

НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

Журнал **H&ES Research** издается с 2009 года, освещает достижения и проблемы российских инфокоммуникаций, внедрение последних достижений отрасли в автоматизированных системах управления, развитие технологий в информационной безопасности, исследования космоса, развитие спутникового телевидения и навигации, исследование Арктики. Особое место в издании уделено результатам научных исследований молодых ученых в области создания новых средств и технологий космических исследований Земли.

Журнал H&ES Research входит в перечень изданий, публикации в которых учитываются Высшей аттестационной комиссией России (ВАК РФ), в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий.

Тематика публикуемых статей в соответствии с перечнем групп специальностей научных работников по Номенклатуре специальностей:

- 05.11.00 Авиационная и ракетно-космическая техника
- 05.12.00 Радиотехника и связь
- 05.13.00 Информатика, вычислительная техника и управление.

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

- NEICON • CyberLenika (Open Science) • Google Scholar • OCLC WorldCat • Ulrich's Periodicals Directory • Bielefeld Academic Search Engine (BASE) • eLIBRARY.RU • Registry of Open Access Repositories (ROAR)

Мнения авторов не всегда совпадают с точкой зрения редакции. За содержание рекламных материалов редакция ответственности не несет. Материалы, опубликованные в журнале – собственность ООО «ИД Медиа Паблшер». Перепечатка, цитирование, дублирование на сайтах допускаются только с разрешения издателя.

ПЛАТА С АСПИРАНТОВ ЗА ПУБЛИКАЦИЮ РУКОПИСИ НЕ ВЗИМАЕТСЯ

Всем авторам, желающим разместить научную статью в журнале, необходимо оформить ее согласно требованиям и направить материалы на электронную почту:
HT-ESResearch@yandex.ru.

С требованиями можно ознакомиться на сайте: **www.H-ES.ru**.
Все номера журнала находятся в свободном доступе на сайте.

Язык публикаций: русский, английский.
Периодичность выхода – 6 номеров в год.

© ООО «ИД Медиа Паблшер», 2018

HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

H&ES Research is published since 2009. The journal covers achievements and problems of the Russian infocommunication, introduction of the last achievements of branch in automated control systems, development of technologies in information security, space researches, development of satellite television and navigation, research of the Arctic. The special place in the edition is given to results of scientific researches of young scientists in the field of creation of new means and technologies of space researches of Earth.

The journal H&ES Research is included in the list of scientific publications, recommended Higher Attestation Commission Russian Ministry of Education for the publication of scientific works, which reflect the basic scientific content of candidate and doctoral theses. IF of the Russian Science Citation Index.

Subject of published articles according to the list of branches of science and groups of scientific specialties in accordance with the Nomenclature of specialties:

- 05.07.00 Aviation, space-rocket hardware
- 05.12.00 RF technology and communication
- 05.13.00 Informatics, computer engineering and control.

JOURNAL H&ES RESEARCH INDEXING

The opinions of the authors don't always coincide with the point of view of the publisher. For the content of ads, the editorial Board is not responsible. All articles and illustrations are copyright. All rights reserved. No reproduction is permitted in whole or part without the express consent of Media Publisher Joint-Stock company.

POSTGRADUATE STUDENTS FOR PUBLICATION OF THE MANUSCRIPT WILL NOT BE CHARGED

All authors wishing to post a scientific article in the journal, you must register it according to the requirements and send the materials to your email: **HT-ESResearch@yandex.ru.**

The requirements are available on the website: **www.H-ES.ru**.
All issues of the journal are in a free access on a site.

Language of publications: Russian, English.
Periodicity – 6 issues per year.

© "Media Publisher", LLC 2018

Учредитель:
ООО «ИД Медиа Паблшер»

Издатель:
СВЕТЛАНА ДЫМКОВА

Главный редактор:
КОНСТАНТИН ЛЕГКОВ

Редакционная коллегия:
БОБРОВСКИЙ В.И., д.т.н., доцент;
БОРИСОВ В.В., д.т.н., профессор,
Действительный член академии
военных наук РФ;
БУДКО П.А., д.т.н., профессор;
БУДНИКОВ С.А., д.т.н., доцент,
Действительный член Академии
информатизации образования;
ВЕРХОВА Г.В., д.т.н., профессор;
ГОНЧАРОВСКИЙ В.С., д.т.н., профессор,
заслуженный деятель науки
и техники РФ;
КОМАШИНСКИЙ В.И., д.т.н., профессор;
КИРПАНЕВ А.В., д.т.н., доцент;
КУРНОСОВ В.И., д.т.н., профессор,
академик Арктической академии наук,
член-корреспондент Международной
академии информатизации, академик
Международной академии обороны,
безопасности и правопорядка,
Действительный член Российской
академии естественных наук;
МАНУЙЛОВ Ю.С., д.т.н., профессор;
МОРОЗОВ А.В., д.т.н., профессор,
Действительный член Академии
военных наук РФ;
МОШАК Н.Н., д.т.н., доцент;
ПРОРОК В.Я., д.т.н., профессор;
СЕМЕНОВ С.С., д.т.н., доцент;
СИНИЦЫН Е.А., д.т.н., профессор;
ШАТРАКОВ Ю.Г., д.т.н., профессор,
заслуженный деятель науки РФ.

N&ES Research зарегистрирован
Федеральной службой по надзору
за соблюдением законодательства в
сфере массовых коммуникаций и охране
культурного наследия.
Издательская лицензия
ПИ № ФС 77-60899.

Адрес редакции:
111024, Россия, Москва,
ул. Авиамоторная, д. 8, офис 512-514;

194044, Россия, Санкт-Петербург,
Лесной Проспект, 34-36, к. 1,
Тел.: +7(911) 194-12-42.

Отдел развития и рекламы:
ОЛЬГА ДОРОШКЕВИЧ
ovd@media-publisher.ru
тел.: 8(916) 951-55-36

Дизайн и компьютерная верстка:
ОКСАНА ИВАНОВА
ok-ivanova@yandex.ru

СОДЕРЖАНИЕ

АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

Лебедев Е. Л., Лебедев А. С., Михайленко А. В.

Основы методики оценивания качества поверхностей стенок камер жидкостных ракетных двигателей по статистическим характеристикам параметров отраженного света 4

Симонов П. И., Кубанков Ю. А.

Методика декодирования сообщений ADS-B как часть проверки качества бортовых систем воздушного судна в составе автоматизированных измерительных стендов, построенных в среде графического языка программирования LabVIEW 12

РАДИОТЕХНИКА И СВЯЗЬ

Белов А. С., Скубьев А. В.

Теоретический подход по оцениванию и обеспечению живучести распределенных сетей связи в условиях информационного противоборства 22

Логин Э. В., Канаев А. К.

Модель транспортной сети связи как составляющая мультиагентной системы управления 34

Михайлов Р. Л.

Двухуровневая модель координации подсистем радиомониторинга и радиоэлектронной борьбы 43

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Захарченко Р. И., Королев И. Д.

Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве 52

Самойленко Д. В., Еремеев М. А., Финько О. А.

Повышение информационной живучести группы робототехнических комплексов методами модулярной арифметики 62

Варганов В. В., Гривачев А. В., Курочкин А. Г., Титенко Е. А.

Структура интеллектуальной системы управления наземного робототехнического комплекса для формирования маршрута движения 78

Шелухин О. И., Смычек М. А., Симонян А. Г.

Фильтрация нежелательных приложений интернет-ресурсов в целях информационной безопасности 87

ПУБЛИКАЦИИ НА АНГЛИЙСКОМ ЯЗЫКЕ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Петрич Д. О., Охотников Ю. Ю., Шаймухаметов Ш. И.

Применение нечетких нейронных сетей в прогнозировании успешности профессиональной деятельности военных специалистов 100

CONTENTS

AVIATION, SPACE-ROCKET HARDWARE

Lebedev E. L., Lebedev A. S., Mikhaylenko A. V.

Basics of methodology of evaluation of the quality of the surfaces of the walls of the chambers of liquid rocket engines on the statistical characteristics of parameters of the reflected light 4

Simonov P. I., Kubankov Yu. A.

Method of decoding ADS-B messages on automated measurement stands built on LabVIEW framework, as part of the aircraft board systems quality control 12

RF TECHNOLOGY AND COMMUNICATION

Belov A. S., Skubyev A. V.

Theoretical approach on estimation and support of survivability of distributed networks of communication in the conditions of information confrontation 22

Login E. V., Kanaev A. K.

Model of a transport communication network as a component of a multi-agent management system 34

Mikhailov R. L.

Two-level model of coordination of subsystems of radiomonitoring and electronic warfare 43

INFORMATICS, COMPUTER ENGINEERING AND CONTROL

Zakharchenko R. I., Korolev I. D.

Methods of estimation of stability of functioning of objects of critical information infrastructure operating in cyberspace 52

Samoylenko D. V., Ereemeev M. A., Finko O. A.

The increase of information survivability the group of robotic systems methods of modular arithmetic 62

Varganov V. V., Grivachev A. V., Kurochkin A. G., Titenko E. A.

Structure of intellectual system of control of robotic technical complex for formation of route of motion 78

Sheluhin O. I., Smychek M. A., Simonyan A. G.

Filtering unwanted applications of Internet resources for information security purposes 87

PUBLICATIONS IN ENGLISH INFORMATICS, COMPUTER ENGINEERING AND CONTROL

Petrich D. O., Okhotnikov Yu. Yu., Shaymukhametov Sh. I.

Employment of fuzzy neural networks forecasting professional success activities of the military experts 100

Founder:
"Media Publisher", LLC

Publisher:
SVETLANA DYMKOVA

Editor in chief:
KONSTANTIN LEGKOV

Editorial board:
BOBROWSKY V.I., PhD, Docent;
BORISOV V.V., PhD, Full Professor;
BUDKO P.A., PhD, Full Professor;
BUDNIKOV S.A., PhD, Docent,
 Actual Member of the Academy of Education Informatization;
VERHOVA G.V., PhD, Full Professor;
GONCHAREVSKY V.S., PhD, Full Professor,
 Honored Worker of Science and Technology of the Russian Federation;
KOMASHINSKIY V.I., PhD, Full Professor;
KIRPANEV A.V., PhD, Docent;
KURNOSOV V.I., PhD, Full Professor,
 Academician of Academy of Sciences of the Arctic, corresponding member of the International Academy of Informatization, International Academy of defense, security, law and order, Member of the Academy of Natural Sciences;
MANUILOV Y.S., PhD, Full Professor;
MOROZOV A.V., PhD, Full Professor,
 Actual Member of the Academy of Military Sciences;
MOSHAK N.N., PhD, Docent;
PROROK V.Y., PhD, Full Professor;
SEMEV S.S., PhD, Docent;
SINICYN E.A., PhD, Full Professor;
SHATRAKOV Y.G., PhD, Full Professor,
 Honored Worker of Science of the Russian Federation.

Journal H&ES Research has been registered by the Federal service on supervision of legislation observance in sphere of mass communications and cultural heritage protection.
Publishing license
ПН № ФС 77-60899.

Address of edition:
111024, Russia, Moscow,
st. Aviamotornaya, 8, office 512-514;

194044, Russia, St. Petersburg,
Lesnoy av., 34-36, h.1,
Phone: +7 (911) 194-12-42.

Development and advertizing department:
OLGA DOROSHKVICH
ovd@media-publisher.ru,
tel.: 8(916) 951-55-36

Design and computer imposition:
OKSANA IVANOVA
ok-ivanova@yandex.ru

doi 10.24411/2409-5419-2018-10036

ОСНОВЫ МЕТОДИКИ ОЦЕНИВАНИЯ КАЧЕСТВА ПОВЕРХНОСТЕЙ СТЕНОК КАМЕР ЖИДКОСТНЫХ РАКЕТНЫХ ДВИГАТЕЛЕЙ ПО СТАТИСТИЧЕСКИМ ХАРАКТЕРИСТИКАМ ПАРАМЕТРОВ ОТРАЖЕННОГО СВЕТА

ЛЕБЕДЕВ

Евгений Леонидович¹

ЛЕБЕДЕВ

Алексей Сергеевич²

МИХАЙЛЕНКО

Александр Владимирович³

Сведения об авторах:

¹д.т.н., доцент, начальник кафедры контроля качества и испытаний вооружения, военной и специальной техники Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург, Россия, zlebedev@yandex.ru

²к.т.н., преподаватель кафедры контроля качества и испытаний вооружения, военной и специальной техники Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург, Россия, tihaxis@mail.ru

³адъюнкт кафедры контроля качества и испытаний вооружения, военной и специальной техники Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург, Россия, tihaxis@mail.ru

АННОТАЦИЯ

Рассмотрен вопрос необходимости контроля качества поверхности стенок камер жидкостных ракетных двигателей. Дано определение качества поверхности указанных элементов, представлены основные методы его контроля на предприятиях оборонно-промышленного комплекса. Описан оптико-электронный метод неразрушающего контроля качества поверхностей изделий. Предложен статистический подход к оцениванию интенсивности отраженного света в цифровых изображениях поверхностей контролируемых элементов изделий ракетно-космической техники. Приведены экспериментальные исследования, суть которых заключалась в зондировании монохроматическим излучением контролируемых поверхностей экспериментальных образцов, изготовленных из жаростойкого нержавеющей сплава, используемого при изготовлении стенок камер маршевых жидкостных ракетных двигателей с фиксацией отраженного света на цифровой носитель информации. Выполнено физическое моделирование нормированных нарушений качества контролируемых поверхностей. В качестве возможных нарушений обработки и чистоты поверхности принимались повышенная шероховатость, различные уровни загрязнения техническими смазочными материалами, наличие следов коррозии, технологических загрязнений, которые ухудшают технико-экономические показатели, надежность и долговечность деталей и узлов двигателей. Выбраны нарушения обработки и чистоты поверхности и количественные характеристики данных видов нарушений. Полученные цифровые изображения поверхностей описанных экспериментальных образцов обрабатывались с помощью зарегистрированной установленным порядком программы обработки данных цифровых изображений для получения значений матрицы интенсивности света каждой точки цифрового изображения поверхности. Для определения статистической характеристики, а именно вероятности попадания значений яркости каждой точки поверхности в заданный интервал установленного диапазона, анализировалось общее количество значений яркостей точек цифрового изображения (зарегистрированного параметра) в определенных интервалах значений. Результатом статистической обработки параметров цифровых изображений являются вышеуказанные распределения вероятностей, которые содержат в себе первичную информацию о состоянии контролируемой поверхности.

Таким образом, полученные статистические данные позволили сделать вывод о наличии или отсутствии вышеописанных нарушений обработки и чистоты поверхностей.

КЛЮЧЕВЫЕ СЛОВА: контроль качества; интенсивность света; контролируемая поверхность; стенки камеры; шероховатость.

Для цитирования: Лебедев Е. Л., Лебедев А. С., Михайленко А. В. Основы методики оценивания качества поверхностей стенок камер жидкостных ракетных двигателей по статистическим характеристикам параметров отраженного света // Научные технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 4-11. doi 10.24411/2409-5419-2018-10036

Введение

Современные способы ведения боевых действий не представляются без использования космических средств военного назначения, которые предназначены для решения задач разведки, навигации, управления и связи, метеорологии и топогеодезии. Одним из основных условий успешного использования космических средств для решения задач в интересах Министерства обороны Российской Федерации, является обеспечение успешных запусков космических аппаратов (КА) военного и двойного назначения для формирования и поддержания необходимого состава орбитальной группировки в стратегической космической зоне. Решение данной задачи не представляется возможным без обеспечения требуемой оперативности темпов пусков ракет-носителей (РН).

Известно, что по статистике пусков средств выведения различного назначения за период в 30 лет 3,7% из них завершаются аварийным исходом [1]. Кроме того, половина аварий случается по вине жидкостных ракетных двигателей (ЖРД) РН. Каждый аварийный пуск приводит к срыву выполнения задач по предназначению, значительному материальному ущербу и, что более важно, может привести к человеческим жертвам. Одним из основных решений, влияющих на безопасность и успешность пусков РН, является обеспечение надежности [2] ЖРД. Надежность ЖРД достигается, в том числе, в процессе их изготовления посредством соблюдения всех требований, предусмотренных конструкторской, технологической и нормативной документацией [3].

Наиболее ответственным агрегатом ЖРД, работающим в условиях высоких значений температуры и давления, является его камера. Безусловное достижение описанных выше целей становится возможным только при осуществлении непрерывного контроля качества элементов камеры ЖРД на этапах жизненного цикла [4], в том числе в ходе технологического процесса изготовления ее элементов. Самыми энергонапряженными из них являются внутренняя (огневая) и внешняя стенки (оболочки)

камеры, контроль качества поверхностей которых играет одну из ключевых ролей в обеспечении надёжной работы изделия. К тому же, в соответствии с требованиями нормативно-технической документации попадание загрязнений, следов смазки, наличие следов окисления (коррозии) во внутренние полости камеры не допускается.

Теоретические основы исследования

В настоящее время при контроле качества элементов ракетно-космической техники, все чаще находят применение средства и методы неразрушающего контроля, одним из аспектов применения которых является определение качественных параметров рабочих поверхностей изделий. Камера, как наиболее нагруженный агрегат ЖРД, требует особого подхода к контролю качества ее элементов. Это обусловлено как условиями функционирования, так и ее конструктивными особенностями. Последнее обстоятельство объясняется тем, что камера представляет собой тонкостенную, двухслойную конструкцию со сложной внутренней системой трактов подачи компонентов ракетного топлива. Кроме того, в процессе функционирования камеры, возникающие в ее элементах, напряжения могут приближаться к пределу прочности конструкционных материалов, из которых она выполнена, поэтому наличие даже микроскопических посторонних образований на ее поверхностях или нарушений их обработки как при сборке, так и при испытаниях может привести к нарушению работоспособности камеры в целом. Известны нарушения работоспособности камеры ЖРД по причине низкого качества паяных соединений ввиду ненадлежащей технологической подготовки спаиваемых поверхностей (рис. 1) Существенное влияние на работоспособное состояние камеры оказывает достигнутый уровень и стабильность технологического процесса производства, в рамках которого возможно применение методов неразрушающего контроля качества ее элементов. Одними из таких элементов являются, как было уже описано, поверхности внутренней и внешней стенок камеры ЖРД.

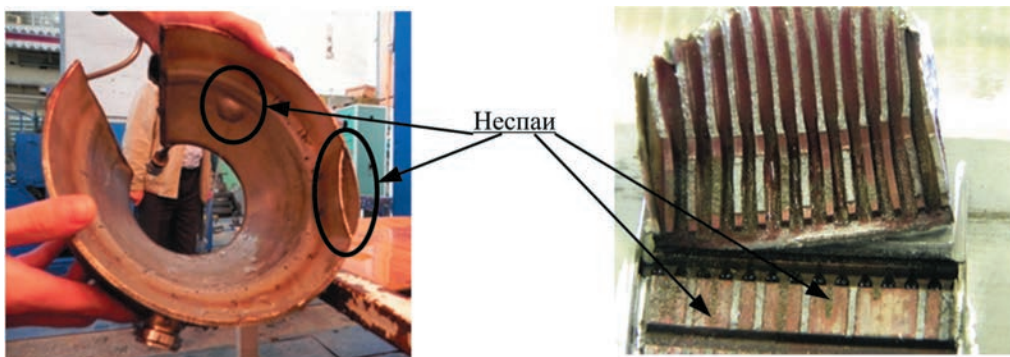


Рис. 1. Дефекты паяных соединений вследствие ненадлежащей технологической подготовки спаиваемых поверхностей

Под качеством поверхности стенок камер сгорания ЖРД будем понимать комплексную характеристику, определяющую уровень (степень) соответствия параметров шероховатости и чистоты поверхности требованиям, установленным в нормативно-технической документации. Важной тенденцией развития методов и средств контроля качества поверхностей является стремление к автоматизации и надежности процессов измерения, оперативности получения измерительной информации. Такими прогрессивными методами контроля качества являются бесконтактные оптико-электронные методы измерений. Оптические методы контроля относятся к неразрушающим методам и основаны на использовании физических явлений света, проявляющихся в результате его взаимодействия с контролируемым объектом при получении информации о состоянии объекта и его параметрах. Так в частности, указанные методы позволяют получить первичную информацию о наличии на контролируемой поверхности (элемента) загрязнений (частицы пыли, следы окисления, смазочные материалы и т.д.) и об уровне шероховатости с высокой точностью. Наиболее подходящими оптико-электронными методами для решения задач контроля качества поверхностей стенок камер ЖРД являются, например, рефлектометрический метод, метод темного поля [5], метод цифровой спекл-интерферометрии, метод цифровой голографии [6] и т.д., особенностью которых являются использование в качестве источника освещения колимированного пучка монохроматического излучения для освещения испытываемой поверхности контролируемого элемента, регистрация отраженного от этой поверхности излучения и обработка отраженного сигнала. Наиболее широкое применение на предприятиях оборонно-промышленного комплекса (ОПК) нашли визуально-оптические (эндоскопы, микроскопы) и контактные средства (профилометры различных типов) контроля. Однако, описанные оптико-электронные методы контроля качества поверхности не всегда могут быть в полной мере применены для контроля поверхностей указанных элементов, так как обладают высокими требованиями по виброустойчивости, имеют относительно малую площадь исследуемого участка поверхности, требуют применения дорогостоящего оборудования для обеспечения необходимой точности и оперативности контроля.

Использование в аппаратных средствах контроля систем распознавания все чаще находит совместное применение в различных образцах оборонной промышленности. Для этого применяются алгоритмы обработки изображений, такие как свертка, преобразование Фурье и статистические методы.

В данной работе предлагается оптико-электронный метод контроля поверхностей, основанный на статистических методах обработки данных цифровых изображений,

в частности, на статистической обработке параметра, характеризующего уровень яркости цифрового изображения поверхности контролируемого элемента.

Для получения достоверной информации о качестве поверхности необходимо выполнение следующих основных этапов, включающих предварительную обработку изображения поверхности, поиск дефектных областей на изображении, расчет классификационных признаков по найденным областям, классификацию дефектов и распознавание этих классов [7].

Для оценивания цифрового изображения контролируемой поверхности можно использовать детерминистский и статистический подходы. Ввиду очень малой визуальной различимости получаемых цифровых изображений поверхностей, будет использоваться именно статистический подход [8].

При обработке цифровых изображений значения яркости могут быть описаны с точки зрения вероятностного подхода. Самый известный из них — когда значения яркости трактуются как значения случайные [9]. Предварительные экспериментальные исследования показали, что с одной стороны, изменение качества поверхности влияет на интенсивность отраженного от нее света, с другой стороны, яркость каждой точки (пиксела) является случайной величиной. Наиболее полной характеристикой, описывающей изменение значения случайной величины, является функция распределения. Таким образом, установление зависимости данной характеристики с параметром нарушения поверхности может быть теоретической основой предлагаемого метода [10].

Исходное изображение испытываемой поверхности, получаемое в результате фотосъемки, представляет собой дискретную функцию двух переменных [11]:

$$I_0 = f(\xi, \eta), \quad (1)$$

где ξ и η — координаты точки в двумерной системе координат исходного изображения; I_0 — относительная интенсивность светового сигнала, пропорциональная яркости точки.

При этом, цифровое изображение (дискретное двумерное пространство), характеризуется относительной интенсивностью светового сигнала каждой точки (пикселя) изображения, которая изменяется в целых числах от 0 до 255 [12].

Для определения статистической характеристики зарегистрированного параметра (интенсивности), а именно распределения вероятности попадания значений интенсивности освещенности каждой точки поверхности в заданный интервал, анализируется общее количество значений интенсивностей точек (пикселей) изображения. Такие интервалы, в пределах которых приращение ис-

следуемой функции минимально, ограничиваются значениями 0–25, 26–50, ..., 226–255.

Для определения вероятности попадания значений интенсивности в освещенности в заданный интервал, рассчитываем заданную вероятность по формуле

$$p(x_i) = \frac{N_i}{N} \quad (2)$$

где N_i — количество пикселей с соответствующими значениями интенсивности, попавших в i -й интервал значений интенсивности; N — общее число пикселей цифрового изображения; $x = \langle x_1, x_2, \dots, x_n \rangle$ — вектор признаков; x_i — уровень освещенности — измеряемый признак.

Экспериментальные исследования

Целью проводимых экспериментальных исследований являлось получение зависимостей параметров интенсивности света, отраженного от поверхности контролируемого элемента, от степени нарушений ее обработки (уровня шероховатости) и чистоты.

При проведении экспериментальных исследований необходимо было решить следующие задачи:

- подбор и подготовку образцов для экспериментальных исследований;
- имитация нормированных нарушений качества исследуемых поверхностей;
- зондирование экспериментальных образцов монохроматическим излучением;
- фиксацию (проведения съемки) зондированных поверхностей подготовленных испытуемых образцов;
- анализ полученных значений и получение экспериментальных зависимостей.

Экспериментальные образцы были изготовлены из жаростойкой стали 12Х18Н10Т, используемой при изготовлении стенок камер действующих ЖРД [13], размер которых составил 70×60×3 мм. Поверхности экспериментальных образцов предварительно были подготовлены к условиям, удовлетворяющим требованиям, предъявляемым к поверхностям стенок камер ЖРД в соответствии с нормативно-технической документацией. Для физической имитации нарушений качества поверхностей были использованы экспериментальные образцы с разными параметрами шероховатости R_z и R_a , где R_z — наибольшая высота профиля поверхности (сумма средних абсолютных высот пяти наибольших выступов профиля и глубин пяти наибольших впадин профиля в пределах базовой длины), а R_a — среднее арифметическое из абсолютных значений отклонений профиля в пределах базовой длины, которые изменялись в пределах $R_z = 0,05 \dots 10$ мкм и $R_a = 0,01 \dots 2,5$ мкм. Производилось нанесение смазочных материалов различной поверхностной плотности на образцы, при этом плотность $\rho_s = 0,00044 \dots 0,0015$ г/см². Кроме того, ис-

пользовались образцы с различной степенью окисления 90% раствором соляной кислоты (HCl) по времени воздействия от 0 до 5 часов.

Для освещения поверхностей контролируемых образцов использовался одномодовый лазерный модуль S-5 (Sanyo) видимого (красного) диапазона с мощностью непрерывного излучения 5 мВт в спектральном диапазоне 635 нм, который является оптимальным источником когерентного излучения для построения систем контроля и автоматики, юстировочных и разметочных устройств, а также для научных целей [14].

Для проведения съемки зондированных монохроматическим излучением поверхностей экспериментальных образцов использовался цифровой микроскоп-камера МК-13 с разрешением 1,3 Мрх1, предназначенный для захвата изображения, фотографирования и записи видео в реальном времени. С использованием программы обработки данных цифровых изображений, зарегистрированной установленным порядком [15], проводился анализ интенсивности светового сигнала в цифровых изображениях поверхностей экспериментальных образцов с различным уровнем технических смазочных материалов, наличием следов коррозии, технологических загрязнений, степенью шероховатости, которые ухудшают технико-экономические показатели, надежность и долговечность деталей и узлов ракетных двигателей при их непосредственной эксплуатации. Схема экспериментальной установки приведена на рис. 2.

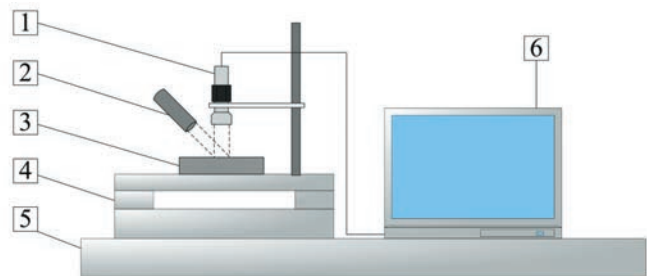


Рис. 2. Схема экспериментальной установки:

- 1 — цифровой микроскоп-камера; 2 — источник монохроматического излучения (лазер); 3 — экспериментальный образец; 4 — предметный столик; 5 — виброустойчивый стол; 6 — ЭВМ

Результатами обработки цифровых изображений контролируемых поверхностей с использованием вышеуказанного программного продукта являлись массивы данных (матрицы) интенсивностей каждой точки (пиксела) с числовым значением из интервала от 0 до 255. Графические изображения данных массивов при различных нарушениях качества поверхности показаны на рис. 3. Полученные массивы значений подвергались обработке

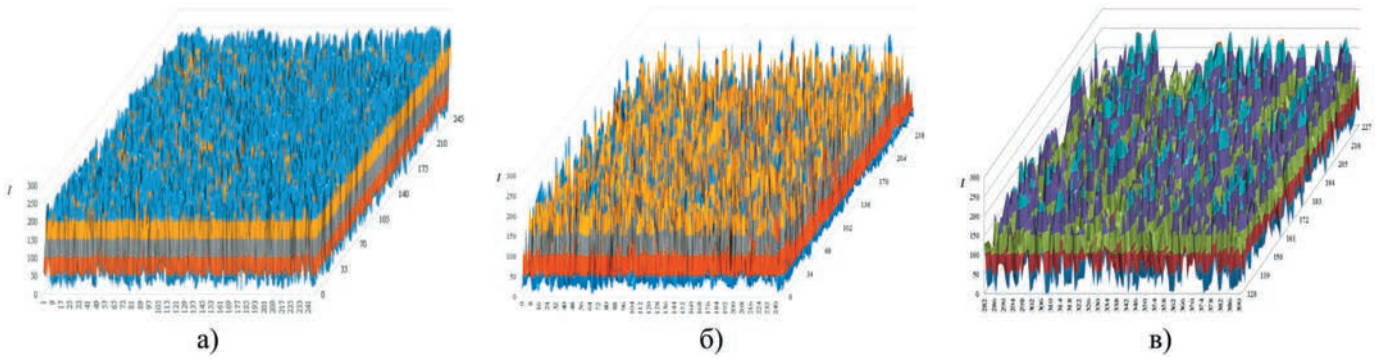


Рис. 3. Графическое представление массивов интенсивности для различных нарушений:
 а) – окисление (3 часа); б) – жировое загрязнение ($\rho_s = 0,0009 \dots 0,001 \text{ г/см}^2$);
 в) – образец шероховатости ($R_z = 0,8 \dots 2,6 \text{ мкм}$, $R_a = 0,16 \dots 0,32 \text{ мкм}$)

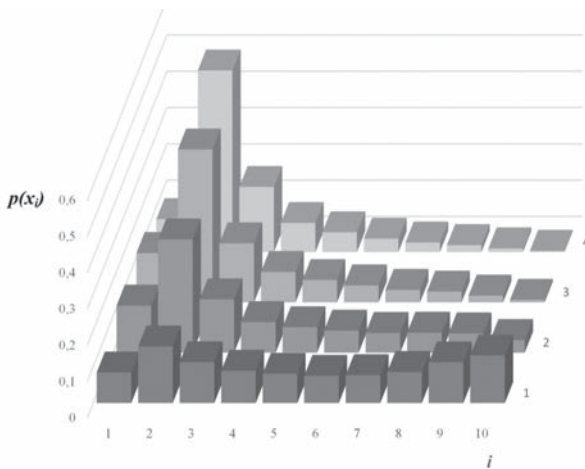


Рис. 4. Сводная гистограмма вероятностных распределений для экспериментальных образцов шероховатости

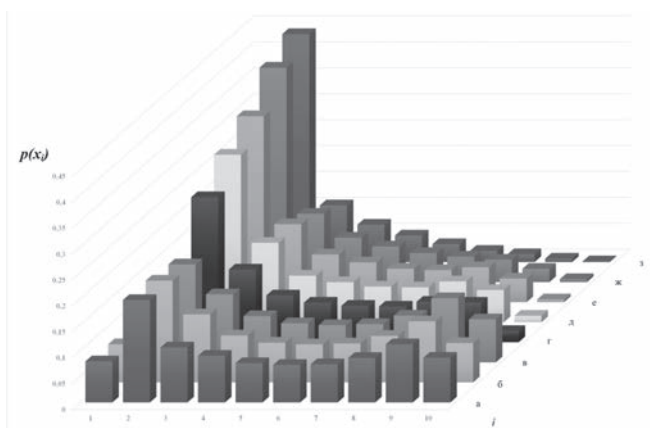


Рис. 5. Сводная гистограмма вероятностных распределений для образцов с различной поверхностной плотностью ρ_s технического смазочного материала (масло): 1 – $\rho_s = 0 \text{ г/см}^2$; 2 – $\rho_s = 0,0004 \dots 0,0005 \text{ г/см}^2$; 3 – $\rho_s = 0,0009 \dots 0,001 \text{ г/см}^2$; 4 – $\rho_s = 0,001 \dots 0,0015 \text{ г/см}^2$

в соответствии с формулой (2) и рассчитывались значения вероятностей попадания значений яркости в заданный интервал. Результаты расчетов сводились в таблицы с последующим построением по их данным гистограмм вероятностных распределений.

Для каждого изображения строилась гистограмма распределения вероятностей попадания N_i -го количества пикселей в i -й интервал. Для большей наглядности полученные гистограммы сведены в одну (рис. 4).

Таким же образом были получены сводные гистограммы вероятностных распределений для образцов указанных уровней загрязнения техническими смазочными материалами (жировым покрытием) (рис. 5), а также уровней окисления (следов коррозии) (рис. 6).

Полученные в результате экспериментальных исследований гистограммы распределения вероятностей позво-

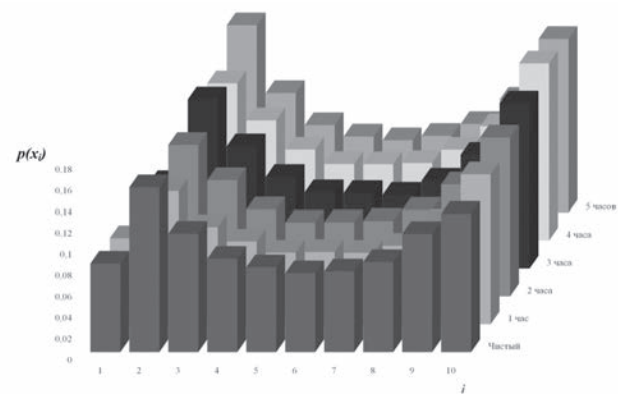


Рис. 6. Гистограмма изменения уровней максимумов распределения вероятностей в зависимости от вида нарушения (загрязнения) поверхности

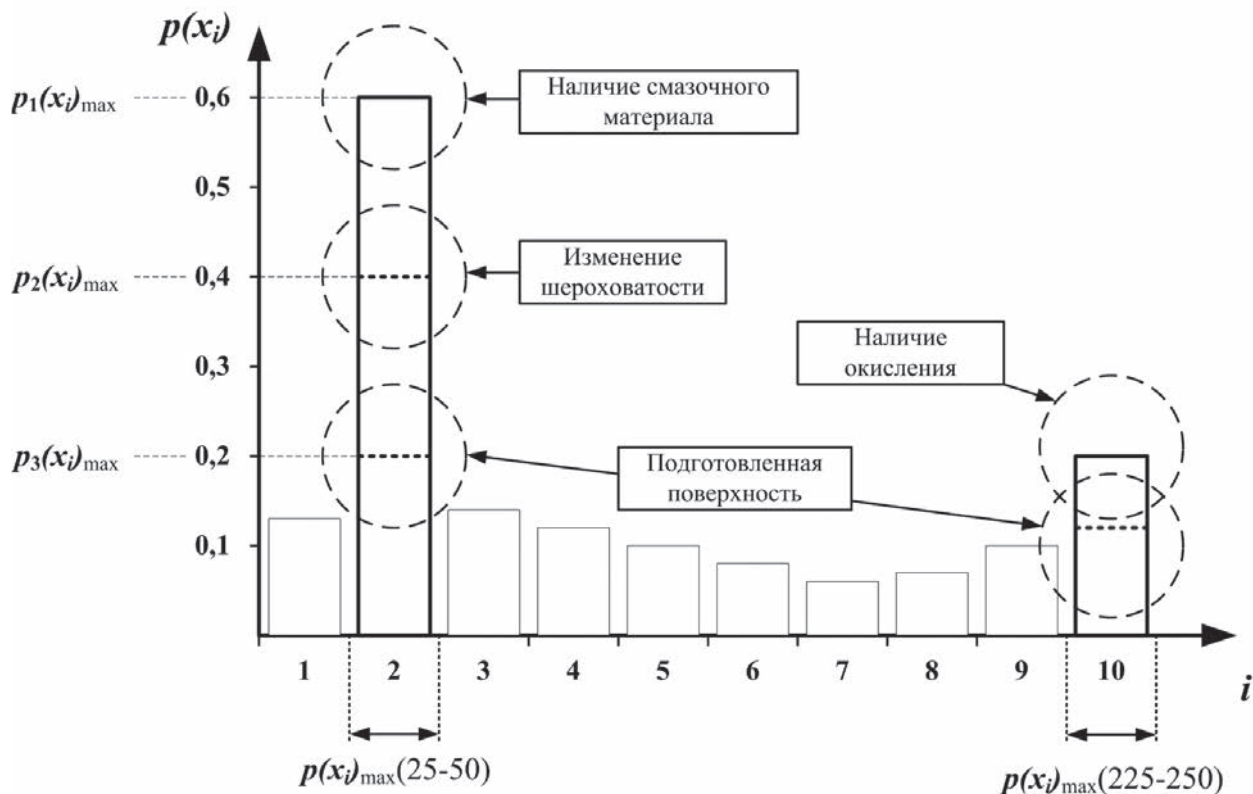


Рис. 7. Гистограмма изменения уровней максимумов распределения вероятностей в зависимости от вида нарушения (загрязнения) поверхности

лили сделать вывод о наличии или отсутствии какого-либо физического изменения поверхности контролируемого элемента (наличия на контролируемой поверхности следов смазочных материалов, коррозии, по положению $p(x_i)_{\max}$ на оси гистограммы значений интервалов яркости i). Оценив расположение на оси i максимальных вероятностей попадания в заданный интервал значений яркостей изображения, можно сделать вывод о наличии какого-либо уровня нарушения качества контролируемой поверхности (рис. 7). Подобный подход был применен к определению степени шероховатости поверхности.

Заключение

Таким образом, в результате проведения экспериментальных исследований, можно сделать вывод о возможности оперативного определения нарушений обработки и чистоты поверхностей, по статистическим зависимостям интенсивности света на их цифровых изображениях, что позволит решить задачу автоматизированного контроля качества поверхностей стенок камер ЖРД, обусловленную требованиями развития современных методов и систем контроля, а также повысить достоверность в определении вида и уровня нарушений и повышения качества самого изделия.

Литература

1. Добрынин В. С. Особенности обеспечения надежности и перспективы резервирования жидкостно-ракетных двигателей // Методы менеджмента качества. 2016. № 9. С. 54–60.
2. Горский Л. К. Статистические алгоритмы исследования надежности. М.: Наука, 1970. 400 с.
3. Добрынин В. С. К вопросу о надежности ракетных двигателей на жидком топливе // Методы менеджмента качества. 2013. № 9. С. 44–48.
4. Александров Е. С., Баранов Л. Т. и др. Основы эксплуатации космических средств. СПб.: Военный инженерно-космический университет имени А. Ф. Можайского, 2000. 499 с.
5. Бигус Г. А., Даниев Ю. Ф., Быстрова Н. А., Галкин Д. И. Диагностика технических устройств. М.: Изд-во Московского государственного технического университета имени Н. Э. Баумана, 2014. 615 с.
6. Неразрушающий контроль: в 8 т. / Под общ. ред. В. В. Клюева. М.: Машиностроение, 2006. Т. 6. С. 540–555.
7. Горелик А. Л., Скрипкин В. А. Методы распознавания. М.: Высш. школа, 1984. 219 с.
8. Шабанов В. А. Контроль микрогеометрии поверхностей, как задача распознавания образов // Инновации,

технологии, наука: сб. статей Междунар. науч.-практической конф. (Самара, 3 декабря 2015). Уфа: МЦИИ «Omega Science», 2015. С. 158–160.

9. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. М.: Техносфера, 2012. 1104 с.

10. *Лебедев А.С., Лебедев Е.Л., Добролюбов А.Н., Безруков А.В.* Методика распознавания степени поврежденности поверхности материалов по параметрам акустико-эмиссионных сигналов // *Современные наукоемкие технологии.* 2017. № 2. С. 36–40.

11. *Кофнов О.В.* Моделирование процесса контроля периодических структур с применением автоматизированных систем // *Известия вузов. Приборостроение.* 2015. № 10 (58). С. 855–858.

12. *Фурман Я.А., Юрьев А.Н., Янишин В.В.* Цифровые методы обработки и распознавания бинарных изображений. Красноярск: Изд-во Краснояр. ун-та, 1992. 248 с.

13. *Назаров В.П., Укачиков А.И.* Повышение энергоэффективности жидкостного ракетного двигателя // *Решетневские чтения: материалы XVIII Междунар. науч. Конф.* (Красноярск, 11–14 ноября 2014). Красноярск, 2014. Ч. 1. С. 163–165.

14. Лазерный модуль S-5. URL: http://komoloff.ru/lazernye-moduli/?single_prod_id=46 (дата обращения 10.09.2017).

15. *Михайленко А.В., Лебедев Е.Л., Кофнов О.В.* Программа обработки данных цифровых изображений. Заяв. № 2016661458 от 26.10.2016. Запат. 07.02.2017. Св-во № 2017611188.

BASICS OF METHODOLOGY OF EVALUATION OF THE QUALITY OF THE SURFACES OF THE WALLS OF THE CHAMBERS OF LIQUID ROCKET ENGINES ON THE STATISTICAL CHARACTERISTICS OF PARAMETERS OF THE REFLECTED LIGHT

EVGENIY L. LEBEDEV,

St-Peterburg, Russia, zlebedev@yandex.ru

ALEKSEY S. LEBEDEV,

St-Peterburg, Russia, tihaxis@mail.ru

ALEXANDER V. MIKHAYLENKO,

St-Peterburg, Russia, tihaxis@mail.ru

KEYWORDS: quality control; intensity; controlled surface; the chamber wall; roughness.

ABSTRACT

The issue of the necessity to control the quality of the surface of the walls of the chambers of liquid rocket engines is considered. The definition of the surface quality of these elements is given, the main methods of its control at the enterprises of the defense-industrial complex are presented. The optical-electronic method of non-destructive quality control of product surfaces is described. A statistical approach to the estimation of the intensity of reflected light in digital images of the surfaces of controlled elements of rocket and space equipment is proposed. Experimental studies were carried out, the essence of which was the monochromatic radiation probing of the controlled surfaces of experimental samples made of a heat-resistant stainless

alloy used in the manufacture of the walls of the chambers of marching liquid rocket engines with the fixation of reflected light onto a digital storage medium. Physical modeling of normalized quality violations of controlled surfaces was performed. As possible violations of processing and surface purity, increased roughness, different levels of contamination with technical lubricants, the presence of traces of corrosion, technological contaminants, which worsen the technical and economic performance, reliability and durability of engine parts and assemblies. The violations of processing and surface purity and the quantitative characteristics of these types of disturbances were selected. The resulting digital images of the surfaces of the described

experimental samples were processed using a digital image data program registered with the established order to obtain the values of the light intensity matrix of each point of the digital image of the surface. To determine the statistical characteristic, namely, the probability that the brightness values of each point of the surface hit a given range of the set range, the total number of brightness values of the points of the digital image (the registered parameter) in certain intervals of values was analyzed. The result of statistical processing of digital image parameters is the above probability distributions, which contain the primary information about the state of the monitored surface.

Thus, the obtained statistical data allowed to draw a conclusion about the presence or absence of the above-described violations of processing and surface cleanliness.

REFERENCES

1. Dobrynin V.S. Features ensure reliability and the prospects for reserving a liquid-propellant rocket engines. *Metody menedzhmenta kachestva*. [Methods of quality management]. 2016. No. 9. Pp. 54–60. (In Russian)
2. Gorskiy L.K. *Statisticheskie algoritmy' issledovaniya nadezhnosti* [Statistical Reliability Research Algorithms]. Moscow: Science, 1970. 400 p. (In Russian)
3. Dobrynin V.S. To the question about the reliability of rocket engines on liquid fuel. *Metody menedzhmenta kachestva*. [Methods of quality management]. 2013. No. 9. Pp. 44–48. (In Russian)
4. Aleksandrov E.S., Baranov L.T. *Osnovy jekspluatsii kosmicheskikh sredstv* [Fundamentals of operation of space vehicles]. St. Peterburg: Voenny inzhenerno-kosmicheskiy universitet imeni A.F. Mozhayskogo, 2000. 499 p. (In Russian)
5. Bigus G.A., Daniev Yu.F., Bystrova N.A., Galkin D.I. *Diagnostika texnicheskix ustrojstv* [Diagnostics of technical devices]. Moscow: Moskovskiy gosudarstvennyy tekhnicheskiy universitet imeni N.E. Baumana Publ., 2014. 615 p. (In Russian)
6. Klyuyev V.V. (Ed.). *Nerazrushajushij kontrol'* [Non-destructive testing]. Moscow: Mashinostroenie, 2006. Vol. 6. Pp. 540–555 (In Russian)
7. Gorelik A.L., Skripkin V.A. *Metody raspoznavanijaj* [Methods of recognition]. Moscow: Vysshaya shkola, 1984. 219 p. (In Russian)
8. Shabanov V.A. Kontrol' mikrogeometrii poverhnostej, kak zadacha raspoznavanija obrazov [Control of microgeometry of surfaces, as the problem of pattern recognition] *Innovacii, tehnologii, nauka: sbornik statej Mezhdunarodnoj nauchno-prakticheskoy konferencii* [Innovations, technologies, science: Sat. articles of Intern. scientific and practical conf., Samara, December 3, 2015]. Ufa: Omega Science, 2015. Pp. 158–160. (In Russian)
9. Gonzalez R., Woods R. *Digital image processing*. 3rd Edition. Prentice-Hall, 2007. 976 p.
10. Lebedev A.S., Lebedev E.L., Dobrolyubov A.N., Bezrukov A.V. Method for recognizing the degree of damage to the surface of materials by the parameters of acoustic emission signals. *Modern high technologies*. 2007. No. 2. Pp. 36–40. (In Russian)
11. Kofnov O.V. Modeling of the process of control of periodic structures with the use of automated systems. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie* [Journal of Instrument Engineering]. 2015. Vol. 10. No. 58. Pp. 855–858. (In Russian)
12. Furman Ya.A., Yur'ev A.N., Yanshin V.V. *Cifrovye metody obrabotki i raspoznavaniya binarnyx izobrazhenij* [Digital methods for processing and recognizing binary images]. Krasnoyarsk: Krasnoyarskiy universitet Publ., 1992. 248 p. (In Russian)
13. Nazarov V.P., Ukachikov A.I. Povyshenie energoeffektivnosti zhidkostnogo raketnogo dvigatelya [Increasing the energy efficiency of a liquid rocket engine]. *Reshetnevskie chteniya: materialy XVIII Mezhdunarodnoy nauchnoy konferentsii (Krasnoyarsk, 11–14 noyabrya 2014)* [Proceedings of the XVIII international scientific conference "Reshetnev readings" (Krasnoyarsk, 11–14 November 2014)]. Krasnoyarsk, 2014. Pt. 1. Pp. 163–165. (In Russian)
14. *Lazernyj modul'* [Laser module S-5]. URL: http://komoloff.ru/lazernye-moduli/?single_prod_id=46 (date of access 10.09.2017). (In Russian)
15. Mikhailenko A.V., Lebedev E.L., Kofnov O.V. *Programma obrabotki dannyh cifrovyyh izobrazhenij* [Digital image data processing program]. Declaring 2016661458 of 26.10.2016. It is registered on 07.02.2017. St. 2017611188. (In Russian)

INFORMATION ABOUT AUTHORS:

Lebedev E.L., PhD, Docent, Head of Department of Quality Control and Testing of Weapon of Military Space Academy;
 Lebedev A.S., PhD, Lecturer of Department of Quality Control and Testing of Weapon of Military Space Academy;
 Mikhaylenko A.V., Postgraduate at the Department of Quality Control and Testing of Weapon of Military Space Academy.

doi 10.24411/2409-5419-2018-10037

МЕТОДИКА ДЕКОДИРОВАНИЯ СООБЩЕНИЙ ADS-B КАК ЧАСТЬ ПРОВЕРКИ КАЧЕСТВА БОРТОВЫХ СИСТЕМ ВОЗДУШНОГО СУДНА В СОСТАВЕ АВТОМАТИЗИРОВАННЫХ ИЗМЕРИТЕЛЬНЫХ СТЕНДОВ, ПОСТРОЕННЫХ В СРЕДЕ ГРАФИЧЕСКОГО ЯЗЫКА ПРОГРАММИРОВАНИЯ LABVIEW

СИМОНОВ

Павел Игоревич¹

КУБАНКОВ

Юрий Александрович²

АННОТАЦИЯ

Рассмотрен способ построения SDR-систем для приема, демодуляции и декодирования сообщений автоматического зависимого наблюдения в режиме радиовещания (ADS-B), принимаемых от воздушного судна, в контексте унификации комплекса программного обеспечения для автоматизированных измерительных стендов, построенных с использованием технологии виртуальных приборов, и выполняющих задачи комплексной имитации бортовых систем с учетом моделирования реальных факторов полета, включая имитацию радиообстановки. Рассмотрена суть концепции программируемого радио, которая заключается в том, что базовые параметры аппаратных компонентов приемопередающего устройства определяются именно программным обеспечением, а не аппаратной конфигурацией, в отличие от аналоговых приемопередающих систем.

Раскрыта суть технологии виртуальных приборов и виртуальных измерительных систем, построенных на их основе, отмечены их достоинства применительно к построению автоматизированных измерительных стендов. Дано определение автоматизированного измерительного стенда как совокупности программных средств и средств вычислительной техники, обеспечивающей воспроизведение, моделирование и измерение параметров высокочастотных сигналов с помощью виртуального прибора, под которым понимается средство измерения, реализованное на основе компьютерной программы, написанной на LabVIEW.

Подробно рассмотрена методика проверки: раскрыта суть технологии ADS-B, позволяющая лётчикам и авиадиспетчерам получать аэронавигационную информацию от ВС с большей точностью. Также рассмотрен метод получения и переноса демодулированного сообщения в программную часть SDR-системы для последующего декодирования. Рассмотрена структура, типы и виды широковещательных сообщений, а также основные регистры GICB, передаваемые в сообщениях ADS-B. Рассмотрен процесс извлечения информации на примере сообщений о местоположении воздушного судна в воздухе, закодированных методом Compact Position Report.

Полученные результаты позволили сделать заключение о том, что унификация программного обеспечения совместно с программной обработкой демодулированной информации позволяет существенно расширить спектр принимаемых от воздушного судна сообщений, например, сообщений от вторичного обзорного радиолокатора или системы предупреждения столкновений в воздухе без необходимости модернизации и доработки аппаратной части автоматизированных измерительных стендов.

КЛЮЧЕВЫЕ СЛОВА: ADS-B; LabVIEW; измерения; автоматизированный измерительный стенд; виртуальная измерительная система; качество.

Сведения об авторах:

¹к.т.н., ведущий инженер Государственного научно-исследовательского института авиационных систем, г. Москва, Россия, sonar83@mail.ru

²к.э.н., доцент Московского технического университета связи и информатики, г. Москва, Россия, yury.kubankov@ya.ru

Для цитирования: Симонов П. И., Кубанков Ю. А. Методика декодирования сообщений ADS-B как часть проверки качества бортовых систем воздушного судна в составе автоматизированных измерительных стендов, построенных в среде графического языка программирования LabVIEW // Научные технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 12-21. doi 10.24411/2409-5419-2018-10037

Задача унификации программного обеспечения (ПО) в составе автоматизированных измерительных стендов для проверки качества бортовых систем воздушных судов (ВС) гражданской авиации, а также в задачах прототипирования при их разработке, тестировании и проверке качества является достаточно актуальной, так как это позволяет минимизировать расходы на разработку, модернизацию этих стендов, тем самым снижая общую финансовую нагрузку на решение прикладных задач. Вместе с тем происходит, как правило, усложнение как самих расчетных задач, так и различных моделируемых систем и т.п., что объективно указывает на необходимость адаптации функциональных возможностей автоматизированных измерительных стендов под новые требования и задачи.

Одним из наиболее прогрессивных подходов к решению указанной выше задачи является совместное использование технологий программируемого радио (software-defined radio, SDR) [1] и технологии виртуальных приборов (ВП), функционирующих в составе виртуальной измерительной системы (ВИС) [2] на основе магистрально-модульной архитектуры PXI/PXIe. При этом ПО для указанных стендов предполагается разрабатывать в среде LabVIEW по следующему ряду причин, суть которых будет рассмотрена ниже.

Концепция SDR [3–4] заключается в том, что базовые параметры аппаратных компонентов приемопередающего устройства определяются именно программным обеспечением, а не аппаратной конфигурацией, как это устроено в аналоговых приемопередающих системах.

Такой подход позволяет получить ряд преимуществ:

— возможность синтеза практически любого автоматизированного измерительного (проверочного) стенда для любого бортового блока;

— автоматизация процесса выполнения и обработки результатов измерений.

С другой стороны, наличие ПЛИС в составе SDR-устройств предоставляет пользователю возможность более гибко конфигурировать автоматизированный измерительный стенд в зависимости от проверяемого бортового блока, при этом программирование ПЛИС выполняется в той же среде LabVIEW, что и остальные программные части стенда [5–6]. Таким образом, рассматривая ВИС на основе стандарта PXI/PXIe, у инженеров-разработчиков появляется возможность пользоваться привычными средствами разработки без необходимости привлечения дополнительного штата программистов ПЛИС, что особенно актуально при разработке стендов для проверки бортовых систем, в частности, для проверки бортовых систем наблюдения. При этом одним из множества видов проверок систем наблюдения является проверка системы автоматического зависимого наблюдения в режиме радиовещания (англ. Automatic Dependent Surveillance-Broadcast, ADS-B)

с использованием методов и средств программно-аппаратного моделирования.

Дадим определение автоматизированного измерительного стенда в контексте решаемых задач. Автоматизированный измерительный стенд — это совокупность программных средств и средств вычислительной техники, обеспечивающая воспроизведение, моделирование и измерение параметров ВЧ сигналов с помощью ВП, при этом под ВП понимается средство измерения, реализованное на основе компьютерной программы, написанной на LabVIEW.

Рассмотрим более подробно предмет проверки — технологию ADS-B. Это технология, позволяющая лётчикам и авиадиспетчерам на наземном пункте наблюдать движение воздушных судов с большей точностью и получать аэронавигационную информацию. Суть технологии заключается в следующем. ВС, оборудованное приемопередатчиком (транспондером), посылает на частоте 1090 МГц широкополосные сообщения своих собственных текущих координат месторасположения на протяжении всего полёта. Кроме того, в данных широкополосных сообщениях передаются курс, высота, горизонтальная и вертикальная скорость. Приёмники ADS-B, встроенные в авиадиспетчерские пункты и системы управления воздушным движением, а также установленные на борту ВС, обеспечивают точное отображение на их экране вторичных радиолокационных систем (вторичных радиолокаторов, ВОРЛ). При этом ВС, посылающие сигналы ADS-B, могут находиться как в небе, так и на земле.

Таким образом, Таким образом, ADS-B — это система, предназначенная для взаимодействия между ВС [4], находящимися в воздухе или на земле, или иными наземными транспортными средствами в пределах зоны контроля за движением на аэродроме, которая периодически передает данные о векторе состояния (горизонтальное и вертикальное положение, горизонтальная и вертикальная составляющие скорости), а также иную информацию. Система ADS-B функционирует в автоматическом режиме, т.к. для нее не требуются внешние управляющие воздействия; она является зависимой в том смысле, что получает данные от инерциальных систем, баро- и радиовысотометров, навигационных источников и прочих других бортовых систем, передающих данные наблюдений другим пользователям. Для воздушных судов или транспортных средств не имеет значения, какие пользователи получают передаваемые ими данные; при этом пользователь, как воздушное судно, так и наземное транспортное средство, находящиеся в радиусе действия вещания, могут получать и обрабатывать данные наблюдения системы ADS-B. Система ADS-B позволяет оптимально использовать воздушное пространство, снижает ограничения по высоте / видимости, обеспечивает улучшенный контроль за состоянием наземных объектов, а также по-

вышает безопасность работы, например, путем разрешения конфликтных ситуаций.

Кроме того, имеется возможность получать информацию о погодных условиях и аэронавигации в зоне пролета для самолетных систем в графическом виде посредством технологии Flight Information Service — Broadcast (FIS-B). В конечном счете это позволяет пилоту ВС наглядно представлять динамично меняющуюся информацию об условиях полета [7].

Таким образом, технология ADS-B — это востребованный, эффективный инструмент, повышающий эффективность работы систем наблюдения, а кроме того, имеющий широкий спектр потенциального применения как в малой авиации, так и при использовании малых БПЛА [8–9].

Суть проверки ADS-B заключается в следующем. Комплексу бортового оборудования (КБО), функционирующему в составе имитационного стенда в реальном времени «подыгрывается» актуальная летная информация и соответствующая ей радиообстановка, которая задается в соответствии с моделью полета: данные маяков ILS, VOR, DME, координаты GNSS, воздушная скорость, барометрическая высота, направление движения, широта, долгота и т. д.

Блок ADS-B, в свою очередь, принимает от КБО эту информацию, и через приемопередатчик режима S, который отвечает за передачу по линии «воздух-земля», передает ее по ВЧ-тракту на приемную часть имитационного стенда (рис. 1).

Информация, передаваемая по линии «воздух-земля», представляет собой передаваемый на частоте 1090 МГц PPM-модулированный сигнал — т. е. сигнал, информация которого закодирована положением импульсов.

В данном случае это сигнал, состоящий из четырех импульсов преамбулы (представляющей вхождение в синхронизм) и 56 или 112 одно микросекундных отрезков, где импульс 0,5 мкс присутствует либо в его первой, либо во второй половине одно микросекундного интервала [10–11]. Импульс, содержащийся в первой части одно микросекундного отрезка будет считаться двоичной ЕДИНИЦЕЙ, а если импульс содержится во второй части одно микросекундного отрезка, то двоичным НУЛЕМ. Нумерация бит происходит в порядке их передачи, то есть начинается с первого бита. Если не предусмотрен иной вариант, цифровые значения групп (полей) битов, кодируются с помощью положительной двоичной системы, где первым передаваемым в сообщении битом является самый старший (most significant bit, MSB). Информация кодируется в полях, каждое из которых состоит по крайней мере из одного бита. Необходимо отметить, что сообщения ADS-B, а также любые другие сообщения, используемые описанный выше способ передачи информации, получили общее название как ответы режима S. Структура ответов режима S приведена на рис. 2.

Как нетрудно предположить из рис. 2 ответы режима S в целях однозначного декодирования представляет собой детерминированный набор полей, содержащий определенный тип информации о ВС. Структура и содержание полей блока данных, используемых в сообщениях ADS-B, приведена на рис. 3.

