УДК 681.324

ОПТИМИЗАЦИЯ ИНТЕРВАЛОВ ПРОВЕРКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ

В.А. Богатырев[a], А.В. Богатырев[a], С.В. Богатырев[b]

[a] Университет ИТМО, 197101, Санкт-Петербург, Россия, Vladimir.bogatyrev@gmail.com
[b] Санкт-Петербургский государственный университет аэрокосмического приборостроения, 190000, Санкт-Петербург, Россия

Аннотация. Предложена марковская модель защищенных информационных систем, функционирующих в условиях деструктивных воздействий, последствия которых обнаруживаются оперативным и тестовым контролем. Предполагается, что оперативный контроль, в отличие от тестового, характеризуется ограниченной полнотой контроля, но не требует остановки вычислительного процесса. Целью исследований является построение моделей, позволяющих оптимизировать интервалы инициализации тестового контроля по критерию максимизации вероятности нахождения системы в состоянии готовности к безопасному выполнению функциональных запросов и минимизации опасных состояний системы с учетом неопределенности и вариантности интенсивности деструктивных воздействий. Рассмотрены варианты задачи оптимизации интервалов тестирования в зависимости от интенсивности деструктивных воздействий по критерию достижения максимума готовности системы к безопасному выполнению запросов. Оптимизация проведена без адаптации и с адаптацией к изменениям реальной интенсивности деструктивных воздействий.
Показана эффективность адаптивного изменения периодов тестирования в зависимости от наблюдаемой активности деструктивных воздействий. Решение задачи оптимизации проведено с использованием встроенных средств системы компьютерной математики Mathcad 15, включая средства символьной математики решения систем алгебраических уравнений. Предложенные модели и методы определения оптимальных интервалов тестирования могут найти применение при системотехническом проектировании компьютерных систем и сетей критического применения, работающих в условиях дестабилизирующих воздействий при повышенных требованиях к их безопасности.

Ключевые слова: марковская модель, контроль, опасные состояния, деструктивные воздействия, оптимизация.
Благодарности. Работа выполнена в рамках НИР «Методы и модели обеспечения интегрированной безопасности и устойчивости функционирования компьютерных систем».

INTERVALS OPTIMIZATION OF SYSTEMS INFORMATION SECURITY INSPECTION

V.A. Bogatyrev[a], A.V. Bogatyrev[a], S.V. Bogatyrev[b]

[a] ITMO University, 197101, Saint Petersburg, Russia, Vladimir.bogatyrev@gmail.com
[b] Saint Petersburg State University of Aerospace Instrumentation, 190000, Saint Petersburg, Russia, Vladimir.bogatyrev@gmail.com

Abstract. A Markov model is suggested for secure information systems, functioning under conditions of destructive impacts, which aftereffects are found by on-line and test control. It is assumed that on-line control, in contrast to the test one, is characterized by the limited control completeness, but does not require the stopping of computational process. The aim of research is to create models that optimize intervals of test control initialization by the criterion of probability maximization for system stay in the ready state to secure fulfillment of the functional requests and minimization of the dangerous system states in view of the uncertainty and intensity variance of the destructive impacts. Variants of testing intervals optimization are considered depending on the intensity of destructive impacts by the criterion of the maximum system availability for the safe execution of queries. Optimization is carried out with and without adaptation to the actual intensity change of destructive impacts.
The efficiency of adaptive change for testing periods is shown depending on the observed activity of destructive impacts. The solution of optimization problem is obtained by built-in tools of computer mathematics Mathcad 15, including symbolic mathematics for solution of systems of algebraic equations. The proposed models and methods of determining the optimal testing intervals can find their application in the system design of computer systems and networks of critical applications, working under conditions of destabilizing actions with the increased requirements for their safety.

Keywords: Markov model, control, dangerous states, destructive impacts, optimization.
Acknowledgements. The work is done within the framework of S&R “Methods and Models for Integrated Security and Operation Stability of Computer Systems”.

