academic Congress «Fundamental and Applied Studies in the Modern World» (United Kingdom, Oxford, 06–08 September 2016). Volume XV. «Oxford University Press», 2016. – 718 p.

6. www.roszeldor.ru.[Электронный ресурс] – Режим доступа http://doc.rzd.ru.

7. Процесс эволюции не остановить // Транспортная и технологическая безопасность. – 2017. – № 3. – С. 34.

Сведения об авторе

Наталья А. Кузьмина – кандидат педагогических наук, доцент кафедры «Организация перевозок и безопасность на транспорте» Дальневосточного государственного университета путей сообщения, Хабаровск, Россия, e-mail: kuzminaprepodavatel@mail.ru

Поступила: 10.01.2018

Gnedenko e-Forum
International Group on Reliability

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.

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: evgenya.patrikeeva@yandex.ru
ИНН 7709868505 КПП 770901001
р/с 40702810100430000017, ПАО «УРАЛСИБ БАНК» г. Москва
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

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

АО «НИИАС» – ведущее предприятие ОАО «РЖД» в области создания комплексов и систем обеспечения безопасности движения, управления движением, геоинформационного обеспечения, мониторинга состояния подвижного состава и инфраструктуры железных дорог

Цели:
- ❑ эффективность,
- ❑ безопасность
- ❑ надежность

перевозок

Основные направления деятельности

•Интеллектуальные системы управления
•Технологии управления перевозками и транспортного обслуживания
•Системы автоматики и телемеханики
•Центры автоматизированного управления
•Информационные системы
•Геоинформационные системы и спутниковые технологии
•Системы транспортной безопасности
•Системы управления инфраструктурой
•Системы управления топливно-энергетическими ресурсами
•Испытания, сертификация и экспертиза
•Информационная безопасность
•Нормативно-правовое обеспечение

www.vniias.ru