ISSN 2412-1363 (Online) ISSN 2409-5419 (Print)

НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

Научно-технический журнал

H&ES RESEARCH

Том 9, № 2–2017

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: • 01.01.00 Математика • 05.11.00 Авиационная и ракетно-космическая техника • 05.11.00 Приборостроение, метрология и информационно-измерительные приборы и системы • 05.12.00 Радиотехника и связь • 05.13.00 Информатика, вычислительная техника и управление.

Учредитель: ООО «ИД Медиа Паблишер». **Издатель:** СВЕТЛАНА ДЫМКОВА.
H&ES Research зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия. Издательская лицензия ПИ № ФС 77-60899.
Язык публикаций: русский, английский.
Периодичность выхода – 6 номеров в год.

Адрес редакции: 111024, Россия, Москва, ул. Авиамоторная, д. 8, офис 512-514; 194044, Россия, СПб, 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.

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.

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: • 01.01.00 Mathematics • 05.07.00 Aviation, space-rocket hardware • 05.11.00 Instrument engineering, metrology and information-measuring devices and systems • 05.12.00 RF technology and communication • 05.13.00 Informatics, computer engineering and control.

Founder: "Media Publisher", LLC. **Publisher:** SVETLANA DYMKOVA.
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 ПИ № ФС 77-60899.
Language of publications: Russian, English.
Periodicity – 6 issues per year.

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 Doroshkevich, ovd@media-publisher.ru, tel.: 8(916) 951-55-36.

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.

HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

Scientific and Technical Journal

HES_Research club55425245 HES-Research

СОДЕРЖАНИЕ

АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

РАДИОТЕХНИКА И СВЯЗЬ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

ПУБЛИКАЦИИ НА АНГЛИЙСКОМ ЯЗЫКЕ

ТЕМАТИЧЕСКИЕ НАПРАВЛЕНИЯ

• Вопросы развития автоматизированных систем управления • Физико-математическое обеспечение разработки новых технологий • Развитие автоматизированных систем управления технологическим процессом • Вопросы исследования космоса • Телекоммуникационные технологии и технические новинки систем подвижной связи • Перспективы развития единого инфокоммуникационного пространства • Использование радиочастотного спектра в системах подвижной связи • Антенно-фидерное оборудование • Спутниковое телевидение, системы спутниковой навигации, GLONASS, построение навигационных систем GPS • Вопросы развития геодезии и картографии • Информационная и кибербезопасность • Вопросы исследования Арктики • Волоконно-оптическое оборудование и технологии • Метрологическое обеспечение • Программное обеспечение и элементная база для сетей связи • Производители, поставщики и дистрибьюторы телекоммуникационного оборудования • Работа отечественных ассоциаций, региональных и координирующих операторов • Правовое регулирование инфокоммуникаций, законодательство в области связи • Экономика связи, конвергенция сетей, универсальные коммуникации • Выставки, форумы, конференции, семинары, интервью (оригинальные и новые проекты, итоги деятельности, проблемы отрасли и пути их решения и т.д.)

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

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

CONTENTS

TOPICAL COLUMNS

• Automated control systems • Physical and mathematical software development of new technologies • Development of automated process control systems • Questions of space exploration • Telecommunication technology and technical innovations of mobile systems • Prospects for unified info communication space • Use of a radio-frequency range in systems of mobile communication • Antenna-feeder equipment • Satellite TV, satellite navigation system, GLONASS, GPS navigation systems construction • Issues of Geodesy and Cartography • Information and cyber security • Questions Arctic research • Fiber-optic equipment and technology • Metrological maintenance • Software and electronic components for communication networks • Manufacturers, suppliers and distributors of telecommunications equipment • National associations, regional and coordinating operators • Legal regulation of Infocomm, legislation in the communication field • Economy of communications, networks convergence, universal communication • Exhibitions, forums, conferences, seminars, interview (original and new projects, results of activity, a problem of branch and a way of their decision, etc.)

JOURNAL H&ES RESEARCH INDEXING

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

Юрию Алексеевичу Гагарину
посвящается

ПЕРВЫЙ НАВСЕГДА

КНИГА «ПЕРВЫЙ НАВСЕГДА»

Институт изучения реформ и предпринимательства издал уникальную подарочную книгу «ПЕРВЫЙ НАВСЕГДА», посвященную юбилею со дня первого полета человека в космос.

Для нашей страны и всего мира полет Гагарина стал национальным триумфом. О судьбе первого космонавта Земли Юрия Гагарина написано множество книг. В этой юбилейной книге сделана попытка приобщить еще несколько новых страниц к летописи истории космонавтики, свидетелями и участниками которой были многие из авторов, выступившие со своими воспоминаниями.

С обращениями к читателям книги выступили Президент России В. В. Путин, Председатель Правительства России Д. А. Медведев, Заместитель Председателя Правительства России, Председатель Военно-Промышленной комиссии при Правительстве России Д. О. Рогозин, Руководитель Федерального космического агентства.

Книга состоит из 11-ти глав. Первые шесть глав полностью посвящены историческому полету Юрия Алексеевича Гагарина.

По документальной хронике воссоздан по минутам исторический день 12 апреля 1961 года. О Юрии Гагарине вспоминают дочь, друзья, коллеги космонавта, участники Гагаринского старта. В книге впервые представлен полный список гражданских специалистов боевого расчета пультовой системы управления, офицеров первого испытательного управления, а также офицеров инженерно-испытательной части 25741, которые участвовали в запуске космического корабля «Восток». Некоторые из свидетелей этого исторического дня выступили со своими воспоминаниями.

Полет Юрия Гагарина был невозможен без труда великих ученых, создавших ракетно-космическую отрасль. Таких, как С. Королев, В. Бармин, В. Глушко, В. Кузнецов, Н. Пилюгин, М. Рязанский. Об этом повествуется в главе «Первооткрыватели космической эры».

В книге дана история освоения космоса более чем за 50 лет: строительство космодрома Байконур, запуск первых искусственных спутников Земли, изучение Луны, Венеры, Марса, первые пилотируемые полеты, международное сотрудничество, современный космос на службе народного хозяйства.

В книге представлена Государственная программа РФ «Космическая деятельность России на 2013–2020 гг.». О строительстве космодрома «Восточный» выступил Герой России, Летчик-космонавт РФ, начальник ФГБУ «НИИ ЦПК имени Ю. А. Гагарина» Ю. В. Лончаков.

На страницах книги представлено множество документов, фотоматериалов из личных архивов, часть которых читатель увидит впервые.

Формат книги — 245 х 325 мм. Объем — 712 стр.

Оформление: синяя бархатная обложка, тиснение золотой фольгой.

Стоимость — 5250 рублей. Оплата возможна за наличный и безналичный расчет.

Заказать книгу можно по телефону: 8-903-543-09-09 и по эл.почте: inirpp@yandex.ru klimashevskaia@mail.ru.

АЛГОРИТМ УПРАВЛЕНИЯ ПРОЦЕССАМИ ХРАНЕНИЯ ИНФОРМАЦИИ В ГЕТЕРОГЕННЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ХРАНЕНИЯ ДАННЫХ ПЕРСПЕКТИВНЫХ КОСМИЧЕСКИХ АППАРАТОВ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

Басыров Александр Геннадьевич,
д.т.н., профессор, начальник кафедры информационно-вычислительных систем и сетей Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, alexanderbas@mail.ru

Максимов Владимир Андреевич,
адъюнкт кафедры информационно-вычислительных систем и сетей Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, falcon225@yandex.ru

АННОТАЦИЯ

Рассмотрена проблема повышения достоверности информации, обрабатываемой и хранимой в бортовой системе хранения данных космических аппаратов дистанционного зондирования земли, работающих в условиях повышенных нагрузок и рисков, а также обрабатывающих данные, имеющие критическую важность.

Предметом исследования являются системы хранения данных космических аппаратов дистанционного зондирования земли. В ходе исследования космический аппарат дистанционного зондирования земли рассматривается как информационная система. Рассмотрены вопросы повышения достоверности информации обрабатываемой в таких аппаратах. В основу механизма, обеспечивающего повышение достоверности, положен принцип обеспечения максимальной безошибочности как одного из основных свойств, обеспечивающих достоверность.

Целью работы является разработка алгоритма управления процессами хранения информации в гетерогенных системах хранения данных информационных систем. Алгоритм управления хранения должен учитывать важность и актуальность хранимой информации для конечного потребителя, а также состояние системы в текущий момент времени.

Результаты: Предложен подход к управлению процессами, происходящими в ходе хранения данных, в соответствии с жизненным циклом информации, учетом ее важности для потребителя, а также состоянием самой системы. Описан общий механизм хранения информации и алгоритм управления процессами хранения, обеспечивающий заданный уровень безошибочности.

Наличие в системе хранения данных гетерогенных как по своей природе, так и характеристикам узлов допускает гибкое управление хранимыми данными, что позволяет уменьшить уровень информационной избыточности в системе, а также гибко регулировать эксплуатационные параметры системы. Управление системой подразумевает как физическое управление структурой системы, так и динамическое управление параметрами сетевого кодирования и репликацией хранимых данных.

Практическая значимость: представленный алгоритм при определенных доработках может быть применен к любой проектируемой системе хранения данных с учетом особенностей ее построения и функционирования. Преимущественным объектом для практического применения видятся системы хранения данных, работающие в неблагоприятных условиях, а также системы обрабатывающие и хранящие критически важную информацию. Алгоритм позволяет обеспечить либо заданный уровень безошибочности в системе, либо сохранность данных в зависимости от целей функционирования информационной системы в условиях деградации ее параметров.

Ключевые слова: информационные системы; система хранения данных; достоверность; безошибочность.

Для цитирования: *Басыров А.Г., Максимов В.А.* Алгоритм управления процессами хранения в гетерогенных распределенных системах хранения данных космических аппаратов дистанционного зондирования земли // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 6–15.

Введение

Современный этап развития космической техники характеризуется устойчивыми тенденциями к увеличению объемов данных, накапливаемых в процессе функционирования космических аппаратов, и к переносу процессов обработки этих данных с наземных комплексов обработки на борт. Данная информация может носить различный характер (телеметрическая, специальная, навигационная и т.д.), а также различную важность для потребителя (наземного комплекса управления, бортовых систем и пр.). Наибольшие объемы данных генерируются в результате работы целевой бортовой аппаратуры космических аппаратов дистанционного зондирования земли. При этом ее характеристики совершенствуются с каждым поколением и, как следствие, значительно растет объем данных, накапливаемый на борту. Однако, проблема безошибочного хранения на борту космического информации не ограничивается космическими аппаратами дистанционного зондирования. Так, ошибки, возникающие в процессе хранения командно-программной или навигационной информации могут привести к выходу из строя не только отдельных систем, но и космического аппарата в целом.

Переход на полупроводниковые технологии и достаточно продолжительная эксплуатация космических систем, позволила выявить ряд противоречий, в части касающейся системы хранения данных, требующих решения для успешного решения целевых задач.

1. В силу высокой производительности всех видов аппаратуры космических систем дистанционного зондирования, регистрируемые ей данные имеют большие объемы, что затрудняет их обработку и хранение. В то же время, возможности отечественных предприятий по производству запоминающих устройств, пригодных к использованию в условиях космоса, весьма ограничено. Как результат, например, значительно меньшая емкость системы хранения данных отечественных космических аппаратов (КА) по сравнению с зарубежными и неизбежное применение в них импортных микросхем памяти [1].

2. Одной из устойчивых тенденций на протяжении последних лет в области повышения оперативности получения информации является перенос решения ряда задач с наземного пункта приема и обработки информации на борт КА. Решение вопросов частичной или полной обработки данных на борту требует существенного увеличения объемов системы хранения данных, а также повышения безошибочности хранения данных на борту, так как любая ошибка в процессе обработки данных может внести значительные искажения и ошибки в результаты обработки. Это также вступает в противоречие с ограниченным объемом существующих систем хранения данных [2].

3. Требования, предъявляемые к существующим и перспективным космическим аппаратам в вопросах продления сроков активного существования и надежности функционирования, непрерывно растут. Однако, способы построения бортовой аппаратуры и в том числе систем хранения данных, устойчивых к продолжительному воздействию факторов космического пространства, недостаточно разработаны [3].

4. Одним из неотъемлемых требований к информации является ее достоверность, которая неизбежно страдает от искажения и потери данных как передаваемых по высокоскоростным радиолиниям вследствие помех, так и в процессе хранения в системе хранения данных вследствие воздействия различных факторов космического пространства. Повышение безошибочности хранимых на борту данных, как составной части достоверности информации в целом, требует введения различных видов избыточности (информационной, аппаратной, временной), что не всегда приемлемо с точки зрения массо-габаритных ограничений.

Как один из перспективных вариантов построения системы хранения данных космических аппаратов предложен вариант построения на базе запоминающих устройств, основанных на различных физических принципах. Данные микросхемы (например, MRAM, FRAM, SONOM и др.) обладают существенными отличиями, как в физическом принципе хранения данных, так и с точки зрения архитектуры. Различные исследования, в том числе ряд натурных экспериментов, проведенных NASA показывают, что такие микросхемы обладают рядом преимуществ с точки зрения устойчивости функционирования и надежности хранения данных в условиях космоса, что делает их привлекательными для применения на борту космических аппаратах. Стоит отметить, что выбор одного определенного типа запоминающего устройства затруднен ввиду существенного различия их характеристик (например, обладая большей радиационной стойкостью, они обладают меньшими объемами хранимых данных и пр.).

При этом, данные хранимые в системе хранения данных космического аппарата обладают также различными атрибутами. Так, некоторые данные теряют актуальность по прошествии некоторого промежутка времени, а другим задается более высокий приоритет.

Однако на данный момент методы синтеза и управления гетерогенных систем хранения недостаточно разработаны. [4].

С целью разрешения возникающего противоречия между необходимостью надежного хранения больших объемов данных на борту и отсутствием на текущий момент разработанных методов и средств такого хранения предлагается использовать Алгоритм синтеза гетерогенной структуры системы хранения данных КА на этапе проектирования системы хранения данных А и Алгоритм управления хранением данных в гетерогенной структуре системы хранения данных перспективных КА в процессе ее функционирования с целью обеспечения устойчивого функционирования КА в целом и выполнения целевого предназначения космической системы.

В то же время, КА дистанционного зондирования земли являются прежде всего информационными системами. Руководящие документы, определяют термин информационная система как автоматизироованную систему, результатом функционирования которой является представление выходной информации для последующего использования.

На схеме (рис. 1) представлены свойства, определяющие состояние достоверности информации. Голубым цветом выделены свойства и понятия, затрагиваемые в данной работе.

Очевидно, что за истинность исходных данных и корректность обработки целевой информации в космическом аппарате дистанционного зондирования земли отвечает целевая аппаратура. Одним из способов повышения уровня достоверности является обеспечение безошибочности хранения информации в процессе ее хранения и передачи. Таким образом, очевидно, что одним из основных аспектов на пути повышения достоверности информации в целом, является разработка алгоритмов синтеза и управления системы хранения данных, обеспечивающей заданный уровень безошибочности хранения специальной информации [5].

Подход к построению гетерогенной системы хранения данных

В общем случае подход к вопросу построения гетерогенной системы хранения данных (СХД) сводится к последовательному итерационному выполнению следующих этапов: анализ условий функционирования КА, анализ требований к СХД КА ДЗЗ, расчет состава модулей накопителя (МН) в соответствии с Моделью хранения данных [6], имитационное моделирование рассчитанной СХД при работе в соответствии с алгоритмом управления хранением данных, коррекция требований к СХД (при необходимости). Более подробно шаги методики описаны ниже.

1. Анализ условий функционирования КА (высота орбиты, вероятность воздействия тяжелых заряженных частиц (ТЗЧ) (P_{SEL}, P_{SEL}) и средний поток радиации (N)), вероятность механического воздействия (P_{SEL}).

2. Анализ доступной номенклатуры модулей накопителя.

$$M_j = <K^j, P^j>,$$

где K^j — контроллер модулей памяти j-го типа;

P^j — страницы памяти, обслуживаемые контроллером j-го типа.

Выборка из них типов МН, пригодных для использования в условиях воздействия неблагоприятных факторов космического пространства.

3. Анализ возможности применения средств дополнительной защиты. Составление вектора корректив параметров

$$< k_M, k_B, k_{SEL}, k_{SEU}, k_{rd}, k_{mi} >,$$

где k_M — коэффициент увеличения массы МН в случае применения средств дополнительной защиты;

k_B — коэффициент увеличения габаритов МН в случае применения средств дополнительной ащиты;

k_{SEL} — коэффициент уменьшения влияния *SEL* — эффектов на МН в случае применения средств дополнительной защиты;

k_{SEU} — коэффициент уменьшения влияния *SEU* — эффектов на МН в случае применения средств дополнительной защиты;

k_{rd} — коэффициент уменьшения накапливаемой дозы МН в случае применения средств дополнительной защиты;

k_{mi} — коэффициент уменьшения влияния механического воздействия в случае применения средств дополнительной защиты.

Рис. 1. Достоверность информации и способы ее достижения

4. Расчет параметров надежности P_w^j для каждой разновидности МН и составление вектора эксплуатационных для каждой разновидности МН:

$$KM^j = <E^j, T^j, B^j, M^j, V^j, P_w^j, P_{SEL}^j, P_{SEU}^j, C_{\max}^j, Rd_{\max}^j,$$

$$P_{mi}^j, k_M^j, k_{\text{SEL}}^j, k_{\text{SEU}}^j, k_{rd}^j, k_{mi}^j>,$$

где: E^j — энергопотребление j-м типом МН;

T^j — максимальное номинальное время доступа к j-му типу МН;

B^j — объем, занимаемый j-м типом МН;

M^j — масса j-го типа МН;

V^j — максимальный объем данных, который может хранить j-й тип МН;

P_w^j — вероятность безотказной работы для j-го типа МН;

P_{SEL}^j — вероятность возникновения *SEL* — эффектов для j-го типа МН;

P_{SEU}^j — вероятность возникновения *SEU* — эффектов для j-го типа МН;

$C_{\max}^j$ — максимальное количество циклов чтение / запись для j-го типа МН;

$Rd_{\max}^j$ — максимальная накопленная доза радиации для j-го типа МН;

P_{mi}^j — вероятность возникновения сбоев/отказов при механическом воздействии ограниченной силы на МН.

5. Анализ технических требований к СХД КА ДЗЗ в соответствии с его функциональным предназначением и формирование ограничений на параметры системы:

$$E_{dem,}\, T_{dem,}\, B_{dem,}\, M_{dem,}\, V_{dem,}\, P_{dem.}$$

6. Задание предполагаемого срока активного существования для КА — $T_{AF.}$

7. Задание первоначальных параметров помехоустойчивого и сетевого кодирования — μ, σ.

8. Выбор первоначального правила распределения (ω) блоков информации по блокам СХД в соответствии предполагаемой важностью информации (W).

9. Расчет состава модулей накопителя (МН). Данный этап выполняется в соответствии с методологическими основами внешнего проектирования целеустремленных систем [7]. В качестве такой системы выступает СХД. Основной целевой функцией является вероятность безошибочного хранения данных (P_{EL})в течении некоторого среднего директивного промежутка времени τ. На данном шаге определяются количество и типы МН, предполагаемые для использования в системе. Расчет происходит путем решения задачи математического программирования. Ищутся такие варианты МН j их число n_j, доставляющие максимум функции безошибочности P_{EL} и при этом удовлетворяющие критерию пригодности:

$$(E_S \le E_{dem} \cup T_S \le T_{dem} \cup B_S \le B_{dem} \cup M_S \le M_{dem} \cup V_S \ge V_{dem} \cup P_{ELS} \ge P_{ELD}).$$

10. Проводится имитационное моделирование функционирования системы с рассчитанными параметрами в соответствии с Моделью хранения данных. Производится анализ выполнения требования $P_{ELS} > P_{ELD}$ для различных условий, в том числе для предельных ситуаций: функционирование за пределами срока активного существования, хранение информации сверх директивного времени хранения τ, и длительного отсутствия сеансов сброса информации (переполнение СХД).

По результатам этапа 10 проводится принятие решение о пригодности СХД для применения с учетом особенностей разрабатываемого КА ДЗЗ. В случае принятия положительного решения, рассчитанные параметры СХД служат основой для технического проектирования СХД. В случае отрицательного решения проводится коррекция исходных данных (корректируются требования к СХД, либо требуемая вероятность безошибочности хранения P_{ELD}).

Общая схема хранения данных в гетерогенной структуре системы хранения данных

В общем случае процесс сохранения информации в СХД можно описать следующим образом (рис. 2):

В результате функционирования информационной системы КА ДЗЗ происходит генерация определенной информации I_n.

Информация I_n обладает свойствами:

V_n — объем информации, $W^n(t)$ — функция важности данной информации для потребителя (задается в ходе выдачи задания на информационной системе на сбор и обработку данных). Очевидно, что различные задания будут иметь различную степень важности для потребителя.

Кроме того, в зависимости от первоначальной важности для наземного пункта приема и управления (НППОИ), актуальность данной информации для потребителя также будет меняться (убывать) с различной скоростью для различных объектов. В общем виде функция важности $W^n(t)$ представляет собой монотонно убывающую функцию в пределах [0, 1]. Вид данной функции, а также ее начальное значение задаются потребителем (либо некоторой системой управления по запросу от потребителя) в ходе выдачи задания на проведение сбора и обработки информации.

На основании начального значения функции $W^n(t_0)$ управляющее устройство (УУ) СХД рассчитывает требования по безошибочности хранения информации Q^n в течении директивного срока τ^n. Требования по безошибочности хранения представляют собой вероятность того, что в течении директивного срока хранения τ^n в хранимых данных будут отсутствовать ошибки.

Директивной срок хранения τ^n зависит от начального значения функции $W^n(t_0)$, а также от режима функционирования СХД Y. Режим функционирования СХД зависит от условий обстановки. В случае, если система работает в неблагоприятных условиях (чрезвычайные ситуации, непредусмотренные отказы и сбои в системе, недоступность отдельных узлов) директивный срок хранения τ^n может быть увеличен, и, соответственно, изменится и Q^n.

