

3(70)/2014

# INFORMATSIONNO- UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

REFEREED EDITION

**Founder**

«Information and Control Systems», Ltd.

**Editor-in-Chief**

M. Sergeev

Dr. Sc. Tech., Professor, St.-Petersburg, Russia

**Deputy Editor-in-Chief**

E. Krouk

Dr. Sc. Tech., Professor, St.-Petersburg, Russia

**Executive secretary**

O. Muravtsova

**Editorial Council**

L. Chubraeva

RAS Corr. Member, Dr. Sc. Tech., Professor, St. Petersburg, Russia

L. Fortuna

PhD, Professor, Catania, Italy

A. Fradkov

Dr. Sc. Tech., Professor, St. Petersburg, Russia

V. Kozlov

Dr. Sc. Tech., Professor, St. Petersburg, Russia

C. Christodoulou

PhD, Professor, Albuquerque, New Mexico, USA

B. Meyer

PhD, Professor, Zurich, Switzerland

A. Ovodenko

Dr. Sc. Tech., Professor, St. Petersburg, Russia

Y. Podoplyokin

Dr. Sc. Tech., Professor, St. Petersburg, Russia

Yu. Shokin

RAS Academician, Dr. Sc. Phys.-Math., Novosibirsk, Russia

V. Simakov

Dr. Sc. Tech., Professor, Moscow, Russia

V. Vasilev

RAS Corr. Member, Dr. Sc. Tech., Professor, St. Petersburg, Russia

R. Yusupov

RAS Corr. Member, Dr. Sc. Tech., Professor, St. Petersburg, Russia

**Editorial Board**

V. Anisimov

Dr. Sc. Tech., Professor, St. Petersburg, Russia

B. Bezruchko

Dr. Sc. Phys.-Math., Saratov, Russia

N. Blaunstein

Dr. Sc. Phys.-Math., Professor, Beer-Sheva, Israel

A. Dudin

Dr. Sc. Tech., Professor, Minsk, Belarus

V. Khimenko

Dr. Sc. Tech., Professor, St. Petersburg, Russia

G. Maltsev

Dr. Sc. Tech., Professor, St. Petersburg, Russia

V. Melekhin

Dr. Sc. Tech., Professor, St. Petersburg, Russia

A. Shalyto

Dr. Sc. Tech., Professor, St. Petersburg, Russia

A. Shepeta

Dr. Sc. Tech., Professor, St. Petersburg, Russia

A. Smirnov

Dr. Sc. Tech., Professor, St. Petersburg, Russia

Z. Yuldashev

Dr. Sc. Tech., Professor, St. Petersburg, Russia

A. Zeifman

Dr. Sc. Phys.-Math., Vologda, Russia

**Editor: A. Larionova****Proofreader:** T. Zvertanovskaia**Design:** A. Koleshko, M. Chernenko**Layout and composition:** N. Karavaeva**Contact information**

The Editorial and Publishing Center, SUAI

67, B. Morskaia, 190000, St. Petersburg, Russia

Website: <http://i-us.ru/en>, E-mail: [ius.spb@gmail.com](mailto:ius.spb@gmail.com)

Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation. Registration Certificate JD № 77-12412 from April, 19, 2002. Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder: «Information and Control Systems», Ltd., JD № FS77-49181 from March, 30, 2012.

The journal is distributed by subscription. Subscription can be made in the Editorial and publishing center, SUAI as well as in any post office based on «Rospechat» catalogue: № 48060 — annual subscript, № 15385 — semiannual subscript.

© Corporate authors, 2014

**INFORMATION AND CONTROL SYSTEMS**

**Viktorov D. S., Chislov S. G.** Method of Correction of the Non-Linear Distortions Entered by an Analog Key in Probing Signals 2

**Turubanov M. A., Shishlakov V. F., Shyshlakov A. V.** Impulse Control System for Combined Solar and Wind Installation with Superconductor Equipment 8

**Zakharova O. L., Kirsanova J. A., Kniga E. V., Zharinov I. O.** Algorithms and Software of Testing Onboard Digital Computer Systems Integrated Modular Avionics 19

**SYSTEM AND PROCESS MODELING**

**Kuchmin A. Yu.** Modeling of Equivalent Stiffness of Adaptive Platforms with the Parallel Structure Executive Mechanism 30

**HARDWARE AND SOFTWARE RESOURCES**

**Balonin N. A., Marley V. E., Sergeev M. B.** New Opportunities of the Mathematical Network for Collaborative Research and Modeling in the Internet 40

**Marakhovsky V. B.** CMOS Implementation of the Trainee's Threshold Logical Element. Part I. Design and Training Diagram 47

**Kolchin I. V., Filippov S. N.** The Architecture of Bare-Metal Real-Time Microhypervisor and Automated Measurement of Time Response 57

**Shoshmina I. V.** A Methodology of Eliciting Context Requirements to Program Logic Control Systems 68

**INFORMATION SECURITY**

**Bezzateev S. V., Voloshina N. V., Sankin P. S.** Safety Analysis Methodology of Complex Systems Taking Into Account the Threats to Information Security 78

**Boyko A. A., Djakova A. V.** Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools 84

**INFORMATION CODING AND TRANSMISSION**

**Cheprukov Yu. V., Socolov M. A.** Correlation Characteristics and Application of Some Binary Codes 93

**Alekseev M. O.** On the Detection of Algebraic Manipulations by Means of Multiplication Operation 103

**INFORMATION AND MEASURING SYSTEMS**

**Allakhverdiyeva N. R.** Development of a Method for Improving the Accuracy of the Measuring Channel 109

**INFORMATION INSTRUMENTATION AND EDUCATION**

**D'yachuk P. P., Loginov D. A., Karabalykov S. A.** Synergetic Approach to Management of Educational Activity in Verbal Problem Environments 118

**CONTROL IN MEDICAL AND BIOLOGICAL SYSTEMS**

**Tichonov E. P.** Adaptive Filtering Algorithms Electrocardiogram High Time Resolution Part I. Background Information and Analysis Approach to Solving the Problem 125

**CHRONICLES AND INFORMATION**

**IV International Forum «TELECOM NETWORKS 2.0. Sharing, Engineering, Outsourcing, Development & Metering»** 132

**INFORMATION ABOUT THE AUTHORS**

134

Submitted for publication 07.04.14. Passed for printing 17.06.14. Format 60×84/8. Offset paper. Phototype SchoolBookC. Offset printing.

Layout original is made at the Editorial and Publishing Center, SUAI.  
67, B. Morskaia, 190000, St. Petersburg, Russia  
Printed from slides at the Editorial and Publishing Center, SUAI.  
67, B. Morskaia, 190000, St. Petersburg, Russia

Учредитель  
ООО «Информационно-управляющие системы»

Главный редактор  
М. Б. Сергеев,  
д-р техн. наук, проф., С.-Петербург, РФ

Зам. главного редактора  
Е. А. Крук,  
д-р техн. наук, проф., С.-Петербург, РФ

Ответственный секретарь  
О. В. Муравцова

Редакционный совет:  
Председатель А. А. Оводенко,  
д-р техн. наук, проф., С.-Петербург, РФ  
В. Н. Васильев,  
чл.-корр. РАН, д-р техн. наук, проф., С.-Петербург, РФ  
В. Н. Козлов,  
д-р техн. наук, проф., С.-Петербург, РФ  
К. Кристоделу,  
д-р наук, проф., Альбукерке, Нью-Мексико, США  
Б. Мейер,  
д-р наук, проф., Цюрих, Швейцария  
Ю. Ф. Подоплекин,  
д-р техн. наук, проф., С.-Петербург, РФ  
В. В. Симаков,  
д-р техн. наук, проф., Москва, РФ  
Л. Фортуна,  
д-р наук, проф., Катания, Италия  
А. Л. Фрадков,  
д-р техн. наук, проф., С.-Петербург, РФ  
Л. И. Чубраева,  
чл.-корр. РАН, д-р техн. наук, С.-Петербург, РФ  
Ю. И. Шокин,  
акад. РАН, д-р физ.-мат. наук, проф., Новосибирск, РФ  
Р. М. Юсупов,  
чл.-корр. РАН, д-р техн. наук, проф., С.-Петербург, РФ