Как видно из рис. 3, сообщение ADS-B содержит 5 наборов полей:

— DF — закодированный в первых пяти битах формат сообщения ADS-B (форматы сообщений ADS-B кодируются как двоичные 17 (10001) или 18 (10010));

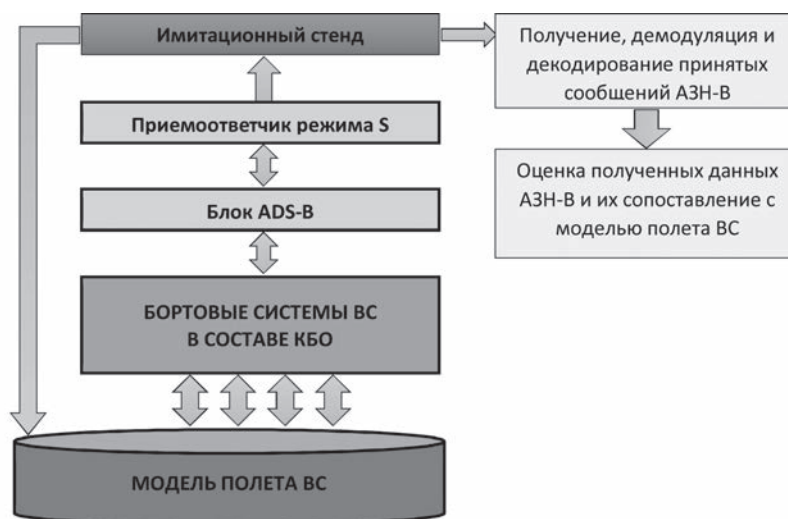


Рис. 1. Общая схема проверки АЗН-В

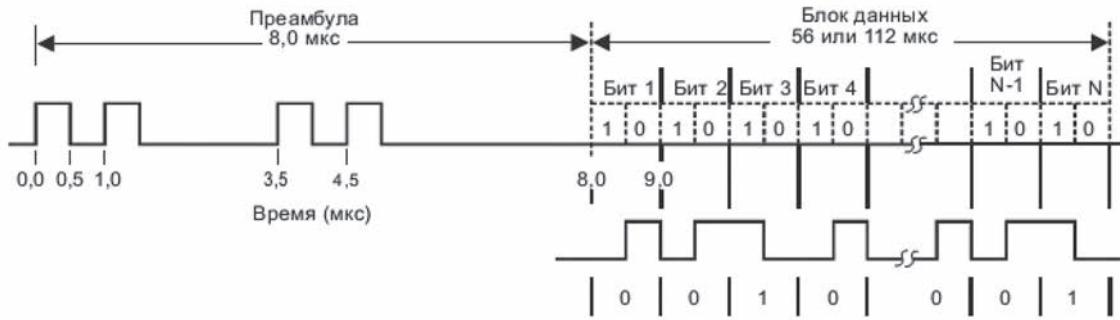


Рис. 2. Структура ответов режима S

DF:5	CA:3	AA:24	ME:56	PI:24
-------------	-------------	--------------	--------------	--------------

Рис. 3. Формат сообщений ADS-B

- CA — закодированные в 3-х битах возможности приемопередатчика режима S;
- AA — закодированный в 24 битах адрес BC;
- ME — закодированные в 56 битах сообщения;
- PI — закодированная в 24 битах проверка четности «четность-идентификатор запросчика»;

Ключевым полем, содержащим информацию о собственном ВС и передаваемом в виде всенаправленных сообщений, является поле ME. Данное поле имеет вид определенных регистров GICB (Ground-initiated Comm-B) [12,

13], значения которых для сообщений ADS-B приведены в табл. 1.

В качестве примера рассмотрим структуру поля ME, содержащую информацию о координатах BC в воздухе (GICB05₁₆), которая приведена в табл. 2.

Как видно из табл. 2, координаты BC содержатся в битах 22–38 и 39–55 поля ME и закодированы методом Compact Position Report (CPR). Суть алгоритма CPR [14] заключается в следующем: для эффективного кодирования данных о широте/долготе в сообщениях ряд старших

Таблица 1

Информация, содержащаяся в регистрах GICB, передаваемых в сообщениях ADS-B

Код регистра GICB (HEX)	Описание регистра
05	информация о местоположении в воздухе
06	информация о местоположении на земле
07	информация о статусе
08	информация об опознавательном индексе
09	информация о скорости при нахождении в воздухе

Таблица 2

Структура поля ME, содержащая информацию о местоположении BC в воздухе

Порядок следования бит	Описание полей
0-4	Код типа формата (Type Code)
5-6	Статус наблюдения (Surveillance Status)
7	Признак одной антенны (NIC supplement-B)
8-19	Высота (Altitude)
20	Время (Time UTC)
21	Формат (CPR odd/even frame flag)
22-38	Кодированная широта в формате CPR (Latitude in CPR format)
39-55	Кодированная долгота в формате CPR (Longitude in CPR format)

битов, которые, как правило, не меняются в течение длительного периода времени, не будут передаваться в каждом сообщении. Например, в прямом двоичном представлении данных о широте 1 бит указывает на то, находится ли воздушное судно в северном или южном полушарии. Этот бит и будет оставаться неизменным в течение достаточно длительного периода времени, возможно, даже на протяжении всего срока службы ВС. Повторяющаяся передача этого бита в каждом сообщении о местоположении по своей сути неинформативна [12].

Поскольку старшие биты передаваться не будут, то из этого следует, что многочисленные точки на земле возможно, будут выдавать аналогичную кодированную информацию о местоположении. То есть, если будет получено лишь одно сообщение о местоположении, декодирование будет являться неоднозначным с точки зрения определения правильности местоположения ВС, то есть, какое из множества решений будет являться правильным.

Метод CPR позволяет в принятых от ВС сообщениях однозначно определить его местоположение. Это достигается посредством совмещения при кодировании двух методов кодирования, которые между собой несильно отличаются. Каждый из двух фрагментов сообщений, называемых четным форматом и нечетным форматом, передается в течение примерно 50% времени. После получения обоих фрагментов в течение короткого периода (около 10 с) приемная система (или приемоответчик ВС) может однозначно определить местоположение ВС.

Алгоритм декодирования местоположения в воздухе заключается в следующем. Так как алгоритм CPR использует одно закодированное в четном формате сообщение о местоположении в воздухе, обозначенное как $XZ0$, $YZ0$ в совокупности с одним закодированным в нечетном формате, обозначенном как $XZ1$, $YZ1$, для восстановления значений широты R_{lat} и долготы R_{lon} глобального географического местоположения потребуется, как было сказано выше, некоторый период времени между, необходимый для сбора и анализа, не превышающее, однако 10 с.

Ограничение промежутка времени между донесениями о местоположении в четном и нечетном формате 10 с выбрано из следующих соображений. Максимальное допустимое разделение в 3 морские мили (5,56 км) и скорость ВС находятся в прямой зависимости: ВС, способное развивать скорость 1852 км/ч (1000 уз), пролетит за 10 с примерно 5,1 км (2,8 м. мили). Поэтому алгоритм CPR сможет однозначно декодировать его местоположение в течение 10-секундной задержки между донесениями о местоположении.

Рассмотрим процесс декодирования координат. Как было указано выше, в поле ME биты, отвечающие за кодирование широты имеют позицию 22–38, а за кодирование долготы — 39–55, то есть, на кодирование координат

отводится по 17 бит. Тогда при получении 17-битного донесения о местоположении в воздухе, закодированного в четном формате ($XZ0$, $YZ0$), и другого сообщения, закодированного в нечетном формате ($XZ1$, $YZ1$), с интервалом не более чем 10 с (примерно 3 м. мили), алгоритм CPR восстанавливает географическое местоположение на основе закодированных донесений о местоположении в следующей последовательности:

Как видно из табл. 2, координаты ВС содержатся в битах 22–38 и 39–55 поля ME и закодированы методом Compact Position Report (CPR). Суть алгоритма CPR [14] заключается в следующем: для эффективного кодирования данных о широте/долготе в сообщениях ряд старших битов, которые, как правило, не меняются в течение длительного периода времени, не будут передаваться в каждом сообщении. Например, в прямом двоичном представлении данных о широте 1 бит указывает на то, находится ли воздушное судно в северном или южном полушарии. Этот бит и будет оставаться неизменным в течение достаточно длительного периода времени, возможно, даже на протяжении всего срока службы ВС. Повторяющаяся передача этого бита в каждом сообщении о местоположении по своей сути неинформативна [12].

Поскольку старшие биты передаваться не будут, то из этого следует, что многочисленные точки на земле возможно, будут выдавать аналогичную кодированную информацию о местоположении. То есть, если будет получено лишь одно сообщение о местоположении, декодирование будет являться неоднозначным с точки зрения определения правильности местоположения ВС, то есть, какое из множества решений будет являться правильным.

Метод CPR позволяет в принятых от ВС сообщениях однозначно определить его местоположение. Это достигается посредством совмещения при кодировании двух методов кодирования, которые между собой несильно отличаются. Каждый из двух фрагментов сообщений, называемых четным форматом и нечетным форматом, передается в течение примерно 50% времени. После получения обоих фрагментов в течение короткого периода (около 10 с) приемная система (или приемоответчик ВС) может однозначно определить местоположение ВС.

Алгоритм декодирования местоположения в воздухе заключается в следующем. Так как алгоритм CPR использует одно закодированное в четном формате сообщение о местоположении в воздухе, обозначенное как $XZ0$, $YZ0$ в совокупности с одним закодированным в нечетном формате, обозначенном как $XZ1$, $YZ1$, для восстановления значений широты R_{lat} и долготы R_{lon} глобального географического местоположения потребуется, как было сказано выше, некоторый период времени между, необходимый для сбора и анализа, не превышающее, однако 10 с.

Ограничение промежутка времени между донесениями о местоположении в четном и нечетном формате 10 с выбрано из следующих соображений. Максимальное допустимое разделение в 3 морские мили (5,56 км) и скорость ВС находятся в прямой зависимости: ВС, способное развивать скорость 1852 км/ч (1000 уз), пролетит за 10 с примерно 5,1 км (2,8 м. мили). Поэтому алгоритм CPR сможет однозначно декодировать его местоположение в течение 10-секундной задержки между донесениями о местоположении.

Рассмотрим процесс декодирования координат. Как было указано выше, в поле ME биты, отвечающие за кодирование широты имеют позицию 22–38, а за кодирование долготы — 39–55, то есть, на кодирование координат отводится по 17 бит. Тогда при получении 17-битного донесения о местоположении в воздухе, закодированного в четном формате (XZ0, YZ0), и другого сообщения, закодированного в нечетном формате (XZ1, YZ1), с интервалом не более чем 10 с (примерно 3 м. мили), алгоритм CPR восстанавливает географическое местоположение на основе закодированных донесений о местоположении в следующей последовательности:

1. Расчет размера широтной зоны в направлении север– юг для четных ($i = 0$) и нечетных ($i = 1$) пар (D_{lat0} и D_{lat1}) по формуле:

$$D_{lat} = \frac{360^\circ}{4 \cdot NZ - i}, \quad (1)$$

где NZ — число географических широтных зон между экватором и полюсом устанавливается равным 15.

2. Расчет индекса широты j по формуле:

$$j = floor\left(\frac{59 \cdot YZ_0 - 60 \cdot YZ_1}{2^{17}} + \frac{1}{2}\right). \quad (2)$$

3. Расчет значений для четных сообщений ($i = 0$) R_{lat0} и нечетных ($i = 1$) сообщений R_{lat1} по формуле:

$$R_{lati} = D_{lati} \cdot \left(MOD(j, 60 - i) + \frac{YZ_i}{2^{17}} \right). \quad (3)$$

Значения R_{lati} в южном полушарии будут лежать в диапазоне 270°–360°. Посредством вычитания из этих значений 360° устанавливается значение R_{lati} в диапазоне от –90° до +90°.

4. Проверка на удвоение переходной широты $NL(R_{lati})$.

$NL(x)$ обозначает функцию «число долготных зон», представляющую широтный угол x . Значение, определяемое функцией $NL(x)$, ограничивается диапазоном 1–59. Значение $NL(x)$ определяется для большинства широт следующим уравнением:

$$NL(x) = floor\left(2\pi \cdot \left[\arccos\left(1 - \frac{1 - \cos\left(\frac{\pi}{2 \cdot NZ}\right)}{\cos^2\left(\frac{\pi}{180} \cdot |lat|\right)}\right) \right]^{-1}\right), \quad (4)$$

где lat — широтный аргумент, представленный в градусах.

В случае, когда (4) для расчетов в реальном времени непригодно, рекомендуется предварительно рассчитать таблицу переходных широт, используя следующую формулу [7]:

$$lat = \frac{180^\circ}{\pi} \cdot arccos\left(\sqrt{\frac{1 - \cos\left(\frac{\pi}{2 \cdot NZ}\right)}{1 - \cos\left(\frac{2\pi}{2 \cdot NL}\right)}}\right), \quad (5)$$

где NL принимает значения $2 \dots 4 \cdot NZ - 1$.

Таким образом, если $NL(R_{lat0}) \neq NL(R_{lat1})$, то два местоположения удваивают переходную широту и, следовательно, невозможно определить глобальную долготу. В этом случае необходимо дождаться новых сообщений ADS-B с координатами местоположения и провести расчеты по формулам 1–5 заново.

5. Расчет размера долготной зоны в направлении «восток– запад» для четных ($i = 0$) и нечетных ($i = 1$) пар (D_{lon0} и D_{lon1}) по формуле:

$$D_{lat} = \frac{360^\circ}{n_i}, \quad (6)$$

где n_i — максимальное значение из $[NL(R_{lati}) - i, 1]$, где расчет R_{lati} производится рассчитанное согласно (5).

6. Расчет индекса долготы по формуле:

$$j = floor\left(\frac{XZ_0 \cdot (NL - 1) - XZ_1 \cdot NL}{2^{17}} + \frac{1}{2}\right), \quad (7)$$

где $NL = NL(R_{lati})$

7. расчет глобальной долготы R_{loni} для четного ($i = 0$) и нечетного ($i = 1$) сообщения по формуле:

$$R_{loni} = D_{loni} \cdot \left(MOD(m, n_i) + \frac{XZ_i}{2^{17}} \right); \quad (8)$$

Таким образом, пары для четных и нечетных сообщений, рассчитанные по (3) и (8) и есть принятые и декодированные координаты.

Рассмотрим процесс декодирования сообщений ADS-B. Для обеспечения высокой скорости обработки, модулированные сообщения ADS-B принимаются автоматизированным измерительным стендом на приемник ПЛИС, где происходит его демодуляция в соответствии с положениями, указанными на рис. 2 и рис. 3. Для приня-

тия решения о целостности принятого сообщения проводится проверка на четность в соответствии с правилами, изложенными в [10, 15]. Если результат проверки четности положительный, то демодулированное сообщение подлежит декодированию, в противном случае необходимо дождаться нового сообщения. Результат демодуляции представляет собой массив из 112 булевских элементов, который передается в систему реального времени посредством буфера DMA FIFO target-to-host для потокового декодирования.

В общем случае система реального времени проводит расчет параметров радиообстановки для КБО, а задача декодирования сообщений ADS-B является лишь одной из частных задач. В целях экономии вычислительных ресурсов система реального времени передает принятый из ПЛИС двоичный массив на декодирование на ЭВМ оператора (HOST PC). Для решения задачи декодирования сообщений ADS-B был разработан набор пользовательских библиотек в LabVIEW. Данный набор библиотек позволяет декодировать все регистры GICB сообщений ADS-B, приведенные в таб. 1, а также выполнять необходимые расчеты, позволяющие проводить однозначное в глобальном масштабе декодирование местоположения в воздухе.

Схема виртуальной измерительной системы, представляющей прототип автоматизированного измерительного стенда, и выполняющей функции SDR-приемника приведена на рис 4.

Следует отметить, что наличие системы реального времени позволяет выполнять в том числе потоковое декодирование принятых сообщений за время, кратное 1 мкс, а имеющихся ресурсов системы достаточно не только для декодирования ADS-B, но и других сообщений, например, ответов ВС на запросы вторичного обзорного радиолока-

тора (ВОРЛ) или бортовой системы предупреждения столкновений (БСПС).

Таким образом, полученный подход позволяет рассматривать процесс декодирования сообщений как одну из подпрограмм, которая будет вызываться при распознавании соответствующего типа сообщения.

Так как сообщения ADS-B — лишь часть общего протокола взаимодействия «воздух-земля» и «воздух-воздух», основанный на тех же принципах модуляции, то в дальнейшем в планируется на основе унифицированного подхода при написании ПО как для FPGA так и для HOST-PC расширить функциональность измерительного стенда за счет декодирования однозначного в местном масштабе местоположения в воздухе (на земле), ответов от приемопередатчиков режима А/С (данные о барометрической высоте ВС), ответов на запросы ВОРЛ и БСПС.

Таким образом, полученные результаты позволяют сделать вывод о том, что унификация ПО автоматизированных измерительных стендов вкпе с программной обработкой позволяет существенно расширить спектр принимаемых от ВС сообщений без необходимости модернизации и доработки аппаратной части автоматизированных измерительных стендов.

Литература

1. *Симонов П.И., Кубанков Ю.А.* Компьютерные методы измерений параметров телекоммуникационных средств: стандарты и подходы. М.: Горячая линия – Телеком, 2018. 106 с.
2. *Рубичев Н.А.* Измерительные информационные системы. М.: Дрофа. 2010. 334 с.
3. *Симонов П.И., Кубанков Ю.А.* Повышение качества проверки высокочастотных радиотехнических

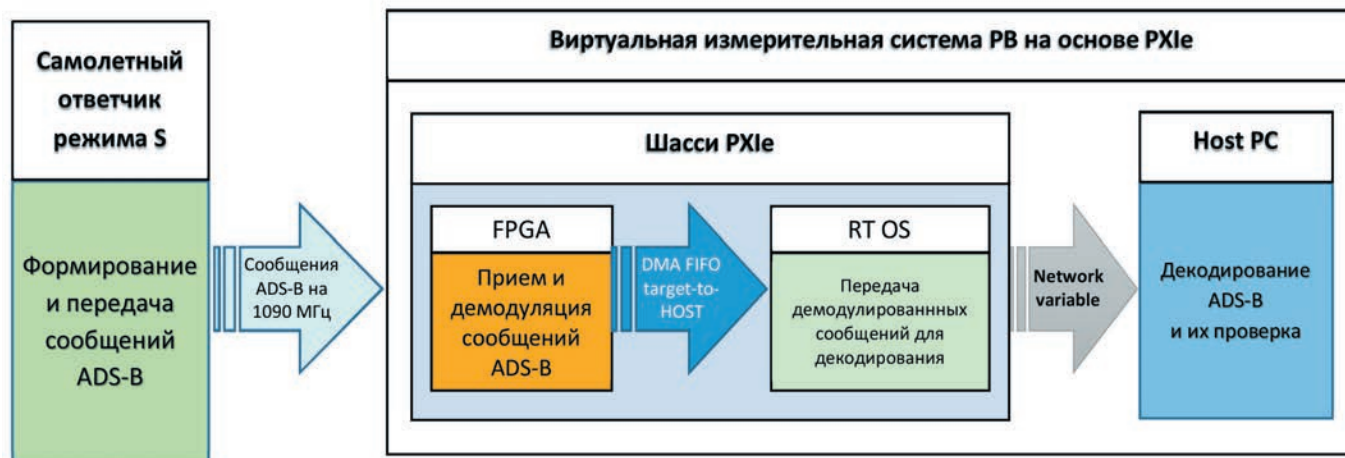


Рис. 4. Схема ВИС, выполняющей функции SDR-приемника

средств радиоизмерительным оборудованием на основе стандартов PXI/PXIe // Специальная техника. 2016. № 5. С. 16–21.

4. 1090-WP30–18. Minimum operational performance standards for 1090 MHz extended squatter Automatic Dependent Surveillance — Broadcast (ADS-B) and Traffic Information Services — Broadcast (TIS-B)/ Washington, DC. SC-186. RTCA Inc. 2009.

5. *Симонов П. И.* Предложения по увеличению числа доступных приборов в виртуальных измерительных системах с ограниченным числом измерительных трактов // Системы и средства связи, телевидения и радиовещания. 2012. № 1, 2. С. 65–66.

6. *Силин А.* Технология Software Defined Radio. Теория, принципы и примеры аппаратных платформ // Беспроводные технологии. 2007. № 2. URL: <http://www.wireless-e.ru/articles/technologies/200> (дата обращения 22.01.2018).

7. National Instruments: Software Defined Radio: Past, Present, and Future. 2017. URL: <http://www.ni.com/white-paper/53706/en/> (дата обращения: 19.01.2018)

8. *Смирнов В. С., Знаменская К. С.* Метод АЗН-В (автоматическое зависимое наблюдение в режиме радиовещания) // Актуальные проблемы гуманитарных и социально-экономических наук. Специальный выпуск. 2016. Т. 10s-1. С. 129–131.

9. Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic, Depend-

ent Surveillance — Broadcast (ADS-B). Washington, DC: SC-186, RTCA Inc. 2009.

10. *Guterres R. M., Jones S. R., Dr. Massimini S. V., Strain R. C.* ADS-B Surveillance in High Density SUAS Applications at Low Altitudes // International Symposium on Enhanced Solutions for Aircraft and Vehicle Surveillance Applications. Berlin, 07–08 April 2016.

11. Приложение 10. Авиационная электросвязь. Том IV: Системы наблюдения и предупреждения столкновений. 5-е издание. Монреаль: ИКАО, 2014. 232 с.

12. *Guterres R. M., Jones S. R., Orrell G. L., Strain R. C.* ADS-B Surveillance System Performance with Small UAS at Low Altitudes // AIAA Information Systems-AIAA Infotech @ Aerospace, AIAA SciTech Forum, (AIAA 2017–1154). 2017. 15 p. doi.org/10.2514/6.2017–1154

13. Doc 9871. Технические положения, касающиеся услуг режима S и расширенного сквиттера. 2-е издание. 2012. Монреаль: ИКАО, 352 с

14. 1090-WP-14–09R1. Appendix A. Extended Squitter and TIS-B Formats And Coding Definitions/Washington, DC. SC-186. RTCA Inc. 2002.

15. *Gertz J. L.* Fundamentals of Mode S Parity Coding. Project Report ATC-117. Lexington, Lincoln Laboratory. Massachusetts Institute Of Technology. 1984. 36 p.

16. Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II)/ Washington, DC. RTCA Inc. 2008.



METHOD OF DECODING ADS-B MESSAGES ON AUTOMATED MEASUREMENT STANDS BUILT ON LABVIEW FRAMEWORK, AS PART OF THE AIRCRAFT BOARD SYSTEMS QUALITY CONTROL

PAVEL I. SIMONOV

Moscow, Russia, sonar83@mail.ru

YURY A. KUBANKOV

Moscow, Russia, yury.kubankov@ya.ru

KEYWORDS: ADS-B, LabVIEW, measurements, automated measuring stand, virtual measuring system, quality.

ABSTRACT

The article reviews a method for constructing SDR-systems for receiving, demodulating and decoding automatic dependent surveillance (ADS-B) broadcast messages received from an aircraft in the context of unifying a software package for automated measuring stands built using virtual instrument technology and imitating board systems and real flight factors, including the radio environment.

The essence of the concept of a programmable radio is considered, which means that the basic parameters of the hardware components of the transceiver are determined not by hardware, but by the software indeed, opposite to the analog transceiver systems.

The essence of the technology of virtual instruments and virtual measuring systems, built on their basis, is revealed, their advantages are noted in relation to the construction of automated measuring stands. The definition of an automated measuring stand as a combination of software and computer facilities providing reproduction, modeling and measurement of high-frequency signals by means of a virtual device, is provided. This means a measurement tool implemented on the LabVIEW framework.

The article narrowly reviews verification procedure and the essence of the technology of ADS-B, which allows the pilots and air traffic controllers at the ground station to obtain aeronautical information with greater accuracy.

The method of obtaining and transferring a demodulated message to the program part of the SDR-system for subsequent decoding is reviewed. The structure, types and kinds of broadcast messages, as well as the main GICB registers transmitted in ADS-B messages, are considered. The process of extracting information using a sample of position messages in the air coded by the Compact Position Report method is shown.

The obtained results allowed to conclude that unification of software together with software processing of demodulated information allows to significantly expand the range of messages received from the aircraft, for example, messages from a secondary surveillance radar or an airborne collision avoidance system without the need to upgrade and refine the hardware of automated measuring stands.

REFERENCES

1. Simonov P.I., Kubankov Y.A. *Komp'yuternye metody izmereniy parametrov telekommunikatsionnykh sredstv: standarty i podkhody* [Computer methods for measuring the parameters of telecommunications: standards and approaches]. Moscow: Goryachaya Linia – Telecom, 2018. 106 p.
2. Rubichev N.A. *Izmeritel'nye informatsionnye sistemy* [Measuring information systems: a manual]. Moscow: Drofa, 2010. 334 p.
3. Simonov P.I., Kubankov Y.A. Povyshenie kachestva proverki vysokochastotnykh radiotekhnicheskikh sredstv radioizmeritel'nykh oborudovaniem na osnove standartov PXI/PXIe [Improving the quality of testing high-frequency radio equipment using radio equipment based on PXI / PXIe standards]. *Spetsialnaya Tekhnika* [Special equipment]. 2016. No. 5. Pp.16-21.
4. 1090-WP30-18. Minimum operating performance standards for 1090 MHz extended squatter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B) / Washington, DC. SC-186. RTCA Inc. 2009.
5. Simonov P.I. Proposals for increasing the number of available instruments in virtual measuring systems with a limited number of measuring paths. *Sistemy i sredstva svyazi, televideniya i radioveshchaniya* [Systems and means of communication, television and radio broadcasting]. 2012. No. 1, 2. Pp. 65-66.
6. Silin A. *Tekhnologiya Software Defined Radio. Teoriya, printsipy i primery apparatnykh platform* [Software Defined Radio technology. Theory, principles and examples of hardware platforms]. *Wireless Technologies*. 2007. No. 2. URL: <http://www.wireless-e.ru/articles/technologies/200> (date of access 22.01.2018)
7. National Instruments: *Software Defined Radio: Past, Present, and Future*. 2017. URL: <http://www.ni.com/white-paper/53706/en/> (date of access 01.19.2018)
8. Smirnov V.S., Znamenskaya K.S. Method ADS-B (automatic dependent surveillance broadcast mode). *Aktual'nye problemy humanitarnykh i sotsial'no-ekonomicheskikh nauk. Spetsial'nyy vypusk*. [Actual problems of humanitarian and socio-economic sciences. Special issue]. 2016. Vol. 10s-1. Pp. 129-131.

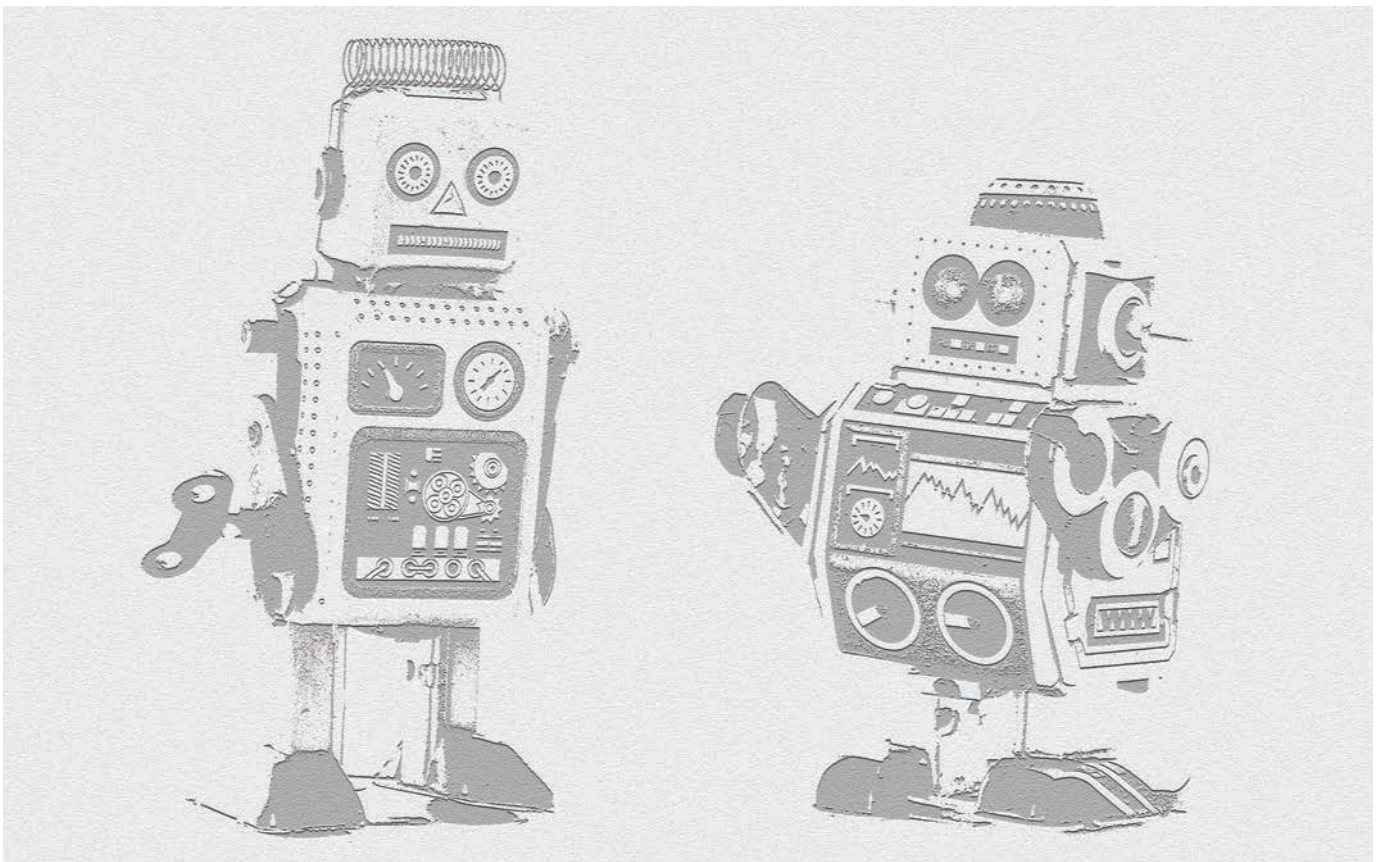
9. Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic, Dependent Surveillance – Broadcast (ADS-B). Washington, DC: SC-186, RTCA Inc. 2009.
10. Guterres R.M., Jones S.R., Dr. Massimini S.V., Strain R.C. ADS-B Surveillance in High Density SUAS Applications at Low Altitudes. *International Symposium on Enhanced Solutions for Aircraft and Vehicle Surveillance Applications*. Berlin, 07-08 April 2016.
11. Annex 10. Aeronautical Telecommunications. Vol. 4. Observation and collision avoidance systems. 5th edition. International Civil Aviation Organization. Montreal: ICAO, 2014. 232 p.
12. Guterres R.M., Jones S.R., Orrell G.L., Strain R.C. ADS-B Surveillance System Performance with Small UAS at Low Altitudes. AIAA Information Systems-AIAA Infotech @ Aerospace, AIAA SciTech Forum, (AIAA 2017-1154). 2017. 15 p. doi.org/10.2514/6.2017-1154
13. Doc 9871. Technical provisions for Mode S services and ex-

- tended squitter. International Civil Aviation Organization. Second edition 2012. 352 p.
14. 1090-WP-14-09R1. Appendix A. Extended Squitter and TIS-B Formats And Coding Definitions. Washington, DC. SC-186. RTCA Inc. 2002.
15. Gertz J.L. *Fundamentals of Mode S Parity Coding*. Project Report ATC-117. Lexington, Lincoln Laboratory. Massachusetts Institute Of Technology. 1984. 36 p.
16. Minimum Operational Performance Standards for Traffic Alert and Collision Avoidance System II (TCAS II). Washington, DC. RTCA Inc. 2008.

INFORMATION ABOUT AUTHORS:

Simonov P.I., PhD, Lead Engineer of State Research Institute of Aviation Systems (GosNIIAS);
Kubankov Yu.A., PhD, Docent of Moscow Technical University of Communication and Informatics.

FOR CITATION: Simonov P.I., Kubankov Yu.A. Method of decoding ADS-B messages on automated measurement stands built on LabVIEW framework, as part of the aircraft board systems quality control. *H&ES Research*. 2018. Vol. 10. No. 2. Pp. 12-21. doi 10.24411/2409-5419-2018-10037 (In Russian)



doi 10.24411/2409-5419-2018-10038

ТЕОРЕТИЧЕСКИЙ ПОДХОД ПО ОЦЕНИВАНИЮ И ОБЕСПЕЧЕНИЮ ЖИВУЧЕСТИ РАСПРЕДЕЛЕННЫХ СЕТЕЙ СВЯЗИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

БЕЛОВ**Андрей Сергеевич¹****СКУБЬЕВ****Александр Васильевич²****АННОТАЦИЯ**

В условиях совершенствования форм и способов ведения информационного противоборства, существенное значение в поддержании требуемых показателей качества сетей связи приобретает процесс оценивания и обеспечения живучести ее элементов. Существующие методы и способы построения радиоизлучающих средств распределенных сетей связи не способны обеспечить основные показатели живучести из-за наличия явных демаскирующих признаков. В работе рассмотрен теоретический подход (модель, метод оценивания и способ обеспечения живучести), применение которого позволит оценивать и обеспечивать живучесть распределенных сетей связи в условиях внешних деструктивных воздействий. При оценивании живучести распределенных сетей связи производится декомпозиция сети связи на составные части и основные показатели живучести рассчитываются отдельно по каждой составной части сети связи, в том числе по всем радиоизлучающим средствам. Например, основные показатели живучести i -й абонентской станции оцениваются от соотношения сигнал/шум на входе приёмника средства мониторинга противника при заданной вероятности ложной тревоги. Результаты проведенных расчетов позволяют обеспечивать живучесть сетей связи, используя организационные и организационно-технические способы, а именно, за счет: реконфигурации сетей связи, управления основными показателями живучести распределенных сетей связи с учетом соотношений сигнал/шум на входах средств мониторинга злоумышленников при заданной вероятности ложной тревоги, корректировки диаграмм направленности радиоизлучающих средств и их соответствующего построения на распределенной территории, координации маршрутов движения абонентов, в которых вероятность обнаружения средствами мониторинга противника будет минимальной и максимальной, а также соответствующих им азимутов ориентаций главных лепестков диаграммы направленности передающих антенн абонентских станций на приёмные базовые станции.

Сведения об авторах:

¹к.в.н., доцент, докторант Михайловской военной артиллерийской академии, г. Санкт-Петербург, Россия, andrej2442016@yandex.ru

²адъюнкт Академии Федеральной службы охраны Российской Федерации, г. Орел, Россия, skub777@mail.ru

КЛЮЧЕВЫЕ СЛОВА: живучесть; информационное противоборство; деструктивные воздействия; абонент; станция.

Для цитирования: Белов А.С., Скубьев А.В. Теоретический подход по оцениванию и обеспечению живучести распределенных сетей связи в условиях информационного противоборства // Научные технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 22-33. doi 10.24411/2409-5419-2018-10038.

В условиях информационного противоборства (ИП) возможны злонамеренные скрытые деструктивные воздействия на арендованные распределённые сети связи (РСС), задействованные для обеспечения функционирования автоматизированных систем управления военного назначения. Основными воздействиями могут быть несанкционированный доступ (атаки, взломы и т. п.) повлекшие как нарушение работоспособного состояния РСС, так и полный или частичный отказ в обслуживании их пользователей. Эффективность деструктивных воздействий прямо пропорциональна уровню технологического развития и масштабам использования компьютерной техники в современных РСС.

Под РСС понимают распределённую радиально-зональную сеть связи, предназначенную для предоставления услуг связи мобильным абонентам. В состав сети входят: абонентские станции, базовые станции, узлы связи, вспомогательные технические средства и программное обеспечение, с помощью которых формируется распределённая территориальная зона, на которой возможны подключения через радиointерфейс абонентских станций [1, 11].

Влияние на РСС и ее элементы последствий применения злоумышленником деструктивных воздействий приведут к существенному снижению эффективности функционирования РСС в условиях ИП.

Кроме того, многочисленные исследования, проведенные в данной области, показывают, что существующие инфо-телекоммуникационные ресурсы, обеспечивающие основные свойства, например, живучесть РСС, обладают крайней медлительностью и негибкостью. Это приводит к неспособности данных систем адаптироваться к быстро изменяющимся условиям, в которых функционируют РСС и вследствие этого, снижается эффективность их функционирования в условиях ИП.

Разработанные теоретические подходы не учитывают изменившуюся динамику функционирования, а также, многофазность и нестационарность РСС. Существующие подходы, а также критерии эффективности функционирования РСС требуют существенной корректировки [1–11].

Таким образом, реформирование системы государственного и военного управления, зависимость успешности задач, решаемых системой государственного и военного управления от требуемого уровня живучести РСС, наличие динамически развивающихся методов и способов ведения ИП обуславливают необходимость комплексного решения сформулированной задачи.

В ходе проведения исследований сформулирован теоретический подход, в частности, модель и метод оценивания живучести РСС в условиях ИП, позволяющие набрать соответствующую статистику, а также, способ обеспечения живучести РСС, позволяющий управлять основными показателями живучести РСС.

Живучесть характеризует устойчивость РСС против действия причин (стихийных и преднамеренных), лежащих вне системы и приводящих к разрушениям или значительным повреждениям некоторой части её элементов — узлов, абонентских и базовых станций, линий и каналов связи [13].

Блок-схема, поясняющая теоретический подход по оцениванию и обеспечению живучести РСС представлена на (рис. 1), где в блоке 1 задают (вводят) исходные данные, необходимые для проектирования и моделирования РСС, а именно: район SMR перемещения мобильных абонентов, количество K мобильных абонентов, потребности каждого из абонентов в скорости A_i ($i=1..K$) информационного обмена, количество ближайших к району SMR перемещения мобильных абонентов узлов доступа ЕСЭ [1.. m]; районы NNR_i ($i=1..m$) размещения ближайших к району SMR перемещения мобильных абонентов узлов доступа ЕСЭ, технические данные используемых абонентских и базовых станций (мощность передатчиков P_{BS} и P_{AC} , реальная чувствительность приёмников q_{BS} и q_{AC} , ширина диаграммы направленности передающих и приёмных антенн $\Theta_{BS}^{пер}$, $\Theta_{BS}^{прм}$, $\Theta_{AC}^{пер}$, $\Theta_{AC}^{прм}$, коэффициенты усиления передающих и приёмных антенн $G_{BS}^{пер}$, $G_{BS}^{прм}$, $G_{AC}^{пер}$, $G_{AC}^{прм}$), множество частот FF , разрешённых для назначения в качестве передающих частот базовых станций и передающих частот абонентских станций, район ER размещения злоумышленников, имеющиеся у злоумышленников средства и возможности по мониторингу и воздействию на сети связи, требования к живучести РСС $K_{ж\text{треб}}$, время t_k окончания обслуживания абонентов в заданном районе SMR .

В блоке 2 моделируют разделение на передающую и приемную части антенно-фидерного тракта абонентских станций. Для разделения антенно-фидерного тракта абонентской станции необходимо исключить из состава абонентской станции дуплексер, приёмопередающую антенну, вновь ввести в состав абонентской станции передающую направленную антенну и фидер, соединяющий передающую антенну с передатчиком абонентской станции, а также направленную приемную антенну и фидер, соединяющий приёмную антенну с приёмником. Моделируют оснащение абонентских станций системами наведения передающих и приёмных антенн.

В блоке 3 моделируют разделение базовых станций по выполняемым функциям на передающие и приёмные, при этом сами станции могут оставаться в готовности выполнить в требуемый момент времени функции передающих или приёмных.

Разделение базовых станций по выполняемым функциям на передающие и приёмные может быть выполнено по типовому варианту развертывания и эксплуатационного обслуживания стационарных КВ радиолиний с территориально-разнесенными приёмными и передающими радиоцентрами.

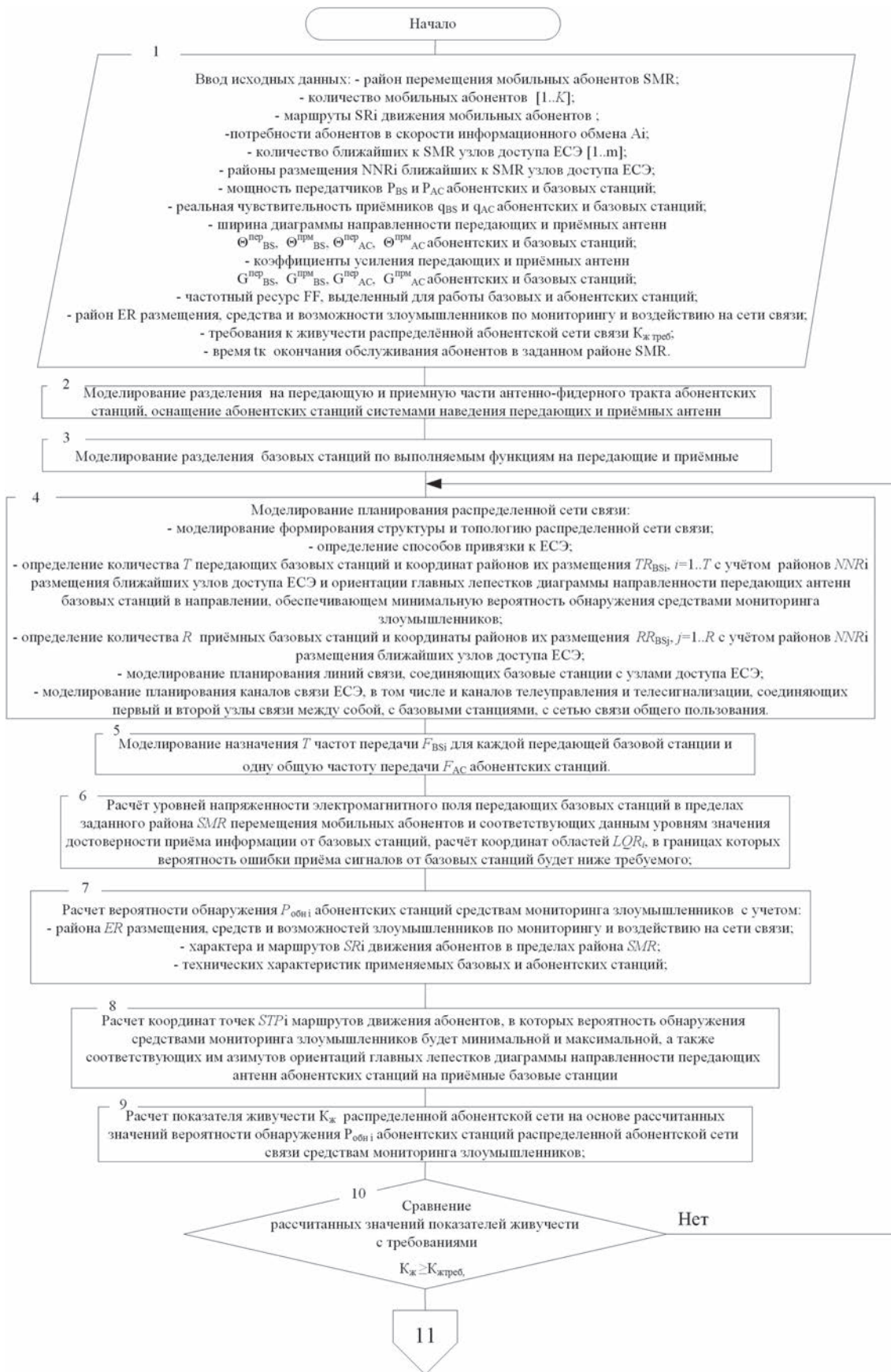


Рис. 1а. Блок-схема, поясняющая теоретический подход по оцениванию и обеспечению живучести РСС (начало)

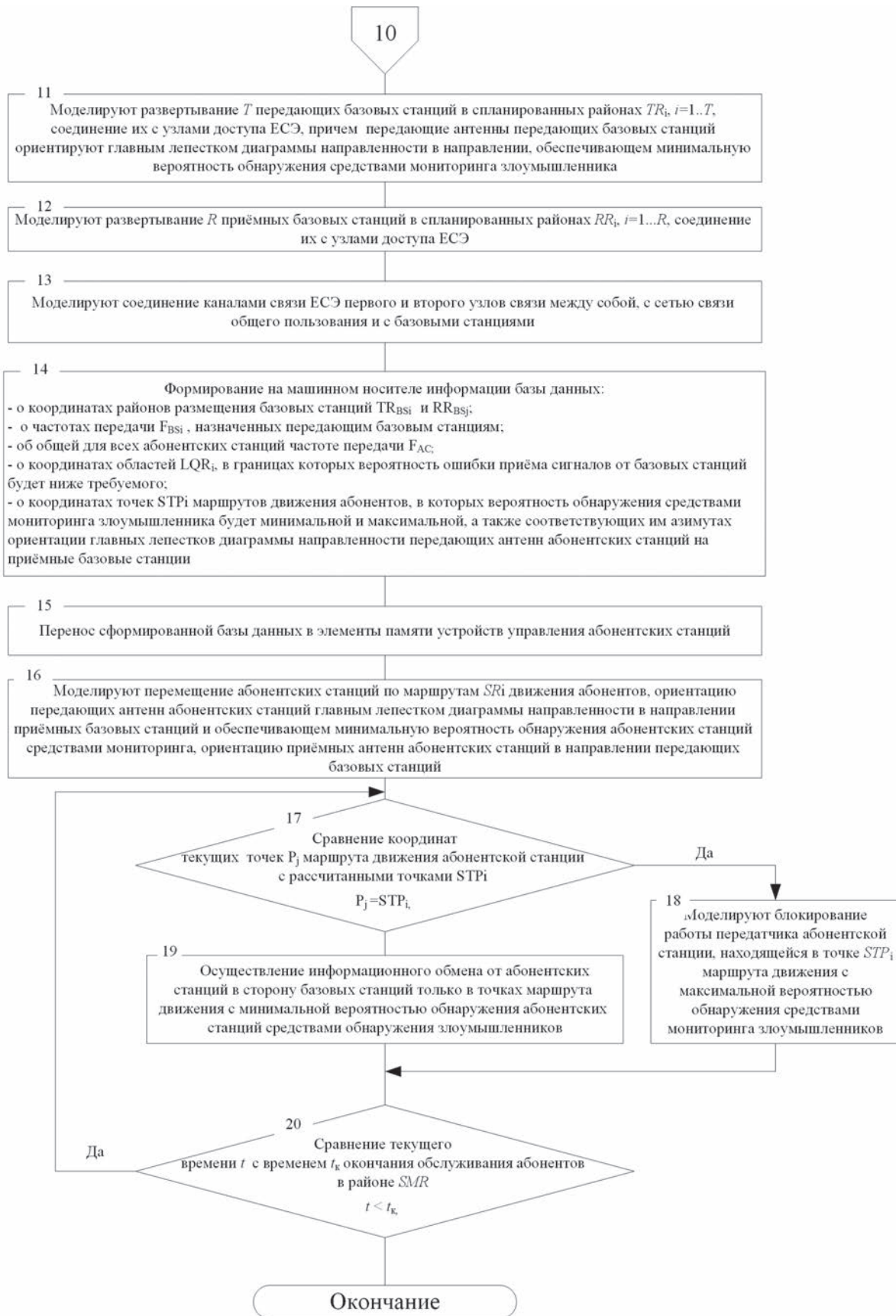


Рис. 16. Блок-схема, поясняющая теоретический подход по оцениванию и обеспечению живучести РСС (окончание)

В блоке 4 моделируют планирование РСС, а именно: моделируют формирование структуры и топологии РСС, определяют способы привязки к ЕСЭ с учетом количества узлов доступа — m и районов их размещения — $NNR_i (i=1..m)$.

Узлы доступа для привязки РСС располагаются, как правило, на объектах сети связи общего пользования ЕСЭ. Привязка к такому объекту и приём из ЕСЭ необходимого числа цифровых каналов и трактов передачи осуществляется с использованием оборудования плезеохронной и синхронной цифровой иерархии.

Структурно — топологическое построение РСС осуществляется с учетом следующих элементов: базовых станций (передающих и приёмных), узлов связи (первого и второго), линий связи и каналов связи.

Определяют количество T передающих базовых станций координаты районов их размещения $TR_{BSj}, i=1..T$. Определяют количество R приёмных базовых станций координаты районов их размещения $RR_{BSj}, j=1..R$. При определении количества базовых станций R, T и координат районов их размещения исходят из: предполагаемого района ER размещения средств мониторинга злоумышленников и недопустимости ориентации главных лепестков диаграммы направленности передающих антенн абонентских и передающих базовых станций в направлении на средства мониторинга злоумышленников.

Моделируют планирование линий связи, соединяющих базовые станции с узлами доступа ЕСЭ, а именно: каждой линии определяется род связи, её образующий (радиорелейный, кабельный), пропускная способность линии, а при необходимости — частоты и азимуты антенн. При этом сформированные линии не должны излучать главным лепестком диаграммы направленности антенны в сторону района ER размещения злоумышленников.

Моделируют планирование каналов связи ЕСЭ для соединения первого и второго узлов связи между собой, для соединения первого и второго узлов связи с сетью связи общего пользования, для соединения первого и второго узлов связи с базовыми станциями.

В блоке 5 из множества FF разрешенных к использованию частот, моделируют назначение T частот передачи F_{BSi} для каждой передающей базовой станции и одну общую частоту передачи F_{AC} абонентских станций. Частоты выбирают с учётом правил назначения рабочих частот конкретных моделей базовых и абонентских станций [14–31].

В блоке 6 осуществляют расчёт уровней напряженности электромагнитного поля передающих базовых станций в пределах заданного района SMR перемещения мобильных абонентов и соответствующих данным уровням значений достоверности приёма информации от базовых станций, имитируют формирование координат областей LQR_p в границах которых достоверность приёма сигналов от базовых станций будет ниже требуемого значения [3–11].

В блоке 7 осуществляют расчет вероятности обнаружения Робнi абонентских станций средствами мониторинга злоумышленников с учетом: района ER размещения, средств и возможностей злоумышленников по мониторингу и воздействию на РСС; характера и маршрутов SR_i движения абонентов в пределах района SMR ; технических характеристик применяемых базовых и абонентских станций. Расчёт вероятности обнаружения $P_{обнi}$ i -й абонентской станции с учётом направления (ориентации) передающей антенны абонентской станции главным лепестком диаграммы направленности на приёмную базовую станцию и соответствующему данной ориентации положению побочных лепестков диаграммы направленности антенны (боковых, задних) относительно средств мониторинга злоумышленников производится по формуле [13–14]:

$$P_{обнi} = \frac{q - \overline{\Phi}(1 - P_{ЛТ})}{\sqrt{1 + q}}, \quad (1)$$

где $P_{обнi}$ — вероятность обнаружения (правильного обнаружения);

q — отношение сигнал/шум на входе средства мониторинга злоумышленников;

$\overline{\Phi}(1 - P_{ЛТ})$ — интеграл вероятности;

$P_{ЛТ}$ — вероятность ложной тревоги.

Отношением сигнал/шум называется частное от деления мощности сигнала на входе приёмника средства мониторинга $P_{Свх}$ на мощность шума $P_{Швх}$ в той же точке:

$$q = \frac{P_{Свх}}{P_{Швх}}, \quad (2)$$

В блоке 8 осуществляют расчет координат точек STP_i маршрутов движения абонентов, в которых вероятность обнаружения средствами мониторинга злоумышленников будет минимальной и максимальной, а также соответствующих им азимутов ориентаций главных лепестков диаграммы направленности передающих антенн абонентских станций на приёмные базовые станции.

В блоке 9 осуществляют расчёт показателя живучести: коэффициента $K_{ж}$ РСС на основе рассчитанных значений вероятности обнаружения $P_{обнi}$ абонентских станций средствами мониторинга злоумышленников.

Живучесть $K_{жи}$ i -й абонентской станции определяется по формуле [13–14]:

$$K_{жи} = 1 - (1 - (1 - P_{обнi} \cdot P_{оци})) \cdot P_{поi}, \quad (3)$$

где $P_{обнi}$ — вероятность обнаружения i -й абонентской станции;

$P_{оци}$ — вероятность оценки параметров абонентской станции, необходимых для её уничтожения злоумышленниками;

$P_{поi}$ — вероятность применения злоумышленниками воздействия по абонентской станции.

С развитием средств высокоточного вооружения и увеличением способностей средств мониторинга злоумышленников по обнаружению наземных объектов в любых погодных условиях примем, что вероятности $P_{\text{ош}}$ и $P_{\text{пог}}$ стремятся к единице. Тогда выражение (3) преобразуется к виду:

$$K_{\text{ж}i} = 1 - P_{\text{обн}i} \quad (4)$$

В блоке 10 сравнивают рассчитанные значения показателей живучести $K_{\text{ж}}$ моделируемой РСС с требуемыми значениями показателей живучести $K_{\text{ж} \text{ треб}}$.

В случае, если рассчитанной живучести недостаточно для функционирования моделируемой РСС, осуществляется возврат к блоку 4, где происходит имитация реконфигурирования РСС, исходя из предъявляемых к ней требований. Реконфигурация РСС заключается в изменении ее структуры, топологии, режимов работы (введении в работу резервных каналов (линий) и средств связи, восстановлении поврежденных и отказавших средств связи, изменении частот передачи, приема, мощности передачи, видов обработки сигналов, маршрутов прохождения каналов (трактов), азимутов антенн, помехозащищенных режимов и т.д.).

В блоке 11 моделируют развертывание T передающих базовых станций в спланированных районах TR_p , $i = 1..T$, соединяют их с узлами доступа ЕСЭ, причем передающие антенны передающих базовых станций ориентируют главным лепестком диаграммы направленности в направлении, обеспечивающем минимальную вероятность обнаружения средствами мониторинга злоумышленников.

В блоке 12 моделируют развертывание R приёмных базовых станций в спланированных районах RR_p , $i = 1..R$, соединяют их с узлами доступа ЕСЭ.

В блоке 13 моделируют соединение каналами связи ЕСЭ первый и второй узлы связи между собой, с сетью связи общего пользования и с базовыми станциями.

В блоке 14 на машинном носителе информации формируют базу данных, содержащую сведения о местоположении базовых станций для системы наведения приёмных антенн абонентских станций на передающие базовые станции, а передающих антенн абонентских станций — на приёмные базовые станции, о частотах передачи F_{BSi} , назначенных конкретной передающей базовой станции для перестройки частот приёмников абонентских станций, об общей для всех абонентских станций частоте передачи F_{AC} о координатах областей LQR_p , в границах которых вероятность ошибки приёма сигналов от базовых станций будет ниже требуемого.

В блоке 15 переносят сформированную базу данных в элементы памяти устройств управления абонентских станций.

В блоке 16 моделируют перемещение абонентских станций по маршрутам SR_i движения абонентов, ори-

ентирование передающих антенн абонентских станций главным лепестком диаграммы направленности в направлении приёмных базовых станций и обеспечивающем минимальную вероятность обнаружения абонентских станций средствами мониторинга злоумышленников, ориентирование приёмных антенн абонентских станций в направлении передающих базовых станций.

В блоке 17 сравнивают координаты текущих точек P_j маршрута движения каждой абонентской станции с рассчитанными точками STP_p , в случае несовпадения текущей координаты точки маршрута движения переходят к блоку 19.

В блоке 18 моделируют блокирование работы передатчика абонентской станции, находящейся в точке STP_i маршрута движения с максимальной вероятностью обнаружения средствами мониторинга злоумышленников.

Блокирование работы передатчика является известной ограничительной мерой, направленной на скрытие радиоизлучающего средства от средств мониторинга злоумышленников и заключается в прекращении излучения передатчиком электромагнитной энергии в передающую антенну.

В блоке 19 осуществляют информационный обмен от абонентских станций в сторону базовых станций только в точках маршрута движения с минимальной вероятностью обнаружения абонентских станций средствами мониторинга злоумышленников.

Для передачи сообщений (информации) за i -й абонентской станцией РСС выделяется промежуток времени (подкадр) в общем кадре передачи всех K абонентских станций, когда данная i -я станция может передать информацию на одной общей частоте FAC передачи абонентских станций. Арбитром, выдающим токен на право передачи информации от абонентской станции, является первый узел связи. В случае выхода из строя первого узла связи его функции выполняет второй узел связи.

Все R приёмных базовых станций, принимая радиосигналы от передатчиков базовых станций на одной общей частоте FAC , направляют принятые от абонентских станций сообщения по каналам связи ЕСЭ в сторону первого узла связи. Первый узел связи, получив сообщение от абонентской станции, принимает решение об отправке сообщения по имеющемуся в сообщении адресу, в соответствующий канал ЕСЭ. При получении первым узлом связи сообщения, адресованного абоненту распределённой абонентской сети, первый узел связи отправляет сообщение по каналам ЕСЭ одновременно T передающим базовым станциям. Каждая i -я передающая базовая станция передает данное сообщение на закреплённой за данной базовой станцией частоте F_{BSi} . Приёмники абонентских станций, получив сообщение на одной из частот приёма F_{BSi} сравнивают адресную информацию, содержащуюся в сообщении, с собственным адресом. В случае, если

адрес назначения, содержащийся в сообщении, совпадает с собственным адресом абонентской станции, сообщение принимается, в случае несовпадения — отбрасывается. Второй узел связи в информационном обмене не участвует, но находится в готовности заменить первый узел связи в случае неисправности первого узла связи или на время выключения первого узла при реконфигурации сети.

В блоке 20 сравнивают текущее время t с временем t_k окончания обслуживания абонентов распределенной абонентской сети в заданном районе SMR , в случае если текущее время t меньше времени окончания обслуживания абонентов t_k , переходят к блоку 17.

По результатам имитационного моделирования, возможно спроектировать РСС, функционирующей в условиях ИП. Заданные условия служат исходными данными для оценивания эффективности функционирования РСС.

Вариант построения РСС представлен на (рис. 2) и содержит: первый узел связи — 1, второй узел связи — 2, узел доступа ЕСЭ — 3.1–3.10, линия, соединяющая первый узел связи с узлом доступа ЕСЭ — 4.1, линия, соединяющая второй узел связи с узлом доступа ЕСЭ — 4.2, передающая базовая станция — 5.1–5.4, передающая антенна передающей

базовой станции — 6.1–6.4, соединительная линия от узлов доступа к базовым станциям — 7.1–7.8, приёмная базовая станция — 8.1–8.4, средство мониторинга злоумышленников — 9.1–9.5, абонентская станция — 10.1–10.2, передающая антенна антенно-фидерного тракта абонентской станции — 11.1–11.2, приёмная антенна антенно-фидерного тракта абонентской станции — 12.1–12.2, антенна средства мониторинга злоумышленников — 13.1–13.5, каналы связи ЕСЭ, соединяющие первый и второй узлы связи между собой и с базовыми станциями — 14.1–14.10, главный лепесток диаграммы направленности передающей антенны абонентской станции — 15.1–15.2, главный лепесток диаграммы направленности передающей антенны передающей базовой станции — 15.3–15.6.

