УДК 519.873
DOI 10.25205/1818-7900-2019-17-4-5-33-45

Математическое моделирование отказоустойчивости информационных систем

А. И. Голева, Н. Р. Стороженко, В. И. Потапов, О. П. Шافеева

*Омский государственный технический университет
Омск, Россия*

Аннотация

В статье рассматривается проблема надежности информационных систем, в целях решения данной проблемы предложен метод оценки отказоустойчивости систем передачи данных с применением аппарата математического моделирования отказоустойчивых систем с тремя уровнями функционирования. Разработана математическая модель в виде графа состояний и вероятности отказов с системой дифференциальных уравнений для ее описания, решение которой позволяет получить вероятности отказов на различных уровнях функционирования информационных систем с целью обнаружения и поиска неисправностей и отказов оборудования.

Ключевые слова

информационная система, диагностика сетевых параметров, надежность сетевых ресурсов, отказ, уровень функционирования сети

Для цитирования

Голева А. И., Стороженко Н. Р., Потапов В. И., Шافеева О. П. Математическое моделирование отказоустойчивости информационных систем // Вестник НГУ. Серия: Информационные технологии. 2019. Т. 17, № 4. С. 33–45. DOI 10.25205/1818-7900-2019-17-4-33-45

Mathematical Modeling of Fault-Tolerance of the Information Systems

A. I. Goleva, N. R. Storozhenko, V. I. Potapov, O. P. Shafeeva

*Omsk State Technical University
Omsk, Russian Federation*

Annotation

The article deals with the problem of reliability of information systems, in order to solve this problem, a method for assessing the fault tolerance of data transmission systems using the apparatus of mathematical modeling of fault-tolerant systems with three levels of operation was introduced. Also the mathematical model in the form of a graph of states and the probability of failure with a system of differential equations for its description was formulated. The solution of mathematical model allows to obtain the probability of failure at different levels of functioning of information systems in order to detect and find faults and equipment failures.

Keywords

information system, diagnosis of network parameters, reliability of network resource, failure, the level of functioning of the network

For citation

Goleva A. I., Storozhenko N. R., Potapov V. I., Shafeeva O. P. Mathematical Modeling of Fault-Tolerance of the Information Systems. *Vestnik NSU. Series: Information Technologies*, 2019, vol. 17, no. 4, p. 33–45. (in Russ.) DOI 10.25205/1818-7900-2019-17-4-33-45

© А. И. Голева, Н. Р. Стороженко, В. И. Потапов, О. П. Шавеева, 2019

ISSN 1818-7900 (Print). ISSN 2410-0420 (Online)
Вестник НГУ. Серия: Информационные технологии. 2019. Том 17, № 4
Vestnik NSU. Series: Information Technologies, 2019, vol. 17, no. 4

Введение

В настоящее время современные возможности в области информационных технологий внедряются и используются во всех отраслях жизнедеятельности. Повсеместное применение современных средств вычислительной техники делает актуальными задачи обеспечения надежности, защищенности и доступности сетевых ресурсов в современных информационных системах (ИС). Проблема анализа уровня надежности и отказоустойчивости ИС сейчас стоит довольно остро. Однако, несмотря на стремительное развитие сферы информационных технологий и большое внимание к проблемам надежности ИС по данным международной статистики уровень вторжений в сеть, число отказов и уровни потери данных и работоспособности устройств не снижается. По исследованиям компании «Лаборатория Касперского», более 40 % компьютеров ИС были атакованы в первой половине 2018 года, исходя из этого ИС организаций в 2018 году не стали менее уязвимы к отказам по сравнению с 2017 годом. Кроме того, на сегодняшний день, проблема является особенно актуальной в связи с проявлением таких деструктивных факторов в сети, как: переполнение буфера (нарушение границ памяти и аварийное завершение), отказы в обслуживании, отказ почтовых служб, перехват текущей сессии, получение нелегального доступа к частным сетевым ресурсам, анализ трафика, использование манипуляций, направленных на отказы (вирусов, sniffеров, руткитов, SQL-инъекций, RНР-инъекций, поддельных онлайн сервисов).

