19. *Moussid M., Sayouti A., Medromi H.* Dynamic Modeling and Control of a HexaRotor using Linear and Nonlinear Methods, *International Journal of Applied Information Systems,* 2015, Vol. 9, Issue 5, pp. 9-17.
20. *Pshikhopov V., Medvedev, M, Gurenko B., Beresnev M.* Basic algorithms of adaptive position-path control systems for mobile units, *ICCAS 2015 - 2015 15th International Conference on Control, Automation and Systems,* 2015, pp. 54-59.
21. *Beloglazov D.A., Guzik V.F., Kosenko E.Yu., Krukhmalev V.A., Medvedev M.Yu., Pereverzev V.A., Pshikhopov V.Kh., P'yavchenko A.O., Saprykin R.V., Solov'ev V.V., Finaev V.I., Chernukhin Yu.V., Shapovalov I.O.* Intellektual'noe planirovanie traektoriy podvizhnykh ob"ektov v sredakh s prepyatstviyami [Intelligent trajectory planning of moving objects in environments with obstacles], ed. by V.Kh. Pshikhopova. Moscow: Fizmatlit, 2014, 300 s. ISBN 978-5-9221-1595-7.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Белоглазов Денис Александрович – Южный федеральный университет; e-mail: d.beloglazov@gmail.com; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 88634371689; кафедра систем автоматического управления; к.т.н.; доцент.

Соловьев Виктор Владимирович – e-mail: soloviev-tti@mail.ru; кафедра систем автоматического управления; ст. преподаватель.

Шаповалов Игорь Олегович – e-mail: shapovalovio@gmail.ru; кафедра систем автоматического управления; ассистент.

Beloglazov Denis Alexandrovich – Southern Federal University; e-mail: d.beloglazov@gmail.com; 44, Nekrasovsky, Taganrog, 347928, Russia; phone: 88634371689; the department of automatic control systems; cand. of eng. sc.; associate professor.

Soloviev Victor Vladimirovich – e-mail: soloviev-tti@mail.ru; the department of automatic control systems; senior lecturer.

Shapovalov Igor Olegovich − e-mail: shapovalovio@gmail.ru; the department of automatic control systems; assistant.

УДК 681.142 DOI 10.23683/2311-3103-2018-3-209-219

В.А. Балыбердин, А.М. Белевцев, О.А. Степанов

О ТЕСТИРОВАНИИ ПРОГРАММНЫХ СРЕДСТВ МОБИЛЬНЫХ АСУ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Рассматриваются некоторые вопросы организационно-технологического плана в отношении тестирования ПС с учетом специфики прикладной области мобильных АСУ специального назначения (СН). При этом внимание уделяется таким важным факторам надежности ПС как завершенность и отказоустойчивость, которые имеют существенное значение для эффективности функционирования АСУ СН. Факторы восстанавливаемости и готовности ПС не рассматриваются как не критичные в условиях специфики рассматриваемых АСУ. Анализируются вопросы организации статического и динамического тестирования ПС завершенности и отказоустойчивости ПС. Отмечается, что существующие методы организации и проведения динамического тестирования завершенности ПС требуют использования достаточно объемной статистики отказов ПС, которую не всегда возможно получить в практических ситуациях. В этом плане предлагается оригинальный подход для реализации процедуры динамического тестирования завершенности ПС, основанный на обработке статистики положительных исходов тестирования ПС и позволяющий значительно упростить практическую реализацию процедуры тестирования. В качестве проверяемых

характеристик ПС используются: – вероятность выхода на программную ошибку (программный дефект) при очередном испытании ПС; – среднее время до проявления очередного дефекта (ошибки) в ПС в процессе проведения тестирования (эксплуатации) ПС; – вероятность безошибочного функционирования ПС за заданный промежуток времени время; – число обнаруженных дефектов ПС до выхода на зачетную серию прогонов. Оценка отказоустойчивости ПС проводится с помощью представленных оценочных показателей отказоустойчивости ПС. При этом способность ПС поддерживать необходимый уровень пригодности при проявлении дефектов ПС или нарушении установленных интерфейсов, при сбоях и отказах ТС обеспечивается введением избыточности на различных уровнях рассмотрения прикладной системы. Различаются следующие основные виды избыточности: временная, информационная и программная. Оценочные показатели соотносятся с рассмотренными выше формами действий. Для определения оценочных показателей используются стратегии статического и динамического тестирования.

Программные средства; надежность; дефекты; тестирование; завершенность; испытания; отказоустойчивость; уровень пригодности; избыточность; оценочный показатель; полнота данных; актуальность данных.