Оценивание эффективности функционирования моделированной РСС возможно осуществлять с использованием основных показателей живучести РСС (рис. 3).

В качестве абонентских станций 10.1–10.2 рассмотрим условное оборудование, с мощностью излучения, подводимой к антенне, равной 5 Вт и использующее на (рис. 3А) (известные технические решения) [1–2] абсолютно ненаправленную приёмопередающую антенну 11.1,

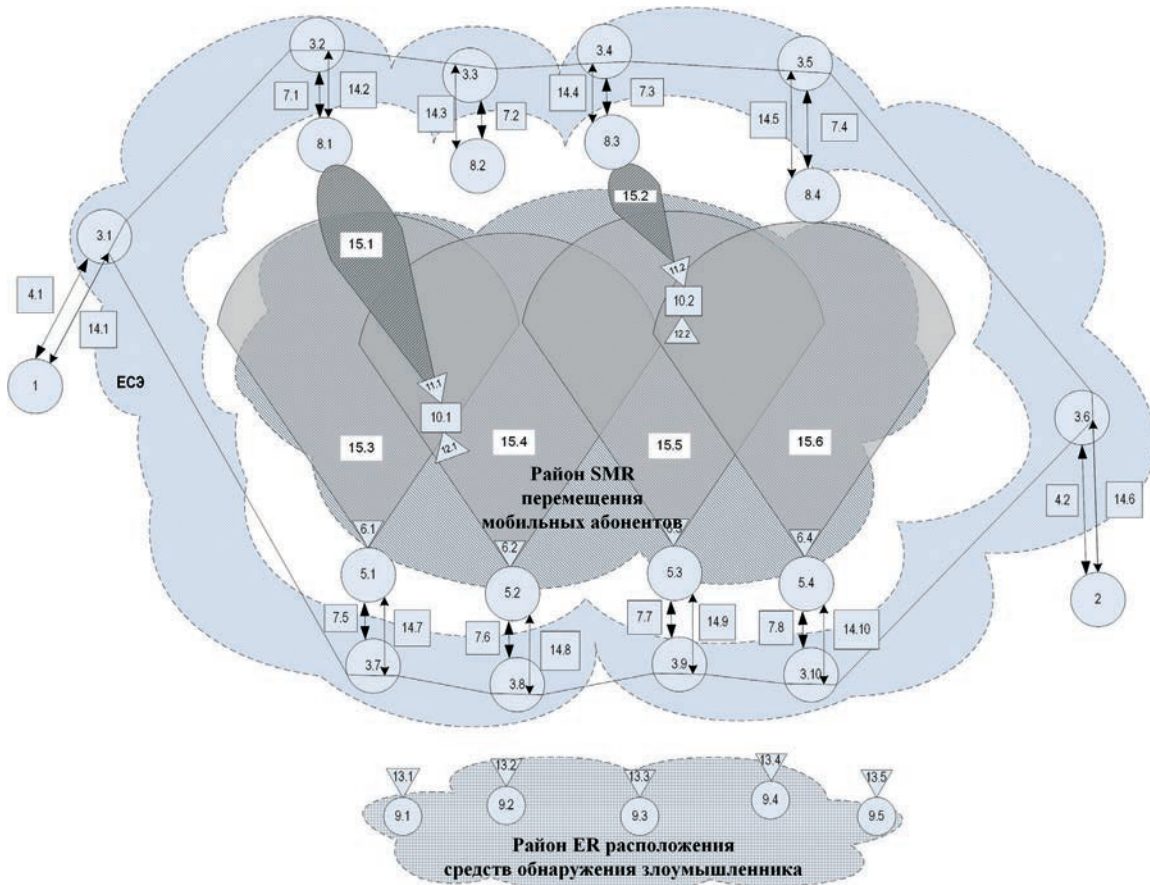


Рис. 2. Вариант построения распределенной сети связи

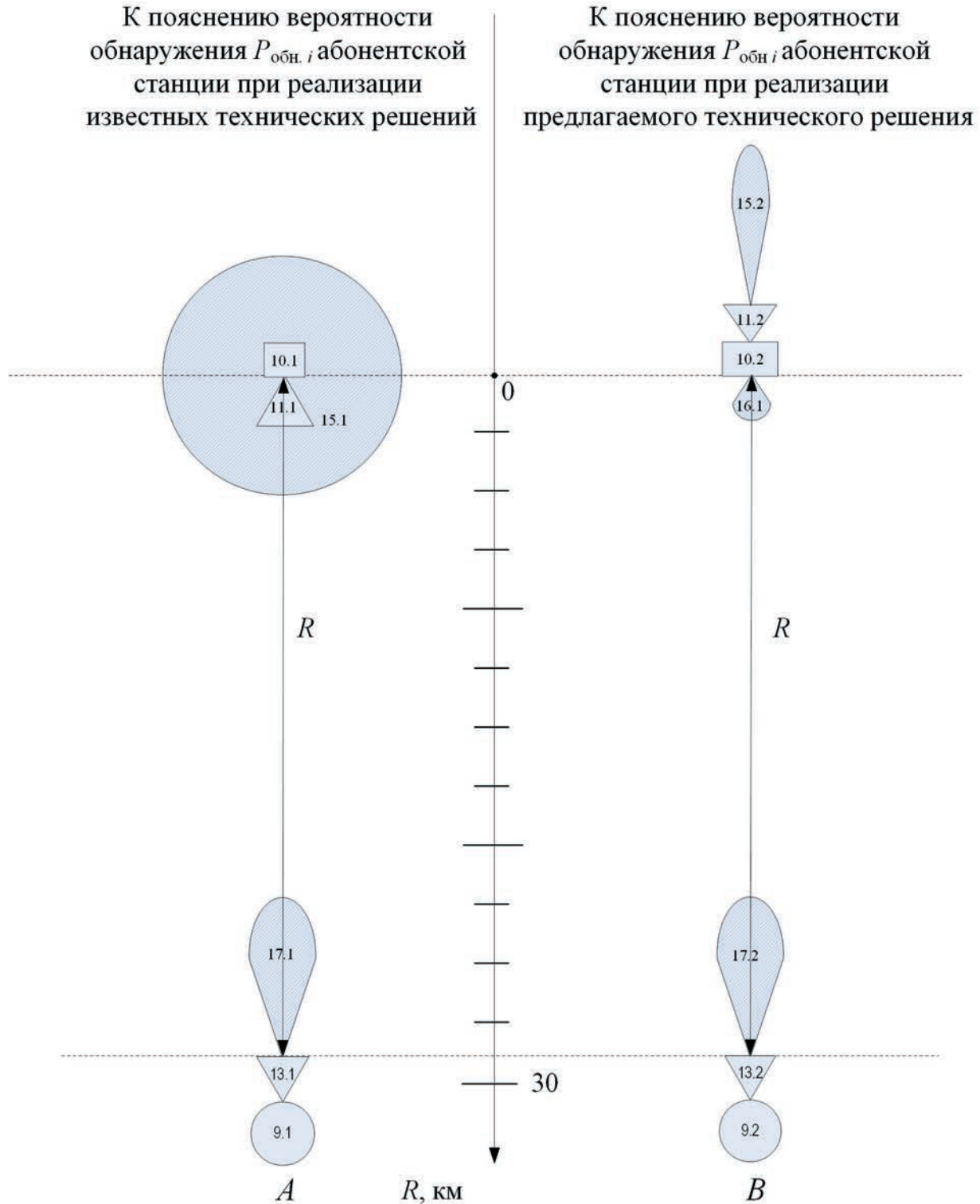


Рис. 3. Вариант оценивания эффективности функционирования РСС

а на (рис. 3В) (предлагаемое техническое решение) передающую антенну 11.2, например, типа АА-450/7. Коэффициент усиления G_{a_1} абсолютно ненаправленной антенны 15.1, равен единице. Антенна АА-450/7 имеет коэффициенты усиления антенны: по главному лепестку 15.2 диа-

граммы направленности 7 дБ, а по заднему лепестку 16.1 на 13 дБ ниже главного, т.е. минус 6 дБ.

Допустим, что средство мониторинга 9.1–9.2 злоумышленника имеет приёмную антенну 13.1–13.2 типа АА-450/7, направленную главным лепестком 17.1–17.2

диаграммы направленности на абонентскую станцию 10.1–10.2 (рис. 3).

Предположим, что радиоволны от абонентской станции к средству мониторинга злоумышленников распространяются в свободном пространстве, не встречая препятствий на своем пути. Тогда мощность сигнала $P_{\text{Свх}}$ (без учета потерь) на входе $P_{\text{Свх}}$ приёмника средства мониторинга злоумышленников в пределах его полосы пропускания можно определить по формуле [13–14]:

$$P_{\text{Свх}} = \frac{P_{\text{изл}} \cdot G_{\text{изл}} \cdot G_{\text{пр}} \cdot \lambda^2}{4 \cdot \pi \cdot R^2}, \quad (5)$$

где λ — длина волны, на которой излучает передатчик абонентской станции, м;

$P_{\text{изл}}$ — мощность, подводимая к передающей (приёмопередающей) антенне абонентской станции, Вт;

$G_{\text{изл}}$ — коэффициент усиления передающей (приёмопередающей) антенны абонентской станции в направлении на средство мониторинга злоумышленников;

$G_{\text{пр}}$ — коэффициент усиления приёмной антенны средства мониторинга злоумышленников в направлении на абонентскую станцию;

R — расстояние между средствами мониторинга злоумышленников и абонентской станцией, м.

Так как, коэффициенты усиления G_a антенн, как правило, приводятся в децибелах, определим порядок обратного пересчёта в безразмерные единицы:

$$G_{a(\text{раз})} = 10^{\frac{G_{\text{изл}}(\text{дБ})}{10}}. \quad (6)$$

На частоте 460 МГц антенна АА-450/7 имеет коэффициент усиления (по главному лепестку диаграммы направленности), равный 7 дБ, что в соответствии с формулой (6) составляет $G_{a_2} = 10^{0,7} \approx 5$. Для заднего лепестка коэффициент усиления составляет $G_{a_2} = 10^{-0,6} \approx 0,25$. Частоте 460 МГц соответствует длина волны:

$$\lambda = \frac{A}{F} = \frac{3 \cdot 10^8}{460 \cdot 10^6} = 0,65 \text{ м} \quad (7)$$

Предположим, что расстояние R равно 29000 метров (рис. 3). При использовании известных технических решений (рис. 3А) [1–2, 15], когда абонентская станция излучает в сторону средств мониторинга злоумышленников ненаправленной приёмопередающей антенной, с соответствующим коэффициентом усиления $G_{\text{изл}} = G_{a_1} = 1$, а приёмная антенна средства мониторинга злоумышленника имеет коэффициент усиления $G_{\text{пр}} = G_{a_2} = 7$, из выражения (5) получим:

$$P_{\text{Свх}} = \frac{P_{\text{изл}} \cdot G_{\text{изл}} \cdot G_{\text{пр}} \cdot \lambda^2}{4 \cdot \pi \cdot R^2} = \frac{5 \cdot 1 \cdot 5 \cdot 0,65^2}{4 \cdot 3,1459 \cdot 29000^2} = 1000 \cdot 10^{-12} \text{ Вт}$$

Реализация предлагаемого способа (рис. 3В), когда абонентская станция работает в сторону средств мониторинга злоумышленников направленной передающей антенной, с соответствующим заднему лепестку коэффициентом усиления $G_{\text{изл}2} = G_{a_3} = 0,25$, из выражения (5) получим:

$$P_{\text{Свх}2} = \frac{P_{\text{изл}} \cdot G_{\text{изл}} \cdot G_{\text{пр}} \cdot \lambda^2}{4 \cdot \pi \cdot R^2} = \frac{5 \cdot 0,25 \cdot 5 \cdot 0,65^2}{4 \cdot 3,1459 \cdot 29000^2} = 251 \cdot 10^{-12} \text{ Вт}$$

Предположим, что уровень шума на входе приёмника средства мониторинга злоумышленника равен $63 \cdot 10^{-12}$ Вт. Тогда из выражения (2) определим отношение сигнал/шум на входе приёмника средства мониторинга злоумышленников. При реализации известных технических решений (рис. 3А) отношение сигнал/шум q_1 составит [1–2]:

$$q_1 = \frac{P_{\text{Свх}2}}{P_{\text{Швх}}} = \frac{1000 \cdot 10^{-12}}{63 \cdot 10^{-12}} = 15,9 \approx 16$$

При реализации предлагаемого технического решения (рис. 3В) отношение сигнал/шум q_2 составит [12]:

$$q_2 = \frac{P_{\text{Свх}2}}{P_{\text{Швх}}} = \frac{251 \cdot 10^{-12}}{63 \cdot 10^{-12}} = 3,99 \approx 4$$

Основные выходные результаты, полученные при оценивании эффективности функционирования РСС получены следующим образом. Воспользуемся зависимостью коэффициента живучести РСС — $K_{\text{ж}}(q)$ от соотношения сигнал/шум на входе средства мониторинга злоумышленников при заданной вероятности ложной тревоги, приведенной на (рис. 4), для случая, когда вероятность ложной тревоги РЛТ = 10–6 и определим примерные значения $K_{\text{ж}}$ графическим способом (рис. 4) при $q_2 = 4$ и $q_1 = 16$. Из графических построений, выполненных на рис. 4, видно, что при реализации известных технических решений $K_{\text{ж}1}$ i -й абонентской станции равен 0,05, а при реализации предлагаемого технического решения $K_{\text{ж}2}$ i -й абонентской станции равен 0,5.

Рассчитаем выигрыш N в увеличении живучести $K_{\text{ж}}$ i -й абонентской станции при применении для построения сети предлагаемого технического решения как кратность увеличения коэффициента живучести $K_{\text{ж}}$ по формуле:

$$N = \frac{K_{\text{ж}2}}{K_{\text{ж}1}} = \frac{0,5}{0,05} = 10.$$

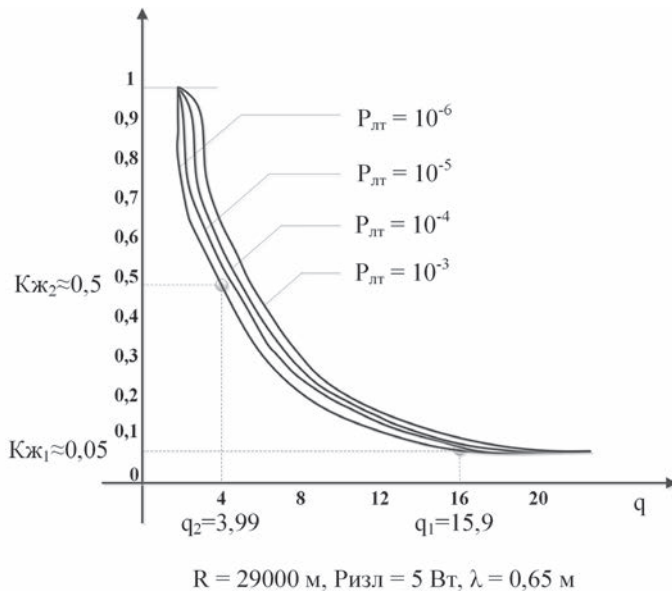


Рис. 4. Основные выходные результаты, полученные при оценивании эффективности функционирования РСС

В статье предложен теоретический подход по оцениванию и обеспечению живучести РСС, функционирующих в условиях ИП. С помощью сформулированного подхода возможно оценить эффективность проектируемой РСС. Теоретический подход реализован в виде Патента РФ на изобретение [12]. Может применяться при проектировании и разработке РСС, а также, при задании требований по живучести сложных технических систем, функционирующих в условиях деструктивных воздействий и в учебном процессе высших учебных заведений.

Литература

1. Патент РФ 2459370. Способ построения защищенной системы связи / Белов А. С., Иванов В. А., Будилкин С. А., Стародубцев Ю. И., Гречишников Е. В., Стукалов И. В. Заявл. 28.06.2010. Оpubл. 20.08.2012. Бюл. № 1. 13 с.
2. Патент РФ 2544786. Способ формирования защищенной системы связи, интегрированной с единой сетью электросвязи в условиях внешних деструктивных воздействий / Гречишников Е. В., Белов А. С., Шумилин В. С., Сучков А. М. Заявл. 03.06.2013. Оpubл. 11.02.2015. Бюл. № 7. 17 с.
3. Anisimov V. G., Anisimov Ye. G. A branch-and-bound algorithm for one class of scheduling problem // Computational Mathematics and Mathematical Physics. 1992. Vol. 32: No.12. Pp. 1827–1832.

4. Anisimov V. G., Anisimov Ye. G. Algorithm for the optimal distribution of discrete nonuniform resources on the web // Computational Mathematics and Mathematical Physics. 1997. Vol. 37. No. 1. Pp. 54–60.

5. Alekseyev A. O., Alekseyev O. G., Anisimov V. G., Anisimov Ye. G. The use of duality to increase the effectiveness of the branch and bound method when solving the knapsack problem // USSR Computational Mathematics and Mathematical Physics. 1985. Vol. 25. No. 6. Pp. 50–54.

6. Anisimov V. G., Anisimov Ye. G. A method of solving one class of integer programming problems // USSR Computational Mathematics and Mathematical Physics. 1989. Vol. 29(5). Pp. 238–241.

7. Anisimov V. G., Anisimov Ye. G. Modification of the method for solving a class of integer programming problems // Computational Mathematics and Mathematical Physics. 1997. Vol. 37. No. 2. Pp. 179–183.

8. Барабанов В. В., Филиппов А. А. Модели организации и проведения испытаний элементов системы информационного обеспечения применения высокоточных средств // Труды Военно-космической академии имени А. Ф. Можайского. 2015. № 648. С. 6–12.

9. Анисимов В. Г., Анисимов Е. Г. Обобщенный показатель эффективности взаимодействия федеральных органов исполнительной власти при решении задач обеспечения национальной безопасности государства. // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2017. № 5–6 (107–108). С. 101–106.

10. Гасюк Д. П., Сосюра О. В. Основы теории эффективности боевых действий ракетных войск и артиллерии. М.: Министерство обороны РФ, 2003. 168 с.

11. Буренин А. Н., Легков К. Е. Современные инфокоммуникационные системы и сети. Основы построения и управления. М.: Медиа Паблишер, 2015. 348 с.

12. Патент РФ 2600941. Способ обеспечения живучести распределенной абонентской сети связи / Белоконев Д. О., Горелик С. П., Скубьев А. В., Белов А. С., Чуляев И. И. Заявл. 21.07.2015. Оpubл. 05.10.2016. Бюл. № 30. 25 с.

13. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки. М.: РГТУ, 2002. 399 с.

14. Заика П. В., Копичев О. А. Имитационное моделирование радиоэлектронной обстановки на основе агрегативного подхода // Радиотехника, электроника и связь: сб. докладов III Междунар. науч.-технической конф. (Омск, 6–8 октября 2015). Омск: Омский научно-исследовательский институт приборостроения, 2015. С. 207–212.

15. Математическая энциклопедия: в 5 т. / под ред. И. М. Виноградова. М.: Советская энциклопедия, 1984. Т. 4. С. 135–140.

THEORETICAL APPROACH ON ESTIMATION AND SUPPORT OF SURVIVABILITY OF DISTRIBUTED NETWORKS OF COMMUNICATION IN THE CONDITIONS OF INFORMATION CONFRONTATION

ANDREY S. BELOV,

St-Peterburg, Russia, andrej2442016@yandex.ru

ALEXANDER V. SKUBYEV,

Oryol, Russia, skub7777@mail.ru

KEYWORDS: survivability; informational confrontation; destructive influences; subscriber; station.

ABSTRACT

In the conditions of enhancement of forms and methods of guiding of information confrontation, essential value in maintenance of the required figures of merit of communication networks acquires process of estimation and support of survivability of its elements. The existing methods and methods of creation of radio radiating means of distributed networks of communication are not capable to provide key indicators of survivability because of existence of the strong unmasking indications. In article theoretical approach (model, a method of estimation and a method of support of survivability) which application will allow to evaluate and provide survivability of distributed networks of communication in the conditions of external destructive influences is considered. In case of estimation of survivability of distributed networks of communication decomposition of a communication network on components is made and key indicators of survivability are calculated separately on each component of a communication network, including on all radio radiating means. For example, key indicators of survivability of i -y of the subscriber station are evaluated from a ratio signal/noise on an input of the receiver of the monitor of the opponent in case of the given probability of false alarm. Results of the carried-out calculations allow to provide survivability of communication networks, using organizational and organizational and technical methods, namely, for the score: reconstructions of communication networks, controls of key indicators of survivability of distributed networks of communication taking into account ratios signal/noise on inputs of monitors of malefactors in case of the given probability of false alarm, adjustment of direction characteristics of radio radiating means and their appropriate creation in the distributed territory, coordination of routes of movement of subscribers in which the probability of detection monitors of the opponent will be the minimum and maximum and also corresponding to them azimuths of orientations of the principal lobes of the direction characteristic of the transferring antennas of subscriber stations to receiving base stations.

REFERENCES

1. Patent RF 2459370. *Sposob postroeniya zashchishchennoj sistemy svyazi* [A way of construction protected communication system]. Belov A.S., Ivanov V.A., Budilkin S.A., Starodubtsev Yu.I., Grechishnikov E.V., Stukalov I.V. Declared. 28.06.2010. Published. 20.08.2012. Bulletin No. 1. 13 p. (In Russian)
2. Patent RF 2544786. *Sposob formirovaniya zashchishchennoj sistemy svyazi, integrirovannoj s edinoj set'yu ehlektrosvyazi v usloviyah vneshnih destruktivnyh vozdeystvij* [A way of formation of the protected communication system integrated with uniform network of telecommunication in the conditions of external destructive influences]. Grechishnikov E.V., Belov A.S., Shumilin V.S., Suchkov A.M. Declared. 03.06.2013. Published. 11.02.2015. Bulletin No. 7. 17 p. (In Russian)
3. Anisimov V.G., Anisimov Ye.G. A branch-and-bound algorithm for one class of scheduling problem. *Computational Mathematics and Mathematical Physics*. 1992. Vol. 32. No. 12. Pp. 1827-1832.
4. Anisimov V.G., Anisimov Ye.G. Algorithm for the optimal distribution of discrete nonuniform resources on the web. *Computational Mathematics and Mathematical Physics*. 1997. Vol. 37. No. 1. Pp. 54-60.
5. Alekseyev A.O., Alekseyev O.G., Anisimov V.G., Anisimov Ye.G. The use of duality to increase the effectiveness of the branch and bound method when solving the knapsack problem. *Computational Mathematics and Mathematical Physics*. 1985. Vol. 25. No. 6. Pp. 50-54.
6. Anisimov V.G., Anisimov Ye.G. A method of solving one class of integer programming problems. *Computational Mathematics and Mathematical Physics*. 1989. Vol. 29. No. 5. Pp. 238-241.
7. Anisimov V.G., Anisimov Ye.G. Modification of the method for solving a class of integer programming problems. *Computational Mathematics and Mathematical Physics*. 1997. Vol. 37. No. 2. Pp. 179-183.
8. Barabanov V.V., Filippov A.A. Modeli organizacii i provedeniya ispytanij ehlementov sistemy informacionnogo obespecheniya

primeneniya vysokotochnykh sredstv [Models of the organization and carrying out tests elements of system information support of application high-precision means]. *Trudy voenno-kosmicheskoi akademii imeni A.F. Mozhaiskogo* [Works of Military space academy named after A.F. Mozhaysky]. 2015. No. 648. Pp. 6-12. (In Russian)

9. Anisimov V.G., Anisimov Ye.G. Obobshchennyj pokazatel' ehffektivnosti vzaimodeystviya federal'nykh organov ispolnitel'noj vlasti pri reshenii zadach obespecheniya nacional'noj bezopasnosti gosudarstva [The generalized indicator of interaction efficiency federal executive authorities at the solution of problems ensuring national security the state] *Voprosy oboronnoy tekhniki. Seriya 16. Tekhnicheskie sredstva protivodeystviya terrorizmu* [Questions of the defensive equipment. Series 16: Technical means of counteraction to terrorism]. 2017. No. 5-6 (107-108). Pp. 101-106. (In Russian)

10. Gasyuk D.P., Saussure O.V. *Osnovy teorii ehffektivnosti boevykh deystvij raketnykh voysk i artillerii* [Bases of the theory efficiency fighting of rocket troops and artillery]. Moscow: Ministerstvo oborony RF [Ministry of Defence of the Russian Federation]. 2003. 168 p. (In Russian)

11. Burenin A.N., Legkov K.E. *Sovremennyye infokommunikatsionnyye sistemy i seti. Osnovy postroeniya i upravleniya transliteratsiya nuzhna* [Modern infocommunication systems and networks. Fundamentals of construction and management]. Moscow: Media Publisher Publ., 2015. 348 p. (In Russian)

12. Patent RF 2600941. *Sposob obespecheniya zhivuchesti raspredelennoy abonentskoy seti svyazi* [A method of support of survivability

ity of the distributed subscriber premises network Communication]. Belokonev D.O., Gorelik S.P., Skubyev A.V., Belov A.S., Chuklyayev I.I. Declared. 21.07.2015. Published 05.10.2016. Bulletin No. 30. 25 p. (In Russian)

13. Menshakov Y.K. *Zashchita ob"ektov i informacii ot tekhnicheskikh sredstv razvedki* [Protection of objects and information from technical means of investigation]. Moscow: RGGU, 2002. 399 p. (In Russian)

14. Zaika V.P., Kopichev O.A. Imitatsionnoe modelirovanie radioelektronnoy obstanovki na osnove agregativnogo podhoda [Imitating modeling of a radio-electronic situation on the basis of an aggregate approach] *Radiotekhnika, elektronika i svyaz': Sbornik dokladov III Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii* [The collection of reports of 3th International scientifictechnical conference "Radio engineering, electronics and communication", Omsk, October 6-8, 2015]. Omsk: Omskiy nauchnoissledovatel'skiy institut pri borostroeniya Publ., 2015. Pp. 207-212. (In Russian)

15. Vinogradov I.M. (Ed.). *Matematicheskaya entsiklopediya* [Mathematical encyclopedia]. Moscow: Sovetskaya Entsiklopediya. 1984. Vol. 4. Pp. 135-140. (In Russian)

INFORMATION ABOUT AUTHORS:

Belov A.S., PhD, Docent, Doctoral Candidate of Mikhaylovsky military artillery academy;

Skubyev A.V., Postgraduate Student of Academy of Federalalny security service of the Russian Federation.

For citation: Belov A.S., Skubyev A.V. Theoretical approach on estimation and support of survivability of distributed networks of communication in the conditions of information confrontation. *H&ES Research*. 2018. Vol. 10. No. 2. Pp. 22-33. doi 10.24411/2409-5419-2018-10038 (In Russian)



doi 10.24411/2409-5419-2018-10039

МОДЕЛЬ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ КАК СОСТАВЛЯЮЩАЯ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ УПРАВЛЕНИЯ

ЛОГИН

Элина Валерьевна¹

КАНАЕВ

Андрей Константинович²

АННОТАЦИЯ

На сегодняшний день не существует единой методики для разработки системы управления сетью на основе технологии Carrier Ethernet. Существует множество стандартов, где описаны архитектура и механизмы контроля и управления элементами сети Carrier Ethernet (механизмы OAM), но не сформированы требования к системе управления такой сетью связи. Решение этой задачи возможно путем моделирования процесса функционирования транспортной сети на основе технологии Carrier Ethernet для управления ее конфигурацией. Для создания модели выбран аппарат имитационного моделирования AnyLogic. Целью работы является выявление взаимозависимостей между надежностными показателями функционирования транспортной сети на основе технологии Carrier Ethernet и процессом функционирования подсистем управления и восстановления транспортной сети. А также получение зависимостей коэффициента готовности от длительностей времени наработки на отказ и времени восстановления отказа, а также от количественных характеристик конфигурации моделируемого фрагмента сети. Мультиагентная система, являющаяся частью управляющей системы, находится во взаимодействии с ней. Использование в МАСУ распределенного объекта управления транспортной сети на основе технологии Carrier Ethernet позволит получить демонстрацию динамики изменения состояния фрагмента транспортной сети и получить оценку сетевой надежности. Решение задачи по построению модели МАСУ основано на использовании метода агентного моделирования, который относится к классу агент-ориентированных моделей. В работе используются положения теории вероятностей, теории управления и теории систем. Новизна представленной модели заключается в выборе нового объекта управления Carrier Ethernet, выборе оригинального комплекса механизмов контроля и управления для их включения в модель, применении математического аппарата агентного моделирования. Использование представленной модели для исследования функционирования транспортной сети позволяет проследивать динамику поведения каждого узла и каждого маршрута со своими значениями интенсивностей отказов и восстановления для структуры сети любой сложности, позволяет решать задачи, связанные с определением длительности времени до потери связности в маршруте и длительности времени наработки на отказ всех маршрутов одновременно, позволяет формировать оценки сетевой надежности и отказоустойчивости.

КЛЮЧЕВЫЕ СЛОВА: транспортная сеть связи; Carrier Ethernet; агентное моделирование; AnyLogic; механизмы OAM; система управления; сетевая надежность.

Сведения об авторах:

¹ ассистент кафедры электрической связи
Петербургского государственного
университета путей сообщения
Императора Александра I,
г. Санкт-Петербург, Россия,
elinabeneta@yandex.ru

² д.т.н., профессор, заведующий
кафедрой электрической связи
Петербургского государственного
университета путей сообщения
Императора Александра I,
г. Санкт-Петербург, Россия,
kanaevak@mail.ru

С развитием телекоммуникационных технологий и увеличением структурной сложности транспортных сетей связи (ТрС) актуализируются вопросы исследования и моделирования систем управления (СУ) соответствующими сетями связи. В работах [1–5] освещаются вопросы надежности и устойчивости сетей связи. Представленная работа отличается от известных включением в модель в качестве объекта управления ТрС а также построением СУ) на основе аппарата агентного моделирования. Еще одной отличительной чертой данного исследования является использование новой технологии построения ТрС операторского класса — Carrier Ethernet (CE). В основе технологии CE лежат механизмы для контроля состояния и управления сетевыми элементами (механизмы OAM). Построение СУ такой сетью возможно с использованием результатов агентного способа моделирования, что подразумевает возможность построения моделей большого масштаба и сложности. В качестве объекта управления в работе рассматривается сеть CE. Сеть связи имеет строго определенную структуру, состоящую из элементов. Под элементом понимается узел и канал передачи информации. В качестве узлов в такой сети может выступать комплекс специального оборудования (маршрутизаторы, коммутаторы, мультиплексоры и пр.), обеспечивающий передачу разного рода данных и связность сети. Задачей сети связи является выполнение функций предоставления и поддержания услуг связи с заданными параметрами.

Для выявления взаимозависимостей между надежностными показателями функционирования сети и процессом функционирования подсистем управления и восстановления ТрС необходимо получить значения параметров, характеризующих надежность сети. Таким образом, целью работы является получение длительности наработки времени на отказ и длительности восстановления отказа. Для достижения цели работы необходимо решить задачу, связанную с разработкой модели функционирования ТрС в составе мультиагентной системы управления (МАСУ), которая в свою очередь формализует функции механизмов OAM.

В соответствии с функциональной моделью МАСУ [6] сбор и регистрация данных для реализации механизмов OAM осуществляется агентами регистрации и анализа событий. Поэтому при моделировании МАСУ ТрС под агентом МАСУ будем понимать агента регистрации и анализа событий, который в свою очередь отражает состояние и параметрическое пространство некоторого элемента ТрС. Каждый агент МАСУ содержит информацию об элементе ТрС. Для создания модели МАСУ использовалась среда моделирования AnyLogic, отличающаяся от остальных многообразием способов оценки результатов и возможностью использования агентного способа моделирования.

Процесс разработки модели включает в себя несколько этапов, которые в виде отдельных блоков представлены на рис. 1.

Так как основными элементами ТрС являются узловые коммутаторы (маршрутизаторы) и их соединения, то элементы ТрС в модели функционирования можно классифицировать на элементы, к которым относятся узлы ТрС, и маршруты, к которым относится совокупность нескольких узлов и каналов передачи информации ТрС. При создании модели МАСУ предполагается создание таких агентов, которые являются информационным отражением каждого элемента ТрС. Модель функционирования описывает фрагмент ТрС под управлением одного узла МАСУ. Предполагается, что в каждом фрагменте ТрС имеется множество узлов E и множество маршрутов C , а в соответствующем узле МАСУ имеется множество агентов-узлов A^E и множество агентов-маршрутов A^C . Так как в среде AnyLogic при агентном способе моделирования моделируемой единицей является агент, то понятие агента МАСУ как программной реализации элемента ТрС будет совпадать с понятием агента модели. Но если в первом случае агентом является структурном блоке МАСУ [6], то агентом в модели является программная реализация узла ТрС или маршрута, соединяющего некоторое количество узлов.

В среде моделирования AnyLogic множеством агентов одного и того же типа называется популяция агентов [7–8]. По такому принципу в модели созданы две популяции: «equipments» с типом агентов «Equipment» — для создания агентов-узлов и «connect» с типом агентов «Connect» — для создания агентов-маршрутов (блок 1 на рис. 1). В силу того, что к задачам узла МАСУ относится управление фрагментом ТрС, то конфигурация фрагмента ТрС должна быть задана для соответствующего узла МАСУ. В среде моделирования формируется пространство, в котором будут существовать и взаимодействовать агенты (блок 2 на рис. 1). Причем пространство формируется путем настроек сети автоматически или вручную путем задания статических и динамических координат местоположения для каждого агента.

Все элементы ТрС характеризуются набором параметров. Изменение значений параметров в результате воздействия на сеть различных факторов оказывает влияние на состояние соответствующих узлов и маршрутов ТрС, и в целом всего фрагмента ТрС. Эти изменения будут отражать агенты МАСУ, а в конечном итоге это изменение будет влиять на формирование новой конфигурации ТрС. В данной работе изменение параметров задавалось с помощью функции случайного распределения для времени наработки на отказ и функции случайного распределения для времени восстановления отказа элемента ТрС. Модель предусматривает наличие параметрического пространства, изменение которого влияет на значение надежности



Рис. 1. Структура имитационной модели МАСУ

ТрС. В [2, 11] представлено множество параметров узлов ТрС, которые в МАСУ отражаются в виде множества атрибутов. В табл. 1 представлены параметры агентов МАСУ, которые учитывались в модели как дополнительные свойства у агентов модели (блок 3 на рис. 1).

Правила поведения для агентов МАСУ, учитывающих особенности архитектуры ОАМ Carrier Ethernet основываются на разработанных алгоритмах управления [9–11]. Данные алгоритмы включают в себя ряд подпроцессов по управлению и контролю неисправностями. Результаты моделирования [11] этих подпроцессов использованы в исследовании данной работы. В модели у агентов учитывается ряд состояний, характеризующих их работоспособность (блок 4 на рис. 1).

Переход агентов из одного состояния в другое задается с помощью соответствующих параметров (блок 5 на рис. 1):

1) функция распределения вероятности отказа элемента ТрС задана с помощью закона случайного распределения Вейбулла-Гнеденко:

$$E(t) = 1 - e^{-\left(\frac{t}{a}\right)^b} = 1 - e^{-\left(\frac{t}{2,017}\right)^{2,138}}$$

Данное распределение было получено на основе статистических данных функционирования телекоммуникационного оборудования по результатам двух лет его работы, а также для получения такого распределения были рассчитаны его параметры [6–7].

$$\hat{b} = \frac{\ln \ln F_2 - \ln \ln F_1}{\ln \frac{t_2}{t_1}} = 2,138$$

$$\hat{a} = \frac{t_1}{(-\ln F_1)^{1/b}} = 2,017$$

где F_1 и F_2 — точки эмпирической функции распределения времени, а t_1 и t_2 — интервалы времени эксплуатации оборудования получены в результате построения эксперимен-

Таблица 1

Дополнительные свойства агентов МАСУ

Классификация параметра в МАСУ	Название параметра	Тип	Множество значений
Параметры конфигурации	Ethernet	boolean	<i>VLAN tunneling (Q-in-Q) for TLS</i>
		boolean	<i>IEEE 802.3u (Fast Ethernet)</i>
		string	<i>IEEE 802.3x,z,d,q,ad,ab,ah,s</i>
		boolean	<i>VLAN Translation</i>
	Защита соединения и пути	boolean	<i>Ручная агрегация соединения</i>
		boolean	<i>STP</i>
		boolean	<i>RSTP Self Loop Detection</i>
	Тип порта	boolean & integer	<i>4 x 1000 BASE-FX ports</i>
			<i>16 x 1000 BASE-FX ports</i>
			<i>24 x 100 BASE-FX ports</i>
			<i>1 x OOB Management port</i>
			<i>1 x Console Port (RS-232)</i>
	Управление сетью	boolean	<i>SNMP, SNMP MIB II (RFC 1213)</i>
		boolean	<i>Y.1731 Performance Monitoring</i>
		boolean	<i>IEEE 802.1ag</i>
boolean		<i>Connectivity Fault Management</i>	
boolean		<i>Fault Detection (Trace route, packet trace, IFG shaving)</i>	
Параметры оценки состояния	Качество предоставляемых услуг <i>QoS</i>	string	<i>128 уровней сервисов</i>
		integer	<i>CIR</i>
		integer	<i>EIR</i>
		string	<i>DiffServ</i>

тальной функции распределения отказов оборудования связи различного типа [12–13].

2) функция распределения времени восстановления элемента ТрС задана с помощью переменных AnyLogic, которые позволяют задавать данную величину как случайную и формировать для нее нормальное распределение с требуемыми характеристиками. Задание характеристик этой переменной также обуславливалось данными статистики эксплуатации сетей связи железнодорожного транспорта [13].

Стоит отметить, что агенты внутри своей популяции, а также между популяциями обмениваются управляющей информацией, например, сообщая агенту-маршруту о неисправных агентах-узлах, входящих в конфигурацию данного маршрута. Таким образом, в агентной среде состояния элементов задаются с помощью функций распределения вероятности и восстановления отказа, а состояние маршрутов будет зависеть от состояния элементов, которые входят в данный маршрут.

Изменение состояния элемента ТрС отражается в МАСУ путем изменения состояния соответствующего

агента узла МАСУ. После чего непосредственно агент, а также другие блоки управления узла МАСУ [6] реагируют на изменения в соответствии с алгоритмом контроля состояния и управления элементами ТрС. В данном моделировании использовался полученный ранее алгоритм работы процессов периодического контроля и состояния фрагмента ТрС [11].

При изменении состояние какого-либо агента, запускается алгоритм контроля состояния и управления элементами ТрС. Состояние агента-узла диагностируется с помощью сообщения ССМ (Continuity Check Message) [14–15]. В результате оценки данных сообщения ССМ для одного маршрута фрагмента сети возможны два случая:

1) несоответствий не обнаружено, маршрут исправен, узлы маршрута находятся в исправном состоянии. В этом случае алгоритм запускает подпроцесс проверки параметров элементов данного маршрута;

2) обнаружена неисправность в маршруте. В этом случае маршрут устанавливается в неисправное состояние; запускается подпроцесс локализации неисправности для поиска неисправного агента; далее запускаются подпро-

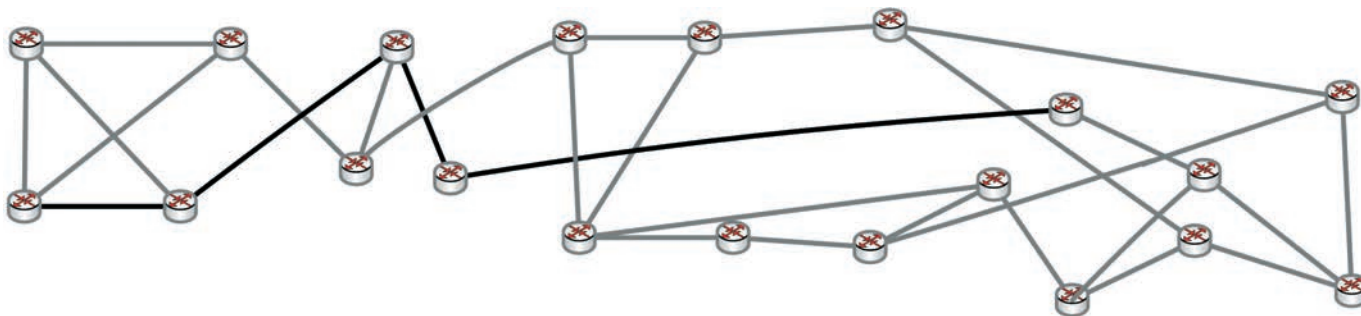


Рис. 2. Структура моделируемого фрагмента TrC с указанием примера маршрута

цессы восстановления агента и формирования множества вариантов по изменению конфигурации фрагмента сети.

При моделировании приняты следующие ограничения и допущения (блок 6 на рис. 1):

Рассматривается фрагмент TrC под управлением одного узла МАСУ;

1. Узел МАСУ состоит из 20 агентов, которые отражают состояние соответствующих узлов TrC;
2. Функции распределения случайных величин относятся к классу нормальных и Вейбулла-Гнеденко;
3. Характеристики случайных величин определяются статистическими способами;
4. Длительность эксперимента не превышает 10 лет модельного времени;
5. Среднее количество узлов, входящих в состав маршрута составляет 5.

На рис. 2 представлен прототип фрагмента TrC, на основе которой проводилось моделирование функционирования.

В результате моделирования были получены следующие данные. На рис. 3 представлены полученные в ходе моделирования значения величин времени наработки на

отказ и времени восстановления для маршрутов фрагмента сети, представленного на рис. 2. Так как результаты моделирования в AnyLogic представляются в виде крупного массива данных для каждого отказа каждого агента, поэтому на рис. 3 представлены средние значения соответствующих величин.

На рис. 4 представлены данные величин времени наработки на отказ и времени его восстановления для узлов фрагмента сети.

Для решения задачи, связанной с получением значений оценки надежности TrC, необходимо определить основные показатели надежности. В данной работе оцениваются такие показатели надежности как средняя наработка времени на отказ (T_{mno}), среднее время восстановления отказа (T_{vvo}) и коэффициент готовности TrC (K_g) [13].

По результатам моделирования получены два значения коэффициента готовности. Для оценки надежности фрагмента сети, структурированного по маршрутам и использующего для управления неисправностями алгоритмы контроля состояния и управления элементами TrC на базе технологии CE, получено среднее значение коэффициента готовности сети $K_g = 0,981$. Второе значение $K_g = 0,941$ было получено при тех же условиях, но без учета доменов технологии CE, предусмотренных архитектурой OAM технологии CE. Это значит то, что помимо механизмов контроля и управления состояниями сетевых элементов в значительной степени на значение надежности TrC влияет архитектура OAM, которая определяет конфигурацию маршрутов TrC.

Основным выводом по результатам моделирования является то, что коэффициент готовности сети чувствителен к ключевым параметрам модели — k (количество узлов в маршруте), L (количество узлов внутри фрагмента сети), T_{mno} (время наработки на отказ элемента CE), T_{vvo} (время восстановления отказа элемента CE).

На рис. 5 представлен график зависимости коэффициента готовности фрагмента TrC от количества элементов в маршруте и от количества элементов во фрагменте TrC.

График на рис. 5 иллюстрирует выбор приемлемого количества элементов в маршруте и в отдельно сформиро-

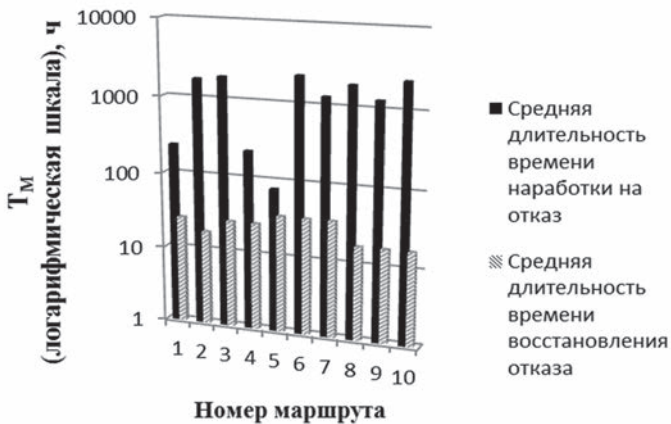


Рис. 3. Данные длительностей времени наработки на отказ и времени восстановления отказа на логарифмической шкале модельного времени (T_m) для маршрутов фрагмента TrC

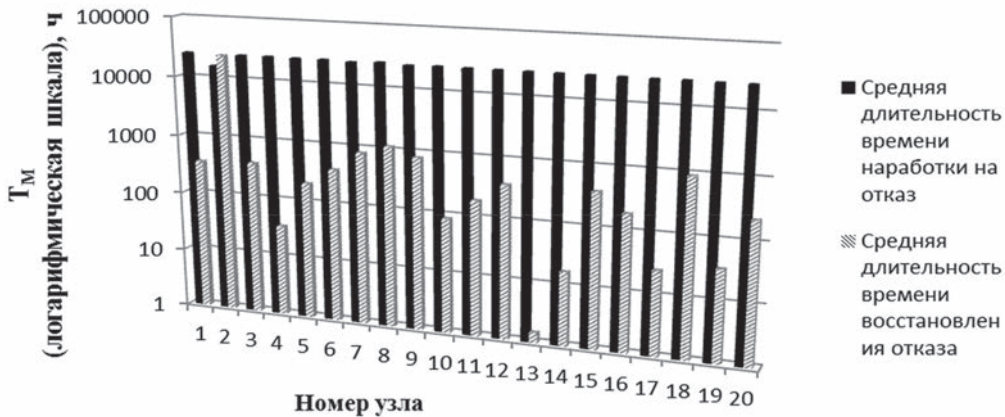


Рис. 4. Данные длительностей времени наработки на отказ и времени восстановления отказа на логарифмической шкале модельного времени (T_m) для узлов фрагмента ТрС

ванных фрагментах ТрС в зависимости от требуемого значения коэффициента готовности.

На рис. 6 представлена зависимость коэффициента готовности от времени наработки на отказ и времени восстановления отказа.

В случае параметров длительности восстановления и наработки на отказ, то полученные графики иллюстрируют взаимную зависимость значений этих параметров от K_g . Таким образом, график на рис. 6 позволяет также обоснованно выбирать рациональный уровень надежности сети в рамках параметра K_g и при этом соответствовать требованиям по отказоустойчивости элементов сети.

Проводимые исследования [1–5] в области решения задач, связанных с оценкой надежности сетей, являлись основой и предпосылкой представленного в данной рабо-

те исследования. Полученная модель позволяет проследить динамику поведения каждого узла и каждой линии со своими значениями интенсивностей отказов и интенсивностей восстановления для конфигурации сети высокой сложности, а также позволяет решать задачи, связанные с определением длительности времени до потери связности в маршруте и длительности наработки на отказ всех маршрутов одновременно. Это в свою очередь позволяет формировать оценки сетевой надежности и отказоустойчивости. На основании этого получены значения коэффициента готовности для маршрутов и отдельно взятых узлов ТрС. При оценке полученных значений выявлено то, что наибольшее значение коэффициента готовности имеет сеть при наличии в ней маршрутов, контролируемые и управляемые посредством процессов на основе

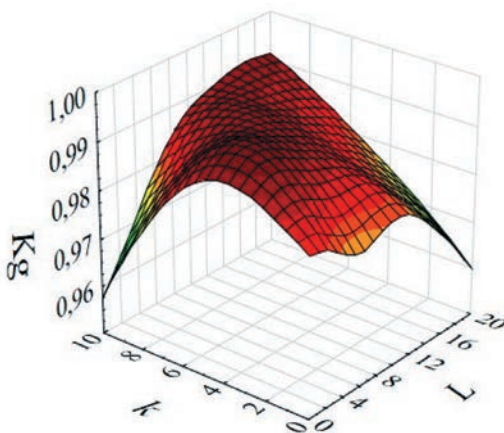


Рис. 5. График зависимости коэффициента готовности (K_g) от количества элементов в маршруте (k) и от количества элементов во фрагменте сети (L)

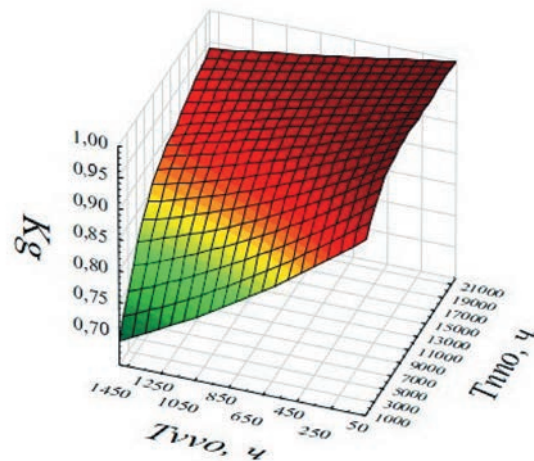


Рис. 6. График зависимости коэффициента готовности (K_g) сети от времени наработки на отказ (T_{mto}) и времени восстановления отказа (T_{mvo}) сетевого элемента Carrier Ethernet

механизмов ОАМ. Несмотря на то, что значение длительности времени наработки на отказ для отдельно взятого узла ТрС намного превышает значение этого параметра для маршрута ТрС, возможность управления состоянием маршрутов с предварительным контролем состояния входящих в него узлов (табл. 3) позволяет получить наибольшее значение коэффициента готовности $K_g = 0,981$.

Моделирование процесса функционирования ТрС позволяет на этапе проектирования перспективной СУ ТрС на базе технологии СЕ выбирать тот или иной вариант формирования конфигурации сети СЕ.

Кроме этого по результатам моделирования выявлена чувствительность модели к таким параметрам как — количество элементов в маршруте, количество элементов внутри фрагмента сети, время наработки на отказ у элемента СЕ, время восстановления отказа у элемента СЕ. Установленные по результатам моделирования закономерности зависимости коэффициента готовности от этих параметров могут быть использованы для выбора приемлемого количества элементов в маршруте и в отдельных сформированных фрагментах сети, а также выбор рационального уровня надежности сети в зависимости от требуемого значения коэффициента готовности.

Литература

1. *Опарин Е. В.* Методика формирования интеллектуальной системы поддержки принятия решений по управлению сетью тактовой сетевой синхронизацией: дис. канд. техн. наук. СПб., 2013. 159 с.
2. *Сахарова М. А.* Разработка моделей функционирования и методики формирования интеллектуальной системы поддержки принятия решений по управлению сетью передачи данных: дис. канд. техн. наук. СПб., 2015. 161 с.
3. *Буренин А. Н., Курносков В. И.* Теоретические основы управления современными телекоммуникационными сетями. М.: Наука, 2011. 464 с.
4. *Карпов Е. А., Котенко И. В., Боговик А. В., Ковалёв И. С., Забело А. Н., Загоруйко С. С. Олейник В. В.* Основы теории управления в системах военного назначения. СПб.: Изд-во ВУС, 2000. 158 с.
5. *Котенко И. В., Боговик А. В.* Теория управления в системах военного назначения. М.: Изд-во МО РФ, 2001. 320 с.
6. *Логин Э. В., Ануфренко А. В., Канаев А. К.* Мультиагентный подход к формированию структуры системы управления транспортной сетью связи на основе технологии Carrier Ethernet // Актуальные проблемы инфотелекоммуникаций а науке и образовании: сборник научных статей (Санкт-Петербург, 1–2 марта 2017). СПб.: Изд-во СПбГУТ, 2017. С. 57–59.
7. *Боев В. Д.* Исследование адекватности GPSS WORLD и ANYLOGIC при моделировании дискретно-событийных процессов: Монография. СПб., 2011. 404 с.
8. *Каталевский Д. Ю.* Основы имитационного моделирования системного анализа в управлении. Изд. 2-е. М.: Изд-во РАНХИГИС, 2015. 496 с.
9. *Бенета Э. В., Канаев А. К.* Формирование алгоритма управления отказами в телекоммуникационной сети связи, построенной по технологии Carrier Ethernet // Информационные технологии на транспорте: сборник материалов секции «Информационные технологии на транспорте» юбилейной XV Междунар. конф. «Региональная информатика — 2016» (Санкт-Петербург, 26–28 октября 2016). СПб.: Изд-во ВО ПГУПС, 2016. С. 95–100.
10. *Бенета Э. В., Канаев А. К.* Анализ функций ОАМ в технологии Carrier Ethernet // 72-я Всероссийская научно-техническая конференция, посвященная Дню радио Секция: «Телекоммуникации на железнодорожном транспорте», (Санкт-Петербург, 27–29 апреля 2017). СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2017. С. 241–242.
11. *Бенета Э. В., Канаев А. К., Сахарова М. А.* Комплексная математическая модель процесса функционирования интеллектуальной системы управления сетью Carrier Ethernet // Сборник докладов в 3-х томах XX Международной конференции по мягким вычислениям и измерениям (SCM-2017) (Санкт-Петербург, 24–26 мая 2017). СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2017. Т. 1. С. 282–285.
12. *Канаев А. К., Опарин Е. В.* Методика оценки и прогнозирования технического состояния оборудования сети синхронизации // Транспорт Урала. 2015. № 1. С. 41–47.
13. *Котов В. К., Антонец В. Р., Лабеецкая Г. П., Шмытинский В. В.* Научно-методические основы управления надежностью и безопасностью эксплуатации сетей связи железнодорожного транспорта: Монография. СПб.: Изд-во Учебно-методического центра по образованию на железнодорожном транспорте, 2012. 193 с.
14. *Бенета Э. В., Канаев А. К.* Выбор телекоммуникационной технологии операторского класса // Автоматика, связь, информатика. 2016. № 7. С. 13–15.
15. *Логин Э. В., Канаев А. К., Сахарова М. А., Муравцов А. А.* Сценарий управления сетью операторского класса Carrier Ethernet и оценка длительности цикла управления // Бюллетень результатов научных исследований. 2017. № 3. С. 159–170. URL: brni.info/view/выпуск-24.html#0 (дата обращения 21.03.2018).

MODEL OF A TRANSPORT COMMUNICATION NETWORK AS A COMPONENT OF A MULTI-AGENT MANAGEMENT SYSTEM

ELINA V. LOGIN,

St-Petersburg, Russia, elinabeneta@yandex.ru

ANDREY K. KANAEV

St-Petersburg, Russia, kanaevak@mail.ru

KEYWORDS: transport network; Carrier Ethernet; agent modeling; AnyLogic; OAM mechanisms; management system; network reliability.

ABSTRACT

To date, there is no unified methodology for the development of a management system (MS) network based on the technology of Carrier Ethernet (CE). There are many standards that describe the architecture and mechanisms for monitoring and managing elements of the CE network (OAM mechanisms), but there are no requirements for the MS for such a communication network. The solution of this problem is possible by modeling the process of functioning of transport network (TrN) on the basis of CE technology for managing its configuration. AnyLogic simulation device was chosen to create the model. The aim of the work is to identify the interdependencies between the reliability indicators of the TrN functioning on the basis of the CE technology and the process of the operation of the TrN management and recovery subsystems. As well as obtaining dependencies of the availability factor on the duration of the time between failure and failure recovery times, as well as on the quantitative characteristics of the configuration of the modeled network fragment. To achieve this goal, it is necessary to develop a model for the operation of the TrN, for the management of which it is proposed to use the agency of the agency management (MAMS) as part of the MS structure. The multi-agent system, which is part of the control system, is in interaction with it. Physically, agents are the information realization of the elements of the structure of the communication network, and their behavior is set up algorithmically in order to jointly achieve the objective function. The use of the distributed control object TrN on the basis of CE technology in MAMS will allow to obtain a demonstration of the dynamics of the state change of the TrN fragment and obtain an estimate of the network reliability. The solution to the problem of building the MAMS model is based on the use of the agent modeling method, which belongs to the class of agent-oriented models. The paper uses the provisions of probability theory, control theory and systems theory. The novelty of the presented model is the choice of a new CE management object, the choice of an original set of control and management mechanisms for their inclusion in the model, the application of the mathematical apparatus of agent modeling. Using the presented model to investigate the functioning of the TrN allows one to trace the dynamics of the behavior of each node and each route with its failure and recovery

rates for a network structure of any complexity, allows solving tasks related to determining the length of time before the loss of connectivity in the route and the duration of the time between failures of all routes simultaneously, allows to form estimates of network reliability and fault tolerance. The presented model of TrN functioning and the obtained network reliability estimates taking into account the architecture of CE domains and the mechanisms for monitoring and managing the network state allow one to choose one or another variant of the configuration of the CE network at the design stage of the advanced MS based on the CE technology. That is, based on the network availability factor values, you can select an existing OAM architecture or specify a different architecture for the network elements routes in accordance with the requirements for the network availability factor required for the advanced MS.