Проблемы диагностики и надежности информационных систем рассматриваются в работах многих отечественных и зарубежных авторов [1–14]. Так, в работах [1–8] рассматриваются общие методы и принципы построения математических моделей, а также подходы к расчету и моделированию параметров классической теории надежности [2]. В работах [9–14] описаны причины применения систем контроля и диагностики ИС, а также описываются основные принципы их работы без применения математического аппарата.

Литературный обзор источников, посвященных вопросам повышения непрерывности функционирования информационных систем, позволил сделать ряд выводов.

В рассмотренных работах при построении математических моделей в расчет берутся лишь базовые показатели надежности ИС, при этом не учитываются некоторые важные функции ИС, в данной статье делается попытка устранения указанных недостатков путем моделирования отказов ресурсов ИС на каждом из уровней функционирования ИС: локальном уровне, уровне сетевого окружения, уровень критически важных узлов.

Объект моделирования

В общем виде при рассмотрении ИС необходимо учитывать ее структурные, функциональные и системно-технические особенности. С точки зрения структурных особенностей ИС могут иметь разнообразную топологию, с содержанием нескольких локальных вычислительных сетей. ИС могут объединять филиалы, создавая единое пространство для хранения и обмена данными.

С точки зрения функциональных особенностей ИС – это среда для хранения и передачи информации необходимой для решения многофункциональных задач обработки данных. В такой среде можно выделить три уровня (рис. 1):

- локальный уровень (уровень функционирования отдельно взятого узла или блока ИС);
- уровень сетевого окружения (подсети и сети с взаимодействующими узлами ИС);
- уровень критически важных узлов системы (в частности, коммутационное оборудование и сервера). Функции для каждого такого узла приведены в табл. 1.

Рис. 1. Состав информационной системы
Fig. 1. Structure of the information system

Критически важные узлы ИС

Таблица 1

Critical nodes of the information system

Table 1

Критически важный узел		Назначение и выполняемые функции
Устройства связи	Коммутаторы и маршрутизаторы	Передача сообщений по выделенным каналам, хранение таблиц коммутации
	Файл – сервер	Хранение общих папок и файлов
Сервера	Почтовый сервер	Отправка, получение и хранение данных корпоративной переписки
	Контроллер домена	Централизованное управление и администрирование рабочих станций и серверов сети
	Сервер приложений	Хранение данных и доступ клиентов к прикладным программам, выполняющимся на сервере; управление жизненным циклом производимых изделий
	Сервер бухгалтерии	Хранение и управление финансовой отчетностью; организация и оптимизация бизнес процессов
	Сервер безопасности	Защита от утечки конфиденциальной информации; разграничение доступа пользователей к внешним и внутренним устройствам сети, централизованное управление системой антивирусной защиты

Характеристики функционирования ИС могут быть представлены следующим образом (рис. 2), при этом эффективное функционирование характеризуется состояниями способности и готовности выполнять функции отправки пакетов, обслуживания запросов клиентов, в то время как неэффективное можно охарактеризовать состояниями задержек, сбоев и отказов. Наряду с тем здесь можно выделить категорий ошибок, которые могут привести к отказам ИС (рис. 3).

Рис. 2. Характеристика функционирования ИС
Fig. 2. Characteristics of functioning of the information system

Рис. 3. Ошибки, которые могут привести к отказам ИС
Fig. 3. Errors that can lead to failures of the information system

С точки зрения системно-технических особенностей ИС представляют собой целостную структуру, включающую взаимосвязанные и взаимодействующие уровни (рис. 4). Наиболее важными компонентами ИС являются системное и прикладное программное обеспечение, система управления базами данных, функции и сервисы передачи, хранения и обработки данных.

Рис. 4. Состав информационной системы
Fig. 4. Structure of the information system

Постановка задачи и описание модели

При проектировании надежных и отказоустойчивых ИС и сетей для минимизации времени и затрат на восстановление и замену отказавших блоков, – в последнее время оказываются актуальны и широко применимы на практике различные методы моделирования в целях реализации обоснованного выбора оптимальной стратегии внедрения резервных элементов с учетом отказов соответствующих блоков.

Актуальной является следующая задача: моделирование и оценка вероятностей отказов в информационной системе для определения блоков, нуждающихся в модернизации или замене резервными [15].

Реализацию данной задачи было решено произвести с помощью аппарата цепей Маркова, так как это один из наиболее наглядных и нетрудоемких способов математического моделирования множества разнообразных операций, – в том числе и отказов в ИС, – развивающихся в форме случайных процессов.