Введение

В настоящее время большое внимание уделяется развитию методов системотехнического проектирования компьютерных систем и сетей с высокой надежностью, отказоустойчивостью и производительностью при минимизации затрат на их реализацию и эксплуатацию [1–7].

Достижение высокой надежности [8–25], функциональной и информационной безопасности систем хранения и обработки данных требует использования комплекса средств оперативного и тестового контроля, направленных на обнаружение и минимизацию последствий деструктивных воздействий как злонамеренного, так и случайного характера. Оперативный контроль [1] позволяет быстро обнаружить последствия деструктивных воздействий, но замедляет вычислительный процесс, и достижимая им полнота контроля, как правило, ограничена, в результате чего возможно нарушение безопасности системы (переход в опасные состояния необнаружения последствий деструктивных воздействий). Для обнаружения опасных состояний в системе может дополнительно проводиться периодический тестовый контроль.

При организации тестового контроля возникает задача определения оптимальных интервалов между тестированием, так как уменьшение этого интервала позволяет снизить вероятности опасных состояний, но приводит к потере реальной производительности и к возрастанию среднего времени пребывания запросов в системе, что отрицательно сказывается на ее эффективности, особенно при работе в реальном времени.

В теории надежности известны марковские модели, учитывающие влияние оперативного и тестового контроля на готовность системы и позволяющие оптимизировать периодичность тестового контроля [1, 7–9, 20] с целью максимизации коэффициента готовности системы. Использование известных надежностных моделей для исследования защищенных информационных систем, подверженных злонамеренным деструктивным воздействиям, затруднено тем, что их интенсивность (в отличие от отказов), как правило, характеризуется вариантностью, переменностью и неопределенностью последовательности и частоты смены вариантов.

Таким образом, для защищенных информационных систем с целью повышения их готовности к безопасному обслуживанию запросов возникает потребность определения оптимальных интервалов тестирования в зависимости от вариантности и изменяемой интенсивности деструктивных воздействий. Адаптация периодов тестирования к изменениям интенсивности воздействий, с одной стороны, позволяет увеличить готовность системы при снижении вероятности ее опасных состояний, но, с другой, увеличивает простои системы, вызываемые необходимостью обнаружения изменений интенсивности деструктивных воздействий, что обусловливает целесообразность постановки и решения задачи оптимизации процесса тестирования.

Модель защищенной системы

Для построения марковской модели защищенной информационной системы интервалы между деструктивными воздействиями, инициализацией тестирования, а также время тестирования будем считать распределенными по показательному закону. Граф состояний и переходов моделируемого процесса на рис. 1 соответствует идеальному случаю обнаружения тестовым контролем всех опасных состояний системы в предположении постоянной интенсивности нарушений.

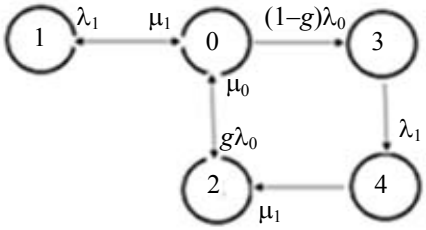

Рис. 1. Граф состояний и переходов системы с контролем злонамеренных воздействий: 0 – готовность системы к безопасному выполнению функциональных запросов; 1 – тестирование при отсутствии нарушений (последствий деструктивных воздействий); 2 – обнаружение последствий деструктивных воздействий и восстановление безопасного состояния; 3 – опасное состояние функционирования при необнаруженных последствиях деструктивных воздействиях; 4 – тестирование при наличии нарушений

На рис. 1 введены обозначения: λ_0 – интенсивность потока деструктивных воздействий (величина, обратная среднему времени между деструктивными воздействиями); λ_1 – интенсивность инициализации тестового контроля (величина, обратная среднему времени между тестированием); g – полнота оперативного контроля (вероятность обнаружения нарушений оперативным контролем); μ_1 – интенсивность тестирования (величина, обратная среднему времени тестирования); μ_0 – интенсивность восстановления безопасного состояния.