REFERENCES

1. Oparin E.V. *Metodika formirovanija intellektual'noj sistemy podderzhki prinjatija reshenij po upravleniju set'ju taktovoj setevoj sinhronizaciej* [Method of forming an intelligent decision support system for network management by clock network synchronization. Ph. tech. sci. diss.]. St. Petersburg, 2013. 159 p. (In Russian)
2. Sakharova M.A. *Razrabotka modelej funkcionirovanija i metodiki formirovanija intellektual'noj sistemy podderzhki prinjatija reshenij po upravleniju set'ju peredachi dannyh* [Development of models of functioning and methods of formation of an intelligent decision support system for managing a data network. Ph. tech. sci. diss.]. St. Petersburg, 2015. 161 p. (In Russian)
3. Burenin A.N., Kurnosov V.I. *Teoreticheskie osnovy upravlenija sovremennymi telekommunikacionnymi setjami* [Theoretical bases of management of modern telecommunication networks]. Moscow: Nauka, 2011. 464 p. (In Russian)
4. Karpov E.A., Kotenko I.V., Bogovik A.V., Kovalev I.S., Zabelo A.N., Zagorulko S.S., Oleinik V.V. *Osnovy teorii upravlenija v sistemah voennogo naznachenija* [Fundamentals of control theory in military systems]. Saint-Petersburg: VUS, 2000. 158 p. (In Russian)
5. Kotenko I.V., Bogovik A.V. *Teorija upravlenija v sistemah voennogo naznachenija* [The theory of control in military systems]. Moscow:

Ministry of defence of Russian Federation, 2001. 320 p. (In Russian)

6. Login, E.V., Anufrenko, A.V., Kanaev, A.K. Mul'tiagentnyj podhod k formirovaniju struktury sistemy upravlenija transportnoj set'ju svjazi na osnove tehnologii Carrier Ethernet [Multi-agent approach to structure formation of management of transport networks based on Carrier Ethernet technology] *Aktual'nye problemy infotelekomunikacij a nauke i obrazovanii: sbornik nauchnyh statej* [Collection of scientific papers by 6th International conference on Advanced infotelecommunication, Saint-Petersburg, March 1-2, 2017]. St. Petersburg: Sankt-Peterburgskij gosudarstvennyj universitet telekomunikacij Publ., 2017. Pp. 57-59. (In Russian)

7. Boev V.D. *Issledovanie adekvatnosti GPSS WORLD i ANYLOGIC pri modelirovanii diskretno-sobytijnyh processov* [A study of the adequacy of GPSS WORLD and ANYLOGIC in modeling discrete-event processes]. St. Petersburg: Voennaya akademiya svyazi imeni marshala Sovetskogo Soyuza S. M. Budennogo Publ., 2011. 404 p. (In Russian)

8. Katalievsky D. Yu. *Osnovy imitacionnogo modelirovanija sistemnogo analiza v upravlenii* [Tutorial Principles of simulation modeling of system analysis in management], 2nd ed. St. Petersburg, Rossiyskaya akademiya narodnogo khozyaystva i gosudarstvennoy sluzhby Publ., 2015. 496 p. (In Russian)

9. Beneta E.V., Kanaev A.K. Formirovanie algoritma upravlenija otkazami v telekommunikacionnoj seti svjazi, postroennoj po tehnologii Carrier Ethernet [Development of control algorithm by failures in the telecommunication network based on Carrier Ethernet technology] *Informacionnye tehnologii na transporte: sbornik materialov sekcii "Informacionnye tehnologii na transporte" jubilejnoy XV Mezhdunar. konf. "Regional'naja informatika – 2016"* [Information technologies at transport: proc. section "Information technologies at transport" XV St. Petersburg International conference "Regional informatics – 2016", Saint-Petersburg, October 26-28, 2016]. St. Petersburg, 2016. Pp. 95-100. (In Russian)

10. Beneta E.V., Kanaev A.K. Analiz funkcyj OAM v tehnologii Carrie Ethernet [Analysis of OAM functions in Carrier Ethernet technology] *72-aja Vserossijskaja nauchno-tehnicheskoy konferencija, posvjash-*

hennaja Dnju radio Sekcija: «Telekommunikacii na zheleznodorozhnom transporte» [Proceedings of the 72st International Scientific and Technical Conference, cons. Day of radio, 20-28 April, 2017]. Saint-Petersburg, 2017. Pp. 241-242. (In Russian)

11. Beneta E.V., Kanaev A.K., Sakharova M.A. Kompleksnaja matematicheskaja model' processa funkcionirovanija intellektual'noj sistemy upravlenija set'ju Carrier Ethernet [Mathematical metamodel of the process of functioning of the intelligent management system of the Carrier Ethernet network]. *Sbornik dokladov XX Mezhdunarodnoy konferencii po myagkim vychisleniyam i izmereniyam (SCM-2017)* [Proceeding of XX International conference on soft computing and measurements, Saint-Petersburg, May 24-26, 2017]. St. Petersburg, 2017. Vol. 1. Pp. 282-285. (In Russian)

12. Kanaev A.K., Oparin E.V. Technique of estimation and forecasting of the technical condition of the synchronization network equipment. *Transport of the Urals*. 2015. No.1. Pp. 41-47. (In Russian)

13. Kotov V.K., Antonets V.R., Labetskaia G.P., Shmytinskii V.V. *Nauchno-metodicheskie osnovy upravlenija nadezhnost'ju i bezopasnost'ju jekspluatacii setej svjazi zheleznodorozhnogo transporta* [Scientific and methodical foundations for managing the reliability and safety of operation of communication networks of railway transport]. St.Petersburg: Uchebno-metodicheskij tsentr po obrazovaniju na zheleznodorozhnom transporte, 2012. 193 p. (In Russian)

14. Beneta E.V., Kanaev A.K. The choice of carrier-class telecommunication technology. *Automation, communication and Informatics*. No. 7. Pp. 13-15. (In Russian)

15. Login E.V., Kanaev A.K., Muravtsov A.A. Carrier Ethernet network operation scenario and the assessment of control cycle duration. *Bulletin of scientific research results*. No. 3. Pp. 159-170. URL: <http://brni.info/view/выпуск-24.html#/158>. (In Russian)

INFORMATION ABOUT AUTHORS:

Login E.V., Applicant PhD, lecturer at the Department of "Electrical Communication" of the St. Petersburg State Transport University;
Kanaev A.K., PhD, Full Professor, Head at the Department of "Electrical Communication" of the St. Petersburg State Transport University.

doi 10.24411/2409-5419-2018-10040

ДВУХУРОВНЕВАЯ МОДЕЛЬ КООРДИНАЦИИ ПОДСИСТЕМ РАДИОМОНИТОРИНГА И РАДИОЭЛЕКТРОННОЙ БОРЬБЫ

МИХАЙЛОВ
Роман Леонидович

АННОТАЦИЯ

В работе проведен анализ путей развития систем управления боевыми действиями и особенностей их функционирования при переходе к сетевому принципу. Показана важность ведения информационного противоборства и направление, в рамках которого оно может быть развернуто на тактическом и оперативном уровнях, а именно решение задач дезорганизации функционирования систем управления противника и обеспечения устойчивости функционирования своих систем управления. Ввиду того, что решение данных задач возлагается на подсистемы радиомониторинга и радиоэлектронной борьбы, большую важность приобретают вопросы управления сложными организационно-техническими комплексами, входящими в их состав, при организации взаимодействия. Сделан вывод о необходимости использования математического аппарата теории иерархических многоуровневых систем при моделировании данного взаимодействия. На основе известных исследований в данной области предложена двухуровневая модель координации подсистем радиомониторинга и радиоэлектронной борьбы, описаны и формализованы связи между ее составными частями. Противостоящая сторона в модели представлена совокупностью внешних воздействий, поступающих на вход процесса информационного противоборства. Проведена декомпозиция этого процесса на подпроцессы радиомониторинга и радиоподавления, показана и формализована взаимосвязь между ними. Особенностью разработанной модели является установленная взаимосвязь показателей эффективности подсистем радиомониторинга и радиоэлектронной борьбы от выходного сигнала того подпроцесса, на который они оказывают влияние и отсутствие возможности для координатора непосредственно влиять на подпроцессы или процесс в целом, что отражает специфику функционирования частей и подразделений радиомониторинга и радиоэлектронной борьбы, объединенных единым командно-штабным центром. Обозначены дальнейшие направления исследований.

Сведения об авторе:

к.т.н., преподаватель Череповецкого
высшего военного инженерного
училища радиоэлектроники,
г. Череповец, Россия,
mikhailov-rom2012@yandex.ru

КЛЮЧЕВЫЕ СЛОВА: сетевый принцип управления; информационное противоборство; радиомониторинг; радиоэлектронная борьба; иерархические многоуровневые системы; координация.

Анализ войн и вооруженных конфликтов конца XX начала XXI века убедительно показывает, что сегодня появился принципиально новый тип войн — высокотехнологичные войны, в которых применяются новейшие виды высокоточного и информационного оружия. Впервые они наблюдались в 2003 году в ходе действий коалиционных сил в Ираке, когда вместо длительных сражений имели место скоротечные боевые столкновения сравнительно небольших воинских формирований (бригадного уровня), оснащенных современными системами разведки, управления и обеспечения. Произошел переход от «линейных» фронтовых и армейских операций к «объемным» сетцентрическим действиям. Очевидно, что изменение форм и способов военных действий непосредственно определяет организацию управления войсками [1].

Таким образом, есть все основания полагать, что в ближайшее время ключевая парадигма ведения вооруженного противоборства, действующая в армиях США и стран НАТО, а также внедряемая в Вооруженных Силах РФ, будет базироваться на концепции управления боевыми действиями по сетцентрическому принципу. Следует напомнить что в соответствии с этим принципом в составе привлекаемой к военным действиям группировки войск (сил) выделяются функционально взаимосвязанные подсистемы: сенсорно-разведывательная, боевая (исполнительная) и информационно-управляющая.

На основе формируемого коммуникационными системами единого информационного пространства (ЕИП) происходит объединение этих подсистем между собой, что дает значительный прирост в эффективности применения войск и оружия [2–5].

В задачи сенсорно-разведывательной подсистемы входят: информирование своих войск и дезинформация противника; дезорганизация его сетей информационного обмена и защита своих сетей; формирование требуемой «виртуальной» общественно-политической реальности; информационно-психологическое давление на противника. Таким образом, в ее состав входят части и подразделения радиомониторинга (РМ), психологических операций, радиоэлектронной борьбы (РЭБ), а также обслуживания АСУ и связи.

Информационно-управляющая подсистема предназначена для обеспечения взаимодействия между боевыми частями и командно-штабными центрами путем создания единого информационного пространства (ЕИП) ведения боевых действий. ЕИП представляет собой совокупность информации о противнике, своих войсках и условиях ведения боевых действий, получаемой автономными командно-штабными и боевыми модулями и характеризующейся согласованностью по составу, объему и срокам доведения. Создание такого пространства предполагает формирование совокупности информационных контуров, к которым

относятся: контур информации о своих войсках, контур разведывательной информации, навигационный контур, контур метеорологической информации и другие.

В предлагаемой организации принципиально изменяются функции командно-штабных центров, играющих роль органов управления. Во-первых, командно-штабные центры выполняют функции скорее координатора (диспетчера), чем руководителя, как в иерархических организациях, что будет проявляться в предоставлении определенной степени свободы в принятии решений на низших уровнях управления. Во-вторых, принятие решения на ведение военных действий может проводиться децентрализованно [1].

О сущности и содержании концепции управления боевыми действиями по сетцентрическому принципу написано достаточно подробно и много, из последних публикаций по этой тематике следует отметить работы [6–11]. Ключевыми и неразрывно связанными компонентами данной концепции стали такие понятия, как «информационное противоборство», «информационное превосходство», «информационные операции», «действия в кибернетическом пространстве». Не пытаясь «привести к общему знаменателю» взгляды различных авторов, следует отметить, что все они сходятся в определении, что основной целью информационного противоборства в военной сфере является достижение информационного превосходства над противостоящей стороной. Это связано с тем, что именно завоевание и удержание информационного превосходства в настоящее время становится обязательным этапом и необходимым условием начала и ведения современных военных действий. При этом под информационным превосходством понимается *возможность и способность осуществлять непрерывный сбор сведений, их обработку, распределение потока достоверной информации, а также способность не допустить выполнения аналогичных действий противником*. Проявляться информационное превосходство может в различных формах — от возможности и способности более качественно и быстро оценивать обстановку, принимать и доводить до подчиненных адекватные решения, до исключения (существенного затруднения) информационного обеспечения противника за счет проведения наступательных информационных операций [5].

В работе [12] указывается на два направления, в рамках которых может быть развернуто информационное противоборство: информационно-техническое и информационно-психологическое. Последнее из направлений применимо, в основном, на стратегическом уровне управления, в то время как на тактическом и оперативном уровнях под информационным противоборством в настоящее время понимаются отдельные вопросы организации управления и РЭБ [12].

Для достижения указанной цели конфликтный характер информационного противоборства в военной сфере

ре предопределяет необходимость решения двух асимметричных задач: дезорганизации систем управления противника и обеспечение устойчивости функционирования своих систем управления. При этом под дезорганизацией систем управления понимается, как правило, снижение их эффективности. Учитывая радиоэлектронную природу РМ и РЭБ и оставляя в стороне информационно-психологический аспект информационного противоборства, можно утверждать, что все мероприятия, осуществляемые в мирное и военное время для решения указанных выше задач на тактическом и оперативном уровнях, будут решаться именно соответствующими частями и подразделениями [13].

В этих условиях актуальными являются вопросы организации взаимодействия между подсистемами РМ и РЭБ, в частности, решение задачи распределения ограниченного числа объектов информационного пространства противостоящей стороны между данными подсистемами. Целью подсистемы РМ, в самом общем описании, является перехват сообщений, циркулирующих по каналам связи, в целях обеспечения военного руководства информацией о противостоящей стороне, в то время как подсистема РЭБ функционирует в целях срыва процесса управления противостоящей стороной путем подавления соответствующих каналов связи. В интересах достижения своих целей каждая из этих подсистем заинтересована в использовании как можно большего количества объектов информационного пространства противостоящей стороны, однако вследствие естественных причин один объект не может одновременно служить целью воздействия РМ и РЭП.

В работе [14] показано, что процесс организации взаимодействия подсистем РМ и РЭБ в интересах достижения информационного превосходства может быть исследован с помощью математического аппарата теории координации, широко используемого в различных предметных областях [15].

Анализ работ [16–18] позволил формализовать процесс организации взаимодействия подсистем РМ и РЭБ при ведении информационного противоборства в виде двухуровневой модели координации, представленной на рисунке. Отдельные блоки изображают отдельные подсистемы, а их взаимное расположение отражает иерархическую структуру всей системы в целом. Система включает в себя следующие основные подсистемы:

- вышестоящую управляющую подсистему C_0 (командно-штабной центр);
- нижестоящие управляющие подсистемы C_1 и C_2 (подсистемы правления процессами РМ и РЭБ соответственно);
- управляемый процесс A (информационного противоборства).

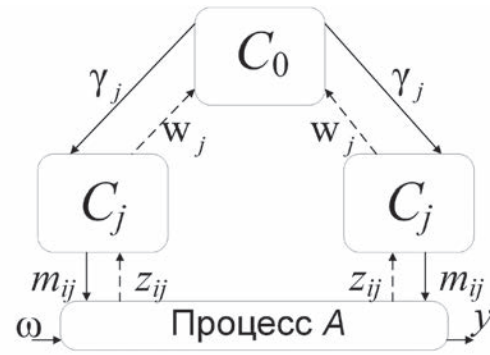


Рис. Двухуровневая модель координации подсистем РМ и РЭБ

В рамках модели описаны два вида вертикального межуровневого взаимодействия между подсистемами. Первый вид такого взаимодействия — это передача «вниз» командных сигналов; при этом сигналы от нижестоящих управляющих подсистем C_1, C_2 являются управляющими воздействиями (входами) для процесса A , тогда как сигналы от вышестоящей подсистемы C_0 к нижестоящим управляющим подсистемам C_1, C_2 являются координирующими сигналами (входами), координирующими выдачу соответствующих управляющих воздействий на процесс A . Второй вид вертикального взаимодействия — это передача «вверх» подсистемам C_1, C_2 информационных сигналов, или сигналов обратной связи для вышестоящей подсистемы C_0 . Эти сигналы показаны на рисунке пунктирными линиями. Описание подсистем двухуровневой системы произведено с использованием терминальных переменных: входов и выходов. При этом подсистемы описаны как функциональные в том смысле, что входы однозначно определяют выходы; т.е. эта ситуация рассматривается как та, в которой известно текущее состояние. Поэтому каждый из блоков на рисунке представляет собой отображение.

Рассмотрим процесс A , как некую управляемую подсистему, к которой поступают управляющие воздействия от подсистем управления нижнего уровня C_1, C_2 . В этом случае на входы процесса A поступают сигналы двух видов:

- управляющие сигналы $m_{ij}, m_{ij} \in M_j$, где M_j — множество управляющих сигналов j -той подсистемы управления $C_j, i=1, \dots, I, j=1, 2$;
- сигналы $\omega, \omega \in \Omega$, представляющие собой внешние возмущения для процесса A .

Под $u, y \in Y$ принят «выход» процесса A (исход информационного противоборства), соответственно, множество Y является множеством выходов процесса A . Под внешними возмущениями $\omega, \omega \in \Omega$ понимаются действия противника в ходе информационного противоборства. Таким образом, процесс A может быть представлен в виде отображения:

$$A : M \times \Omega \rightarrow Y.$$

Поскольку имеется две нижестоящие (локальные) управляющие подсистемы C_1, C_2 , представим множество управляющих сигналов M для процесса A в виде декартова произведения двух множеств

$$M = M_1 \times M_2,$$

причем j -я локальная управляющая подсистема C_j может выбирать только один из управляющих сигналов m_{ij} , оказывая тем самым соответствующее воздействие на процесс A . Рассмотрим j -ю локальную подсистему управления C_j , представляющую собой систему вход — выход. К подсистеме C_j также поступают входные сигналы двух видов:

- координирующие сигналы $\gamma_j, \gamma_j \in \xi$, поступающие на C_j от вышестоящей управляющей подсистемы C_0 ,
- информационный сигнал z_{ij} (сигнал обратной связи) $i = 1, \dots, I, j = 1, 2$, поступающий от процесса A .

Выходом C_j является (локальное) управление m_{ij} , выбираемое из множества M_j . Будем считать, что с помощью рассматриваемой системы реализуется отображение

$$C_j : \xi \times \mathbb{Z}_j \rightarrow M_j,$$

где \mathbb{Z}_j — множество информационных сигналов (сигналов обратной связи), $z_{ij} \in \mathbb{Z}_j, i = 1, \dots, I, j = 1, 2$.

Множество ξ является множеством координирующих сигналов, а его элементы γ_i — соответственно координирующими сигналами, так как с помощью этих сигналов управляющая подсистема C_0 воздействует на нижестоящие, локальные управляющие подсистемы C_1 и C_2 .

Управляющая подсистема C_0 является координатором, так как ее выходные сигналы $\gamma_i \in \xi$ являются координирующими сигналами для подсистем C_1, C_2 . В рамках представленной модели имеется только один вход для подсистемы C_0 — информационный сигнал w_p , получаемый посредством обратной связи от нижестоящих управляющих подсистем и используемый для формирования координирующих сигналов γ_j . В этом случае управляющая подсистема C_0 осуществляет отображение

$$C_0 : W \rightarrow \xi,$$

где W представляет собой множество сигналов w_p , с помощью которых реализуется обратная связь.

Как показано в работе [16] для успешной работы системы, формализованной разработанной моделью, существенно, чтобы цели (задачи) ее подсистем управления были согласованы между собой. В двухуровневой системе имеются цели трех типов, формально описываемые тремя типами решаемых задач: глобальными и решаемыми вышестоящей и нижестоящими подсистемами управления. Совместимость этих целей (принцип совместимости задач) формально вытекает из следующих положений:

1. Только нижестоящие элементы двухуровневой системы являются подсистемами, находящимися в непосредственном контакте со всем процессом. Если должна быть достигнута глобальная цель, то этого можно добиться только через действия нижестоящих подсистем управления элементов; задачи, решаемые на этом уровне, или расположенные на этом уровне решающие элементы должны быть координируемы относительно решаемой глобальной задачи.

2. Вышестоящий элемент, осуществляя координацию, воздействует на нижестоящие элементы, имея в виду свои собственные интересы: координатор выбирает координирующий сигнал так, чтобы продвигаться к осуществлению своей собственной цели. В этом случае задачи, решаемые на уровне нижестоящих элементов, должны быть координируемы по отношению к задачам, решаемым вышестоящим элементом.

3. Глобальная задача, как правило, лежит вне сферы деятельности двухуровневой системы; ни один из решающих элементов внутри иерархии не облечен специально полномочиями решать глобальную задачу и тем самым преследовать общую (глобальную) цель, хотя задача определена в терминах всего процесса. Таковой целью в военной сфере является нанесение поражения противнику. Для совместимости решаемых задач, а тем самым и целей внутри двухуровневой системы, координация задач, решаемых нижестоящими элементами, относительно задачи вышестоящего элемента должна быть соответствующим образом связана с подлежащей решению глобальной задачей.

Для того чтобы завершить описание двухуровневой системы, необходимо уточнить характер сигналов, поступающих по каналам обратной связи. Сигналы обратной связи z_{ij} , поступающие на вход локальной управляющей подсистемы C_j , содержат информацию относительно состояния процесса A ; поэтому они связаны функциональной зависимостью с управляющим сигналом m_{ij} , внешним возмущением ω и с выходным сигналом y . Эта зависимость может быть представлена в виде отображения:

$$f_j : M \times \Omega \times Y \rightarrow \mathbb{Z}_j$$

Аналогично, сигнал w_p , поступающий по каналам обратной связи от локальных подсистем управления C_1 и C_2 , в вышестоящую управляющую подсистему C_0 , содержит в себе информацию относительно состояния нижестоящих управляющих подсистем C_1, C_2 ; Таким образом, сигнал w_p может быть задан отображением:

$$f_0 : \xi \times \mathbb{Z} \times M \rightarrow W,$$

где $\mathbb{Z} = \mathbb{Z}_1 \times \mathbb{Z}_2$; W является множеством координирующих сигналов γ_j , информационных сигналов обратной

связи z_{ij} , получаемых нижестоящими управляющими подсистемами C_j , C_2 , и их управляющих воздействий m_{ij} . На рисунке информация, поступающая по каналам обратной связи, представлена совокупностью информационных сигналов w_j , где w_j — информационный сигнал обратной связи, поступающий от управляющей подсистемы C_j .

Для каждой из подсистем двухуровневой системы необходимо произвести дальнейшую декомпозицию. Наиболее важна из них декомпозиция процесса A . Что касается отдельных управляющих подсистем, то они нуждаются в декомпозиции только в том случае, если их выходными результатами являются уже не сами решения стоящих перед ними задач, а преобразования получаемых решений.

Процесс A является первопричиной взаимодействия между нижестоящими управляющими подсистемами C_j и именно он вызывает необходимость введения координатора, т.е. вышестоящей управляющей системы. Процесс A рассмотрим как состоящий из двух подпроцессов, каждый из которых управляется одной из управляющих подсистем C_1 или C_2 . Определим, что каждый j -тый подпроцесс есть отображение:

$$A_j : M_j \times U_j \times \Omega \rightarrow Y_j,$$

где U_j — множество (входных) сигналов u_{ij} , $i = 1, \dots, I$, $j = 1, 2$, посредством которых подпроцесс A_j связывается с другим подпроцессом. Формально можно представить себе, что на каждый подпроцесс воздействует одно и то же внешнее возмущение ω из Ω ; однако влияние одного и того же внешнего возмущения может по-разному сказаться на каждом из подпроцессов. Таким образом, внешние возмущения ω из Ω могут быть двухкомпонентными наборами (ω_1, ω_2) , так что на j -й подпроцесс воздействует только j -я компонента ω . Для каждого j задано отображение:

$$H_j : M \times Y \rightarrow U_j,$$

которое связывает подпроцессы. Как показано в работе [16], H_j является проекционным отображением.

Множества U_j являются множествами связующих сигналов, а их элементы — связующими сигналами (входами). Отображения H_j являются связующими функциями подпроцессов.

Соотношение между процессом A и его подпроцессом A_j выглядит следующим образом. Положим $U = U_1 \times U_2$ и определим функции H на множестве $M \times Y$ и \bar{A} на множестве $M \times U \times \Omega$ в виде

$$H(m_{ij}, y) = (H_1(m_{ij}, y), H_2(m_{ij}, y))$$

$$\bar{A}(m_{ij}, u, \omega) = (A_1(m_{i1}, y_{i1}, \omega), A_2(m_{i2}, y_{i2}, \omega))$$

В этом случае компонентами A являются не связанные между собой подпроцессы, в то время как с помощью H осуществляется их соединение. Процесс A состоит из связанных между собой подпроцессов, если условие:

$$y = \bar{A}(m_{ij}, H(m_{ij}, y), \omega) \Leftrightarrow y = A(\omega)$$

выполняется для всех (m_{ij}, y, ω) в $M \times Y \times \Omega$; т.е. существует решение системы уравнений

$$y = \bar{A}(m_{ij}, u_{ij}, \dot{E}),$$

$$u = H(m_{ij}, y)$$

для любого заданного управляющего воздействия m из M и возмущающего воздействия ω из Ω и дает выход $y = A(m_{ij}, \omega)$. Отсюда следует, что связующие сигналы u_{ij} , поступающие на входы подпроцессов, могут быть функционально связаны с управляющими воздействиями m и внешними возмущениями ω . Точнее, u_{ij} является результатом отображения:

$$K : M \times \Omega \rightarrow U,$$

которое, в свою очередь, определяется уравнением:

$$K(m_{ij}, \omega) = H(m_{ij}, A(m_{ij}, \omega)).$$

Функция K является функцией взаимодействия подпроцессов. Таким образом процесс A определяется через подпроцессы, а отображение K — с помощью соотношения:

$$P(m_{ij}, \omega) = \bar{P}(m_{ij}, K(m_{ij}, \omega), \omega).$$

Таким образом, разработанная модель учитывает следующие особенности организации взаимодействия подсистем РМ и РЭБ.

1. Каждая из подсистем заинтересована главным образом в одном аспекте процесса, хотя окончательный результат ее действий зависит от всего процесса. Имея в виду этот «локальный» интерес, каждая j -ю локальная управляющая система C_j связана с j -ми компонентами управляющего воздействия m_{ij} и выхода y ; т.е. j -я локальная управляющая подсистема C_j в первую очередь интересуется связью между управляющим воздействием m_{ij} и выходом y_j , являющимся результатом осуществления j -го подпроцесса A_j .

2. Связующие функции подпроцессов H_j определяют характер декомпозиции процесса A . Как показано в работе [16] в большинстве случаев связующие функции H_j будут проекционными отображениями: связующие сигналы u_{ij} будут образованы компонентами терминальных переменных процесса m_{ij} и y .

3. Функция взаимодействия K отражает весь процесс A , так как для любого управляющего сигнала m и возмущающего воздействия ω K определяет (поскольку $K(m, \omega)=u$) связующие сигналы, которые поступят на вход подпроцессов A_j и, кроме того, $u = H(m, P(m, \omega))$. K может также рассматриваться как отображение подпроцесса, который порождает взаимодействия подпроцессов A_j .

В ходе дальнейших исследований планируется уточнить декомпозицию процесса информационного противоборства и формализовать управляющие воздействия, оказываемые подсистемами РМ и РЭБ, с помощью математического аппарата теории распределения ресурсов [19–22]. При этом под распределяемым ресурсом предлагается принять объекты информационного пространства противника. Учесть динамический характер ведения информационного противоборства планируется путем применения элементов математического аппарата теории дифференциальных игр [23]. При разработке методов координации подсистем РМ и РЭБ будут использованы особенности функционирования объектов информационного пространства противника на сетевом уровне эталонной модели взаимодействия открытых систем [24–25].

Литература

1. Раскин А. В., Тарасов И. В. «Сетецентризм» как информационно-управляющая технология высокотехнологичной войны // Информационные войны. 2014. № 3 (31). С. 2–5.
2. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3(48). С. 93–101.
3. Макаренко С. И., Бережнов А. Н. Перспективы использования сетецентрических технологий управления боевыми действиями и проблемы их внедрения в ВС РФ // Вестник академии военных наук. 2011. № 4 (37). С. 64–68.
4. Налетов Г. А. К вопросу о разработке концепции нетрадиционных войн и вооруженных конфликтов (Новые формы и способы ведения вооруженной борьбы) // Вестник Академии военных наук. 2012. № 1 (38). С. 29–34.
5. Антонович П. И., Шаравов И. В., Лойко В. В. Сущность операций в кибернетическом пространстве и их роль в достижении информационного превосходства // Вестник Академии военных наук. 2012. № 1 (38). С. 41–45.
6. Донсков Ю. Е., Зимарин В. И., Илларионов Б. В. Подход к построению систем радиоэлектронной борьбы в условиях реализации сетецентрических концепций развития вооруженных сил // Военная мысль. 2015. № 2. С. 40–48.
7. Выпасняк В. И., Гуральник А. М., Тиханычев О. В. Система поддержки принятия решений как «виртуальный штаб» // Военная мысль. 2015. № 2. С. 23–29.
8. Воробьев И. Н., Киселев В. А. Киберпространство как сфера непрямого вооруженного противоборства // Военная мысль. 2014. № 12. С. 21–28.
9. Скоков С. И., Грушка Л. В. Влияние концепции сетецентризма на эволюцию и функционирование системы управления Вооруженными Силами Российской Федерации // Военная мысль. 2014. № 12. С. 33–41.
10. Кузнецов В. И., Донсков Ю. Е., Никитин О. Г. К вопросу о роли и месте киберпространства в современных боевых действиях // Военная мысль. 2014. № 3. С. 13–17.
11. Богданов А. Е., Попов С. А., Иванов М. С. Перспективы ведения боевых действий с использованием сетецентрических технологий // Военная мысль. 2014. № 3. С. 3–12.
12. Троценко К. А. Информационное противоборство в оперативно-тактическом звене управления // Военная мысль. 2016. № 8. С. 20–25.
13. Ильин А. П., Шакин Д. Н. К вопросу о месте радиоэлектронной разведки, радиоэлектронной борьбы и радиоэлектронной маскировки в информационной борьбе // Военная мысль. 2008. № 1. С. 25–30.
14. Макаренко С. И., Михайлов Р. Л. Информационные конфликты — анализ работ и методологии исследований // Системы управления, связи и безопасности. 2016. № 3. С. 95–178. URL: <http://scs.intelgr.com/archive/2016-03/04-Makarenko.pdf>.
15. Михайлов Р. Л. Анализ научно-методического аппарата теории координации и его использования в различных областях исследований // Системы управления, связи и безопасности. 2016. № 4. С. 1–29. URL: <http://scs.intelgr.com/archive/2016-04/01-Mikhailov.pdf>.
16. Месарович М, Мако Д., Такахара И. Теория иерархических многоуровневых систем. М.: Мир, 1973. 343 с.
17. Воронов Е. М. Методы оптимизации управления многообъектными многокритериальными системами на основе стабильно-эффективных игровых решений. М.: Изд-во МГТУ им Н. Э. Баумана, 2001. 576 с.
18. Мистров Л. Е., Серблов Ю. С. Методологические основы синтеза информационно-обеспечивающих функциональных организационно-технических систем. Воронеж: Научная книга, 2007. 281 с.
19. Михайлов Р. Л., Ларичев А. В., Смылова А. Л., Леонов П. Г. Модель распределения ресурсов в информационном конфликте организационно-технических систем // Вестник Череповецкого государственного университета. 2016. № 6. С. 24–29.
20. Гурин Л. С., Дымарский Я. С., Меркулов А. Д. Задачи и методы оптимального распределения ресурсов. М.: Сов. радио, 1968. 463 с.
21. Берзин Е. А. Оптимальное распределение ресурсов и элементы синтеза систем. М.: Сов. радио, 1974. 304 с.
22. Величко С. В., Сербулов Ю. С., Лемешкин А. В. Информационные технологии выбора и распределения ре-

сурсов технологических систем. Монография. Воронеж: Воронежского института высоких технологий, 2006. 244 с.

23. Берзин Е. А. Оптимальное распределение ресурсов и теория игр. М.: Радио и связь, 1983. 216 с.

24. Михайлов Р. Л. Помехозащищенность транспортных сетей связи специального назначения: Монография.

Череповец: Изд-во Череповецкого высшего военного инженерного училища радиоэлектроники, 2016. 128 с.

25. Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18–68. URL: <http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf>.

TWO-LEVEL MODEL OF COORDINATION OF SUBSYSTEMS OF RADIOMONITORING AND ELECTRONIC WARFARE

MIKHAILOV L. ROMAN

Cherepovets, Russia, mikhailov-rom2012@yandex.ru

ABSTRACT

The work analyzes the ways of development of combat management systems and the features of their functioning in the transition to a network-centric principle. The importance of conducting information confrontation and the direction within which it can be deployed at the tactical and operational levels, namely, the resolution of problems of disorganization of the functioning of enemy control systems and ensuring the sustainability of the functioning of their control systems, is shown. In view of the fact that the solution of these tasks is entrusted to the subsystems of radio monitoring and electronic warfare, great importance is attached to the management of complex organizational and technical complexes that are part of them, in the organization of interaction. A conclusion is drawn on the need to use the mathematical apparatus of the theory of hierarchical multi-level systems in the simulation of this interaction. On the basis of known research in this field, a two-level model of coordination of radio monitoring and electronic warfare subsystems is proposed, and the connections between its components are described and formalized. The opposing side in the model is represented in the form of external influences entering the input of the process of information confrontation. The decomposition of this process into radiomonitoring and radio suppression subprocesses has been carried out, and the relationship between them has been shown and formalized. The peculiarity of the developed model is the dependence of the performance indicators of the radio monitoring subsystems and electronic warfare against the output signal of the subprocess to which they influence and the lack of the ability for the coordina-

KEYWORDS: network-centric principle of control; information warfare; radio monitoring; electronic warfare; hierarchical multi-level systems; coordination.

tor to directly influence the subprocesses or the process as a whole, which reflects the specifics of the functioning of radio monitoring and radio- a single command and staff center. Further directions of research are indicated.

REFERENCES

1. Raskin A. V., Tarasov I. V. "Setetsentrizm" as management information technology high-tech warfare. *Informacionnye vojny* [Information Wars]. 2014. No. 3. Pp. 2-5. (In Russian)
2. Antonovich P. I., Makarenko S. I., Mihaylov R. L., Ushanev K. V. New means of destructive effects on network centric military command, control and communication systems in the common information space. *Vestnik akademii voennyh nauk* [Academician of the military sciences]. 2014. No. 3. Pp. 93-101. (In Russian)
3. Makarenko S. I., Berezhnov A. N. Prospects of use of network-centric technologies of combat operations control and problems of their implementation in the armed forces of the Russian Federation. *Vestnik akademii voennyh nauk* [Academician of the military sciences]. 2011. No. 4. Pp. 64-68. (In Russian)
4. Naletov G. A. On the issue of development of concept of non-traditional wars and military conflicts (New forms and ways of military struggle). *Vestnik akademii voennyh nauk* [Academician of the military sciences]. 2012. No. 1. Pp. 29-34. (In Russian)
5. Antonovich P. I., Sharovov I. V., Loiko V. V. Essence of operations in the cybernetic space and their role in the achievement of information superiority. *Vestnik akademii voennyh nauk* [Academician of the

- military sciences]. 2012. No 1. Pp. 41-45. (In Russian)
6. Donskov Y. E., Zimarin V. I., Illarionov B. V. An approach to construction of electronic warfare system in the conditions of realized network-centric concepts of the Armed Forces' development. *Military Thought*. 2015. No 2. Pp. 40-48. (In Russian)
7. Vypasnyak V. I., Guralnik A. M., Tikhanychev O. V. Decision Support System as a «virtual headquarters». *Military Thought*. 2015. No. 2. Pp. 23-29. (In Russian)
8. Vorobyov I. N., Kiselyov V. A. Cyberspace as a sphere of indirect armed confrontation. *Military Thought*. 2014. No. 12. Pp. 21-28. (In Russian)
9. Skokov S. I., Grushka L. V. Influence of network centrism concept on evolution and functioning of the control system of the Armed Forces of the Russian Federation. *Military Thought*. 2014. No. 12. Pp. 3-41. (In Russian)
10. Kuznetsov V. I., Nikitin O. G. On the role of cyberspace in modern warfare. *Military Thought*. 2014. No. 3. Pp. 13-17. (In Russian)
11. Bogdanov A. Ye., Popov S. A., Ivanov M. S. Prospects of warfare using network-centric technologies. *Military Thought*. 2014. No. 3. Pp. 3-12. (In Russian)
12. Trotsenko K. A. Information warfare at the operational-tactical level of control. *Military Thought*. 2016. No. 8. Pp. 20-25. (In Russian)
13. Il'in A. P., Shakin D. N. On the issue of the location of radio electronic reconnaissance, electronic warfare and electronic masking in the information warfare. *Military Thought*. 2008. No. 1. Pp. 25-30. (In Russian)
14. Makarenko S. I., Mikhailov R. L. Information Conflicts - Analysis of papers and research methodology. *Systems of Control, Communication and Security*. 2016. No. 3. Pp. 95-178. URL: <http://sccs.intelgr.com/archive/2016-03/04-Makarenko.pdf>. (In Russian)
15. Mikhailov R. L. An analysis of the scientific and methodological apparatus of coordination theory and its use in various fields of study. *Systems of Control, Communication and Security*. 2016. No. 4. Pp. 1-29. URL: <http://sccs.intelgr.com/archive/2016-04/01-Mikhailov.pdf>. (In Russian)
16. Mesarovic M. D., Macko D., Takahara Y. *Theory of multilevel hierarchical systems*. New York: Academic, 1970. 340 p.
17. Voronov E. M. *Metody optimizatsii upravleniia mnogoob"ektnymi mnogokriterial'nymi sistemami na osnove stabil'no-effektivnykh igrovyykh reshenii* [Optimization Methods, Multi-Site Management Multi-Criteria-Based Systems Consistently-Effective Gaming Solutions]. Moscow: Bauman Moscow State Technical University Publ., 2001. 576 p. (In Russian)
18. Mistrov L. E., Serbulov Iu. S. *Metodologicheskie osnovy sinteza informatsionno-obespechivaiushchikh funktsional'nykh organizatsionno-tekhnicheskikh sistem* [Methodological Basis of the Synthesis for Information and Functional Organizational-Technical Systems]. Voronezh: Nauchnaia kniga Publ., 2007. 232 p. (In Russian)
19. Mikhailov R. L., Larichev A. V., Smyslova A. L., Leonov P. G. Model of resource allocation in a information conflict of complicated organizational and technical systems. *Cherepovets State University Bulletin*. 2016. No. 6. Pp. 24-29. (In Russian)
20. Gurin L. S., Dymarskii Ia. S., Merkulov A. D. *Zadachi i metody optimal'nogo raspredeleniia resursov* [Objectives and methods of optimal resource allocation]. Moscow: Sovetskoe radio, 1968. 463 p. (In Russian)
21. Berzin E. L. *Optimal'noe raspredelenie resursov i elementy sinteza sistem* [Optimal resource allocation and elements of synthesis systems]. Moscow: Sovetskoe Radio, 1974. 304 p. (In Russian)
22. Velichko S. V., Serbulov Iu. S., Lemeshkin A. V. *Informatsionnye tekhnologii vybora i raspredeleniia resursov tekhnologicheskikh sistem. Monografiia* [Information technology acquisition and resource allocation process systems]. Voronezh, 2006. 244 p. (In Russian)
23. Berzin E. L. *Optimal'noe raspredelenie resursov i teoriiia igr.* [The optimal allocation of resources and game theory]. Moscow: Radio i sviaz', 1983. 216 p. (In Russian)
24. Mikhailov R. L. *Pomehozashhishhennost' transportnyh setej svyazi special'nogo naznachenija. Monografiia* [Interference immunity of special transport communication networks]. Cherepovets: Cherepovets Higher Military Engineering School of Radio Electronics Publ., 2016. 128 p. (In Russian)
25. Makarenko S. I. Prospects and Problems of Development of Communication Networks of Special Purpose. *Systems of Control, Communication and Security*. 2017. No. 2. Pp. 18-68. URL: <http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf>. (In Russian)

INFORMATION ABOUT AUTHOR:

Mikhailov R. L., PhD, Lecturer of the Cherepovets Higher Military Engineering School of Radio Electronics.

For citation: Mikhailov R. L. Two-level model of coordination of subsystems of radiomonitoring and electronic warfare. *H&ES Research*. 2018. Vol. 10. No. 2. Pp. 43-50. doi 10.24411/2409-5419-2018-10040 (In Russian)



ВУС

Военно-учетный стол

Программный комплекс

- Информационное сопряжение с БД военных комиссариатов и проведение сверки в электронном виде
- Совместимость с Комплексом программно-информационных средств мобилизационной подготовки экономики (КПИС МПЭ), построен на той же платформе и расширяет возможности данного комплекса
- Возможность загрузки картотек из других программ, организация работы в сети
- Авторский надзор за эксплуатацией ПК ВУС для наращивания рабочих функций и совершенствования программного комплекса, гарантийное обслуживание

Воинский учет в организациях:

- Ведение электронных Картотек организаций, филиалов и граждан (по Т-2 и Т-2 ГС);
- Документы необходимые для ведения ВУ в организации (приказ, план работы, журнал проверок, расписки о приеме документов ВУ и др.);
- Создание и печать отчетных документов по установленным формам в соответствии с Инструкцией ГШ ВС РФ по ведению ВУ в организациях;
- Генерация документов по бронированию.

Первичный воинский учет в органах местного самоуправления:

- Ведение Картотеки организаций зарегистрированных на территории ОМСУ;
- Построение и управление картотекой граждан пребывающих в запасе и призывников в ОМСУ;
- Создание отчетных форм документов и других данных в соответствии с Методическими рекомендациями ГШ ВС РФ по ведению первичного ВУ в ОМСУ;
- Распределение организаций ведущих учет ГПЗ по видам экономической деятельности, формам собственности и численности работающих в ней граждан.

Учет и Бронирование в Межведомственных комиссиях:

- Организация картотеки различных органов РФ от правительства до организации включительно с различными формами учета и отчетности, ведение структуры подчиненности;
- Автоматический расчет форм №6, формы №18 расчет и обобщение суммарной формы №6 за все подотчетные объекты;
- Анализ обеспеченности трудовыми ресурсами;
- Ведение перечня должностей и профессий по бронированию граждан;
- Определение сотрудников подлежащих бронированию, бронирование сотрудников в соответствии с ПДП;
- Заполнение, передача, сбор и обобщение форм ГД.



НПЦ ИРС

Научно-производственный центр
Информационных региональных систем

▶ npcirs.ru

doi 10.24411/2409-5419-2018-10041

МЕТОДИКА ОЦЕНКИ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ФУНКЦИОНИРУЮЩЕЙ В КИБЕРПРОСТРАНСТВЕ

ЗАХАРЧЕНКО

Роман Иванович¹

КОРОЛЕВ

Игорь Дмитриевич²

АННОТАЦИЯ

Функционирование объектов критической информационной инфраструктуры в новой среде – киберпространстве, порождает новые уязвимости и угрозы, и требует разработки нового инструментария обеспечения устойчивости функционирования в условиях компьютерных атак. Управление устойчивостью функционирования критической информационной инфраструктуры ведомственной информационной системы Вооруженных Сил Российской Федерации основывается на знаниях о состоянии объектов управления, состоянии среды функционирования и оказываемых воздействиях. Неотъемлемым элементом таких систем управления является подсистема поддержки принятия решения. Возможности системы управления напрямую зависят от способности подсистемы поддержки принятия решения обеспечить лицо принимающее решение в качественно сбалансированной информацией характеризующей реальное и прогнозируемые состояния объектов критической информационной инфраструктуры и обеспечить обоснованный выбор траектории достижения цели. В связи с этим, разработка методики оценки критической информационной инфраструктуры функционирующей в киберпространстве является актуальной задачей.

Рассматривается методика оценки критической информационной инфраструктуры ведомственной информационной системы федеральных органов исполнительной власти, функционирующей в киберпространстве в условиях противоборства. Результатом оценки выступает значение интегрального критерия фактической способности выполнения целевой функции критической информационной инфраструктуры ведомственной информационной системы. Новизной работы является предложенная авторами методика оценки сложных технических систем, имеющих высокую степень критичности и неопределенности описания. Практическая значимость представленной методики состоит в возможности ее использования для повышения эффективности управления критической информационной инфраструктуры, а также для обоснования новых форм и способов противоборства в киберпространстве. Рассматриваются вопросы кибернетической устойчивости функционирования, её основные компоненты, свойства управления, определяющие киберустойчивость. Осуществлена классификация объектов критической информационной инфраструктуры. Получены зависимости уровня качества от класса состояния объекта критической информационной инфраструктуры и приведена методика и алгоритм его расчета.

КЛЮЧЕВЫЕ СЛОВА: свойства процесса управления; объекты критической информационной инфраструктуры; методика оценки киберустойчивости; киберпространство; кибернетическое противоборство; деструктивные информационные воздействия.

Сведения об авторах:

¹к.т.н., доцент, докторант
Краснодарского высшего
военного училища имени
генерала армии С.М. Штеменко,
г. Краснодар, Россия,
romanzakharchenko@yandex.ru

²д.т.н., профессор, профессор
Краснодарского высшего
военного училища имени
генерала армии С.М. Штеменко,
г. Краснодар, Россия,
romanzakharchenko@yandex.ru

Для цитирования: Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Научные технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52-61. doi 10.24411/2409-5419-2018-10041

Высокая степень автоматизации управления и глобализации информационных систем (ИС) через информационно-телекоммуникационные сети общего пользования (ИТКС ОП) привело к формированию глобального информационного общества и новой среды его функционирования — киберпространству [1–5], что ставит объекты критической информационной инфраструктуры (КИИ) в зависимость от степени защищенности государственной информационной системы (ГИС РФ).

Вся история человечества — это борьба в том или ином ее проявлении за всевозможные ресурсы и новая среда — киберпространство не стала исключением. В [2–3, 6–7] вводится понятие кибернетическое противоборство — разновидность вооруженной борьбы, в ходе которой осуществляется целенаправленное и организованное кибернетическое воздействие на аппаратно-программные комплексы автоматизированных систем управления военного и гражданского назначения противника, направленные на нарушение их нормального функционирования, что ставит объекты КИИ в зависимость от степени защищенности ГИС РФ.

Функционирование объектов КИИ в новой среде — киберпространстве, порождает новые уязвимости и угрозы, и требует разработки нового инструментария обеспечения безопасности КИИ, под которой понимается состояние ее защищенности, обеспечивающее ее устойчивое функционирование в условиях компьютерных атак (ФЗ-187 от 26.07.2017 «О безопасности критической информационной инфраструктуры РФ»).

Анализ научной литературы, посвященной обеспечению безопасности КИИ, надежности и устойчивости

функционирования АСУ объектов КИИ показал, что в них практически не рассмотрены вопросы, связанные:

с разработкой моделей и методов по построению системы оценки состояния объектов КИИ;

с разработкой моделей и методов формирования признаков пространства функционирования КИИ;

с разработкой научно-методического аппарата построения автоматической системы сбора и приведение к единому виду информации характеризующей состояние КИИ в условиях деструктивных информационных воздействий (ДИВ);

с разработкой моделей, методов и методик формирования и ведения единой распределённой системы БД с оперативной аналитической обработкой данных (OLAP);

с разработкой моделей и методов адаптивного управления КИИ учитывающих текущее и прогнозируемое состояние объектов КИИ в условиях ДИВ.

Таким образом, возникает необходимость в разработке подходов к построению системы оценки устойчивости функционирования КИИ РФ.

Кибернетическое противоборство представляет собой процесс противоборства как минимум двух сторон [2, 4, 6–7], причем осуществляемое при совместном использовании общего ресурса (глобального информационного пространства), управление которым должно рассматриваться, как целенаправленное воздействие двух (и более) подсистем управления, стремящихся распространить управляющие воздействия друг на друга (рис. 1).

При этом надо отметить, несмотря на существенные упрощения и идеализацию, модель, представленная

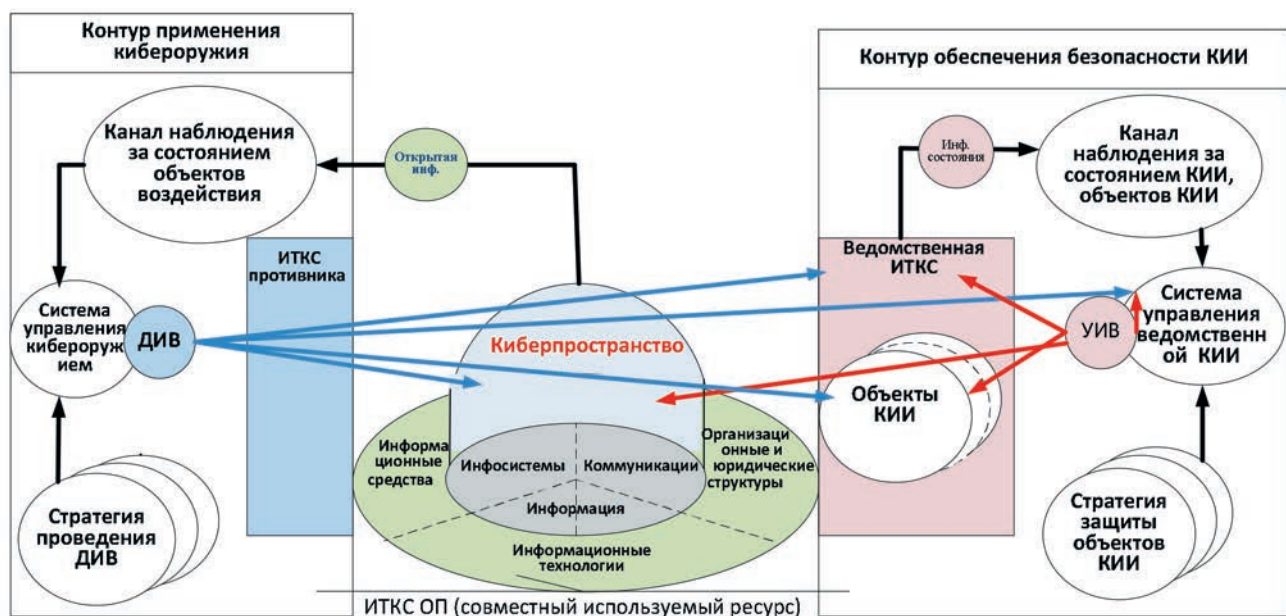


Рис. 1. Модель информационного противоборства в киберпространстве

на рис. 1, позволяет сформулировать важнейшие свойства присущие процессам управления [8–9]: адекватность, оптимальность, оперативность, устойчивость, непрерывность, скрытность.

Рассмотрим данные свойства более детально, с точки зрения функционирования объектов КИИ в киберпространстве в условиях применения нового вида оружия — кибероружия.

1. Адекватность. Адекватность управления заключается в способности данного процесса осуществлять преобразование информации состояния объекта, полученной от подсистемы мониторинга, в управляющие воздействия, на основе которых объект управления переходит в состояние, соответствующее сложившейся ситуации. Очевидно, что корректность данных преобразований во многом будет зависеть от достоверности полученной информации о состоянии и правильности определения целевой функции объекта управления. Таким образом, свойство адекватности в существенной степени зависит от достоверности и полноты информации, корректности операций преобразования информации и их последовательности, а также правильности целей и траекторий их достижения.

2. Оптимальность. Под оптимальностью понимается способность управления осуществлять «продвижение» в направлении достижения цели по кратчайшей (лучшей относительно других, с точки зрения принятых критериев и имеющихся ресурсов) траектории. Иными словами, так как все допустимые траектории приводят к цели, и каждая из них характеризуется определенным расходом ресурсов (временем, дополнительной нагрузкой на вычислительные ресурсы и т.д.), то в смысле «лучшего» потребления этих ресурсов (с точки зрения целесообразности их потребления) существует наиболее предпочтительная траектория. Если в процессе управления система «движется» в пространстве ситуаций именно по этой траектории, то говорят, что управление оптимальное.

3. Оперативность. Оперативность управления представляет собой способность данного процесса преобразовывать информацию в соответствии с установленными временными ограничениями. Иными словами, оперативность есть свойство управления преобразовывать информацию в соответствии с темпом изменения текущей ситуации. В зависимости от вида операции, которая доминирует в том или ином процессе управления, различают оперативность семантического (смыслового) преобразования (например, выработки решения), оперативность преобразования информации (например, оперативность передачи данных или выполнения каких-то расчетов) и др.

4. Устойчивость. Устойчивость управления определяется способностью системы управления выполнять свои функции в сложной, резко меняющейся обстановке в условиях деструктивных воздействий различной при-

роды противоборствующей стороны (сторон). Как правило, устойчивость является интегральным свойством, определяемым живучестью, помехоустойчивостью и надежностью, под которыми понимается способность осуществлять управление в условиях воздействия всех видов оружия (огневого, радиоэлектронного, информационного), технических и программных отказов, а также ошибочных действий технического персонала и должностных лиц, сохраняя при этом значения все показателей управления в установленных пределах.

5. Непрерывность. Под непрерывностью понимается возможность управляющего органа постоянно влиять на объект (объекты) управления, т.е. обеспечить своевременность доведения до объекта управления управляющих воздействий и получать от них информацию о текущем состоянии объекта, независимо от складывающихся условий функционирования.

6. Скрытность. Свойство процесса управления сохранять в тайне от противоборствующей стороны факт, время и место преобразования информации, а также ее содержание и принадлежность управляющим объектам.

Таким образом, важное политическое, военное, хозяйственное значение объектов КИИ с одной стороны и зачастую, их большой разрушительный потенциал с другой стороны в условиях кибернетического противоборства накладывает на процесс управления дополнительные требования по безопасности КИИ. При этом в ФЗ-187 от 26.07.2017 безопасность КИИ предлагается обеспечивать через устойчивость ее функционирования.

Рассмотрим данное свойство с учетом вышесказанного.

В терминах общей теории управления, деструктивные информационные воздействия (компьютерные атаки) в кибернетическом пространстве являются возмущающим воздействием, система управления объектом должна компенсировать эти возмущения, а в целом объект + система управления должны обладать устойчивостью к этим возмущениям, т.е. быть киберустойчивыми (cyber stability). Введем новое свойство устойчивости — киберустойчивость объекта КИИ, под которым в данной работе понимается, способность системы управления объекта КИИ выполнять свои функции в сложной, резко меняющейся обстановке в условиях деструктивных информационных воздействий (рис. 2).

При оценке киберустойчивости объектов КИИ, как составных элементов функционирующей в киберпространстве КИИ, возникает ряд проблем, связанных со сложностью самих объектов КИИ, сложностью и разнородностью связей между ними и условиями совместного с противником использования ресурсов ИТКС.

Из рис. 3 очевидно, что существует достаточно разнообразных объекты КИИ и для дальнейшего их рассмо-

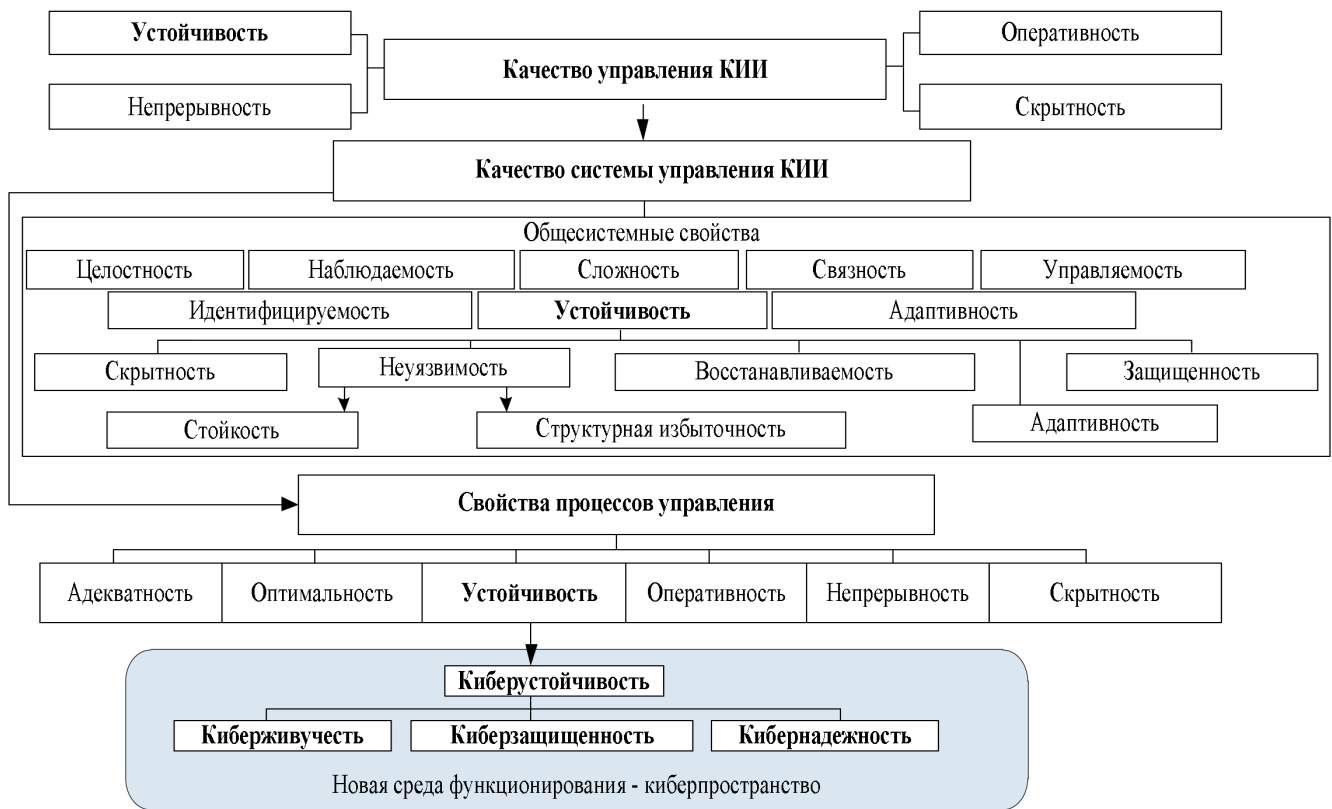


Рис. 2. Схема декомпозиции свойств процесса управления

тения целесообразно произвести их декомпозицию по признакам влияющим на обеспечение киберустойчивости:

1. По структурной организации:

Однозвенные и многозвенные.

Однозвенный объект КИИ — это самодостаточный объект обладающий всей необходимой структурой для выполнения целевой функцией (самостоятельный единичный (базовой) элемент).

Примером однозвенной структуры могут выступать отдельные комплексы средств автоматизации.

Многозвенный объект КИИ — объект, представляющий собой структурное последовательное объединение нескольких однозвенных объектов КИИ в единую систему в рамках выполнения единой целевой функции.

2. По функциональному единству:

Многозвенные однородные и многозвенные неоднородные.

Многозвенные однородные объекты КИИ — объект, представляющий собой структурное последовательное объединение нескольких однозвенных объектов КИИ выполняющих одинаковую целевую функцию, в единую систему в рамках выполнения единой целевой функции.

Примером многозвенной однородной структуры является, много интервальная (составная) сеть передачи данных состоящая из разнотипных однозвенных СПД образующая ИТКС ВС РФ.

Многозвенные разнородные объекты КИИ — объект, представляющий собой структурное последовательное объ-

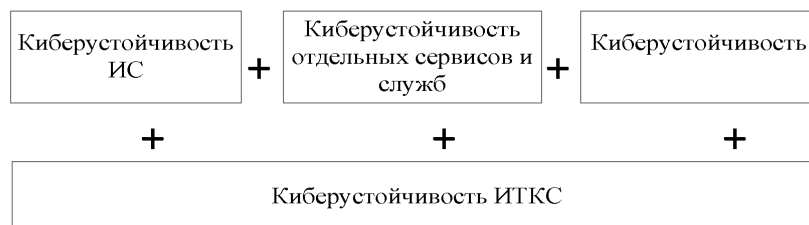


Рис. 3. Слагаемых обеспечения киберустойчивости КИИ

единение нескольких однозвенных объектов КИИ выполняющих разные функции, например информационно-телекоммуникационную сеть, информационные системы и т.д.

Для объектов КИИ использующих ИТКС ОП, предоставляемые сети передачи данных, как правило, всегда являются многозвенными составными. Причем состав отдельных звеньев этих линий зависит от выбранных маршрутов прохождения информации по ИТКС общего пользования и ведомственной ИТКС ВС РФ.

Проведенная выше классификация, позволяет осуществить оценку киберустойчивости сложных организационных систем, как совокупности взаимосвязанных (с учетом коэффициента связанности) однозвенных объектов КИИ с учетом индивидуального (персонального) вклада в выполнение целевой функции системой.

При этом под **киберустойчивостью однозвенного объекта КИИ**, понимается, способность его системы управления выполнять свои функции при всех видах деструктивных информационных воздействий.