Редакционная коллегия:  
В. Г. Анисимов,  
д-р техн. наук, проф., С.-Петербург, РФ  
Б. П. Безручко,  
д-р физ.-мат. наук, проф., Саратов, РФ  
Н. Блаунштейн,  
д-р физ.-мат. наук, проф., Беэр-Шева, Израиль  
А. Н. Дудин,  
д-р физ.-мат. наук, проф., Минск, Беларусь  
А. И. Зейфман,  
д-р физ.-мат. наук, проф., Вологда, РФ  
Г. Н. Мальцев,  
д-р техн. наук, проф., С.-Петербург, РФ  
В. Ф. Мелехин,  
д-р техн. наук, проф., С.-Петербург, РФ  
А. В. Смирнов,  
д-р техн. наук, проф., С.-Петербург, РФ  
В. И. Хименко,  
д-р техн. наук, проф., С.-Петербург, РФ  
А. А. Шалыто,  
д-р техн. наук, проф., С.-Петербург, РФ  
А. П. Шепета,  
д-р техн. наук, проф., С.-Петербург, РФ  
З. М. Юлдашев,  
д-р техн. наук, проф., С.-Петербург, РФ

Редактор: А. Г. Ларионова  
Корректор: Т. В. Звертановская  
Дизайн: А. Н. Колешко, М. Л. Черненко  
Компьютерная верстка: Н. Н. Караваева

Адрес редакции: 190000, Санкт-Петербург,  
Б. Морская ул., д. 67, ГУАП, РИЦ  
Тел.: (812) 494-70-02, e-mail: ius.spb@gmail.com, сайт: http://i-us.ru

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.  
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.  
Перерегистрирован в Роскомнадзоре.  
Свидетельство о регистрации ПИ № ФС77-49181 от 30 марта 2012 г.

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук».

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогу «Роспечать»: № 48060 — годовой индекс, № 15385 — полугодовой индекс.

© Коллектив авторов, 2014

**ОБРАБОТКА ИНФОРМАЦИИ И УПРАВЛЕНИЕ**

**Викторов Д. С., Числов С. Г.** Метод коррекции нелинейных искажений, вносимых аналоговым ключом в зондирующие сигналы 2

**ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ**

**Турубанов М. А., Шишлаков В. Ф., Шишлаков А. В.** Импульсная система управления комбинированной солнечно- и ветроэнергетической установкой со сверхпроводниковым оборудованием 8  
**Захарова О. Л., Кирсанова Ю. А., Книга Е. В., Жаринов И. О.** Алгоритмы и программные средства тестирования бортовых цифровых вычислительных систем интегрированной модульной авионики 19

**МОДЕЛИРОВАНИЕ СИСТЕМ И ПРОЦЕССОВ**

**Кучмин А. Ю.** Моделирование эквивалентной жесткости адаптивных платформ с исполнительными механизмами параллельной структуры 30

**ПРОГРАММНЫЕ И АППАРАТНЫЕ СРЕДСТВА**

**Балонин Н. А., Марлей В. Е., Сергеев М. Б.** Новые возможности математической сети для коллективных исследований и моделирования в Интернете 40  
**Мараховский В. Б.** КМОП-реализация обучаемого порогового логического элемента. Часть 1: Проектирование и схема обучения 47  
**Колчин И. В., Филиппов С. Н.** Архитектура автономного микро-гипервизора реального времени и автоматизированное измерение его временных характеристик 57  
**Шошмина И. В.** Методика составления контекстных требований к программным системам логического управления 68

**ЗАЩИТА ИНФОРМАЦИИ**

**Беззатеев С. В., Волошина Н. В., Санкин П. С.** Методика расчета надежности сложных систем, учитывающая угрозы информационной безопасности 78  
**Бойко А. А., Дьякова А. В.** Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств 84

**КОДИРОВАНИЕ И ПЕРЕДАЧА ИНФОРМАЦИИ**

**Чепруков Ю. В., Соколов М. А.** Корреляционные характеристики и применение некоторых бинарных R3-кодов 93  
**Алексеев М. О.** Об обнаружении алгебраических манипуляций с помощью операции умножения 103

**ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ СИСТЕМЫ**

**Аллахвердиева Н. Р.** Разработка метода повышения точности измерительного канала 109

**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ОБРАЗОВАНИЕ**

**Дьячук П. П., Логинов Д. А., Карабалыков С. А.** Синергетический подход к управлению учебной деятельностью в вербальных проблемных средах 118

**УПРАВЛЕНИЕ В МЕДИЦИНЕ И БИОЛОГИИ**

**Тихонов Э. П.** Адаптивные алгоритмы фильтрации и фрагментации электрокардиограмм высокого временного разрешения. Часть 1: Исходные сведения и анализ подхода к решению проблемы 125

**ХРОНИКА И ИНФОРМАЦИЯ**

**IV Международный Форум «TELECOM NETWORKS 2.0. Sharing, Engineering, Outsourcing, Development & Metering»** 132

**СВЕДЕНИЯ ОБ АВТОРАХ**

134

Сдано в набор 07.04.14. Подписано в печать 17.06.14. Формат 60×84/8. Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная. Усл. печ. л. 16,0. Уч.-изд. л. 20,1. Тираж 1000 экз. Заказ 258.

Оригинал-макет изготовлен в редакционно-издательском центре ГУАП. 190000, Санкт-Петербург, Б. Морская ул., 67.

Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП. 190000, Санкт-Петербург, Б. Морская ул., 67.

УДК 004.05

# СПОСОБ РАЗРАБОТКИ ТЕСТОВЫХ УДАЛЕННЫХ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ НА ПРОСТРАНСТВЕННО РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СРЕДСТВ

А. А. Бойко<sup>а</sup>, канд. техн. наук, доцент

А. В. Дьякова<sup>а</sup>, научный сотрудник

<sup>а</sup>Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия им. профессора Н. Е. Жуковского и Ю. А. Гагарина», Воронеж, РФ

**Постановка проблемы:** при разработке и эксплуатации пространственно распределенных систем информационно-технических средств особое значение имеет оценка устойчивости их функционирования в условиях удаленных информационно-технических воздействий со стороны злоумышленника. Несовершенство известных подходов к разработке таких воздействий не позволяет анализировать реакцию информационно-технических средств на полное множество факторов, комплексно нарушающих точность и своевременность обрабатываемых ими сообщений. Эффективным путем решения данной проблемы является генерация тестовых информационно-технических воздействий на базе формализации процессов функционирования исследуемого объекта. **Методы:** создание формальных моделей пространственно распределенной системы информационно-технических средств и автоматическая генерация на их основе полного множества тестовых удаленных информационно-технических воздействий. **Результаты:** предложена теоретико-множественная модель функционирования пространственно распределенной системы информационно-технических средств в виде комплекса локальных алгоритмов, взаимодействующих в рамках единого распределенного алгоритма посредством асинхронного обмена сообщениями. На базе модели предложен способ, обеспечивающий разработку на основе общедоступной спецификации алгоритмов функционирования информационно-технических средств полного множества тестовых удаленных информационно-технических (программных и электромагнитных) воздействий. Суть способа заключается в фиксации в каждом локальном алгоритме каждого информационно-технического средства множества состояний, непосредственно использующих неделимые элементы данных или характеристики электромагнитных или электрических сигналов, полученные от всех локальных алгоритмов других информационно-технических средств; определении для каждого из этих состояний множества конечных цепочек из состояний локальных алгоритмов, описывающих путь прохождения одинаковых элементов данных или сигналов от состояния, в котором они возникли (получены), до состояния, в котором они используются; выделении для каждого зафиксированного состояния множества тех цепочек, которые содержат используемые в нем элементы данных или характеристики сигнала, и определении для каждого выделенного множества цепочек тестовых удаленных информационно-технических воздействий, учитывающих потенциально реализуемые наборы взаимосвязанных факторов, влияющих на точность и своевременность сообщений. **Практическая значимость:** впервые получена возможность анализировать реакцию существующих и разрабатываемых информационно-технических средств пространственно распределенных систем на все потенциально возможные наборы факторов, комплексно нарушающих точность и своевременность обрабатываемых этими средствами сообщений.