Представленный на рис. 1 граф состояний и переходов позволяет составить системы алгебраических или дифференциальных уравнений, из которых находятся вероятности всех состояний $P_0 - P_4$ в стационарном или нестационарном режимах [1].

Система алгебраических уравнений Колмогорова для графа на рис. 1 имеет следующий вид:

$$\lambda_1 P_0 - \mu_1 P_1 = 0,$$
$$\lambda_1 P_3 - \mu_1 P_4 = 0,$$
$$\mu_1 P_4 + g\lambda_0 P_0 - \mu_0 P_2 = 0,$$
$$(1-g)\lambda_0 P_0 - \lambda_1 P_3 = 0,$$
$$\sum_{i=0}^{4} P_i = 1.$$

Решение получаем с использованием встроенных средств символьной математики Mathcad 15:

$$P_0 = \lambda_1\mu_0\mu_1 W,\ P_1 = \lambda_1^2\mu_0 W,\ P_2 = \mu_1\lambda_0\lambda_1 W,\ P_3 = \lambda_0\mu_0\mu_1(1-g)W,\ P_4 = \lambda_0\lambda_1\mu_0(1-g)W,$$

где $W = \left(\lambda_1^2\mu_0 + \mu_1\lambda_0\lambda_1 + \mu_0\lambda_0\lambda_1 + \lambda_1\mu_0\mu_1 + \lambda_0\mu_0\mu_1 - g\lambda_0\mu_0\left(\lambda_1 + \mu_1\right)\right)^{-1}$.

Результаты расчета вероятностей состояний системы в зависимости от интенсивности инициализации тестового контроля λ_1 при $\lambda_0 = 0{,}1$ 1/ч, $\mu_1 = 10$ 1/ч, $\mu_0 = 2$ 1/ч и $g = 0{,}5$ представлены на рис. 2. Кривая 1 соответствует вероятности готовности системы к безопасному выполнению запросов, кривая 2 – вероятности простоя системы при ее тестировании или восстановлении, кривая 3 – вероятности простоя системы при ее тестировании в безопасном состоянии, кривая 4 – вероятности нахождения системы в опасном состоянии. Кривая 5 соответствует вероятности опасных состояний по уточненной шкале правой оси ординат. Представленные зависимости показывают возможность существования оптимального интервала между инициализацией процедуры тестирования, при котором достигается максимум вероятности нахождения системы в состоянии готовности к безопасному выполнению функциональных запросов, что подтверждает целесообразность постановки и решения задачи оптимизации интервалов тестирования.

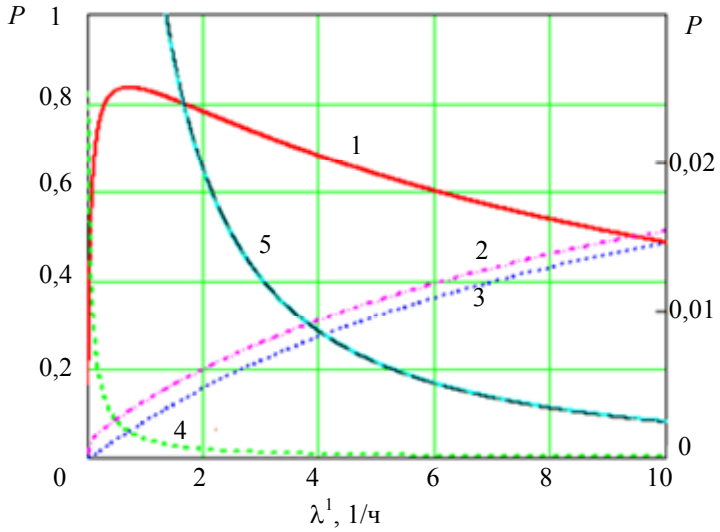

Рис. 2. Вероятности состояний системы в зависимости от интенсивности инициализации контроля: кривые 1–4 соответствуют вероятностям состояний P_0, P_1+P_2+P_4, P_1, P_3 соответственно; кривая 5 представляет вероятность P_3 по уточненной шкале правой оси ординат