Таким образом, n-й набор данных, поступивший в систему можно описать вектором параметров:

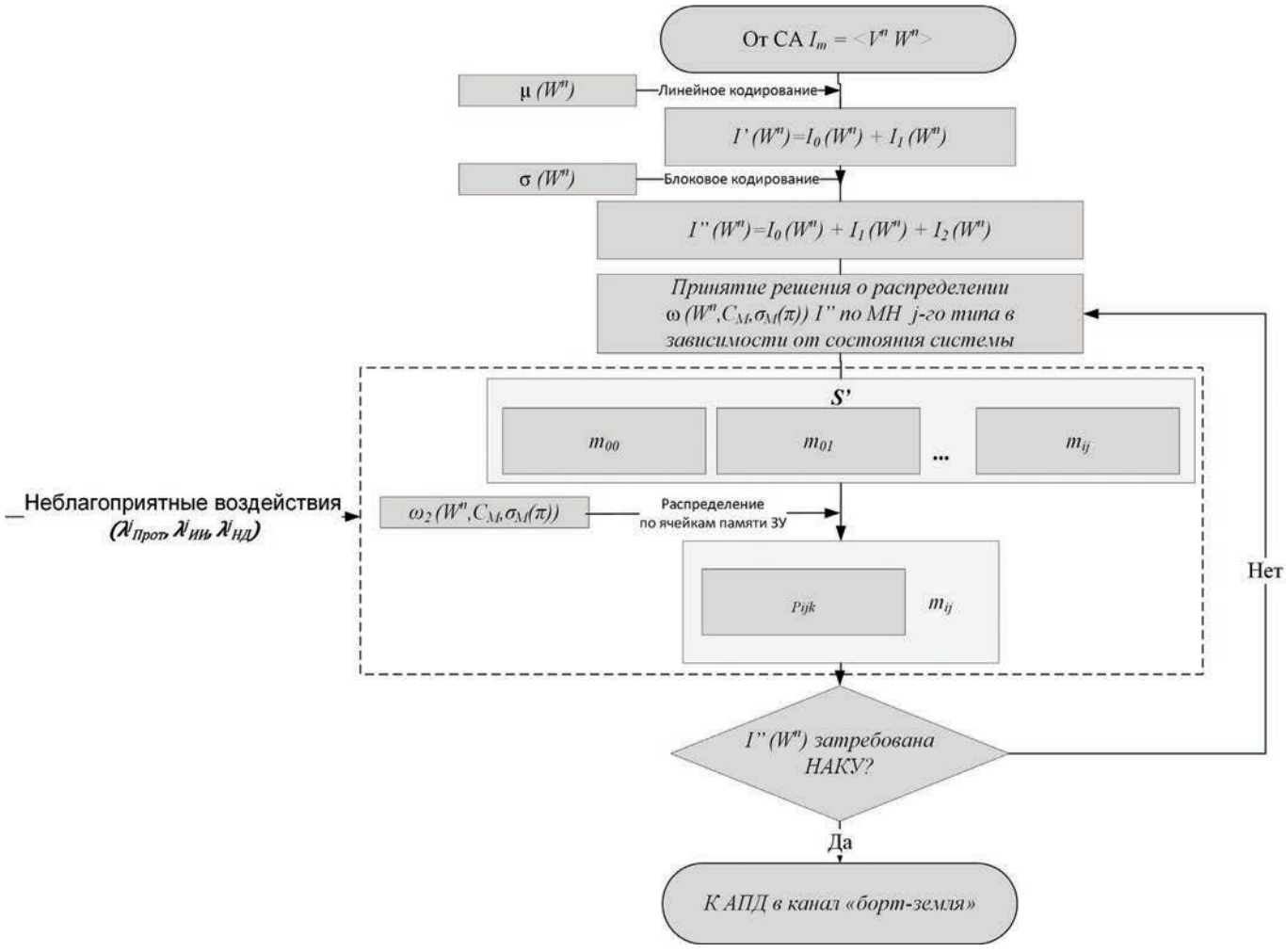


Рис. 2. Процесс сохранения информации в СХД КА ДЗЗ

$$I_n = <k^n, V_k^n, W^n, Q^n>,$$

где k^n — число блоков, на которые разбит n-й набор;

V_k^n — объем блока данных n-го набора;

W^n — функция важности результатов n-го сеанса;

Q^n — заданные требования по безошибочности хранения результатов работы СА.

УУ СХД КА ДЗЗ с установленной периодичностью, а также при поступлении в систему новой информации осуществляет функциональный контроль.

В результате проведения функционального контроля и данных о предыдущем состоянии системы для каждого модуля накопителя формируется вектор состояния МН:

$$SS^{ij} = < K_E^{i,j}, K_T^{ij}, K_{rw}^{ij}, K_{rd}^{ij}, K_{AP}^{ij}, V^{ij}, k^{mij}[W^{mij}]>,$$

где: $K_E^{i,j}$ — нормированный показатель энергопотребления i-го узла j-го типа;

K_T^{ij} — нормированный показатель времени доступа к i-му узлу j-го типа;

K_{rw}^{i} — нормированный показатель циклов чтения/записи i-го узла j-го типа;

K_{rd}^{ij} — нормированный показатель поглощённой дозы i-го узла j-го типа;

K_{AP}^{ij} — нормированный показатель активной работы i-го узла j-го типа;

V^{ij} — объем i-го узла j-го типа (с учетом модулей накопителя (МН));

$k^{mij}[W^{mij}]$– количество блоков данных предыдущих наборов данных, с соответствующим им показателями важности.

Также для дальнейшего удобства описания алгоритма введем показатель $C^{ij} = k^{mij}[W^{mij}]V_k^n$ — общий занятый объем МН СХД.

В общем случае управление жизненным циклом информации (всех m наборов данных), хранимой в СХД осуществляется на основании соответствующих значения функции $W^m(t)$, заданных требований по безошибочности Q^n, а также состояния СХД SS^{ij}. Под жизненным циклом здесь понимается: поступление информации в систему, первоначальное размещение ее в структуре СХД, перераспределение информации по СХД в ходе ее хранения (в случае возникновения такой необходимости), а также стирание ее из СХД

(после выдачи потребителю или после утери актуальности (снижения функции важности ниже $Q^n_{\min}$).

После поступлении в буферное устройство системы хранения данных, расчета управляющим устройством требований по безошибочности и оценки состояния системы, выполняются следующие операции.

Информация $I_n(W^n)$ подвергается преобразованию (блоковое помехоустойчивое кодирование) $\mu_1(W^n)$ с параметрами (n_1, k_1, d_1, α, γ) в результате чего вводится информационная избыточность ($I' = I_n + I_1$, позволяющая восстанавливать исходную информацию I_n в случае утери одного или нескольких блоков информации.

Информация $I' = I_n + I_1$ подвергается преобразованию (линейное помехоустойчивое кодирование) $\mu_2(W^n)$ с параметрами (n_2, k_2, d_2) в результате чего вводится избыточность $I' = I_n + I_1$, $I'' = I_0(\pi) + I_1(\pi) + I_2(\pi)$, позволяющая исправлять ошибки, вызванные ошибками в каналах связи и одиночными сбоями в ячейках памяти (ЯП). При этом параметры кодирования $\mu_1(\pi)$, $\mu_2(\pi)$ выбираются исходя из приоритета π поступающей информации и текущего состояния СХД S' (в частности доступного объема свободной памяти и параметров надежности элементов).

Информация I'' (W) подвергается распределению ω_1 по структуре SS (n блоков по i модулям j-го типа) в соответствии с правилом g_1.

Далее n блоков, поступивших на модуль накопителя (МН) m_{ij} подвергаются распределению ω_2 по страницам МН P_{ijk} МН m_{ij} в соответствии с правилом g_2.

Параметры распределения СИ по МН и ЯП выбираются исходя из приоритета π поступающей информации и текущего состояния СХД SS (в частности доступного объема свободной памяти и параметров надежности элементов).

При проведении сеанса связи с наземным комплексом управления (НАКУ) хранимая информация выдается в канал «борт-земля». При этом на выходе СХД существует возможность искажения битов целевой информации, вызванная неустранимыми искажениями исходной информации при хранении в СХД.

Таким образом, предложенный подход позволяет провести дальнейшую детальную проработку моделей СХД и модели процесса хранения данных в СХД.

В условиях штатного функционирования (своевременной выдачи информации потребителю, корректная работа аппаратуры передачи данных, отсутствие сбоев и отказов в аппаратуре СХД) данные кодируются и размещаются таким образом, чтобы их безошибочность была не ниже требуемой ($P_{EL} > Q^n$), определяемой УУ СХД. Однако в случае возникновения особых условий (например, длительной недоступности ИС для потребителей и переполнения СХД, либо отказа части узлов СХД в результате чрезвычайной ситуации) возникает необходимость с одной стороны обеспечить надежное хранение результатов работы ИС, а с другой стороны уместить данные в имеющийся объем СХД. В таких ситуациях алгоритмом предусмотрено снижение требований к безошибочности информации и, как следствие, снижение занимаемого объема СХД (за счет уменьшения информационной избыточности: уменьшение длинны кодов и снижения степени репликации). При этом обеспечение безошибочного хранения наиболее важных результатов работы ИС возможно за счет их размещения в узлах СХД с потенциально максимальным ресурсом надежности. При этом в условиях критической нехватки объема СХД происходит стирание СИ, ценность которой наименьшая для НППОИ и за счет высвободившегося объема происходит обеспечение безошибочности хранения более важной СИ.

Алгоритм управления процессами хранения в гетерогенных распределенных системах хранения данных информационных систем и сетей

Алгоритм управления процессами хранения в гетерогенных распределенных системах хранения данных (рис. 3) и (рис. 4) функционирует в соответствии с представленным ниже описанием.

Шаг 1. В информационную систему поступает новая информация (введенная пользователями, полученная от внешних датчиков или каким-либо другим образом).

Шаг 2. Управляющее устройство (УУ) системы хранения данных осуществляет внеочередной функциональный контроль.

Шаг 3. Производится составление вектора параметров состояния СХД $SS^{ij} = < K_E^{ij}, K_T^{ij}, K_{rw}^{ij}, K_{rd}^{ij}, K_{AP}^{ij}, V^j, k^{ij}[W^{nj}] >$.

Шаг 4. Осуществляется контроль показателей K_E^{ij}. В случае выхода параметров энергопотребления узла за установленные пределы ($K_E^{ij} > 1$), осуществляется переход к шагу 5. Иначе — переход к шагу 7.

Шаг 5. Проводится перераспределение содержимого узла с параметрами энергопотребления, превышающими установленные (для $K_E^{ij} > 1$) по другим узлам с учетом показателя важности хранимой информации W^{mij} и состоянием узлов SS^{ij}.

Шаг 6. Выдача команды на выключение узла СХД из работы.

Шаг 7. Осуществляется контроль показателей K_T^{ij}. В случае превышения времени доступа к одному из узлов (сбой или отказ в работе узла или сбой/отказ в устройстве передачи данных узла) ($K_T^{ij}>1$), осуществляется переход к шагу 8. Иначе — переход к шагу 11.

Шаг 8. Проводится поиск МН P^{ijk} для которой $K_T^{ikj}>1$.

Шаг 9. Перераспределение содержимого МН P^{ijk} по другим узлам с учетом показателя важности хранимой информации P^{ijk} и их состоянием SS^{ij}. В случае невозможности чтения содержимого МН P^{ijk} производится восстановление утерянных блоков k^{ijk}, принадлежащих странице P^{ijk} с помощью блоковых кодов и перераспределение этих блоков по другим узлам СХД с учетом показателя важности хранимой информации W^{mij} и их состоянием SS^{ij}.

Шаг 10. Выдача команды контроллеру узла на выключение МН из работы.

Шаг 11. Производится расчет ценности полученной информации (расчет ценности осуществляется исходя из правила W^n в момент поступления информации в СХД).

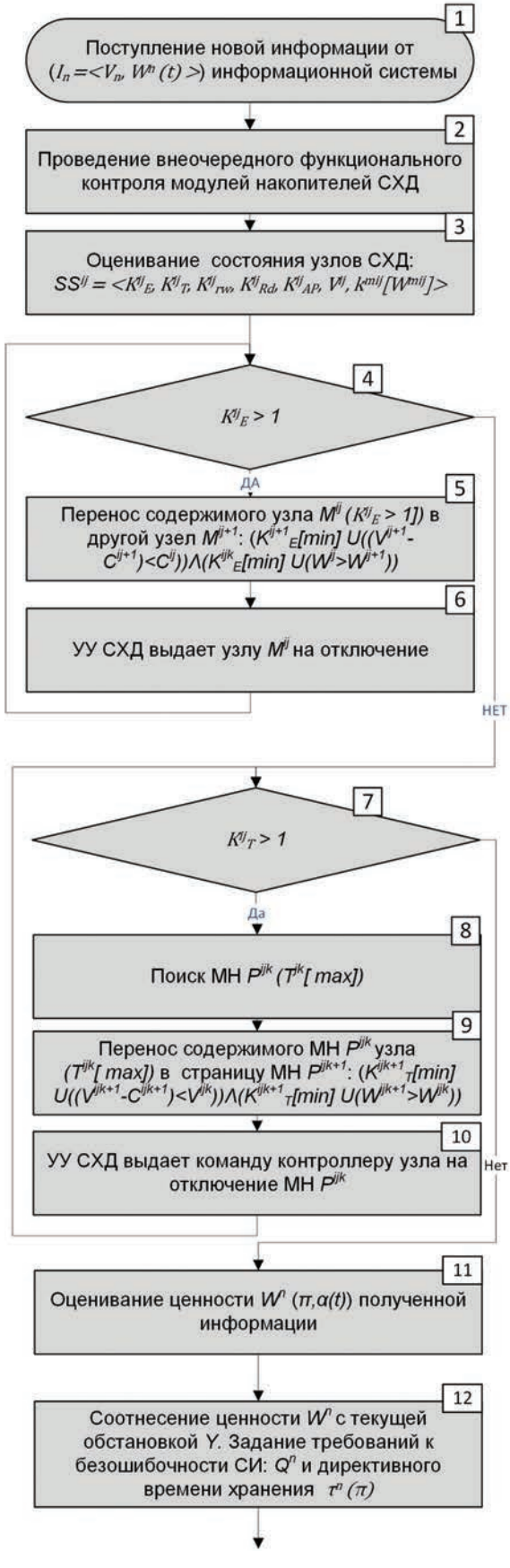


Рис. 3. Алгоритм управления процессами хранения (начало)

Шаг 12. При поступлении от БСК новой информации $I_n(W^n)$ производится начальное задание требований к безошибочности СИ Q^n на основе важности информации W^n текущих условий обстановки Y.

Шаг 13. В соответствии с заданными требованиями по безошибочности информации Q^n УУ СХД рассчитывает параметры кодирования μ^n и параметры восстанавливающего кодирования σ^n для обеспечения вероятности безошибочности $P_{EL}{}^n > Q^n$.

Шаг 14. Производится расчет планируемого распределения ω^n по страницам модулей накопителей для обеспечения вероятности безошибочности $P_{EL}{}^n > Q^n$.

Шаг 15. Производится оценка доступного объема СХД. Если доступный объем СХД позволяет разместить информацию в СХД с планируемыми параметрами кодирования μ^n, σ^n и распределением ω^n, то осуществляется переход к шагу 25. Если нет — переходим к шагу 16.

Шаг 16. Осуществляется расчёт важности W^mдля всех наборов данных m на текущий момент времени t.

Шаг 17. Поочередное сравнение важности вновь поступившей информации с важностью каждого из наборов данных, хранимых в системе. В случае если важность вновь поступивших данных больше важности набора данных, осуществляется переход к шагу 19. Иначе — к шагу 18.

Шаг 18. Снижение требований к безошибочности вновь поступившей информации и переход к шагу 13 с учетом этих требований.

Шаг 19. Расчет требований к безошибочности информации Q^m m-го сеанса (W^n>W^m) с учетом рассчитанной на шаге 16 важности W^m. Расчет параметров кодирования μ^m, σ^m и распределение ω^m для обеспечения вероятности безошибочности $P_{EL}{}^m > Q^m$.

Шаг 20. Расчет вероятности безошибочности $P_{EL}{}^m$ с учетом параметров, рассчитанных на шаге 19.

Шаг 21. Вероятность безошибочности $P_{EL}{}^m$ больше требований по безошибочности Q^m и объем СХД позволяет произвести запись вновь поступившей информации с параметрами μ^n, σ^n, ω^n и информации m-го сеанса с параметрами μ^m, σ^m, ω^m. Если да, то переходим к шагу 22. Если нет — к шагу 23.

Шаг 22. Производится перезапись информации I_m с параметрами μ^m, σ^m, ω^m и информации I_n с параметрами μ^n, σ^n, ω^n.

Шаг 23. Производится снижение требований к безошибочности хранения СИ Q^m и Q^n. Переход к шагу 13.

Шаг 24. Производится запись информации I_n с параметрами μ^n, σ^n, ω^n

Шаг 25. Проведение внеочередного функционального контроля. В случае выхода параметров за пределы нормы переход к шагу 4.

Шаг 26. Расчет вероятности безошибочности для всех наборов данных $P_{EL}{}^m$. Проверка удовлетворения неравенства $P_{EL}{}^{m+1} > Q^{m+1}$. Если условие выполняется, переход к шагу 27. Если нет — к шагу 19.

Шаг 27. Переход СХД в режим ожидания новой информации из информационной системы с проведением периодического функционального контроля.

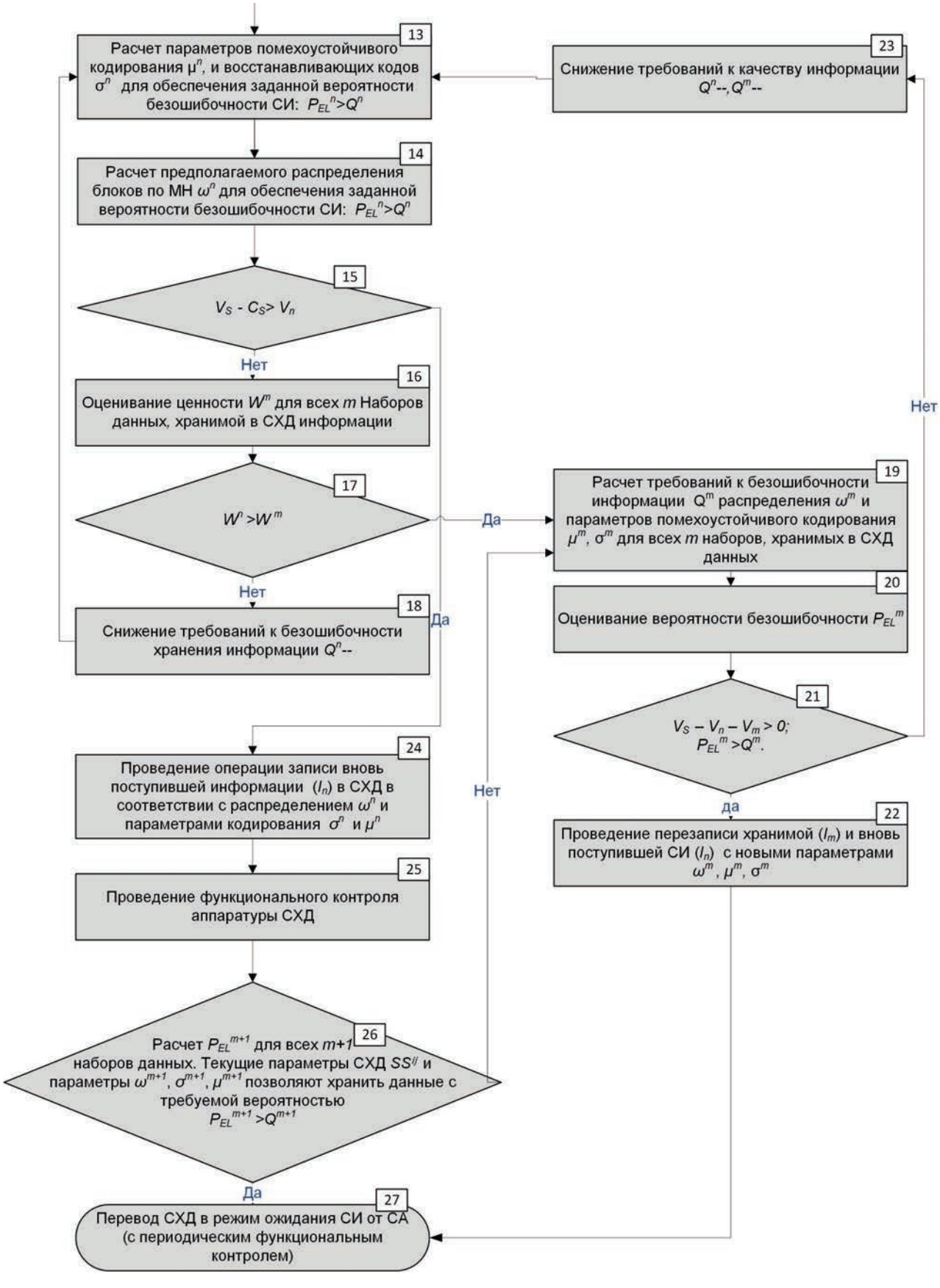


Рис. 4. Алгоритм управления процессами хранения (продолжение)

Заключение

Предложенный подход к обеспечению заданного уровня безошибочности информации, хранимой в СХД КА ДЗЗ как информационных системах позволяет гибко управлять процессами хранения и их параметрами (параметрами кодирования и размещения блоков данных по узлам системы), а также непосредственно состоянием системы хранения данных в условиях ее деградации (старение входящих в состав системы структурных элементов, их сбои и отказы). При этом учитывается начальная важность поступившей в систему информации, ее актуальность в текущий момент времени, а также непосредственно состояние СХД и условия в которых осуществляются процессы сбора и хранения информации. Результаты проведенного моделирования показывают, что применение алгоритма в совокупности с использованием показателя важности информации позволяет повысить безошибочность хранения информации, наиболее важной для потребителя в среднем на 5–9% по сравнению с «плоским» хранением (в случае когда вся информация имеет одинаковое значение важности и распределяется по системе с одинаковыми параметрами распределения и кодирования). Приведенные цифры приведены для гомогенной системы хранения данных на которой производились расчёты. В случае применения гетерогенной системы, эти цифры будут выше вследствие значительного преимущества характеристик некоторых микросхем памяти для космического применения по сравнению с испытуемыми FLASH накопителями. Однако, здесь становятся критически важными такие параметры, как массо-габаритные, энергетические и прочие показатели, которые необходимо учитывать на этапе синтеза системы хранения данных.

Литература

1. *Петров А.Г., Уланова А.В., Чумаков А.И., Васильев А.Л.* Исследования потери информации в микросхемах флэш-памяти в активном и пассивном режимах при ионизирующем воздействии // Тезисы докладов 17 научно-технической конференции по радиационной стойкости электронных систем «Стойкость-2014» (Москва, 3–4 июня 2014). М.: Научно-исследовательский институт приборов, 2014. С. 175–176.

2. *Савиных В.П.* Оптико-электронные системы дистанционного зондирования. М.: Недра, 1996. 315 с.

3. Концепция развития российской космической системы дистанционного зондирования земли на период до 2025 года. М.: Федеральное космическое агентство, 2006. 72 с.

4. *Захаров И.В., Кремез Г.В., Максимов В.А.* Построение распределенных запоминающих устройств бортовых вычислительных систем космических аппаратов дистанционного зондирования земли // Труды военно-космической академии имени А.Ф. Можайского. 2016. № 652. С. 160–166.