Цепи Маркова представляют собой широко известный математический аппарат для описания разнообразных проблем вероятностного характера. Цепь может записываться в виде графа с вершинами – состояниями системы и ребрами – интенсивностями перехода в данное состояние. Имея в распоряжении размеченный граф, можно найти вероятности каждого из состояний, как в условиях изменения параметров во времени, так и в условиях предельного стационарного режима работы системы [16].

Перед началом моделирования необходимо определить входные параметры: возможные состояния отказов, характерные для исследуемой информационной системы, а также учесть всевозможные связи между состояниями – интенсивности того потока событий, который переводит систему из одного состояния в другое.

После определения входных параметров системы можно приступить к построению модели. В данном случае предлагается использование графовой модели, основанной на теории Марковских цепей.

Отказ в информационной системе рассматривается как случайный процесс с конечным числом состояний. При этом события происходят поодиночке, а не группами сразу по несколько, – что означает ординарность описываемой модели. Кроме того, модель не содержит последствия в силу того, что для любых двух непересекающихся участков времени число событий, попадающих на один из них, не зависит от того, сколько событий попало на другой.

Для построения модели и расчета характеристик отказоустойчивости сети полагаем, что в рассматриваемой информационной системе в случайный момент времени может быть осуществлен отказ на одном из уровней функционирования сети: локальный уровень, уровень сетевого окружения, уровень критически важных узлов системы.

На этапе построения модели принимаем, что система может перейти к следующим состояниям отказа на одном из уровней функционирования сети S_{ij} , где

i – уровни функционирования сети ($j = 1, 2, 3$), мы рассматриваем в данном примере:

- локальный уровень;
- уровень сетевого окружения;
- уровень критически важных узлов системы;

j – это типы отказа ($i = 1, 2, 3, 4, 5$), к которым можно отнести:

- отказ аппаратного обеспечения;
- отказ на общесистемном уровне;
- отказ приложений;
- отказ сетевых устройств;
- отказ физических каналов связи.

Начальное состояние системы – нормальное функционирование системы без отказов, когда все ресурсы исправны. Все дальнейшие состояния отличны от начального и характеризуются внештатным функционированием при осуществлении отказов.

Далее строится связный граф состояний моделируемой системы, где показаны связи каждого из j -х отказов на каждом i -м уровне функционирования информационной системы (состояния S_{ij}) с вершиной в S_0 (состояние системы без отказов), а также λ_i – интенсивности того потока событий, который переводит систему из одного состояния в другое.

Для наглядности построенную цепь событий в сети можно представить в виде графа, где вершины – это возможные состояния системы, а ребра – интенсивности перехода в них. Графически предлагаемую модель системы можно представить на рис. 1.

Для оценки уровня отказоустойчивости и нахождения вероятностей отказов в сети по построенному графу составляем математическую модель в виде системы дифференциальных либо же линейных алгебраических уравнений по следующему правилу: слева – производная вероятности состояния, а справа – сумма произведений вероятностей тех состояний, из которых идут стрелки в данное состояние, на интенсивности соответствующих потоков событий, минус суммарная интенсивность потоков, ведущих из данного состояния, умноженная на вероятность данного состояния (1).

Рис. 1. Граф отказов информационной системы,
 где S_{ij} – это состояния системы,
 λ_i – интенсивности i -го отказа
 Fig. 1. Graph of the information system failures,
 where S_{ij} is the state of the system,
 λ_i is the intensity of the i -th failure