V.A. Baliberdin, A.M. Belevtsev, O.A. Stepanov

ON MOBILE SPECIAL AUTOMATED SYSTEMS SOFTWARE RELIABILITY

Some organizational and technological problems for software reliability in the field of special automated systems are discussed. The attention is paid to the most important factors of software reliability such as maturity and fault tolerance. The availability and recoverability factors are not discussed due to be of no importance for the field under consideration. Some aspects of static and dynamic testing for software maturity and fault tolerance estimating are analyzed. It is pointed out that modern methods for software maturity dynamic testing need using large statistical material for software defaults calculating. Such the material is not available in practical situations. That is why the problem requires a new solution. In the article some original method for software maturity dynamic testing is presented. The method is based on treating positive statistics and makes the testing procedure rather simple. The characteristics under consideration are: – the default probability in a single software testing; – the default mean time during software testing; – the software faultless probability for the predetermined time period; – the number of defaults obtained before the pass testing is gained. The fault tolerance estimation is made by means of a number estimation indicators presented. The software abilities to perform its functions in spite of defaults is maintained by insertion of some kinds of excess. The following kinds of excess are examined: temporal, information and program. The fault tolerance estimation indexes are in concordance with the kinds of excess examined. The static and dynamic testing strategies are used for the fault tolerance estimation indexes to be determined.

Software; reliability; defaults; maturity; fault tolerance; testing; suitability level; excess; estimation indicator; data completeness; data relevancy.

Введение. В данной работе рассматриваются некоторые вопросы организационно-технологического плана в отношении тестирования ПС с учетом специфики прикладной области мобильных АСУ специального назначения (СН). При этом внимание уделяется таким важным факторам надежности ПС как завершенность и отказоустойчивость, которые имеют существенное значение для эффективности функционирования АСУ СН, как это показано в работах [2, 4, 9]. Факторы восстанавливаемости и готовности ПС не рассматриваются как не критичные в условиях специфики рассматриваемых АСУ.

Известно, что в основе проверки надежности разработанного ПС лежат процессы верификации и валидации ПС, основанные на реализации процедур установления соответствия ПС заданным требованиям и реальным потребностям прикладного использования ПС [2–4]. В основу этих процедур положены процессы тестирования ПС.

В широком смысле понятие тестирование ПС включает два аспекта: *статическое* тестирование и *динамическое* тестирование. Статическое тестирование базируется на анализе всей доступной документации ПС без исполнения ПС на ЭВМ, а динамическое тестирование – на проведении прогонов ПС (исполнения ПС) на реальных исходных данных.

Постановка задачи. Вопросы тестирования ПС в настоящее время недостаточно проработаны в методическом и организационном плане, что не обеспечивает уверенность Заказчика в надежном функционировании ПС в процессе эксплуатации. Особенно это относится к этапу приемо-сдаточных испытаний ПС, когда существующие подходы к оценке надежности ПС не могут быть использованы ввиду недостаточного объема статистических данных. Необходимы новые подходы и новые решения в этой области, что и изложено в последующем материале.

*Тестирование завершенности ПС***.** Целью испытаний является оценка фактора завершенности ПС (ГОСТ 28806-90, ГОСТ ИСО/МЭК 25010), характеризующего возможность возникновения отказов, обусловленных дефектами ПС (т.е. ошибками, внесёнными в ПС в процессе его создания или модификации).

При статическом тестировании ПС осуществляется анализ всей имеющейся документации на ПС. При этом целевая установка заключается в поиске различного рода несоответствий и дефектов (ошибок) ПС, допущенных на различных этапах создания ПС:

- при постановке проблемы, решаемой посредством ПС;
- при алгоритмизации решаемой проблемы;
- при реализации проблемы в рамках ПС;
- при отработке необходимой документации.

При этом главное внимание следует обращать на возможные дефекты ПС, допущенные на этапах постановки и алгоритмизации решаемой проблемы, поскольку эти дефекты труднее обнаружить при динамическом тестировании ПС. Для работы на этих этапах должны привлекаться наиболее квалифицированные специалисты.

Существует ряд методов организации и проведения динамического тестирования ПС [2, 3]. Однако эти методы требуют использования достаточно объемной статистики отказов ПС, которую не всегда возможно получить в практических ситуациях.

Предлагаемый нами метод проведения динамического тестирования ПС для оценки *завершенности* ПС достаточно прост в практической реализации и заключается в следующем.