5. *Гончаренко В.А., Дудкин А.С., Максимов В.А.* Обоснование производительности вычислительных систем при решении группы неоднородных задач // Естественные и технические науки. 2016. № 8 (98). С. 79–81.

6. *Максимов В.А., Дудкин А.С.* Подход к формированию модели системы хранения данных в перспективных космических аппаратах дистанционного зондирования земли // Международный научно-исследовательский журнал. 2016. № 10 (52). Ч. 2. С. 82–85.

7. *Петухов Г.Б., Якунин В.И.* Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М.: АСТ, 2006. 502 с.

ALGORITHM OF INFORMATION STORAGE MANAGEMENT IN HETEROGENEOUS DATA STORAGE SYSTEMS FOR PROSPECTIVE SPACE PROBES

Alexander G. Basyrov,
Saint-Petersburg, Russia, alexanderbas@mail.ru

Vladimir A. Maksimov,
Saint-Petersburg, Russia, falcon225@yandex.ru

ABSTRACT

In article considered problem of onboard information accuracy increasing for storage system operating in various conditions.

The subjects of research are onboard storage systems for Earth monitoring probes. In article earth monitoring probes presented as information system. Considered aspects of information accuracy and correctness increasing. Increasing of information correctness leads to information accuracy.

Target of article is research of algorithm of information storage management in heterogeneous data storage systems for prospective space probes. Algorithm should take in to account significant and relevance of stored information and condition of data storage system.

As result proposed approach to management of information storage according to information lifetime cycle. Described mechanic of data storage that maintain demanded level of correctness.
Existing in data storage system heterogeneous nodes allows flexible management of stored data that leads to decreasing of information redundancy in system. Management of storage means management of system structure and dynamic management of network coding settings.
Importance of practical usage is that Algorithm with some modifications may be applied to any prospective data storage system, that works in adverse conditions. Main objects for algorithm application seems data storage systems with critical information.
Algorithm allows to maintain data correctness in condition of system degradation.

Keywords: information systems; data storage system; data accuracy; data correctness.

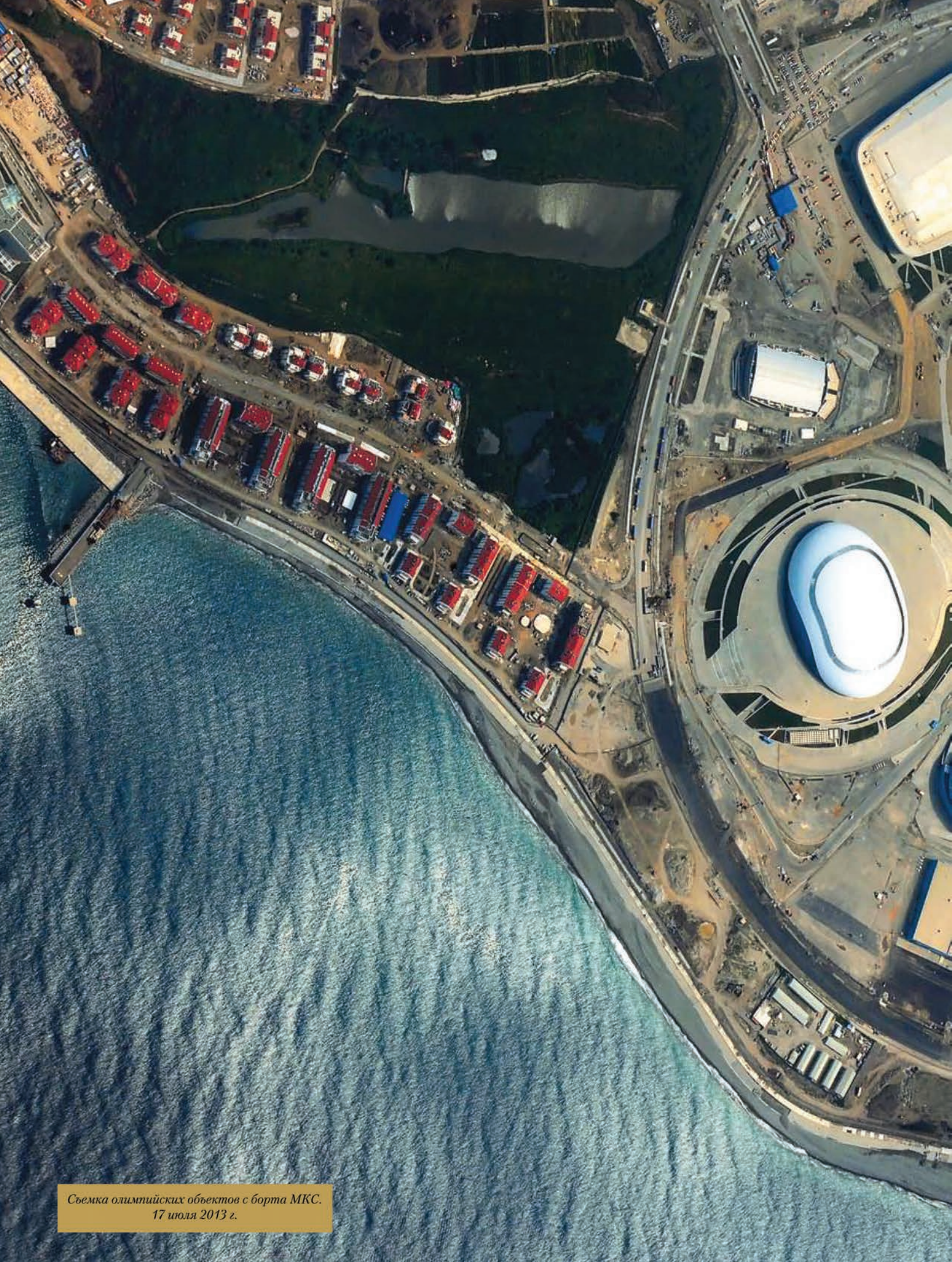
References

1. Petrov A.G., Ulanova A.V., Chimakov A.I. Issledovanija poteri informacii v mikroshemah fljesh-pamjati v aktivnom i passivnom rezhimah pri ionizirujushhem vozdejstvii [Research of information loss in FLASH during ionizing in active and passive modes] Tezisy dokladov 17 nauchno-tehnicheskoj konferencii po radiacionnoj stojkosti jelektronnyh sistem "Stojkost'-2014" [The collection of reports of scientifictechnical conference "Electronic systems radiation resistance", Moscow, June 3–4, 2014]. Moscow: Nauchno-issledovatel'skij institut priborov Publ., 2014. Pp. 175–176. (In Russian)
2. Savinyh V.P. *Optiko-jelektronnye sistemy distancionnogo zondirovanija*. [Optic and electronic Earth monitoring systems]. Moscow: Nedra, 1996. 315 p. (In Russian)
3. Koncepcija razvitija rossijskoj kosmicheskoj sistemy distancionnogo zondirovanija zemli na period do 2025 goda [Concept of Russian space Earth monitoring systems development till 2025]. Moscow: Federal'noe kosmicheskoe agentstvo, 2006. 72 p. (In Russian)
4. Zaharov I.V., Kremez G.V., Maksimov V.A. Postroenie raspredelennyh zapominajushhih ustrojstv bortovyh vychislitel'nyh sistem kosmicheskih apparatov distancionnogo zondirovanija zemli [Building of distributed onboard data storage systems for space earth monitoring probes] *Trudy voenno-kosmicheskoi akademii imeni A.F. Mozhaiskogo* [Proc. of the Military Space academy named after A.F. Mozhaisky]. 2016. No. 652. Pp. 160–166.
5. Goncharenko V.A., Dudkin A.S, Maksimov V.A. Perfomance Substantial of Computing Systems at the decision of a group of heterogeneous tasks. *Natural and technical Sciences*. 2016. No. 8 (98). Pp. 79–81. (In Russian)
6. Dudkin A. S, Maksimov V.A. The approach to earth remote sensing spacecrafts storage system model creation. *International research journal*. 2016. No. 10 (52). Vol. 2. Pp. 82–85. (In Russian)
7. Petuhov G.B., Yakunin V.I. *Metodologicheskie osnovy vneshnego proektirovanija celenapravlennyh processov i celeustremlennyh sistem* [Methodological bases of target-aimed processes and target-aimed systems processes]. Moscow: AST, 2006. 502 p. (In Russian)

Information about authors:

Basyrov A.G., PhD, Full Professor, Chief of Department of Information Systems and Networks of Military Space Academy.
Maksimov V.A. postgraduate student at the Department of Department of Information Systems and Networks of Military Space Academy.

For citation: Basyrov A.G., Maksimov V.A., Algorithm of Information Storage Management in Heterogeneous Data Storage Systems for Prospective Space Probes. *H&ES Research*. 2017. Vol. 9. No. 2. Pp. 6–15. (In Russian)



Съемка олимпийских объектов с борта МКС. 17 июля 2013 г.

КНИГА «О СПОРТ! ТЫ – МИР!»

Институт изучения реформ и предпринимательства выпустил уникальную книгу «О спорт! Ты – мир!», в название которой положены слова основателя современного Олимпийского движения барона Пьера де Кубертена.

Эта книга – своеобразный экскурс в многовековую историю Олимпийского движения от Афин до Сочи. Это прекрасные романтические мифы и легенды с определенной исторической достоверностью, которые сложила человеческая фантазия о возникновении античных игр. В книге в хронологическом порядке представлены все Олимпийские игры, начало которым положила древняя Греция, как праздники спорта и мира. Благодаря Пьеру де Кубертену через полторы тысячи лет Олимпийские игры были вновь возвращены и во второй раз подарены человечеству.

В книге читатель окунется в мир большого спорта. Каждая Олимпиада наполнена яркими страницами мировых спортивных достижений, именами великих спортсменов, навсегда вписанных в историю олимпизма. Каждый, кто возьмет эту книгу в руки, станет свидетелем фантастических зрелищ спортивных достижений, достойных восхищения. В книге приводятся слова древнегреческого поэта Пиндара: «Нет ничего благороднее солнца, дающего столько света и тепла. Так и люди прославляют те состязания, величественнее которых нет ничего».

Особое место в книге уделено России. Представлена ее неповторимая индивидуальность, которая ярче всего проявилась в культурных сокровищах прошлого и настоящего. Страна, гордившаяся собственными спортивными традициями и спортсменами международного класса. В книге представлена история развития национальных видов спорта на Руси, первые всероссийские Олимпиады.

Поражает воображение раздел «Олимпийский Сочи из космоса» панорамными фотографиями космических съемок олимпийских объектов, природного ландшафта окрестностей Сочи, морского побережья. Космический мониторинг позволяет ощутить огромный масштаб стройки, детально рассмотреть не только спортивные сооружения, но и уникальную природу сочинского побережья. Надо отметить, что подобные материалы публикуются впервые.

В книге читатель познакомится с космической одиссеей, о том, как Роскосмос доставил олимпийский факел на космический борт МКС на транспортном пилотируемом корабле ТПК «Союз ТМА-11М» с помощью ракетоносителя «Союз». В открытый космос с факелом вышли российские космонавты Олег Котов и Сергей Рязанский.

Отправка факела олимпийского огня в открытый космос – беспрецедентное событие в истории как олимпийского движения, так и мировой космонавтики. Его доставка на орбиту и вынос в открытый космос российскими космонавтами стало новой яркой страницей космической летописи.

Вошел в олимпийскую космическую историю и экипаж, который принял орбитальную эстафету и доставил на борт олимпийский факел. Этот всемирный спортивный символ обтелел Землю. Выше олимпийская символика еще не поднималась. Орбитальная эстафета на высоте в 400 километров – это поистине олимпийский рекорд. В книге рассказано, как на космодроме Байконур тоже принимали эстафету: готовили ракету и ее особенный олимпийский внешний вид – это 200 квадратных метров олимпийского рисунка. Так ракета оформлялась впервые.

Космическая съемка строительства олимпийских объектов производилась с российских и зарубежных спутников, начиная с 2008 года после утверждения Правительством РФ Программы строительства олимпийских объектов и развития города Сочи. С этой целью были задействованы российские спутники: «Ресурс-ДК», «Метеор-М» № 1, «Канопус-В», «Ресурс-П». Спутник «Метеор-М» № 1 был предназначен для решения задач гидрометеорологического обеспечения, мониторинга климата и окружающей среды, контроля гелиогеофизической обстановки в околоземном космическом пространстве в интересах Росгидромета. Еще один космический комплекс «Электро-Л», разработанный в НПО им. С.А. Лавочкина, был запущен в 2013 году для обеспечения Росгидромета оперативной информацией для анализа и прогноза погоды, изучения состояния акваторий морей и океанов, а также изучения состояния ионосферы и магнитного поля Земли. В книге рассказано, как вели наблюдения за строительством олимпийских объектов космонавты с борта МКС.

Книга «О спорт! Ты – мир!» издана в подарочном варианте: бархатная обложка, золотое тиснение, 40% книги напечатано на золотом понтоне.

Формат книги – 245х325 мм. Объем – 987 стр.

Стоимость – 6200 рублей. Оплата возможна за наличный и безналичный расчет.

Заказать книгу можно по телефону: 8-903-543-09-09 и по эл.почте: inirpp@yandex.ru klimashevskaia@mail.ru.

АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО СПЕЦИАЛИСТА ПУНКТА УПРАВЛЕНИЯ СЕТЬЮ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Верхова Галина Викторовна,
д.т.н., профессор, заведующий кафедрой автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, galina500@inbox.ru

Белоус Константин Владимирович,
к.т.н., доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, kostos_84@mail.ru

АННОТАЦИЯ

В статье представлены результаты научных исследований в области автоматизированного управления сетью связи специального назначения в условиях применения противником средств радиоэлектронной борьбы. Приводится разработанная авторами система комплексных показателей эффективности функционирования сети связи, которая формируется в виде иерархической системы в соответствии с единой методологической концепцией построения информационных систем, предусматривающая рассмотрение любой сети обмена информацией с позиций эталонной модели взаимодействия открытых систем (ЭМВОС). Данный подход обеспечит возможность использования системы показателей качества для оценки и управления любыми ведомственными сетями связи, входящими в состав инфокоммуникационной среды Единого информационного пространства Российской Федерации.

Управление сетью связи в условиях радиоэлектронной борьбы интерпретируется как поиск оптимального показателя качества функционирования сети в условиях воздействия различных угроз. Основными факторами, меняющими частные показатели эффективности функционирования сети на всех уровнях рассмотрения, являются воздействия угроз, исходящих от системы радиоэлектронной борьбы. Так как задача поиска оптимальной стратегии управления сетью связи специального назначения относится к классу NP-трудных, она не может быть решена за приемлемое время путём прямого перебора; для ее решения требуется разработка специального программно-алгоритмического обеспечения, обеспечивающего приближенное рациональное решение. Такое программно-алгоритмическое обеспечение может быть использовано в программно-аппаратных комплексах систем управления сетями связи и боевых информационно управляющих системах.

Программно-алгоритмическое обеспечение должно создаваться на основе современных программных платформ, с использованием технологии объектно-ориентированного программирования. Прототип системы программного обеспечения написан на программно-алгоритмическом языке C#. Приложение реализовано с использованием стандартных элементов управления, имеет эргономичный интерфейс, обеспечивает вывод данных на экран монитора. Программно-алгоритмическое обеспечение позволяет по заданным параметрам (ресурсу сети, возможностям противоборствующей стороны, перечню доступных направлений связи и их приоритетности) смоделировать возможные стратегии РЭБ с целью выбора оптимальной стратегии противодействия средствам радиоэлектронной борьбы противника, обеспечив снижение объёма причиняемого ущерба.

Ключевые слова: сеть связи специального назначения; радиоэлектронная борьба; автоматизированное управления; система комплексных показателей эффективности функционирования сети связи; Единое информационное пространство Российской Федерации; программно-алгоритмическое обеспечение управления сетью связи специального назначения; оптимальная стратегия управления

Для цитирования: *Верхова Г.В., Белоус К.В.* Автоматизированное рабочее место специалиста пункта управления сетью связи специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 18–23.

В настоящий момент времени в связи с активным внедрением инфотелекоммуникационных технологий в деятельность органов государственной власти федерального, регионального и местного уровней возникла необходимость в создании Единого информационного пространства Российской Федерации на базе защищенной инфокоммуникационной среды, объединяющей информационные ресурсы и средства их обработки, используемые различными подразделениями и ведомствами (рис. 1). Особенностью инфокоммуникационной среды специального назначения является возможность ее стабильного функционирования в условиях радиоэлектронной борьбы (РЭБ).

Единая инфокоммуникационная среда создается на базе существующих сетей связи специального назначения, стабильное функционирование которых обеспечивается пунктами управления [1]. Эффективное функционирование пунктов управления спецсвязью требует получения и обработки информации о состоянии сети в режиме реального времени в условиях преднамеренного воздействия на узлы и линии связи различными средствами поражения и подавления [2]. Объективная оценка состояния сети, необходимая для эффективного оперативного управления, минимизирующего ущерб от применения средств РЭБ, предполагает наличие системы количественных показателей эффективности функционирования как отдельных узлов и линий связи, так и инфокоммуникационной среды в целом.

Система комплексных показателей эффективности функционирования сети связи формируется в виде иерархической системы в соответствии с единой методологической концепцией построения информационных систем, предусматривающая рассмотрение любой сети обмена информацией с позиций эталонной модели взаимодействия открытых систем (ЭМВОС). Данный подход обеспечит возможность использования системы показателей качества для оценки и управления любыми ведомственными сетями связи, входящими в состав инфокоммуникационной среды [3,4]. Единого информационного пространства Российской Федерации.

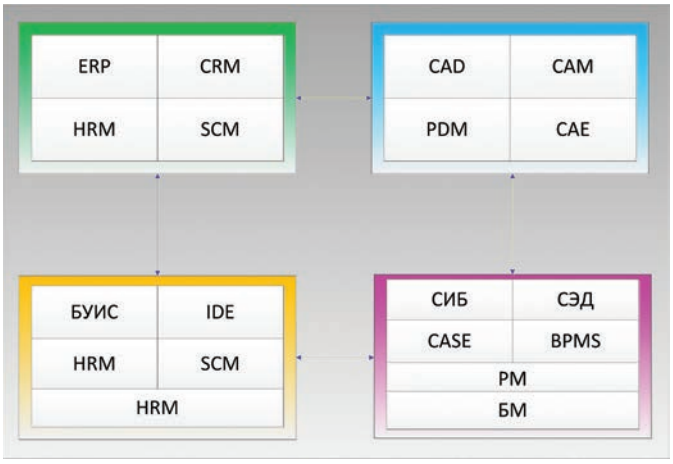


Рис. 1. Объединение информационных ресурсов и средств их обработки в единое информационное пространство

Квалиметрическая модель системы комплексных показателей эффективности сети связи особого назначения

Представим сеть связи в виде системы, в состав которой входят (рис. 2):

– входные и выходные информационные потоки I и I';

– структурная матрица B, определяющая множество допустимых структур сети связи, размерности $N \times N$, где N — максимальное число информационных направлений.

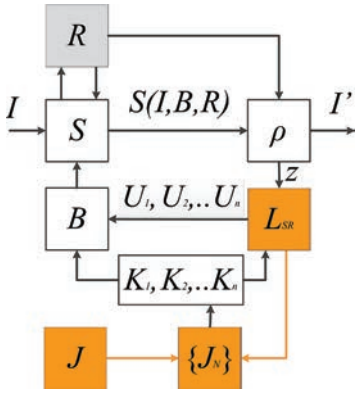


Рис. 2. Обобщённая модель функционирования сети связи в условиях радиоэлектронной борьбы

Учитывая независимость направлений получим конечное счетное множество матриц с количеством элементов 2^N, в которых $b_{ij} = 1$, если организуется передача информации от i-го узла связи к j-му, и $b_{ij} = 0$ — в противном случае.

Ресурс сети S, подвергшийся воздействию средств РЭБ, задается множеством стохастических матриц размера $M \times N$:

$$|S|^1_{M\times N} = \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1N} \\ s_{21} & s_{22} & \dots & s_{2N} \\ \dots & \dots & \dots & \dots \\ s_{M1} & s_{M2} & \dots & s_{MN} \end{pmatrix} \quad (1)$$

где матрица S_k является стратегией системы управления сетью связи, а S_{ij} — вероятность работы j-го направления в i-м варианте построения сети связи, при ограничениях:

$$\sum_{i\in M} s_{ij} \le 1$$

где M — количество типов линий связи j-го направления. Множество стратегий системы управления сетью связи представляет собой множество всех матриц $S = \{S_k\}$.

Приоритетность информационных направлений задается диагональной матрицей $|A|_{N\times N}$, элементами которой являются весовые коэффициенты α_{ii}, учитывающие важность i-го информационного направления

$$\|A\|_{N\times N} = \begin{pmatrix} a_{11}, 0, \dots, 0 \\ 0, a_{22}, \dots, 0 \\ 0, 0, \dots, a_{NN} \end{pmatrix}, \sum_{i\in N} a_{ij} = 1, \quad (2)$$

Другими элементами модели являются:

– оператор взаимодействия ρ ресурса сети и воздействий (угроз) РЭБ. В общем случае ρ — представляет собой оператор вида $(S, R)^{\rho} \to Z$, где Z — матрица наблюдений на входах приемных устройств различных информационных направлений сети связи. В частных случаях ρ может иметь вид «+» или «×»;

– L_{SR} — множество допустимых алгоритмов обработки наблюдений Z;

– U — множество допустимых алгоритмов правления ресурсом S;

– J_n — показатели качества функционирования отдельных информационных направлений; обобщенным показателем качества работы сети J.