**Ключевые слова** — распределенный алгоритм, удаленное информационно-техническое воздействие, информационно-техническое средство.

## Введение

В процессе разработки и эксплуатации пространственно распределенных систем информационно-технических средств (ИТС), к которым относятся радиоэлектронные средства, средства вычислительной техники и их комбинации друг с другом и с другими классами технических средств, особое значение имеет оценка устойчивости функционирования этих средств и систем в целом в условиях удаленных информационно-технических воздействий (ИТВ) со стороны злоумышленника. Для обеспечения достоверности результатов такой оценки необходимо решить задачу разработки полного множества тестовых удаленных ИТВ для потенциально доступной злоумышленнику информации об алгоритмах функционирования ИТС системы.

С учетом ГОСТов [1, 2] в настоящей работе под ИТВ будем понимать последовательность дей-

ствий по формированию совокупности факторов, нацеленной на нарушение конфиденциальности, целостности и (или) доступности обрабатываемой ИТС информации и (или) алгоритмов, и (или) электронных компонентов и (или) схем ее обработки и достаточной для реализации с использованием электромагнитных полей и (или) электрических токов некоторого условия функционирования ИТС, при выполнении которого это средство переходит в состояние потери работоспособности, сниженной эффективности функционирования, управляемости или доступности для углубленного анализа источником воздействия. К ИТВ будем относить программные и электромагнитные воздействия. Их различие в том, что воздействующим фактором в первом случае является полученная после выделения из электромагнитных или электрических сигналов совокупность цифровых данных, являющихся исходными для алгоритмов функционирования

ИТС, а во втором случае — электромагнитный или электрический сигнал, несущий исходные данные для алгоритмов функционирования ИТС только в своих амплитудных, частотных, фазовых, временных и пространственных характеристиках. С позиции эталонной модели взаимодействия открытых систем (ЭМОС) электромагнитные воздействия применяют на физическом уровне, а программные воздействия — на вышестоящих шести уровнях, используя физический уровень в качестве среды доставки воздействующего фактора.

На сегодняшний день для разработки тестовых ИТВ применяются следующие подходы:

1) эмпирический — основан на предположении аналитиками уязвимостей в ИТС и проверке этих предположений путем формирования и реализации соответствующих тестовых ИТВ;

2) феноменологический — основан на накоплении фактов проявления уязвимостей в процессе функционирования ИТС и разработке соответствующих тестовых ИТВ, реализующих эти уязвимости;

3) использование аналогий — основан на анализе доступных баз данных с уязвимостями ИТС и реализующими их тестовыми ИТВ и выборе в этих базах данных подходящих тестовых ИТВ для исследуемой системы [3];

4) тестирование реализации — основан на разработке возможных тестовых ИТВ для текущей реализации ИТС, содержащих входные данные, сформированные по установленным правилам в целях обнаружения ошибок в этой реализации [4, 5];

5) проверка на модели — основан на представлении процесса функционирования ИТС в виде дискретно-событийной модели, в наборе состояний которой выделяется подмножество нештатных состояний [6]. Проверка сводится к формализации требований к функционированию ИТС и попытке доказательства того, что подмножество нештатных состояний не является пустым. Если это подмножество не пустое, то предлагаются тестовые ИТВ, реализующие нештатные состояния;

6) генерация на основе модели — основан на таком стиле разработки ИТС, когда итерационно создается программная реализация его математической модели и автоматически генерируются программный код и тестовые ИТВ для проверки корректности кода [7].

Для решения указанной задачи первых двух подходов недостаточно, поскольку первый опирается на безупречный человеческий фактор, а второй в течение длительного времени может не показать большей части уязвимостей. Третий подход ориентирован на поиск в ИТС известных уязвимых элементов. С его применением решить указанную задачу возможно лишь в том случае,

когда ИТС состоит только из известных элементов. Четвертый подход сегодня достаточно глубоко проработан для алгоритмов функционирования программного и технического обеспечения ИТС с единственным потоком управления. Для случая распределенного многопоточного взаимодействия ИТС используется пятый подход. Однако его применение связано со сложностью определения состояний и формализации требований. Данные действия производятся эмпирически, и даже квалифицированный аналитик при работе с некоторым элементом локального алгоритма функционирования ИТС способен пропустить целый класс состояний или важное требование к корректности этого элемента. Шестым подходом пользуются крайне редко, поскольку затраты только на его внедрение и создание программной реализации математической модели ИТС соизмеримы с затратами на разработку всего ИТС без модели. Поэтому на практике в подавляющем большинстве случаев для решения поставленной задачи реализуются комбинации первых четырех подходов, а адекватность их применения проверяется только временем.

Такое положение дел для пространственно распределенных систем ИТС не является удовлетворительным, поскольку уязвимости в них могут проявляться при различных сочетаниях удаленно воздействующих деструктивных факторов, комплексно влияющих на точность и своевременность обрабатываемых ИТС сообщений, а использование хотя бы одной из таких уязвимостей способно привести к критичным последствиям для системы и ее пользователей. В первую очередь это касается систем, для обеспечения возможности установления информационного взаимодействия с которыми общедоступна спецификация их алгоритмов.

Цель работы — создание способа, обеспечивающего разработку полного множества тестовых удаленных ИТВ на пространственно распределенные системы ИТС на основе общедоступной спецификации их алгоритмов функционирования путем учета всех наборов взаимосвязанных факторов, комплексно нарушающих точность и своевременность обрабатываемых ИТС сообщений.

### **Модель функционирования пространственно распределенной системы ИТС**

В основе предлагаемого способа лежит модель функционирования пространственно распределенной системы ИТС, базирующаяся на следующих основных положениях:

1) функционирование ИТС представляется в виде комплекса локальных алгоритмов, взаи-

мосвязанных единым распределенным алгоритмом функционирования системы, включающей эти ИТС. Способ ориентирован на программные и электромагнитные воздействия, так как в виде алгоритма представляется функционирование ИТС на всех уровнях ЭМВОС;

2) взаимодействие ИТС рассматривается с позиции обмена сообщениями, под которыми понимается как совокупность цифровых данных, так и электромагнитный (в том числе отраженный) или электрический сигнал. Передача сообщений между ИТС является асинхронной, поскольку синхронный обмен сообщениями в общем случае является разновидностью асинхронного обмена [8].

По мнению авторов, наиболее полные определения локального и распределенного алгоритмов на сегодняшний день приведены в работе [9]. Однако в интересах достижения цели работы определение локального алгоритма требует дополнительного учета потоков управления и данных [5], а определение распределенного алгоритма требует следующих уточнений:

1) каждый локальный алгоритм в некотором состоянии распределенного алгоритма может находиться только в одном состоянии;

2) в структуре множества переходов распределенного алгоритма рассматриваются только те переходы локальных алгоритмов, которые связаны с событиями передачи и приема сообщений и тем самым способны оказать влияние на другие локальные алгоритмы.

Исходя из этого в настоящей работе предлагаются следующие теоретико-множественные определения локального и распределенного алгоритмов.