Обобщенный показатель киберустойчивости однозвенного объекта КИИ в данном случае имеет вид:

$$K_{\text{окии}^{\text{УО}}} = K_{\text{окии}^{\text{ЖИВ}}} * K_{\text{окии}^{\text{ПОМ}}} * K_{\text{окии}^{\text{НАД}}} \quad (1)$$

где $K_{\text{окии}^{\text{ЖИВ}}}$ — **киберживучесть** — живучесть объекта КИИ, трактуемая как вероятность сохранения его работоспособности (выживания) в условиях выхода из строя технических средств обработки информации, т.е. по сути — вклад каждого базового элемента однозвенного объекта КИИ в выполнение им целевой функции;

$K_{\text{окии}^{\text{ПОМ}}} = (1 - P_{\text{ПКА}}) * (1 - P_{\text{ПЦКА}})$ — **киберзащищенность** однозвенного объекта КИИ, трактуемая как вероятность обеспечения выполнения целевой функции объекта КИИ с заданным качеством в условиях применения «общих» и целенаправленными деструктивными информационными воздействиями;

РПКА и РПЦКА — вероятности поражения технических средств обработки информации, входящих в объект КИИ, «общими» и целенаправленными деструктивными информационными воздействиями соответственно;

$K_{\text{окии}^{\text{НАД}}}$ — **кибернадежность** однозвенного объекта КИИ, трактуемая как вероятность обеспечения выполнения целевой функции объекта КИИ на протяжении определенного временного интервала в условиях возникновения программных ошибок, технических сбоев и непреднамеренных ошибочных действий технического персонала и должностных лиц объекта КИИ.

где
$$K_{\text{окии}^{\text{НАД}}} = \prod_{i=1}^N K_{\text{окии}^{\text{НАД}i}} (1 - P_i) \quad (2)$$

К объектам КИИ уже на этапах проектирования закладываются довольно жесткие требования по техниче-

ской надежности и предусматривается ряд специальных мер по повышению оперативности устранения технических и программных отказов технических средств обработки информации (например, за счет кластеризация серверов, за счет резервирования отдельных обладающих низкой надежностью компонентов ТСОИ). В соответствии с этим в задачах оценки киберустойчивости критической информационной инфраструктуры в условиях деструктивных информационных воздействий, вполне допустимо считать вероятность технических отказов ТСОИ при своевременном и качественном проведении технического обслуживания пренебрежительно малой, т.е. $P_{\text{ТН}} = 1$. В данном случае кибернадежность однозвенного объекта КИИ будет определяться следующим выражением:

$$K_{\text{окии}^{\text{УО}}} = K_{\text{окии}^{\text{ЖИВ}}} * K_{\text{окии}^{\text{ПОМ}}} \quad (3)$$

Если считать выходы из строя звеньев КИИ в условиях деструктивных информационных воздействий независимыми событиями, то киберустойчивость многозвенного объекта КИИ может быть найдена из выражения:

$$K_{\text{окии}^{\text{УМ}}}(N) = \prod_{i=1}^N K_{\text{окии}^{\text{УО}i}} \quad (4)$$

В противном случае киберустойчивость многозвенного объекта КИИ должна рассчитываться как совместная N -мерная вероятность сохранения работоспособности одновременно N звеньев, составляющих данный многозвенный объект КИИ:

$$K_{\text{окии}^{\text{УМ}}}(N) = P \left\{ K_{\text{окии}^{\text{УО}1}} \geq K_{\text{окии}^{\text{УО}оп}}, K_{\text{окии}^{\text{УО}N}} \geq K_{\text{окии}^{\text{УО}оп}} \right\} \quad (5)$$

При этом, очевидно, выражение (4) может служить нижней (гарантированной) оценкой киберустойчивости многозвенного (составного) объекта КИИ.

Как следует из выражений (3) и (4) основой расчета киберустойчивости объектов КИИ является расчет показателей киберзащищенность и киберживучести отдельных звеньев объекта КИИ.

Т.о. необходимо разработать методику расчета показателей киберзащищенности и киберживучести объекта КИИ, причем определяющим свойством с точки зрения возможности выполнения объектом КИИ целевой функции будет киберживучесть, а киберзащищенность будет являться ее составной частью.

Методика оценки киберживучести объектов КИИ

В связи с тем, что свойства, характеризующие киберживучесть объекта КИИ в условиях осуществления деструктивных информационных воздействия, начинают

проявляться только после того, как она подверглась воздействию, то мера живучести должна определяться условной вероятностью сохранения работоспособности, при условии, что система получила локальное повреждение Ω [10].

Под показателем киберживучести однозвенного объекта КИИ, под $K_{\text{ОКИИ}^{\text{жив}}}$ будем понимать условную вероятность невыхода конечного состояния объекта КИИ за границы заданной области безопасных состояний S' пространства S в случае проведения деструктивных информационных воздействий Ω .

$$K_{\text{ОКИИ}^{\text{жив}}} = P\left[\left(\|S - s_0\| < S^I\right) \Omega\right] \quad (6)$$

Исходя из понятия структурной уязвимости системы [1, 6], под которой будем понимать вероятность выхода конечного состояния системы из заданной безопасной области $S' - V_s$ справедливо:

$$K_{\text{ОКИИ}^{\text{жив}}} = 1 - V_s, \quad (7)$$

а в конкретной точке на исследуемом временном интервале:

$$K_{\text{ОКИИ}^{\text{жив}}}(t) = 1 - V_s(t), \quad (8)$$

Критерием оценки киберживучести однозвенного объекта КИИ будем рассматривать выражение:

$$K_{\text{ОКИИ}^{\text{жив}}}^{\text{тек}}(t) \geq K_{\text{ОКИИ}^{\text{жив}}}^{\text{тр}}(t), \quad (9)$$

где $K_{\text{ОКИИ}^{\text{жив}}}^{\text{тек}}(t)$ — текущий уровень живучести однозвенного объекта КИИ, а $K_{\text{ОКИИ}^{\text{жив}}}^{\text{тр}}(t)$ — требуемый уровень его живучести в условиях осуществления деструктивных информационных воздействий.

Также согласно [11–13] определим следующий критерий способности объекта КИИ выполнять целевую

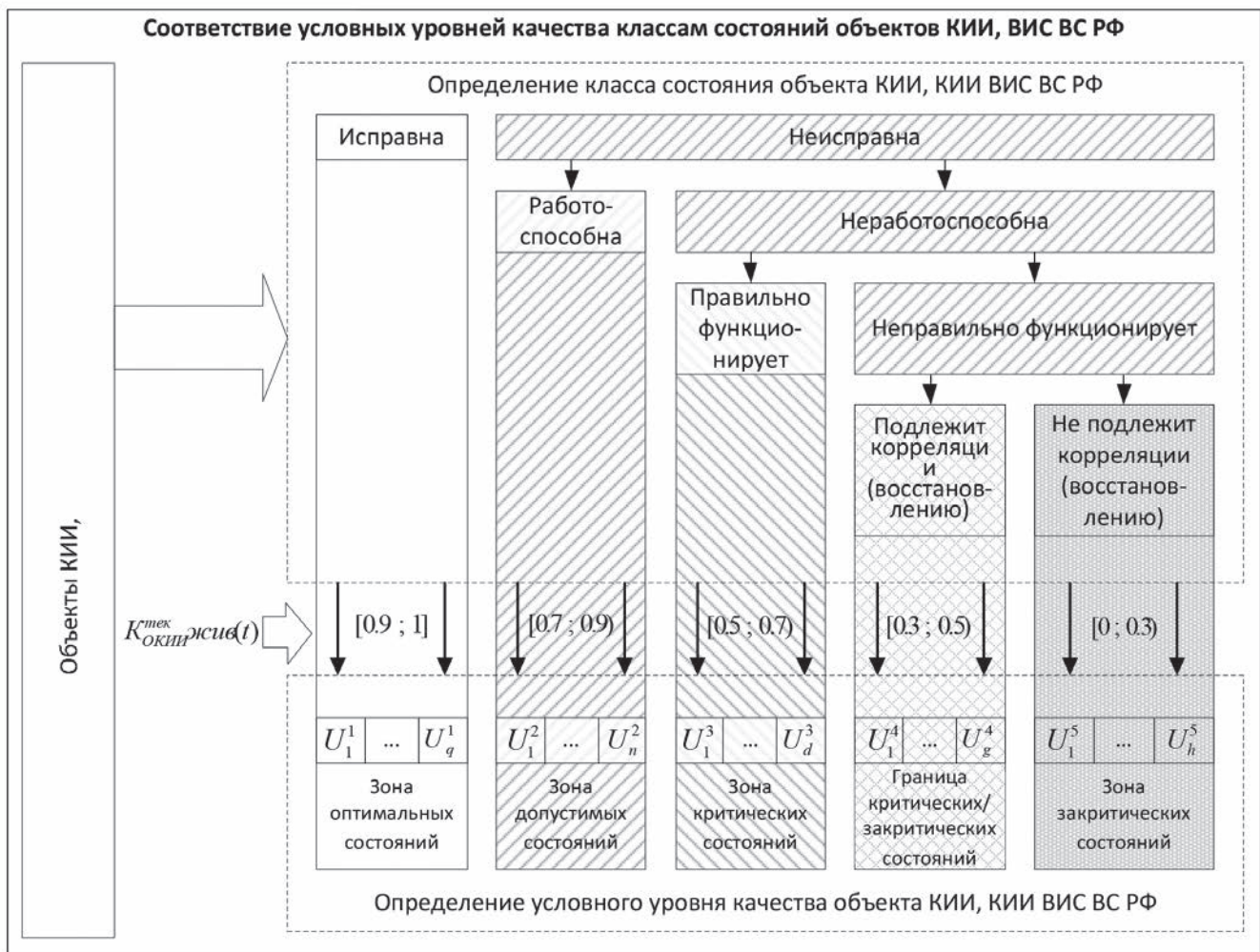


Рис. 4. Схема соответствия класса состояния объекта КИИ уровню качества

функцию в условиях деструктивных информационных воздействий W_6

$$W_6 = \begin{cases} K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) > 0,9 & \text{— объект КИИ полностью боеспособен} \\ 0,9 \leq K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) < 0,7 & \text{— объект КИИ в целом боеспособен} \\ 0,7 \leq K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) < 0,5 & \text{— объект КИИ ограничено б. (основная цель)} \\ 0,5 \leq K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) < 0,3 & \text{— объект КИИ не б., подлежит восстановлению} \\ K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) \leq 0,3 & \text{— объект КИИ не б., не подлежит восстановлению} \end{cases} \quad (10)$$

Для определения общего коэффициента живучести $K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t)$ [12–16] введем следующие уровни киберживучести:

$$K_{\text{окси}^{\text{жив}}}(t) = \begin{cases} K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) - K_{\text{окси}^{\text{тр}}_{\text{окси}^{\text{жив}}}}(t) > 0 & \text{— оптимальный уровень} \\ K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) - K_{\text{окси}^{\text{тр}}_{\text{окси}^{\text{жив}}}}(t) = 0 & \text{— допустимый уровень} \\ K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) - K_{\text{окси}^{\text{тр}}_{\text{окси}^{\text{жив}}}}(t) < 0 & \text{— критический уровень} \\ K_{\text{окси}^{\text{тек}}_{\text{окси}^{\text{жив}}}}(t) = 0 & \text{— закритический уровень (нулевая)} \end{cases} \quad (11)$$

Обобщении результатов полученных в выражениях (10) и (11) и их визуализация представлены на рис. 4.

В общем виде методика оценки киберустойчивости представлена следующими этапами:

1. Этап оценка киберустойчивости каждого объекта КИИ отдельно.

1.1. Оценка однозвенного объекта КИИ.

Оценка киберзащищенности — вероятность выхода из строя i -го ТСОИ в условиях деструктивных информационных воздействий.

Оценить коэффициент связанности i -го ТСОИ и его вклад в целевую функцию объекта КИИ.

Оценка киберживучести — предел состояний однозвенного объекта КИИ.

1.2. Оценка многозвенного объекта КИИ.

Оценка киберзащищенности — вероятность выхода из строя j -го однозвенного объекта КИИ в условиях воздействия деструктивных информационных воздействий.

Оценить коэффициент связанности j -го однозвенного объекта КИИ и его вклад в целевую функцию многозвенного объекта КИИ.

Оценка киберживучести — предел состояний многозвенного объекта КИИ.

2. Этап оценка киберустойчивости взаимодействующих объектов КИИ (стволов объектов КИИ).

Оценка киберзащищенности — вероятность выхода из строя n -го многозвенного объекта КИИ в условиях воздействия деструктивных информационных воздействий.

Оценить коэффициент связанности n -го многозвенного объекта КИИ и его вклад в целевую функцию многозвенного объекта КИИ.

Оценка киберживучести — предел состояний ствола КИИ.

3. Этап оценки киберустойчивости КИИ, через сумму устойчивости ее элементов с учетом их коэффициента связанности.

Оценка киберживучести КИИ в целом, в соответствии с текущим состоянием стволы КИИ и степенью важности, в данный момент времени, выполнения ими функций.

Методика оценки киберустойчивости КИИ в виде блок-схемы схематично приведена на рис. 5.

Таким образом, в рамках разработки методики оценки устойчивости объектов КИИ, функционирующих в киберпространстве, было предложено расширить свойство устойчивости, являющегося интегральным свойством, за счет введения нового свойства — киберустойчивости. Необходимость введения нового свойства вызвана новой средой функционирования ГИС РФ (киберпространство), применения нового вида оружия — кибероружия и как следствие появлением новых уязвимостей и угроз для КИИ и объектов КИИ РФ. Предложенная методика за счет декомпозиции критической информационной структуры на отдельные объекты КИИ с учетом коэффициентов связанности и степени важности, выполняемых в данный момент функций, позволяет осуществить оценку состояния защищенности КИИ в соответствии с заданным уровнем качества. Полученный результат, в соответствии с разработанной схемой соответствия класса состояния объекта уровню качества (рис. 4), позволяет однозначно дать оценку состоянию безопасности КИИ от компьютерных атак (деструктивных информационных воздействий).

Литература

1. Стародубцев Ю. И., Бегаев А. Н., Давлятова М. А. Управление качеством информационных услуг / Под общ. ред. Ю. И. Стародубцева. СПб.: Изд-во Политехнического университета, 2017. 454 с.
2. Глобальная безопасность в цифровую эпоху: стратегия для России / Под общ. ред. Смирнова А. И. М.: ВНИИгеосистем, 2014. 394 с.
3. Макаренко С. И., Чуляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1(2). С. 13–21.
4. Буренин А. Н., Легков К. Е. К вопросу управления современными инфокоммуникационными сетями, функционирующими в условиях интенсивных воздействий // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2014. № 1. С. 101–103.
5. Бедрицкий А. В. Информационная война: концепции и их реализация в США / Под ред. Е. М. Кожокина. М.: Изд-во РИСИ, 2008. 187 с.
6. Слипченко В. И. Войны шестого поколения оружие и военное искусство будущего. М.: Вече, 2002. 382 с.
7. Буренок В. М., Кравченко А. Ю., Смирнов С. С. Курс на сетевую систему вооружений // Военно-

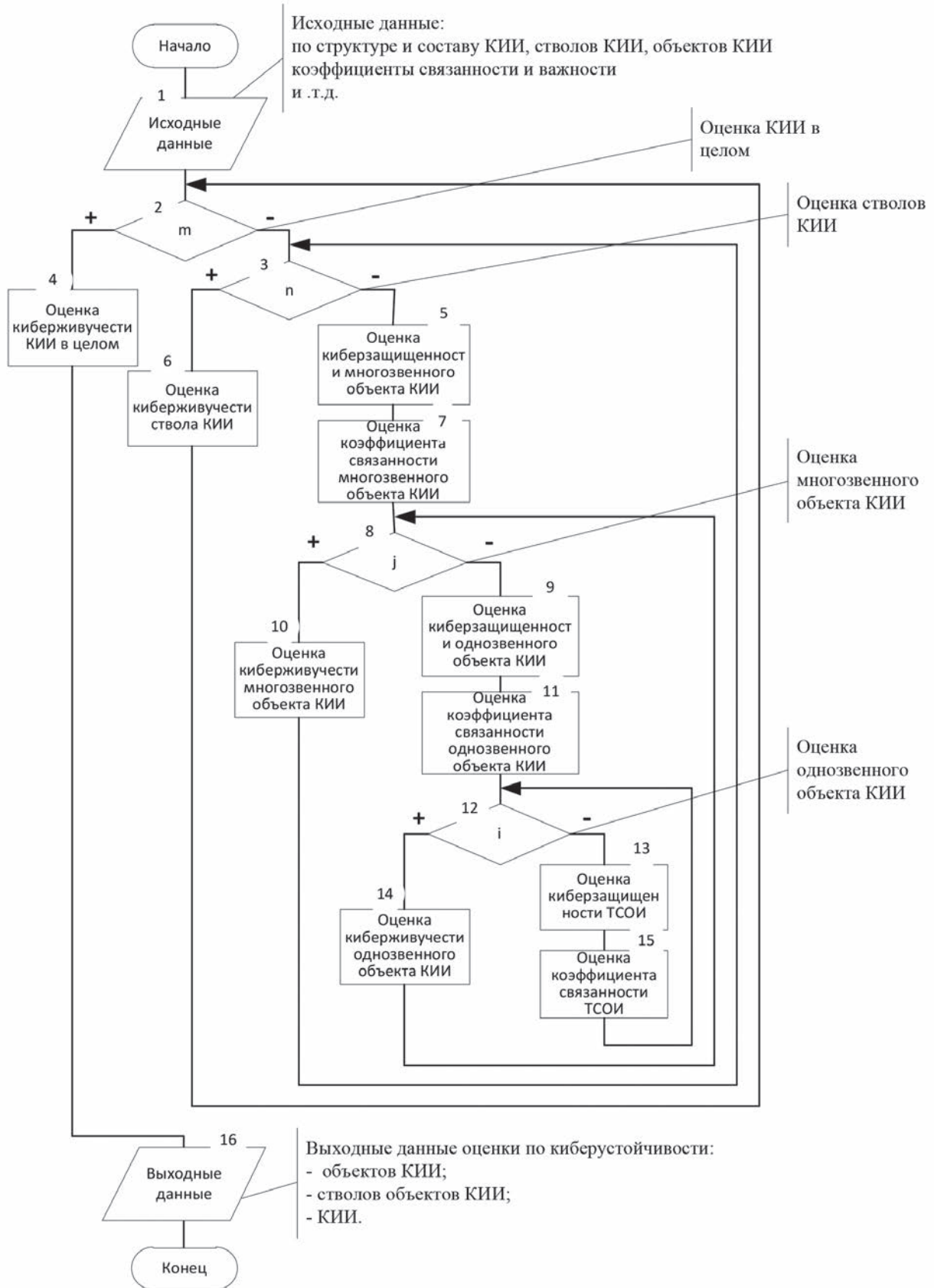


Рис. 5. Обобщенная блок-схема методики оценки киберустойчивости КИИ

космическая оборона. 2009. № 5. URL: <http://www.vko.ru/konceptii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya> (дата обращения 28.11.17).

8. *Боговик А.В., Игнатов В.В.* Теория управления в системах военного назначения. СПб.: ВАС, 2008. 460 с.

9. *Давыдов А.Е., Савицкий О.К., Максимов Р.В.* Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. Москва: Воентелеком, 2015. 520 с.

10. *Мухортов В.В., Королев И.Д.* Концептуальная модель обнаружения внешних программно-аппаратных воздействий на беспилотные летательные аппараты военного назначения // Труды XXXV Всероссийской научно-технической конференции «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (г. Серпухов, 23–24 июня 2016). Серпухов, 2016. Ч. 9. 468 с.

11. *Минаев В.А., Королев И.Д., Мухортов В.В.* Марковские модели защиты информационных систем беспилотных робототехнических объектов // Технологии

техносферной безопасности. 2016. № 6 (70). URL: <http://agps-2006.narod.ru/ttb/2016-6/17-06-16.ttb.pdf>.

12. *Легков К.Е., Никифоров О.Г., Лебякин И.А.* К вопросу многоуровневой защиты информации // Труды Военно-космической академии имени А.Ф.Можайского. 2013. № 640. С. 214–219.

13. *Казаков В.И.* Основы теории топогеодезического обеспечения боевых действий войск. Раздел 1. М.: ВИА, 1977.

14. *Климов С.М., Сычёв М.П., Астрахов А.В.* Противодействие компьютерным атакам. М.: Изд-во МГТУ имени Н.Э.Баумана, 2013. 108 с.

15. *Махутов Н.А., Резников Д.О., Петров П.В.* Оценка живучести сложных технических систем // Проблемы безопасности и чрезвычайных ситуаций. 2009. № 3. С. 47–66.

16. *Сафонов Р.А.* Методика оценки живучести сложных систем военного назначения. URL: <https://www.xreferat.com/17/622-1-metodika-ocenki-zhivuchesti-slozhnyh-sistem-voennogo-naznacheniya.html> (дата обращения 08.09.17).

METHODS OF ESTIMATION OF STABILITY OF FUNCTIONING OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE OPERATING IN CYBERSPACE

ROMAN I. ZAKHARCHENKO,

Krasnodar, Russia, romanzakharchenko@yandex.ru

IGOR D. KOROLEV

Krasnodar, Russia

KEYWORDS: properties of the management process; objects of critical information infrastructure; methods of assessment of cyber stability; cyberspace; cybernetic confrontation; destructive information impact.

ABSTRACT

The functioning of critical information infrastructure in a new environment – cyberspace, creates new vulnerabilities and threats, and requires the development of new tools to ensure the sustainability of functioning in terms of computer attacks. Managing sustainability of critical information infrastructure the armed forces is based on the knowledge about the state of the control objects, the state of the environment functioning and its impacts. An integral part of such management systems is the decision support subsystem. The possibilities of the control system directly depend on the ability of the decision support subsystem to provide the decision-maker with qualitatively balanced information characterizing the real and predictable state of the critical information infrastructure facilities and

to provide a reasonable choice of the trajectory of the goal achievement. In this regard, the development of a methodology for evaluating critical information infrastructure functioning in cyberspace is an urgent task.

The work discusses the method of evaluation of the critical information infrastructure of the departmental information system of Federal Executive authorities, which operates in cyberspace in the conditions of confrontation. The result of the evaluation is the value of the integral criterion of the actual ability to perform the target function of critical information infrastructure of the departmental information system. Novelty of the work is the proposed method of evaluation of complex technical systems with a high degree of criticality and

uncertainty of description. The practical significance of the presented technique is the possibility of its use to improve the efficiency of management of critical information infrastructure, as well as to justify new forms and methods of confrontation in cyberspace. The work deals with the issues of cybernetic stability of functioning, its main components, the properties of management that determine cyber stability. Classification of critical information infrastructure objects is carried out. The dependences of the quality level on the class of the critical information infrastructure object state are obtained and the method and algorithm of its calculation are given.

REFERENCES

1. Starodubtsev Yu.I., Bugaev A.N., Davlyatova M.A. *Kachestvom informacionnykh uslug* [Quality management of information services]. St-Peterburg: Publishing house of Polytechnic University, 2017. 454 p. (In Russian)
2. Smirnova A.I. (Ed.) *Global'naya bezopasnost' v cifrovuyu ehpo: strategiy dlya Rossii* [Global security in the digital age: stratagems for Russia]. Moscow: Vniigeosystem, 2014. 394 p. (In Russian).
3. Makarenko S.I., Chuklyaev I.I. Terminological basis in the field of information warfare. *Voprosy kiberbezopasnosti* [Cybersecurity issues]. 2014. No. 1 (2). Pp. 13–21. (In Russian)
4. Burenin A.N., Legkov K.E. K voprosu upravleniya sovremennymi infokommunikatsionnymi setyami, funktsioniruyushchimi v usloviyakh intensivnykh vozdeystviy [To a question of management of the modern infokommunikatsionny networks functioning in the conditions of intensive influences]. *Trudy Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki* [Proc. of the North Kavkazsky of branch of the Moscow technical university of communication and informatics]. 2014. No. 1. Pp. 101–103. (In Russian)
5. Bedritsky A.V. *Informacionnaya vojna: koncepcii i ih realizatsiya v SSHA* [Information warfare: concepts and their implementation in the United States]. Moscow: Rossiyskiy institut strategicheskikh issledovaniy Publ., 2008. 187 p. (In Russian)
6. Slipchenko V.I. *Vojny shestogo pokoleniya oruzhie i voennoe iskusstvo budushchego* [Wars of the sixth generation weapons and military art of the future]. Moscow: Veche, 2002. 382 p. (In Russian).
7. Burenok V.M., Kravchenko A. Yu., Smirnov S.S. *Kurs na setecentricheskuyu sistemu vooruzhenij* [Course on network-centric weapons system]. *Vozdushno-kosmicheskaya oborona* [Military-space defense]. 2009. No. 5. URL: <http://www.vko.ru/koncepcii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya> (date of access 28.11.17). (In Russian)
8. Bogovik A.B., Ignatov V.V., *Teoriya upravleniya v sistemakh voennogo naznacheniya* [The control theory in military systems] St. Petersburg: Voennaya Akademiya Svyazi Publ., 2008. 460 c. (In Russian)
9. Davydov A.E., Savickj O.K., Maksimov R.V. *Zashita i bezopasnost' vedomstvennykh integriruyemykh infokommunikatsionnykh sistem* [The protection and security of departmental integrated information communication system]. Moscow: Voentelekom, 2015. 520 p. (In Russian)
10. Mukhortov V.V., Korolev I.D., *Konceptual'naija model' obnaruzheniya vnevnikh programmno-apparatnykh vozdeystviy na bespilotnye letatel'nye apparaty voennogo naznacheniya* [Conceptual model of hardware effects on unmanned aerial vehicles for military use]. *Trudy XXXV Vserossijskoj naychno-tekhnicheskoy konferentsii "Problemy effektivnosti i bezopasnosti funkcionirovaniya slozhnykh tekhnicheskikh i informacionnykh sistem (VNTK-2016)"* [Proc. XXXV of the All-Russia scientific and technical conference «Problems of efficiency and safety of functioning of difficult technical and information systems» (Serpukhov, June 23-24, 2016)]. Serpukhov, 2016. Pt. 9. 468 p. (In Russian).
11. Minaev V.A., Korolev I.D., Mukhortov V.V. Markov models of drones information systems protection. *Technology of technosphere safety*. 2016 No. 6 (70). URL: <http://agps-2006.narod.ru/ttb/2016-6/17-06-16.ttb.pdf> (date of access 28.11.17). (In Russian).
12. Legkov K.E., Nikiforov O.G., Ledyankin I.A. K voprosu mnogourovnevnoy zashchity informatsii [To a question of multilevel protection of information]. *Trudy voenno-kosmicheskoi akademii imeni A.F. Mozhaiskogo* [Proc. of the Military Space academy named after A.F.Mozhaisky]. 2013. No. 640. Pp. 214–219. (In Russian)
13. Kazakov V.I. *Osnovu teorii topogeodezicheskogo obespecheniya boevykh deystviy vojsk*. [Fundamentals of the theory of topogeodetic support of combat operations]. Section 1. Moscow: VIA, 1997. (In Russian)
14. Klimov S.M., Sychev M.P., Astrakhov A.V. *Protivodeystvie komp'uternym atakam* [Counteracting computer attacks]. Moscow: Moskovskiy gosudarstvennyy tekhnicheskii universitet imeni N.E. Baumana Publ., 2013. 108 p. (In Russian)
15. Makhutov N.A., Reznikov D.O., Petrov P.V. Ocenka zhivuchesti slozhnykh tekhnicheskikh sistem [Assessment of survivability of complex technical systems]. *Problemy bezopasnosti i chrezvychaynykh situatsiy* [Problems of security and emergency situation]. 2009. No. 3. Pp. 47–66. (In Russian)
16. Safonov R.A. *Metodika ocenki zhivuchesti slozhnykh sistem voennogo naznacheniya* [Methods of evaluating of complex systems for military purposes]. URL: <https://www.xreferat.com/17/622-1-metodika-ocenki-zhivuchesti-slozhnykh-sistem-voennogo-naznacheniya.html> (date of access 08.09.17). (In Russian)

INFORMATION ABOUT AUTHORS:

Zakharchenko R.I., PhD, Doctoral Candidate of the Krasnodar Higher Military School named after army General S.M. Schtemenko; Korolev I.D., PhD, Full professor, Professor of the Krasnodar Higher Military School named after army General S.M. Schtemenko.

doi 10.24411/2409-5419-2018-10042

ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ ЖИВУЧЕСТИ ГРУППЫ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ МЕТОДАМИ МОДУЛЯРНОЙ АРИФМЕТИКИ

САМОЙЛЕНКО

Дмитрий Владимирович¹

ЕРЕМЕЕВ

Михаил Алексеевич²

ФИНЬКО

Олег Анатольевич³

Сведения об авторах:

¹к.т.н., докторант Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, 19sam@mail.ru

²д.т.н., профессор, профессор кафедры прикладных информационных технологий института комплексной безопасности и специального приборостроения Московского технологического университета, г. Москва, Россия, maef1@rambler.ru

³д.т.н., профессор, академический советник Российской академии ракетных и артиллерийских наук (отделение технических средств и технологий разведки, навигации, связи и управления), профессор Краснодарского высшего военного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия, ofinko@yandex.ru

АННОТАЦИЯ

Рассматривается автономная группа робототехнических комплексов, образующая распределенную децентрализованную сетевую информационно-вычислительную систему обработки информации с непредсказуемой и динамически изменяющейся структурой, в которой выполнение «целевой» функции – информирования находится в прямой зависимости от коммуникационной среды. Деструктивные воздействия нарушителя направлены на изменение качественных характеристик информации, определяющих ее пригодность в решении целевых функций автономной группы робототехнических комплексов. Одним из ключевых требований, определяющих качественные характеристики и предъявляемых к информации, является обеспечение ее целостности на всех этапах жизненного цикла. При этом эффективность классических методов контроля и обеспечения целостности определяется в рамках микроуровня (уровень отдельного робота) и не решает этой задачи для группировки в целом. Вследствие чего возникает необходимость в формировании «активного» свойства (защитной функции) преодоления последствий вредных факторов – информационной живучести. Предлагается для таких условий функционирования с целью повышения информационной живучести автономной группы задачу обеспечения и контроля целостности информации осуществлять следующим образом: совокупность запоминающих устройств, размещенных на борту различных, но объединенных единой целью функционирования робототехнических комплексов, рассматривать как единую систему запоминающих устройств с подсистемой криптокодированного преобразования информации. Подсистема криптокодированного преобразования информации, основана на агрегированном применении блочных алгоритмов шифрования и полиномиальных кодов системы остаточных классов. Комплексирование различных по уровням «модели Open Systems Interconnection» методов обработки информации обеспечивает целостность информации с возможностью ее восстановления в автономной группе робототехнических комплексов при воздействии на нее деструктивных факторов, в том числе при физической утрате некоторой установленной предельной численности комплексов или введении нового аппарата в группу (реконфигурирование системы).

КЛЮЧЕВЫЕ СЛОВА: автономная группа робототехнических комплексов; криптография; модулярная арифметика; помехоустойчивое кодирование в классах вычетов; целостность информации; информационная живучесть.

Для цитирования: Самойленко Д.В., Еремеев М.А., Финько О.А. Повышение информационной живучести группы робототехнических комплексов методами модулярной арифметики // Научные технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 62-77. doi 10.24411/2409-5419-2018-10042

На сегодняшний день для решения различных специальных задач широкое применение получают роботехнические комплексы, а получаемые преимущества предопределяют необходимость их группового применения. На примере группировки комплексов с беспилотными летательными аппаратами (БЛА) (рис. 1) осуществляется воздушная наблюдение, получение высокоточной геопроостранственной информации о местности, ретрансляция связи, выполняется топогеодезическое и навигационное обеспечение [1].

Как известно, целенаправленным процессом функционирования группировки БЛА является сбор информации об исследуемой предметной области и условно состоящий из трех этапов: этап перемещения комплексов БЛА в зону сбора информации, этап непосредственного сбора информации и этап «доставки» добытой информации получателю в условиях вероятного воздействия нарушителя. При этом мобильность группировки БЛА предполагает динамическую передачу данных между БЛА — на основании связанности радиосети в некоторый момент времени t . Как вариант, подразумевается, что специальной децентрализованной самоорганизующейся радиосети группировки БЛА (типа MANET, FANET) присуще свойство «равноправия», где каждый БЛА обеспечивает передачу данных для НПУ через другие БЛА (ретрансляторы) в сети.

В дополнение к накладываемым временным ограничениям сбора информации процесс доставки добытой информации является демаскирующим признаком БЛА, что допускает возможность осуществления преднамеренных помех. Нарушитель может осуществлять действия, направленные на задержку доставки сообщений, их повторную передачу,

внесение искажений заданной структуры с сохранением конфигурации информационных пакетов [2–5]. Также доставка добытой информации в наземный пункт управления (НПУ) может быть осуществлена непосредственно комплексами БЛА физически — с помощью бортовых запоминающих устройств. На рис. 2 представлена схема поэтапного осуществления сбора информации с доставкой в НПУ.

Потребность в надежном и своевременном представлении информации определяет конечную цель функционирования системы, а степень удовлетворения данных потребностей характеризуется качеством функционирования системы.

Основываясь на положениях [6] качество функционирования группировки БЛА может быть охарактеризовано некоторым комплексом (совокупностью) компонент $\chi = \{Int, R, T\}$, где Int — свойство результата, обуславливающего его пригодность по назначению, $R = \{\zeta_1, \zeta_2, \dots, \zeta_k\}$ — вектор затрат ресурсов (количество БЛА в группировке), $T = \{t, t+1, \dots, t+h\}$ — вектор временных затрат (время выполнения специального задания).

Учитывая различные условия эксплуатации системы, в том числе и агрессивные, достижение требуемого качества функционирования системы не может быть достигнуто без учета выполнения требований к безопасности информации. Так, одним из ключевых требований безопасности информации является контроль и обеспечение целостности информации (Int) на всех этапах жизненного цикла, которое взаимосвязано с требованиями к качеству функционирования системы (полнота и достоверность используемой информации). Представленная на рисунке 3 структура призвана пояснить взаимосвязь совокупности компонент, характе-

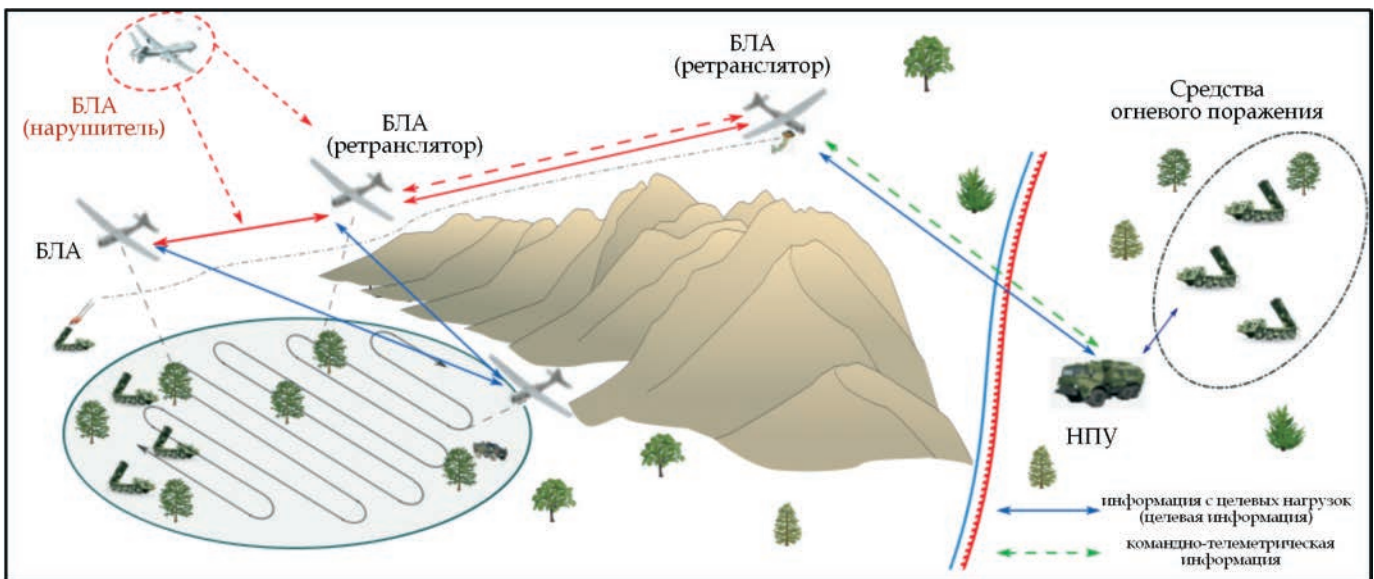


Рис. 1. Схема, поясняющая принцип функционирования (взаимодействия) группировки БЛА при решении специальных задач

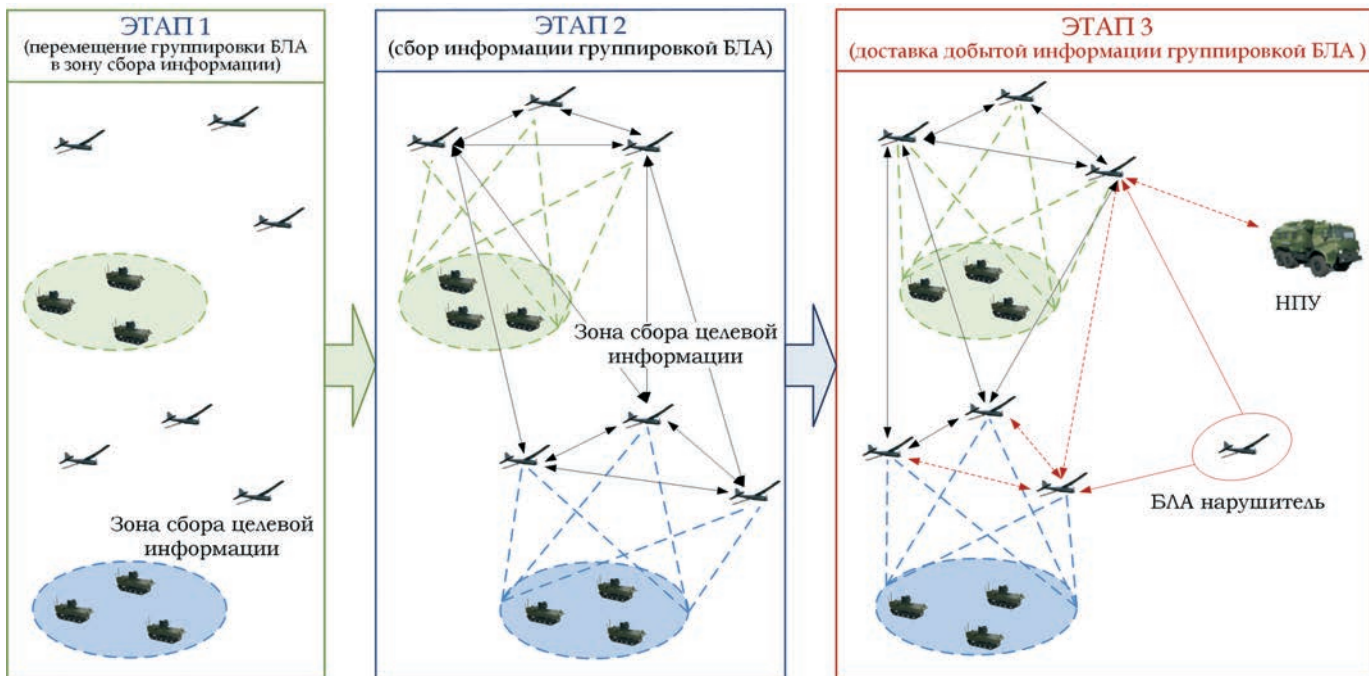


Рис. 2. Вариант структуры децентрализованной самоорганизующейся сети группировки БЛА, осуществляющей сбор и доставку добытой информации на НПУ (получателю)

ризующих качество функционирования группировки БЛА в условиях деструктивных воздействий нарушителя.

При этом в области защиты информации под целостностью информации принято понимать:

— состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право¹;

— состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право²;

— состояние ресурсов информационной системы, при котором их изменение осуществляется только преднамеренно субъектами, имеющими на него право, при этом сохраняются их состав, содержание и организация взаимодействия²;

— способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа³;

— обеспечение достоверности и полноты информации и методов ее обработки⁴.

Известно, что технологии реализующие требование целостности информации могут быть классифицированы на контролирующие и обеспечивающие.

Так, известные методы контроля целостности (криптографические и некриптографические) основаны на так называемых хэш-функциях⁵ и контролируют целостность информации на микроуровне (уровень отдельного БЛА) [7]. В тоже время, как ни парадоксально, но существующие решения, связанные с обеспечением целостности информации, находятся в плоскости не теории защиты информации, а положений теории отказоустойчивости, и достигаются, как правило, резервированием (репликацией), дублированием или просто избыточным кодированием [8–9]. Обобщенная схема существующих технологий контроля и обеспечения целостности информации представлена на рис. 4.

Отличительной особенностью приведенной терминологии и существующих решений контроля и обеспечения целостности информации является общий «пассивный» признак, сводящийся к установлению различий между информационными объектами, или осуществления репликации данных на различных узлах хранения и не отражающий регенеративного механизма восстановления первоначального состояния информации, соответствующего эталонному представлению и позволяющему использовать ее по дальнейшему назначению.

¹Р 50.1.053-2005 Рекомендации по стандартизации. «Информационные технологии. Основные термины и определения в области технической защиты информации».

²Р 50.1.056-2005 Рекомендации по стандартизации. «Техническая защита информации. Основные термины и определения».

³ГОСТ Р ИСО/МЭК 7498-2-99 «Информационная технология. Взаимос-

вязь открытых систем. Базовая эталонная модель. Ч.2. Архитектура защиты информации».

⁴ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»

⁵ГОСТ Р 34.11–2012, циклический избыточный код Cyclic Redundancy Code (CRC)

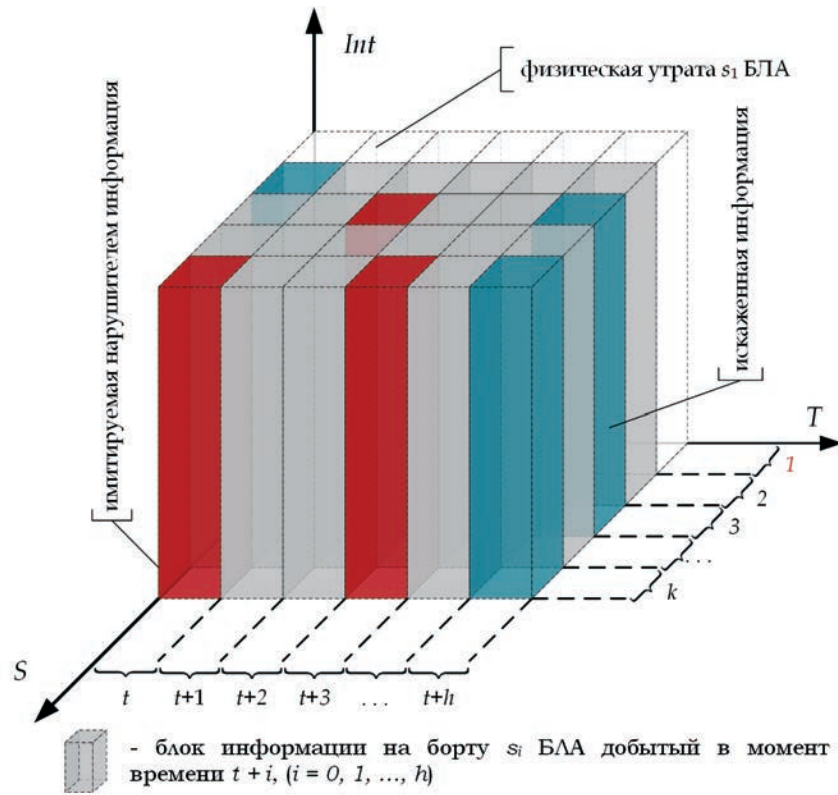


Рис. 3. Структура взаимосвязи совокупности компонент качественного функционирования группировки БЛА в условиях деструктивных воздействий нарушителя

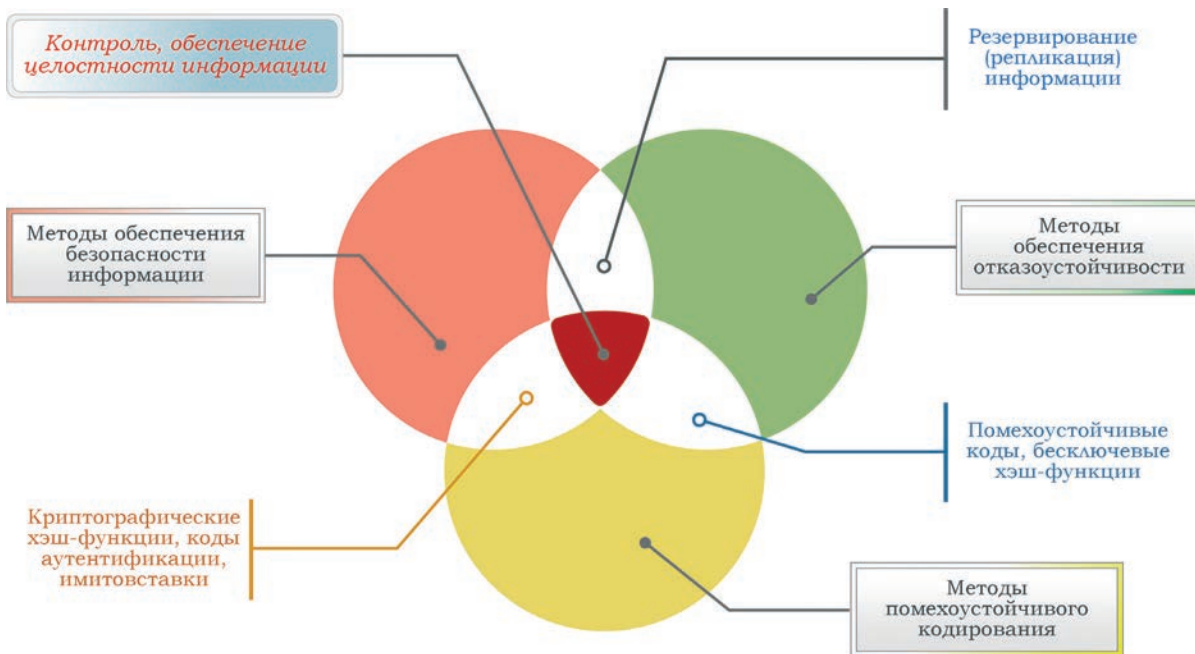


Рис. 4. Технологии контроля и обеспечения целостности информации

При этом применительно к группировке БЛА, взаимодействие которой образует распределенную децентрализованную сетевую информационно-вычислительную систему обработки информации (РСОИ) с непредсказуемо и динамически изменяющейся структурой, формирующую макроуровень, задача контроля и обеспечения целостности информации в явном виде является неопределенной. Вследствие чего для подсистемы защищенной обработки информации возникает необходимость в формировании «активного» свойства (защитной функции) преодоления последствий вредных факторов — *информационной живучести* Sr . При этом информационной живучестью подсистемы защищенной обработки информации РСОИ будем понимать ее способность инициировать регенеративный процесс восстановления данных (максимальной длительности) при деструктивных воздействиях злоумышленника.

Для чего условимся РСОИ интерпретировать как сеть, состоящую из k кластеризованных по определенным признакам (минимальному расстоянию среди доступных узлов, допустимой информационной нагрузке, равномерному распределению энергетических характеристик) узлов $S = \{s_1, s_2, \dots, s_k\}$ обработки информации, которые помимо функции хранения могут выполнять функцию ретрансляции данных, например, используются оптические линии связи [10]. Кластеризованное множество узлов хранения S представлено в виде графа (рис. 5) $G(S, E)$. Ребра $(s_i, s_j) \in E$ являются смежными, когда узлы хранения s_i и s_j функционируют в пределах сети и отсутствуют препятствия, обусловленные воздействиями помех.

Деструктивные воздействия нарушителя на узлы хранения связаны как с их физической утратой (разрушением), так и со способностью нарушителя осуществлять «алгебраические манипуляции», заключающиеся в изменении содержимого узлов хранения без непосредственно

го их чтения [11]. В том или ином случае все это ведет к нарушению целостности информации и снижению качества функционирования всей группировки БЛА в целом.

В предлагаемом методе совокупность запоминающих устройств, размещенных на борту различных, но объединенных единой целью функционирования БЛА, рассматривается как единая система запоминающих устройств с подсистемой криптокодowego преобразования информации (формирование «криптокодowych» конструкций) [12–13], предусматривающая введение избыточности в сохраняемую информацию.

Синтез криптокодowych конструкций осуществляется следующим образом. Пусть каждый исходный узел в некоторый момент времени t формирует пакет данных, представленный как

$$M(z) = v_0 + v_1z + \dots + v_{p-1}z^{p-1} \text{ над } GF(2),$$

где $\deg \Omega_i(z) = p-1$ — степень полинома $\Omega_i(z)$ над $GF(2)$. С целью обеспечения необходимого уровня конфиденциальности информации сформированный пакет данных $M(z)$ узла s_i хранения подлежит процедуре блочного шифрования

$$\Omega_i(z) \rightarrow \text{Enc}(\kappa_{e,i}(z), M_i(z)),$$

где $\kappa_{e,i}(z)$ соответствующий ключ шифрования [14], $M(z) = M_1(z) || M_2(z) || \dots || M_k(z)$ блоки данных фиксированной длины (ГОСТ Р 34.12-2015 с блоками 64 и 128 бит соответственно), а «||» — символ конкатенации.

Далее, узлы s_j хранения (БЛА) на основании связности радиосети в момент времени t осуществляют передачу блоков криптограмм другим (доступным) узлам хранения, т.е. узел s_j хранения (принимающий БЛА) принимает и сохраняет совокупность блоков криптограмм $\Omega_i(z)$ ($i = 1, 2, \dots, k$) от других узлов хранения. В полиномиальной модулярной

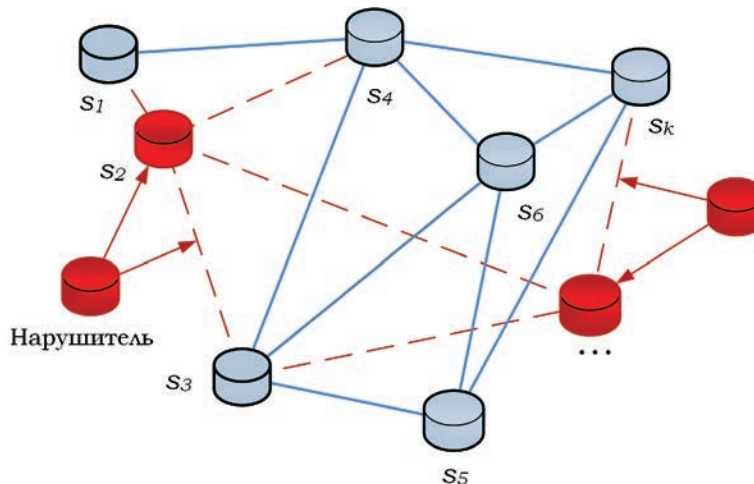


Рис. 5. Структура децентрализованной масштабируемой РСОИ с кластеризованным множеством узлов хранения

арифметике совокупность информационных блоков криптограмм $\Omega_i(z)$ ($i = 1, 2, \dots, k$) узла s_i хранения может быть представлена в виде наименьших неотрицательных вычетов по основаниям (полиномам) $m_i(z)$, где $\gcd(m_i(z), m_j(z)) = 1$, $i \neq j$; $i, j = 1, 2, \dots, k$; $\deg \Omega_i(z) < \deg m_i(z)$. Далее, в подсистеме кодирования информации узла s_i хранения по дополнительно введенным неприводимым r избыточным основаниям (полиномам) $m_j(z)$ ($j = k+1, k+2, \dots, n$), удовлетворяющим условию $\deg m_1(z), \dots, \deg m_k(z) \leq \dots \leq \deg m_n(z)$, в соответствии с выражением:

$$\omega_j(z) \equiv \langle a(z) \rangle_{m_j(z)} = \sum_{i=1}^k \langle k_i(z) \Omega_i(z) \rangle_{m_i(z)} \langle \mu_i(z) \rangle_{m_j(z)}$$

где $\langle a(z) \rangle_{m_j(z)}$ — операция приведения $a(z)$ по модулю $m_j(z)$, $\mu_i(z) = m_1(z)m_2(z) \dots m_{i-1}(z)m_{i+1}(z) \dots m_k(z)$, $\langle k_i(z)\mu_i(z) \rangle_{m_i(z)} = 1$, вырабатываются избыточные полиномиальные вычеты $\omega_j(z)$ ($j = k+1, k+2, \dots, n$).

При этом для обеспечения «математического» разрыва процедуры (непрерывной функции) формирования избыточных элементов криптокодовых конструкций, а также исключения подмены (изменения) информации по оптимальной стратегии имитации злоумышленника, элементы криптокодовых конструкций должны распределяться случайным образом. Для этого, сформированные избыточные полиномиальные вычеты $\omega_j(z)$ ($j = k+1, k+2, \dots, n$) подвер-

гаются процедуре зашифрования: $\vartheta_i(z) \rightarrow \text{Enc}(\kappa_{e,i}, \omega_i(z))$, где $\kappa_{e,i}(z)$ ($i = k+1, k+2, \dots, n$; $g-1, g-2, \dots, 0$), $n = k+r$.

Операция зашифрования избыточных полиномиальных вычетов не позволяет противнику на основании перехваченной совокупности блоков криптограмм («информационной» составляющей) сформировать проверочную последовательность для преодоления механизмов защиты и навязывания ложной информации.

Полученная совокупность информационных и избыточных блоков криптограмм образует «криптокодовые» конструкции, отождествляемые как кодовый вектор расширенного модулярного полиномиального кода (МПК): $\{\Omega_1(z), \dots, \Omega_k(z), \vartheta_{k+1}(z), \dots, \vartheta_n(z)\}_{\text{МПК}}$.

Схема, поясняющая принцип формирования совокупности информационных и избыточных блоков криптограмм в узле s_k хранения (на борту принимающего БЛА) представлена на рис. 6.

После вычисления избыточных элементов МПК принятая совокупность информационных блоков криптограмм от других узлов хранения удаляется. Вычисленные избыточные блоки криптограмм $\vartheta_{k+1}(z)$, $\vartheta_{k+2}(z)$, $\vartheta_n(z)$ поступают в подсистему хранения информации. Структура формируемых данных в памяти узла s_i хранения (памяти БЛА) представлена на рис. 7.

Отсутствие фиксированной инфраструктуры и централизованного управления, обусловленное динамически самоорганизующейся топологией построения сети радио-

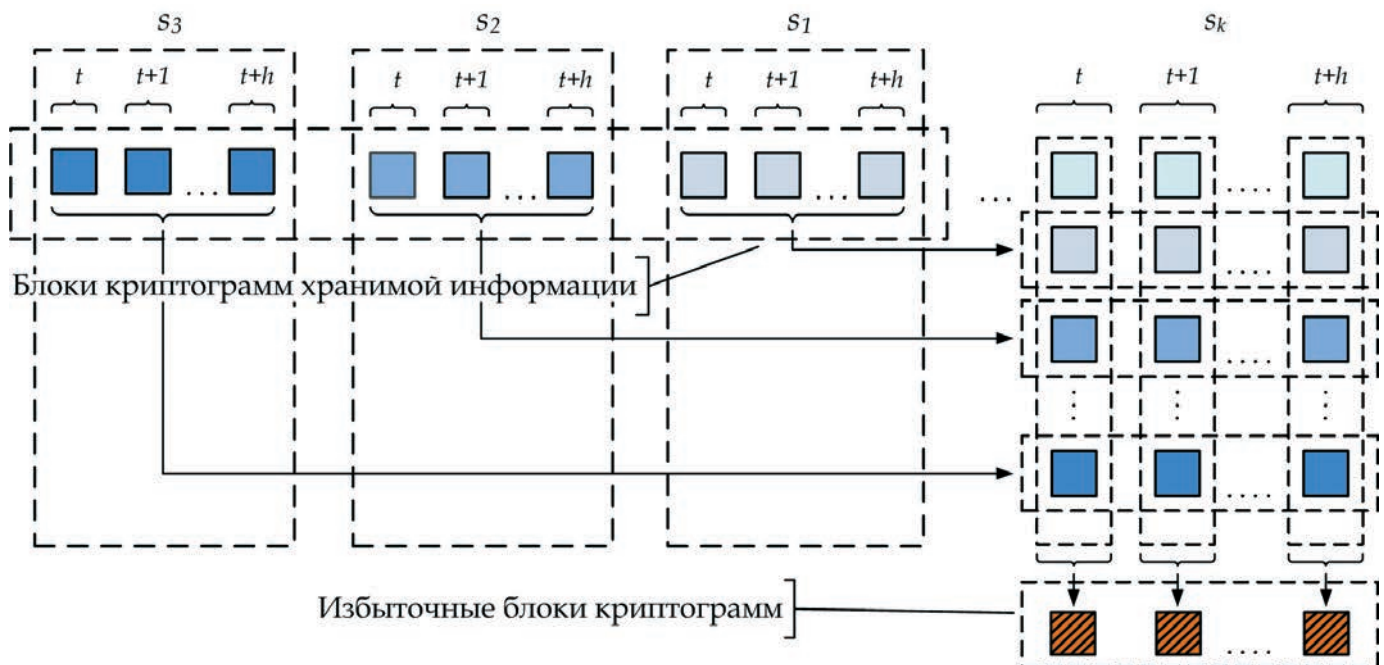
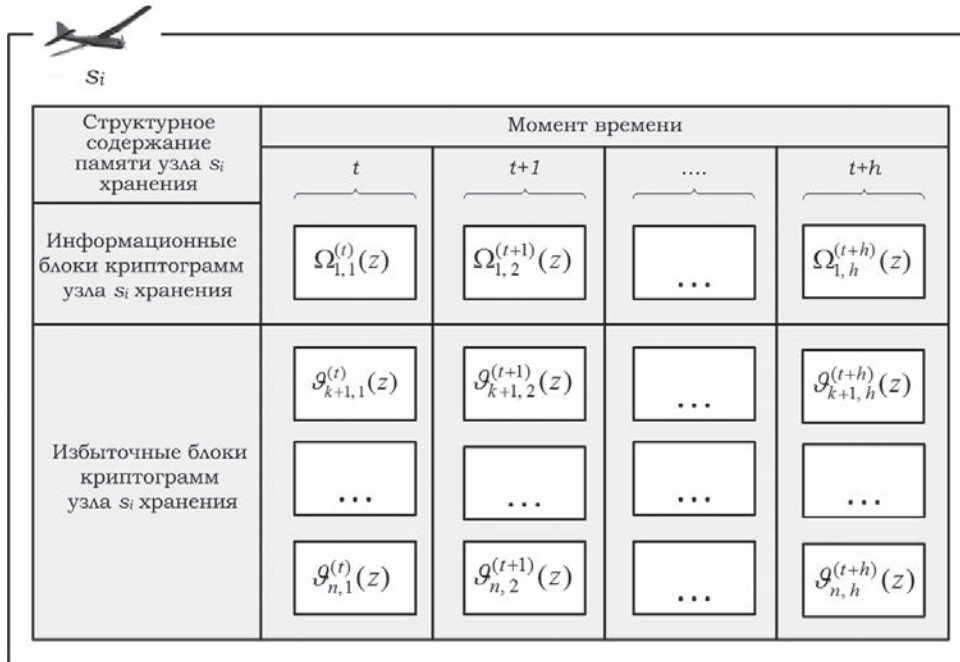


Рис. 6. Схема, поясняющая принцип формирования информационных и избыточных блоков криптограмм узла s_k хранения (принимающего БЛА)



S_i				
Структурное содержание памяти узла S_i хранения	Момент времени			
	t	$t+1$...	$t+h$
Информационные блоки криптограмм узла S_i хранения	$\Omega_{1,1}^{(t)}(z)$	$\Omega_{1,2}^{(t+1)}(z)$...	$\Omega_{1,h}^{(t+h)}(z)$
Избыточные блоки криптограмм узла S_i хранения	$\mathcal{G}_{k+1,1}^{(t)}(z)$	$\mathcal{G}_{k+1,2}^{(t+1)}(z)$...	$\mathcal{G}_{k+1,h}^{(t+h)}(z)$

	$\mathcal{G}_{n,1}^{(t)}(z)$	$\mathcal{G}_{n,2}^{(t+1)}(z)$...	$\mathcal{G}_{n,h}^{(t+h)}(z)$

Рис. 7. Структура формируемых данных в памяти узла S_i хранения (памяти БЛА)

связи, гомогенностью РСОИ, позволяет совокупность запоминающих устройств (памяти), размещенных в узлах хранения (БЛА), рассматривать как единую систему памяти, а ее содержимое представить в виде информационной матрицы:

$$L = \begin{pmatrix} \Omega_{1,1}^{(t)}(z) & \Omega_{1,2}^{(t+1)}(z) & \Omega_{1,3}^{(t+2)}(z) & \dots & \Omega_{1,h}^{(t+h)}(z) \\ \Omega_{2,1}^{(t)}(z) & \Omega_{2,2}^{(t+1)}(z) & \Omega_{2,3}^{(t+2)}(z) & \dots & \Omega_{2,h}^{(t+h)}(z) \\ \Omega_{3,1}^{(t)}(z) & \Omega_{3,2}^{(t+1)}(z) & \Omega_{3,3}^{(t+2)}(z) & \dots & \Omega_{3,h}^{(t+h)}(z) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \Omega_{k,1}^{(t)}(z) & \Omega_{k,2}^{(t+1)}(z) & \Omega_{k,3}^{(t+2)}(z) & \dots & \Omega_{k,h}^{(t+h)}(z) \end{pmatrix}.$$

С учетом вычисленных избыточных блоков криптограмм узла S_i хранения информационная матрица L примет «расширенный» вид (таб. 1):

При этом на приемной стороне (НПУ) прежде всего последовательность избыточных блоков криптограмм $\mathcal{G}_{k+1}(z), \mathcal{G}_{k+2}(z), \mathcal{G}_n(z)$ подвергается процедуре расшифрования $\omega_i(z) \rightarrow D_i(\kappa_{d,i}, \mathcal{G}_i(z))$, где $\kappa_{d,i}$ — ключи расшифрования ($i = k+1, k+2, \dots, n; j = g-1, g-2, \dots, 0$).