Возможности противоборствующей стороны описываются стратегией системы РЭБ в виде стохастических матриц размером $N \times C$:

$$\|R\|^1_{N\times C} = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1C} \\ r_{21} & r_{22} & \dots & r_{2C} \\ \dots & \dots & \dots & \dots \\ r_{N1} & r_{N2} & \dots & r_{NC} \end{pmatrix}, \quad (3)$$

элементы которой r_{ij} трактуются как вероятности воздействия j-го варианта фактора угрозы (применительно к угрозе радиоэлектронного подавления — варианта помех) на i-й вариант информационного направления, причем

$$\sum_{j\in K} r_{ij} \le 1$$

Оптимизация сети связи по показателю качества

Управление сетью связи в условиях радиоэлектронной борьбы интерпретируется как поиск оптимального показателя качества функционирования сети J в условиях воздействия различных угроз. Основными факторами, меняющими частные показатели эффективности функционирования сети на всех уровнях рассмотрения, являются воздействия угроз, исходящих от системы радиоэлектронной борьбы: $J_n = J_n(S, R)$. Тогда для любого n-го элемента сети (сети в целом) может быть составлена матрица $\|J\|^n_{M\times C}$ частных показателей эффективности его функционирования, элементами которой g_{ij} будут показатели эффективности функционирования n-го элемента, если используется i-й вариант его реализации и j-й вариант воздействий:

$$\|J\|^1_{M\times C} = \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1C} \\ g_{21} & g_{22} & \dots & g_{2C} \\ \dots & \dots & \dots & \dots \\ g_{M1} & g_{M2} & \dots & g_{MC} \end{pmatrix}, \quad (4)$$

Если J выражается количественно, то задача оптимизации сети связи может быть сведена к задаче нахождения супремума или инфинума функционала J

$$\sup J\{S(u), R, Z(u)\} \quad (5)$$

в области, определяемой системой ограничений:

$$\begin{cases} S(u) \in S \\ R \in R \\ Z(u) \in Z \\ u \in U \end{cases} \quad (6)$$

Цель оптимизации состоит в выборе одной из матриц S_k, обеспечивающей наибольшую эффективность системы по введенному показателю качества. Если считать, что цель системы РЭБ противоборствующей стороны неизвестна, то оценкой эффективности выбора варианта управления ресурсом, на который оказывают воздействие угрозы РЭБ, при заданном показателе качества J, может являться

$$\inf_{R\in R} J(S, R) \quad (7)$$

Тогда из области гарантированных оценок, задаваемой (7), всегда можно выбрать наилучшее распределение линий по информационным направлениям, с учетом ограниченности ресурсов системы РЭБ и сети связи:

$$S_{\text{огр}} = \arg\max_{S\in S} \min_{R\in R} J(S, R) \quad (8)$$

$$J_{\text{огр}} = \arg\max_{S\in S} \min_{R\in R} J(S, R) \quad (9)$$

Выражение (9) дает нижнюю оценку значения оптимального гарантированного результата показателя качества функционирования сети связи в случае выбора ресурса $S_{\text{огр}}$. Физически это соответствует случаю, когда органы управления сетью связи, не располагая информацией о том, какие из известного класса воздействий угроз и по каким линиям сети будут использованы противоборствующей стороной, выбирают наилучшее распределение линий связи в предположении, что выбор будет известен.

Если в качестве обобщенного критерия эффективности функционирования сети связи выбрать критерий взвешенной по приоритетам суммы частных показателей (10),

$$J(S, R) = \sum_{i\in N} a_i J_i(S, R) \quad (10)$$

то математическая модель управления сетью связи в условиях РЭБ может быть построена следующим образом. Пусть рассматривается сеть связи, состоящая из N направлений информационного обмена, а система РЭБ противоборствующей стороны имеет возможность оказать C воздействий на любую из M типов линий.

Учитывая выражения (1–3), составим матричное произведение

$$\|\$\|_{M\times K} = \|S\|_{M\times N} \times \|A\|_{N\times M} \times \|R\|_{N\times C} \quad (11)$$

Состояние сети связи и системы РЭБ в некоторый дискретный момент времени представляет собой тензорное произведение:

$$\|H(n)\|_{M\times K} = \|\$\|_{M\times K} \otimes \|J\|_{M\times K} \quad (12)$$

Тогда интегральный показатель качества функционирования сети связи в условиях РЭБ может быть выражен через стратегии управления сетью связи и РЭБ следующим образом:

$$J\{S(n)R(n)\} = \|I\|_{1\times M} \times \|H(n)\|_{M\times C} \times \|I\|_{C\times 1} \quad (13)$$

где $\|I\|_{1\times M}$ *и* $\|I\|_{C\times 1}$ — единичные вектор-строка и вектор-столбец размером $1\times M$ и $1\times C$, соответственно.

Для описания стратегий сети связи и системы РЭБ используем стохастические матрицы вида (1) и (3), что позволит рассматривать задачу рационального управления сети связи в виде поиска оптимальных решений в классе стохастических игр. Непрерывные наблюдения за состоянием элементов сети связи и системы РЭБ в сочетании с принципами последовательного (пошагового) принятия решений превращает процесс оптимизации в многошаговый минимаксный процесс поиска наилучших распределений S_{ij}, обусловленных всеми предыдущими состояниями и наблюдений:

$$S^*(n) = \arg\begin{cases} \max_{S(n)/S(n-1),\ldots,S(0),R(n-1),\ldots,R(0)} \min_{R(1)/S(\mathbf{0}),R(0)} \\ \max_{S(0)/R(0)} \min_{R(0)\in R} J(S,R) \end{cases} \quad (14)$$

С целью упрощения решения задачи, учитывая высокую динамичность современных сетецентрических войн и возможность резких изменений обстановки, целесообразно использование марковских моделей, в которых учитываются только текущие и прогнозируемые (на основе текущих) состояния сети связи и системы РЭБ. Тогда задачу оптимального управления сетью связи можно рассматривать как задачу поиска наилучшей по показателю (13) стратегии ее поведения в виде условных распределений (1) по прогнозируемым на один шаг вперед стратегиям системы РЭБ (3):

$$S^+(n+1) = \\ = \arg\{\max_{S(n+)/R^*(n+1)} \min_{R^*(n+1)/S(n+1/n)} \max_{S(n+1)/R^*(n)} J(S,R)\} \quad (15)$$

Согласно (12) алгоритм поиска оптимальных решений для СС СН состоит из трех последовательно выполняемых этапов. Вначале, на основе разведки радиоэлектронной обстановки определяется вариант стратегии РЭБ $R(n)$, применяющийся на n-м этапе (цикле управления); определяется оптимальное для данной обстановки распределение ресурсов сети связи $S(n+1/n)$, путем максимизации (13):

$$S(n+1/n) = \arg\max_{S\in S} J(S, R^*(n)\} \quad (16)$$

Затем решается противоположная задача для системы РЭБ противоборствующей стороны с целью найти прогнозируемое распределение помех и объектов поражения огневыми средствами и оружием функционального поражения $R^*(n+1)$:

$$R^*(n+1/n) = \arg\min_{R\in R} J(S(n+1), R\} \quad (17)$$

Далее определяется наилучшее по прогнозируемым воздействиям распределение ресурсов сети связи на следующий (n+1)-й цикл управления:

$$S^*(n+1) = \arg\max_{S\in S} J\{S, R^*(n+1)\} \quad (18)$$

Сформулированный в виде соотношений (15–18) алгоритм оптимального управления сетью связи позволяет существенно упростить процедуру поиска рациональных стратегий, разбив ее на ряд последовательно решаемых задач максимизации и минимизации. Предложенная модель взаимодействия сети связи и системы РЭБ противоборствующей стороны является достаточно общей и в сочетании с принципом максимина (8), (9) позволяет описывать процессы выбора оптимальных стратегий в достаточно широком классе целей функционирования и решаемых задач. Конкретные цели функционирования определяются физическим смыслом, вкладываемым в частные показатели качества J_i. Например, в случае решения задачи по оценке эффективности сети связи при задании частных показателей качества в виде связности отдельных информационных направлений в условиях РЭБ, критерий (13) будет характеризовать взвешенную по важности суммарную связность сети связи, а решение задачи оптимизации (5), (6) позволит обеспечить либо максимально гарантированную связность сети в условиях РЭБ, либо максимальное число информационных направлений связи, работающих с заданной связностью. Стратегию РЭБ можно задавать через алгоритм целераспределения [5].

Программно-алгоритмическое обеспечение

Так как задача поиска показателя качества J относится к классу NP-трудных, она не может быть решена за приемлемое время путём прямого перебора; для ее решения требуется разработка специального программно-алгоритмического обеспечения, обеспечивающего приближенное рациональное решение. Такое программно-алгоритмическое обеспечение может быть использовано программно-аппаратных комплексах систем управления сетями связи и боевых информационно управляющих системах. Обобщённый вариант алгоритмического обеспечения представлен на рис. 3.

Программно-алгоритмическое обеспечение должно создаваться на основе современных программных платформ, с использованием технологии объектно-ориентированного программирования. Прототип системы программного обеспечения написан на программно-алгоритмическом языке C#. Приложение реализовано с использованием стандартных элементов управления, имеет эргономичный интерфейс, обеспечивает вывод данных на

Рис. 3. Обобщённый алгоритм функционирования

экран монитора. Программно-алгоритмическое обеспечение позволяет по заданным параметрам (ресурсу сети, возможностям противоборствующей стороны, перечню доступных направлений связи и их приоритетности) смоделировать возможные стратегии РЭБ с целью выбора оптимальной стратегии противодействия средствам радиоэлектронной борьбы противника, обеспечив снижение объёма причиняемого ущерба.

Литература

1. *Белоус К. В.*, *Курносов В. И.* Задачи оценки эффективности функционирования сетей связи Единой системы управления органов государственной власти, применительно к условиям радиоэлектронного противодействия // Материалы IV-й научно-практической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании». Кн.1. СПб.: СПбГУТ, 2015.

2. *Антонюк Л. Я.*, *Игнатов В. В.* Эффективность радиосвязи и методы её оценки. СПб: Военная академия связи имени Маршала Советского Союза С.М. Буденного, 1994. 138 с.

3. *Бураченко Д. Л.*, *Савищенко Н. В.* Сигнальные конструкции. Ч. 1–3. СПб: СПбГУТ, 2004. 240 с.

4. *Барабаш П. А.*, *Воробьев С. П.*, *Курносов В. И.*, *Советов Б. Я.* Инфокоммуникационные технологии в глобальной информационной инфраструктуре. СПб.: Наука, 2008. 550 с.

5. *Курносов В. И.*, *Лихачев А. М.* Методология проектных исследований и управление качеством сложных технических систем электросвязи. СПб.: Тирекс, 1998. 496 с.

AUTOMATED OPERATOR WORKPLACE OF COMMUNICATIONS NETWORK SPECIAL PURPOSE POINT

Galina V. Verkhova,
Saint-Petersburg, Russia, galina500@inbox.ru

Konstantin V. Belous,
Saint-Petersburg, Russia, kostos2@yandex.ru

ABSTRACT
The article presents the results of scientific research in the field of automated control network a special purpose in the application of enemy electronic warfare. Given the authors developed the system of integrated indicators of efficiency of functioning of a communication network, which is formed in a hierarchical system in accordance with the unified methodological concept of construction of information systems providing for the examination of any network of information exchange from the standpoint of the reference model for open systems interconnection (OSI). This approach will allow for the use of the system of quality indicators to evaluate and manage all departmental communication networks comprising the infocommunication environment of the Unified information space of the Russian Federation.

Managing communication network in terms of electronic warfare was governed as the search for the best indicator of the quality of functioning of the network in terms of the impact of various threats. The main factors that change the specific indicators of efficiency of functioning of networks at all levels of review are the impact of threats from electronic warfare systems. As the problem of finding optimal strategies for the management network special purpose belongs to the class NP-hard, it cannot be solved in reasonable time by brute force; it requires the development of specific software and algorithmic support, which provides an approximate rational decision. Such algorithmic software can be used in the software and hardware complexes of control systems communication networks and combat information control systems.
Algorithmic software should be based on modern software platforms, technology of object-oriented programming. A prototype of a software system had written in a software programming language C#. The application is implemented using the standard controls, has an ergonomic interface that provides a data output on the screen. Program-algorithmic support allows on the specified parameters (the network capabilities of the opposing side, the list of available destinations and their priority) to simulate possible strategies EW to select the optimal strategy of counter-electronic warfare of the enemy, provided the decline in damage caused.

Keywords: interactive educational and methodical complex; electronic learning; virtual enterprises; cyber environment; a single information educational space; multimedia educational content.

References

1. Belous K.V., Kurnosov V.I. Zadachi ocenki jeffektivnosti funkcionirovanija setej svjazi Edinoj sistemy upravlenija organov gosudarstvennoj vlasti, primenitel'no k uslovijam radiojelektronnogo protivodejstvija [The tasks of assessing the effectiveness of the functioning of communication networks of the Unified Management System of public authorities, in relation to the conditions of electronic countermeasures]. *Materialy IV-j nauchno-prakticheskoj konferencii "Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii"* [Materials of the IV-th scientific-practical conference "Actual problems of information telecommunications in science and education"]. St. Petersburg: Sankt-Peterburgskiy gosudarstvennyy universitet telekommunikatsiy im. prof. M.A. Bonch-Bruevicha Pulb., 2015. (in Russian)
2. Antonjuk L. Ja., Ignatov V.V. *Jeffektivnost' radiosvjazi i metody ejo ocenki* [The effectiveness of radio communication and methods for its evaluation]. St. Petersburg: Voennaya akademiya svyazi Pulb., 1994. 138 p. (In Russian)
3. Burachenko D.L., Savishhenko N.V. *Signal'nye konstrukcii* [Signaling structures]. In 3 part. St. Petersburg: Sankt-Peterburgskiy gosudarstvennyy universitet telekommunikatsiy im. prof. M.A. Bonch-Bruevicha Pulb., 2004. 240 p. (In Russian)
4. Barabash P.A., Vorob'ev S.P., Kurnosov V.I., Sovetov B. Ya. Infokommunikacionnye tehnologii v global'noj informacionnoj infrastrukture. [Infocommunication technologies in the global information infrastructure] St. Petersburg: Nauka, 2008. 552 p. (In Russian)
5. Kurnosov V.I., Lihachev A.M. *Metodologija proektnyh issledovanij i upravlenie kachestvom slozhnyh tehnicheskih sistem jelektrosvjazi* [Methodology of design studies and quality management of complex technical telecommunication systems]. St. Petersburg: Tireks, 1998. 496 p. (In Russian)

Information about authors:

Verkhova G. V., PhD, professor, head of the department of telecommunications companies automation, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.
Belous K. V., PhD, assistant professor of department of telecommunications companies automation, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.

For citation: Verkhova G.V., Belous K.V. Automated operator workplace of communications network special purpose point. *H&ES Research*. 2017. Vol. 9. No. 2. Pp. 18–23. (In Russian)

ФОРМИРОВАНИЕ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА-МИЛЛСА-ВЕЛЧА

Стародубцев Виктор Геннадьевич,
к.т.н., доцент, доцент Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики,
г. Санкт-Петербург, Россия, vgstarod@mail.ru

Бородько Денис Николаевич,
к.т.н., старший преподаватель Военно-космической академии имени А.Ф. Можайского,
г. Санкт-Петербург, Россия, denisborodko@yandex.ru

Попов Антон Михайлович,
слушатель Военно-космической академии имени А.Ф. Можайского,
г. Санкт-Петербург, Россия, antony57rus@gmail.com

АННОТАЦИЯ

Введение: широкополосные сигналы с хорошими корреляционными свойствами, формируемые на основе псевдослучайных последовательностей, используются в системах спутниковой связи, в системах навигационного обеспечения, а также в системах радиолокации. В современных телекоммуникационных системах наряду с требованиями по корреляционным свойствам к псевдослучайным последовательностям предъявляются повышенные требования по структурной скрытности. Необходимость применения последовательностей Гордона-Миллса-Велча в современных системах связи, навигации и радиолокации, к которым предъявляются жесткие требования по конфиденциальности и структурной скрытности, определяется их более высокой эквивалентной линейной сложностью по сравнению с М-последовательностями, которые также обладают одноуровневой периодической автокорреляционной функцией. Широкому применению ГМВ-последовательностей в системах передачи информации мешает отсутствие практически реализуемых алгоритмов их формирования. **Цель:** разработка алгоритма синтеза устройств формирования ГМВ-последовательностей на основе совокупности регистров сдвига. Решаемые задачи: разработка алгоритма формирования проверочных полиномов ГМВ-последовательностей, основанного на использовании структурных свойств конечных полей с двойным расширением и алгоритма определения начальных состояний регистров сдвига, входящих в устройство формирования, полиномы которых задаются произведением нескольких неприводимых полиномов. При проведении исследований используется математический аппарат теории сигналов и теории конечных полей. **Результаты**: разработан алгоритм синтеза устройств формирования ГМВ-последовательностей на основе совокупности регистров сдвига с линейными обратными связями, в состав которого входят алгоритм формирования проверочных полиномов ГМВ-последовательностей и алгоритм определения начальных состояний регистров сдвига. Получен полный перечень проверочных полиномов для двоичных ГМВ-последовательностей с периодом N = 63. Для периода N = 255 получено распределение корней полиномов-сомножителей проверочного полинома для произвольной базисной М-последовательности. Распределение корней позволяет однозначно определять начальные состояния регистров сдвига через символы базисной М-последовательности. **Практическая значимость:** полученные результаты позволяют применять ГМВ-последовательности вместо М-последовательностей в системах передачи информации по широкополосным радиоканалам, к которым предъявляются повышенные требования по конфиденциальности. Эквивалентная линейная сложность ГМВ-последовательностей на на 3-6 дБ превышает значения для М-последовательностей. С увеличением периода выигрыш по ЭЛС возрастает. Алгоритм может найти применение для разработки методов формирования других классов псевдослучайных последовательностей, допускающих аналитическое представление в конечных полях.

Ключевые слова: псевдослучайные последовательности; конечные поля; неприводимые и примитивные полиномы; функция корреляции; эквивалентная линейная сложность; регистры сдвига.

Для цитирования: *Стародубцев В.Г., Бородько Д.Н., Попов А.М.* Формирование двоичных последовательностей Гордона-Миллса-Велча // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 24–31.

Одним из направлений развития систем передачи информации является применение широкополосных сигналов на основе псевдослучайных последовательностей (ПСП) Данные ПСП могут быть использованы как в целях обеспечения синхронизации в качестве скремблирующих последовательностей, так и в виде последовательностей, расширяющих спектр передаваемых сигналов для широкополосных радиоканалов [1–3].

Широкополосные сигналы используются в системах спутниковой связи, в системах навигационного обеспечения, а также в системах радиолокации [4–6].

В качестве ПСП широко применяются М-последовательности (МП), последовательности Голда, малого и большого множеств Касами и др [7].

Основной причиной применения МП в системах связи, навигации и радиолокации является тот факт, что они обладают одноуровневой периодической автокорреляционной функцией (ПАКФ) при достаточно простой аппаратурной реализации в виде регистра сдвига с линейными обратными связями (РС ЛОС).

К недостаткам МП можно отнести низкую структурную скрытность, которая численно характеризуется эквивалентной линейной сложностью (ЭЛС). ЭЛС зависит от степени проверочного полинома, задающего ПСП, и численно равна количеству символов последовательности, которые необходимо принять для определения проверочного полинома, по которому строится данная последовательность.

Решению задачи повышения ЭЛС ПСП при условии сохранения авто и взаимно-корреляционных свойств посвящено большое количество работ как в нашей стране, так и за рубежом [8–11].

Среди циклических последовательностей, обладающих наряду с МП одноуровневой ПАКФ, можно выделить последовательности Гордона-Миллса-Велча (ГМВП), которые обладают более высокой ЭЛС и соответственно более высокой структурной скрытностью [12–15]. Данное свойство определяет приоритетность применения ГМВП в системах связи, навигации и радиолокации, к которым предъявляются жесткие требования по конфиденциальности.

В настоящее время широкому применению ГМВП в системах передачи информации мешает отсутствие алгоритмов формирования проверочных полиномов и алгоритмов определения начальных состояний РС ЛОС, входящих в устройства формирования ГМВП.

Целью статьи является разработка алгоритма синтеза устройств формирования ГМВП на основе совокупности РС ЛОС.

Для достижения поставленной цели в статье решаются следующие задачи.

1. Разработка алгоритма формирования проверочных полиномов ГМВП, основанного на использовании структурных свойств конечных полей с двойным расширением.

2. Разработка алгоритма определения начальных состояний РС ЛОС, входящих в устройство формирования ГМВП, проверочные полиномы которых задаются произведением нескольких неприводимых полиномов.

При решении поставленных задач используется математический аппарат теории сигналов и теории конечных полей (полей Галуа).

ГМВП формируются над конечными полями с двойным расширением вида $GF[(p^m)^n]$, вследствие чего период данных последовательностей является составным числом, то есть $N = p^{mn} - 1$, где p-характеристика поля, m, n — натуральные числа. В настоящее время широкое применение получили двоичные ГМВП над полями с двойным расширением вида $GF[(2^m)^n]$. Символы d_i данных последовательностей с периодом $N = 2^{mn}–1$ формируются в соответствии с выражением [13–15]

$$d_i = \mathrm{tr}_{m,1}[(\mathrm{tr}_{mn,\,m}(\alpha^i))^r],\ 1 \le r < 2^m - 1,\ (r,\ 2^m - 1) = 1, \qquad (1)$$

где $\mathrm{tr}_{mn,\,m}(\cdot)$ — след элемента из поля с двойным расширением $GF[(2^m)^n]$ в расширенном поле $GF(2^m)$; $\mathrm{tr}_{m,1}(\cdot)$ — след элемента из расширенного поля $GF(2^m)$ в простом поле GF(2); $\alpha \in GF[(2^m)^n]$ — примитивный элемент поля с двойным расширением. Параметр r является числом, взаимно простым с порядком мультипликативной группы расширенного поля $GF(2^m)$, который равен $2^m –1$.

В настоящее время общий алгоритм формирования проверочных полиномов ГМВП в известной литературе отсутствует. Для каждой конкретной последовательности проверочный полином определяется итеративным путем, например, с помощью алгоритма Берлекемпа-Месси.

Разработка предлагаемого алгоритма основана на использовании структурных свойств конечных полей с двойным расширением и проводится на примере двоичной ГМВП с составным периодом $N = 63$, сформированной с учетом базисной МП с аналогичным периодом и проверочным полиномом $h_{\text{мп}}(x) = x^6+x+1$. Символы МП записываются построчно в виде матрицы размерности $[J \times L] = [7 \times 9]$, в которой ненулевые столбцы соответствуют различным сдвигам «короткой» МП с периодом $J = 7$, называемой характеристической последовательностью (ХП), а параметр L характеризует число таких сдвигов [12–13]

$$\mathbf{F}_{\text{МП}} = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}. \qquad (2)$$

С использованием алгоритма формирования ГМВП, основанного на матричном представлении МП с составным периодом [13], формируется ГМВП с периодом $N = 63$, которая также представляется в виде матрицы размерности $[J \times L] = [7 \times 9]$

$$\mathbf{F}_{\Gamma} = \begin{vmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{vmatrix}. \qquad (3)$$

Алгоритм формирования ГМВП с помощью матричного представления МП основан на замене в каждом столбце матрицы ХП на другую МП с аналогичным периодом.

Затем определяется полином для ГМВП вида (3) с помощью алгоритма Берлекемпа-Месси

$$h_г(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^2 + 1. \quad (4)$$

Данный полином является произведением неприводимых над полем $GF(2)$ полиномов меньших степеней. Для их определения используется полный перечень неприводимых над $GF(2)$ полиномов степени 6, корнями которых являются элементы расширенного поля $GF(2^6)$. Данные полиномы, их корни с минимальным показателем степени, а также периоды корней представлены в табл. 1.