*Определение 1.* Локальным алгоритмом будем называть семерку вида

$$al = (Z, I, \vdash^i, \vdash^s, \vdash^r, AP, L), \quad (1)$$

где  $Z$  — конечное непустое множество состояний;  $I$  — множество начальных состояний;  $\vdash^i$  — отношение на множестве  $Z \times Z$ ;  $\vdash^s$  и  $\vdash^r$  — отношения на множестве  $Z \times \Xi \times Z$ ,  $\Xi = \{m_\xi\}; \xi = 1..|\Xi|$  — конечное непустое множество сообщений с уникальной семантикой;  $AP$  — конечное непустое множество атомарных предикатов, соответствующих всем возможным неделимым элементам данных или характеристикам сигналов, используемым локальным алгоритмом в ходе его выполнения;  $L: Z \rightarrow 2^{AP}$  — функция меток состояний (сообщений), сопоставляющая каждому состоянию (сообщению) локального алгоритма множество истинных в нем атомарных предикатов и показывающая, какие неделимые элементы данных или характеристики сигналов в этом состоянии обрабатываются или ожидают обработки (или в этом сообщении передаются). Отношения  $\vdash^i$ ,  $\vdash^s$  и  $\vdash^r$  пред-

ставляют переходы между состояниями, связанные с внутренними событиями, передачей и приемом сообщений соответственно. Отношение  $\vdash$  на  $Z$  определяется соотношением

$$\forall z \in Z \left( \begin{array}{l} (z \vdash z' \Leftrightarrow \langle z, z' \rangle \in \vdash^i) \vee \\ \vee \exists m_\xi \in \Xi (\langle z, m_\xi, z' \rangle \in \vdash^s \cup \vdash^r) \end{array} \right), \quad (2)$$

где  $\langle \dots \rangle$  — упорядоченное множество.

Сообщение описывается следующим образом:

$$\begin{aligned} L(m_\xi) &= \{\varphi_{\xi, v}\}; \varphi_{\xi, v} \in AP_\xi; \\ AP_\xi &\subseteq AP; v \in 1..|AP_\xi|, \end{aligned} \quad (3)$$

где  $\varphi_{\xi, v}$  —  $v$ -й предикат, передаваемый в  $\xi$ -м сообщении;  $AP_\xi$  — множество предикатов, передаваемых в  $\xi$ -м сообщении;  $|\dots|$  — обозначение числа элементов множества.

Распределенный алгоритм  $R$  функционирования системы ИТС описывает процесс взаимодействия локальных алгоритмов, которые выполняются на  $S$  входящих в эту систему ИТС и  $S'$  ИТС других распределенных систем, с которыми может взаимодействовать распределенная система, по схеме  $1 : s$ , ( $j = 1..|AL_s|, AL_s \subseteq AL, s = 1..|S| + |S'|$ ).

*Определение 2.* Распределенным алгоритмом будем называть четверку вида

$$R = (C, \rightarrow, I, \Xi), \quad (4)$$

где  $C = \{c_r\}; r = 1..|C|$  — конечное непустое множество состояний в  $R$ ;  $\rightarrow = \{\langle C_{g'}, C_{g'} \rangle\} \cup \{\langle C_v, C_{v'} \rangle\}$ ,  $g, g', v, v' \leq r, g \neq g', v \neq v'$  — конечное непустое множество прямых  $\{\langle C_{g'}, C_{g'} \rangle\}$  и опосредованных  $\{\langle C_v, C_{v'} \rangle\}$  переходов между состояниями  $R$ ;  $I = \{c_{g''}\}; g'' < r$  — конечное множество начальных состояний  $R$ , в которые нет переходов;  $\Xi$  — конечное непустое множество сообщений с уникальной семантикой.

Каждое состояние в  $R$  является совокупностью таких состояний всех локальных алгоритмов всех ИТС, для которых одному состоянию, предшествующему некоторому исходящему сообщению одного локального алгоритма одного ИТС с некоторой семантикой, соответствует множество состояний множества локальных алгоритмов множества ИТС, получивших сообщение с той же семантикой. При этом один и тот же локальный алгоритм в некотором ИТС не может передавать сообщение себе.

Элементы  $C$  предлагается описывать следующим образом:

$$\begin{aligned} c_r &= (z_{s, j, k}, \{z_{s', j', k'}\}, m_\xi): \\ &\left( \begin{array}{l} \forall s, s' = 1..|S| + |S'|, \forall j, j', h = 1..|AL_s|, \\ \forall k, k' = 1..|Z_{s, j}|, \forall m_\xi \in \Xi \end{array} \right) \end{aligned}$$

$$\left( \begin{aligned} & \langle z_{s,j,k}, m_{\xi}, z'_{s',j,k} \rangle \in \vdash^s \wedge \\ & \langle \wedge \langle z_{s',j',k'}, m_{\xi}, z'_{s',j',k'} \rangle \in \vdash^r \rangle, \\ & ((al_{s,j} \neq al_{s,h}) \wedge (j \neq h)), \\ & (z_{s,j,k} \in Z_{s,j}), (z_{s,j,k} \neq z'_{s',j',k'}) \wedge \\ & \wedge (s = s') \wedge (j = j') \end{aligned} \right). \quad (5)$$

Из некоторого состояния  $R$  существует прямой переход во все состояния  $R$ , у которых состояния локальных алгоритмов, порождающие исходящие сообщения, без промежуточных входящих сообщений следуют за состоянием, порождающим исходящие сообщения в данном состоянии  $R$ , или состояниями, получившими входящее сообщение в данном состоянии  $R$ . Прямой переход предлагается описывать следующим образом:

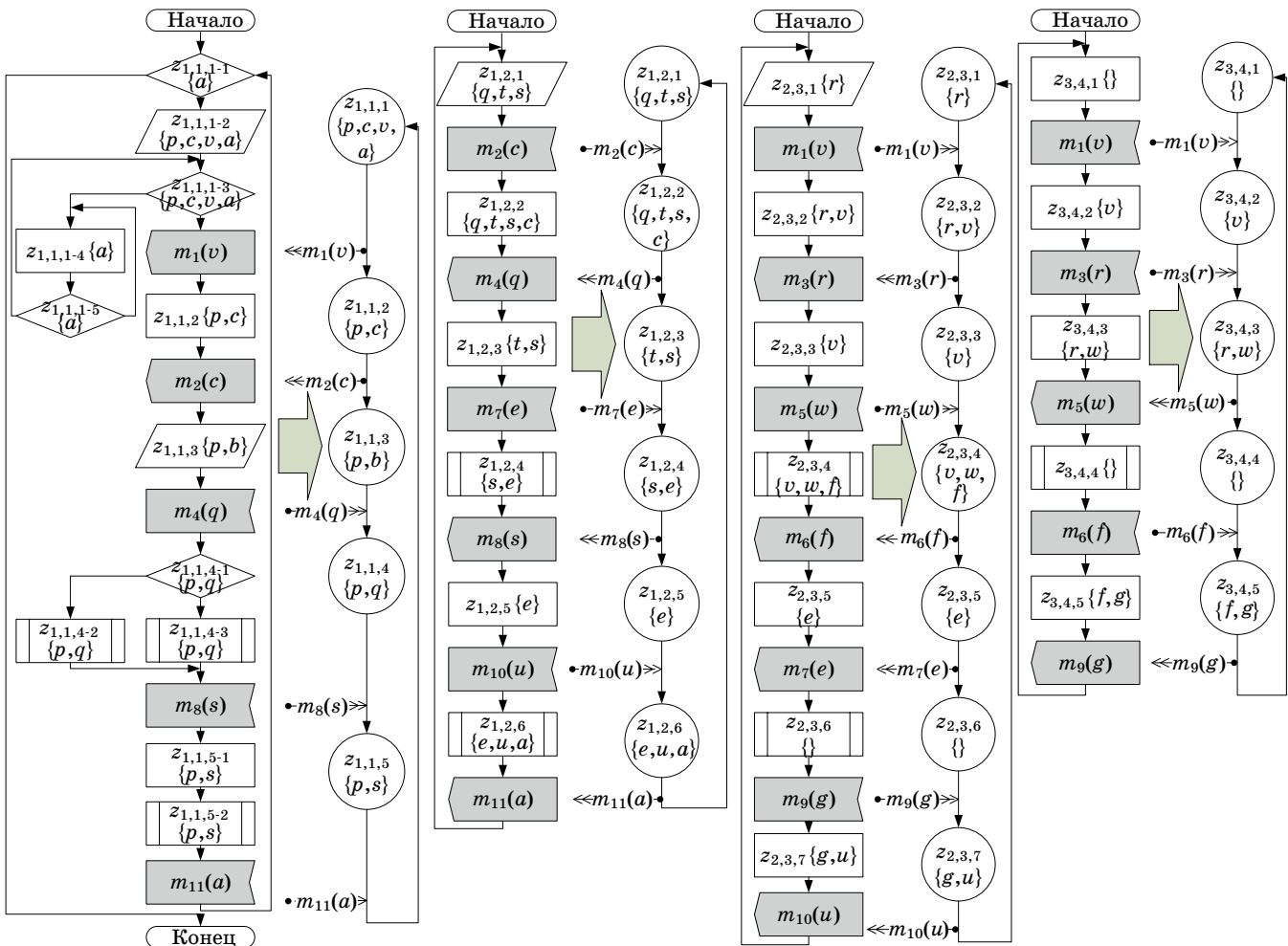
$$\begin{aligned} & \langle C_g, C_{g'} \rangle_l = \\ & = \langle z_{s,j,k}, \{z_{s',j',k'}\}, m_{\xi}, \{\hat{z}_{\hat{s},\hat{j},\hat{k}}, \{\hat{z}_{\hat{s}',\hat{j}',\hat{k}'}\}, m_{\xi}\} \rangle: \\ & \left( \forall s, \hat{s}, s' = 1..|S| + |S'|, \forall j, \hat{j}, j' = 1..|AL_s|, \right) \end{aligned}$$