$$\begin{cases}
 \frac{dp_0}{dt} = -p_0(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5), \\
 \frac{dp_{1,1}}{dt} = p_0\lambda_1 + p_{1,2}\lambda_2 + p_{2,1}\lambda_1 - p_{1,1}(2\lambda_1 + \lambda_2), \\
 \frac{dp_{1,2}}{dt} = p_0\lambda_2 + p_{1,1}\lambda_2 - p_{1,2}(\lambda_2 + \lambda_3), \\
 \frac{dp_{1,3}}{dt} = p_0\lambda_3 + p_{1,2}\lambda_3 - p_{1,3}\lambda_3, \\
 \frac{dp_{1,4}}{dt} = p_0 \cdot \lambda_4 + p_{1,5}\lambda_4 - p_{1,4}\lambda_4, \\
 \frac{dp_{1,5}}{dt} = p_0 \cdot \lambda_1 - p_{1,5}(\lambda_4 + \lambda_5), \\
 \frac{dp_{2,1}}{dt} = p_{1,1} \cdot \lambda_2 + p_{3,1}\lambda_1 - p_{2,1}(2\lambda_1 + \lambda_2), \\
 \frac{dp_{2,2}}{dt} = p_{1,2}\lambda_2 + p_{2,3}\lambda_3 - p_{2,2}(\lambda_2 + \lambda_3), \\
 \frac{dp_{2,3}}{dt} = p_{1,3}\lambda_3 + p_{2,2}\lambda_3 + p_{2,4}\lambda_4 - p_{2,3}(2\lambda_3 + \lambda_4), \\
 \frac{dp_{2,4}}{dt} = p_{1,4} \cdot \lambda_4 + p_{2,3}\lambda_4 + p_{2,5}\lambda_4 - p_{2,4}(3\lambda_4 + \lambda_3), \\
 \frac{dp_{2,5}}{dt} = p_{2,4} \cdot \lambda_4 + p_{1,5}\lambda_5 - p_{2,5}(\lambda_4 + \lambda_5), \\
 \frac{dp_{3,1}}{dt} = p_{2,1} \cdot \lambda_1 + p_{3,3}\lambda_3 + p_{3,4}\lambda_3 - p_{3,1}(\lambda_1 + 2\lambda_3 + \lambda_2), \\
 \frac{dp_{3,2}}{dt} = p_{2,2}\lambda_2 + p_{3,1}\lambda_3 + p_{3,3}\lambda_3 - p_{3,2}\lambda_3, \\
 \frac{dp_{3,3}}{dt} = p_{2,3}\lambda_3 + p_{2,4}\lambda_3 + p_{3,1}\lambda_3 + p_{3,2}\lambda_3 + p_{3,4}\lambda_3 - 3\lambda_3 p_{3,3}, \\
 \frac{dp_{3,4}}{dt} = p_{2,4} \cdot \lambda_4 + p_{3,1}\lambda_3 + p_{3,5}\lambda_4 - p_{3,4}(2\lambda_3 + \lambda_4), \\
 \frac{dp_{3,5}}{dt} = p_{2,5} \cdot \lambda_5 + p_{3,4}\lambda_4 - p_{3,5}\lambda_4.
 \end{cases} \quad (1)$$

Определив значения интенсивностей отказов, можно приступить к решению системы полученных уравнений.

В итоге решением станут искомые значения вероятностей нахождения рассматриваемой информационной системы в каждом из описанных состояний – от состояния безотказной работы до различных типов отказов ее блоков.

Выходные данные моделирования позволят сделать выводы о наиболее критичных блоках, нуждающихся в замене или модернизации.

Реализация модели

Для численного решения системы уравнений (1) необходимо определить начальные условия и интенсивности отказов ИС λ_i . Для определения значений λ_i можно использовать метод экспертных оценок (когда специалистами на основе состава, качества и производительности оборудования ИС оценивается степень интенсивности отказов), либо данные о работоспособности и пиковых нагрузках ИС, полученные при помощи системы мониторинга параметров ИС.

В данном случае, на примере небольшой ИС производственного предприятия – в качестве наиболее объективного – решено было использовать второй вариант. Так, в течение 72 часов на каждом из трёх уровней рассматриваемой ИС (локально – с отдельно взятых узлов; с сетевых компьютеров ИС; с сервера ИС) при помощи системы мониторинга были получены следующие показатели (рис. 2).

В качестве интенсивности потока событий, который переводит систему в отказ аппаратного обеспечения – Disk Usage, показывающий процент общей загруженности диска. Представляет из себя сумму значений загруженности диска операциями чтения и записи.

Для оценки интенсивности отказов на общесистемном уровне и отказов приложений среднее количество BSoD (blue screen of death) и ошибок / аварийных завершений работы ПО соответственно.

В качестве интенсивности отказов сетевых устройств – Current Bandwidth для оценки полосы пропускания (в байтах в секунду) сетевых адаптеров.

Для оценки интенсивности отказов физических каналов связи – утилита Ping отправляет запросы протокола ICMP и фиксирует поступающие ответы. Наличие отклика свидетельствует о том, что канал связи установлен и работает, что в противном случае позволяет косвенно определять недоступность каналов передачи данных.