Таблица 1

Неприводимые полиномы в поле $GF(2^6)$

Корни полиномов	Полиномы $h_i(x)$	Период корней
α^1	$h_1(x) = x^6 + x + 1$	63
α^3	$h_2(x) = x^6 + x^4 + x^2 + x + 1$	21
α^5	$h_3(x) = x^6 + x^5 + x^2 + x + 1$	63
α^{11}	$h_4(x) = x^6 + x^5 + x^3 + x^2 + 1$	63
α^{31}	$h_5(x) = x^6 + x^5 + 1$	63
α^{15}	$h_6(x) = x^6 + x^5 + x^4 + x^2 + 1$	21
α^{23}	$h_7(x) = x^6 + x^5 + x^4 + x + 1$	63
α^{13}	$h_8(x) = x^6 + x^4 + x^3 + x + 1$	63
α^7	$h_9(x) = x^6 + x^3 + 1$	9
α^9	$h_{10}(x) = x^3 + x + 1$	7
α^{27}	$h_{11}(x) = x^3 + x^2 + 1$	7
α^{21}	$h_{12}(x) = x^2 + x + 1$	3

Искомые неприводимые полиномы определяются путём последовательного деления $h_г(x)$ на $h_i(x)$. В результате получим, что $h_г(x)$ вида (4) может быть представлен в виде произведения двух полиномов $h_{ci}(x)$ шестой степени

$$h_г(x) = h_{c1}(x)h_{c2}(x) = h_2(x)h_3(x) =$$
$$= (x^6 + x^4 + x^2 + x + 1)(x^6 + x^5 + x^2 + x + 1) \quad (5)$$

Для поля $GF(2^6)$ можно показать, что корни полинома $h_{c1}(x) = h_2(x)$ являются 3-ми степенями корней полинома $h_{мп}(x)$, а корни полинома $h_{c2}(x) = h_3(x)$ являются 5-ми степенями его корней.

Алгоритм формирования полной совокупности проверочных полиномов ГМВП основан на свойстве повторяемости соотношений между корнями проверочного полинома $h_{мп}(x)$ исходной МП и корнями полиномов $h_{c1}(x)$ и $h_{c2}(x)$, являющихся сомножителями проверочного полинома $h_г(x)$ [16].

Известно [7], что в поле $GF(2^6)$ существует шесть различных примитивных полиномов, которые могут выступать в качестве проверочных полиномов при формировании МП. Таким образом, для шести МП с периодом $N = 63$ можно получить шесть ГМВП и, соответственно, шесть проверочных полиномов двенадцатой степени.

В качестве примера сформируем проверочный полином ГМВП, основанной на МП с полиномом $h_{мп}(x) = h_7(x) = x^6 + x^5 + x^4 + x + 1$, одним из корней которого является элемент α^{23} (см. табл. 1).

Полиномы-сомножители для $h_г(x) = h_{c1}(x)h_{c2}(x)$ определяются следующим образом. Исходный полином $h_{мп}(x)$ имеет корень α^{23}. Тогда одним из корней полинома $h_{c1}(x)$ должен быть элемент $(\alpha^{23})^3 = \alpha^{69 \bmod 63} = \alpha^6$, что соответствует полиному $h_{c1}(x) = h_2(x) = x^6 + x^4 + x^2 + x + 1$.

Заметим, что полином $h_{c1}(x) = h_2(x)$ является сомножителем и в выражении (5) для ГМВП вида (3).

Полином $h_{c2}(x)$ должен иметь корень $(\alpha^{23})^5 = \alpha^{115 \bmod 63} = \alpha^{52}$, что соответствует полиному $h_{c2}(x) = h_8(x) = x^6 + x^4 + x^3 + x + 1$.

Искомый проверочный полином для ГМВП

$$h_г(x) = h_2(x)h_8(x) = x^{12} + x^9 + x^7 + x^6 + x^5 + x^4 + 1.$$

Аналогичные вычисления для остальных примитивных полиномов поля $GF(2^6)$ позволяют сформировать полный перечень проверочных полиномов для ГМВП с периодом $N = 63$, представленный в табл. 2.

Разработанный алгоритм может быть использован для формирования совокупности проверочных полиномов ГМВП в виде произведения неприводимых полиномов для произвольного поля $GF[(p^m)^n]$.

Структура проверочного полинома ГМВП $h_г(x)$, представляющего собой для конечных полей $GF[(p^m)^n]$ произведение двух или более неприводимых полиномов $h_{ci}(x)$ степени $S = mn$, определяет возможность построения устройства формирования в виде совокупности нескольких РС ЛОС.

Устройство формирования представляет собой два или более РС ЛОС, число ячеек $Я_i$ в каждом из которых равно S, т.е. степени полиномов $h_{ci}(x)$, а сумматоры по mod p расставляются в соответствии с коэффициентами этих полиномов. Выходные сигналы РС ЛОС поступают на общий сумматор по mod p, являющийся выходом устройства.

Таблица 2

Полиномы ГМВП с периодом $N = 63$

$h_{гi}(x)$	Полиномы-сомножители ГМВП $h_{c1}(x)\,h_{c2}(x)$	Полиномы базисных МП
$h_{г1}(x)$	$h_2(x)h_3(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^2 + 1$	$h_1(x)$
$h_{г2}(x)$	$h_6(x)h_4(x) = x^{12} + x^8 + x^7 + x^6 + x^5 + x^3 + 1$	$h_3(x)$
$h_{г3}(x)$	$h_2(x)h_5(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$	$h_4(x)$
$h_{г4}(x)$	$h_6(x)h_7(x) = x^{12} + x^{10} + x^5 + x^3 + x^2 + x + 1$	$h_5(x)$
$h_{г5}(x)$	$h_2(x)h_8(x) = x^{12} + x^9 + x^7 + x^6 + x^5 + x^4 + 1$	$h_7(x)$
$h_{г6}(x)$	$h_6(x)h_1(x) = x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1$	$h_8(x)$

Основным препятствием для широкого применения устройств формирования ГМВП на основе регистров сдвига является отсутствие в литературе алгоритмов определения их начальных состояний.

Поэтому второй задачей, решаемой в данной статье, является разработка алгоритма определения начальных состояний при построении устройств формирования ГМВП на основе совокупности РС ЛОС.

Разработанный алгоритм основан на использовании следующего структурного свойства проверочных полиномов: корни полиномов $h_{ci}(x)$ — сомножителей полинома $h_{гмв}(x)$ — являются фиксированными степенями корней полинома $h_{мп}(x)$ базисной МП, на основе которой формируется ГМВП [17].

В рамках алгоритма необходимо определить начало базисной МП в соответствии с (1) при $r = 1$, а затем провести децимацию символов данной МП по индексам децимации, равным наименьшим показателям степени корней полиномов $h_{ci}(x)$.

Одним из способов определения начала МП, то есть символов d_0, d_1, d_2 и т.д., является использование свойства примитивных полиномов, согласно которому для конечных полей характеристики $p = 2$ значение функции следа $\mathrm{tr}_{s,1}\alpha^1$ равно значению коэффициента при $(S - 1)$-й степени переменной x полинома $h_{мп}(x)$, а значение функции следа $\mathrm{tr}_{s,1}\alpha^{-1}$ — значению коэффициента при первой степени переменной x.

Для полинома $h_{мп}(x) = x^6 + x + 1$ функции следа $\mathrm{tr}_{6,1}\alpha^1 = 0$, $\mathrm{tr}_{6,1}\alpha^{-1} = 1$. Тогда символу d_1 МП в (2) соответствует позиция, для которой сумма 1, 2, 4, 8, 16 и 32-го символов (каждая позиция по очереди считается первой) равна нулю. Такая позиция единственная, и ей соответствует первый символ в первой строке матрицы (2). Для дальнейшего анализа МП записывается, начиная с символов $d_0 = 0$, $d_1 = 0$, $d_2 = 0$, $d_3 = 0$ и т.д. (см. табл. 3).

Таблица 3

МП с $h_{мп}(x) = x^6 + x + 1$ и периодом $N = 63$

i	0	1	2	3	4	5	6	7	8
d_i	0	0	0	0	0	1	0	0	0
i	9	10	11	12	13	14	15	16	17
d_i	0	1	1	0	0	0	1	0	1
i	18	19	20	21	22	23	24	25	26
d_i	0	0	1	1	1	1	0	1	0
i	27	28	29	30	31	32	33	34	35
d_i	0	0	1	1	1	0	0	1	0
i	36	37	38	39	40	41	42	43	44
d_i	0	1	0	1	1	0	1	1	1
i	45	46	47	48	49	50	51	52	53
d_i	0	1	1	0	0	1	1	0	1
i	54	55	56	57	58	59	60	61	62
d_i	0	1	0	1	1	1	1	1	1

Затем формируется ПСП с проверочным полиномом $h_{c1}(x) = x^6 + x^4 + x^2 + x + 1$, корни которого являются третьими степенями корней полинома $h_{МП}(x)$ и имеют период $\varepsilon = 21$. Полином $h_{c1}(x)$ является неприводимым, но не примитивным. Соответственно период псевдослучайной последовательности $N = 21$, и она представляет собой последовательность функций следа для элементов α^0, α^3, α^6, α^9,…, α^{54}, α^{57}, α^{60}, т.е. набор символов исходной МП d_0, d_3, d_6, d_9, …, d_{54}, d_{57}, d_{60}. Процесс формирования этой последовательности можно интерпретировать как децимацию базисной МП по индексу децимации $I_{d1} = 3$. При этом начала обеих последовательностей связаны между собой.

Так же формируется МП с проверочным полиномом $h_{c2}(x) = x^6 + x^5 + x^2 + x + 1$, корни которого являются пятыми степенями корней полинома $h_{мп}(x)$ и имеют период $\varepsilon = 63$. Полином $h_{c2}(x)$ является примитивным, поэтому период данной МП $N = 63$. Она представляет собой последовательность функций следа для элементов α^0, α^5, α^{10}, α^{15},…, α^{48}, α^{53}, α^{58}. Процесс формирования этой последовательности также можно интерпретировать как децимацию базисной МП, но по индексу децимации $I_{d2} = 5$.

Начальные состояния регистров сдвига, построенных в соответствии с коэффициентами неприводимых полиномов, являющихся сомножителями проверочного полинома ГМВП, определяются начальными сегментами длиной S формируемых последовательностей [17].

На практике начальные состояния регистров сдвига определяются децимацией символов базисной МП по соответствующему индексу децимации, начиная с символа d_0. Для двоичных ГМВП с периодом $N = 63$ $I_{d1} = 3$, $I_{d2} = 5$.

Начальное состояние РС ЛОС с полиномом $h_{c1}(x)$ определяется символами d_0, d_3, d_6, d_9, d_{12}, d_{15}, а с полиномом $h_{c2}(x)$ — символами d_0, d_5, d_{10}, d_{15}, d_{20}, d_{25} базисной МП.

Алгоритм синтеза устройств формирования ГМВП на основе совокупности РС ЛОС представляется как совокупность двух разработанных алгоритмов.

1. Задание проверочного полинома базисной МП с периодом $N = p^{mn} - 1$.

2. Формирование МП и определение начала последовательности, то есть символов d_0, d_1, d_2 и т.д.

3. Формирование ГМВП из базисной МП путем замены ХП при ее матричном представлении.

4. Определение проверочного полинома ГМВП $h_г(x)$

5. Определение полиномов-сомножителей $h_{ci}(x)$ для проверочного полинома ГМВП $h_г(x)$ и построение соответствующих регистров сдвига с обратными связями. Показатели степени корней полиномов-сомножителей соответствуют индексам децимации.

4. Определение начальных состояний регистров сдвига из символов базисной МП в соответствии с полученными индексами децимации.

5. Формирование последовательностей с проверочными полиномами-сомножителями $h_{ci}(x)$ для полученных начальных состояний.

6. Формирование искомой ГМВ-последовательности путем посимвольного сложения последовательностей на выходах регистров сдвига.

Для рассмотренной базисной МП с полиномом $h_{мп}(x) = x^6 + x + 1$ и периодом $N = 63$ устройство формирования ГМВП показано на рис. 1.

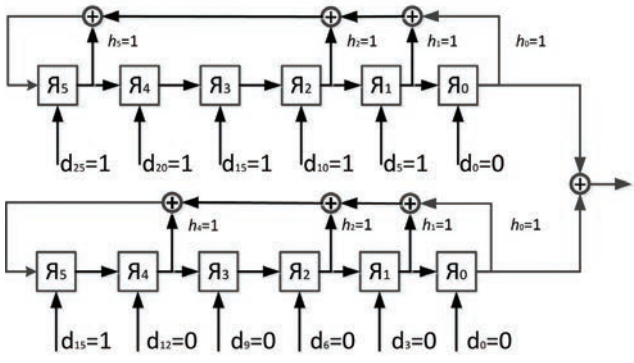


Рис. 1. Устройство формирования ГМВП на основе полинома базисной МП $h_{мп}(x) = x^6 + x + 1$

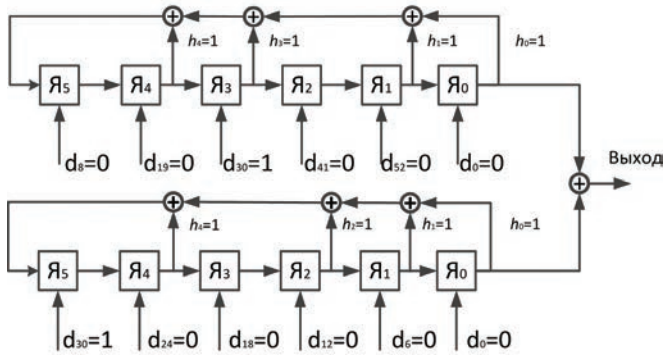


Рис. 2. Устройство формирования ГМВП на основе полинома базисной МП $h_{мп}(x) = x^6 + x^5 + x^4 + x + 1$

На выходе верхнего регистра формируется МП с полиномом $h_{c2}(x) = x^6 + x^5 + x^2 + x + 1$, начальные состояния выбираются из табл. 3: $d_0 = 0$, $d_5 = d_{10} = d_{15} = d_{20} = d_{25} = 1$.

На выходе нижнего регистра формируется последовательность с проверочным полиномом $h_{c1}(x) = x^6 + x^4 + x^2 + x + 1$, начальные состояния также выбираются из табл. 3: $d_0 = d_3 = d_6 = d_9 = d_{12} = 0$, $d_{15} = 1$. Период данной последовательности $N = 21$, поэтому на одном периоде МП с верхнего регистра укладывается три периода ПСП с нижнего регистра.

Сумматоры по модулю 2 в цепи обратной связи регистров сдвига расставляются в соответствии с коэффициентами проверочных полиномов $h_{c2}(x)$ и $h_{c1}(x)$.

Первая ГМВП с периодом $N = 63$ формируется на выходе общего сумматора по модулю 2.

Для базисной МП с проверочным полиномом $h_{мп}(x) = h_7(x) = x^6 + x^5 + x^4 + x + 1$ и периодом $N = 63$ устройство формирования ГМВП показано на рис. 2.

Структура нижнего регистра осталась без изменений. Значения начальных состояний также остались прежними, хотя номера символов базисной МП изменились. На выходе регистра формируется ПСП с периодом $N = 21$.

На выходе верхнего регистра формируется МП с полиномом $h_{c2}(x) = h_8(x) = x^6 + x^4 + x^3 + x + 1$.

Особенность алгоритма определения начальных состояний регистров сдвига заключается в том, что для получения значений начальных состояний не требуется формирование новой базисной МП. Номера символов для начальных состояний регистров определяются путем двойной децимации символов базисной МП из табл. 3. Новые индексы децимации определяются умножением индексов $I_{d1} = 3$ и $I_{d2} = 5$ на показатель степени корня полинома новой базисной МП $h_{мп}(x) = x^6 + x^5 + x^4 + x + 1$, равный 23: $I_{d3} = 23 I_{d1} \bmod 63 = 6$, $I_{d4} = 23 I_{d2} \bmod 63 = 52$.

Для нижнего регистра начальные состояния выбираются из табл. 3 с индексом децимации $I_{d3} = 6$: $d_0 = d_6 = d_{12} = d_{18} = d_{24} = 0$, $d_{30} = 1$.

Для верхнего регистра начальные состояния также выбираются из табл. 3, но с индексом децимации $I_{d4} = 52$: $d_0 = d_{52} = d_{41} = 0$, $d_{30} = 1$ $d_{19} = d_8 = 0$. Вычисление номеров символов выполняется по mod 63.

Новая ГМВП с периодом $N = 63$ формируется на выходе общего сумматора по модулю 2.

В соответствии с разработанным алгоритмом получено распределение корней полиномов-сомножителей для ГМВП с периодом $N = 255$ относительно произвольной базисной МП с тем же периодом. Они являются соответственно 7-й, 11-й, 13-й и 37-й степенями корней полинома базисной МП. При этом степень полинома ГМВП равна 32, то есть ЭЛС ГМВП на 6 дб превышает ЭЛС МП.

Таким образом, в статье разработан алгоритм синтеза устройств формирования ГМВП на основе совокупности РС ЛОС, в состав которого входят алгоритм формирования проверочных полиномов ГМВП и алгоритм определения начальных состояний регистров сдвига.

Для произвольного примитивного полинома, выбранного для базисной МП, начальные состояния определяются путем двойной индексации символов базисной МП с учетом показателей степени как корней ее полинома, так и полиномов-сомножителей. При этом не требуется вычисление непосредственно проверочного полинома для ГМВП.

Полученные результаты позволяют применять ГМВП вместо МП в системах передачи информации по широкополосным радиоканалам, к которым предъявляются повышенные требования по конфиденциальности, включая требования по повышению их структурной скрытности.

В качестве показателя структурной скрытности выступает ЭЛС, значения которой для ГМВП на 3–6 дБ превышают значения для МП с аналогичными периодами. С увеличением периода выигрыш по ЭЛС возрастает.

Получен полный перечень проверочных полиномов для двоичных ГМВП с периодом $N = 63$. Для периода $N = 255$ получено распределение корней полиномов-сомножителей для $h_г(x)$, однозначно определяющее начальные состояния регистров сдвига через символы базисной МП.

Данные полиномы могут быть использованы при разработке как программных методов формирования ГМВ-

последовательностей, так и устройств формирования, основанных на регистрах сдвига с линейными обратными связями.

Также представленный алгоритм может найти применение для разработки методов формирования других классов псевдослучайных последовательностей, допускающих аналитическое представление в конечных полях.

Литература

1. *Ипатов В.П.* Широкополосные системы и кодовое разделение сигналов. Принципы и приложения: пер. с англ. / под ред. В.П. Ипатова. М.: Техносфера. 2007. 488 с.

2. *Вишневский В.М.*, *Ляхов А.И.*, *Портной С.Л.*, *Шахнович И.В.* Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. 592 с.

3. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение: пер. с англ. Изд. 2-е, испр. М.: Вильямс, 2003. 1104 с.

4. CDMA: прошлое, настоящее, будущее / под ред. Л.Е. Варакина и Ю.С. Шинакова. М.: МАС, 2003. 608 с.

5. *Ershen Wang*, *Shufang Zhang*, *Qing Hu*. GPS Correlator Research and FPGA Implementation // Journal of System Simulation. 2008. Vol. 20. Pp. 3582–3585.

6. *Golomb S.W.*, *Gong G.* Signal Design for Good Correlation for Wireless Communication, Criptography and Radar. Cambridge University Press. 2005. 438 p.

7. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.

8. *Прозоров Д.Е.*, *Смирнов А.В.*, *Баланов М.Ю.* Алгоритм быстрой кодовой синхронизации шумоподобных сигналов, построенных на последовательностях повышенной структурной сложности // Вестник РГРТУ. 2015. № 1 (51). С. 3–9.

9. *Golomb S.W.* Two-valued sequences with perfect periodic autocorrelation // IEEE Transactions on Aerospace and Electronic Systems. 1992. Vol. 28. No. 2. Pp. 383–386.

10. *Lie-Liang Yang*, *Hanzo L.* Acquisition of m-sequences using recursive soft sequential estimation // Wireless Communications and Networking. 2003. Vol. 1. Pp. 683–687.

11. *Cho Chang-Min*, *Kim Ji-Youp*, *No Jong-Seon*. New p-ary sequence families of period (p^n-1)/2 with good correlation property using two decimated m-sequences // IEICE Transactions on Communications. 2015. Vol. E98. No. 7. Pp. 1268–1275.

12. *Юдачев С.С.*, *Калмыков В.В.* Ансамбли последовательностей GMW для систем с кодовым разделением каналов // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2012. № 1. URL: http:// elibrary.ru/item.asp?id=17650851 (дата обращения 13.01.2017).

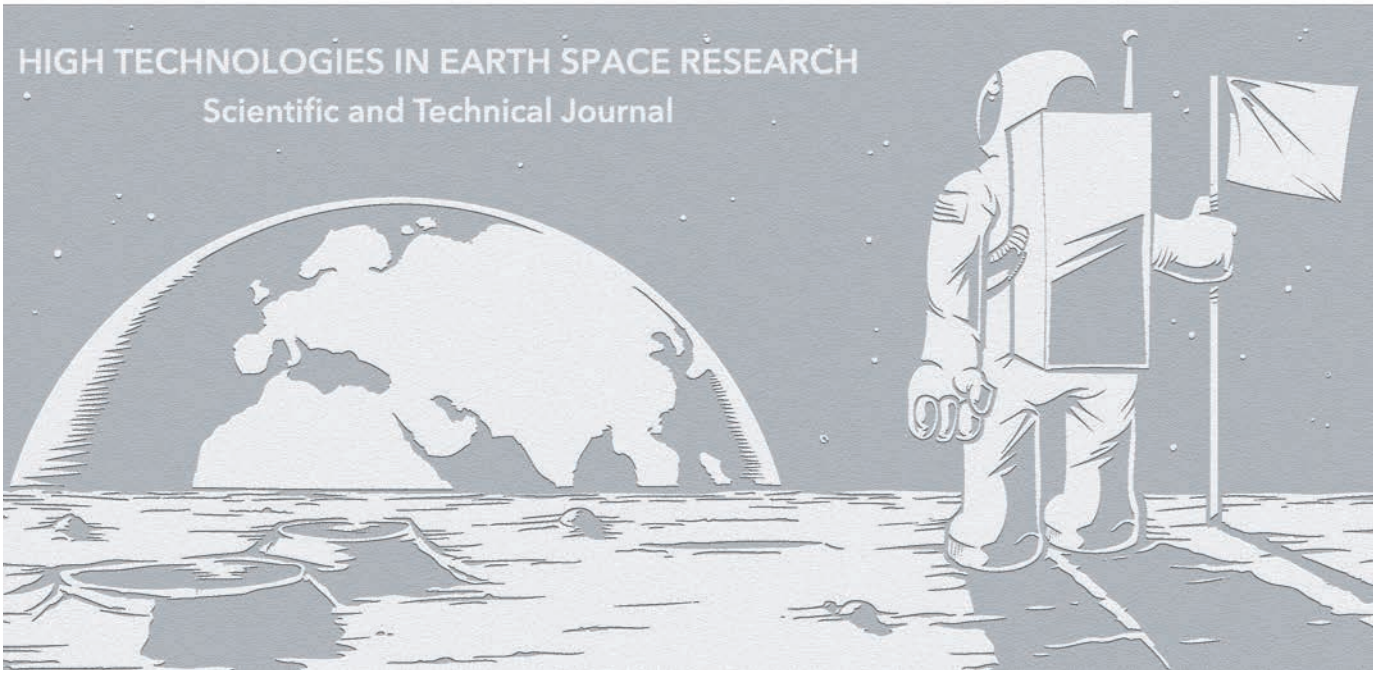
13. *Стародубцев В.Г.* Алгоритм формирования последовательностей Гордона-Миллса-Велча // Изв. вузов. Приборостроение. 2012. Т. 55. № 7. С. 5–9.