Осуществляется совокупность прогонов испытуемых ПС. Каждый такой прогон проводится на собственном оригинальном наборе исходных данных. При выявлении ошибки в ПС, испытания прерываются, осуществляется устранение ошибки и процедура тестирования и отсчет количества успешных прогонов начинается заново. Испытания проводятся до тех пор, пока не появится серия из n подряд проведённых прогонов ПС, ни в одном из которых не возникло программной ошибки. Величина n определяется на основе определенных соотношений [2, 9]. При этом важно соблюсти условие, что каждый отдельный прогон ПС осуществляется на своем индивидуальном «фоне», т.е. на оригинальном наборе исходных данных.

Проверяемые характеристики:

- вероятность p – выхода на программную ошибку (программный дефект) при очередном испытании ПС;
- среднее время $T_{ср}$ до проявления очередного дефекта (ошибки) в ПС в процессе проведения тестирования (эксплуатации) ПС;

- вероятность безошибочного функционирования ПС за время T – P(T);
- число обнаруженных дефектов ПС – M до выхода на зачетную серию прогонов.

Вероятность p принято характеризовать двумя параметрами [1, 2]: значением q верхней границы доверительного интервала (нижняя граница есть 0) и доверительной вероятностью β, которая определяет вероятность нахождения истинного значения p в доверительном интервале [0,q].

Пусть событие B состоит в том, что за n прогонов не возникла ни одна программная ошибка (не произошло событие A). Допустим, что вероятность обнаружения ошибки есть p (эту величину можно считать постоянной в процессе серии прогонов ПС, так как ошибки не выявляются и, естественно, не устраняются). Очевидно, справедливо соотношение

$$P(B) = (1 - p)^n. \quad (1)$$

Полагая P(B)=1- β, получаем уравнение для q [1]:

$$1- \beta= (1 - q)^n. \quad (2)$$

Откуда

$$q=1-\sqrt[n]{1 - \beta}. \quad (3)$$

Таким образом, задаваясь значением доверительной вероятности и числом успешных испытаний, получаем оценку верхней границы доверительного интервала для оценки надежности (завершенности) ПС.

Больший интерес представляет также оценка необходимого числа испытаний при заданных β и q. Эта величина непосредственно определяется из формулы (2), а именно:

$$n=\frac{\ln (1-\beta)}{\ln (1-q)}. \quad (4)$$

Среднее время $T_{ср}$ до первого проявления программного дефекта определяется на основе:

- заданной доверительной вероятности – β для вероятности p;
- полученного объёма серии бездефектных прогонов ПС – n;
- заданной интенсивности практического использования рассматриваемого комплекса ПС – λ.

Последняя величина измеряется средним количеством обращений на использование ПС за единицу времени.

В качестве исходных данных задаются:

- T_0 – наименьшее требуемое значение среднего времени до появления первого дефекта;
- λ – интенсивность использования рассматриваемого ПС в работе;
- β – доверительная вероятность того, что собственно вероятность p обнаружения ошибки при очередном прогоне ПС лежит в доверительном интервале [0,q].

В качестве расчетной используется формула [2]:

$$T_0 = \frac{1}{(1-\sqrt[n]{1-\beta})\lambda}. \quad (5)$$

Из этой формулы определяется требуемое число подряд полученных бездефектных испытаний n:

$$n=\ln(1-\beta)/\ln(1-1/T_0\lambda). \quad (6)$$

Получение серии из n бездефектных прогонов свидетельствует о том, что при доверительной вероятности β среднее значение времени между проявлениями дефекта ПС не менее заданного T_0.

Таким образом, для того, чтобы убедиться, что $T_{ср} \geq T_0$, необходимо добиться получения серии из n бездефектных прогонов ПС, меняя каждый раз исходные данные.

Вероятность безошибочного функционирования ПС за время T – P(T) характеризует надежность (завершенность) ПС на заданном временном интервале T. При этом задается пороговое значение $P_0(T)$, так что P(T) не должно быть меньше $P_0(T)$. Задается также интенсивность использования испытуемого ПС – λ и доверительная вероятность β для доверительного интервала [0,q] для вероятности p выхода на программный дефект (программную ошибку) при очередном прогоне ПС. Последовательность расчетов заключается в следующем.

На основе заданных T и λ определяется среднее число прогонов ПС, осуществляемых за время T: N=Tλ.

Строится уравнение, определяющее зависимость $P_0(T)$ от q (верхней границы доверительного интервала для p):

$$P_0(T) = (1 - q)^N, \quad (7)$$

Рассчитывается значение q по формуле:

$$q = 1 - (P_0(T))^{1|N}. \quad (8)$$

Соотношение (8) фактически определяет требования к доверительному интервалу для неизвестной величины p – вероятности выхода на программный дефект (программную ошибку) при очередном прогоне ПС.