Рис. 2. Мониторинг значений по отслеживаемым параметрам
Fig. 2. Monitoring a values of the watched parameters

Для преобразования полученных данных (рис. 2) в значения интенсивностей отказов необходима нормировка данных, которая состоит в преобразовании их к унифицированной форме представления, шкале. В данном случае все собранные значения приводятся к виду

$$\tilde{x}_j = \frac{x_j}{\max}, \quad (2)$$

$$\lambda_i = \frac{\sum_{j=1}^N \tilde{x}_j}{N}, \quad (3)$$

где

$\tilde{x}_j$ – нормированные (стандартизованные) значения параметра, $j = 1, \dots, N$;

N – количество измеренных системой мониторинга значений параметра;

i – количество отслеживаемых системой мониторинга параметров, которое в данном случае соответствует количеству типов отказов ($i = 1, 2, 3, 4, 5$).

Исходя из полученных при помощи системы мониторинга данных (см. рис. 2) и приведения их к виду в соответствии с формулами (2) и (3), были получены следующие значения интенсивностей: $\lambda_1 = 0,65$, $\lambda_2 = 0,21$, $\lambda_3 = 0,3$, $\lambda_4 = 0,71$, $\lambda_5 = 0,82$.

В данном примере при нахождении вероятностей отказов – в рассматриваемой ИС небольшого производственного предприятия – преимущественно представляет интерес состояние системы в предельном, установившемся режиме. Так, основной характеристикой при решении поставленной задачи будет являться вектор финальных вероятностей, определяющий установившийся режим работы ИС.

Поскольку предельные вероятности системы постоянны, то, заменив в уравнениях (1) соответствующие производные нулевыми значениями, получим систему линейных алгебраических уравнений, описывающих стационарный режим работы системы. Для решения необходимо добавить нормировочное условие, отбросив при этом одно из уравнений, так как оно является следствием остальных. Так, от системы уравнений (1) осуществляется переход к системе (4).

$$\begin{cases} p_0(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5) = 0, \\ p_{1,1}(2\lambda_1 + \lambda_2) = p_0\lambda_1 + p_{1,2}\lambda_2 + p_{2,1}\lambda_1, \\ p_{1,2}(\lambda_2 + \lambda_3) = p_0\lambda_2 + p_{1,1}\lambda_2, \\ p_{1,3}\lambda_3 = p_0\lambda_3 + p_{1,2}\lambda_3, \\ p_{1,4}\lambda_4 = p_0\lambda_4 + p_{1,5}\lambda_4, \\ p_{1,5}(\lambda_4 + \lambda_5) = p_0\lambda_5, \\ p_{2,1}(2\lambda_1 + \lambda_2) = p_{1,1}\lambda_2 + p_{3,1}\lambda_1, \\ p_{2,2}(\lambda_2 + \lambda_3) = p_{1,2}\lambda_2 + p_{2,3}\lambda_3, \\ p_{2,3}(2\lambda_3 + \lambda_4) = p_{1,3}\lambda_3 + p_{2,2}\lambda_3 + p_{2,4}\lambda_4, \\ p_{2,4}(3\lambda_4 + \lambda_3) = p_{1,4}\lambda_4 + p_{2,3}\lambda_4 + p_{2,5}\lambda_4, \\ p_{2,5}(\lambda_4 + \lambda_5) = p_{2,4}\lambda_4 + p_{1,5}\lambda_5, \\ p_{3,1}(\lambda_1 + 2\lambda_3 + \lambda_2) = p_{2,1}\lambda_1 + p_{3,3}\lambda_3 + p_{3,4}\lambda_3, \\ p_{3,2}\lambda_3 = p_{2,2}\lambda_2 + p_{3,1}\lambda_3 + p_{3,3}\lambda_3, \\ 3\lambda_3 p_{3,3} = p_{2,3}\lambda_3 + p_{2,4}\lambda_3 + p_{3,1}\lambda_3 + p_{3,2}\lambda_3 + p_{3,4}\lambda_3, \\ p_{3,4}(2\lambda_3 + \lambda_4) = p_{2,4}\lambda_4 + p_{3,1}\lambda_3 + p_{3,5}\lambda_4, \\ p_0 + p_{1,1} + p_{1,2} + p_{1,3} + p_{1,4} + p_{1,5} + p_{2,1} + p_{2,2} + p_{2,3} + p_{2,4} + p_{2,5} + p_{3,1} + p_{3,2} + p_{3,3} + p_{3,4} + p_{3,5} = 1. \end{cases} \quad (4)$$