14. *No Jong-Seon*. Generalization of GMW sequences and No sequences // IEEE Transactions on Information Theory. 1996. Vol. 42. No. 1. Pp. 260–262.

15. *Chung H.*, *No J.S.* Linear span of extended sequences and cascaded GMW sequences // IEEE Transactions on Information Theory. 1999. Vol. 45. No. 6. Pp. 2060–2065.

16. *Стародубцев В.Г.* Проверочные полиномы последовательностей Гордона-Миллса-Велча // Изв. вузов. Приборостроение. 2013. Т. 56. № 12. С. 7–14.

17. *Стародубцев В.Г.* Формирование последовательностей Гордона-Миллса-Велча на основе регистров сдвига // Изв. вузов. Приборостроение. 2015. Т. 58. № 6. С. 451–457.



FORMING OF A BINARY GORDON-MILLS-WELCH SEQUENCES

Viktor G. Starodubtsev,
Saint Petersburg, Russia, vgstarod@mail.ru

Denis N. Borodko,
Saint Petersburg, Russia, denisborodko@yandex.ru

Anton M. Popov,
Saint Petersburg, Russia, antony57rus@gmail.com

ABSTRACT
Introduction: broadband signals with good correlation properties, formed on the basis of pseudo-random sequences, used in satellite communications systems, navigation support systems, and in radar systems. In modern telecommunication systems the requirements for the correlation properties and increased demands on structural secrecy imposed on the pseudo-random sequence. The need for Gordon-Mills-Welch sequences in modern communication systems, navigation and radar, which are subject to strict requirements for privacy and structural secrecy, defined by their higher equivalent linear complexity in comparison with the M-sequences, which also have a single-level periodic autocorrelation function. Virtually no ongoing formation GMW sequences algorithms prevents their wide use in data transmission systems. Objective: to develop a synthesis algorithm of devices forming GMW-sequences on the basis of shift registers. Tasks: to develop the algorithm of formation of testing polynomials of GMW-sequences based on the use of the structural properties of finite fields with a double extension, and the algorithm for determining the initial states of the shift registers with linear feedback, included in the device forming GMW-sequences, which testing polynomials are the product of several indivisible polynomials. In conducting research using mathematical apparatus of signal theory and the theory of finite fields. Results: a synthesis algorithm of devices forming GMW-sequences on the basis of shift registers is developed. It includes the algorithm of formation of testing polynomials of GMW-sequences and algorithm for determining the initial states of shift registers. Complete list of test polynomials for binary GMW-sequences of period N = 63 is obtained. For period N=255 the distribution of roots of polynomials-factors of test polynomial for an arbitrary base M-sequence is obtained. The distribution of the roots allows to uniquely determine the initial state of the shift registers through the symbols of the basic M-sequence. Practical relevance: the obtained results allow the use of GMW-sequences instead of M-sequences in the transmission systems for wideband radio channels, which are increased requirements on confidentiality. Equivalent linear complexity of GMW-sequences for 3–6 dB higher than the values for M-sequences. With increasing period the win for ELS increases. The algorithm can be used to develop methods for the formation of other classes of pseudorandom sequences, allowing for analytical representation in finite fields.

Keywords: pseudorandom sequences; finite fields; indivisible and primitive polynomials; correlation function; equivalent linear complexity; shift registers.

References
1. Ipatov V.P. *Spread Spectrum and CDMA: Principles and Applications*. New York, John Wiley and Sons Ltd. 2005. 398 p.
2. Vishnevskij V.M., Lyahov A.I., Portnoj S.L., SHahnovich I.V. *Shirokopolosnye bespro-vodnye seti peredachi informacii* [Broadband wireless data transmission network]. Moscow, Tekhnosfera, 2005. 592 p. (In Russian)
3. Sklar B. *Digital Communications: Fundamentals and Applications*. 2 edition. Prentice Hall, 2001. 1079 p.
4. Varakin L.E., Shinakov Yu.S. (Eds). *CDMA: proshloe, nastoyashchee, budushchee* [CDMA: Past, Present, Future]. Moscow, MAS, 2003. 608 p. (In Russian)
5. Ershen Wang, Shufang Zhang, Qing Hu, GPS Correlator Research and FPGA Implementation. *Journal of System Simulation*. 2008. Vol. 20. Pp. 3582–3585.
6. Golomb S.W., Gong G. *Signal Design for Good Correlation for Wireless Communication, Criptography and Radar*. Cambridge University Press. 2005. 438 p.
7. Ipatov V.P. *Periodicheskie diskretnye signaly s optimal'nymi korrelyacionnymi svojstvami* [Periodic discrete signals with optimum correlation properties]. Moscow, Radio i Svyas', 1992. 152 p. (In Russian)

8. Prozorov D.E., Smirnov A.V., Balanov M. Yu. Algorithm fast code synchronization noise-like signals, constructed on an elevated structural complexity sequences. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta* [Vestnik of Ryazan State Radio Engineering University]. 2015. Vol. 51. No. 1. Pp. 3–9. (In Russian)
9. Golomb S.W. Two-valued sequences with perfect periodic autocorrelation. *IEEE Transactions on Aerospace and Electronic Systems*. 1992. Vol. 28. No. 2. Pp. 383–386.
10. Lie-Liang Yang, Hanzo L. Acquisition of m-sequences using recursive soft sequential estimation. *Wireless Communications and Networking*. 2003. Vol. 1. Pp. 683–687.
11. Cho Chang-Min, Kim Ji-Youp, No Jong-Seon. New p-ary sequence families of period (p^n-1)/2 with good correlation property using two decimated m-sequences. *IEICE Transactions on Communications*. 2015. Vol. E98. No. 7. Pp. 1268–1275.
12. Yudachev S.S., Kalmykov V.V. Ensemble GMW sequences for systems with CDMA. *Nauka i obrazovanie: nauchnoe izdanie MGTU im.N.E.Baumana* [Science and Education: Scientific Publication of BMSTU]. 2012. No. 1. URL: http:// elibrary.ru/item.asp?id=17650851 (date of access 13.01.2017). (In Russian)
13. Starodubtsev V.G. The algorithm of formation of Gordon-Mills-Welch sequences. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie* [Journal of Instrument Engineering]. 2012. Vol. 55. No. 7. Pp. 5–9. (In Russian)
14. No Jong-Seon. Generalization of GMW sequences and No sequences. *IEEE Transactions on Information Theory*. 1996. Vol. 42. No. 1. Pp. 260–262.
15. Chung H., No J.S. Linear span of extended sequences and cascaded GMW sequences. *IEEE Transactions on Information Theory*. 1999. Vol. 45. No. 6. Pp. 2060–2065.
16. Starodubtsev V.G. Testing polynomials of Gordon-Mills-Welch sequences. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie* [Journal of Instrument Engineering]. 2013. Vol. 56. No 12. Pp. 7–14. (In Russian)
17. Starodubtsev V.G. Forming of Gordon-Mills-Welch sequences on the basis of the shift registers. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie* [Journal of Instrument Engineering]. 2015. Vol. 58. No. 6. Pp. 451–457. (In Russian)

Information about authors:
Starodubtsev V.G., PhD, Docent, assistant professor of the Saint Petersburg National Research University of Information Technologies, Mechanics and Optics;
Borodko D.N., PhD, chief lecturer of the Military Space Academy;
Popov A.M., student of the Military Space Academy.

For citation: Starodubtsev V.G., Borodko D.N., Popov A.M. Forming of a binary Gordon-Mills-Welch sequences. *H&ES Research*. 2017. Vol. 9. No. 2. Pp. 24–31. (In Russian)

ПРИМЕНЕНИЕ АДАПТИВНОЙ ФИЛЬТРАЦИИ И ЭКСПЕРТНОЙ СИСТЕМЫ В ИМПУЛЬСНОЙ РЕФЛЕКТОМЕТРИИ ДЛИННЫХ ЛИНИЙ

Филатов Владимир Иванович,
к.т.н., доцент Московского государственного технического университета мени Н.Э. Баумана, г. Москва, Россия, vfil10@mail.ru

Бакулина Елена Леонидовна,
студент Московского государственного технического университета имени Н.Э. Баумана, г. Москва, Россия

Бонч-Бруевич Андрей Михаилович,
к.т.н, доцент Московского государственного технического университета имени Н.Э. Баумана, г. Москва, Россия

АННОТАЦИЯ

Рассмотрена возможность подавления шумов в рефлектограммах длинных линий на основе применения алгоритмов адаптивной фильтрации и использования технологии экспертных систем для повышения достоверности идентификации подключенных устройств. Приведены результаты экспериментов, подтверждающие эффективность разработанных методик.

Анализ современного уровня развития и применения метода импульсной рефлектометрии для поиска неисправностей и идентификации подключенных к длинной линии устройств показал, что на результаты измерений значительное влияние оказывает естественный и искусственный шум, а также состояние самой линии. Вследствие этого, полезный сигнал, отражённый от устройств несанкционированного съёма информации и неоднородностей линии, обусловленных наличием поврежденных участков, может значительно искажаться. В результате чего возникают ошибки при обнаружении неисправностей линии и идентификации подключенных к ней устройств.

Цель работы состоит в повышении точности импульсной рефлектометрии длинных линий и достоверности идентификации подключенных устройств. При поведении исследований показано, что положительный эффект может быть достигнут за счет применения алгоритмов адаптивной фильтрации принятого сигнала и использования технологии экспертных систем. Создан экспериментальный стенд из программно-аппаратных средств, позволяющий проводить моделирование задачи идентификации подключенных к линии устройств и исследовать свойства рефлектограмм. Для повышения значения отношения сигнал/шум применялась адаптивная фильтрация принятого сигнала.

Для принятия решения о наличии сигнала и его принадлежности к тому или иному типу была предложена экспертная система. Она состоит из блока формирования априорных данных, базы знаний, блока формирования потока, базы данных, блока входных данных. В работе выделено особое место механизма логического вывода в структуре экспертной системы, который реализует алгоритмы прямого и обратного вывода. Данный механизм может быть представлен последовательностью процедур.

В ходе выполненной работы показана возможность подавления шумов в рефлектограммах длинных линий на основе применения алгоритмов адаптивной фильтрации и использования технологии экспертных систем для повышения достоверности идентификации подключенных устройств.

Результатом исследований стала разработка экспертной системы, которая позволит диагностировать не только наличие неоднородностей в длинной линии, но и проводить идентификацию подключенных устройств.

Ключевые слова: длинные линии; импульсная рефлектометрия; адаптивная фильтрация; экспертные системы; импульсный сигнал.

Для цитирования: *Филатов В. И.*, *Бакулина Е. Л.*, *Бонч-Бруевич А. М.* Применение адаптивной фильтрации и экспертной системы в импульсной рефлектометрии длинных линий // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 32–38.

Одним из основных недостатков современных методы импульсной рефлектометрии для поиска неисправностей и идентификации подключенных к длинной линии устройств является отсутствие возможности избегать влияния естественных и искусственных помех [1]. Данный факт подтверждается значительными искажениями сигналов, отражённый от устройств несанкционированного съёма информации, что затрудняет процедуру обнаружения и идентификации.

Для снижения влияния шумов в простейшем случае наиболее применимо адаптивное устройство, которое содержит программируемый фильтр обработки данных и блок, реализующий алгоритм адаптации, настраивающий коэффициенты программируемого фильтра. При этом могут использоваться фильтры с конечной и бесконечной импульсной характеристикой [2].

Для решения поставленной задачи выбран градиентный алгоритм адаптивной обработки сигналов с использованием критерия минимума среднеквадратичного отклонения. Применение данного алгоритма оправдано, так как он прост в реализации и не требует больших вычислительных ресурсов. В данном случае, требования к скорости сходимости алгоритма не являются существенными.

Для проведения математического моделирования использовался алгоритм NLMS, а также информационные возможности системы MATLAB и средой моделирования Simulink. Эта система располагает всеми необходимыми средствами для проведения моделирования адаптивной фильтрации. Кроме того, задействованы возможности библиотеки Signal Processing Blockset. Цифровая фильтрация выполнялась с использованием критерия минимума среднеквадратичного отклонения (Least Mean Squares, LMS), основанного на поиске минимума целевой функции методом наискорейшего спуска.

Стандартный LMS — алгоритм выполняет следующие операции:

– вычисляет выходной сигнал $y'(n)$ адаптивного фильтра;

– вычисляет сигнал ошибки $e(n)$, используя следующее выражение:

$$e(n) = y(n) - y'(n) \tag{1}$$

– обновляет коэффициенты фильтра, используя следующее выражение

$$\begin{aligned} w(n+1) &= w(n) - \left(\frac{\mu}{2}\right)\left(grad(J(w(n)))\right) = \\ &= w(n) + \mu p - \mu R w(n) \end{aligned} \tag{2}$$

где μ — положительный коэффициент (определяет размер шага) и $w(n)$ — вектор коэффициентов фильтра. Алгоритм сходится, если $0 < \mu < 2/\lambda_{max}$, где λ_{max} — максимальное собственное число корреляционной матрицы $R = u(n)u^T(n)$, с размерностью $(N+1)$ $x(N+1)$, $u(n)$ — входной вектор фильтра, N — порядок программируемого фильтра.

Скорость сходимости алгоритма зависит от величины разброса собственных чисел матрицы R, то есть чем меньше отношение λ_{max} / λ_{min}, тем быстрее сходится итерационный процесс. Однако, для реализации градиентного метода необходимо знать значения матрицы R и вектора взаимных корреляций P. На практике могут быть доступны лишь оценки этих значений, получаемые без какого-либо усреднения:

$$\hat{R} = u(n)u^T(n) \tag{3}$$

$$\hat{P} = y(n)u(n) \tag{4}$$

При использовании данных оценок получим:

$$\begin{aligned} w(n+1) &= w(n) + \mu y(n)u(n) - \mu u(n)u^T(n)w(n) = \\ &= w(n) + \mu u(n)\left(y(n) - u^T(n)w(n)\right) \end{aligned} \tag{5}$$

Выражение, стоящее в скобках, представляет собой разность между образцовым и выходным сигналом фильтра на n-м шаге, то есть ошибку фильтрации. С учетом этого, выражение для рекурсивного обновления коэффициентов фильтра примет вид:

$$w(n+1) = w(n) + \mu e(n)u(n) \tag{6}$$

Верхняя граница для размера шага μ определяется из выражения:

$$\mu_{max} = \frac{2}{\left[(N+1)\left(\sigma_x^2\right)\right]}. \tag{7}$$

где σ_x^2 — средний квадрат входного сигнала фильтра. Нормализованный алгоритм по критерию наименьшего среднеквадратичного отклонения (Normalized Least Mean Squares, NLMS) представляет собой модифицированную форму стандартного LMS — алгоритма. NLMS — алгоритм обновляет коэффициенты адаптивного фильтра, используя следующее выражение:

$$w(n+1) = w(n) + \mu e(n)\frac{u(n)}{\left\|u(n)\right\|^2} \tag{8}$$

Данное выражение можно привести к следующему виду [3]:

$$w(n+1) = w(n) + \mu(n)e(n)u(n) \tag{9}$$

где $\mu(n) = \dfrac{\mu}{\left\|u(n)\right\|^2}$. Таким образом, очевидно, что алгоритм NLMS практически аналогичен алгоритму LMS, за исключением меняющегося во времени размера шага $\mu(n)$.

Разработка модели адаптивной фильтрации и экспертной системы

Основное достоинство алгоритмов LMS состоит в простоте реализации. Его функционирование обеспечивается наименьшим числом арифметических операций по сравнению с другими алгоритмами. При подстройке коэффициентов фильтра на каждом шаге нужно выполнить $N + 1$ пар операций «сложение — умножение», где N — порядок фильтра.

Как правило, реализация таких алгоритмов требует меньше вычислительных ресурсов и памяти, чем, напри-

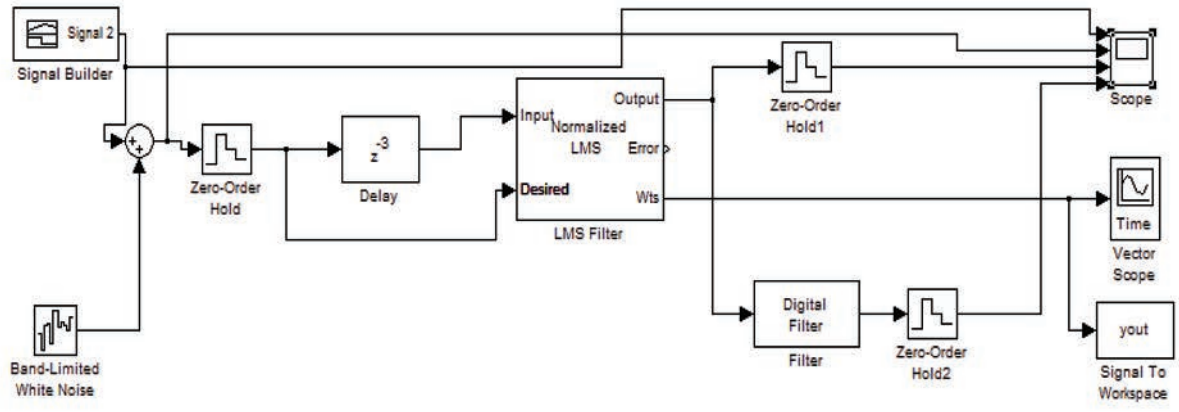


Рис. 1. Схема моделирования работы адаптивного фильтра

мер, рекурсивные алгоритмы, использующие критерий наименьших квадратов (Recursive Least Squares, RLS) [4]. Следует отметить, что использование данного алгоритма не позволяет получить достаточно высокую скоростью сходимости и повышает дисперсию ошибки.

Схема, реализующая адаптивную фильтрацию, составленная из функциональных блоков системы Simulink приведена на рис. 1. Меняющийся во времени шаг в нормализованном LMS — алгоритме позволяет несколько увеличить время сходимости по сравнению со стандартным LMS-алгоритмом. Таким образом, алгоритм NLMS является наиболее оптимальным алгоритмом для решение поставленной задачи. Форма полезного сигнала изображена на графике (рис. 2).

Для того чтобы уменьшить остаточный шум в сигнале, который снимается с выхода адаптивного фильтра, был применён цифровой фильтр низких частот сорокового порядка. Расчёт фильтра производился с помощью пакета FDAtool.

Данный фильтр обладает конечной импульсной характеристикой, имеет частоту дискретизации 48 кГц и граничную частоту полосы пропускания 4 кГц. Амплитудно-частотная характеристика (АЧХ) этого фильтра представлена на рис. 3.

При проведении эксперимента полезный сигнал генерировался блоком Signal Builder (рис. 1). Далее с помощью сумматора на него накладывался белый шум. Смесь полезного сигнала с шумом, проходя через АЦП, поступала на элемент задержки. Далее сигнал поступал на вход адаптивного фильтра (Input).

Зашумлённый сигнал с АЦП поступал на вход адаптивного фильтра (Desired). Таким образом, сигнал на входе адаптивного фильтра был задержан в данном случае на три такта относительно сигнала, поступающего на задающий вход. Сигнал с выхода адаптивного фильтра (Output) поступал на дискретный фильтр низких частот (ФНЧ). Отфильтрованный сигнал с выхода ФНЧ поступал на ЦАП и далее регистрировался осциллографом.

Так же на осциллограф подавался сигнал с выхода адаптивного фильтра, полезный и зашумлённый сигналы. Полезный сигнал имел амплитуду равную 0,9685 В.

Аддитивная смесь полезного сигнала с шумом формировалась с использованием белого шума с максимальной амплитудой равной 4,229 В. При этом обеспечивалось отношение амплитуды полезного сигнала к амплитуде шума Δ_1 = 0,229. Осциллограмма зашумлённого сигнала представлена на рис. 5.

В результате проведения эксперимента были получены следующие данные: за счет адаптивной фильтрации амплитуда шума была уменьшена до 0,3085 В. Амплитуда полезного сигнала изменилась незначительно. Осциллограмма

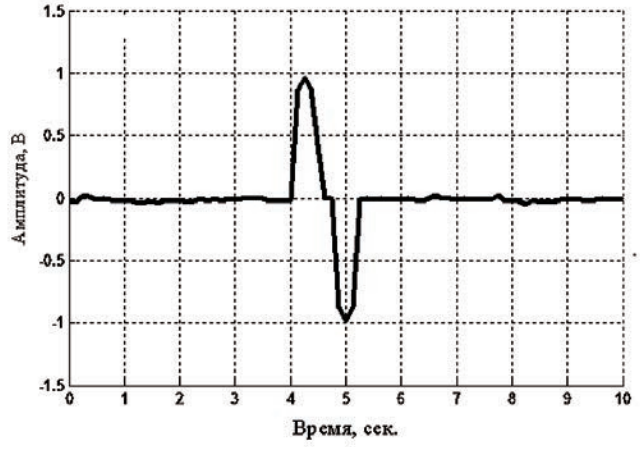


Рис. 2. Полезный сигнал рефлектометрии

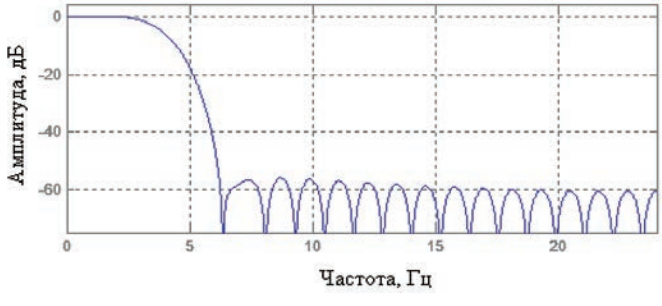


Рис. 3. АЧХ цифрового фильтра низких частот

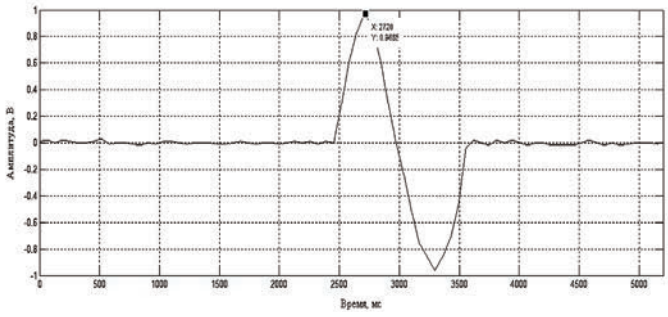


Рис. 4. Осциллограмма полезного сигнала

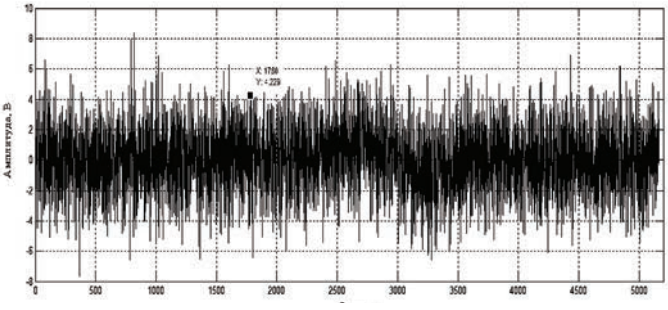


Рис. 5. Осциллограмма зашумлённого сигнала

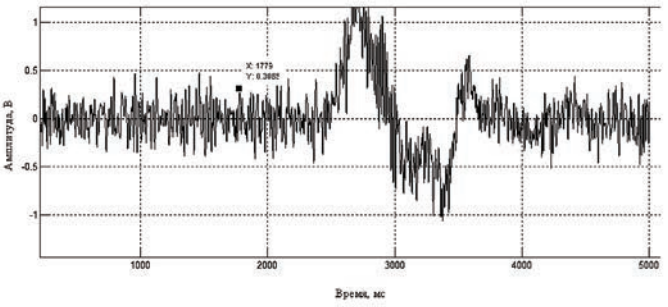


Рис. 6. Осциллограмма отфильтрованного сигнала

отфильтрованного сигнала изображена на рис. 6. Для повышения достоверности идентификации устройств, подключенных в длинной линии, предложено использовать технологию экспертных систем (ЭС).