Теперь, зная верхнюю границу доверительного интервала q (нижняя граница есть 0) и задаваясь доверительной вероятностью β, определяем по формуле (4) n – необходимое число подряд идущих «успешных» прогонов ПС на различных исходных данных, необходимое для установления факта того, что вероятность безошибочного функционирования ПС за время T – $P(T) \geq P_0(T)$ [2], а именно:

$$n = \frac{\ln(1-\beta)}{\ln(\sqrt[T\lambda]{P_0(T)})}. \quad (9)$$

Таким образом, задавая P_0, T и λ, получаем значение n – количества подряд «успешных» прогонов ПС (без выхода на программный дефект), которое необходимо обеспечить за время T. А собственно факт получения n подряд «успешных» прогонов ПС свидетельствует о том, что вероятность безошибочного функционирования ПС за время T – $P(T) \geq P_0(T)$.

Количество попыток проведения испытаний до выхода на зачетную совокупность прогонов – M определяется путем фиксации числа таких попыток в процессе проведения испытаний ПС. Эта величина может характеризовать тот факт, насколько ответственно относится Разработчик ПС к предварительному тестированию представленного им Заказчику программного продукта.

Проведенный нами анализ имеющегося опыта разработки и испытаний ПС систем рассматриваемого класса показал, что наиболее приемлемым подходом при организации динамического тестирования ПС для проверки требований к завершенности РС на приемо-сдаточных испытаниях является тестирование на базе анализа спецификаций (стратегия «черного ящика») [2, 5]. Это объясняется следующими основными обстоятельствами.

Приемо-сдаточные испытания обычно проводятся под эгидой Заказчика, который хорошо ориентируется в спецификациях ПС и, в то же время, не имеет возможности и желания разобраться в «хитросплетениях» конкретной структурной реализации ПС. Поэтому стратегия «черного ящика» является для Заказчика наиболее предпочтительной.

При этом в качестве основной технологии тестирования целесообразно использовать технологию случайного тестирования с учетом некоторой ее модификации.

Иными словами, исходя из общих требований к ПС методика тестирования *завершенности* ПС, в своей основе, должна быть рассчитана на самый общий подход к тестированию ПС, когда исходят из применения технологии случайного тестирования (random testing) в соответствии со стандартом ISO/IEC 29119-4. Этот подход является универсальным и применим «на все случаи жизни». Соответственно и набор тестовых данных формируется случайным образом.

Основным недостатком такого подхода является неучет особенностей конкретики испытуемого ПС. Вследствие чего могут возникать ситуации, когда даже при достаточно объемном тестовом материале могут оказаться непроверенными некоторые важные частные аспекты функционирования ПС.

Выход видится в том, чтобы перейти на использование комбинированной технологии тестирования ПС, существо которой заключается в следующем.

За основу принимается технология случайного тестирования. Однако к сгенерированному на основе этой технологии набору тестовых данным (ТД) добавляется дополнительный набор ТД. В состав этого набора включаются ТД, специально ориентированные на учет специфики прикладного ПС. К этой специфике можно отнести:

- ТД для проверки поведения ПС на границах областей значений входной информации тестируемого ПС: собственно граница, чуть больше, чуть меньше;
- ТД для проверки правильности функционирования отдельных процедур обработки информации в тестируемом ПС и составляющих их алгоритмов.

Исходя из конкретики прикладного ПС могут быть отражены и другие аспекты специфики ПС.

Основные преимущества принятого подхода заключаются в том, что он позволяет учесть прикладную специфику тестируемого ПС и, в то же время, обеспечить достаточно детальную проверку возможных «неожиданностей» за счет реализации случайного процесса формирования основного набора тестовых данных.

Тестирование отказоустойчивости ПС. Целью испытаний является оценка фактора отказоустойчивости ПС (ГОСТ 28806-90, ГОСТ ИСО/МЕК 25010, 25012), характеризующего способность ПС поддерживать необходимый уровень пригодности при проявлении дефектов ПС, сбоев и отказов технических средств или нарушении установленных интерфейсов. При этом необходимый уровень пригодности включает в себя способность к безопасному функционированию при сбоях и отказах ТС и обнаружении дефектов ПС, к минимизации возможных потерь данных и исключению опасных действий при внезапном нарушении условий функционирования.

Способность ПС поддерживать необходимый уровень пригодности при проявлении дефектов ПС или нарушении установленных интерфейсов, при сбоях и отказах ТС обеспечивается введением избыточности на различных уровнях рассмотрения прикладной системы. Различаются следующие основные виды избыточности [2, 3]:

(1) Временная избыточность. Заключается в использовании некоторой части производительности ЭВМ для контроля исполнения программ и восстановления вычислительного процесса после отработки нештатных ситуаций.