Как следствие, для данного примера, подставив в систему (4) полученные значения интенсивностей ($\lambda_1 = 0,65$, $\lambda_2 = 0,21$, $\lambda_3 = 0,3$, $\lambda_4 = 0,71$, $\lambda_5 = 0,82$) и произведя расчеты при помощи математического пакета, позволяющего осуществлять решение систем линейных уравнений, – получим следующие значения (табл. 2).

Таблица 2

Решение системы уравнений – вероятности различных типов отказов на каждом уровне ИС

Table 2

Probabilities of different failures types for each level of the information system

P_0	$P_{1.1}$	$P_{1.2}$	$P_{1.3}$	$P_{1.4}$	$P_{1.5}$	$P_{2.1}$	$P_{2.2}$	$P_{2.3}$	$P_{2.4}$	$P_{2.5}$	$P_{3.1}$	$P_{3.2}$	$P_{3.3}$	$P_{3.4}$	$P_{3.5}$
0	0,02	0,01	0,01	0	0	0,04	0,01	0	0	0	0,08	0,25	0,17	0,16	0,26

Исходя из этого, наибольшими значениями обладают:

- на локальном уровне: вероятность отказа аппаратного обеспечения $p_{1.1} = 0,02$;
- на уровне сетевого окружения: вероятность отказа аппаратного обеспечения $p_{2.1} = 0,04$;
- на уровне критически важных узлов: вероятность отказа ОС $p_{3.2} = 0,25$, вероятность

отказа канала связи $p_{3.5} = 0,26$.

Таким образом, в статье при помощи аппарата цепей Маркова применительно к сети с 3 уровнями функционирования подробно описана разработанная математическая модель безотказной работы информационной системы с построением системы дифференциальных уравнений, решение которой позволяет получить значения вероятностей различных типов отказов блоков ИС на трех уровнях ее функционирования: локальном, сетевом, а также на уровне критически важных узлов.

Заключение

В условиях роста и изменчивости качественных и количественных характеристик сетевых аномалий в работе оборудования ИС и отказов, а также различных инцидентов возникает потребность в совершенствовании существующего аппарата по моделированию отказоустойчивых систем, систем и алгоритмов обнаружения неисправностей. Необходимость повышения отказоустойчивости информационной системы обусловлена непреднамеренными случайными сбоями в работе сервисов и служб ИС, которые могут вызвать нежелательные последствия. К числу таких последствий можно отнести замедление реагирования аппаратного или программного обеспечения вплоть до полного прекращения функционирования критично важных служб и программ.

Для решения проблем в данной области исследования в статье приводится математическое описание процесса поиска неисправностей и отказов оборудования для сети с 3 уровнями функционирования: локальным, сетевым и уровнем критически важных узлов. Важно при моделировании проводить оценку возможных отказов, чтобы определять риски и иметь возможность максимально быстро нивелировать последствия.

Решение дифференциальных уравнений позволяет отследить динамику изменения степени отказоустойчивости системы через отслеживание в определенные промежутки времени вероятностей отказов. Для определения вероятности состояния системы в предельном установившемся режиме можно перейти к линейной системе алгебраических уравнений, приравняв все левые части дифференциальных уравнений к нулю.

Таким образом, решение полученной модели позволяет получить конкретные значения вероятностей отказов на каждом из 3 уровней функционирования ИС. При необходимости,

данный метод можно описать большим количеством состояний для моделирования поведения более сложных систем, а создание алгоритма и программной его реализации позволит не только оптимизировать процесс моделирования, но и предоставит возможность наблюдения за поведением системы в условиях изменения параметров.