В таком случае целостность информации РСОИ выразим через систему функций от переменных (информационных блоков криптограмм и избыточных блоков данных) расширенной матрицы L :

$$\begin{cases} f_t(\Omega_{1,1}^{(t)}(z), \Omega_{2,1}^{(t)}(z), \dots, \Omega_{k,1}^{(t)}(z), \omega_{k+1,1}^{(t)}(z), \dots, \omega_{n,1}^{(t)}(z)) = a_t(z), \\ f_{t+1}(\Omega_{1,2}^{(t+1)}(z), \Omega_{2,2}^{(t+1)}(z), \dots, \Omega_{k,2}^{(t+1)}(z), \omega_{k+1,2}^{(t+1)}(z), \dots, \omega_{n,2}^{(t+1)}(z)) = a_{t+1}(z), \\ f_{t+2}(\Omega_{1,3}^{(t+2)}(z), \Omega_{2,3}^{(t+2)}(z), \dots, \Omega_{k,3}^{(t+2)}(z), \omega_{k+1,3}^{(t+2)}(z), \dots, \omega_{n,3}^{(t+2)}(z)) = a_{t+2}(z), \\ \dots \\ f_{t+h}(\Omega_{1,h}^{(t+h)}(z), \Omega_{2,h}^{(t+h)}(z), \dots, \Omega_{k,h}^{(t+h)}(z), \omega_{k+1,h}^{(t+h)}(z), \dots, \omega_{n,h}^{(t+h)}(z)) = a_{t+h}(z). \end{cases}$$

Значение полиномов $a_b(z)$ находятся из выражения:

$$a_b(z) = \left\langle \sum_{i=1}^k \left\langle k_{i,j}^{(b)}(z) \Omega_{i,j}^{(b)}(z) \right\rangle_{m_i(z)} \mu_i(z) + \sum_{i=k+1}^n \left\langle k_{i,j}^{(b)}(z) \omega_{i,j}^{(b)}(z) \right\rangle_{m_i(z)} \mu_i(z) \right\rangle_{P(z)},$$

где $P(z) = \prod_{i=1}^k m_i(z)$, ($b = t, t+1, \dots, t+h; j = 1, 2, \dots, h$).

Элементы кодового слова

$$\Omega_{1,j}^{(b)*}(z), \dots, \Omega_{k,j}^{(b)*}(z), \dots, \omega_{k+1,j}^{(b)*}(z), \dots, \omega_{n,j}^{(b)*}(z)$$

из совокупности запоминающих устройств и, соответственно, блоки открытых данных $M_1^*(z), M_2^*(z), \dots, M_k^*(z)$ могут содержать искажения (ошибки). Критерием отсутствия обнаруживаемых ошибок является выполнение условия

$$a_i^*(z) \in F[z] / (P(z)).$$

Таблица 1

Расширенный вид информационной матрицы L

Блоки криптограмм, данных	$\underbrace{\quad}_t$	$\underbrace{\quad}_{t+1}$	$\underbrace{\quad}_{t+2}$...	$\underbrace{\quad}_{t+h}$
Информационные блоки криптограмм узла s_i хранения	$\left \begin{matrix} (t) \\ 1,1 \end{matrix} (z) \right.$	$\Omega_{1,2}^{(t+1)}(z)$	$\Omega_{1,3}^{(t+2)}(z)$...	$\Omega_{1,h}^{(t+h)}(z)$
Информационные блоки криптограмм других узлов хранения	$\left \begin{matrix} (t) \\ 2,1 \end{matrix} (z) \right.$	$\Omega_{2,2}^{(t+1)}(z)$	$\Omega_{2,3}^{(t+2)}(z)$...	$\Omega_{2,h}^{(t+h)}(z)$
	$\left \begin{matrix} (t) \\ 3,1 \end{matrix} (z) \right.$	$\Omega_{3,2}^{(t+1)}(z)$	$\Omega_{3,3}^{(t+2)}(z)$...	$\Omega_{3,h}^{(t+h)}(z)$
	\vdots	\vdots	\vdots	\vdots	\vdots
	$\left \begin{matrix} (t) \\ k,1 \end{matrix} (z) \right.$	$\Omega_{k,2}^{(t+1)}(z)$	$\Omega_{k,3}^{(t+2)}(z)$...	$\Omega_{k,h}^{(t+h)}(z)$
Избыточные блоки криптограмм узла s_i хранения	$\mathfrak{G}_{k+1,1}^{(t)}(z)$	$\mathfrak{G}_{k+1,2}^{(t+1)}(z)$	$\mathfrak{G}_{k+1,3}^{(t+2)}(z)$...	$\mathfrak{G}_{k+1,h}^{(t+h)}(z)$
	\vdots	\vdots	\vdots	\vdots	\vdots
	$\mathfrak{G}_{n,1}^{(t)}(z)$	$\mathfrak{G}_{n,2}^{(t+1)}(z)$	$\mathfrak{G}_{n,3}^{(t+2)}(z)$...	$\mathfrak{G}_{n,h}^{(t+h)}(z)$

Критерием существования обнаруживаемых ошибок — выполнение условия [15–16]:

$$a_i^*(z) \notin F[z]/(P(z)),$$

где символ «*» указывает на наличие возможных искажений в кодовом слове.

В случае физической утраты некоторой предусмотренной предельной численности узлов хранения совокупность запоминающих устройств, представленной расширенной матрицы L примет вид (табл. 2):

С учетом заранее введенной избыточности в сохраняемую информацию физическая утрата узла S_i хранения не приводит к полной или частичной потере информации

Таблица 2

Расширенный вид информационной матрицы L при физической утрате запоминающих устройств

Блоки криптограмм, данных	$\underbrace{\quad}_t$	$\underbrace{\quad}_{t+1}$	$\underbrace{\quad}_{t+2}$...	$\underbrace{\quad}_{t+h}$
Информационные блоки криптограмм узла s_i хранения	$\left \begin{matrix} (t) \\ 1,1 \end{matrix} (z) \right.$	$\Omega_{1,2}^{(t+1)}(z)$	$\Omega_{1,3}^{(t+2)}(z)$...	$\Omega_{1,h}^{(t+h)}(z)$
Информационные блоки криптограмм других узлов хранения	$\left \begin{matrix} (t) \\ 2,1 \end{matrix} (z) \right.$	$\Omega_{2,2}^{(t+1)}(z)$	$\Omega_{2,3}^{(t+2)}(z)$...	$\Omega_{2,h}^{(t+h)}(z)$
Утраченные информационные блоки криптограмм узла хранения	0	0	0	...	0
	\vdots	\vdots	\vdots	\vdots	\vdots
Информационные блоки криптограмм других узлов хранения	$\left \begin{matrix} (t) \\ k,1 \end{matrix} (z) \right.$	$\Omega_{k,2}^{(t+1)}(z)$	$\Omega_{k,3}^{(t+2)}(z)$...	$\Omega_{k,h}^{(t+h)}(z)$
Избыточные блоки криптограмм узла s_i хранения	$\mathfrak{G}_{k+1,1}^{(t)}(z)$	$\mathfrak{G}_{k+1,2}^{(t+1)}(z)$	$\mathfrak{G}_{k+1,3}^{(t+2)}(z)$...	$\mathfrak{G}_{k+1,h}^{(t+h)}(z)$
	\vdots	\vdots	\vdots	\vdots	\vdots
	$\mathfrak{G}_{n,1}^{(t)}(z)$	$\mathfrak{G}_{n,2}^{(t+1)}(z)$	$\mathfrak{G}_{n,3}^{(t+2)}(z)$...	$\mathfrak{G}_{n,h}^{(t+h)}(z)$

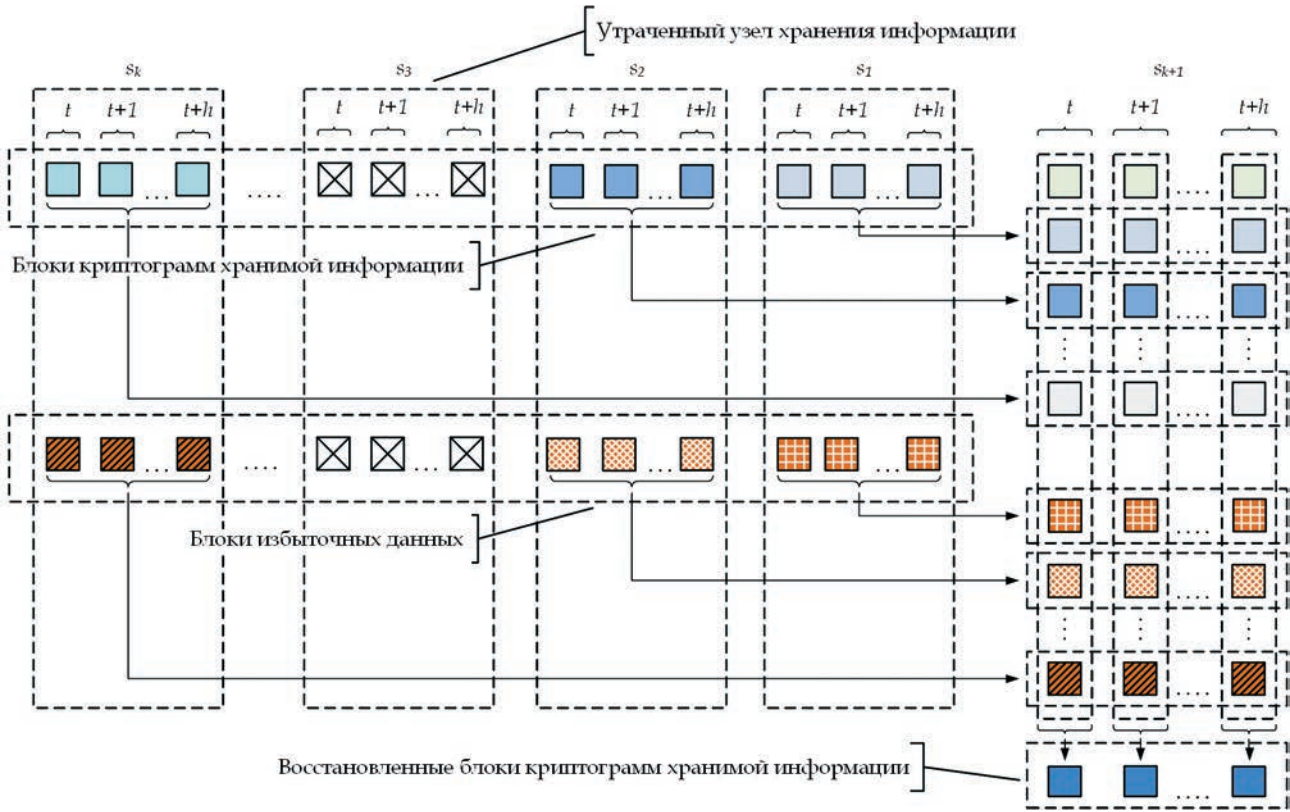


Рис. 8. Схема, поясняющая принцип восстановления информационных блоков криптограмм с утраченного узла \$s_3\$ хранения

и позволяет инициировать регенеративный процесс восстановления потерянной или искаженной информации путем вычисления наименьших вычетов или любым другим известным методом декодирования расширенных МПК:

$$\left\{ \begin{array}{l} \Omega_{1,1}^{(t)**}(z) \equiv \langle a_t^*(z) \rangle_{m_1(z)}, \\ \Omega_{2,1}^{(t)**}(z) \equiv \langle a_t^*(z) \rangle_{m_2(z)}, \\ \dots \\ \Omega_{k,1}^{(t)**}(z) \equiv \langle a_t^*(z) \rangle_{m_k(z)}, \\ \Omega_{1,2}^{(t+1)**}(z) \equiv \langle a_t^*(z) \rangle_{m_1(z)}, \\ \Omega_{2,2}^{(t+1)**}(z) \equiv \langle a_t^*(z) \rangle_{m_2(z)}, \\ \dots \\ \Omega_{k,2}^{(t+1)**}(z) \equiv \langle a_t^*(z) \rangle_{m_k(z)}, \\ \dots \\ \Omega_{1,h}^{(t+h)**}(z) \equiv \langle a_t^*(z) \rangle_{m_1(z)}, \\ \Omega_{2,h}^{(t+h)**}(z) \equiv \langle a_t^*(z) \rangle_{m_2(z)}, \\ \dots \\ \Omega_{k,h}^{(t+h)**}(z) \equiv \langle a_t^*(z) \rangle_{m_k(z)} \quad \square \end{array} \right.$$

где символы «**» указывают на вероятностный характер восстановления.

Схема, поясняющая принцип восстановления информационных блоков криптограмм утраченного узла \$s_3\$ хранения при введении нового узла хранения \$s_{k+1}\$ и распределения добытой информации представлена на рис. 8. При этом непосредственно перед выполнением указанных преобразований по восстановлению утраченной информации осуществляется расшифрование избыточных блоков криптограмм узлов хранения, восстановление информации с утраченного узла хранения, ее перераспределение и последующее зашифрование избыточных блоков данных, включая вновь вычисленные.

На основании вышеизложенных положений сформулируем утверждение. Утерянные исходные данные деградирующего узла \$s_i\$ хранения РСОИ могут быть восстановлены, если количество утерянных элементов кодовой комбинации МПК, формируемой функционирующими узлами хранения, не превышает предельной численности \$q = d_{\min} - 1\$. Тогда вероятность успешного восстановления исходных данных может быть выражена как:

$$P_{rec}(q) = 1 - \sum_{q=d_{\min}}^n \binom{n}{q} p_m^q (1 - p_m)^{n-q}$$

где p_m — вероятность того, что кодовая комбинация МПК имеет случайные ошибки, $\binom{n}{q} = \frac{n!}{(n-q)!q!}$ — сочетание из n элементов по q .

Пусть $P(A)$ — вероятность наступления случайного события A , заключающегося в невозможности восстановления исходных данных, обусловленных потерей s_i узла хранения, а $P(H_q)$ — вероятность наступления событий (гипотез) H_q заключающихся в том, что q узлов считаются потерянными (отказавшими). Вероятности $P(H_q)$ соответствует выражение:

$$P(H_q) = \binom{n}{q} p_m^q (1-p_m)^{n-q}.$$

Тогда, основываясь на корректирующих способностях МПК, потерянные (искаженные) данные могут быть успешно восстановлены, если k из n элементов формируемой кодовой комбинации МПК являются доступными. В противном случае исходные данные в кодовой комбинации МПК не могут быть восстановлены. Условная вероятность события A , при гипотезах $P(A/H_q) = 1$, если $q \in \{d_{\min}, n\}$ и $P(A/H_q) = 0$, если $q \in \{0, d_{\min} - 1\}$. Тогда получим:

$$P(A) = \sum_{q=0}^n P(H_q) P(A/H_q). \quad (1)$$

Представим выражение (1) в виде двух слагаемых:

$$\begin{aligned} P(A) &= \sum_{q=0}^{d_{\min}-1} P(H_q) P(A/H_q) + \sum_{q=d_{\min}}^n P(H_q) P(A/H_q) = \\ &= \sum_{q=d_{\min}}^n P(H_q) P(A/H_q) = \sum_{q=d_{\min}}^n \binom{n}{q} p_m^q (1-p_m)^{n-q}. \end{aligned}$$

Таким образом, вероятность успешного восстановления данных в зависимости от случайной потери s_i узла хранения:

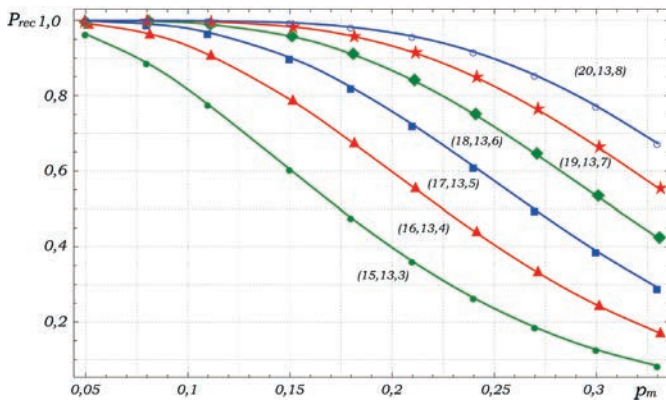


Рис. 9. Зависимости вероятностей успешного восстановления данных от вероятности p_m потери узла s_i хранения

$$P_{rec} = 1 - P(A) = 1 - \sum_{q=d_{\min}}^n \binom{n}{q} p_m^q (1-p_m)^{n-q}.$$

При этом вероятности P_{rec} при больших значениях n и $p_m < \theta = \frac{q}{n}$ соответствует неравенство [с.62, 17]:

$$P_{rec} > 1 - 2^{-q \left((\theta+q^{-1}) \log_2 \frac{\theta+q^{-1}}{p_m} + (1-\theta-q^{-1}) \log_2 \frac{1-\theta-q^{-1}}{1-p_m} \right)}$$

На рис. 9 представлены расчетные данные зависимости вероятностей успешного восстановления данных от вероятности потери узла s_i хранения для МПК формируемой различной конфигурацией РСОИ и рис. 10 расчетные данные зависимости вероятностей успешного восстановления данных от минимального кодового расстояния d_{\min} МПК.

Вместе с тем, очевидно, что в дополнение к деструктивным воздействиям нарушителя, влекущим физическую утрату некоторых узлов s_i хранения, решение задачи обеспечения целостности информации для РСОИ (макроуровня) ограничено имеющимся предельным объемом единой системы памяти V , формируемым группировкой БЛА:

$$V \leq \sum_{i=1}^k v_i,$$

где v_i — объем информации, включающий информационный и избыточный фрагменты, выработанные в момент времени t и хранящиеся на каждом узле s_i хранения.

При этом хорошо известно [18], что оптимальное распределение объема памяти среди распределенных узлов хранения максимизирует вероятность успешного восстановления данных, в том числе утраченных.

Несмотря ограничения совокупного объема единой системы памяти V , необходимо подчеркнуть, что подси-

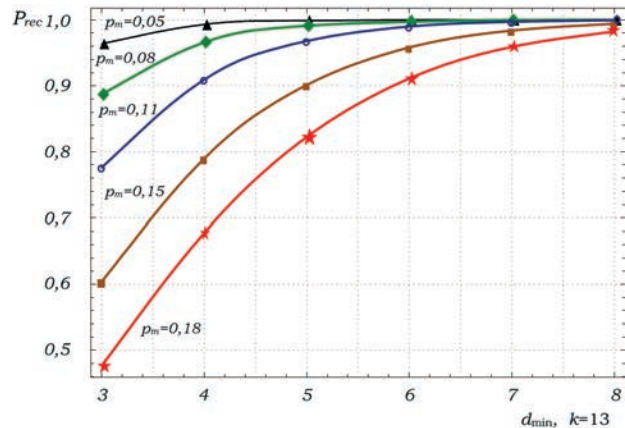


Рис. 10. Зависимости вероятностей успешного восстановления данных от минимального кодового расстояния d_{\min}

система криптокодированной информации осуществляет ее обработку и последующее распределение, позволяет НПУ (получателю) для успешного восстановления информации осуществить доступ к некоторому подмножеству $Y \cdot (|Y| = \tau)$, принадлежащему множеству S узлов s_i хранения (рис. 11), формирующемуся случайным образом из совокупности возможных $\binom{k}{\tau}$ подмножеств.

Что касается параметра τ , то с учетом корректирующих способностей МПК может быть получен с помощью выражения:

$$\tau = k - \left\lfloor \frac{q}{l} \right\rfloor,$$

где $\lfloor N \rfloor$ — наибольшее целое число, не превосходящее N ; l — количество фрагментов (информационных и избыточных), выработанных на узле s_i хранения в момент времени t .

Более того, успешное восстановление информации в рамках РСОИ в условиях деструктивных воздействий нарушителя, влекущих физическую утрату некоторых узлов s_i хранения обеспечивается в случае гарантированного доступа НПУ к τ узлам s_i хранения, совокупный объем информации в которых равен или превышает значения $|S|$ т.е.

$$\sum_{i \in Y} v_i \geq |S| \quad (2)$$

Тогда, по аналогии с [18–20] вероятность успешного восстановления информации для таких условий функционирования, обусловленных в итоге случайным (равновероятным) доступом НПУ к подмножеству Y может быть выражена:

$$P_{rec} = \sum_{\varsigma} \binom{k}{\tau}^{-1} I_{|S|},$$

при условии, что $\varsigma = \frac{g!}{(g-\tau)!}$,

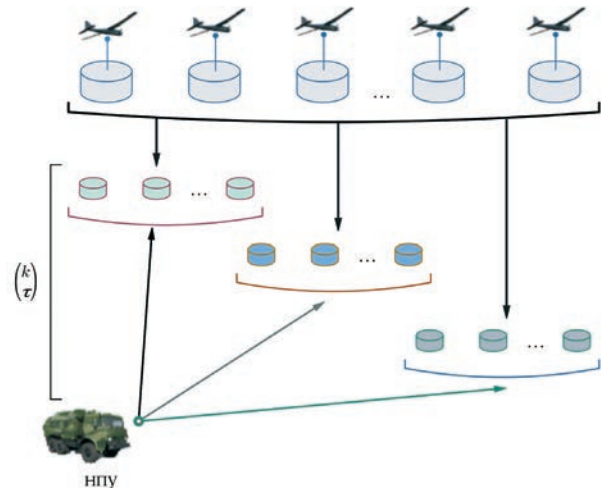


Рис. 11. Схема доступа НПУ к некоторому подмножеству Y множества S узлов s_i хранения

где g — количество узлов s_i хранения, для которых $v_i \neq 0$;

$$I_{|S|} = I_{|S|} \left(\sum_{i \in Y} v_i \right) = \begin{cases} 1, & \sum_{i \in Y} v_i \geq |S|; \\ 0, & \sum_{i \in Y} v_i \leq |S| \end{cases} \quad \text{— индикаторная функция.}$$

На рис. 12 (а, б) представлены расчетные данные зависимости вероятностей успешного восстановления информации от распределения совокупного объема единой системы памяти V для следующих параметров системы: а) $n = 10, k = 5, d_{min} = 6, l = 2, \tau = 3$; б) $n = 14, k = 7, d_{min} = 8, l = 2, \tau = 4$.

На рис. 13 (а, б) представлены аналогичные зависимости для следующих параметров системы: а) $n = 20, k = 10, d_{min} = 11, l = 2, \tau = 5$; б) $n = 30, k = 10, d_{min} = 21, l = 3, \tau = 4$.

Как видно из представленных зависимостей наиболее оптимальным является симметричное распределение совокупного объема памяти V среди узлов s_i хранения, при условии гарантированного доступа к некоторому фиксированному подмножеству Y , совокупный объем информации, в которых удовлетворяет условию (2).

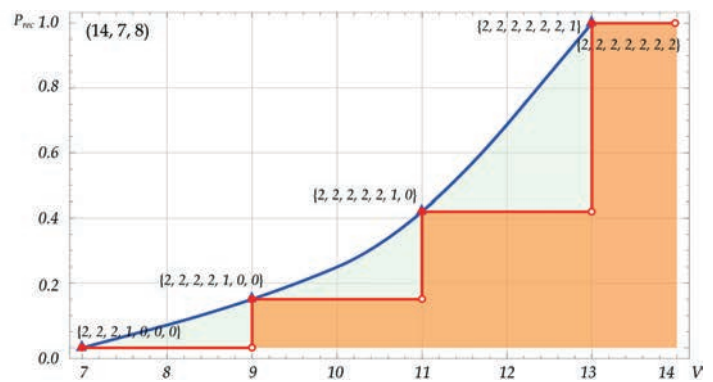
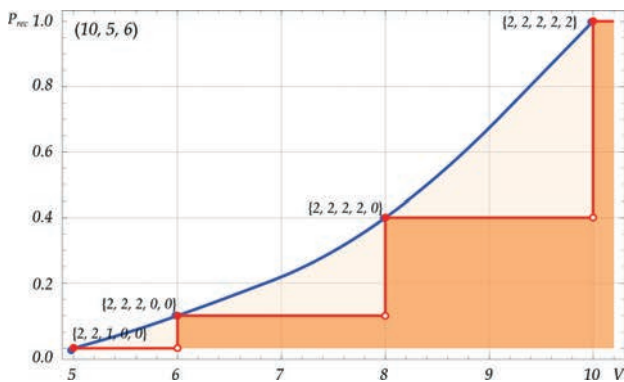


Рис. 12. Зависимости вероятностей успешного восстановления информации от распределения совокупного объема единой системы памяти V

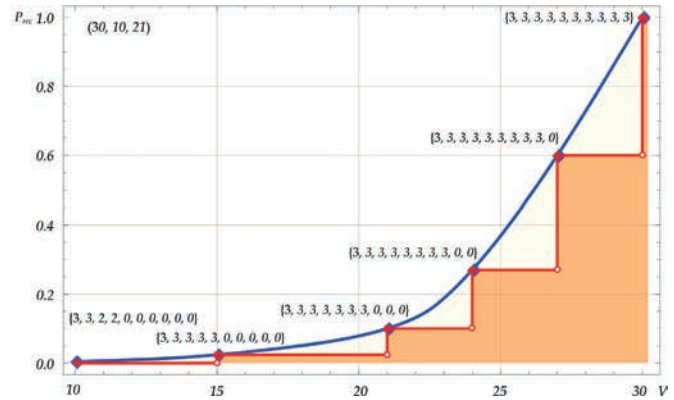
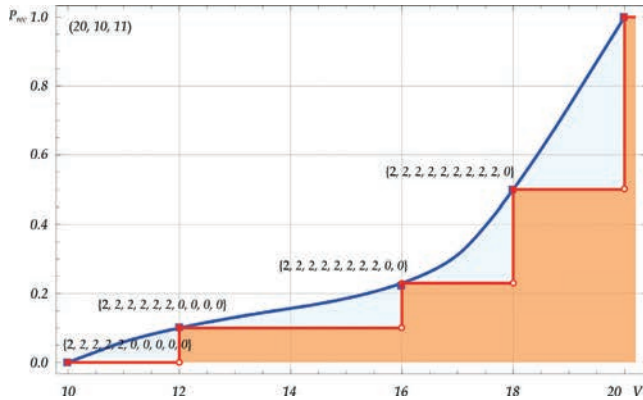


Рис. 13. Зависимости вероятностей успешного восстановления информации от распределения совокупного объема единой системы памяти V

Вместе с тем в условиях деструктивных воздействий злоумышленника группировка комплексов БЛА должна обладать способностью (свойством) мобилизации всего активного ресурса на решение поставленной задачи. Иными словами группировка комплексов БЛА должна обладать реконфигурационными возможностями, позволяющими осуществлять изменение структуры, с целью минимизации нанесенного ущерба, обусловленного, например, физической утратой (отказом) некоторых узлов s_i хранения.

Аналитическое описание функции реконфигурации группировки комплексов БЛА основывается на положениях, изложенных в [21].

В качестве примера, рассмотрим группировку состоящую из одинаковых (однотипных) s_i ($i = 1, 2, \dots, k$) БЛА. При этом БЛА могут различаться некоторым весом (например, первоочередностью решаемой задачи отдельным БЛА, исследуемым районом местности) x_i ($i = 1, 2, \dots, k$), определяющим их «местоположение» в группировке, и текущим состоянием работоспособности ρ_i ($i = 1, 2, \dots, k$). Состояние s_i БЛА есть функция времени, тогда введем соответствующее обозначение $\rho_i(t)$ — состояние i -го БЛА группировки в момент времени t . При этом

$$\rho_i(t) = \begin{cases} 1, & \text{если } s_i \text{ БЛА является работоспособным;} \\ 0, & \text{если } s_i \text{ БЛА в противном случае.} \end{cases}$$

Допустим, группировка БЛА состоит из равновесных БЛА, при этом исходный ресурс определяется следующим выражением:

$$B = \sum_{i=1}^k \eta_i.$$

В случае физической утраты (неработоспособности) s_j БЛА он заменяется работоспособным s_i БЛА ($i \neq j$) из

исходного ресурса B . По аналогии с [21] обозначим процедуру замены s_j БЛА на s_i БЛА как $s_i \rightarrow s_j$. Тогда процедура замены s_j БЛА через ресурс группировки БЛА в аналитическом представлении может быть выражена в виде:

$$\sum_{\substack{i=1, \\ i \neq j}}^k \eta_i \rightarrow \eta_j \tag{3}$$

Функция замены s_j БЛА на s_i БЛА $f(s_i \rightarrow s_j) = \bar{\rho}_j(t) \rho_i(t)$ с учетом (3) примет вид:

$$f \left(\sum_{\substack{i=1, \\ i \neq j}}^k \eta_i \rightarrow \eta_j \right) = \bar{\rho}_j(t) \prod_{\substack{i=1, \\ i \neq j}}^k \rho_i$$

где $\bar{\bullet}$ — символ логического отрицания, при этом полученное выражение позволяет получить обобщенную схему группировки комплексов БЛА с реконфигурацией равновесных БЛА, представленную на рис. 14.

Теперь, допустим, что группировка БЛА состоит из неравновесных БЛА характеризующихся весом x_i . При этом вполне очевидны ограничения, накладываемые на функцию замены и направленные в первую очередь на снижение ущерба и допускающие возможность замены $s_i \rightarrow s_j$ при условии $x_i < x_j$. Тогда с учетом ранжирования БЛА в группировке $\sum_{i=l'+1}^k \eta_i \rightarrow \eta_j$, функция замены примет вид:

$$f \left(\sum_{i=j+1}^k \eta_i \rightarrow \eta_j \right) = \bar{\rho}_j \prod_{i=j+1}^k \rho_i.$$

Исходя, из этого выражения на рис. 15 представлена обобщенная схема группировки комплексов БЛА с рекон-

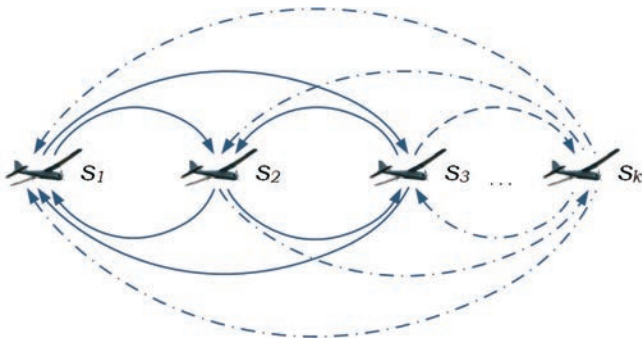


Рис. 14. Схема группировки комплексов БЛА с реконfigurацией равновесных БЛА

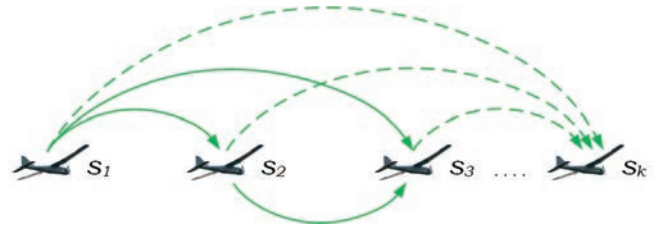


Рис. 15. Схема группировки комплексов БЛА с реконfigurацией неравновесных БЛА

фигурацией неравновесных БЛА. При этом взаимозаменяемость БЛА в рамках группировки определяется их весами x_i , иначе местоположением (рангом) в группировке

Обобщая вышеизложенное можно определить число рабочих Λ состояний для заданных структур:

$$\Lambda = \sum_{i=k_0}^k \binom{k}{k_0},$$

где k_0 — количество функционирующих (работоспособных) БЛА в группировке. Тогда вероятности гарантированного функционирования группировки БЛА в течении времени t соответствует выражение:

$$P_g(t) = \Lambda p_s^i b^{k-i}.$$

где p_s — вероятность физической утраты s_i БЛА, $b = 1 - p_s$.

Расчетные данные зависимости вероятности гарантированного выполнения целевой функции группировкой БЛА различной конфигурации от p_s представлены на рис. 16.

При этом для рисунка а) $p_s \in \{2,5 \times 10^{-3}, 3,5 \times 10^{-2}\}$; $k_0 = 3$; б) $p_s \in \{2,5 \times 10^{-4}, 3,5 \times 10^{-3}\}$; $k_0 = 3$.

Представленные графические зависимости вероятности гарантированного функционирования группировки БЛА при физической утрате некоторых БЛА в итоге иллюстрируют результативность выполнения целевой функции — информирования.

Выводы

Предложен метод повышения информационной живучести группировки БЛА для случая частичной потери целевой информации или деградации — физической утраты БЛА. Получаемые преимущества являются следствием синергетического эффекта, заключающимся в комплексировании методов криптографической защиты информации и помехоустойчивого кодирования (синтез криптокодовых конструкций) с учетом сбалансированного (симметричного) распределения совокупного объема единой системы памяти. Кроме того, в отличие от традиционных методов контроля и обеспечения целостности информации, осно-

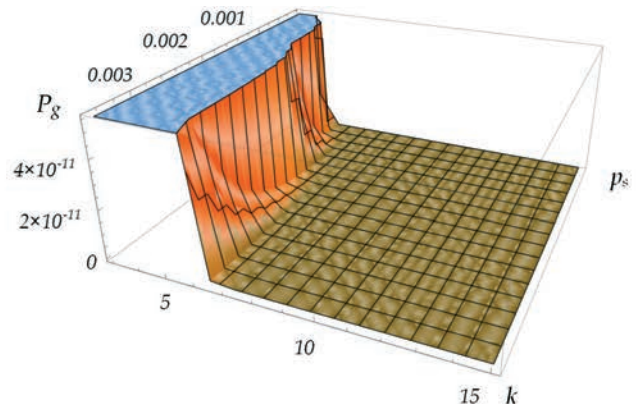
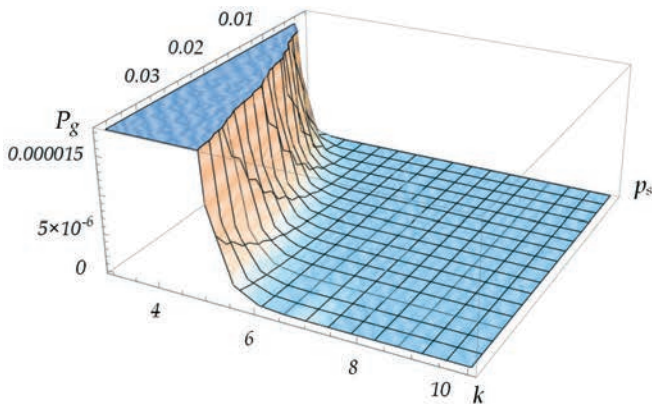


Рис. 16. Зависимости вероятностей гарантированного функционирования различной конфигурации от p_s

ванных на различных методах резервирования (копирования, репликации), связанных с кратным увеличением объема избыточной информации, разработанный метод предполагает существенное ее уменьшение. Также рассмотрены различные варианты реконфигурации группировки комплексов, учет которых, в совокупности с защитным свойством преодоления последствий воздействий вредных факторов позволяет существенно повысить результативность выполнения целевой функции — информирования.

Литература

1. Unmanned Aircraft Systems (UAS) Roadmap, 2005–2030. URL: http://fas.org/irp/program/collect/uav_roadmap2005.pdf (дата обращения 03.10.2017).
2. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power // 8th International Conference on Cyber Conflict (CyCon). 2016. Pp. 205–221.
3. Maxal J., Mahmoud M-S. B., Larrieu N. Secure Routing Protocol Design for UAV Ad Hoc Networks // DASC'2015, IEEE/AIAA 34th Digital Avionics Systems Conference. 2015. DOI: 10.1109/DASC.2015.7311581
4. Самойленко Д. В., Финько О. А. Имитоустойчивая передача данных в защищенных системах однонаправленной связи на основе полиномиальных классов вычетов // Нелинейный мир. 2013. Т. 11. № 9. С. 647–659.
5. Самойленко Д. В., Финько О. А. Криптографическая система в полиномиальных классах вычетов для каналов с шумом и имитирующим злоумышленником // Теория и техника радиосвязи. 2010. № 4. С. 39–45.
6. Петухов Г. Б., Якунин В. И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М.: АСТ, 2006. 504 с.
7. Jamshidi M., Betancour Jaimes A. S., Gomez J. Cyber-physical control of unmanned aerial vehicles // Scientia Iranica. 2011. Vol. 18. No. 3. Pp. 663–668.
8. Fragouli C, Boudec J.-Y. L., Widmer J. Network coding: An instant primer // ACM SIGCOMM Computer Communication Review. 2006. Vol. 36. No. 1. Pp. 63–68.
9. Weatherspoon H., Kubiatowicz J. Erasure Coding vs. Replication: A Quantitative Comparison // Peer-to-Peer Systems. IPTPS 2002. Lecture Notes in Computer Science. 2002. Vol. 2429. Pp.328-337.
10. Chlestil C., Leitgeb E., Sheikh M. S., Friedl A., Zettil K., Schmitt N. P., Rahm W., Perlot N. Optical Wireless on Swarm UAVs for High Bit Rate Applications // IEEE5th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP). 2006.
11. Harshan J. On Algebraic Manipulation Detection codes from linear codes and their application to storage systems // IEEE Information Theory Workshop. 2015. Pp. 64–68.
12. Самойленко Д. В., Финько О. А. Обеспечение целостности информации в автономной группе беспилотных летательных аппаратов методами модулярной арифметики // Наука. Инновации. Технологии. 2016. № 4. С. 77–91.
13. Самойленко Д. В., Еремеев М. А., Финько О. А. Метод обеспечения целостности информации в группе робототехнических комплексов на основе криптокодовых конструкций // Проблемы информационной безопасности. Компьютерные системы. 2017. № 1. С. 70–78.
14. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. М.: Диалектика, 2016. 1024 с.
15. Yu J-H., Loeliger H-A. On Irreducible Polynomial Remainder Codes // Information Theory Proceedings (ISIT). 2011. Pp. 1115–1119.
16. Калмыков И. А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов. М.: Физматлит, 2005. 276 с.
17. Флейшман Б. С. Элементы теории потенциальной эффективности сложных систем. М.: Советское радио. 1971. 224 с.
18. Leong D., Dimakis A. G., Ho T. Distributed storage allocation problems // In Proc. Workshop Netw. Coding, Theory, Appl. (NetCod). 2009. Pp. 86–91.
19. Leong D., Dimakis A. G., Ho T. Distributed storage allocations // IEEE Transactions on Information Theory. 2012. Vol. 58. Pp. 4733–4752.
20. Leong D., Dimakis A. G., Ho T. Symmetric allocations for distributed storage // Proc. IEEE Global Telecommun. Conf. (GLOBECOM). Miami, 2010. 7 p.
21. Кухарев Г. А., Шмерко В. П., Зайцева Е. Н. Алгоритмы и систолические процессоры для обработки многозначных данных. Мн.: Наука и техника, 1990. 296 с.

THE INCREASE OF INFORMATION SURVIVABILITY THE GROUP OF ROBOTIC SYSTEMS METHODS OF MODULAR ARITHMETIC

DMITRY V. SAMOYLENKO,

St-Peterburg, Russia, 19sam@mail.ru

MIKHAIL A. EREMEEV,

Moscow, Russia, mae1@rambler.ru

OLEG A. FINKO,

Krasnodar, Russia, ofinko@yandex.ru

KEYWORDS: autonomous group of robotic complexes; cryptography; modular arithmetic; noiseproof coding in the classes of residues; integrity of information; informational vitality.

ABSTRACT

High risks are associated with threats of occurrence of technogenic extreme situations and disasters, necessitate the search of the most effective ways of improving the prevention, detection, containment, extreme situations and liquidation of their consequences. Under extreme situation refers to a situation in a certain space-time region characterized by the emergence of factors immediate threat to the health and lives of people or the threat of disruption of their activities for solving problems in this area.

At the moment, as we have in the country and abroad massively created robotic systems for various target destination, the application of which should ensure the safety of people in conditions of emergency. A group application for robotic systems can be achieved from certain spaces in which they must be deployed before use and to be called original borders. Locomotion of robotic systems in these space-time region is a key area of application poses a number of problems one of which is discussed in the present article, namely the problem of determining routes of similar robotic systems eliminate emergency situations in case of group method of application.

In the process, identified according to a maximum time of movement of robotic systems to sites of key application areas, the time of liquidation of extreme situations in the nodes with the highest level of hazardous factors, the total time of application of robotic systems and the intensity of the elimination of emergency situations groups of robotic systems in each of these nodes from variable performance values the elimination of hazards of extreme situations of robotic systems (the intensity of consumption of resource manipulation subsystem for robotic systems).

Dependences give the possibility of calculating the time of the liquidation, consumption and manipulation locomotional subsystems, and allow the planning phase to determine the rational route of similar robotic systems eliminate extreme situations, if the group method of application.

REFERENCES

1. Unmanned Aircraft Systems (UAS) Roadmap, 2005-2030. URL: http://fas.org/irp/program/collect/uav_roadmap2005.pdf (date of access 03.10.2017).
2. Hartmann K., Giles K. UAV exploitation: A new domain for cyber power. *8th International Conference on Cyber Conflict (CyCon)*. 2016. Pp. 205-221.
3. Maxal J., Mahmoud M-S. B., Larrieu N. Secure Routing Protocol Design for UAV Ad Hoc Networks. *DASC'2015, IEEE/AIAA 34th Digital Avionics Systems Conference*. 2015. DOI: 10.1109/DASC.2015.7311581
4. Samoilenko D.V., Finko O.A. Imitation proof data transmission in protected system of one-way communication by means of polynomial residue classes. *Nelineinyi mir [Nonlinear World]*. 2013. Vol. 11. No. 9. Pp. 647-659. (In Russian)
5. Samoilenko D.V., Finko O.A. Kriptograficheskaja sistema v polinomial'nyh klassah vychetov dlja kanalov s shumom i imitirujushhim zloumyshlennikom]. *Radio communication theory and equipment*. 2010. Vol. 4. Pp. 39-44. (In Russian).
6. Petuhov G.B., Jakunin V.I. *Metodologicheskie osnovy vneshnego proektirovanija celenapravlennyh processov i celeustremlynyh sistem* [Methodological basis of external design of purposeful processes and purposeful systems]. Moscow: AST, 2006. 504 p. (In Russian)
7. Jamshidi M., Betancour Jaimes A.S., Gomez J. Cyber-physical control of unmanned aerial vehicles. *Scientia Iranica*. 2011. Vol. 18. No. 3. Pp. 663-668.
8. Fragouli C., Boudec J.-Y. L., Widmer J. Network coding: An instant primer. *ACM SIGCOMM Computer Communication Review*. 2006. Vol. 36. No. 1. Pp. 63-68.
9. Weatherspoon H., Kubiawicz J. Erasure Coding vs. Replication: A Quantitative Comparison. *Peer-to-Peer Systems. IPTPS2002. Lecture Notes in Computer Science*. 2002. Vol. 2429. Pp. 328-337.
10. Chlestil C., Leitgeb E., Sheikh M.S., Friedl A., Zettl K., Schmitt N.P.,

Rahm W., Perlot N. Optical Wireless on Swarm UAVs for High Bit Rate Applications. IEEE5th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP). Patras Greece, July 2006.

11. Harshan J. On Algebraic Manipulation Detection codes from linear codes and their application to storage systems. *IEEE Information Theory Workshop*. 2015. Pp. 64-68.

12. Samoylenko D.V., Finko O.A. Ensuring the integrity of information in an autonomous group of unmanned aerial vehicles by methods of modular arithmetic. *Nauka. Innovacii. Tehnologii*. 2016. No. 4. Pp. 77-91. (In Russian)

13. Samoylenko D.V., Ereemeev M.A., Finko O.A. A method of providing the integrity of information in the group of robotic engineering complexes based on crypt-code constructions. *Information Security Problems. Computer Systems*. 2017. No. 1. Pp. 70-78. (In Russian)

14. Schneier B. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley & Sons, 1996. 784 p.

15. Yu J-H., Loeliger H-A. On Irreducible Polynomial Remainder Codes. *IEEE International Symposium on Information Theory Proceedings*. 2011. Pp. 1115-1119.

16. Kalmykov I.A. *Matematicheskie modeli nejrosetevyh otkazoustojchivyh vychislitel'nyh sredstv, funkcionirujushhih v polinomial'noj sisteme klassov vychetov* [Mathematical model of neural network fault-tolerant computing facilities operating in polynomial system classes deductions]. Moscow: Fizmatlit, 2005. 276 p. (In Russian)

17. Fleyshman B.S. *Jelementy teorii potencial'noj jeffektivnosti slozh-*

nyh sistem [Elements of the theory of the potential effectiveness of complex systems]. Moscow: Sovetskoe radio. 1971. 224 p. (In Russian)

18. Leong D., Dimakis A.G., Ho T. Distributed storage allocation problems. In Proc. Workshop Netw. Coding, Theory, Appl. (NetCod). 2009. Pp. 86-91.

19. Leong D., Dimakis A.G., Ho T. Distributed storage allocations. *IEEE Transactions on Information Theory*. 2012. Vol. 58. Pp. 4733-4752.

20. Leong D., Dimakis A.G., Ho T. Symmetric allocations for distributed storage. Proc. IEEE Global Telecommun. Conf. (GLOBECOM). Miami, 2010. 7 p.

21. Kuharev G.A., Shmerko V.P., Zajceva E.N. *Algoritmy i sistolicheskie processory dlja obrabotki mnogoznachnyh dannyh* [Algorithms and systolic processors for processing multivalued data]. Minsk: Nauka i tehnika. 1990. 296 p. (In Russian)

INFORMATION ABOUT AUTHORS:

Samoylenko D. V., PhD, Doctoral Candidate Military Space Academy; Ereemeev M. A., PhD, Full Professor, Professor of the Department "Applied information technology" Institute a comprehensive safety and special instrumentation of the "Moscow Technological University";

Finko O. A., PhD, Full Professor, Academic Adviser of the Russian academy of rocket and artillery sciences (department of technical means and technologies of investigation, navigation, communication and management), professor of the department "Special communication" Krasnodar highest military college of the general S. M. Shtemenko.

For citation: Samoylenko D.V., Ereemeev M.A., Finko O.A. The increase of information survivability the group of robotic systems methods of modular arithmetic. *H&ES Research*. 2018. Vol. 10. No. 2. Pp. 62-77. doi 10.24411/2409-5419-2018-10042 (In Russian)

doi 10.24411/2409-5419-2018-10043

СТРУКТУРА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ НАЗЕМНОГО РОБОТОТЕХНИЧЕСКОГО КОМПЛЕКСА ДЛЯ ФОРМИРОВАНИЯ МАРШРУТА ДВИЖЕНИЯ

ВАРГАНОВ

Вячеслав Валерианович¹

ГРИВАЧЕВ

Александр Валерьевич²

КУРОЧКИН

Александр Геннадиевич³

ТИТЕНКО

Евгений Анатольевич⁴

Сведения об авторах:

¹к.с.н., доцент, заместитель директора научно-исследовательского института радиоэлектронных систем Юго-Западного государственного университета, г. Курск, Россия, prcvvv@yandex.ru

²аспирант Юго-Западного государственного университета, г. Курск, Россия, garpin-22@mail.ru

³аспирант Юго-Западного государственного университета, г. Курск, Россия, ak.kursk@gmail.com

⁴к.т.н., доцент, начальник управления научно-исследовательского института радиоэлектронных систем Юго-Западного государственного университета, г. Курск, Россия, johntit@mail.ru

АННОТАЦИЯ

В работе построена структура системы управления для подвижного наземного робота. С точки зрения проектирования сложных информационных систем робот понимается как программируемый подвижный исполнитель команд. При этом команда движения считается базовой среди выполняемых работ. Указаны ограничения и недостатки классических систем управления движением, не позволяющие роботу самостоятельно планировать маршрут. Классическая система управления не имеет встроенных средств для интеллектуального объединения данных от разнородных датчиков. Данное ограничение не позволяет автоматически строить маршрут движения робота и анализировать объекты окружающей среды. Предложена структура системы управления, содержащая иерархическую схему комплексирования разнородных данных и модуль построения модели окружающей среды. Объединение выходных потоков от различных типов датчиков позволяет построить непротиворечивую и полную модель окружающей среды. Установлено, что данная модель, в дальнейшем, позволит роботу автоматически строить маршруты движения (поиск в трёхмерном пространстве, выбор наилучших вариантов поверхности для движения, объезд потенциально опасных участков местности и т.д.). Схема комплексирования является модульной по составу и конвейерной по схеме вычислений. Показано преимущество, позволяющее применять модель для представительного класса подвижных роботов с различным набором датчиков и средств измерения. Создана структура системы управления, она содержит блоки видового, межвидового комплексирования. Также в системе управления выполнена агрегация данных об объектах окружающей среды в метаданные. Агрегация выполняется на основе базы характеристик робота и баз правил для оценки внешних ситуаций. Такая иерархия объединений разнородных данных позволяет динамически строить и изменять маршрут при наличии препятствий и использовать подвижный робот во внешней среде без участия человека.

КЛЮЧЕВЫЕ СЛОВА: система управления; робототехнический комплекс; уровень управления; схема комплексирования; маршрут.

Для цитирования: Варганов В.В., Гривачев А.В., Курочкин А.Г., Титенко Е.А. Структура интеллектуальной системы управления наземного робототехнического комплекса для формирования маршрута движения // Научные исследования в космических исследованиях Земли. 2018. Т. 10. № 2. С. 78-86. doi 10.24411/2409-5419-2018-10043

Актуальность работы

Одной из перспективных тенденций современного развития наземной военной робототехники является плановый переход от дистанционно управляемых робототехнических комплексов (РТК) к автоматически функционирующим наземным РТК [1–3], способным достаточно самостоятельно принимать решения по подготовке и исполнению маршрута движения [4–5] на основе текущей информации о состоянии комплекса и характеристиках объектов окружающей среды [6–7].

Движение робота понимается как обособленный вид работы, непосредственно связанный с выполнением типовых элементов движения в условиях неопределенности окружающей обстановки и формированием рационального (оптимального) маршрута движения. Одним из автоматизированных способов уменьшения такой неопределенности является синтез системы (СУ) управления РТК, имеющей возможности как для поддержки расчетных задач по контролю состояния РТК и исполнения движения, так и по обеспечению поисковых задач в условиях неопределенности, неполноты исходных данных [6–9]. Важнейшей такой задачей является задача формирования и/или коррекции маршрута движения [10]. Решение задачи связано с привлечением значительных вычислительных и емкостных ресурсов (фильтрация, поворот участков раstra, подготовка картограммы проходимости, генерация и проверка альтернатив участков маршрута, глобальные нерегулярные проверки геодезических и топологических свойств объектов местности, автоматизированный учет сезонных и иных изменений участков местности, гидрографических объектов, синтез 3D-модели и др.) [11–12].

Метеорологические, топографические и иные свойства местности оказывают существенное влияние на планирование и контроль движения РТК по маршруту. Для экипажных машин эти факторы учитываются их командирами и механиками-водителями при организации и выполнении работ. Вместе с тем степень автоматизации этих процессов пока является недостаточной, что определяет актуальность разработки структуры СУ и алгоритмов функционирования основных подсистем, прежде всего планирования и реализации движения по цифровой карте местности и аэрокосмических снимков в разные периоды времени года.

Структура системы управления нижнего уровня

Одним из ключевых элементов перспективных РТК является система управления. Разработка перспективных систем управления, аппаратно ориентированных на работу в условиях неполноты или нечеткости исходной информации, неопределенности внешних воздействий и среды функционирования, требует привлечения нетривиальных подходов к управлению и использованию технологий искусственного интеллекта [16–17].

Очевидно, что при наличии различного рода неопределенностей при случайном характере внешних воздействий, к которым можно отнести непредусмотренное изменение фоно-целевой обстановки, собственных эксплуатационных характеристик объекта управления и параметров среды, высокий уровень автономности работы, адаптивности режимов работы систем управления должен обеспечиваться за счет повышения их интеллектуальных возможностей. Можно выделить современные *информационно-технических требований к системам управления* робототехнических комплексов:

- построение системы управления по распределенному принципу с использованием как универсальных, так и специализированных вычислительных средств;
- использование мощной бортовой вычислительной системы, способной как производить универсальные алгоритмические вычисления, так и обрабатывать большие параллельные информационные потоки;
- применение многоканальной системы локальной навигации;
- наличие многоспектральной системы технического зрения, способной работать в условиях пониженной освещенности и сложных метеоусловиях;
- наличие высокоскоростных, помехозащищенных каналов связи и управления.

Наземные РТК оснащаются различными сенсорами, а также средствами наблюдения, связи и навигации, которые позволяют им действовать автономно или под управлением оператора, передавать оператору аудио-и видеоинформацию в реальном масштабе времени практически в любое время суток. Вместе с тем вопросы комплексирования информации от различных средств ее добывания не получили систематического рассмотрения в составе существующих систем управления РТК. Исследуемым является вопрос набора средств восприятия данных от приборов и датчиков, устанавливаемых на машины использующих различные физические принципы получения данных и их последующей интерпретации. Этот вопрос будет последовательно детализироваться разработкой принципов и алгоритмов комплексной разнородной информации и эксплуатацией используемых устройств, приборов и датчиков съема, сканирования, измерения характеристик до внешних объектов.

Тенденция по структурной организации СУ состоит в проектировании многоуровневой структуры, разграничивающей процессы непосредственного управления устройствами и органами (модельно-привязанные к типу робота программы) и процессы планирования и реализации автономного движения

Такое разграничение является основой модульной независимости решаемых задач, экономит ресурсы и обеспечивает автономность выполняемых роботом типов

работ. Кроме того, для систематического учета разнородных требований к движению РТК в условиях неопределенности представляется целесообразным использовать иерархический подход к построению СВУ, сохраняющий преемственность решений и наработок дистанционно управляемых и полуавтономных наземных роботов на нижнем (исполнительном) уровне управления [13–14].

СУ на нижнем уровне имеет классическую структуру: выделяются первичные измерительные средства, исполнительные агрегаты, узлы, подсистемы (АУП), модуль приема-передачи данных (ПП) от командного пункта (КП) и единый центр сбора и обработки информации — контроллер платформы РТК. Робот в этом случае понимается как подвижный непрограммируемый исполнитель команд, в том числе команд движения. Сенсорные средства ввода данных о внешней среде непосредственно передают/транслируют оператору без первичного анализа и обработки исходную информацию. Фактически система управления РТК представляет систему измерения и сбора данных о состоянии исполнительных АУП и получения первичной (видео-, измерительной) информации. Принятие решения по планированию движения реализуется оператором РТК.

Структура системы управления верхнего уровня

Система управления РТК верхнего уровня, в том числе, предназначена для автоматизации действий по планированию, исполнению и контролю работ поисково-аналитического характера. Планирование и коррекция маршрута является важнейшей задачей такого типа. Ее решение призвано дополнить и/или заменить действия оператора в условиях разнородных данных о состоянии машины и окружающей обстановки [14].

В качестве общей схемы СУ верхнего уровня предлагается следующее представление (рис. 2.), состоящее из взаимодействующих модулей планирования работ (движения), исполнения и контроля команд движения, модельного описания окружающей среды [10].