$$\forall k, \hat{k}, k' = 1..|Z_{s,j}|, \forall \xi, \hat{\xi} = 1..|\Xi|$$

$$\left( (s = \hat{s}) \wedge (j = \hat{j}) \wedge \left( \langle z_{s,j,k}, m_{\xi}, \hat{z}_{\hat{s},\hat{j},\hat{k}} \rangle \in \vdash^s \right) \vee \vee \left( (s' = \hat{s}') \wedge (j' = \hat{j}') \wedge \left( \langle z_{s',j',k'}, m_{\xi}, \hat{z}_{\hat{s}',\hat{j}',\hat{k}'} \rangle \in \vdash^r \right) \right) \right). \quad (6)$$

Из некоторого состояния  $R$  существует опосредованный переход во все состояния  $R$ , у которых состояния локальных алгоритмов, порождающие исходящие сообщения, через одно входящее сообщение следуют за состоянием, порождающим исходящие сообщения в данном состоянии  $R$ , или состояниями, получившими входящее сообщение в данном состоянии  $R$ . Опосредованный переход описывается следующим образом:

$$\begin{aligned} & \langle C_v, C_{v'} \rangle_f = \\ & = \langle z_{s,j,k}, \{z_{s',j',k'}\}, m_{\xi}, \{\hat{z}_{\hat{s},\hat{j},\hat{k}}, \{\hat{z}_{\hat{s}',\hat{j}',\hat{k}'}\}, m_{\xi}\} \rangle: \\ & \left( \forall s, \hat{s}, \hat{s}' = 1..|S| + |S'|, \forall j, \hat{j}, \hat{j}' = 1..|AL_s|, \right) \\ & \left( \forall k, \hat{k}, \hat{k}' = 1..|Z_{s,j}|, \forall \xi, \xi' = 1..|\Xi| \right) \end{aligned}$$



■ Рис. 1. Редукция локальных алгоритмов распределенной системы

$$\left( \begin{array}{l} (s = \hat{s} = \hat{s}) \wedge (j = \hat{j} = \hat{j}) \wedge \\ \wedge ((z_{s,j,k}, m_{\xi}, \hat{z}_{\hat{s},\hat{j},\hat{k}}) \in \vdash^s) \wedge \\ \wedge ((\hat{z}_{\hat{s},\hat{j},\hat{k}}, m_{\xi'}, \hat{z}_{\hat{s},\hat{j},\hat{k}}) \in \vdash^r) \vee \\ \vee ((s = \hat{s}) \wedge (j = \hat{j}) \wedge \\ \wedge ((z_{s',j',k'}, m_{\xi'}, \hat{z}_{\hat{s},\hat{j},\hat{k}}) \in \vdash^r) \end{array} \right). \quad (7)$$

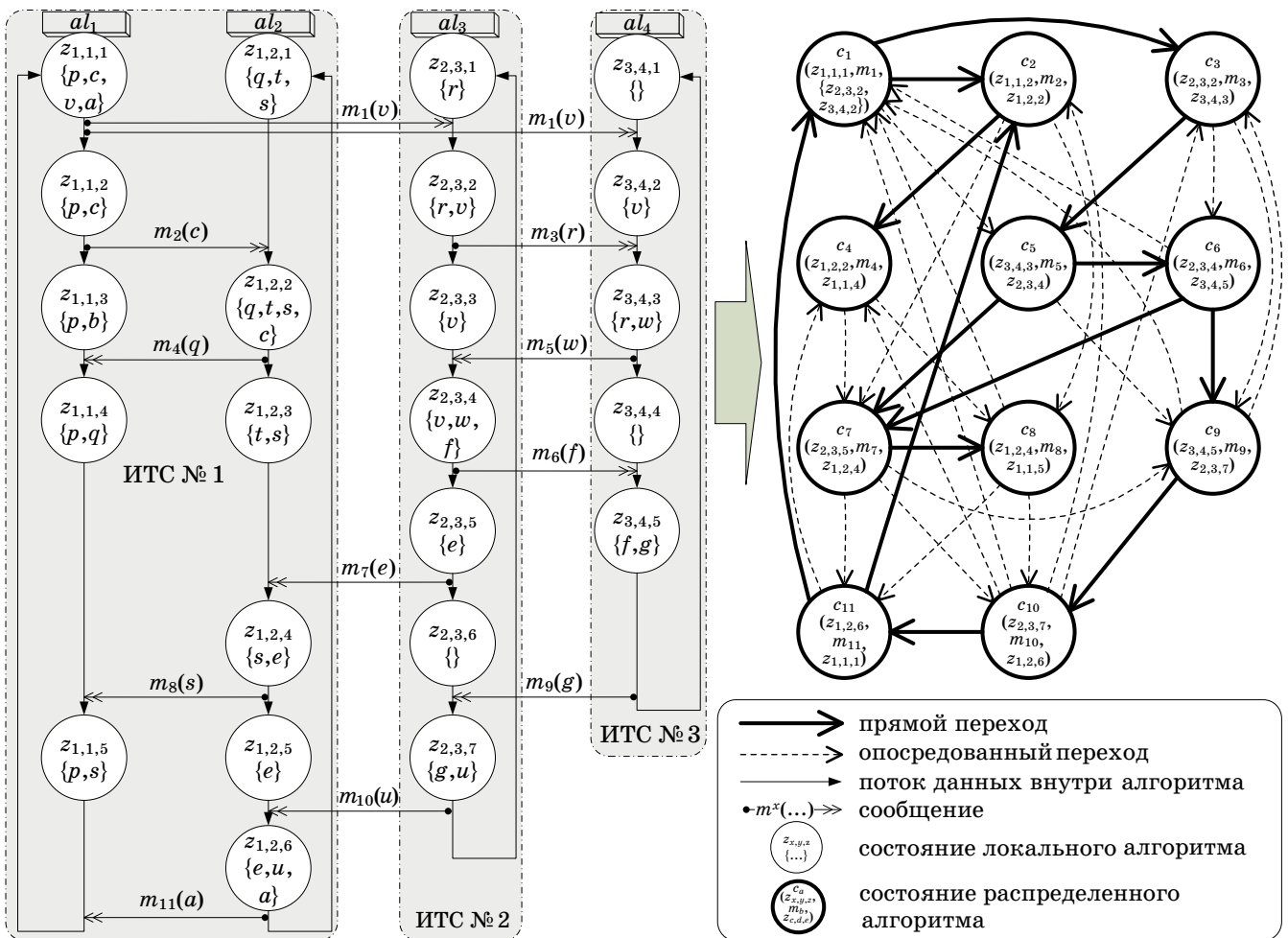
Для определения элементов состояний распределенного алгоритма локальные алгоритмы предлагается представлять в редуцированной форме. Редукция предлагается производить по правилу: каждая последовательность элементов локального алгоритма, начинающаяся после приема (передачи) сообщения и заканчивающаяся перед приемом (передачей) сообщения, заменяется соответствующим этой последовательности состоянием. Редукция локальных алгоритмов распределенной системы, включающей три ИТС, представлена на рис. 1.