Список литературы

1. **Дружинин Г. В.** Надежность автоматизированных систем. М.: Энергия, 1977. 536 с.
2. **Ушаков И. А.** Надежность технических систем. М.: Радио и связь, 1985. 606 с.
3. **Можаев А. С.** Универсальный графоаналитический метод, алгоритм и программный модуль построения монотонных и немонотонных логических функций работоспособности систем // Моделирование и анализ безопасности, риска в сложных системах: Тр. Междунар. науч. школы. СПб.: СПбГУАП, 2003. С. 101–110.
4. **Потапов В. И.** Постановка и решение игровой задачи противоборства аппаратно-избыточной динамической системы с атакующим противником, действующим в условиях неполной информации в процессе конфликта // Мехатроника, автоматизация, управление. 2017. Т. 18, № 8. С. 525–531. DOI 10.17587/mau.18.525-531
5. **Sandoval Y., Gallizo G., Curiel M.** Evaluation of monitoring tools for cloud computing environments. In: Proc. Conf. on Informatica (CLEI), 2012, p. 1–10. DOI 10.1109/CLEI.2012.6427251
6. **Honda K., Shrestha A., Witayangkurn A., Chinnachodteeranun R., Shimamura H.** Fieldservers and sensor service grid as real-time monitoring infrastructure for ubiquitous sensor networks. *Sensors*, 2009, vol. 9, no. 4, p. 2363–2370. DOI 10.3390/s90402363
7. **Kufel L.** Security Event Monitoring in a Distributed Systems Environment. *IEEE Security and Privacy*, 2013, vol. 11, no. 1, p. 36–43. DOI 10.1109/MSP.2012.61
8. **Kufel L.** Tools for Distributed Systems Monitoring. *Foundations of Computing and Decision Sciences*, 2016, vol. 41, no. 4, p. 237–260. DOI 10.1515/fcds-2016-0014
9. **Mitra S., Ransbotham S.** Information Disclosure and the Diffusion of Information Security Attacks. *Information Systems Research*, 2015, vol. 26, no. 3, p. 565–584. DOI 10.1287/isre.2015.0587
10. **Ачилов Р.** Построение защищенных корпоративных сетей. М.: Наука и техника, 2013. 368 с.
11. **Papantoni-Kazakos P.** Multiple-access algorithms for a system with mixed traffic: high and low priority. *IEEE Transactions on Communications*, 1992, vol. 40, no. 3, p. 541–555. DOI 10.1109/ICC.1989.49777
12. **Wolters D., Gerth C., Engels G.** Visual Requirements Modeling for Cross-Device Systems. *Computer Science and Information Systems*, 2017, vol. 14, no. 3, p. 517–536. DOI 10.2298/CSIS160930015W
13. **Atia S., Messaoud A., Abdenmour R.** An online identification algorithm of unknown time-varying delay and internal multimodel control for discrete non-linear systems. *Mathematical and Computer Modelling of Dynamical Systems*, 2017, vol. 24, p. 26–41. DOI 10.1080/13873954.2017.1352607
14. **Литвяк Р. К., Воробьев С. П., Кацупеев А. А.** Модель исследования надежности информационной системы высокой готовности на базе архитектуры с резервированием серверов // Изв. высших учебных заведений. Северо-Кавказский регион. 2016, вып. 2. С. 21–27. DOI 10.17213/0321-2653-2016-2-21-27
15. **Потапов В. И.** Противоборство технических систем в конфликтных ситуациях: модели и алгоритмы. Омск: ОмГТУ, 2015. 168 с.
16. **Вентцель Е. С.** Исследование операций: задачи, принципы, методология. 6-е изд. М.: Юстиция, 2018. 192 с.