Оптимизация интервалов тестирования по критерию максимизации готовности системы к безопасному выполнению запросов

Особенность модели контроля для исследования систем, подверженных злонамеренным деструктивным воздействиям, заключается в необходимости учета неопределенности интенсивности этих воздействий и их изменений во времени. При оптимизации интервалов тестирования будем предполагать считать заданными вектор вариантов возможных интенсивностей (q_i) и вектор вероятностей этих вариантов (r_i), имеющие размерность $n\times1$.

При неопределенности потока деструктивных воздействий рассмотрим различные варианты постановки задачи оптимизации интервалов тестирования, обеспечивающих максимум вероятности нахождения системы в состоянии готовности к безопасному выполнению функций, обозначаемые как В1–В3.

При варианте В1 определяется значение интервалов тестирования $1/\lambda_1$ обеспечивающее максимум вероятности состояния готовности к безопасному выполнению запросов P_0 по критерию

$$\max_{\lambda_1}\left(\lambda_1\mu_0\mu_1 / \left(\lambda_1^2\mu_0 + \mu_1\lambda_0\lambda_1 + \mu_0\lambda_0\lambda_1 + \lambda_1\mu_0\mu_1 + \lambda\mu_0\mu_1 - g\lambda_0\mu_0\left(\lambda_1 + \mu_1\right)\right)\right)$$

при средней интенсивности воздействий $\lambda_0 = \sum_{i=0}^{n-1} q_i r_i$.

При варианте В2 определяется значение интервалов тестирования $1/\lambda_1$ (интенсивности инициализации тестирования λ_1), обеспечивающее максимум математического ожидания вероятности состояния готовности к безопасному выполнению запросов с учетом всех возможных интенсивностей воздействий q_i (i=0,1,…,n–1). В этом случае критерий оптимальности имеет вид

$$\max_{\lambda_1}\sum_{i=0}^{n-1} r_i\left(\lambda_1\mu_0\mu_1 / \left(\lambda_1^2\mu_0 + \mu_1 q_i\lambda_1 + \mu_0 q\lambda_1 + \lambda_1\mu_0\mu_1 + q_i\mu_0\mu_1 - g q_i\mu_0\left(\lambda_1 + \mu_1\right)\right)\right),$$

где q_i – i-й вариант возможной интенсивности деструктивных воздействий, вероятность которой r_i.

При варианте В3 для каждой возможной интенсивности деструктивных воздействий определяется вектор значений интенсивности инициализации тестирования (a_i), обеспечивающий максимум математического ожидания готовности системы к безопасному выполнению запросов. При этом критерий оптимальности имеет вид

$$\max_a \sum_{i=0}^{n-1} r_i \left(a_i \mu_0 \mu_1 / \left(a_i^2 \mu_0 + \mu_1 q_i a_i + \mu_0 q_i a_i + a_i \mu_0 \mu_1 + q_i \mu_0 \mu_1 - g q_i \mu_0 \left(a_i + \mu_1 \right) \right) \right).$$

Вариант В3 предполагает предварительное формирование (на основе оптимизации) вектора интервалов тестирования в зависимости от варианта интенсивности воздействий. Адаптивный переход к выбираемому значению интервала тестирования происходит в результате измерений текущей активности (интенсивности) деструктивных воздействий и идентификации соответствующего варианта градации активности q_i .

Возможна модификация адаптивного варианта назначения интервалов тестирования, когда градации активности не вводятся, а осуществляются измерения активности воздействий в реальном времени, и при обнаружении их изменений решается расчетная задача оптимизации интервалов тестирования. Следует заметить, что реализация рассмотренных вариантов адаптивного задания интервалов тестирования требует дополнительных временных издержек, а поэтому его применение требует обоснования.