В этой системе два локальных алгоритма выполняются в ИТС № 1 и по одному —

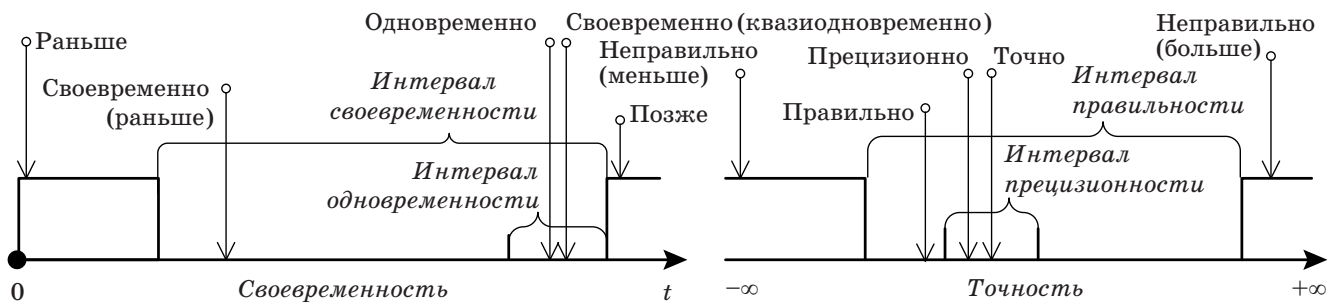
в ИТС № 2 и ИТС № 3. В блоках и узлах схем и полученных из них графов на рис. 1 показаны идентификаторы состояний локальных алгоритмов ИТС (например,  $z_{1,1,1-2}$ ) и в фигурных скобках приведены перечни соответствующих этим состояниям атомарных предикатов (для  $z_{1,1,1-2}$  это  $\{p,c,v,a\}$ ). Взаимодействие локальных алгоритмов в рассматриваемой системе и соответствующий этой системе распределенный алгоритм показаны на рис. 2.

Факторы удаленного ИТВ с позиции нарушения конфиденциальности, целостности и (или) доступности обрабатываемой ИТС информации способны влиять на две характеристики сообщений (рис. 3):

1) своевременность, когда сообщения могут приниматься локальными алгоритмами в течение интервала своевременности (с момента начала ожидания поступления легитимного сообщения от легитимного локального алгоритма до начала интервала одновременности, в течение которого принимается легитимное сообщение и приемное устройство все принятые сообщения



■ Рис. 2. Распределенная система ИТС и ее распределенный алгоритм



■ Рис. 3. Варианты передачи сообщения с учетом влияния факторов ИТВ

рассматривает как одно), раньше или позже него. При раннем приеме сообщения получивший его локальный алгоритм преждевременно переходит к последующим состояниям, в которых он отправит сообщение или будет ожидать поступления других сообщений. В случае отправки сообщения локальному алгоритму, сообщение от которого скомпрометировало ИТВ, он не будет готов к приему. В случае ожидания сообщения от локального алгоритма, сообщение от которого скомпрометировало ИТВ, сообщение от него не поступит. В иных случаях принявший ранее сообщение локальный алгоритм будет выполняться с учетом данных или характеристик сигналов, заданных злоумышленником. Ранний прием может быть инициирован многократно в целях непредусмотренного расходования ресурсов ИТС. Поздний прием, равно как и невозможность приема, ожидающий локальный алгоритм воспримет как сбой, а поступление легитимного и нелегитимного сообщений в интервале одновременности — как ошибку на физическом уровне ЭМВОС;

2) точность передаваемых в сообщениях данных или характеристик сигналов, которые, согласно работам [4, 5], могут быть точными, больше, меньше граничных значений, равны им, а согласно ГОСТу [10], могут также быть прецизионными (входят в интервал прецизионности) или правильными (не в интервале прецизионности, но входят в интервал правильности). Получение данных или характеристик сигналов за границами интервала правильности локальный алгоритм воспримет как сбой. Прецизионные данные или характеристики сигналов незаметно способны внести существенные погрешности в вычисления, выполняемые локальным алгоритмом и системой в целом, а правильные способны дезориентировать локальный алгоритм и систему вплоть до применения ИТС во вред его системе и (или) пользователям.

Временная характеристика факторов ИТВ определяется попаданием в следующие интервалы времени:

1) «своевременно» ( $\Delta t_{\circ} = [t(m_{\xi}), t(m_{\xi}) + \Delta t_{\min}]$ ) — с момента  $t(m_{\xi})$  фиксации передачи сообщения

в одном из состояний распределенного алгоритма, из которого существует прямой переход в состояние распределенного алгоритма, передача сообщения которого рассматривается, до момента окончания минимально необходимого временного интервала  $\Delta t_{\min}$ , затрачиваемого на отправку сообщения в системе;

2) «раньше» ( $\Delta t_{>} = [t(m_{\xi}'), t(m_{\xi}'')]$ ) — с момента  $t(m_{\xi}')$  фиксации передачи сообщения в состоянии распределенного алгоритма, из которого существует опосредованный переход в состояние, в котором передается рассматриваемое сообщение, до момента  $t(m_{\xi}'')$  фиксации передачи сообщения в состоянии распределенного алгоритма, из которого существует прямой переход в состояние с передачей рассматриваемого сообщения;

3) «позже» ( $\Delta t_{<} = [t(m_{\xi}'''), t(m_{\xi}''') + \Delta t_{\text{wait}}]$ ) — с момента  $t(m_{\xi}''')$  фиксации передачи сообщения в одном из состояний распределенного алгоритма, из которого существует прямой переход в состояние с передачей рассматриваемого сообщения, до момента окончания интервала  $\Delta t_{\text{wait}}$ , в течение которого сообщение в ИТС ожидается.

### Содержание способа

С учетом того, что злоумышленник с использованием удаленных ИТВ может комбинированно влиять на точность и своевременность сообщений в состояниях и опосредованных переходах распределенного алгоритма, предлагаемый способ разработки тестовых удаленных ИТВ на пространственно распределенные системы ИТС состоит в выполнении следующей последовательности действий.