Применение ЭС обеспечивает контроль целостности проводных коммуникаций при задействовании элементов: блока распознавания сигнала, состоящего из модуля триггера и блоков обучения и анализа. Как известно, экспертная система обладает следующими возможностями [5]:

– обеспечивается принятие решения в условиях неопределенности;

– способность получения информации для обоснованной интерпретации результатов моделирования;

– возможность пополнения базы знаний;

– полнота полученных данных позволяют формировать рекомендации для решения задачи идентификации подключенных устройств. Общая структурная схема ЭС представлена на рис. 7.

Блок формирования априорных данных предназначен для получения новых фактов на основе сопоставления исходных данных из рабочей памяти и знаний из базы знаний. Механизм логического вывода в структуре экспертной системы занимает наиболее важное место. Он реализует алгоритмы прямого и/или обратного вывода и формально может быть представлен процедурами:

– выбор из базы знаний и рабочей памяти правил и фактов;

– сопоставления правил и фактов, на основании которых производится идентификация;

– разрешение конфликтов, определяющее порядок использования правил, если в заключении указаны одинаковые имена фактов с разными значениями и осуществляющее выполнение действий, соответствующих полученному значению правила.

Подсистема объяснения предоставляет эксперту рекомендации по тестированию системы и повышает достоверность полученных результатов. На рис. 7 показан алгоритм адаптивной фильтрации, который является неотъемлемой частью блока формирования априорных данных в условиях неопределённой шумовой и помеховой обстановки. Данный алгоритм используются для нахождения искомого сигнала и заносится в базу знаний. Для обучения системы в базу данных записываются неизвестные сигналы.

Если экспертная система определяет, что сигнала в базе знаний и правил нет, она вводит в базу новый сигнал. Кроме того, экспертная система реализует диалог с пользователем и дает рекомендации по дальнейшим действиям. Блок схема обучения системы представлена на рис. 8. Решение о подобии выносится на основе сравнения максимальных амплитуд (пиков) по данным пикового детектора полученного и записанного из базы сигналов [6, 7]. Поскольку сигналы с крутыми фронтами имеют в большинстве случаев по одному или двум пикам на каждый период, после аппроксимации пиковых значений с амплитудами, лежащими ниже области пиков можно с достаточной

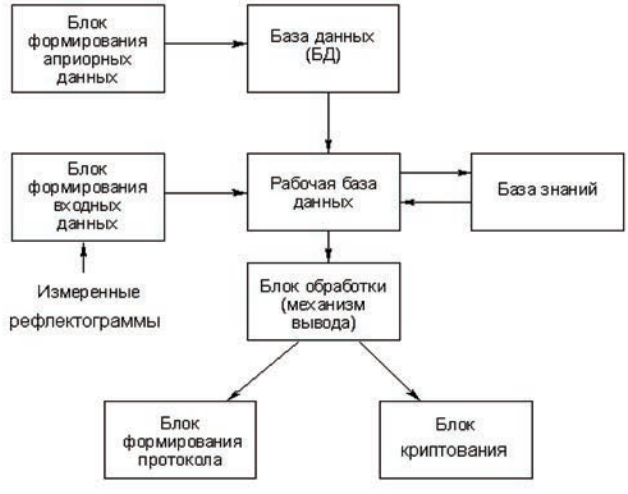


Рис. 7. Структурная схема ЭС

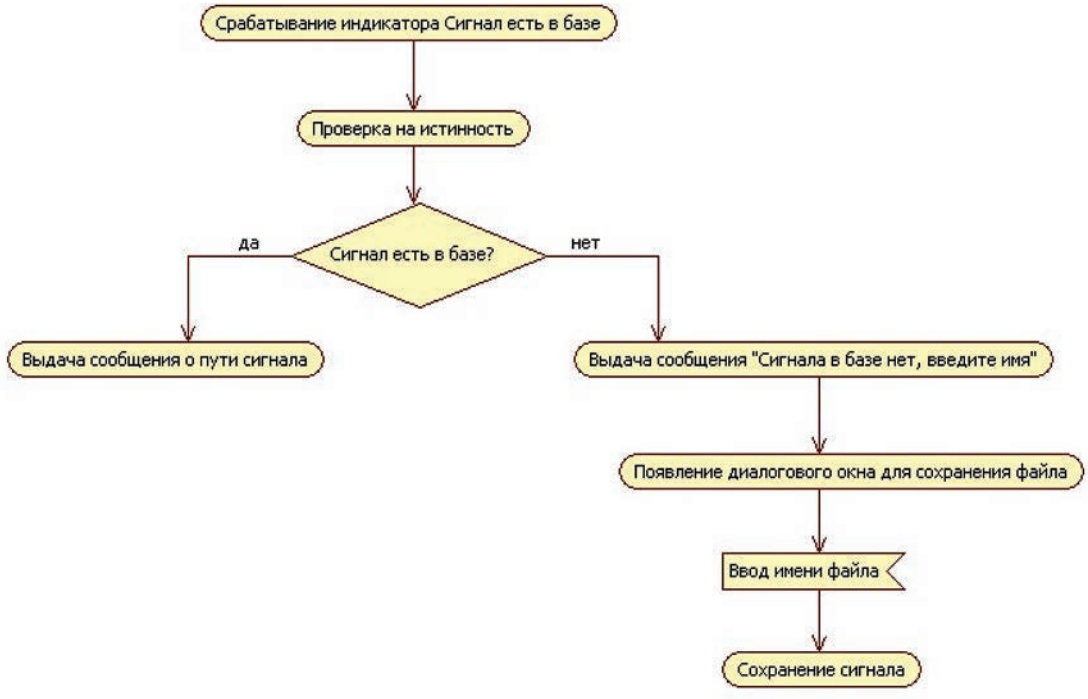


Рис. 8. Блок-схема блока обучения ЭС

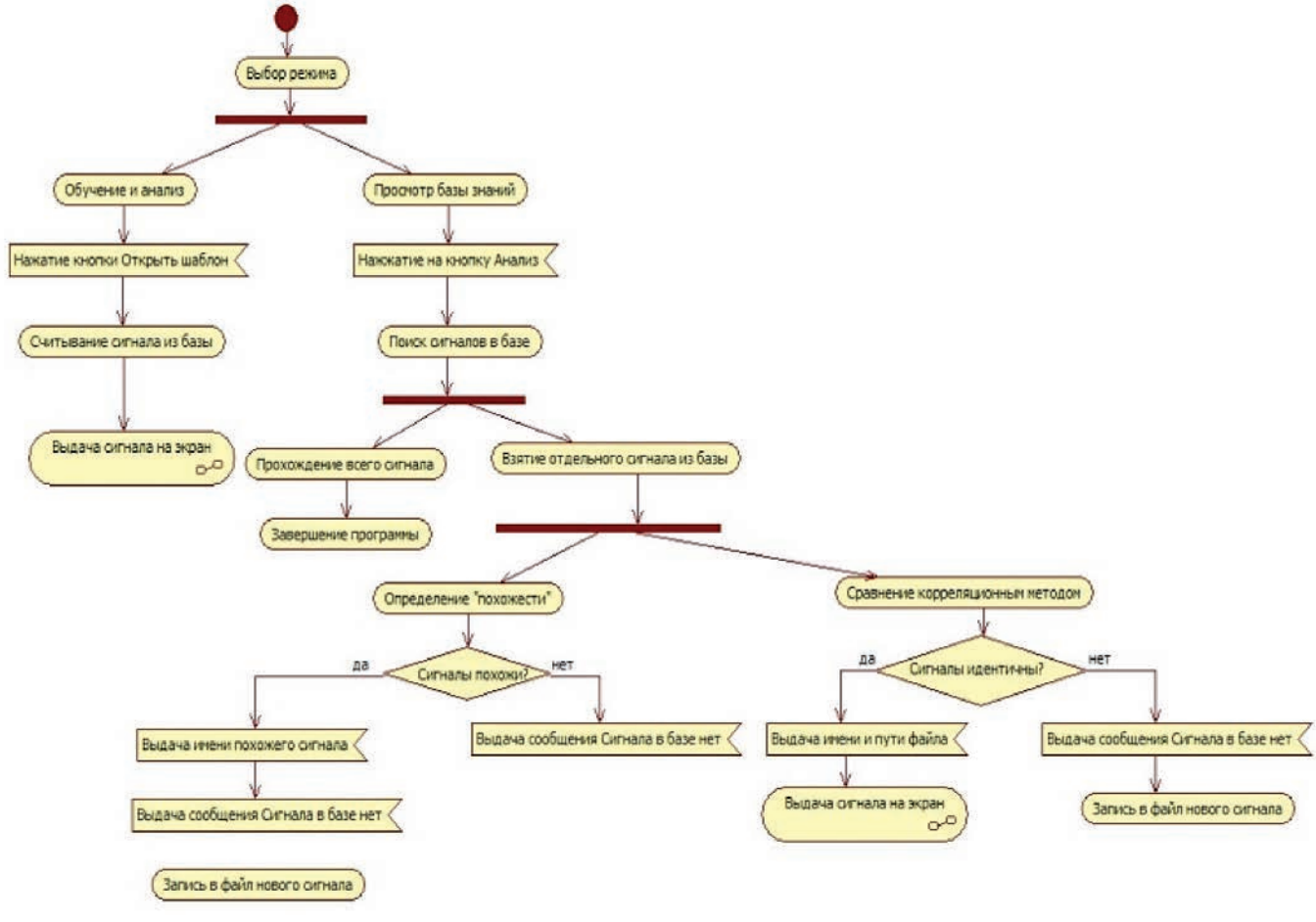


Рис. 9. Блок-схема работы с ЭС в режиме анализа

достоверностью восстановить форму искомого сигнала. Если сигналы имеют одинаковое количество пиков [7, 8], то проверяется предположение, что их расположение на временной оси одинаковое.

Для этого массив позиций пиков первого сигнала вычитается из второго, берётся абсолютное значение каждого элемента, вычисляется их среднее значение путём суммирования всех элементов и деления на их количество.

В случае совпадения указанного числа с первым элементом массива программа — переходит к сравнению максимальных амплитуд в их позициях. Если схожесть определена, выдаётся сообщение о соответствии сигнала искомому в базе.

Блок-схема работы с ЭС в режиме анализа представлена на рис. 9. Если система обнаруживает, что по какому-либо критерию сигнал похож на имеющийся в базе знаний, она выдаёт соответствующее сообщение. В противном случае пользователю выдается сообщение, что сигнал отсутствует в базе предлагается сохранить сигнал [9] в базе знаний, присвоив ему соответствующее имя.

Выводы

В ходе выполненной работы показана возможность подавления шумов в рефлектограммах длинных линий на основе применения алгоритмов адаптивной фильтрации и использования технологии экспертных систем для повышения достоверности идентификации подключенных устройств. Создан макет программно-аппаратного комплекса, позволяющего исследовать эффективность адаптивной фильтрации сигналов в ходе моделирования задачи рефлектометрии длинных линий.

За счет разработанной экспертной системы стало возможным диагностировать не только наличие неоднородностей, но и проводить идентификацию устройств, подключенных к длинной линии.

Литература

1. *Бельчиков А.В.*, *Кривозубов П.А.* Средства обеспечения безопасности проводных телекоммуникационных систем (Обзор) // Вопросы защиты информации 2011. № 1. С. 44–51

2. *Уидроу Б.*, *Стирнз С.Д.* Адаптивная обработка сигналов: пер. с англ. М.: Радио и связь, 1989. 440 с.

3. Сергиенко А.Б. Алгоритмы адаптивной фильтрации: особенности реализации в Matlab // Exponenta Pro. Математика в приложениях. 2003. № 1(1). С. 18–28.

4. *Рябинин А.М.*, *Филатов В.И.*, *Белков И.В.* Модель канала передачи информации с помощью программно-управляемого ПЭМИН // T-comm: телекоммуникации и транспорт. 2016. Т. 10. № 1. С. 77–80.

5. *Савкин Л.В.*, *Дмитриев В.Г.*, *Федоров Е.А.*, *Филатов В.И.*, *Гусенков П.А.* Нейрорегуляторы в бортовых системах космических аппаратов // Промышленные АСУ и контроллеры. 2016. № 4. С. 31–39.

6. Филатов В.И. Широкополосная система радиосвязи повышенной скорости передачи информации // Труды МАИ. 2015. № 81. URL: http://mai.ru//upload/iblock/d39/d39772f28734c7f81f03bf1fcce5c4a3.pdf

7. *Сивов В.А.*, *Васильев В.А.*, *Моисеев В.Ф.*, *Савельева М.В.*, *Филатов В.И.* Спектрально-энергетическая эффективность квадратурной амплитудно-инверсной модуляции сигналов в системах радиосвязи с кодовым разделением каналов // Электросвязь. 2015. № 2. С. 22–24.

APPLICATION OF AN ADAPTIVE FILTRATION AND EXPERT SYSTEM IN A PULSE SCATTEROMETRY OF LONG LINES

Vladimir I. Philatov,
Moscow, Russia, vfil10@mail.ru

Elena L. Bakulina,
Moscow, Russia

Andrei M. Bonch-Bruevich,
Moscow, Russia

ABSTRACT
The possibility of suppressing noise in trace long lines through the use of adaptive filtering algorithms and the use of expert systems technology to improve the reliability of the identification of the connected devices. The results of experiments confirming the effectiveness of the developed techniques. Analysis of the current level of development and application of pulse reflectometry method for troubleshooting and identification of devices connected to a long line showed that the

measurement results are greatly affected by natural and man-made noise, as well as the state of the line. As a result, the useful signal reflected from eavesdropping information devices and line discontinuities due to the presence of damaged areas can greatly distorted. As a result, errors occur in detection and identification of the fault line, and devices connected to it. The aim of the work is to improve the accuracy of pulse reflectometry long lines and the reliability of the identification of the connected devices. If the behavior studies have shown that a positive effect can be achieved through the use of adaptive filtering algorithms of the received signal and the use of expert systems technology. An experimental stand of the software and hardware that allows you to carry out modeling of identifying devices connected to the line and investigate the properties of traces. To increase the value of the signal / noise ratio applied adaptive filtering of the received signal. In the simplest case, the adaptive device comprises a programmable filter and the data processing unit that implements the adaptation algorithm, which is based on a priori information configures the programmable filter coefficients. To solve the problem selected gradient algorithm adaptive signal processing using the minimum criteria of the standard deviation.
For making decision on existence of a signal and its belonging to this or that type the expert system has been offered. It consists of the block of formation of aprioristic data, the knowledge base, the block of formation of a stream, the database, the block of entrance data. In work the special place of the mechanism of a logical conclusion in structure of expert system which realizes algorithms of a direct and return output is allocated. This mechanism can be presented by the sequence of procedures.
During the performed work the possibility of suppression of noise in the reflektogrammakh of long lines on the basis of application of algorithms of an adaptive filtration and use of technology of expert systems for increase in reliability of identification of the connected devices is shown.
Result of researches was development of expert system which will allow to diagnose not only existence of not uniformity in the long line, but also to carry out identification of the connected devices.

Keywords: long lines; pulse reflectometry; adaptive filtering; expert systems; big data; digital analysis; pulse signal.

References

1. Bel'chikov A.V., Krivozubov P.A. Of security facilities for wire telecommunication systems (Review). *Voprosy zashchity informatsii* [Information security questions]. 2011. No. 1. Pp.44–51 (In Russian)
2. Widrow B., Stearns S.D. Adaptive Signal Processing. New Jersey: Prentice-Hall, Inc., 1985. 474 p.
3. Sergienko A.B. Algoritmy adaptivnoy fil'tratsii: osobennosti realizatsii v Matlab [Adaptive Filtering Algorithms: Implementation Features in Matlab]. *Exponenta Pro. Matematika v prilozhenijah*. [Exponenta Pro. Mathematics in applications] 2003. Vol. 1. No. 1. Pp.18–28. (In Russian)
4. Rjabinin A.M., Filatov V.I., Belkov I.V. Model of channel information leakage via software – managed side electromagnetic radiation. *T-Comm*. 2016. Vol. 10. No. 1. Pp. 77–80. (In Russian)
5. Savkin L.V., Dmitriev V.G., Fedorov E.A., Filatov V.I., Gusenkov P.A. Neuroregulators in Spacecraft Onboard Systems. *Promyshlennye ASU i kontrollery***.** [Industrial Automatic Control Systems and Controllers] 2016. No. 4. Pp. 31–39. (In Russian)
6. Filatov V.I. The radio connection broadband system of the increased speed in the process of transmitting the information. *Trudy MAI*. 2015. No. 81. URL: http://mai.ru//upload/iblock/d39/d39772f28734c7f81f03bf1fcce5c4a3.pdf. (In Russian)
7. Sivov V.A., Vasil'ev V.A., Moiseev V.F., Savel'eva M.V., Filatov V.I. Spectrum-energy effectiveness of the signals with multyposition squared amplitude-inversion modulation into the communication systems with orthogonal coding division of the channels. *Electrosvyaz.* 2015. No. 2. Pp. 22–24. (In Russian)

Information about authors:

Philatov V.I., PhD, assistant professor, of theBauman Moscow State Technical University;
Bakulina E.L., student of the Bauman Moscow State Technical University.

For citation: Philatov V.I., Bakulina E.L. Bonch-Bruevich A.M. Application of an adaptive filtration and expert system in a pulse scatterometry of long lines. *H&ES Research.* 2017. Vol. 9. No. 2. Pp. 32–38. (In Russian)

РОССИЙСКАЯ НЕДЕЛЯ ВЫСОКИХ ТЕХНОЛОГИЙ

НАВИТЕХ • NAVITECH

ufi Approved Event

XI МЕЖДУНАРОДНЫЙ НАВИГАЦИОННЫЙ ФОРУМ

www.glonass-forum.ru

9-я международная выставка НАВИТЕХ

www.navitech-expo.ru

25–28 апреля 2017

ЦВК «ЭКСПОЦЕНТР»
МОСКВА

Реклама 12+

При поддержке: МИНПРОМТОРГ РОССИИ

Под патронатом: ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Организатор форума: ГЛОНАСС/ГНСС Форум

Оператор форума: ПроКонф

Стратегический партнер форума: НП "ГЛОНАСС" Федеральный сетевой оператор

Организатор выставки: ЭКСПОЦЕНТР МОСКВА

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОГО ДОСТУПА К ДАННЫМ, РАЗМЕЩЕННЫМ В ОБЛАЧНОЙ ИНФРАСТРУКТУРЕ

Сахаров Дмитрий Владимирович,
к.т.н., доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, d.sakharov@rkn.gov.ru

Левин Марк Вадимович,
аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, m.va.levin@gmail.com

Фостач Елена Сергеевна,
студент Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, elena.fostach@gmail.com

Виткова Лидия Андреевна,
аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, iskinlidia@gmail.com

АННОТАЦИЯ

С развитием облачных технологий возрастает роль распределенной инфраструктуры, функциональная совместимость и портативность которой являются неотъемлемой составляющей. Однако, обеспечение доступности услуг
и масштабируемости виртуальных ресурсов, безопасности и конфиденциальности пользовательских данных имеет первостепенное значение.

В рамках актуальной статьи авторами было проведено исследование, позволяющее более детально разобраться в вопросах безопасности, с которыми приходится сталкиваться при проектировании архитектуры облачных сред.

Первым этапом исследования было выбрано изучение мировых стандартизирующих документов в исследуемой области, на которые опираются результаты данной работы.

В основу проведенного исследования были положены принципы организации доступа к облачному пространству, критерии к шифрованию информации, передаваемой как между клиентами облачных услуг, так и хранимой на удаленном сервере. Особое внимание при проведении исследования было уделено вопросам аутентификации.

Показано, что для создания надежной, с точки зрения безопасности, облачной архитектуры необходимо использовать криптостойкие протоколы смешенного шифрования с проверкой подлинности сообщений, а так же внедрять механизмы аутентификации, которые позволят идентифицировать каждого пользователя, пытающегося получить доступ к конфиденциальным данным. Исследование содержит актуальные для поставщиков облачных услуг решения, которые позволят поддержать доступность, конфиденциальность и целостность личных данных в облачной среде.

Ключевые слова: защита персональных данных; облачная архитектура; безопасность облачных вычислений; конфиденциальность информации; механизмы аутентификации; угрозы информационной безопасности.

Для цитирования: *Сахаров Д. В., Левин М. В., Фостач Е. С., Виткова Л. А.* Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 40–46.

Введение

С развитием облачных технологий, происходит смена парадигм информационной безопасности от идеи локальной защиты ресурсов к облачной модели защиты приложений, данных и сервисов. В связи с этим, для создания безопасных виртуальных услуг, прежде всего, необходимо обеспечить меры защиты со стороны поставщика облачной инфраструктуры.

Мировые стандарты, такие как Security Recommendations for Cloud Computing Providers (BSI), Cloud Computing Information Assurance Framework (ENISA), The Cloud Security Alliance Consensus Assessments Initiative (Cloud Security Alliance) и Security Assessment Provider Requirements and Customer Responsibilities (NIST), диктуют свои требования к построению облачных решений.