Оптимизация интервалов тестирования по критерию минимизации опасных состояний при безопасном выполнении запросов

Определим интервалы тестирования, обеспечивающие минимум вероятности нахождения системы в опасном состоянии необнаруженных последствий деструктивных воздействий в условиях неопределенности и вариантности их интенсивностей. При оптимизации выделим случаи, соответствующие ранее рассмотренным вариантам В1–В3 критериев оптимизации:

$$\min_{\lambda_1} \left(\lambda_0 \mu_0 \mu_1 (1-g) / \left(\lambda_1^2 \mu_0 + \mu_1 \lambda_0 \lambda_1 + \mu_0 \lambda_0 \lambda_1 + \lambda_1 \mu_0 \mu_1 + \lambda_0 \mu_0 \mu_1 - g \lambda_0 \mu_0 \left(\lambda_1 + \mu_1 \right) \right) \right),$$

$$\lambda_0 = \sum_{i=0}^{n-1} q_i r_i,$$

$$\min_{\lambda_1} \sum_{i=0}^{n-1} r_i \left(q_i \mu_0 \mu_1 (1-g) / \left(\lambda_1^2 \mu_0 + \mu_1 q_i \lambda_1 + \mu_0 q \lambda_1 + \lambda_1 \mu_0 \mu_1 + q_i \mu_0 \mu_1 - g q_i \mu_0 \left(\lambda_1 + \mu_1 \right) \right) \right),$$

$$\min_a \sum_{i=0}^{n-1} r_i \left(q_i \mu_0 \mu_1 (1-g) / \left(a_i^2 \mu_0 + \mu_1 q_i a_i + \mu_0 q_i a_i + a_i \mu_0 \mu_1 + q_i \mu_0 \mu_1 - g q_i \mu_0 \left(a_i + \mu_1 \right) \right) \right),$$

где (a_i) – вектор значений интенсивностей инициализации тестирования, обеспечивающий минимум вероятности опасного состояния P_3 для $i = 0,1 \ldots n-1$ возможных вариантов интенсивностей деструктивных воздействий (q_i).

При многокритериальной оптимизации максимизации готовности системы к безопасному выполнению запросов и минимизации опасных состояний воспользуемся аддитивным скалярным критерием, имеющим для рассматриваемых вариантов В1–В3 следующий вид:

$$\max_{\lambda_1} \left(\left[\alpha \lambda_1 \mu_0 \mu_1 - (1-\alpha) \right] \lambda_0 \mu_0 \mu_1 (1-g) / \left(\lambda_1^2 \mu_0 + \mu_1 \lambda_0 \lambda_1 + \mu_0 \lambda_0 \lambda_1 + \lambda_1 \mu_0 \mu_1 + \lambda_0 \mu_0 \mu_1 - g \lambda_0 \mu_0 \left(\lambda_1 + \mu_1 \right) \right) \right),$$

$$\lambda_0 = \sum_{i=0}^{n-1} q_i r_i,$$

$$\max_{\lambda_1} \sum_{i=0}^{n-1} r_i \left(\left[\alpha \lambda_1 \mu_0 \mu_1 - (1-\alpha) q_i \mu_0 \mu_1 (1-g) \right] / \left(\lambda_1^2 \mu_0 + \mu_1 q_i \lambda_1 + \mu_0 q_i \lambda_1 + \lambda_1 \mu_0 \mu_1 + q_i \mu_0 \mu_1 - g q_i \mu_0 \left(\lambda_1 + \mu_1 \right) \right) \right),$$

$$\max_a \sum_{i=0}^{n-1} r_i \left(\left[\alpha a_i \mu_0 \mu_1 - (1-\alpha) q_i \mu_0 \mu_1 (1-g) \right] / \left(a_i^2 \mu_0 + \mu_1 q_i a_i + \mu_0 q_i a_i + a_i \mu_0 \mu_1 + q_i \mu_0 \mu_1 - g q_i \mu_0 \left(a_i + \mu_1 \right) \right) \right).$$