В состав СУ должны входить следующие информационно-управляющие компоненты:

- модель внешней среды — описывает состояния окружающей среды с учетом законов поведения объектов (пассивных и активных, в статике и динамике по времени);
- модуль идентификации и распознавания объектов, изображений, и поведения объектов по заложенным метаданным — закономерности появления/исчезновения ячеек-препятствий на матрице местности;

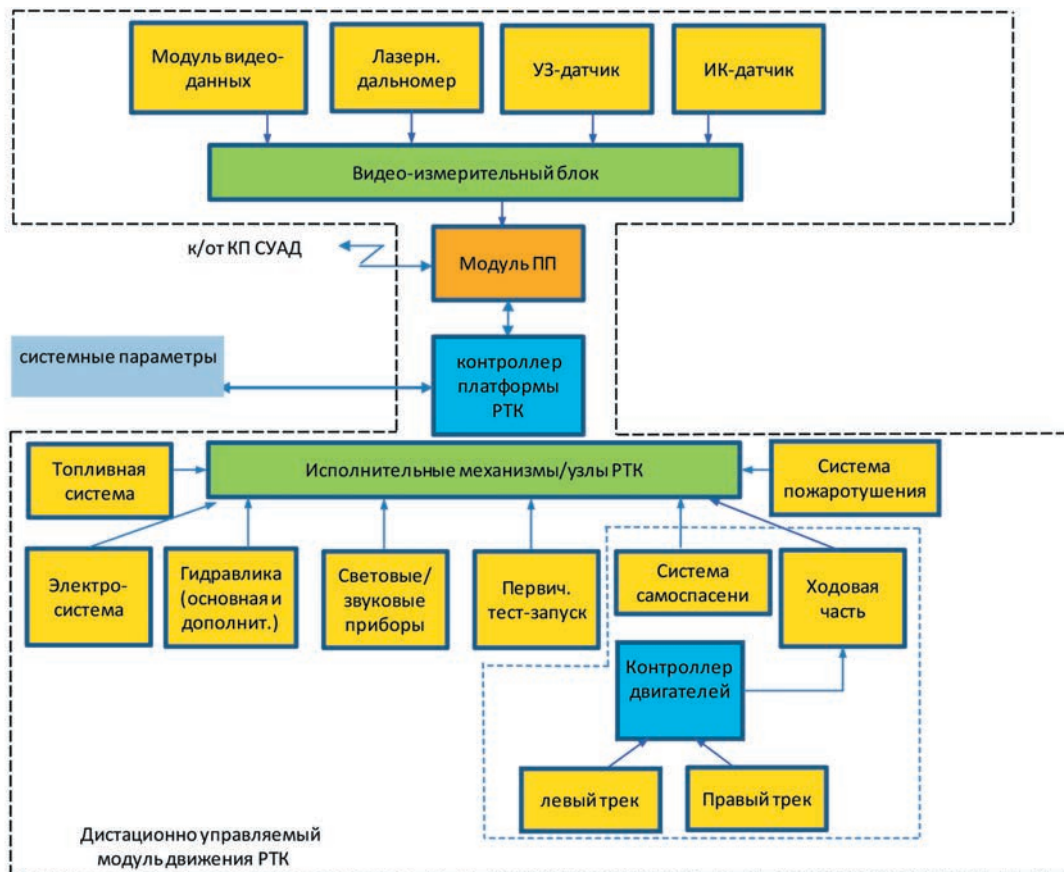


Рис. 1. Структура СУ для наземного РТК (нижний уровень)

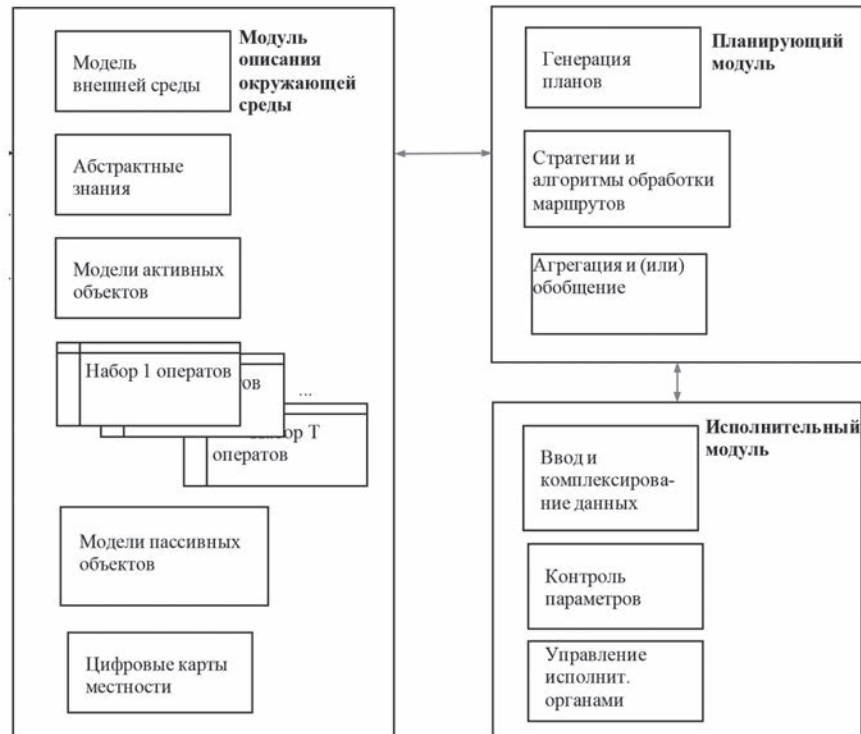


Рис. 2. Общая схема СУ (верхний уровень)

— модуль генерации планов — осуществляет поиск текущего маршрута или его участка на основе модели окружающей обстановки

— модуль исполнения действий осуществляет контроль запланированных действий, подавая команды на исполнительные устройства и контроллеры;

— модуль управления целями определяет иерархию целей, их важность и последовательность достижения при многоцелевой задаче;

— модуль распознавания объектов внешней среды;

— иерархическая система комплексирования данных от различных сенсорных источников, обеспечивающая планирующий модуль информацией различного уровня агрегации.

Модель внешней среды создается на основе заложенных типовых сцен и выполняет функцию запоминания состояния объектов и их характеристик, существенных для процессов движения [15]. Задачей модуля распознавания является обнаружение роботом видовых объектов, их характеристик и географического положения в модели. В результате в процессе движения в работе формируется и постоянно обновляется модель внешней среды, а результатом работы системы планирования является не только (пере)построение маршрутов движения, а также накопление данных об объектах внешней среды (координаты, размер, семантика, вид исходящей угрозы и др.), попавших в локальную окрестность движущегося робота.

Важное место в обеспечении принятия решения при автоматическом движении РТК отводится процессам объединения данных от различных датчиков и системы технического зрения РТК. Основным направлением развития системы технического зрения является комплексирование данных от различного типа средств ввода данных в РТК: стереозрение, лазерные сканеры, ультразвуковые датчики, радары ближнего действия и др. По отдельности каждый тип датчиков предоставляет частичный объём данных об окружающей среде. Комплексирование — синхронизированное по времени совмещение на общий объект окружающей среды измеренных характеристик, имеющих общую начальную точку в единой системе координат — в состоянии снять эти ограничения. Благодаря совмещению выходных потоков от различных типов датчиков система технического зрения может построить непротиворечивую и полную модель окружающей среды. Данная модель, в дальнейшем, позволит роботизированной платформе строить и/корректировать маршруты движения робота при наличии ограничений (поиск в трёхмерном пространстве, выбор наилучших вариантов поверхности для движения, объезд потенциально опасных участков местности и т.д.).

Соответственно СУ РТК верхнего уровня должна иметь расширенные средства ввода данных и восприятия внешнего мира, его отражения в некоторую цифровую модель местности (модель внешней среды). Достижение оперативного и тактического превосходства РТК в усло-

виях конфликта обеспечивается возможностью генерации альтернативных действий, динамического варьирования видами движений, что должно быть связано с введением в общий цикл управления поисковых методов и алгоритмов. Последние способны наряду с расчетно-логическим действиями, определяющими детерминированный характер вычислений и соответственно перемещений РТК в пространстве, выполнять поисковые преобразования и ситуационно выдавать скоординированные по цели, но не запланированные ранее перемещения.

Комплексирование входных данных целесообразно распределить на между нижним и верхним уровнями, обеспечивая переключение между ними и для расширенного восприятия окружающей среды. В этом случае СУ должна использовать все источники данных, а также информацию из баз данных и знаний в виде шаблонов и правил обработки типовых ситуаций.

Далее интеллектуализация возможностей РТК направлена с включение в состав СУ передающе- известительного модуля. Вопросы организации коммутационных обменов сообщениями и последующего автономного принятия решений на борту машины оперативно получать актуализированную информацию и соответственно принимать обоснованные решения, особенно в составе группировки подвижных роботов. Конечно, такой подход требует непосредственного мониторинга ЛПП с командного пункта за каждым действием РТК на местности и своевременного целеуказания подвижному роботу, что также требует наличия ресурсных возможностей в передающе- известительного модуле.

В состав типовой стандартной СУ входят следующие подсистемы:

- а) подсистема управления движением;
- б) подсистема управления ресурсами;
- в) подсистему позиционирования и управления связью.

Как развитие структурно-функционального подхода модифицированная СУ включает в свой состав четыре подсистемы:

- а) подсистему управления движением;
- б) подсистему управления ресурсами;
- в) подсистему позиционирования и управления связью, включая передающе- известительный модуль;
- г) подсистему анализа и реконфигурации.

Введенная подсистема анализа и реконфигурации отвечает за генерацию альтернатив и выбор нового участка траектории в связи с неожиданно возникшим препятствием или нестандартной ситуацией на местности. Как правило, такие препятствия не актуализированы на карте местности, поэтому в задачу РТК входит реконфигурация маршрута и оповещение всех подвижных роботов в составе группы.

Первые три подсистемы имеют собственные локальные модули управления и преимущественно ориен-

тированы на выполнение расчетно- логических действий детерминированного характера. Средства восприятия ИР в принятии решений данных подсистем ориентированы преимущественно на мехатронные функции движения и состоят в приеме и мониторинге внешней информации для предотвращения неконтролируемых перемещений и недопустимых движений.

Вопросы анализа внешнего окружения и соответствующей топологической расстановки роботов на местности входят в функцию четвертой подсистемы. Отличительная особенность подсистемы анализа и реконфигурации заключается в том, что решение о статусе робота через передающе- известительный модуль может быть оттранслировано в соседние роботы в подсистему позиционирования и управления связью, что создает базу для динамического управления конфигурацией роботов (размещением) в составе группировки. Введенная подсистема анализа и реконфигурации расширяет реальные и потенциальные функциональные возможности РТК, что определяет структурную адаптацию связанных процессов при работе в группе. Другими словами, структурная схема подвижного робота с подсистемой анализа и реконфигурации имеет адаптированную структуру под процессы автономного движения и принятия решений.

Для упорядочения процессов комплексирования и выработки общей объединяющей базы предлагается иерархическая (трехуровневая) схема комплексирования данных (рис. 3).

Важнейшим для генерации агрегированных данных является второй уровень. На нем объединяются в пары такие источники данных, которые имеют общий измеряемый признак — дистанции, удаления, расстояния. При этом в паре операндов на комплексирование выделяется стробирующий (селективный) процесс, по которому осуществляется выделение синхронизированных данных из массива измерений (второй операнд) для последующей обработки.

Данная схема комплексирования является модульной по составу и конвейерной по схеме вычислений. Она может расширяться или усекается до номенклатуры имеющихся в подвижном роботе технических средств измерения, съемки, сканирования, что делает ее применимой для представительного класса подвижных роботов.

Детализированная многоуровневая организация СУ для наземного РТК (верхний уровень) содержит три уровня комплексирования данных (рис. 4). На рис. 4 обозначено: ЦКМ — цифровая карта местности, НВ — навигационные вычисления, ПКМ — построение картограммы проходимости, ПМ — планирование маршрута, ВХМ — вычисление характеристик маршрута. Система управления движением имеет линейно-итерационную структуру. Центральное место в ней занимают модули межвидового комплексирования (на основе конвейерных матриц) и пла-

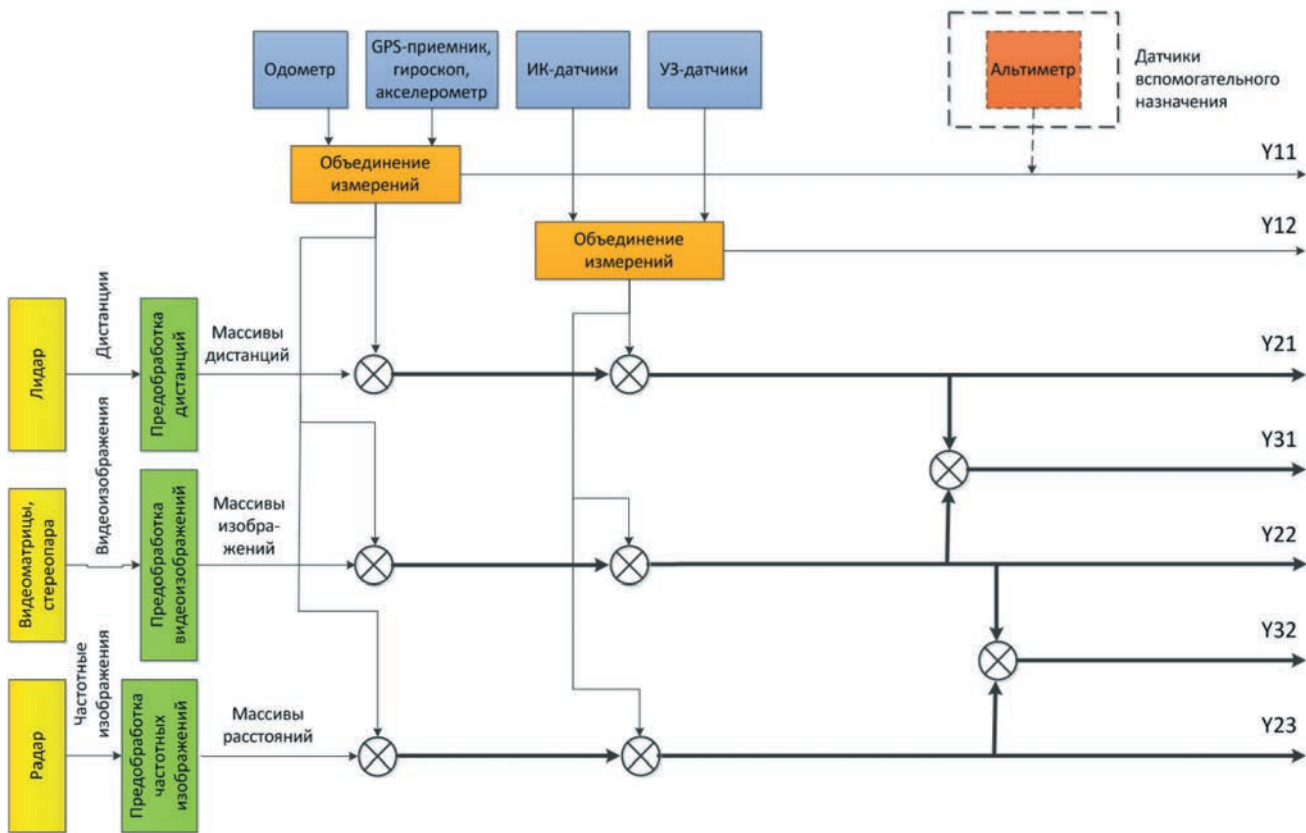


Рис. 3. Иерархическая схема комплексирования данных в РТК

нирования и исполнения движения. В последнем модуле осуществляется цикл поиска маршрута, оценки его характеристик с учетом вновь выявленных препятствий. Эта особенность организации позволяет роботу при планировании движения выполнять этапы межвидового комплексирования и агрегации данных с привлечением БД видовых объектов, базы тактико-технических характеристик робота, баз правил для оценки внешних ситуаций.

Таким образом, создана СУ, имеющая 2 самостоятельных уровня управления и планирования движения. Структура СУ детализирована модулями и блоками для анализа картографической информации о местности, планирования и/коррекции маршрута при наличии объектов-препятствий и ограничений на характеристики маршрута. Отличительная особенность модуля планирования и исполнения маршрута — совместное применение навигационных, картографических данных и данных о состоянии РТК.

Выводы

1. Проанализирована классическая структура СУ нижнего уровня, обеспечивающая для наземного РТК поддержку процессов измерения, сбора данных о состоянии машины и ее доведения до оператора для принятия

решения по планированию движения. Определен основной недостаток СУ нижнего уровня — невозможность построения модели окружающей среды для планирования маршрута на борту РТК.

2. Показано, что основу СУ верхнего уровня составляет модель окружающей среды. Для автоматического планирования маршрута на борту РТК важное место в принятии решения отводится процессам комплексирования данных от различных датчиков и системы технического зрения РТК. Предложена иерархическая схема блока комплексирования — комплексора данных. Данная схема комплексирования является модульной по составу и конвейерной по схеме вычислений, что делает ее применимой для представительного класса подвижных роботов с различными наборами технических средств измерения, съемки, сканирования и др.

3. Разработана структура СУ (верхний уровень), имеющая три уровня комплексирования вплоть до агрегации данных и позволяющая использовать сложные алгоритмы поиска маршрута при наличии тактико-технических ограничений (поиск в трёхмерном пространстве, выбор наилучших вариантов поверхности для движения, объезд потенциально опасных участков местности и т.д.).

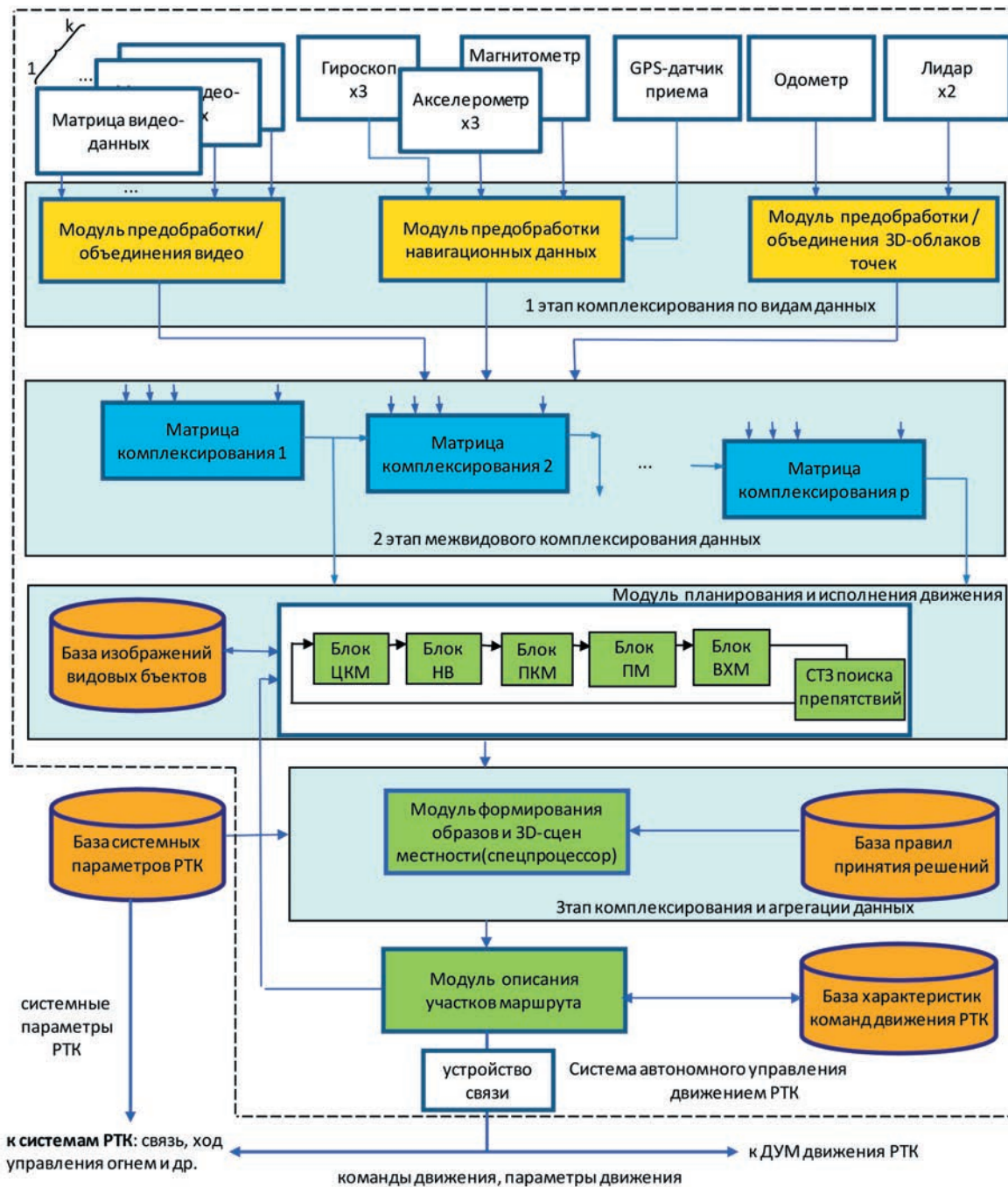


Рис. 4. Структура СУ для наземного РТК (верхний уровень)

Применение модели окружающей среды в составе СУ РТК позволяет оптимизировать взаимодействия роботов в группе. Каждый РТК в состоянии расширить своё представление об окружающей среде за счёт обмена данными между соседними роботами. Имея общую модель окружающей среды, группировка РТК может осуществлять точное позиционирование на сформированной модели, что позволяет осуществлять динамическое изменение положения роботов внутри группировки [15, 17–18].

Литература

1. Макаров И.М., Лохин В.М. Интеллектуальные системы автоматического управления. М.: Наука, 2001. 576 с.
2. Геловани В.А., Башильков А.А., Бритков В.Б., Вязилов Е.Д. Интеллектуальные системы поддержки принятия решений в нестандартных ситуациях с использованием информации о состоянии природной среды. М.: УРСС, 2001. 304 с.
3. Гривачев А.В., Емельянов С.Г., Бородин М.В. Структурно-функциональная схема распознавания и оцен-

ки риска в системе управления роботизированными многофункциональными машинами // Информационно-измерительные и управляющие системы. 2015. Т. 13. № 6. С. 4–9.

4. *Лоторев П. В., Курочкин А. Г., Гривачев А. В., Емельянов С. Г.* Организация системы поддержки принятия решений для управления группой роботов // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2015. № 3. С. 30–36.

5. *Лоторев П. В., Курочкин А. Г., Гривачев А. В.* Математическая модель динамической коррекции маршрута подвижного робота // Научные технологии. 2016. Т. 17. № 3. С. 21–25.

6. *Ларичев О. И.* Теория и методы принятия решений. М.: Логос, 2010. 183 с.

7. *Дружинин В. В.* Системотехника. М.: Радио и связь, 1985. 200 с.

8. *Hofner C., Schmidt G.* Path Planning guidance techniques for an autonomous mobile cleaning robot // Robotics and Autonomous System. 2005. Vol. 14. Pp. 199–212.

9. *Arkin R. C.* Behavior-based Robot Navigation in Extended Domains // J. of Adaptive Behavior. 2002. Vol. 1. No. 2. Pp. 201–225.

10. *Emery R., Balch T.* Behavior-based Control of Non-Holonomic Robot in Pushing Task // IEEE Intern Conf

on Robotics and Automation (ICRA-2011). Seoul, 2011. Pp. 185–189.

11. *Casbeer D. W.* Forest fire monitoring with multiple small UAVs // Proceedings of the 2005 American Control Conference. 2005. No. 1. Pp. 3530–3535.

12. *King A.* Distributed Parallel Symbolic Execution. Kansas: Kansas State University, 2005. 87 p.

13. *Duncan R.* A survey of parallel computer architectures for motion agents // Computer. 2009. Vol. 23. No. 2. Pp. 5–16.

14. *Hennessy J. L., Patterson D. A.* Computer Architecture. A Quantative Approach. 3th ed. San Francisco: Morgan Kaufmann Publishers, Elsevier Science, 2013. 833 p.

15. *Казаков А. А., Семенов В. А.* Обзор современных методов планирования движения // Труды Института системного программирования РАН. 2016. Т. 28. № 4. С. 241–294.

16. *Рыбина Г. В.* Основы построения интеллектуальных систем. М.: Финансы и статистика, 2010. 430 с.

17. *Курочкин А. Г., Емельянов С. Г., Бородин М. В.* Продукционная модель для координации бесконфликтного расположения группы автономных роботов // Информационно-измерительные и управляющие системы. 2015. Т. 13. № 6. С. 10–14.

18. *Люгер Дж. Ф.* Искусственный интеллект: стратегии и методы решения сложных проблем. М.: Вильямс, 2003. 864 с.

STRUCTURE OF INTELLECTUAL SYSTEM OF CONTROL OF ROBOTIC TECHNICAL COMPLEX FOR FORMATION OF ROUTE OF MOTION

VYACHESLAV V. VARGANOV,

Kursk, Russia, npcvvv@yandex.ru

ALEXANDER V. GRIVACHEV,

Kursk, Russia, garpun-22@mail.ru

ALEXANDER G. KUROCHKIN,

Kursk, Russia, ak.kursk@gmail.com

EVGENIY A. TITENKO,

Kursk, Russia, johntit@mail.ru

KEYWORDS: control system; robotic complex; level of control; complexion scheme; route.

ABSTRACT

The work is show the structure of a control system for a mobile ground robot. From an information point of view, the robot is understood as a programmable mobile executor of commands. The movement team is considered to be the base of the work performed. The limitations and disadvantages of classical traffic control systems are indicated,

which do not allow the robot to plan the route independently. Classical control system does not have built-in tools for intelligent data integration from heterogeneous sensors. This restriction does not automatically allow you to build a route of movement of the robot and analyze the objects of the environment. The proposed structure of

the management system contains a hierarchical scheme for combining heterogeneous data and a module for building an environmental model. The combination of output streams from different types of sensors makes it possible to build a consistent and complete model of the environment. This model, in the future, will allow the robot to automatically build traffic routes (search in three-dimensional space, selection of the best variants of the surface for movement, detour of potentially dangerous sections of the terrain, etc.). The blocking scheme is modular in composition and conveyor according to the calculation scheme. This advantage makes it suitable for a representative class of mobile robots with a different set of sensors and measuring instruments. The created structure of the control system contains blocks of species, interspecific integration. Also, the management system aggregates data on environmental objects into metadata. Aggregation is performed based on the robot's characteristics database and rules bases for assessing external situations. Such hierarchy of associations of heterogeneous data allows you to dynamically build and modify the route in the presence of obstacles.

REFERENCES

1. Makarov I.M., Lokhin V.M. *Intellektual'nye sistemy avtomaticheskogo upravleniya* [Intelligent systems of automatic control]. Moscow: Nauka, 2001. 576 p. (In Russian)
2. Gelovani V.A., Bashlykov A.A., Britkov V.B., Vyazilov E.D. *Intellektual'nye sistemy podderzhki prinyatiya reshenij v neshtatnyh situacijah s ispol'zovaniem informacii o sostoyanii prirodnoj sredy* [The intellectual decision support systems in emergency situations using information on the state of the natural environment]. Moscow: URSS, 2001. 304 p. (In Russian)
3. Grivachev A.V., Emel'yanov S.G., Borodin M.V. The structural-functional scheme for recognition and risk assessment in the control system of robotic multifunction machines. *Informatsionno-izmeritel'nye i upravlyaushchie sistemy* [Information-measuring and Control Systems]. 2015. Vol. 13. No. 6. Pp. 4-9. (In Russian)
4. Lotorev P.V., Kurochkin A.G., Grivachev A.V. Design of decision support for control of robots. *Proceeding of the South-West State University. Series Control, computer engineering, information science. Medical instruments engineering*. 2015. No. 3. Pp. 30-36. (In Russian)
5. Lotorev P.V., Kurochkin A.G. Grivachev A.V. Mathematical model of the dynamic correction of the mobile robot route. *Naukoemkie tekhnologii* [Science Intensive Technologies]. 2016. Vol. 17. No. 3. Pp. 21-25.
6. Larichev O.I. *Teoriya i metody prinyatie reshenij* [Theory and methods of decision-making] Moscow: Logos. 2010. 183 p. (In Russian)
7. Druzhinin V.V. *Sistemotekhnika* [System engineering]. Moscow: Radio i Svyaz', 1985. 200 p. (In Russian)
8. Hofner C., Schmidt G., Path Planning guidance techniques for an autonomous mobile cleaning robot. *Robotics and Autonomous System*. 2005. Vol. 14. No. 2. Pp. 199-212.
9. Arkin R.C. Behavior-based Robot Navigation in Extended Domains. *J. of Adaptive Behavior*. 2002. Vol.1 No. 2. Pp.201-225.
10. Emery R., Balch T. Behavior-based Control of Non-Holonomic Robot in Pushing Task. *IEEE Intern Conf on Robotics and Automation (ICRA-2011)*. Seoul, 2011. Pp. 185-189.
11. Casbeer D.W. Forest fire monitoring with multiple small UAVs. *Proceedings of the 2005 American Control Conference*. 2005. No. 1. Pp. 3530-3535.
12. King A. *Distributed Parallel Symbolic Execution*. Kansas: Kansas State University, 2005. 87 p.
13. Duncan R. A survey of parallel computer architectures for motion agents. *Computer*. 2009. Vol. 23. No. 2. Pp. 5-16.
14. Hennessy J.L., Patterson D.A. *Computer Architecture. A Quantitative Approach*. Third Edition. San Francisco: Morgan Kaufmann Publishers. Elsevier Science. 2013. 833 p.
15. Kazakov A.A., Semenov V.A. Obzor sovremennyh metodov planirovaniya dvizheniya [The study of modern methods of traffic planning]. *Trudy Instituta sistemnogo programmirovaniya* [Publications of the Institute for System Programming of the Russian Academy of Sciences]. 2016. Vol. 28. No. 4. Pp. 241-294. (In Russian)
16. Rybina G.V. *Osnovy postroeniya intellektual'nyh sistem* [Fundamentals of the construction of intelligent systems]. Moscow: Financy i Statistika, 2010. 430 p. (In Russian)
17. Kurochkin A.G., Emel'yanov S.G., Borodin M.V. A production model for coordinating the conflict-free location of a group of autonomous robots. *Informatsionno-izmeritel'nye i upravlyaushchie sistemy* [Information-measuring and Control Systems]. 2015. Vol. 13. No. 6. Pp. 10-14. (In Russian)
18. Luger J.F. *Iskusstvennyj intellekt: strategii i metody resheniya slozhnyh problem* [Artificial Intelligence: strategies and methods for solving complex problems]. Moscow: Wil'yams. 2003. 864 p. (In Russian)

INFORMATION ABOUT AUTHORS:

Varganov V.V., PhD, Docent, Deputy Director of the Research Institute Department, South-West State University;
 Grivachev A.V., Postgraduate Student of the South-West State University;
 Kurochkin A.G., Postgraduate Student of the South-West State University;
 Titenko E.A. PhD, Docent, Head of the Research Institute Department, South-West State University.

For citation: Varganov V.V., Grivachev A.V., Kurochkin A.G., Titenko E.A. Structure of intellectual system of control of robotic technical complex for formation of route of motion. *H&ES Research*. 2018. Vol. 10. No. 2. Pp. 78-86. doi 10.24411/2409-5419-2018-10043. (In Russian)

doi 10.24411/2409-5419-2018-10044

ФИЛЬТРАЦИЯ НЕЖЕЛАТЕЛЬНЫХ ПРИЛОЖЕНИЙ ИНТЕРНЕТ-РЕСУРСОВ В ЦЕЛЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ШЕЛУХИН

Олег Иванович¹

СМЫЧЁК

Михаил Александрович²

СИМОНЯН

Айрапет Генрикович³

АННОТАЦИЯ

Рассмотрена актуальная задача контроля доступа к Интернет-ресурсам имеющая важное прикладное значение: блокирование доступа к нелегальной, экстремистской, антисоциальной информации, предотвращение утечки конфиденциальной информации через Интернет и др. Для решения подобных задач широкое распространение используются методы машинного обучения. Традиционные методы классификации сетевого трафика, основанные как на номерах портов, так и на информационной нагрузке, полагаются на прямое изучение сетевых пакетов. При наличии полного и помеченного тренировочного набора данных, целесообразно строить классификатор, используя технологии машинного обучения (Machine Learning) и интеллектуального анализа данных (Data Mining), оказавшиеся наиболее эффективными. Создание «идеального» классификатора невозможно пока не будут решены проблемы, присущие данной области. Прежде всего это отсутствие общего, репрезентативного набора исходных данных, который мог бы стать стандартным для исследований в данной области. Большинство известных работ посвященных проблеме классификации трафика опускают фундаментальное требование определения неизвестного типа трафика.

Целью работы является исследование эффективности алгоритмов классификации приложений сетевого трафика в условиях наличия фонового трафика.

Новизной представленного решения является анализ следующих групп приложений: Web -протоколы просмотра web-сайтов - http, https; ftp -протокол для передачи файлов ftp; mail -протоколы для передачи электронной почты - SMTP, POP3, IMAP; p2p - протоколы приложений, использующие пиринговые сети для передачи файлов путем использования алгоритмов машинного обучения: C4.5; Random Forests; Support Vector Machine; Bagging и Adaptive Boost в условиях наличия неклассифицируемого (фонового) трафика. Показано, что качество классификации в условиях наличия фонового трафика снижается для всех рассматриваемых алгоритмах классификации. Однако поскольку алгоритмы C4.5, Random Forests, Bagging и AdaBoost построены на использовании деревьев принятия решений - одного в случае (C4.5) или множества, их характеристики остаются достаточно высокими и отличаются незначительно.

КЛЮЧЕВЫЕ СЛОВА: классификация сетевого трафика, машинное обучение, нежелательные приложения, информационная безопасность, фоновый трафик, атрибуты.

Сведения об авторах:

¹д.т.н., профессор, заведующий кафедрой информационной безопасности Московского технического университета связи и информатики, г. Москва, Россия, sheluhin@mail.ru

²к.т.н., главный специалист отдела проектирования сетей связи Акционерного общества «Гипрогазцентр», г. Нижний Новгород, Россия, m-smychek@mail.ru

³к.т.н., доцент кафедры информационной безопасности Московского технического университета связи и информатики, г. Москва, Россия, blackman-05@mail.ru

Для цитирования: Шелухин О. И., Смычек М. А., Симонян А. Г. Фильтрация нежелательных приложений интернет-ресурсов в целях информационной безопасности // Научные исследования в космических исследованиях Земли. 2018. Т. 10. № 2. С. 87-98. doi 10.24411/2409-5419-2018-10044

Постановка задачи

Проблема контроля доступа к Интернет-ресурсам актуальна и имеет важное прикладное значение по следующим основным причинам: блокирование доступа к нелегальной (экстремистской, антисоциальной и т. п.) информации, предотвращение доступа к Интернет-ресурсам в личных целях в учебное или рабочее время, предотвращение утечки конфиденциальной информации через Интернет.

Вредоносные программы и атаки обычно используют непроверяемый канал зашифрованного трафика HTTPS. Не соответствующее политике или нежелательное поведение пользователей.

Первая задача, которая встает перед администраторами, это определить, какой тип сетевого трафика генерируется пользователями. Трафик может быть вредоносным (например, кража данных или разведка сети), неприемлемым и нарушающим политику (например, использование служб обмена файлами) или выходящим за рамки обычных бизнес-процессов (например, генерирование трафика в нерабочее время). Приложения, соответствующие вредоносному трафику, называют нежелательными. Это могут быть потенциально опасные приложения. У разных сетевых приложений (для использования социальных сетей, служб обмена мгновенными сообщениями, служб обмена файлами, одноранговых служб и др.) разные риски безопасности. Они могут ставить под угрозу данные и системные активы, влиять на производительность труда сотрудников и использовать пропускную способность сети.

Таким образом проблема контроля доступа к Интернет ресурсам актуальна и имеет важное значение по следующим основным причинам:

- блокирование доступа к нелегальной (экстремистской, антисоциальной и другой) информации;
- предотвращение использования Интернет ресурсов не по назначению, в частности, ограничение и контроль доступа к развлекательным и другим ресурсам для личного пользования;
- предотвращение утечки конфиденциальной информации через Интернет.

Классификация сетевого трафика позволяет обеспечить ясное понимание типа трафика, проходящего через сеть. Она является наиболее существенной частью современных сетевых систем. Для удобства управления администраторы сетевых систем всегда стараются получить точное и ясное соответствие сетевых приложений и создаваемого им трафика, тем самым обеспечив полноценный контроль над теми приложениями, которые используют их сеть.

Ограниченность традиционных подходов классификации трафика на основе номеров портов и нагрузки привела к совершенствованию алгоритмов машинного обучения, опираясь на характеристики трафика на уровне как потоков так и пакетов [1–5]. При наличии набора поме-

ченных тренировочных данных эта задача в большинстве работ формулируется как мультиклассовая классификация с учителем, а полученные при этом результаты показывают, что методами машинного обучения можно достичь высокой точности предсказания. Однако, некоторые свойства таких классификаторов оказываются проигнорированы, причем самым критичным из них является способность идентифицировать неизвестный трафик.

Большинство известных работ посвященных проблеме классификации трафика [6–10] опускают фундаментальное требование определения неизвестного типа трафика. В одних случаях неизвестный трафик полностью исключается при проектировании классификаторов, осуществляющих мультиклассовую классификацию с учителем в условиях только известных классов приложений. В других случаях неизвестный трафик не присутствовал в большинстве экспериментов, в которых классификаторы обучались на данных из ограниченного числа классов приложений и тестировались с помощью других данных из тех же известных классов.

Только в нескольких работах проводилось тестирование классификатора на предмет работы с неизвестным трафиком для различных целей. Так в [10–11], трафик неизвестных протоколов был использован для тестирования одноклассовых классификаторов. В [12] внимание было сфокусировано на задаче распределения недостающих протоколов по категориям.

Классификаторы, основанные на статистике, были использованы в [12] для анализа трафика, который не могли распознать средства DPI, и который мог принадлежать как к одному из известных классов (но пропущенного DPI), так и к неизвестному протоколу. Для осуществления этой задачи был использован внутренний индикатор алгоритма C4.5 — уровень доверия каждого из прогнозов, а принимались только те решения, у которых этот показатель был выше 95%.

В итоге, несмотря на большое количество работ, осталось не ясным, можно ли использовать алгоритмы машинного обучения с учителем для создания классификаторов, способных не только разделять объекты по нужным классам, но также и идентифицировать их из остального фонового или неизвестного трафика.

Целью работы является исследование эффективности алгоритмов классификации приложений сетевого трафика в условиях наличия фонового трафика

Классификация сетевого трафика с учителем

В контексте классификации сетевого трафика, объектом классификации являются сетевые потоки, состоящие из последовательности сетевых пакетов, которыми обмениваются пара узлов с целью межпроцессного взаимодействия через компьютерные сети. В частности, Интернет-

потоки могут быть определены как однонаправленный и двунаправленный потоки.

Однонаправленный поток — последовательность пакетов, имеющих 5 общих параметров, включающих сетевой адрес источника, сетевой адрес получателя, номер порта источника, номер порта получателя и протокол транспортного уровня {srcIP, dstIP, srcPort, dstPort, Protocol}.

Двунаправленный поток (или просто поток). Поток — пара однонаправленных потоков, идущих в противоположных направлениях между двумя узлами, которые можно идентифицировать по их адресу сокета {srcIP, srcPort, Protocol} и {dstIP, dstPort, Protocol}. Все потоки, анализируемые в данной работе, являются двунаправленными. Направление потока определяется по первому захваченному пакету в потоке.

При статистической классификации сетевого трафика, объекты потоков описываются измеренными значениями определенного набора атрибутов, которые затем используются для обучения и классификации. В результате каждый объект представляет собой вектор признаков $X = (x_1, \dots, x_d)$, который может считаться точкой данных в d -мерном пространстве признаков, где d — количество признаков.

Набор признаков как правило состоит из некоторых наблюдаемых характеристик пакетного уровня или уровня потоков трафика, характеризующие отличительное поведение и внутреннюю природу сетевых приложений.

Путем измерения набора пакетов и байтов, передаваемых в потоке можно определить небольшой по размеру набор признаков, а также максимальное, минимальное, среднее значение и стандартное отклонение длины пакета и межпакетного интервала (табл. 1).

Таблица 1

Простые атрибуты трафика

Что наблюдается	Статистика	Количество атрибутов
Пакеты	Количество пакетов	2
Байты	Объем байтов	2
Размер пакета	Мин., макс., среднее знач., станд. отклонение	8
Межпакетный интервал	Мин., макс., среднее знач., станд. отклонение	8
Всего		20

Машинное обучение с учителем представляет собой двухэтапный процесс.

Первый этап — обучение, при котором на вход обучающего алгоритма поступает тренировочный помеченный набор данных $D = \{(x_i, c_i)\}_{i=1}^{N_i}$, где $x_i = (x_1, \dots, x_d) \in R^d$ — это вектор признаков для объекта, а $c_i \in C = \{\omega_1, \dots, \omega_k\}$ —

метка класса объекта (d и k — количество признаков и классов соответственно). На основе набора данных алгоритм выделяет классификационную модель (вероятностную модель или набор правил классификации), которая может считаться функцией, размечающей входной вектор признаков в выходную метку класса, т.е. $F(x): R^d \rightarrow C$.

Второй этап — тестирование (или онлайн-классификация), при котором классификатор используется для предсказания класса приложения новых объектов потоков.

Возможные способы классификации:

1. На основе номеров порта: определяются номера портов протоколов транспортного уровня (TCP или UDP), и на основе него определяется приложение, создавшее трафик. Плюсы: быстрота работы, простота реализации. Минусы: низкая точность.

2. Анализ содержимого (нагрузки) пакетов: анализируется содержимое пакетов, ищутся сигнатуры, характерные для определенных приложений. Плюсы: высокая точность. Минусы: невысокая скорость работы, при зашифрованном содержимом пакетов метод неприменим.

3. Анализ статистических данных потоков: анализируются статистические свойства потоков, для классификации используются алгоритмы машинного обучения. Плюсы: высокая скорость и точность. Минусы: необходимо иметь предварительно классифицированную обучающую выборку.

Большинство алгоритмов машинного обучения с учителем спроектированы для обучения бинарных или мультиклассовых классификаторов [13]. На основе обучающего набора данных, состоящего из объектов обоих классов бинарные (или биномиальные) классификаторы выбирают между двумя классами объектов. Соответственно мультиклассовые (или мультиномиальные) классификаторы разделяют объекты на множество классов в соответствии с тренировочным набором данных, состоящим из объектов всех классов. Оба типа классификаторов основаны на двух предположениях.

Во первых — все классы известны заблаговременно. Во вторых — для каждого класса имеется эффективный и показательный набор данных.

Другими словами, классификаторы с учителем неспособны определить объект неизвестного класса, не представленного в обучающей выборке. В то же время, идентификация неизвестного типа трафика является самым важным требованием в современной классификации сетевого трафика поскольку, в связи с эволюцией Интернета появляются новые приложения и протоколы, новые типы трафика, которые либо неизвестны, либо представлены не полностью на момент обучения. С другой стороны, даже для существующих приложений и протоколов очень тяжело и дорого получить полноценный помеченный набор данных, характеризующих каждый класс.

Таким образом, чтобы построить практичный классификатор трафика методами машинного обучения с учителем, нужно быть очень осторожными с определением класса и построением тренировочного набора.

Критерии оценки качества классификации

Получили распространение несколько численных критериев оценки качества классификаторов [1–2, 13]. В работе использовались такие метрики, как Precision (Точность), Recall (Полнота), F-Measure (F-мера) и AUC (Area Under Curve) — площадь под кривой ROC [14, 20].

Эти метрики вычисляются на основании результатов классификации и полученных показателей TP, FP, TN и FN:

- TP — True Positive (Истинно Положительный) — означает, что объект был правильно отнесен к рассматриваемому классу;
- FP — False Positive (Ложно Положительный) — означает, что объект был отнесен к классу, которому на самом деле не принадлежит;
- TN — True Negative (Истинно Отрицательный) — объект не относится к рассматриваемому классу и был верно классифицирован как объект не этого класса;
- FN — False Negative (Ложно Отрицательный) — объект ошибочно классифицируется как экземпляр не данного класса, хотя на деле принадлежит ему.

Precision и recall являются метриками, которые используются при оценке большинства алгоритмов классификации.

Точность в пределах одного класса вычисляется как доля объектов, которые действительно принадлежат данному классу, по отношению ко всем объектам, которые были отнесены к нему:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}.$$

Другой критерий Recall — полнота — показывает долю найденных классификатором объектов класса из всех объектов в выборке трафика, принадлежащих этому классу:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}.$$

Поскольку на практике тяжело достигнуть максимального значения точности и полноты, можно применять метрику, которая объединяет информацию о точности и полноте классификатора. Такой критерий оценки носит название F-меры (F-Measure). Он лучше всего позволяет показать качество классификатора и оценить, как оно меняется при изменении некоторых параметров — в лучшую или в худшую сторону. F-мера вычисляется как гармоническое среднее между Precision и Recall:

$$F - \text{Measure} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}.$$

Для визуальной оценки качества классификации, удобно пользоваться ROC — кривой (Receiver Operating Characteristic) — рабочей характеристикой приемника, также известная как кривая ошибок, которая отображает соотношение между долей TPR и FPR. TPR (True Positive Rate) — наиболее простая метрика оценки классификатора, показывающая качество разделения классов алгоритмом, вычисляется выражением:

$$\text{TPR} = \frac{\text{TP} + \text{FN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}.$$

Метрика — FPR (False Positive Rate), вычисляется по формуле:

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}}.$$

Количественный показатель ROC — кривой называется AUC (Area Under Curve) — площадь под кривой, соответственно представляет собой площадь фигуры, ограниченной ROC-кривой. Чем выше этот параметр, тем выше и качество классификатора. Стоит заметить, что при AUC = 0.5, вероятность верного принятия решения классификатором будет составлять 50%, что является по своей сути случайным угадыванием. Естественно, в таком случае классификатор не может быть применен для выполнения своей задачи.

Условия проведения эксперимента

Для сбора трафика использовалась машина с ОС Ubuntu 16.04 при помощи программы sniffера (tcpdump). На этапе анализа собранного трафика и формирования выборок (обучающей и тестирующей) трафика для каждого приложения формировались только выборки для выбранных приложений, трафик остальных приложений (фоновый трафик) не рассматривался. Каждой полученной выборке присваивалось название приложения. Так как классификация производилась по потокам то для обучения так же использовались потоки. Варьируя количество потоков в обучающей выборке, экспериментально определялось необходимое количество потоков для заданных приложений и алгоритмов и влияние фонового трафика на качество классификации.

Анализировались следующие группы приложений:

- Web — протоколы просмотра web-сайтов — http, https; ftp — протокол для передачи файлов ftp; mail — протоколы для передачи электронной почты — SMTP, POP3, IMAP; p2p — протоколы приложений, использующие пиринговые сети для передачи файлов;

Использовались следующие алгоритмы машинного обучения: C4.5 [15]; Random Forests [16]; Support Vector Machine (SVM) [17]; Bagging [18]; Adaptive Boost [19].

Для каждого приложения были сформированы две выборки. Одна из выборок использовалась для обучения

(построения модели классификатора), а вторая для тестирования качества алгоритмов (табл. 2). В выборках присутствовал фоновый трафик, содержащий 221 поток и состоящий из 3212 пакетов. Фоновый трафик включал различные приложения, такие как DNS, Skype, Games и трафик системных приложений.

Таблица 2

Обучающие выборки

Тип приложений	Объем обучающей выборки		Объем тестирующей выборки	
	потоков	пакетов	потоков	пакетов
Ftp	587	285934	1010	245183
mail	533	319769	565	322829
P2p	587	642817	767	932525
web	549	33697	920	51862

Выбор атрибутов

При анализе потоков собирались различные данные о характеристиках потока (его продолжительность, количество переданных данных, максимальный и минимальный размеры пакетов, и др.). Всего таких атрибутов было более 30 (табл. 3).

Для улучшения качества классификации и снижения времени на обучение и классификацию каждого отдельного потока определялось, какие атрибуты необходимы, а какие можно не учитывать.

Для определения необходимого количества атрибутов, использовались методы фильтрации атрибутов. Фильтрация атрибутов — процесс выделения наиболее релевантных атрибутов для дальнейшего построения классификатора. Фильтрация атрибутов позволяет уменьшить время обучения и повысить эффективность алгоритмов классификации. Выбор атрибутов осуществлялся методом филь-

Таблица 3

Полный список атрибутов потоков

№	Название	Описание
1	is_tcp	протокол транспортного уровня (1 - TCP, 0 - UDP)
2	max_iat	максимальный межпакетный интервал
3	min_iat	минимальный межпакетный интервал
4	med_iat	медианное значение межпакетного интервала
5	mean_iat	среднее значение межпакетного интервала
6	var_iat	среднеквадратическое отклонение межпакетного интервала
7	total_packet_src	количество пакетов от источника
8	prop_packet_src	доля пакетов источника от общего количества пакетов в потоке
9	total_data	общее количество переданных данных
10	max_src_data	максимальный размер пакета отправителя
11	min_src_data	минимальный размер пакета отправителя
12	med_src_data	медианный размер пакета от отправителя
13	mean_src_data	средний размер пакета отправителя
14	var_src_data_ip	среднеквадратическое отклонение размера пакета отправителя
15	prop_src_data	доля данных, переданных отправителем в общем количестве данных потока
16	total_packet_dst	количество пакетов, переданных от получателя
17	prop_packet_dst	доля пакетов получателя от общего количества пакетов в потоке
18	max_dst_data	максимальный размер пакета от получателя
19	min_dst_data	минимальный размер пакета получателя
20	med_dst_data	медианный размер пакета получателя
21	mean_dst_data	средний размер данных в пакете от получателя
22	var_dst_data	среднеквадратическое отклонение размера пакета получателя

Продолжение табл. 3

23	prop_dst_data	доля данных, переданных получателем в общем количестве данных потока
24	total_packets	общее количество пакетов
25	src_to_dst_ratio_packets	отношение количества пакетов источника к количеству пакетов от получателя
26	total_data	общее количество переданных данных
27	src_to_dst_ratio_data	отношение размера данных, переданных источником к размеру данных, переданных получателем
28	max_data	максимальное значение размера данных в потоке
29	min_data	минимальное значение размера данных в потоке
30	med_data	медианное значение размера данных в потоке
31	mean_data	среднее значение размера данных в потоке
32	var_data_ip	среднеквадратическое отклонение значения размера данных в потоке
33	min_src_iat	минимальный интервал между пакетами отправителя
34	max_src_iat	максимальный интервал между пакетами отправителя
35	mean_src_iat	средний размер интервала между пакетами отправителя
36	min_dst_iat	минимальный интервал между пакетами получателя
37	max_dst_iat	максимальный интервал между пакетами получателя
38	mean_dst_iat	средний размер интервала между пакетами получателя

трации атрибутов, основанным на корреляции (Correlation Feature Selection) [21]. Метод базируется на гипотезе о том, что «хорошее» множество атрибутов состоит из атрибутов, имеющие сильную корреляцию с классом, но слабую друг с другом. Для оценки множества S , состоящего из k атрибутов используется следующее выражение:

$$Merit_{S_k} = \frac{kr'_{cf}}{\sqrt{k + k(k-1)r'_{ff}}}$$

где r'_{cf} — среднее значение корреляции атрибут-класс, а r'_{ff} — среднее значение корреляции между атрибутами

в заданном множестве. В результате работы алгоритма, были выбраны атрибуты (табл. 4).

Влияние объема обучающей выборки на эффективность классификации

Ниже представлены полученные экспериментально зависимости изменения характеристики F-score (взвешенное среднее precision и recall) от количества потоков заданного приложения (а-г) в обучающей выборке в отсутствии ФТ (рис. 1).

Видно, что в отсутствии ФТ объем обучающей выборки лежит в интервале 50 (для приложений типа mail и ftp) до

Таблица 4

Описание выбранных атрибутов

Название атрибута	Описание
max_dst_iat	Максимальный интервал между пакетами получателя
min_src_iat	Минимальный интервал между пакетами отправителя
max_src_iat	Максимальный интервал между пакетами отправителя
min_dst_data	Минимальный размер пакета получателя
max_dst_data	Максимальный размер пакета получателя
max_src_data	Максимальный размер пакета отправителя
mean_src_data	Средний размер пакета отправителя

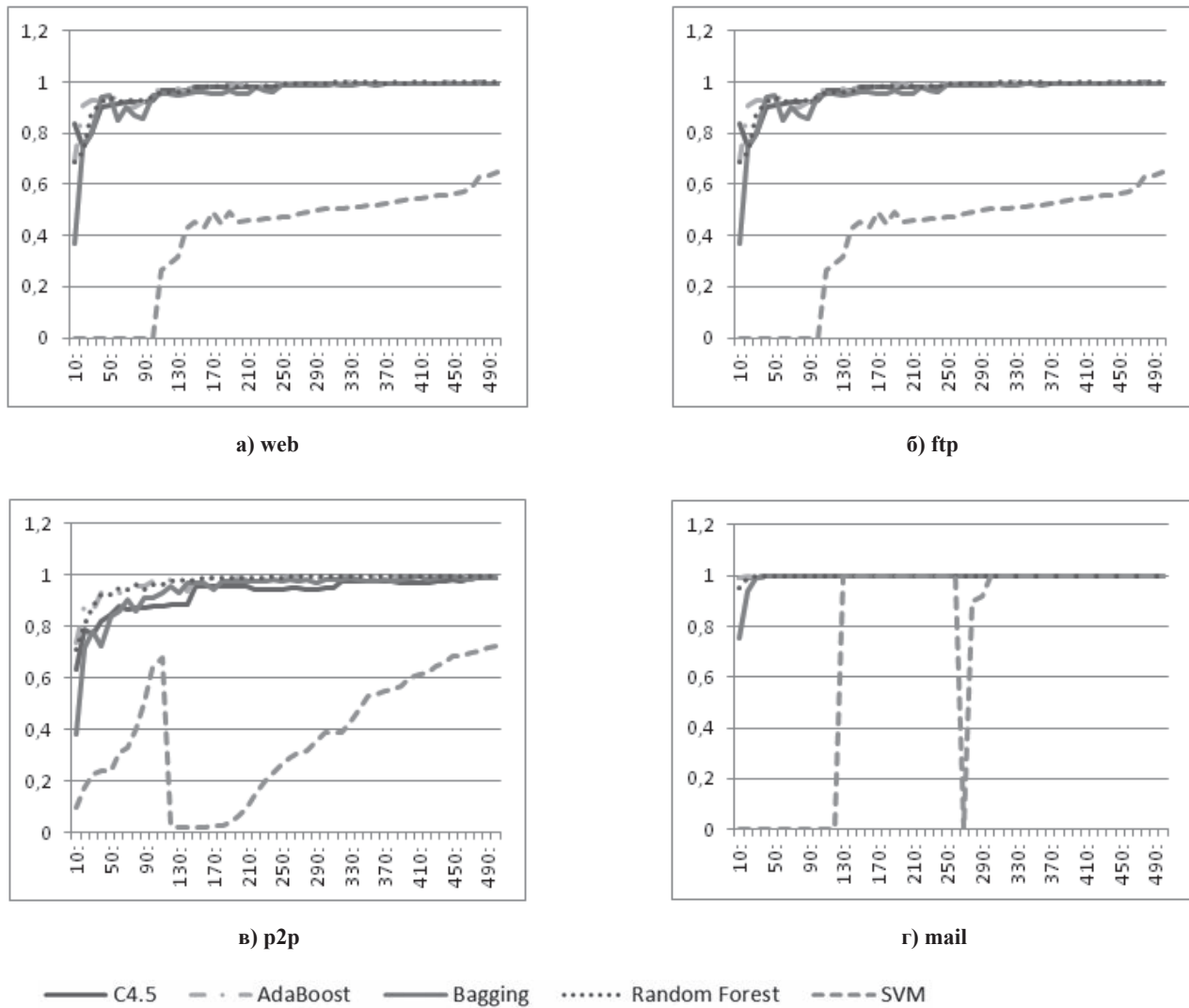


Рис. 1. Изменение характеристики F-score в зависимости от количества потоков заданного приложения (а-г) в обучающей выборке

170–200 (для приложений p2p и web). Наилучшие результаты дают алгоритмы C4.5; Random Forests; Bagging и Adaptive Boos. Наихудшие результаты показывает алгоритм SVM.

Влияние фонового трафика на качественные характеристики классификации

Сравнение трех характеристик precision, recall и F-score при максимальном количестве потоков в обучающей выборке представлены ниже (рис. 2). За исключением SVM, все алгоритмы показали примерно одинаковые результаты.

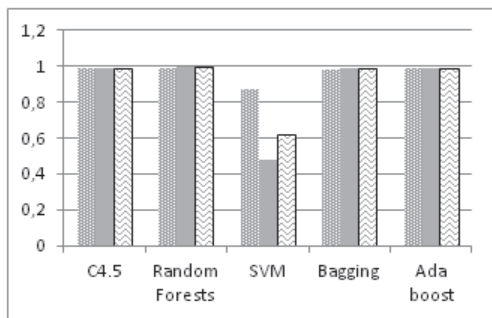
Ниже представлено сравнение тех же трех характеристик при максимальном количестве потоков в обучающей выборке в случае наличия ФТ (рис. 3).

Видно, что качество классификации в условиях наличия ФТ снижается для всех рассматриваемых алгоритмах классификации. Однако поскольку алгоритмы C4.5,

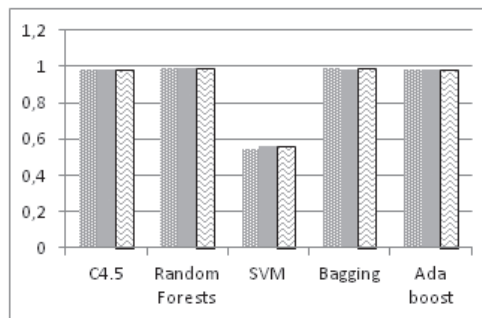
Random Forests, Bagging и AdaBoost использует деревья принятия решений — одно в случае (C4.5) или множество, то их характеристики остаются достаточно высокими и отличаются незначительно. Напротив, поскольку SVM использует принципиально иной подход — строит отдельные классификаторы для каждой комбинации классов то качество этого алгоритма, то результаты показали, что для него экстенсивное увеличение объема обучающей выборки не приносит значительного улучшения результатов.

Рассмотрим зависимость характеристик характеризующих качество классификации (precision и recall) от объема тестирующей выборки в условиях наличия ФТ (рис. 4) и (рис. 5).

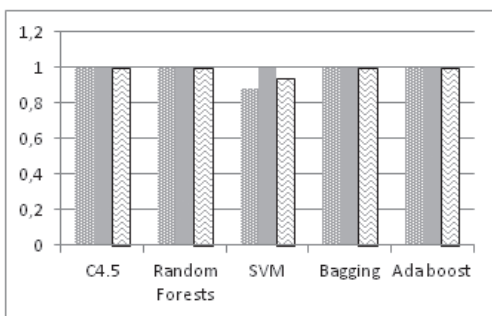
Как видно, фоновый трафик заметно снижает характеристики precision. Так для приложения web она находится на уровне 0,8, для приложения p2p — на уровне 0,85.