**Шаг 1.** Выполняется построение множества локальных алгоритмов для всех ИТС системы.

**Шаг 2.** Выполняется редукция локальных алгоритмов.

**Шаг 3.** Выполняется построение распределенного алгоритма.

**Шаг 4.** Фиксируется в каждом локальном алгоритме каждого ИТС множество состояний  $\Psi_{s,j} = \{z_{s,j,q}\}$ , непосредственно использующих неделимые элементы данных или характеристики



сигналов, полученные от всех локальных алгоритмов других ИТС. Элементы этого множества предлагается определять следующим образом:

$$\left( \begin{array}{l} \forall s' \neq s : s, s' = 1..|S| + |S'|, \forall m_\xi \in \Xi, \\ \forall j, j' = 1..|AL_s|, \forall q, k, k', l, l' = 1..|Z_{s,j}| \\ \exists z_{s,j,q} \in Z_{s,j} : \\ \left( L(z_{s,j,q}) \cap L(m_\xi) \neq \emptyset \right) \wedge \\ \wedge \left( \langle z_{s',j',k'}, m_\xi, z_{s,j,k} \rangle \in \Gamma^r \right) \wedge \\ \wedge \left( \langle z_{s,j,k}, z_{s,j,l}, \dots, \langle z_{s,j,l'}, z_{s,j,q} \rangle \in \Gamma^i \right) \end{array} \right). \quad (8)$$

**Шаг 5.** Определяется для каждого состояния, зафиксированного на шаге 4, множество конечных цепочек из состояний локальных алгоритмов. Цепочка описывает путь прохождения одинаковых данных или сигналов от состояния, в котором они возникли (получены), до состояния, в котором они используются, и имеет вид

$$\sigma_{s,j,q} = z_{s',j',k'} \# \dots \# z_{s,j,k} \# \dots \# z_{s,j,q} :$$

$$\left( \begin{array}{l} \forall s, s' = 1..|S| + |S'| \wedge (s' \neq s), \\ \forall j, j' = 1..|AL_s|, \forall m_\xi \in \Xi \\ \forall k, k', l, l' = 1..|Z_{s,j}|, \forall q \leq |Z_{s,j}| \\ \left( L(z_{s',j',k'}) \cap \dots \cap L(z_{s,j,k}) \cap \right) \wedge \\ \left( \cap L(z_{s,j,q}) \cap L(m_\xi) \neq \emptyset \right) \wedge \\ \wedge \left( \langle z_{s',j',k'}, m_\xi, z_{s,j,k} \rangle \in \Gamma^r \right) \wedge \end{array} \right)$$

$$\wedge \left( \langle z_{s,j,k}, z_{s,j,l} \rangle, \dots, \langle z_{s,j,l'}, z_{s,j,q} \rangle \in \Gamma^i \right), \quad (9)$$

где # — знак конкатенации элементов в цепочке.

**Шаг 6.** Выделяется для каждого зафиксированного на шаге 4 состояния множество определенных на шаге 5 цепочек, которые содержат используемые в этом состоянии данные или характеристики сигнала:

$$\Delta_{s,j,q} = \{ \sigma_{s,j,q,\psi} \} :$$

$$\left( \begin{array}{l} \forall \psi, \psi' = 1..|\Delta_{s,j,q}| \wedge (\psi \neq \psi'), \\ \left( \forall s = 1..|S| + |S'|, \forall j = 1..|AL_s|, \forall q \leq |Z_{s,j}| \right) \\ \left( \sigma_{s,j,q,\psi} \neq \sigma_{s,j,q,\psi'} \right). \end{array} \right) \quad (10)$$

**Шаг 7.** Определяется для каждого выделенного на шаге 6 множества цепочек по одной группе тестовых удаленных ИТВ  $sp_{s,j,q}$ , включающей для каждой цепочки из множества  $\Delta_{s,j,q}$  факторы  $f_{s,j,q,\psi,\gamma}$  для всех возможных вариантов передачи сообщений, приведенных в таблице.

При этом по аналогии с принятым в NASA подходом к тестированию бортового радиоэлектронного оборудования [11] в целях недопущения «взрыва» пространства тестируемых состояний при проверке одной цепочки в остальных входящих в  $\Delta_{s,j,q}$  цепочках принимаются точные и своевременные сообщения. Группу тестовых удаленных ИТВ предлагается определять следующим образом:

$$\left( \begin{array}{l} \forall s = 1..|S| + |S'|, \forall j = 1..|AL_s|, \forall q \leq |Z_{s,j}|, \\ \forall \psi = 1..|\Delta_{s,j,q}|, \forall \gamma = 2..15, \end{array} \right)$$

■ Варианты передачи сообщений

Характеристики сообщений		Значение $\gamma$
Своевременность	Точность	
Своевременно	Точно	1
	Прецизионно	2
	Правильно, но непрецизионно	3
	На нижней границе интервала правильности	4
	На верхней границе интервала правильности	5
	Выше верхней границы интервала правильности	6
	Ниже нижней границы интервала правильности	7
Раньше	Точно	8
	Прецизионно	9
	Правильно, но непрецизионно	10
	На нижней границе интервала правильности	11
	На верхней границе интервала правильности	12
	Выше верхней границы интервала правильности	13
	Ниже нижней границы интервала правильности	14
Позже	Не имеет значения	15

$$sp_{s,j,q} = \left( \bigcup_{\gamma} \left( \begin{array}{l} \langle f_{s,j,q,1,\gamma}, f_{s,j,q,2,1}, \dots, f_{s,j,q,\psi,1} \rangle \text{ при} \\ \Delta t_{\circ}(\sigma_{s,j,q,1}), \Delta t_{>}(\sigma_{s,j,q,1}), \Delta t_{<}(\sigma_{s,j,q,1}) \end{array} \right), \dots, \right. \quad (11)$$

$$\left. \bigcup_{\gamma} \left( \begin{array}{l} \langle f_{s,j,q,1,1}, f_{s,j,q,2,\gamma}, \dots, f_{s,j,q,\psi,1} \rangle \text{ при} \\ \Delta t_{\circ}(\sigma_{s,j,q,2}), \Delta t_{>}(\sigma_{s,j,q,2}), \Delta t_{<}(\sigma_{s,j,q,2}) \end{array} \right), \dots, \right.$$

$$\left. \bigcup_{\gamma} \left( \begin{array}{l} \langle f_{s,j,q,1,1}, f_{s,j,q,2,1}, \dots, f_{s,j,q,\psi,\gamma} \rangle \text{ при} \\ \Delta t_{\circ}(\sigma_{s,j,q,\psi}), \Delta t_{>}(\sigma_{s,j,q,\psi}), \Delta t_{<}(\sigma_{s,j,q,\psi}) \end{array} \right) \right)$$

Последовательная реализация каждой полученной таким образом совокупности наборов взаимосвязанных факторов, определяющей содержание группы тестовых удаленных ИТВ, позволит осуществить поиск ошибок в каждом состоянии локального алгоритма, связанном с обработкой сообщений от всех локальных алгоритмов других ИТС, и в результате проверить возможность приведения ИТС или системы в целом в состояние потери работоспособности, сниженной эффективности функционирования, управляемости или доступности для углубленного анализа источником ИТВ.

В рассматриваемом примере с применением предложенного способа представляется возможным получить 6 групп тестовых удаленных ИТВ, включающих 112 наборов факторов. В частности, для состояния  $z_{2,3,4}$  может быть получена следующая группа:

$$sp_{2,3,1} = \left( \bigcup_{\gamma=2..15} \langle f_{2,3,1,1,\gamma}, f_{2,3,1,2,1} \rangle \right) \cup$$

$$\bigcup_{\gamma=2..15} \langle f_{2,3,1,1,1}, f_{2,3,1,2,\gamma} \rangle \text{ для}$$

$$\Delta_{2,3,1} = (\sigma_{2,3,1,1}, \sigma_{2,3,1,2}):$$

$$\sigma_{2,3,1,1} = z_{1,1,1-2} \# z_{1,1,1-3} \# z_{2,3,2} \# z_{2,3,3} \# z_{2,3,4},$$

$$\sigma_{2,3,1,2} = z_{3,4,3} \# z_{2,3,4} \text{ при}$$

$$\Delta t_{\circ}(\sigma_{2,3,1,1}) = [t(m_{11}), t(m_{11}) + \Delta t_{\min}];$$

$$\Delta t_{>}(\sigma_{2,3,1,1}) = [t(m_6) \vee t(m_8) \vee$$

$$\vee t(m_9) \vee t(m_{10}), t(m_{11})];$$

$$\Delta t_{<}(\sigma_{2,3,1,1}) = [t(m_{11}), t(m_{11}) + \Delta t_{\text{wait}}];$$

$$\Delta t_{\circ}(\sigma_{2,3,1,2}) = [t(m_3), t(m_3) + \Delta t_{\min}];$$

$$\Delta t_{>}(\sigma_{2,3,1,2}) = [t(m_1), t(m_3)];$$

$$\Delta t_{<}(\sigma_{2,3,1,2}) = [t(m_3), t(m_3) + \Delta t_{\text{wait}}].$$

Представленная группа тестовых удаленных ИТВ содержит 28 наборов факторов для предикатов  $v$  и  $w$ , непосредственно используемых в состоянии  $z_{2,3,4}$ . Предикат  $f$ , присутствующий в состоянии  $z_{2,3,4}$ , используется только в состоянии  $z_{3,4,5}$  и поэтому в группе  $sp_{2,3,1}$  не задействован.