(2) Информационная избыточность. Состоит в дублировании накопленных исходных и промежуточных данных и используется для повышения сохранности данных, в наибольшей степени влияющих на нормальное функционирование ПС и требующих значительного времени для восстановления.

(3) Программная избыточность. Используется для контроля и обеспечения достоверности наиболее важных результатов обработки информации, а также обеспечения работы системы при обнаружении дефекта ПС (программной ошибки). Заключается в двойной программной реализации наиболее важных процедур: по основному алгоритму и дублирующему (возможно, упрощенному).

Практическая реализация принципа избыточности может осуществляться в различных формах. Целесообразно выделить следующие основные формы действий в данном направлении, отражающие наиболее общие требования к ПС АСУВ:

♦ реализация контроля входных данных компонентов ПС, включая такие функции как анализ входных данных на возможные диапазоны изменения, непротиворечивость, достаточность (полноту) и др.;

♦ создание копий состояния рабочего поля программ в определённые моменты времени информационно-вычислительного процесса, обеспечивая тем самым возможность возврата к ранее пройденному этапу информационно-вычислительного процесса при возникновении неполадок;

♦ создание резервных реализаций наиболее проблемных компонентов ПС, выполненных по альтернативным алгоритмам.

Оценка отказоустойчивости ПС проводится с помощью оценочных показателей отказоустойчивости ПС. Оценочные показатели соотносятся с рассмотренными выше формами действий.

Оценочные показатели для проверки реализации контроля данных ПС (компонентов ПС), а также для проверки работоспособности ПС при сбоях и отказах технических средств и ОС, нарушениях интерфейса и при обнаружении дефектов ПС представлены в табл. 1. Эти показатели получены на основе рекомендаций ГОСТ 28195-89 и с учетом имеющегося опыта оценки надежности ПС систем рассматриваемого типа.

Таблица 1

Оценочные показатели для проверки отказоустойчивости ПС

Код показателя	Наименование показателя	Оценка показателя
Раздел 1. Проверка реализации контроля данных		
П101	Наличие контроля допустимых значений данных	0-1
П102	Наличие контроля полноты данных	0-1
П103	Наличие контроля непротиворечивости (соответствия) данных	0-1
П104	Наличие контроля актуальности данных	0-1
П105	Наличие средств диагностики и устранения ошибочных значений данных	0-1
Раздел 2. Проверка сохранения работоспособности ПС и информации при сбоях и отказах технических средств и ОС		
П201	Наличие возможности восстановления результатов работы при отказах оборудования	0/1
П202	Наличие средств восстановления процесса в случае сбоя операционной системы	0/1
П203	Наличие средств диагностики сбоев и отказов ТС и ОС	0/1

Окончание табл. 1

Код показателя	Наименование показателя	Оценка показателя
Раздел 3. Проверка работоспособности ПС при обнаружении дефектов (ошибок) в компонентах ПС		
П301	Наличие средств обработки ошибочных ситуаций	0/1
П302	Полнота обработки ошибочных ситуаций	0-1
П303	Наличие резервных копий компонентов ПС	0/1
П304	Наличие средств диагностики и устранения ошибочных ситуаций	0/1
Раздел4. Обобщенная оценка отказоустойчивости ПС		
П401	Доля успешно отработанных ситуаций отказа	A/B

Оценка реализации контроля входных данных ПС (показатели П101 – П105) осуществляется экспертным методом на основе анализа представленной документации (статическое тестирование). Каждому показателю присваивается оценка в диапазоне 0–1 в зависимости от степени реализации соответствующего вида контроля. При необходимости производится уточнение оценки экспериментальным методом (динамическое тестирование).

Оценка сохранения работоспособности ПС при сбоях и отказах технических средств и ОС (показатели П201 – П203) осуществляется экспериментальным методом с имитацией соответствующих ситуаций для ТС и ОС. Каждому показателю присваивается значение 1, при положительном исходе испытаний (наличие соответствующих средств) и 0 – в противном случае.

Оценка работоспособности ПС при обнаружении дефектов (ошибок) в компонентах ПС (показатели П301 – П304) осуществляется экспериментальным методом с имитацией соответствующих ситуаций наличия ошибки в ПС. Каждому показателю присваивается значение 1 при положительном исходе испытаний (наличие соответствующих средств) и 0 – в противном случае. Выбор ошибочных ситуаций осуществляется решением председателя комиссии по испытаниям ПС.