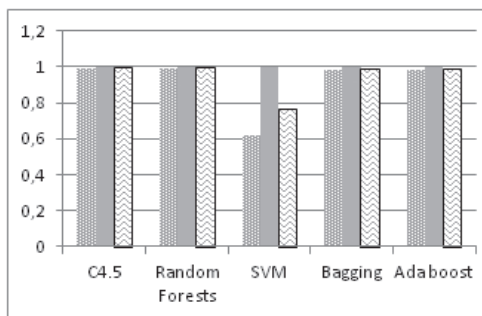
a) web



b) p2p

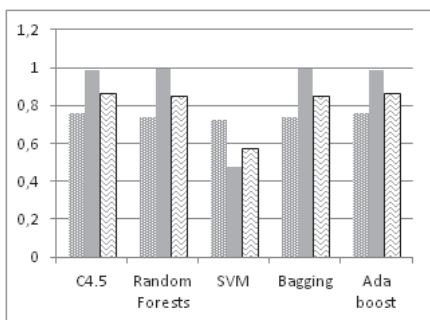


б) ftp

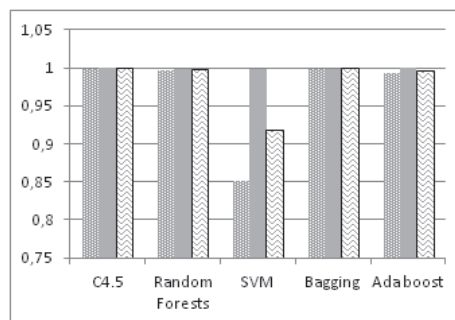


г) mail

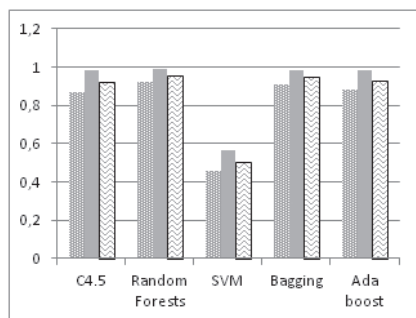
Рис. 2. Сравнение характеристик (precision, recall, F-score) для всех приложений (а-г) при максимальном количестве потоков в обучающей выборке



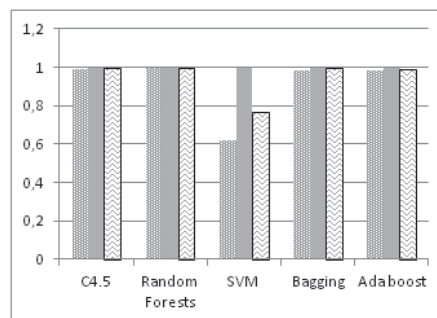
a) web



в) p2p



б) ftp



г) mail

Рис. 3. Сравнение характеристик (precision, recall, F-score) для всех приложений (а-г) при максимальном количестве потоков в обучающей выборке и наличии ФТ

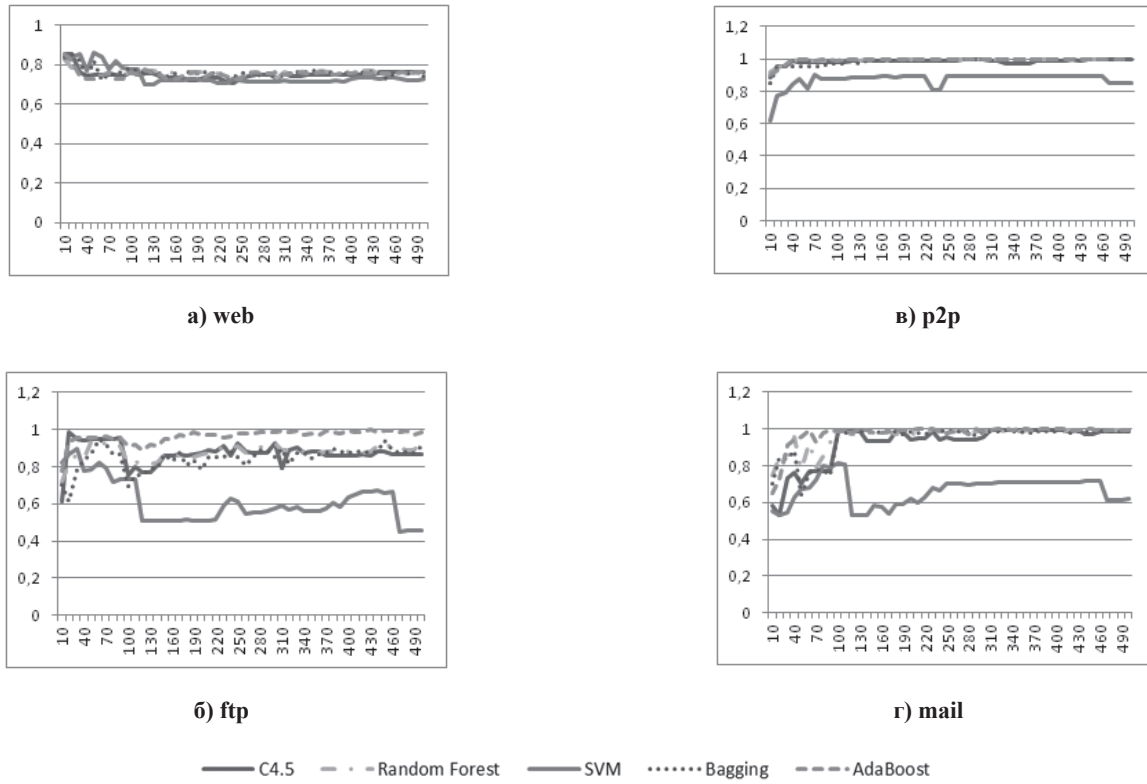


Рис. 4. Изменение характеристики precision для заданного приложения(а-г) в зависимости от количества потоков в обучающей выборке

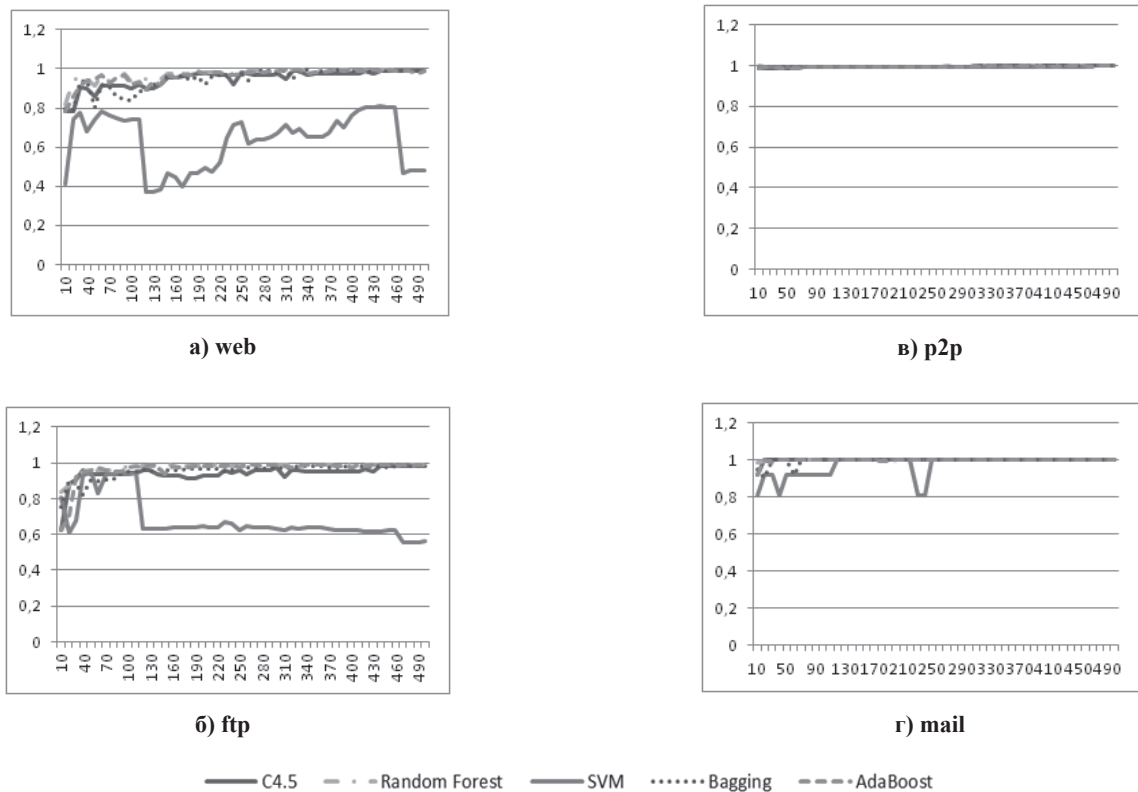


Рис. 5. Изменение характеристики recall для заданного приложения(а-г) в зависимости от количества потоков приложений в обучающей выборке

В результате, большинство потоков фонового трафика классифицируется как web или р2р.

Из зависимостей (рис. 5), видно что фоновый трафик слабо влияет на характеристику recall.

Заключение

Атрибуты для классификации можно выбрать при помощи методов фильтрации атрибутов, например методом CFS (Correlation Feature Selection). Были выбраны 7 атрибутов, которые использовались для классификации.

Проведенные измерения зависимости характеристик классификации precision, recall и F-score от количества потоков в обучающей выборке показали, что при отсутствии фонового трафика достаточное количество потоков для точной классификации 300 и более. Количество потоков в обучающей выборке сильнее влияет на характеристику recall, чем на precision.

Учет наличия фонового трафика, приводит к снижению характеристики precision, которое нельзя компенсировать увеличением количества потоков в обучающей выборке. На характеристику recall фоновый трафик влияет слабо.

В целом, по результатам обучения и тестирования разных алгоритмов МО для классификации трафика, можно сказать, что алгоритм. Random Forest и C4.5 показали наилучшие результаты,

Классификация фонового трафика показала, что алгоритмы МО с учителем, качество работы которых полностью основывается на полноте и достоверности обучающих выборок данных, не способны определить новые, неизвестные данные, что ведёт к неминуемым и критичным ошибкам классификации.

Естественным развитием в данном направлении является применение иных алгоритмов обучения или же методов кластеризации, предназначенных для определения и разграничения неизвестных типов трафика, которые затем анализируются и классифицируются.

Литература

1. Шелухин О. И., Калугин Ю. А. Влияние «прореживания» пакетов на качество классификации потоков сетевого трафика методами машинного обучения // *Нейрокомпьютеры: разработка, применение*. 2016. № 4. С. 14–24.
2. Шелухин О. И., Симомян А. Г., Ванюшина А. В. Эффективность алгоритмов выделения атрибутов в задачах классификации приложений при интеллектуальном анализе трафика // *Электросвязь*. 2016. № 11. С. 45–52.
3. Костин Д. В., Шелухин О. И. Сравнительный анализ алгоритмов машинного обучения для проведения классификации сетевого зашифрованного трафика // *T-Comm: Телекоммуникации и транспорт*. 2016. Т. 10. № 9. С. 46–52.
4. Шелухин О. И., Симомян А. Г., Ванюшина А. В. Влияние структуры обучающей выборки на эффективность классифи-

кации приложений трафика методами машинного обучения // *T-Comm: Телекоммуникации и транспорт*. 2017. Т. 11. № 2. С. 25–31.

5. Шелухин О. И., Симомян А. Г., Ванюшина А. В. Формирование исходных данных и анализ программного обеспечения для классификации приложений трафика методом машинного обучения // *T-Comm*. 2017. Т. 11. № 1. С. 67–72.

6. Soule A., Salamatia K., Taft N., Emilion R., Papagiannaki K. Flow Classification by Histograms or How to Go on Safari in the Internet // In Proceedings of the joint international conference on Measurement and modeling of computer systems (SIGMETRICS'04/Performance'04). New York, 2004. Pp. 49–60.

7. Moore A. W., Zuev D., Crogan M. Discriminators for Use in Flow-Based Classification: Technical Report RR-05-13 / Department of Computer Science, Queen Mary, University of London, 2005. 14 p.

8. Zuev D., Moore A. W. Traffic Classification using a Statistical Approach // In Proceedings of the 6th international conference on Passive and Active Network Measurement (PAM'05). Boston, MA, USA, 2005. Pp. 321–324.

9. Moore A. W., Zuev D. Internet Traffic Classification Using Bayesian Analysis Techniques // In Proceedings of the 2005 ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS'05). Banff, Alberta, Canada, 2005. Pp. 50–60.

10. Crotti M., Gringoli F., Pelosato P., Salgarelli L. A Statistical Approach to IP-level Classification of Network Traffic // In Proceedings of IEEE International Conference on Communications (ICC'06). Istanbul, Turkey, 2006. Vol. 1. Pp. 170–176.

11. Este A., Gringoli F., Salgarelli L. Support Vector Machines for TCP Traffic Classification // *Computer Networks*. 2009. Vol. 53. No. 14. Pp. 2476–2490.

12. Pietrzyk M., Costeux J.-L., Urvoy-Keller G., En-Najjary T. Challenging Statistical Classification for Operational Usage: the ADSL Case // In Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement Conference (IMC'09). Chicago, Illinois, USA, 2009. Pp. 122–135.

13. Witten I. A., Frank E. *Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations*. 2nd edition. San Francisco: Morgan Kaufmann Publ., 2005. 525 p.

14. Lee Suchul, Kim H., Barman D., Lee Sungryoul, Kim Ch., Kwon T., Choi Ya. NeTraMark: A Network Traffic Classification Benchmark // *ACM SIGCOMM Computer Communication Review*. 2011. Vol. 41. No. 1. Pp. 22–30.

15. Quinlan J. *C4.5: Programs for Machine Learning*. San Francisco: Morgan Kaufmann Publ., 1993. 302 p.

16. Ho T. K. Random Decision Forests // Proceedings of the 3rd International Conference on Document Analysis and Recognition (Montreal, QC, 14–16 August 1995). Washington, IEEE Computer Society, 1995. Vol. 1. 278 p.

17. Cortes. C., Vapnik. V. Support-vector networks // *Machine Learning*. 1995. Vol. 20. Issue 3. Pp. 273–297.

18. Breiman L. Bagging predictors // *Machine Learning*. 1996. Vol. 24. Issue 2. Pp. 123–140.

19. Schapire R.E. The Boosting Approach to Machine Learning: An Overview // MSRI Workshop on Nonlinear Estimation and Classification, 2002. 23 p.

20. Powers D. M. W. Evaluation: From precision, recall and f-measure to roc., informedness, markedness & corre-

lation // Journal of Machine Learning Technologies. 2011. Vol. 2. No. 1. C. 37–63.

21. Mark A. Hall Correlation-based Feature Selection for Machine Learning, 1999. URL <http://www.cs.waikato.ac.nz/~mhall/thesis.pdf> (дата обращения 11.09.2017).

FILTERING UNWANTED APPLICATIONS OF INTERNET RESOURCES FOR INFORMATION SECURITY PURPOSES

OLEG I. SHELUHIN,

Moscow, Russia, sheluhin@mail.ru

MIKHAIL A. SMYCHEK,

Nizhny Novgorod, Russia, m-smychek@mail.ru

AIRAPET G. SIMONYAN,

Moscow, Russia, blackman-05@mail.ru

KEYWORDS: classification of network traffic; machine learning; unwanted applications; information security; background traffic; attributes.

ABSTRACT

The work shows the actual task of controlling access to Internet resources, which has important practical importance: blocking access to illegal, extremist, antisocial information, preventing the leakage of confidential information via the Internet, etc. To solve such problems, methods of machine learning are widely used. Traditional methods for classifying network traffic, based on both port numbers and information load, rely on the direct study of network packets. If there is a complete and tagged training dataset, it is advisable to build a classifier using Machine Learning (ML) and Data Mining technologies, which turned out to be the most effective. It is impossible to create an "ideal" classifier, until the problems existing in this field are solved. First of all, this is the absence of a general, representative set of input data that could become standard for research in this field. Most of well-known studies devoted to the problem of traffic classification, omit the fundamental requirement to determine the unknown type of traffic.

The aim of the paper is to investigate the efficiency of algorithms for classifying network traffic applications in the presence of background traffic.

The novelty of the presented solution is the analysis of the following application groups: Web-protocols for browsing web-sites – http,

https; ftp-protocol for transferring ftp files; mail-protocols for sending e-mail – SMTP, POP3, IMAP; p2p-protocols of applications that use peer-to-peer networks for file transfer using machine learning algorithms: C4.5; Random Forests; Support Vector Machine (SVM); Bagging and Adaptive Boost in the presence of unclassified (background) traffic.

It is shown that the quality of classification in the presence of background traffic is reduced for all classification algorithms under consideration. However, since the algorithms C4.5, Random Forests, Bagging, and AdaBoost are built on the use of decision trees – one in the case of C4.5 or the set, their characteristics remain sufficiently high and differ insignificantly.

REFERENCES

1. Sheluhin O.I., Kalugin Y.A. Vliyaniye Sampling packets na effektivnost klassifikatsii trafika metodami mashinnogo obucheniya. *Journal Neurocomputers*. 2016. Vol. No. 4. Pp. 14–24. (In Russian)
2. Sheluhin O.I., Simonyan A.G., Vanyushina A.V. Algorithms efficiency for attributes isolation in applications classification problem with intelligent traffic analysis. *Electrosvyaz'* [Telecommunications]. 2016. No. 11. Pp. 45–52. (In Russian)

3. Kostin D.V. Sheluhin O.I. Comparison of machine learning algorithms for encrypted traffic classification. *T-Comm*. 2016. Vol. 10. No. 9. Pp. 46-52. (In Russian)
4. Sheluhin O.I., Simonyan A.G., Vanyushina A.V. Influence of training sample structure on traffic application efficiency classification using machine-learning methods. *T-Comm*. 2017. Vol. 11. No. 2. Pp. 25-31.
5. Sheluhin O.I., Simonyan A.G., Vanyushina A.V. Benchmark data formation and software analysis for classification of traffic applications using machine learning methods. *T-Comm*. 2017. Vol. 11. No. 1. Pp. 67-72. (In Russian)
6. Soule A., Salamatia K., Taft N., Emilion R., Papagiannaki K. Flow Classification by Histograms or How to Go on Safari in the Internet. In Proceedings of the joint international conference on Measurement and modeling of computer systems (SIGMETRICS'04/Performance'04). New York, NY, USA, 2004. Pp. 49-60.
7. Moore A., Zuev D., Crogan M. Discriminators for Use in Flow-Based Classification. Technical Report RR-05-13, Department of Computer Science, Queen Mary, University of London, 2005.
8. Zuev D., Moore A.W. Traffic Classification using a Statistical Approach. In Proceedings of the 6th international conference on Passive and Active Network Measurement (PAM'05). Boston, MA, USA, 2005. Pp. 321-324.
9. Moore A.W., Zuev D. Internet Traffic Classification Using Bayesian Analysis Techniques. In Proceedings of the 2005 ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS'05). Banff, Alberta, Canada, 2005. Pp. 50-60.
10. Crotti M., Gringoli F., Pelosato P., Salgarelli L. A Statistical Approach to IP-level Classification of Network Traffic. In Proceedings of IEEE International Conference on Communications (ICC'06). Istanbul, Turkey, 2006. Vol. 1. Pp. 170-176.
11. Este A, Gringoli F., Salgarelli L. Support Vector Machines for TCP Traffic Classification. *Computer Networks*. 2009. Vol. 53. No. 14. Pp. 2476-2490.
12. Pietrzyk M., Costeux J.-L., Urvoy-Keller G., En-Najjary T. Challenging Statistical Classification for Operational Usage: the ADSL Case. In Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement Conference (IMC'09). Chicago, Illinois, USA, 2009. Pp. 22-135.
13. Witten I. H., Frank E., Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations. 2nd edition. San Francisco: Morgan Kaufmann Publ., 2005. 525 p.
14. Lee Suchul, Kim H., Barman D., Lee Sungryoul, Kim Ch., Kwon T., Choi Ya. NeTraMark: A Network Traffic Classification Benchmark. *ACM SIGCOMM Computer Communication Review*. 2011. Vol. 41. No. 1. Pp. 22-30.
15. Quinlan J. *C4.5: Programs for Machine Learning*. San Francisco: Morgan Kaufmann Publ., 1993. 302 p.
16. Ho T.K. Random Decision Forests. Proceedings of the 3rd International Conference on Document Analysis and Recognition (Montreal, QC, 14-16 August 1995). Washington, IEEE Computer Society, 1995. Vol. 1. 278 p.
17. Cortes. C., Vapnik. V. Support-vector networks. *Machine Learning*. 1995. Vol. 20. Issue 3. Pp. 273-297.
18. Breiman L. Bagging predictors. *Machine Learning*. 1996. Vol. 24. Issue 2. Pp. 123-140.
19. Schapire R.E. *The Boosting Approach to Machine Learning: An Overview*. MSRI Workshop on Nonlinear Estimation and Classification, 2002. 23 p.
21. Powers D. M.W. Evaluation: From precision, recall and f-measure to roc., informedness, markedness & correlation. *Journal of Machine Learning Technologies*. 2011. Vol. 2. No. 1. C. 37-63.
21. Mark A. Hall Correlation-based Feature Selection for Machine Learning, 1999. URL: <http://www.cs.waikato.ac.nz/~mhall/thesis.pdf> (date of access 11.09.2017).

INFORMATION ABOUT AUTHORS:

Sheluhin O.I., PhD, Full Professor, Head of Department Information Security of the Moscow Technical University of Communications and Informatics;
 Smychek M.A., PhD, Chief Specialist of Design department of communication networks, JSC "Giprogazcentr";
 Simonyan A.G., PhD, Associate Professor of the chair "Information Security", Moscow Technical University of Communication and Informatics.



НПЦ ИРС

Научно-производственный центр
Информационных региональных систем

► npcirs.ru

Закрытое акционерное общество "Научно-производственный центр информационных региональных систем" является предприятием, разрабатывающим автоматизированные системы специального назначения.

Основными направлениями нашей деятельности являются:

- проектирование, создание и ремонт автоматизированных систем управления и их составных частей, систем обработки данных, программного обеспечения, информационных систем для государственных организаций и коммерческих компаний;
- разработка общесистемного и прикладного ПО, внедрение и сопровождение информационных систем;
- защита информации в системах управления, локальных вычислительных сетях, программно-аппаратных комплексах, телекоммуникационных системах;
- производство и поставка технических средств, в офисном и защищенном исполнении;
- создание, внедрение и сопровождение оперативных и учетных систем любой сложности;
- анализ автоматизированных систем на предмет разработки к ним классификаторов и нормативно-справочной информации;
- разработка проектов и создание глобальных, корпоративных, локальных телекоммуникационных систем и структурированных кабельных сетей.

Создаваемые предприятием средства (комплексы средств автоматизации, программные и программно-информационные комплексы, информационные изделия) эксплуатируются в различных государственных органах: в органах военного управления Министерства обороны РФ, а также на предприятиях, в организациях, в органах местного самоуправления субъектов РФ, занимающихся воинским учетом.

Научные исследования в сфере КНСИ позволяют нам качественно анализировать автоматизированные системы и разрабатывать к ним классификаторы и нормативно-справочную информацию.

На данный момент уже имеющиеся разработки позволяют:

- создавать классификаторы по единым правилам, независимо от их содержания;
- создавать массивы классификационной, нормативно-справочной информации в виде эталонных и контрольных экземпляров;
- создавать и вести централизованный банк УММ классификаторов (нормативные документы кодирования сведений);
- комплектовать массивы КНСИ для поставки на объекты, в части касающейся;
- проводить учет КНСИ и поставку на объекты автоматизации;
- централизованно вносить изменения в КНСИ;
- синхронизировать взаимодействие объектов, использующих классификаторы (КНСИ) и УФД;
- обеспечить совместимость данных баз данных объектов;
- обеспечить обмен базами данных между различными автоматизированными системами с территориально разнесенными источниками информации.

Коллектив ЗАО "НПЦ ИРС" образован на основе коллектива Государственного унитарного предприятия. Унаследовав его опыт научно-производственной деятельности, профессиональные знания коллектива специалистов, который целенаправленно занимается проблематикой автоматизации деятельности должностных лиц органов военного управления Вооруженных Сил РФ и разработкой единого информационного обеспечения автоматизированных систем военного назначения более 15 лет, выполняя как теоретические, так и практические работы в этой области.



doi 10.24411/2409-5419-2018-10045

EMPLOYMENT OF FUZZY NEURAL NETWORKS FORECASTING PROFESSIONAL SUCCESS ACTIVITIES OF THE MILITARY EXPERTS

PETRICH

Dmitriy Olegovich¹

Okhotnikov

Yuriy Yur'yevich²

SHAYMUKHAMEDOV

Shamil' Il'dusovich³

ABSTRACT

In the modern world, the ability of a specialist to adapt to the dynamically changing conditions of his professional activity becomes very important. This task is very important in the training of highly qualified personnel in the higher military educational establishments of the Ministry of Defense of the Russian Federation. The high cost of training qualified military specialists, the high level of requirements imposed on the results of their professional activities, makes it extremely important to solve the problem of forecasting and early evaluation of the success of further professional activities of graduates of higher educational institutions of the Ministry of Defense of the Russian Federation. The success of the professional activity of a graduate is determined by the correspondence of professionally important qualities to the requirements for his future military professional activity.

The most preferred mathematical apparatus for modeling such a class of problems, where there are a lot of indistinctly expressed input data, in the aggregates of which the laws and interrelations between them are hidden, is the apparatus of odd neural networks. The expediency of using fuzzy neural networks is also conditioned by incomplete or indistinct information of preferences, as well as by intuitively formulated rules for solving such problems. To implement the process of evaluating performance and predicting the success of a graduate, it is proposed to consider the class of adaptive networks functionally equivalent to systems of fuzzy reasoning. Such an architecture is called ANFIS. ANFIS is one of the first variants of hybrid neural-fuzzy networks - a neural network of direct signal propagation of a special type. The architecture of the neural-fuzzy network is isomorphic to the fuzzy knowledge base. In neural-fuzzy networks, differential implementations of triangular norms (multiplication and probabilistic OR), as well as smooth membership functions, are used. This allows us to apply fast neural network training algorithms based on the method of back-propagating the error to configure neural-fuzzy networks. ANFIS implements a fuzzy inference system in the form of a five-layer neural network of direct signal propagation.

The use of the proposed approach will help with the selection of the most appropriate and exclusive low-information methodologies for professional and psychological selection, with the selection of the most effective teaching methods. Different preferences can be justified using the methods of one-dimensional and multivariate statistics. After this, the development of an algorithm (a decisive rule) for evaluating occupational fitness is carried out. Most often for these purposes, use multiple regression analysis, based on the relationship of psychophysiological properties with "external criteria," which refers to the quality (success) of training or activity.

KEYWORDS: forecasting; professional activity; a graduate of the military school; fuzzy neural network; regression analysis.

Information about authors:

¹PhD, Senior Lecturer of the Military Space Academy, St. Petersburg, Russian, pdo_1985@mail.ru;

²Lecturer of the Military Space Academy, St. Petersburg, Russian, Georgy-03@mail.ru;

³Postgraduate Student of the Military Space Academy, St. Petersburg, Russian, 28_172@mail.ru

For citation: Petrich D. O., Okhotnikov Yu. Yu., Shaymukhamedov Sh. I. Employment of fuzzy neural networks forecasting professional success activities of the military experts. *H&ES Research*. 2017. Vol. 10. No. 2. Pp. 100-106. doi 10.24411/2409-5419-2018-10045

INTRODUCTION

The ability of different specialists to adapt to the dynamically changing conditions of their professional activity becomes very important in the modern world. Also this problem is very important in the process of highly qualified personnel training in the higher military educational institutions of the Ministry of Defense (MoD) of the Russian Federation (RF). The high cost of training skilled military specialists, a high level of requirements for the performance of their professional activity, causes an extremely high importance of solving the problem of forecasting and early evaluation of success of future professional graduate's activity.

The success of the professional graduate's activity is determined by the relevant professional-important qualities that he possesses the requirements for his future military career. Experience shows that a person does not have the ability to certain professional activities which are not only much longer than the others, and with great difficulty seize this activity, but also often make mistakes and failures are to blame for accidents, accidents and emergency situations. Thus, early forecasting of the development path of a military specialist can help in the most effective organization of his future activities.

Approach to predicting the success of professional activity of military specialists on the basis of fuzzy neural networks

Professional activity of a military specialist is complex activity that appears to a specialist as a constituted way of doing something that has a normatively established character. Professional activity is objectively complex, so it is difficult to master, requires a long period of theoretical and practical training [5].

The success of the professional activity of a specialist is determined by his readiness for a certain type of professional activity.

Readiness for professional activity is a psychological state, pre-start activation of a person, including a person's comprehension of his goals, assessment of existing conditions, the definition of the most probable ways of action, predicting motivational, volitional, intellectual efforts, the probability of achieving results, mobilizing forces, self-hypnosis in achievement of goals [4].

Summarizing this definition, one can consider readiness for professional activity as a multilevel and multifaceted system-structural personal formation of the individual.

Most often, it is common to allocate such components of readiness for professional activity as motivational (positive attitude towards the future profession), orientational (knowledge of the profession), operational (professional thinking, set of skills), volitional (self-regulation and behavior management), evaluative (self-evaluation professional preparedness) [7, 13]. Accordingly, the assessment of a specialist's readiness for professional activity is a necessary action and consists in a

comprehensive evaluation of the system of integrative properties and qualities of the individual, as well as the knowledge, skills and skills of the specialist.

There are many different methods for identifying the most suitable specialists at the stage of vocational selection, assessing the quality of education and improving the final training and performance of graduates, which basically use methods of quantitative assessment, but assessing a specialist's readiness for professional work also implies an assessment of a number of qualitative characteristics that are often are of fuzzy nature, and also have different dimensions, meaning and contribution to the integrated indicator [12]. Thus, the problem of assessing the readiness of specialists for professional activity is reduced to the problem of classifying their states on the basis of a huge amount of initial data. The necessity to take into account the psychological, physiological characteristics of individual individuals, the conditions of their work as a result leads to the task of constructing a separating surface, described by a complex multicriteria function.

Proceeding from the above, it can be concluded that the questions of assessing the readiness of specialists for professional activity are a complex task that can be attributed to the tasks and recognition of objects belonging to overlapping classes. One of the most common ways to solve this class of problems is to use mathematical models of neural fuzzy production networks that connect the capabilities of fuzzy inference systems and neural networks [12].

The paper proposes an approach to forecasting the success of professional activities of graduates on the basis of a mathematical model of a fuzzy neural network.

This approach allows to link together all the stages of training and evaluation of a specialist, starting with the selection process, the training process and subsequent evaluation of the graduate's career [1]. The adaptive nature of the fuzzy neural network is also important. It is based on a fuzzy logical inference. In addition, it allows to reconfigure the parameters of the membership functions and to train the neural network.

The most preferred mathematical apparatus for modeling such class of problems, where there are a lot of indistinctly expressed input data, in the aggregate of which the laws and interrelations between them are hidden, is the apparatus of fuzzy neural networks. The expediency of using fuzzy neural networks is also due to incomplete or indistinct information of preferences, as well as intuitively formulated rules for solving such problems.

Psychological fitness for a profession is a property of a person, which can be judged by two criteria: successful mastery of the profession and the degree of satisfaction of a person with his labor. Both these criteria are relative, and sometimes subjective. Nevertheless, these criteria allow us to approach the characterization of professional suitability and subsequently evaluate the success of professional activity. At the very first

stage, the preliminary professional selection of cadets, taking into account the peculiarities of their future professional activity, is very important.

The basis for making an expert decision in the professional selection is the assessment of professional suitability. Profitability in selection is a likely characteristic reflecting a person's ability to master any professional activity. In the professional selection proficiency can be assessed by several criteria:

- on medical indicators, including on indicators of physical readiness;
- according to the educational qualification (results of the USE);
- with the help of psychological examination;
- taking into account some indicators reflecting the applicant's social status;
- taking into account the achieved level of professional adaptation, etc.

In this case, the forecast of the success of training and follow-up is based on the comparison of information about the requirements of the profession to a person and the psychodiagnostic data obtained, with an emphasis on the evaluation of personal characteristics; on the possibility of targeted improvement and compensation of professionally significant qualities; the likelihood of adaptation to the profession; the possibility of emergence of extreme effects.

Forecasting has a probabilistic evaluation and is based on the study of the structure of the personality, the structure of activity and on the correlation of these structures, which includes a very important component as the process of training the profession.

The second important component of forecasting is the "success of training" — an integral characteristic of the success of the training work. Most often, the success of training is assessed by performance indicators. The average score of training is used "as the most non-differentiated indicator of general abilities". For these purposes, the average score of training is used, and the average academic performance in the cycles of subjects over a long period of time. Assessments of the quality of training students are the results of ongoing monitoring of academic performance, intermediate and final attestation [1].

The third component of forecasting is based on information about the professional activities of graduates. This information is contained in the official responses to the graduates after the first year of their service in the troops. The service review provides an integrated assessment of training and performance through the use of multi-level scales of assessments for the most varied indicators, distributed across seven sections. The Academy is carrying out research to improve the methods of training military specialists, within the framework of which principles for the formation of a final assessment of the training and performance of graduates have been developed. A special computer program allows to automate the process of collecting, processing and analyzing data on submitted service reports [3].

Fuzzy neural networks draw conclusions based on the mathematical apparatus of fuzzy logic, but the parameters of the membership functions are tuned using neural network learning algorithms. Therefore, to select the parameters of such networks, we apply the method of back propagation of the error, originally proposed for training a multilayer perceptron. For this, the fuzzy control module is represented in the form of a multilayer network. Fuzzy neural network, as a rule, consists of four layers: the layer of fuzzification of input variables, the layer of aggregation of activation values of the condition, the layer of aggregation of fuzzy rules and the output layer [8–9, 14–15].

Fuzzy associative rules are tool for extracting regularities from databases that are formulated in the form of linguistic utterances. Here are introduced special concepts of fuzzy transaction, support and reliability of fuzzy associative rules.

Fuzzy inference algorithms differ, mainly, by the kind of rules used, logical operations and the type of defuzzification method. Various models of fuzzy inference have been developed (Mamdani, Sugeno, Larsen, Tsukamoto).

Let us consider in more detail the fuzzy conclusion on the example of the Mamdani mechanism [11]. This is the most common method of inference in fuzzy systems. It uses the minimax composition of fuzzy sets. This mechanism includes the following sequence of actions:

1. The procedure of fuzzification: determine the degree of truth, i. e. the values of the membership functions for the left parts of each rule (prerequisites). For a rule base with m rules, the degrees of truth are denoted

$$A_{ik}(x_k), \quad i = \overline{1, m}, \quad k = \overline{1, n}.$$

2. Fuzzy conclusion. First, the "cut-off" levels for the left side of each rule are determined

$$\lambda_i = \min_k (A_{ik}(x_k)).$$

Next, there are "truncated" membership functions

$$B_i^*(y) = \min(\lambda_i, B_i(y)).$$

3. Composition, or combination of the obtained truncated functions, for which the maximum composition of fuzzy sets is used

$$MF(y) = \max_i (B_i^*(y)),$$

where is the membership function of the final fuzzy set.

4. Defuzzification, or reduction to clarity. There are several methods of defuzzification. For example, the method of the middle center, or the centroid method.

Based on the fuzzy logic inference algorithm, a system of reasoning is constructed (fig. 1).

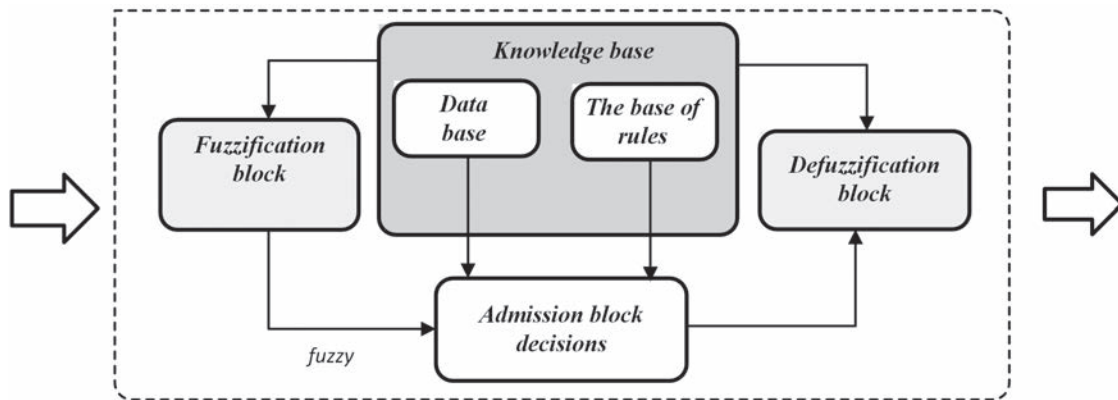


Fig. 1. The system of fuzzy reasoning

The system of fuzzy reasoning consists of five functional blocks:

- a block of fuzzification that converts numerical input values to a degree of compliance with linguistic variables;
- a rule base containing a set of fuzzy rules such as "if something";
- a database in which the fuzzy set membership functions used in fuzzy rules are defined;
- decision-making unit that performs withdrawal operations on the basis of existing rules; — block of defuzzification, which converts the results of output into numerical values.

Traditionally, the rules database and the database are combined into a common block — the knowledge base.

Next we propose to consider the class of adaptive networks functionally equivalent to systems of fuzzy reasoning. This architecture is called ANFIS (an abbreviation Adaptive-Network-Based Fuzzy Inference System — adaptive network of fuzzy inference). ANFIS is one of the first variants of hybrid neural-fuzzy networks — a neural network of direct signal propagation of a special type. The architecture of the neural-fuzzy network is isomorphic to the fuzzy knowledge

base. In neural-fuzzy networks, differentiable implementations of triangular norms (multiplication and probabilistic OR) are used, as well as smooth membership functions. This allows us to apply fast neural network training algorithms based on the method of back propagation of the error to configure neural-fuzzy networks. The architecture and rules for the operation of each layer of the ANFIS network are described below. ANFIS implements a fuzzy inference system in the form of a five-layer neural network of direct signal propagation [6–9].

The purposes of the layers are:

- the first layer — the terms of the input variables;
- the second layer — antecedents (parcels) of fuzzy rules;
- the third layer — the normalization of the degree of implementation of the rules;
- the fourth layer — the conclusion of the rules;
- the fifth layer — the aggregation of the result obtained by different rules.

The network inputs in a separate layer are not allocated. Figure 2 shows an ANFIS network with two input variables (x_1 and x_2) and four fuzzy rules. For linguistic evaluation of the input variable x_1 3 terms are used, for a variable x_2 2 terms are used.

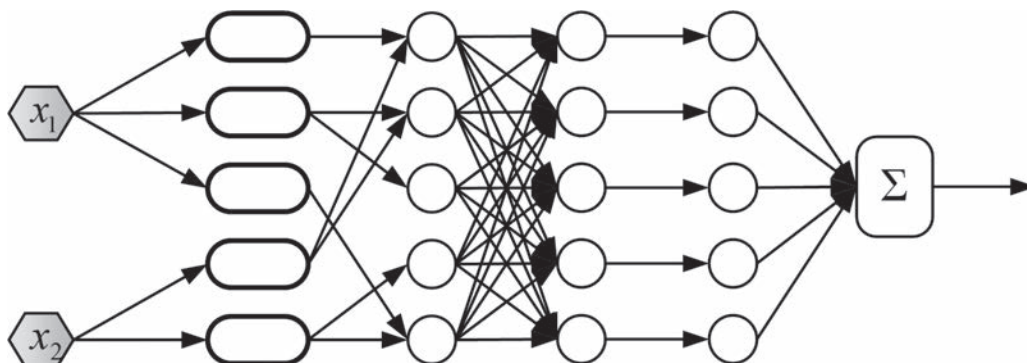


Fig. 2. Network example

The ANFIS network works as follows [8]:

1. The 1st layer is the terms of the input variables. Each node of the first layer represents one term with the membership function. The number of nodes of the first layer is equal to the sum of the powers of the term-sets of the input variables. The output of the node is the degree to which the value of the input variable belongs to the corresponding fuzzy term. The parameters of this layer refer to the so-called prerequisites parameters.

2. The second layer is the antecedents of the fuzzy rules. Each node of a given layer is a fixed node multiplying input signals, with the output value of the node being the weight of a rule: The number of nodes of the second layer is m . Each node of this layer corresponds to one fuzzy rule. The node of the second layer is connected to those nodes of the first layer, which form the antecedents of the corresponding rule. Therefore, each node of the second layer can receive from 1 to n input signals. The output of the node is the degree of execution of the rule, which is calculated as the product of the input signals.

3. The third layer is the normalization of the degree of fulfillment of the rules. Each i -th node of this layer determines the ratio of the weight of the i -th rule to the sum of the weights of all rules: The output signals of the 3rd layer are called normalized weights. The number of nodes of the third layer is also equal to m . Each node in this layer calculates the relative degree of fuzzy rule execution.

4. 4th layer — the conclusion of the rules. The nodes of a given layer are defined by linear functions of the belonging of the output variables. The number of nodes of the fourth layer is also equal to m . Each node is connected to one node of the third layer, and also to all inputs.

5. The 5th layer is the aggregation of the result obtained according to different rules. The only node of this layer is a fixed node in which the total output value of the adaptive network Y is calculated as the sum of all input signals.

CONCLUSION

The use of the proposed approach will help with the selection of the most appropriate and the exclusion of little-informative methods of professional and psychological selection, with the selection of the most effective teaching methods. Different preferences can be justified using the methods of one-dimensional and multivariate statistics. After this, the development of an algorithm (a decisive rule) for evaluating occupational fitness is carried out. Most often for these purposes, use multiple regression analysis, based on the relationship of psychophysiological properties with "external criteria," which refers to the quality (success) of training or activity.

REFERENCES

1. Baibakov M.N., Bobrovskaya A.A. Prognozirovanie uspehnosti professional'noy deyatel'nosti kursantov uchebnykh zavedeniy GPS MChS Rossii na osnove matematicheskoy modeli

nechetkoy neyronnoy seti [Predicting the success of professional activity of cadets of educational institutions of State Fire Service of EMERCOM of Russia on the basis of mathematical model of fuzzy neural network]. *Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii "Podgotovka kadrov v sisteme preduprezhdeniya i likvidatsii posledstviy chrezvychaynykh situatsiy"* [Materials of the International Scientific and Practical Conference "Training of personnel in the system of prevention and liquidation of consequences of emergency situations" (St. Petersburg, October 24, 2013)]. St. Petersburg: State Fire Service University of EMERCOM of Russia, 2013. Pp. 127–130. (In Russian)

2. Viktorova E. V. Application of fuzzy neural networks for technical diagnostics of road vehicles. *Bulletin of Kharkov National Automobile and Highway University*. 2012. Vol. 56. Pp. 98–102. (In Russian)

3. Golubev M. A., Voronkov I. Yu., Mashkov O. G. Metodika otsenki udovletvorennosti zakazchika kachestvom podgotovki vypusknikov akademii na osnove analiza sluzhebnykh otzyvov [Methods of assessment of attorney-client satisfies the quality of training of graduates of the Academy on the basis of office reviews analysis]. *Trudy Voenno-kosmicheskoy akademii imeni A. F. Mozhayskogo* [Proceedings of the A. F. Mozhayskiy Military Space Academy]. 2014. Vol. 644. Pp. 207–211. (In Russian)

4. *Gotovnost' k professional'noy deyatel'nosti. Slovar' po proforientatsii i psikhologicheskoy podderzhke* [Readiness for professional activity. Dictionary on career counseling and psychological support]. URL: https://career_counseling_support.academic.ru/75/Reportability_pro_professional_action. (date of access 01.10.2017).

5. Druzhilov S. A. Psihologija professionalizma cheloveka: integrativnyj podhod [Psychology of human professionalism: an integrative approach]. *Zhurnal prikladnoj psihologii* [Journal of Applied Psychology]. 2003. No. 4–5. Pp. 35–42. (In Russian)

6. Dudkin A. A. Fuzzy neural network for the analysis of the topology of integrated microcircuits. *Artificial Intelligence*. 2015. No. 1–2. Pp. 79–86.

7. Zyryanova A. V. Readiness for professional activity of specialists in the sphere of culture: essence and structure. *Pedagogy of art*. 2012. No. 4. URL: <http://www.art-education.ru/AE-magazine/> № 4, 2012. (In Russian)

8. Ivaskiv Yu. L., Levchenko V. V., Leshchinsky O. L. Formation of fuzzy learning sets for neural networks in problems of data compression without losses. *Mathematical machines and systems*. 2009. No. 2. Pp. 53–60.

9. Lubentsova E. V. Investigation of algorithms for learning the neuro-fuzzy control system of the biotechnological process. *Scientific journal KubSAU*. 2017. No. 128 (04). Pp. 1–11. (In Russian)

10. Matkovskaya M. O. Investigation of fuzzy inference algorithms in decision-making models. *Izvestiya SFU. Technical Sciences*. 2009. Pp. 240–243. (In Russian)

11. Melkov D.A. Sravnenie algoritmov nechetkogo vyvoda s ispol'zovaniem yazykov standarta MEK [Comparison of fuzzy inference algorithms using the IEC standard languages]. *Young Scientist*. 2013. No. 5. Pp. 74–79. (In Russian)

12. Mikhelkevich V.N., Kravtsov P.G. Comprehensive assessment of graduates' readiness for professional work. *Samara Journal of Science*. 2016. No. 2 (15). Pp. 171–175. (In Russian)

13. Pleshakova O.V. Components of psychological readiness for the professional work of a social worker. *Vestnik Bashkirskogo universiteta* [Bulletin of Bashkir University]. 2007. Vol. 12. No. 3. Pp. 200–203. (In Russian)

14. Soldatova O.P., Lyozin I.A., Lyozina I.V., Kupriyanov A.V., Kirsch D.V. Application of fuzzy neural networks to determine the type of crystal lattices observed on nanoscale images. *Computer Optics*. 2015. Vol. 39. No. 5. Pp. 787–795. doi: 10.18287/0134-2452-2015-39-5-787-794 (In Russian)

15. Soldatova O.P., Lezin I.A. Solution of the classification problem using neural fuzzy production networks based on the Mamdani-Zade model of inference. *Vestnik Samarskogo Gosudarstvennogo Tekhnicheskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki* [Bulletin of the Samara State Technological University. Series Physics and mathematics]. 2014. No. 2 (35). Pp. 136–148. doi: 10.14498/vsgtu1266 (In Russian)

ПРИМЕНЕНИЕ НЕЧЕТКИХ НЕЙРОННЫХ СЕТЕЙ В ПРОГНОЗИРОВАНИИ УСПЕШНОСТИ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ВОЕННЫХ СПЕЦИАЛИСТОВ

ПЕТРИЧ Дмитрий Олегович,

г. Санкт-Петербург, Россия, pdo_1985@mail.ru

ОХОТНИКОВ Юрий Юрьевич,

г. Санкт-Петербург, Россия, Georgy-03@mail.ru

ШАЙМУХАМЕТОВ Шамиль Ильдусович,

г. Санкт-Петербург, Россия, 28_172@mail.ru

КЛЮЧЕВЫЕ СЛОВА: прогнозирование; профессиональная деятельность; выпускник военно-учебного заведения; нечеткая нейронная сеть; регрессионный анализ..

АННОТАЦИЯ

В современном мире большое значение приобретает умение специалиста адаптироваться к динамически изменяющимся условиям своей профессиональной деятельности. Эта задача очень актуальна при подготовке высококвалифицированных кадров в высших военных образовательных учреждениях Министерства обороны Российской Федерации. Высокая стоимость обучения квалифицированных военных специалистов, высокий уровень требований, предъявляемых к результатам их профессиональной деятельности, обуславливает чрезвычайно высокую важность решения задачи прогнозирования и раннего оценивания успешности дальнейшей профессиональной деятельности выпускников вузов Министерства обороны Российской Федерации. Успешность профессиональной деятельности выпускника определяется соответствием профессионально-

важных качеств требованиям, предъявляемым к его будущей военно-профессиональной деятельности.

Наиболее предпочтительным математическим аппаратом для моделирования подобного класса задач, где имеется очень много нечетко выраженных входных данных, в совокупностях которых скрыты закономерности и взаимосвязи между ними, является аппарат нечетких нейронных сетей. Целесообразность использования нечетких нейронных сетей также обусловлена неполной или нечетко выраженной информацией предпочтений, а также интуитивно формулируемыми правилами решения таких задач.

Для реализации процесса оценивания результатов деятельности и прогнозирования успешности выпускника предлагается к рассмотрению класс адаптивных сетей функционально экви-

валентных системам нечетких рассуждений. Подобная архитектура носит название ANFIS. ANFIS является одним из первых вариантов гибридных нейро-нечетких сетей – нейронной сети прямого распространения сигнала особого типа. Архитектура нейро-нечеткой сети изоморфна нечеткой базе знаний. В нейро-нечетких сетях используются дифференцируемые реализации треугольных норм (умножение и вероятностное ИЛИ), а также гладкие функции принадлежности. Это позволяет применять для настройки нейро-нечетких сетей быстрые алгоритмы обучения нейронных сетей, основанные на методе обратного распространения ошибки. ANFIS реализует систему нечеткого вывода в виде пятислойной нейронной сети прямого распространения сигнала.

Использование предлагаемого подхода поможет с выбором наиболее адекватных и исключения малоинформативных методик профессионального и психологического отбора, с селекцией наи-

более результативных методик обучения. Различные предпочтения могут обосновываться применением методов одномерной и многомерной статистики. После этого проводится разработка алгоритма (решающего правила) оценки профпригодности. Наиболее часто для этих целей используют множественный регрессионный анализ, основанный на связях психофизиологических свойств с «внешними критериями», под которыми понимаются качество (успешность) обучения или деятельности.

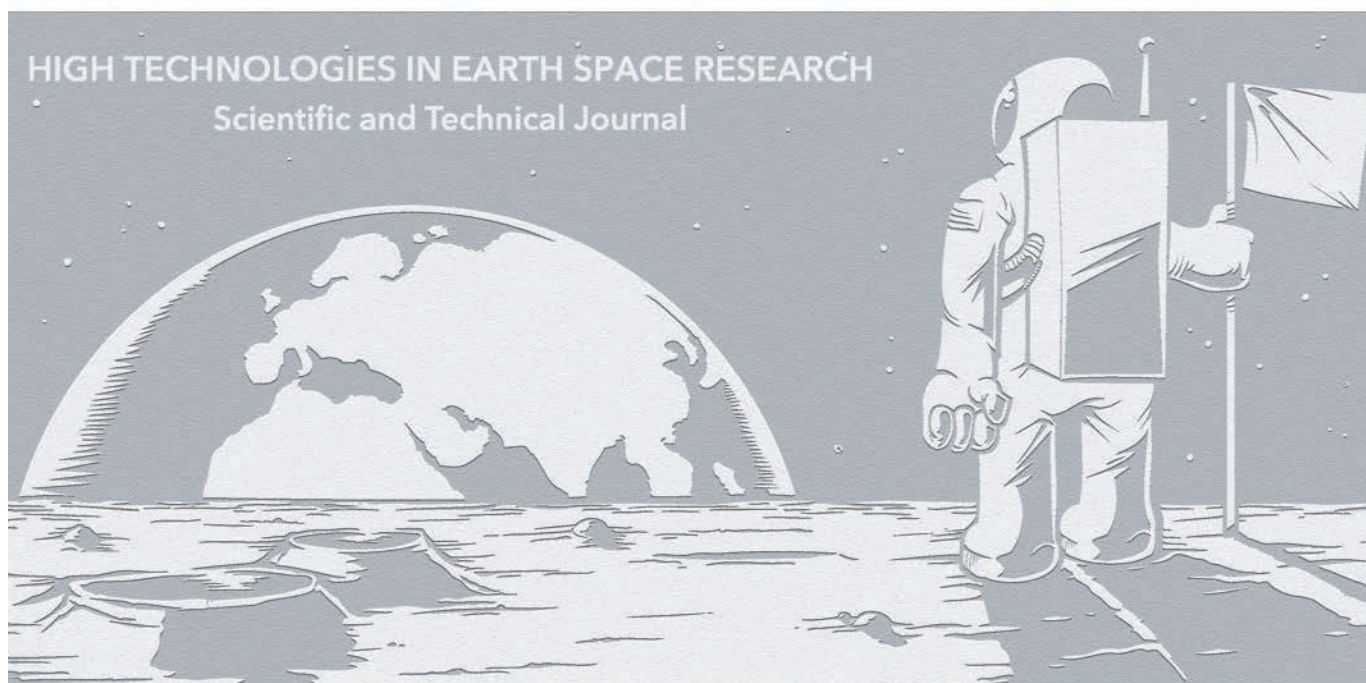
СВЕДЕНИЯ ОБ АВТОРАХ:

Петрич Д.О., к.т.н., старший преподаватель Военно-космической академии имени А.Ф.Можайского;

Охотников Ю.Ю., преподаватель Военно-космической академии имени А.Ф.Можайского;

Шаймухаметов Ш.И., адъюнкт Военно-космической академии имени А.Ф.Можайского.

Для цитирования: Петрич Д.О., Охотников Ю.Ю., Шаймухаметов Ш.И. Применение нечетких нейронных сетей в прогнозировании успешности профессиональной деятельности военных специалистов // Научные технологии в космических исследованиях Земли. 2017. Т. 10. № 2. С. 100-106. doi 10.24411/2409-5419-2018-10045



ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ МАТЕРИАЛОВ

Редакция журнала H&ES Research принимает к публикации статьи на русском и английском языках. Предоставляемая рукопись должна быть актуальной, обладать новизной, отражать постановку задачи, содержать описание основных результатов исследования, выводы, а также соответствовать указанным ниже правилам оформления. Текст должен быть тщательно вычитан автором, который несет ответственность за научнотеоретический уровень публикуемого материала.

Статья предоставляется в электронном виде, единым файлом, имеющим следующую структуру: заглавие статьи, сведения об авторах, аннотация, ключевые слова, текст статьи (включая иллюстрации, таблицы и формулы), пристатейный список литературы, англоязычный блок. Также представляется отдельная папка с экспортированными изображениями рисунков в формате TIFF, EPS по требованиям указанным в п.7.

К статье прилагается экспертное заключение о возможности опубликования статьи в открытой печати и две рецензии кандидатов или докторов наук по профилю планируемой публикации материалов (сканированные копии в электронном виде).

Все материалы высылаются электронной почтой в адрес журнала: HT-ESResearch@yandex.ru.

1. **Статья подготавливается** в редакторе MS Word. Шаблон статьи можно скачать на сайте журнала www.h-es.ru.

2. **Данные об авторе:** фамилия, имя, отчество, ученая степень, звание, должность и полное название организации – места работы, город, страна, адрес электронной почты и почтовый адрес каждого автора полностью.

3. **Объем аннотации** 200–250 слов. Аннотация должна быть информативной (не содержать общих слов), без сокращений, структурированной, отражать основное содержание статьи: предмет, цель, методологию проведения исследований, результаты исследований, область их применения, выводы. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье. Предложения должны начинаться словами: показано, получено, исследовано, предсказано и т.д. и т.п.

4. **Ключевые слова:** от 5 до 7 слов (словосочетаний), разделенных точкой с запятой.

5. **Объем статьи** без аннотации – от 15 до 30 тыс. знаков с пробелами. Рисунки и таблицы в объеме статьи не учитываются.

6. **Формульные выражения** выполняются в редакторе Math Type. Формулы нумеруются в круглых скобках, источники – в прямых. Нумерация формул и приведение в списке источников, на которые нет ссылок по тексту, не допускается. Длина формулы в одну строчку 8–9 см.

Простые формулы и буквенные обозначения величин следует писать в строку обычным текстом. В формулах использовать только буквы латинского и греческого алфавита!

Размеры шрифтов (Size) предварительно перед набором первой формулы установить (в MathType) следующие: кегль основной – 10, крупный индекс – 7, мелкий индекс – 5, крупный символ – 12, мелкий символ – 8. Формулы, не содержащие специальных математических символов, должны быть набраны в тексте (в формате Word). Греческие обозначения, скобки (квадратные и круглые) и цифры всегда набираются прямым шрифтом. Латинские буквы набираются курсивом

как в формулах, так и в тексте, кроме устойчивых форм (max, min, cos, sin, tg, log, exp, det ...).

Нельзя использовать сканированные формулы! Все формулы должны быть набраны вручную!

7. **Рисунки и таблицы** в статье должны быть пронумерованы и снабжены подписями, в тексте статьи должны иметься ссылки на каждый рисунок и таблицу (рис.1 и табл.1). Если рисунок или таблица единственные в статье, то их не нумеруют.

Рисунки должны быть четкими, с хорошо проработанными деталями. Избегать текстовых надписей на иллюстрациях. Заменять их цифровыми обозначениями, которые поясняются в подписи или в основном тексте. Все рисунки прилагаются в виде отдельных файлов в формате TIFF, EPS с разрешением не менее 300 dpi для оригинального размера в печатном издании (для больших рисунков ширина от 14 до 20 см, для маленьких от 7 до 9 см).

8. **Список литературы:** от 15 до 50 наименований. Из них самоцитирований не должно быть более 25%. В числе источников желательны не менее 50 % иностранных источников (для статей на английском языке – 15% российских). Состав источников должен быть актуальным и содержать не менее 8 статей из научных журналов не старше 10 лет, из них 4 – не старше 3 лет.

Ссылки должны быть только на статьи, патенты, книги и статьи из сборников трудов. В списках литературы не размещать ГОСТы, рекомендации, диссертации, авторефераты и другую нормативную и непериодическую документацию. Эти данные можно указывать в теле статьи в скобках или в виде постраничных сносок (если автор непременно хочет указать нормативный документ или сослаться на свою диссертацию). Список литературы оформляется в соответствии с ГОСТ 7.052008. **Образец оформления списка литературы размещен на сайте журнала www.h-es.ru.**

9. **На английском языке** предоставляется: название статьи, фамилия, имя, отчество, информация об авторах (должность, ученая степень, ученое звание, место работы), город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.

Все названия издательств и журналов должны быть транслитерированы, а не переведены. Названия организаций в списках литературы (Труды Академии...) должны быть четко выверены с данными организации и иметь официальное английское наименование, которое указано на их сайте или также транслитерированы. Образец оформления списка литературы размещен на сайте журнала www.h-es.ru.

10. Структура статьи на английском языке

Introduction (введение)

Materials and methods (материалы и методы).

Results and Discussions (результаты и обсуждение).

Conclusions (вывод)

Acknowledgements (благодарности, необязательный раздел)

References (ссылки на использованную литературу)

На русском языке предоставляется: название статьи, фамилия, имя, отчество, информация об авторах (должность, ученая степень, ученое звание, место работы), город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы.

Внимание! Редакция оставляет за собой право отклонить представленные материалы, оформленные не по указанным правилам.

ООО «ИНТЕХ»
ОАО «НПО АНГСТРЕМ»

30 октября 2018
МОСКВА

ВСЕРОССИЙСКАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

ПО ТЕОРЕТИЧЕСКИМ И ПРИКЛАДНЫМ
ПРОБЛЕМАМ РАЗВИТИЯ И СОВЕРШЕНСТВОВАНИЯ
АСУ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

НАУКА И АСУ - 2018

nauka-i-asu.ru

konferencia_asu_vka@mail.ru

при информационной поддержке



НПЦ ИРС

H&ES
RESEARCH



T•Comm
ТЕЛЕКОМУНИКАЦИОННЫЙ ЦЕНТР