References

1. **Druzhinin G. V.** Reliability of automated system. Moscow, Energiya, 1977, 536 p. (in Russ.)
2. **Ushakov I. A.** Reliability of technical systems. Moscow, Radio and communication, 1985, 606 p. (in Russ.)
3. **Mozhaev A. S.** Universal graphical-analytical method, algorithm and software module for the construction of monotonic and non-monotonic logical functions of system efficiency. In: Proc. Int. Scientific. Schools. St. Petersburg, SUAI, 2003, p. 101–110. (in Russ.)
4. **Potapov V. I.** Setting and Solving of the Game Problem of Confrontation of the Hardware-Redundant Dynamic System with an Attacking Enemy Operating in the Conflict Process in Conditions of Incomplete Information. *Mekhatronika, Avtomatizatsiya, Upravlenie*, 2017, vol. 18, no. 8, p. 525–531. (in Russ.) DOI 10.17587/mau.18.525-531
5. **Sandoval Y., Gallizo G., Curiel M.** Evaluation of monitoring tools for cloud computing environments. In: Proc. Conf. on Informatica (CLEI), 2012, p. 1–10. DOI 10.1109/CLEI.2012.6427251
6. **Honda K., Shrestha A., Witayangkurn A., Chinnachodteeranun R., Shimamura H.** Fieldservers and sensor service grid as real-time monitoring infrastructure for ubiquitous sensor networks. *Sensors*, 2009, vol. 9, no. 4, p. 2363–2370. DOI 10.3390/s90402363
7. **Kufel L.** Security Event Monitoring in a Distributed Systems Environment. *IEEE Security and Privacy*, 2013, vol. 11, no. 1, p. 36–43. DOI 10.1109/MSP.2012.61
8. **Kufel L.** Tools for Distributed Systems Monitoring. *Foundations of Computing and Decision Sciences*, 2016, vol. 41, no. 4, p. 237–260. DOI 10.1515/fcds-2016-0014
9. **Mitra S., Ransbotham S.** Information Disclosure and the Diffusion of Information Security Attacks. *Information Systems Research*, 2015, vol. 26, no. 3, p. 565–584. DOI 10.1287/isre.2015.0587
10. **Achilov R.** Building secure enterprise networks. Moscow, Science and technology, 2013, 368 p. (in Russ.)
11. **Papantoni-Kazakos P.** Multiple-access algorithms for a system with mixed traffic: high and low priority. *IEEE Transactions on Communications*, 1992, vol. 40, no. 3, p. 541–555. DOI 10.1109/ICC.1989.49777
12. **Wolters D., Gerth C., Engels G.** Visual Requirements Modeling for Cross-Device Systems. *Computer Science and Information Systems*, 2017, vol. 14, no. 3, p. 517–536. DOI 10.2298/CSIS160930015W
13. **Atia S., Messaoud A., Abdenmour R.** An online identification algorithm of unknown time-varying delay and internal multimodel control for discrete non-linear systems. *Mathematical and Computer Modelling of Dynamical Systems*, 2017, vol. 24, p. 26–41. DOI 10.1080/13873954.2017.1352607
14. **Litvyak R., Vorobyov S., Katsuphev A.** Reliability evaluation model of high availability information system with redundant servers architecture. *Izvestiya vuzov. North Caucasus region. Series: Technical Sciences*, 2016, iss. 2, p. 21–27. DOI 10.17213/0321-2653-2016-2-21-27
15. **Potapov V. I.** Confrontation of technical systems in conflict situations: models and algorithms. Omsk, OmSTU, 2015, 166 p. (in Russ.)
16. **Ventzel E. S.** Operations research: tasks, principles, methodology. Moscow, Justice, 2018, 192 p. (in Russ.)

Материал поступил в редколлегию
Received
26.03.2019

Сведения об авторах

Голева Алина Игоревна, аспирант, Омский государственный технический университет, кафедра «Информатика и вычислительная техника» (Омск, Россия)
frybkf07.93@mail.ru
ResearcherID W-2541-2018

Стороженко Никита Русланович, аспирант, Омский государственный технический университет, кафедра «Информатика и вычислительная техника» (Омск, Россия)
snikr@bk.ru
ResearcherID Y-8341-2018

Потапов Виктор Ильич, доктор технических наук, профессор, Омский государственный технический университет, кафедра «Информатика и вычислительная техника» (Омск, Россия)
ivt@omgtu.ru

Шадеева Ольга Павловна, кандидат технических наук, доцент, Омский государственный технический университет, кафедра «Информатика и вычислительная техника» (Омск, Россия)
ivt_olga_pavlovna@mail.ru

Information about Authors

Alina I. Goleva, postgraduate student, Omsk State Technical University (Omsk, Russia)
frybkf07.93@mail.ru
ResearcherID W-2541-2018

Nikita R. Storozhenko, postgraduate student, Omsk State Technical University (Omsk, Russia)
snikr@bk.ru
ResearcherID Y-8341-2018

Viktor I. Potapov, Ph D (Doctor of Technical Science), Professor, Omsk State Technical University (Omsk, Russia)
ivt@omgtu.ru

Olga P. Shafeeva, PhD, Associate Professor, Omsk State Technical University (Omsk, Russia)
ivt_olga_pavlovna@mail.ru