Интегральная оценка отказоустойчивости ПС. В качестве интегральной оценки отказоустойчивости ПС целесообразно использовать показатель, рекомендуемый международными стандартами, определяемый как «Доля ситуаций отказа, успешно отработанных средствами отказоустойчивости». Обозначим его как П401. Этот показатель вычисляется экспериментальным путем и выражается следующим образом:

$$П401=A/B.$$

Здесь A – количество успешно отработанных отказов;

B – количество обнаруженных при тестировании ситуаций отказа.

Значения величин A и B определяются экспериментальным путем на основе общего количества проведённых прогонов ПС с учётом реально обнаруженных и имитируемых ситуаций отказов ПС.

Выводы:

1. В работе предложен принципиально новый подход к организации тестирования завершенности ПС на этапе приемо-сдаточных испытаний. Представлены, классифицированы и обоснованы оценочные показатели для тестирования отказоустойчивости ПС АСУ рассматриваемого типа.

2. В отличие от существующих моделей оценки завершенности ПС, где в основу анализа положена статистика проявления дефектов при тестировании ПС, предлагаемый подход основывается на анализе статистики положительных исходов. В части тестирования отказоустойчивости ПС представленная система оценочных показателей

3. Основные преимущества предлагаемого подхода к организации тестирования завершенности ПС заключаются в простоте его практической реализации, что позволяет его использовать в ситуациях, когда существующие методы неприменимы из-за невозможности получения необходимой статистики. В части отказоустойчивости ПС, представленная система оценочных показателей позволяет достаточно компактно отобразить все основные требования к отказоустойчивости ПС рассматриваемых АСУ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Вентцель Е.С.* Теория вероятностей. – М.: Наука, 1964. – 576 с.
2. *Балыбердин В.А., Степанов О.А.* Методы оценки и обеспечения надёжности программных средств АСУВ. – М.: 3 ЦНИИ МО РФ, 2014. – 136 с.
3. *Полонников Р.И., Никандров А.В.* Методы оценки показателей надежности программного обеспечения. – СПб.: Политехника, 1992. – 78 с.
4. *Балыбердин В.А., Белевцев А.М., Степанов О.А.* Вопросы оценки и обеспечения надёжности программных средств АСУ специального назначения // Известия ЮФУ. Технические науки. – 2014. – № 5 (154).– С. 115-120.
5. *Балыбердин В.А., Белевцев А.М., Степанов О.А.* Анализ основных процессов обеспечения надежности программных средств АСУ специального назначения // Известия ЮФУ. Технические науки. – 2015. – № 3 (164). – С. 62-70.
6. *Балыбердин В.А., Степанов О.А., Шумило Д.А.* Об оценке надежности программных средств АСУ в условиях приемосдаточных испытаний // Избранные научные труды. XVI Международная научно-практическая конференция «Управление качеством». – М.: МАИ, 2017. – С. 69-73.
7. *Балыбердин В.А., Маркелов Е.Б., Степанов О.А., Морозов О.С., Шумило Д.А.* Некоторые проблемные вопросы оценки и обеспечения надежности программных средств АСУВ // Известия Российской академии ракетных и артиллерийских наук. – 2016. – № 3. – С. 23-28.
8. Systems and Software Engineering – Software Testing – Part 1-6. ISO/IEC 29119 2012.
9. *Балыбердин В.А., Дружинин М.А., Панов В.В., Степанов О.А.* Актуальные вопросы автоматизации управления войсками и оружием. – М.: Минобороны Российской Федерации. ФГБУ «3 ЦНИИ», 2017. – 144 с.
10. *Балыбердин В.А., Степанов О.А. Шумило Д.А.* К оценке надёжности программных средств АСУВ. Актуальные проблемы защиты и безопасности // Труды 14-й Всероссийской научно-практической конференции. Вооружение и военная техника. Т. 1. – СПб., 2011. – С. 603-608.
11. *Балыбердин В.А., Белевцев А.М., Степанов О.А.* Некоторые проблемные вопросы управления надёжностью программных средств // Тезисы доклада на Всероссийской конференции по управлению качеством. – М.: МАТИ, 2014. – С. 136-140.
12. *Балыбердин В.А., Белевцев А.М., Степанов О.А.* Анализ и общая оценка основных процессов управления надёжностью программных средств специализированных АСУ // Избранные научные труды. 14-я международная конференция «Управление качеством». – М.: МАТИ, 2015. – С. 77-81.
13. *Балыбердин В.А., Белевцев А.М., Степанов О.А.* Оптимизация информационных процессов в автоматизированных системах с распределенной обработкой данных. – М.: РИА. Секция «Военно-технические проблемы», 2002. – 280 с.
14. *Балыбердин В.А., Степанов О.А., Иванов В.В.* Методы, модели и алгоритмы рационального построения информационных технологий в АСУ. – М.: 3 ЦНИИ МО РФ, 2012. – 264 с.
15. *Балыбердин В.А., Белевцев А.М., Бендерский Г.П.* Прикладные методы оценки и выбора решений в стратегических задачах инновационного менеджмента. – М.: Дашков, 2013. – 240 с.