Пример оптимизации интервалов тестирования

Проведем оптимизацию интервалов тестирования защищенной информационной системы по критерию максимизации готовности системы к безопасному выполнению запросов. Предположим, что интенсивность тестирования и восстановления безопасного состояния $\mu_1 = 1$ 1/ч, $\mu_0 = 0{,}1$ 1/ч при полноте оперативного контроля $g = 0{,}6$. Пусть возможны варианты деструктивных воздействий и их вероятности, представленные векторами (q_i) и (r_i) соответственно:

$$q_i = \begin{bmatrix} 0,001 \\ 0,002 \\ 0,003 \\ 0,004 \\ 0,005 \\ 0,006 \end{bmatrix}, \; r_i = \begin{bmatrix} 0,1 \\ 0,15 \\ 0,3 \\ 0,2 \\ 0,15 \\ 0,1 \end{bmatrix}.$$

Тогда оптимальным интервалам тестирования, определяемым по критерию максимизации готовности системы к безопасному выполнению запросов, для вариантов В1, В2 соответствуют значения $\lambda_1 = 0{,}03672$ 1/ч и $\lambda_1 = 0{,}03714$ 1/ч. Для варианта В3 вектор оптимальных интенсивностей инициализации тестирования (a_i), обеспечивающий минимум вероятности опасного состояния P_3 для $i = 0,1,\ldots, n–1$ возможных вариантов интенсивностей деструктивных воздействий (q_i), определен в результате оптимизации как

$$a_i = \begin{bmatrix} 0,020 \\ 0,028 \\ 0,035 \\ 0,040 \\ 0,045 \\ 0,049 \end{bmatrix}.$$

Результаты расчета вероятности готовности системы к безопасному выполнению запросов в зависимости от варианта интенсивности деструктивных воздействий представлены на рис. 3. Кривая 1 соответствует варианту В3 адаптивного изменения периодов тестирования в зависимости от наблюдаемой интенсивности деструктивных воздействий. Кривая 2 соответствует вариантам В1, В2, при которых задается постоянный период тестирования независимо от реальной интенсивности деструктивных воздействий. Кривые 3, 4 показывают увеличение вероятности готовности системы к безопасному выполнению запросов в результате адаптации периода тестирования к изменениям интенсивности деструктивных воздействий по варианту В3 относительно вариантов В1 и В2 соответственно.

Представленные графики позволяют сделать вывод об эффективности адаптивного изменения периодов тестирования в зависимости от наблюдаемой интенсивности деструктивных воздействий.

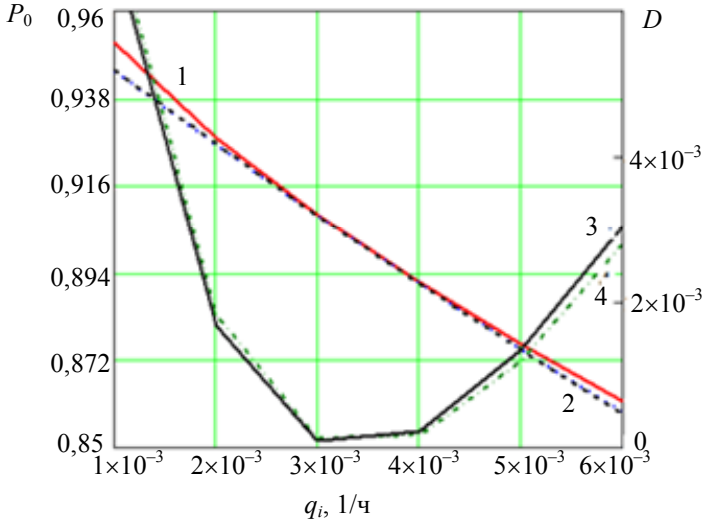

Рис. 3. Вероятности готовности системы к безопасному выполнению запросов: кривая 1 соответствует варианту В3, кривая 2 – вариантам В1, В2, кривые 3, 4 представляют разницу D готовности системы к безопасному выполнению запросов между вариантами В3–В1 и В3–В2

Предложенные модели и методы определения оптимальных интервалов тестирования могут найти применение при системотехническом проектировании компьютерных систем и сетей критического применения, работающих в условиях дестабилизирующих воздействий при повышенных требованиях к их безопасности [14–25].