Способ представляется возможным эффективно использовать не только в ходе эксплуатации, испытаний или системного тестирования пространственно распределенных систем информационно-технических средств, но и при интеграционном тестировании сложных программных проектов или информационно-технических средств, когда используемая в статье категория «информационно-техническое средство» отождествляется с программным модулем или блоком информационно-технического средства, а также в процессе тестирования программных модулей, разработанных с применением объектно-ориентированного подхода, когда категория «информационно-техническое средство» отождествляется с объектом.

### Заключение

Представленный в статье способ с использованием предложенных авторами теоретико-множественных моделей локального и распределенного алгоритмов, формируемых на основе общедоступной спецификации об алгоритмах функционирования информационно-технических средств пространственно распределенных систем, впервые позволяет обеспечить разработку полного множества тестовых удаленных информационно-технических воздействий на эти средства путем учета всех потенциально возможных наборов факторов, комплексно нарушающих точность и своевременность обрабатываемых данными средствами сообщений.

### Литература

- ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. — М.: Изд-во стандартов, 2007. — 8 с.
- ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — М.: Изд-во стандартов, 2007. — 8 с.
- РД Гостехкомиссии России. Защита от несанкционированного доступа к информации. Ч. 1. Про-

- граммное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. — М.: Гостехкомиссия России, 1999. — 15 с.
- Myers G. J. The Art of Software Testing. — New Jersey, John Wiley & Sons, 2004. — 255 p.
- Бейзер Б. Тестирование черного ящика. Технологии функционального тестирования программного обеспечения и систем. — СПб.: Питер, 2004. — 318 с.

6. Clarke E. M., Grumberg O., Peled D. Model Checking. — N. Y.: MIT Press, 1999. — 314 p.
7. Кулямин В. В., Петренко А. К., Косачев А. С., Бурдонов И. Б. Подход UniTesK к разработке тестов // Программирование. 2003. № 29(6). С. 25–43.
8. Charron-Bost B., Mattern F., Tel G. Synchronous, Asynchronous, and Casually Ordered Communication // Distributed Comput. 1996. Vol. 9. P. 173–191.
9. Tel G. Introduction to Distributed Algorithms. — N. Y.: Cambridge University Press, 2001. — 612 p.
10. ГОСТ Р ИСО 5725-1-2002. Точность (правильность и прецизионность) методов и результатов измерений. Ч. 1. Основные положения и определения. — М.: Изд-во стандартов, 2002. — 23 с.
11. Hayhurst K. J., Veerhusen D. S., Chilenski J. J., Riererson L. K. A Practical Tutorial on Modified Condition / Decision Coverage. — NASA, 2001. — 85 p.

UDC 004.05

**Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools**

A. A. Boyko<sup>a</sup>, PhD, Tech., Associate Professor, algeminy@mail.ru

A. V. Djakova<sup>a</sup>, Scientist, alenka\_x@inbox.ru

<sup>a</sup>Military Education-Science Center of Military Air Forces “Professor N. E. Zhukovsky and Yu. A. Gagarin Military Air Academy”, 54A, Staryh Bolshevnikov St., 394064, Voronezh, Russian Federation

**Purpose:** During development and operation of spatially distributed systems of information-technical tools special importance is attached to assessment of sustainability of their operation in the environment of remote information-technical impacts from an attacker. Imperfection of the known approaches to development of such impacts prevents analyzing a response of information-technical tools to a whole set of factors comprehensively violating accuracy and timeliness of processing messages. The most effective solution of this problem is to generate test information-technical impacts on the basis of formalization of processes of a studied object operation. **Methods:** Creation of formal models of a spatially distributed system of information-technical tools and automatic generation of a whole set of remote test information-technical impacts on its basis. **Results:** There has been proposed a set-theoretical operational model of a spatially distributed system of information-technical tools in the form of a complex of local algorithms which interact within a single distributed algorithm using asynchronous messaging. Based on the model there has been proposed a method providing development of a whole set of remote test information-technical (software and electromagnetic) impacts on the basis of a publicly available specification of operational algorithms of information-technical tools. The essence of the method is to fix in each local algorithm of each information-technical tool a set of states directly using indivisible data elements or characteristics of electromagnetic or electric signals received from all local algorithms of other information-technical tools; to define a set of end-chains of states of local algorithms for each of these states describing a path of the same elements of data or signals from a state in which they have appeared (received) to a state in which they are used; to allocate a set of the chains which contain applied data elements or characteristics of a signal for each the fixed states; and to define remote test information-technical impacts for each of selected sets of chains taking into account potentially implementable sets of interrelated factors influencing accuracy and timeliness of messages. **Practical relevance:** For the first time there has been obtained an opportunity to analyze response of the existing and developing information-technical tools of spatially distributed systems to all possible sets of factors comprehensively violating accuracy and timeliness of messages processed by these tools.

**Keywords** — Distributed Algorithm, Remote Information-Technical Impact, Information-Technical Tool.

**References**

1. State Standard R 50922-2006. Protection of Information. Basic Terms and Definitions. Moscow, Standartov Publ., 2007. 8 p. (In Russian).
2. State Standard R 51275-2006. Protection of Information. Object of Informatisation. Factors Influencing the Information. General. Moscow, Standartov Publ., 2007. 8 p. (In Russian).
3. Governing Document of StateTechCommission of Russia. Protection from Unauthorized Access to Information. Part 1. Software of Information Protection Means. Classification by Control Level of Undeclared Possibilities Absence. Moscow, Gostekhkomiissia Rossii Publ., 1999. 15 p. (In Russian).
4. Myers G. J. *The Art of Software Testing*. New Jersey, John Wiley & Sons, 2004. 255 p.
5. Beizer B. *Testirovanie chernogo iashchika. Tekhnologii funktsional'nogo testirovaniia programmnogo obespecheniia i sistem* [Black-box testing. Techniques for Functional Testing of Software and Systems]. Saint-Petersburg, Piter Publ., 2004. 318 p. (In Russian).
6. Clarke E. M., Grumberg O., Peled D. Model Checking. New York, MIT Press, 1999. 314 p.
7. Kuliamin V. V., Petrenko A. K., Kossatchev A. S., Bourdonov I. B. The UniTesK Approach to Designing Test Suites. *Programirovanie*, 2003, vol. 29, no. 6, pp. 310–322 (In Russian).
8. Charron-Bost B., Mattern F., Tel G. Synchronous, Asynchronous, and Casually Ordered Communication. *Distributed Computing*, 1996, vol. 9, pp. 173–191.
9. Tel G. *Introduction to Distributed Algorithms*. New York, Cambridge University Press, 2001. 612 p.
10. State Standard R ISO 5725-1-2002. Accuracy (trueness and precision) of Methods and Measurement Results. Part 1. Main Principles and Definitions. Moscow, Standartov Publ., 2002. 23 p. (In Russian).
11. Hayhurst K. J., Veerhusen D. S., Chilenski J. J., Riererson L. K. *A Practical Tutorial on Modified Condition / Decision Coverage*. NASA, 2001. 85 p.