16. *Василенко Н.В., Макаров В.А.* Модели оценки надёжности программного обеспечения // Вестник Новгородского государственного университета. – 2004. – № 28. – С. 126-132.
17. *Липаев В.В.* Надёжность и функциональная безопасность комплексов программ реального времени. – М.: ИСП РАН, 2013. – 176 с.
18. *Липаев В.В.* Функциональная безопасность программных средств. – М.: СИНТЕГ, 2004. – 348 с.
19. *Степанченко И.В.* Методы тестирования программного обеспечения. – Волгоград: РПК Политехник, 2006. – 76 с.
20. *Балыбердин В.А., Пенкин О.М., Полунин А.И.* Проблемные вопросы создания и внедрения новых информационных технологий в автоматизированных системах военного назначения. – М.: Секция военно-технических проблем Российской инженерной академии, 2001. – 144 с.

REFERENCES

1. *Venttsel' E.S.* Teoriya veroyatnostey [Probability theory]. Moscow: Nauka, 1964, 576 p.
2. *Balyberdin V.A., Stepanov O.A.* Metody otsenki i obespecheniya nadezhnosti programmnykh sredstv ASUV [Methods of evaluation and ensuring the reliability of software tools asuv]. Moscow: 3 TsNII MO RF, 2014, 136 p.
3. *Polonnikov R.I., Nikandrov A.V.* Metody otsenki pokazateley nadezhnosti programmnogo obespecheniya [Methods of estimation of indicators of software reliability]. Saint Petersburg: Politekhnika, 1992, 78 p.
4. *Balyberdin V.A., Belevtsev A.M., Stepanov O.A.* Voprosy otsenki i obespecheniya nadezhnosti programmnykh sredstv ASU spetsial'nogo naznacheniya [Issues of evaluation and ensuring the reliability of special purpose ACS software], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 5 (154), pp 115-120.
5. *Balyberdin V.A., Belevtsev A.M., Stepanov O.A.* Analiz osnovnykh protsessov obespecheniya nadezhnosti programmnykh sredstv ASU spetsial'nogo naznacheniya [Analysis of the main processes to ensure the reliability of special-purpose ACS software], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 3 (164), pp. 62-70.
6. *Balyberdin V.A., Stepanov O.A., Shumilo D.A.* Ob otsenke nadezhnosti programmnykh sredstv ASU v usloviyakh priemosdatochnykh ispytaniy [On the evaluation of the reliability of the software ACS in the conditions of acceptance tests], *Izbrannye nauchnye trudy. XVI Mezhdunarodnaya nauchno-prakticheskaya konferentsiya «Upravlenie kachestvom»* [Selected scientific papers. XVI international scientific and practical conference "quality Management"]. Moscow: MAI, 2017, pp. 69-73.
7. *Balyberdin V.A., Markelov E.B., Stepanov O.A., Morozov O.S., Shumilo D.A.* Nekotorye problemnye voprosy otsenki i obespecheniya nadezhnosti programmnykh sredstv ASUV [Some problematic issues of evaluation and reliability of software asuv], Izvestiya *Rossiyskoy akademii raketnykh i artilleriyskikh nauk* [News of the Russian Academy of rocket and artillery Sciences], 2016, No. 3, pp. 23-28.
8. Systems and Software Engineering – Software Testing – Part 1-6. ISO/IEC 29119 2012.
9. *Balyberdin V.A., Druzhinin M.A., Panov V.V., Stepanov O.A.* Aktual'nye voprosy avtomatizatsii upravleniya voyskami i oruzhiem [Topical issues of automation of control of troops and weapons]. Moscow: Minoborony Rossiyskoy Federatsii. FGBU «3 TsNII», 2017, 144 p.
10. *Balyberdin V.A., Stepanov O.A. Shumilo D.A.* K otsenke nadezhnosti programmnykh sredstv ASUV. Aktual'nye problemy zashchity i bezopasnosti [To assess the reliability of the software asuv. Actual problems of protection and safety], *Trudy 14-y Vserossiyskoy nauchno-prakticheskoy konferentsii. Vooruzhenie i voennaya tekhnika* [Proceedings of the 14th all-Russian scientific-practical conference. Weapons and military equipment]. Vol. 1. Saint Petersburg, 2011, pp. 603-608.
11. *Balyberdin V.A., Belevtsev A.M., Stepanov O.A.* Nekotorye problemnye voprosy upravleniya nadezhnost'yu programmnykh sredstv [Some problematic issues of software reliability management], *Tezisy doklada na Vserossiyskoy konferentsii po upravleniyu kachestvom* [Theses of the report at the all-Russian conference on quality management]. Moscow: MATI, 2014, pp. 136-140.