Таким образом, предложена марковская модель защищенных информационных систем, функционирующих в условиях деструктивных злонамеренных и случайных воздействий, последствия которых обнаруживаются оперативным и тестовым контролем.

Поставлена и решена задача оптимизации интервалов инициализации тестового контроля по критерию максимизации вероятности нахождения системы в состоянии готовности к безопасному выполнению функциональных запросов и минимизации опасных состояний системы с учетом неопределенности и вариантности интенсивности деструктивных воздействий.

Рассмотрены варианты задачи оптимизации интервалов тестирования без их адаптации и с адаптацией к изменениям реальной интенсивности деструктивных воздействий.

Показана эффективность адаптивного изменения периодов тестирования в зависимости от наблюдаемой активности деструктивных воздействий. Так, из рис. 3 видно, что, например, при интенсивности деструктивных воздействий $6 \cdot 10^{-3}$ 1/ч готовность к безопасному выполнению запросов в результате адаптации (вариант В3) увеличивается на $3 \cdot 10^{-3}$ относительно вариантов без адаптации (В1, В2).

Решение задачи оптимизации проведено с использованием встроенных средств системы компьютерной математики Mathcad 15, включая средства символьной математики решения систем алгебраических уравнений.

Литература

1. Черкесов Г.Н. Надежность аппаратно-программных комплексов. СПб: Питер, 2005. 479 с.
2. Kopetz H. Real-Time Systems: Design Principles for Distributed Embedded Applications. Springer, 2011. 396 p.
3. Wang S.-C., Yan K.-Q., Ho C.-L., Wang S.-S. The optimal generalized Byzantine agreement in cluster-based wireless sensor networks // Computer Standards and Interfaces. 2014. V. 34. N 5. P. 821–830.
4. Abd-El-Barr M., Gebali F. Reliability analysis and fault tolerance for hypercube multi-computer networks // Information Sciences. 2014. V. 276. P. 295–318.
5. Dolev D., Függer M., Posch M., Schmid U., Steininger A., Lenzen C. Rigorously modeling self-stabilizing fault-tolerant circuits: an ultra-robust clocking scheme for systems-on-chip // Journal of Computer and System Sciences. 2014. V. 80. N 4. P. 860–900.
6. Li H., Liu H., Gao H., Shi P. Reliable fuzzy control for active suspension systems with actuator delay and fault // IEEE Transactions on Fuzzy Systems. 2012. V. 20. N 2. P. 342–357.
7. Shooman M.L. Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design. John Wiley & Sons Inc., 2002. 527 p.
8. Sorin D.J. Fault Tolerant Computer Architecture. Morgan & Claypool, 2009. 103 p.
9. Koren I., Krishna C.M. Fault Tolerant Systems. San Francisco: Morgan Kaufmann Publishers, 2009. 378 p.
10. Gómez A., Carril L.M., Valin R., Mouriño J.C., Cotelo C. Fault-tolerant virtual cluster experiments on federated sites using BonFIRE // Future Generation Computer Systems. 2014. V. 34. P. 17–25.
11. Bogatyrev V.A, Bogatyrev S.V., Golubev I.Yu. Optimization and the process of task distribution between computer system clusters // Automatic Control and Computer Sciences. 2012. V. 84. N 3. P. 103–111.
12. Bogatyrev V.A. Fault tolerance of clusters configurations with direct connection of storage devices // Automatic Control and Computer Sciences. 2011. V. 45. N 6. P. 330–337.
13. Bogatyrev V.A. Exchange of duplicated computing complexes in fault tolerant systems // Automatic Control and Computer Sciences. 2011. V. 46. N 5. P. 268–276.
14. Алиев Т.И. Проектирование систем с приоритетами // Изв. вузов. Приборостроение. 2014. Т. 57. № 4. С. 30–35.
15. Богатырев В.А., Богатырев С.В., Богатырев А.В. Функциональная надежность вычислительных систем с перераспределением запросов // Изв. вузов. Приборостроение. 2012. Т. 55. № 10. С. 53–56.
16. Колбанев М.О., Татарникова Т.М., Воробьев А.И. Модель обработки клиентских запросов // Телекоммуникации. 2013. № 9. С. 42–47.
17. Богатырев В.А. Отказоустойчивость и сохранение эффективности функционирования многомагистральных распределенных вычислительных систем // Информационные технологии. 1999. № 9. С. 44–48.
18. Богатырев В.А. К повышению надежности вычислительных систем на основе динамического распределения функций // Изв. вузов СССР. Приборостроение. 1981. Т. 23. № 8. С. 62–65.
19. Богатырев В.А. Богатырев С.В. Критерии оптимальности многоуровневых отказоустойчивых компьютерных систем // Научно-технический вестник СПбГУ ИТМО. 2009. № 5 (63). С. 92–97.
20. Перегуда А.И., Тимашов Д.А. Вероятностный анализ показателей надежности подсистем СУЗ с учетом периодического контроля исправности // Изв. вузов. Ядерная энергетика. 2009. № 4. С. 45–53.
21. Богатырев В.А. Мультипроцессорные системы с динамическим перераспределением запросов через общую магистраль // Изв. вузов СССР. Приборостроение. 1985. № 3. С. 33–38.
22. Богатырев В.А. Оценка вероятности безотказной работы функционально-распределенных вычислительных систем при иерархической структуре узлов // Изв. вузов. Приборостроение. 2000. Т. 43. № 3. С. 67–70.