12. *Balyberdin V.A., Belevtsev A.M., Stepanov O.A.* Analiz i obshchaya otsenka osnovnykh protsessov upravleniya nadezhnost'yu programmnykh sredstv spetsializirovannykh ASU [Analysis and General evaluation of the main processes of reliability management of specialized software ACS], *Izbrannye nauchnye trudy. 14-ya mezhdunarodnaya konferentsiya «Upravlenie kachestvom»* [Selected scientific papers. 14th international conference "quality Management"]. Moscow: MATI, 2015, pp. 77-81.
13. *Balyberdin V.A., Belevtsev A.M., Stepanov O.A.* Optimizatsiya informatsionnykh protsessov v avtomatizirovannykh sistemakh s raspredelennoy obrabotkoy dannykh [Optimization of information processes in automated systems with distributed data processing]. Moscow: RIA. Sektsiya «Voenno-tekhnicheskie problemy», 2002, 280 p.
14. *Balyberdin V.A., Stepanov O.A., Ivanov V.V.* Metody, modeli i algoritmy ratsional'nogo postroeniya informatsionnykh tekhnologiy v ASU [Methods, models and algorithms of rational construction of information technologies in ACS]. Moscow: 3 TsNII MO RF, 2012, 264 p.
15. *Balyberdin V.A., Belevtsev A.M., Benderskiy G.P.* Prikladnye metody otsenki i vybora resheniy v strategicheskikh zadachakh innovatsionnogo menedzhmenta [Applied methods of evaluation and selection of solutions in strategic tasks of innovation management]. Moscow: Dashkov, 2013, 240 p.
16. *Vasilenko N.V., Makarov V.A.* Modeli otsenki nadezhnosti programmnogo obespecheniya [Models of software reliability evaluation], *Vestnik Novgorodskogo gosudarstvennogo universiteta* [Bulletin of Novgorod state University], 2004, No. 28, pp. 126-132.
17. *Lipaev V.V.* Nadezhnost' i funktsional'naya bezopasnost' kompleksov programm real'nogo vremeni [Reliability and functional safety of real-time software systems]. Moscow: ISP RAN, 2013, 176 p.
18. *Lipaev V.V.* Funktsional'naya bezopasnost' programmnykh sredstv [Functional security of software]. Moscow: SINTEG, 2004, 348 p.
19. *Stepanchenko I.V.* Metody testirovaniya programmnogo obespecheniya [Software testing methods]. Volgograd: RPK Politekhnik, 2006, 76 p.
20. *Balyberdin V.A., Penkin O.M., Polunin A.I.* Problemnye voprosy sozdaniya i vnedreniya novykh informatsionnykh tekhnologiy v avtomatizirovannykh sistemakh voennogo naznacheniya [Problematic issues of creation and implementation of new information technologies in automated systems of military purpose]. Moscow: Sektsiya voenno-tekhnicheskikh problem Rossiyskoy inzhenernoy akademii, 2001, 144 p.

Статью рекомендовал к опубликованию д.т.н., профессор Р.П. Быстров.

Балыбердин Валерий Алексеевич – 3 Центральный НИИ Министерства Обороны РФ; e-mail: baliberdinv@yandex.ru; Москва, Погонный, 10; д.т.н.; профессор; в.н.с.

Степанов Олег Алексеевич – e-mail: stepoleg@post.ru; к.т.н.; доцент.

Белевцев Андрей Михайлович – Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «МАИ – Российский государственный университет»; e-mail: ambelevtsev@yandex.ru; Москва, Оршанская, 3; д.т.н.; профессор.

Baliberdin Valery Alekseevitch – 3 Central Defence Institute; e-mail:baliberdinv@yandex.ru; Moscow, Pogonny, 10; dr. of eng. sc.; professor; science worker.

Stepanov Oleg Alekseevich – e-mail:stepoleg@post.ru; dr. of eng. sc.; associate professor.

Belevtsev Andrey Michailovitch – MAI-university; e-mail: ambelevtsev@yandex.ru; Moscow, Orshanskaiy, 3; dr. of eng. sc.; professor.