23. Богатырев В.А., Богатырев С.В. Надежность системы управления агрегатами и машинами коммунального хозяйства // Технико-технологические проблемы сервиса. 2008. № 4 (6). С. 23–27.
24. Богатырев В.А., Богатырев С.В., Парантаев Г.В. Балансировки нагрузки в системах управления машинами и агрегатами коммунально-бытовой сферы // Технико-технологические проблемы сервиса. 2008. № 3 (5). С. 54–58.
25. Гатчин Ю.А., Жаринов И.О., Коробейников А.Г. Математические модели оценки инфраструктуры системы защиты информации на предприятии // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 2 (78). С. 92–95.

Богатырев Владимир Анатольевич – доктор технических наук, профессор, Университет ИТМО, 197101, Санкт-Петербург, Россия, Vladimir.bogatyrev@gmail.com

Богатырев Анатолий Владимирович – аспирант, Университет ИТМО, 197101, Санкт-Петербург, Россия, Vladimir.bogatyrev@gmail.com

Богатырев Станислав Владимирович – младший научный сотрудник, Санкт-Петербургский государственный университет аэрокосмического приборостроения, 190000, Санкт-Петербург, Россия, Vladimir.bogatyrev@gmail.com

Vladimir A. Bogatyrev – D.Sc., Professor, ITMO University, 197101, Saint Petersburg, Russia, Vladimir.bogatyrev@gmail.com

Anatoly V. Bogatyrev – postgraduate, ITMO University, 197101, Saint Petersburg, Russia, Vladimir.bogatyrev@gmail.com

Stanislav V. Bogatyrev – junior scientific researcher, Saint Petersburg State University of Aerospace Instrumentation, 190000, Saint Petersburg, Russia, Vladimir.bogatyrev@gmail.com

Принято к печати 13.01.14
Accepted 13.01.14