Облачные вычисления представляют собой технологию распределенной обработки данных, где ресурсы и мощности предоставляются пользователю в качестве услуг. Технология облачных вычислений является результатом конвергенции более ранних технологий, таких как параллельные вычисления и распределенные вычисления.

Согласно документу с рекомендациями Национального Института Стандартизации (The NIST Definition of Cloud Computing) предоставленных Питером Меллом и Тимоти Грансем, облаком называется услуга или форма предоставления услуг, обладающая пятью характеристиками:

1. **Самообслуживание** (on demand self-service) — возможность подключения и отключения облачных услуг самим пользователем за счет предоставляемых ему механизмов.

2. **Доступность по сети** (broad network access) — получение доступа к облачным ресурсам через сеть Интернет независимо от месторасположения потребителя услуг.

3. **Наличие пула ресурсов** (resources pooling) — обеспечение избыточного объема ресурсов с целью возможного предоставления неограниченного количества услуг.

4. **Эластичность и масштабируемость** (scalability and elasticity) — возможность контроля количества и скорости потребления услуг.

5. **Измеримость** (measurable service) — контроль потребления услуг в пределах фиксированного временного отрезка [1].

Провайдеры облачных вычислений предлагают свои услуги на базе трех основных моделей сервисов:

- инфраструктура как услуга (IaaS);
- платформа как сервис (PaaS);
- программное обеспечение как услуга (SaaS) [1].

IaaS представляет собой фундаментальную часть, где вычислительная инфраструктура (серверы, хранилища данных, сетевые ресурсы, операционные системы) предоставляются в качестве подключаемой услуги. Данный подход позволяет потребителю облачных услуг уменьшить совокупную стоимость владения инфраструктурой, т.е. IaaS превращает стоимость капитальных расходов [CAPex] в операционные расходы [OPex]. Так же необходимо отметить еще одно важное преимущество данного сервиса — высокая скорость масштабирования, т.е. увеличение или уменьшение количества используемых инфраструктурных услуг, что позволяет потребителю оптимально задействовать ресурсы.

PaaS предоставляет платформу, включающую в себя средства разработки продуктов и среду исполнения программного кода, размещенную на предоставленной поставщиком услуг инфраструктуре. Данная услуга ориентирована преимущественно на отдельный стек технологий, среди которых можно отметить разнообразие языков программирования и вариативность подключаемых библиотек.

SaaS, в свою очередь, представляет собой набор приложений, которые предоставляются пользователю. Поставщик SaaS услуг осуществляет техническую поддержку приложений, отслеживает и производит их обновление.

Таким образом, исходя из рассмотренных видов предоставляемых провайдером облачных услуг и предъявляемых к ним требований со стороны стандартизирующих организаций, можно сделать вывод, о том, что независимо от того, какой сервис предоставляется потребителю (SaaS, PaaS, IaaS), необходимо обеспечить меры защиты, с точки зрения безопасности, на каждом уровне предоставляемых услуг.

Решение ключевых проблем при построении облачной инфораструктуры

Несмотря на то, что виртуализация сетевых функций и облачные вычисления дают возможность дистанционно разграничить ИТ-инфраструктуру и пользователей, необходимо решить возросшие вместе с этим риски эксплуатации уязвимостей информационной безопасности для того, чтобы в полной мере воспользоваться новыми возможностями вычислительной парадигмы.

Особое значение приобретает данная проблема для поставщиков SaaS услуг. Пользователь, который доверил свои данные для хранения в облаке, теряет контроль над их целостностью, конфиденциальностью и доступностью. Таким образом, одной из важных задач поставщика услуг является обеспечение трех базовых свойств информационной безопасности, включая задачи организации места хранения и способа представления пользовательских данных.

В Российской Федерации в соответствии с действующим ФЗ «Об информации, информационных технологиях и защите информации», «**конфиденциальность информации**» определяется как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя» [2]. **Целостность информации** гарантирует обеспечение одинакового поддержания данных во время любой проводимой над ними операции, например, хранения, передачи, извлечения. **Доступность информации** гарантирует беспрепятственный доступ к защищаемой информации для законных пользователей.

Таким образом, для поддержания трех базовых свойств информационной безопасности — конфиденциальности, целостности и доступности данных пользователей, обозначим ключевые проблемы, которые необходимо решить в первую очередь:

1. Исследование механизмов аутентификации пользователей и использования защищенного канала связи на пути между клиентом и сервером.

2. Исследование способов хранения информации в зашифрованном виде, ее обработки и поиска в облачном хранилище.

Решение данных проблем позволит повысить уровень конфиденциальности, целостности и доступности данных в облачных средах.

Актуальное исследование посвящено изучению первой проблемы — организации доступа к данным пользователей и создания канала безопасной передачи данных. В то время как проблема способа хранения, обработки и поиска запрашиваемой пользователем информации в инфраструктуре облака будет рассмотрена нами в следующей работе.

За основу была взята схема функциональной архитектуры облачной среды (рис. 1), на базе которой построено данное исследование. На схеме показан способ развертывания баз данных и приложений на ресурсах облачной инфраструктуры вместе с сетевой схемой взаимодействия. Наглядно показаны уровни коммутации (L2) и маршрутизации (L3) данных между объектами облачной инфраструктуры.

В соответствии с решаемой проблемой, обозначим ключевые аспекты информационной безопасности, которые должны лежать в основе каждого надежного облачного сервиса:

1. Определение способов **конфиденциальной** передачи данных.

2. Организация доступа **авторизованных** пользователей к данным.

Определение способов конфиденциальной передачи данных

Для решения поставленной задачи необходимо использовать криптографические механизмы, позволяющие обеспечить надежное шифрование данных. Как известно, существует два типа алгоритмов шифрования — симметричные и ассиметричные. Симметричное шифрование дает большое преимущество в скорости шифрования и снижении нагрузки на вычислительные ресурсы, однако уступает в надежности ассиметричному шифрованию в силу особенностей аппаратной реализации специфических математических преобразований.

Очевидно, использование смешанного шифрования даст существенное преимущество. В качестве реализации рассмотрим следующие алгоритмы шифрования AES[3], RSA[4]:

1. Стандарт AES (*Advanced Encryption Standard*), является симметричным алгоритмом блочного шифрования. Алгоритм основан на нескольких заменах, подстановках и линейных преобразованиях, каждое из которых выполняется блоками по 16 байт. Операции повторяются несколько раз, каждый из которых называется «раунд». В течение каждого раунда, на основе ключа шифрования вычисляется уникальный ключ раунда и встраивается в вычисления. Благодаря подобной блоковой структуре AES, изменение даже одного бита или в ключе, или в текстовом блоке приводит к полному изменению всего шифра — явное преимущество относительно традиционных потоковых шифров. Благодаря описанным преимуществам, шифр AES является криптостойким по результатам проведенного исследования Агентством национальной безопасности США.

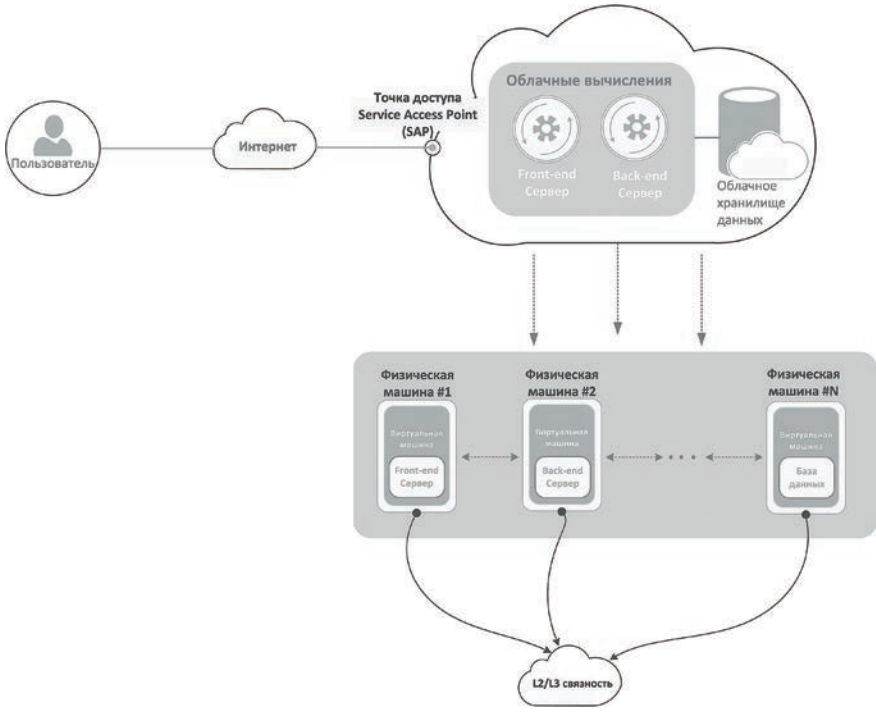


Рис. 1. Функциональная архитектура облачных сред

2. RSA — один из наиболее успешных асимметричных алгоритмов шифрования на сегодняшний день. В противоположность традиционным симметричным системам шифрования, RSA работает с двумя различными ключами: «открытым» и «закрытым» ключом. Оба работают совместно друг с другом, и сообщение, зашифрованное одним из них, может быть расшифровано только вторым. Так как закрытый ключ не может быть вычислен из открытого ключа, последний может храниться в открытом доступе. Безопасность RSA основана на математической проблеме факторизации целых чисел. Шифруемое сообщение рассматривается как одно большое число. Во время шифрования оно возводится в степень ключа и делится с остатком на произведение первых двух. Повторяя процесс с другим ключом, можно получить исходный текст. Лучший из известных методов взлома заключается в факторизации множителя, использованного при делении. На сегодняшний день невозможно произвести подобную факторизацию для чисел длиннее 768 бит. Поэтому современные системы шифрования используют минимальную длину ключа в 3072 бита.

Важно отметить, что с целью снижения вероятности перехвата в открытом виде передаваемого сообщения, шифрование данных должно происходить до того момента, как информация покинет браузер пользователя (т.е. до момента отправки сообщения на сервер).

Рассмотрим протокол защищенной передачи данных TLS v1.2, в котором реализованы алгоритмы шифрования информации на базе уже рассмотренных ранее алгоритмов AES, RSA, аутентификации пользователей и контроля целостности получаемых данных.

Работа TLS протокола начинается с согласования версии используемого протокола, способа шифрования данных между узлами соединения, а так же проверки достоверности полученных сертификатов, после чего будет установлен криптографически безопасный канал. Отметим, что шифрование с открытым ключом должно использоваться только в процедуре во время первоначальной настройки соединения (*TLS Handshake*), которая позволяет установить общий секретный ключ шифрования без предварительных знаний узлов соединения друг о друге. После настройки *TLS*-туннеля должна использоваться симметричная криптография, общение в пределах текущей сессии будет зашифровано именно установленными симметричными ключами. Это необходимо для увеличения быстродействия, так как криптография с открытым ключом требует значительно больше вычислительной мощности.

После того, как мы определили протокол, который обеспечит соединение на участке между клиентом и облаком, необходимо перейти к вопросу аутентификации.

Отметим одну из ключевых особенностей протокола TLS v1.2, которая заключается в возможности установления подлинности личности, клиента и сервера (*Chain of Trust*) за счет использования сертификатов подлинности, предоставляемыми центрами сертификации (*CA – certificate authorities*). Центры сертификации выдают подписанные сертификаты, доверие к которому неоспоримо. Таким образом, целый ряд выданных сертификатов образует цепочку доверия. Благодаря этому можно проверить подлинность каждого доверительного узла. Центры сертификации осуществляют проверку, выявляя тем самым, был ли скомпрометирован закрытый ключ сертификата, или была ли скомпрометирована вся процедура сертификации.

Передача каждого сообщения осуществляется с добавлением MAC-значения (*Message Authentication Code*), который представляет собой одностороннюю криптографическую функцию хэширования, ключи которой известны обоим участникам соединения. При отправке сообщения каждый раз генерируется его MAC-значение, по которому принимающая сторона может проверить полученную информацию на предмет подмены.

Таким образом, показано, что использование протокола TLS v1.2 позволяет создать канал конфиденциальной передачи данных. Однако, отметим, что механизмы работы данного протокола не обеспечивают контроль времени жизни каждой пользовательской сессии и повторную аутентификацию клиента для возобновления сессии в случае разрыва установленного соединения. Так же отметим, что протокол TLS v1.2 не позволяет аутентифицировать самого пользователя, в связи с этим, рассмотрим механизм аутентификации пользователей в рамках протокола OAuth2.0.

Организация доступа авторизованных пользователей к ресурсам

Глобальное развитие облачных сервисов приводит к тому, что каждый пользователь сети Интернет окружен в независимости от используемой платформы доступа, огромным количеством служб, позволяющих создавать и распространять медиа-контент или получать мгновенный доступ к электронным услугам.

Очевидно, что перед разработчиками сервисов возникает задача обеспечения безопасности. Необходимо решать задачи защиты данных от несанкционированного доступа пользователей, работающих в большом количестве приложений. Ситуация осложняется тем, что работа пользователя не должна затрудняться внутренними механизмами безопасности и перемещение между сервисами должно происходить максимально быстро и безопасно для услуг, предоставляемых пользователю.

Чтобы решить задачу, связанную с упрощением авторизации пользователя при работе с большим количеством приложений и онлайн сервисов был разработан протокол OAuth.

При использовании OAuth-авторизации к основным преимуществам принято относить отсутствие передачи логина и пароля в приложение, с которым работает пользователь. Таким образом, приложение может выполнить только то, что явно разрешил пользователь. Так же, отпадает необходимость решения вопроса обеспечения защищенного хранения пароля и логина приложением.

Актуальная версия стандарта OAuth 2.0, опубликована в 2012 году в документе IETF RFC6749. OAuth 2.0 позволяет сторонним приложениям получать доступ от своего

имени или ограниченный доступ к HTTP-службе от имени владельца ресурса, организовав процесс согласования взаимодействия между владельцем ресурса и HTTP-службой. Результатом авторизации является Access Token — ключ, предъявление которого является пропуском к защищенным ресурсам. Стандарт не определяет формат ключа, который получает приложение, поэтому ключ сам по себе не может быть использован для аутентификации пользователя [6].

Приведенный ниже (рис. 2) алгоритм демонстрирует ключевые особенности логики работы протокола, позволяющие решить задачу авторизации, т.е. предоставления права на использование ресурса. Чтобы определить присутствие прав, необходим токен (запись или значение, обеспечивающее уникальную идентификацию). Отметим, что один и тот же токен может быть повторно использован для различных пользователей, в то же время у одного и того же пользователя в процессе авторизации могут поменяться токены при наличии специфических временных требований для их обновления. Чтобы получить права на работу с ресурсом необходимо предъявить соответствующий токен.

Таким образом, снижение риска несанкционированного доступа к ресурсам, и, как следствие, обеспечение доступности информации, можно добиться за счет внедрения механизма аутентификации.

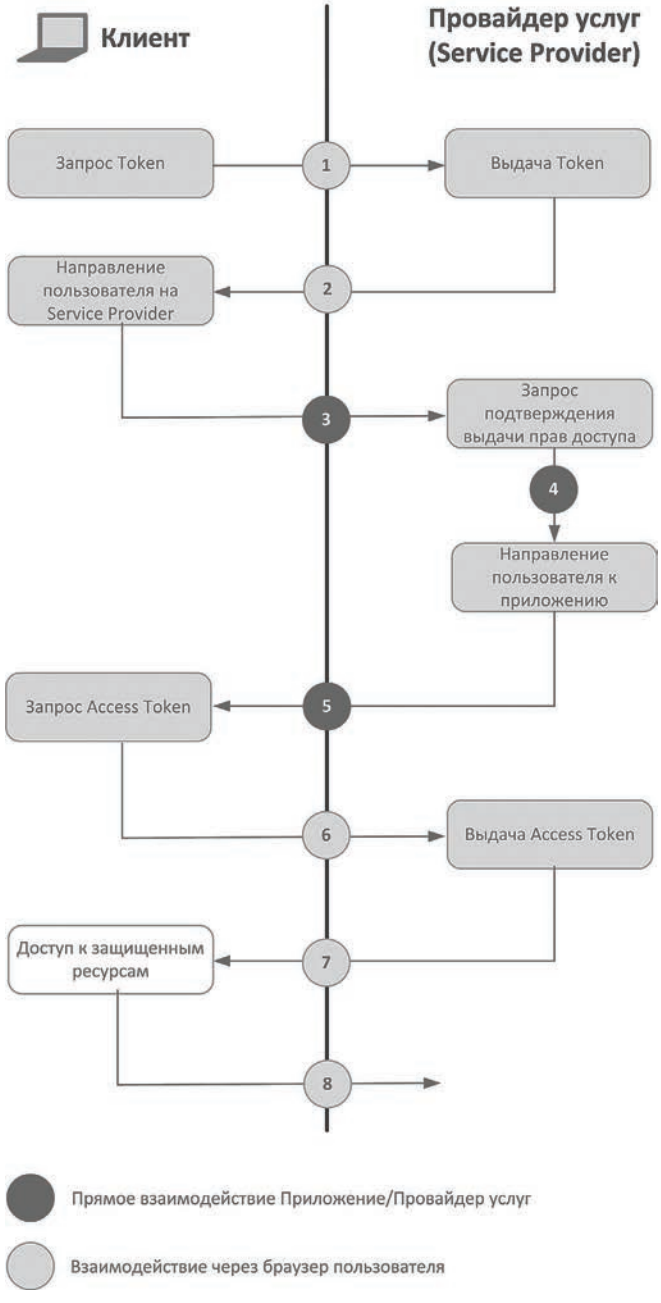


Рис. 2. Алгоритм работы протокола OAuth 2.0

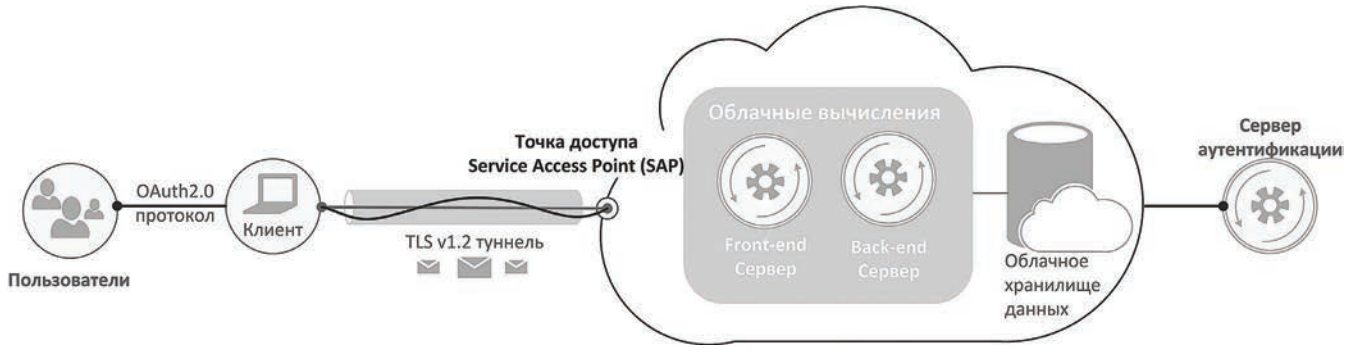


Рис. 3. Концептуальная схема построения защищенной облачной среды

Суммируя описанные ранее подходы, представим концептуальную схему (рис. 3), которая отражает ключевые элементы облачной архитектуры (клиентскую часть приложения, сервер аутентификации, сервер приложения (который включает в себя механизмы обработки информации), а так же хранилище данных). Дополнительно, на схеме отмечено, на каких сегментах сети применимы рассмотренные ранее протоколы OAuth 2.0, TLSv1.2 для обеспечения надежного соединения.

Выводы

В работе рассмотрен алгоритм установления защищенного TLS соединения, в основе которого лежит обмен открытыми ключами шифрования, алгоритм обмена сертификатами для проверки достоверности узлов, участвующих в обмене конфиденциальными данными, а так же алгоритм проверки целостности полученной информации на стороне принимающего узла (клиента, либо сервера), базирующийся на подсчете MAC-суммы каждого отправленного сообщения. Было выявлено, что для создания надежного TLS соединения важно иметь возможность аутентификации именно клиентской части приложения, а не самого пользователя. В работе отмечено, что в основе протокола TSL v1.2 отсутствуют механизмы контроля времени жизни пользовательской сессии и механизмы повторной аутентификации для возобновления сессии в случае разрыва соединения.

Работа содержит исследование возможности получения авторизованного доступа пользователей к ресурсам, где показано, что для этой цели необходимо внедрение средств аутентификации пользователей за счет протокола OAuth2.0. Для этого была описана диаграмма поэтапного обмена информацией между клиентом и провайдером услуг аутентификации.

В заключение исследования представлена генерализованная схема организации защищенного доступа к облачной середе, которая включает в себя рассмотренные ранее механизмы обеспечения целостности, конфиденциальности и доступности.

Последующими шагами исследования можно полагать рассмотрение способов хранения конфиденциальной информации в зашифрованном виде, а так же методов ее обработки и поиска в облачном хранилище.

Литература

1. *Wayne Jansen*, *Timothy Grance*. NIST SP 800–144 Guidelines on Security and Privacy in Public Cloud Computing, December 09, 2011. 80 p. URL: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494

2. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27 июля 2006 г. № 149-ФЗ. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264 (дата обращения 25.12.2016).

3. FIPS197. Advanced Encryption Standard. Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, November 26, 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (дата обращения 01.02.2017).

4. U.S. Patent 4,405,829. Cryptographic Communications system and method. Ronald L. Rivest, Adi Shamir, Leonard M. Adleman. Declared 14.12.1977. Published 20.09.1983.

5. *Dierks T.*, *Rescorla E.* The Transport Layer Security (TLS) Protocol, Version 1.2 (RFC5246). URL: https://tools.ietf.org/html/rfc5246 (дата обращения 13.12.2016).

6. *Li W.*, *Mitchell C.J.* (2014) Security Issues in OAuth 2.0 SSO Implementations. In: Chow S.S.M., Camenisch J., Hui L.C.K., Yiu S.M. (eds) Information Security. ISC2014. Lecture Notes in Computer ScienceSpringer-Verlag, 2014. Vol. 8783. Pp. 529–541.

RESEARCH OF MECHANISMS OF THE PROTECTED ACCESS PROBLEM TO CLOUD DATA STORAGE

Dmitry V. Sakharov,
St. Petersburg, Russia, d.sakharov@rkn.gov.ru

Mark V. Levin,
St. Petersburg, Russia, m.va.levin@gmail.com

Elena S. Fostach,
St. Petersburg, Russia, elena.fostach@gmail.com

Lidiya A. Vitkova,
St. Petersburg, Russia, iskinlidia@gmail.com

ABSTRACT
Cloud computing is a new computational paradigm that offers a distributed infrastructure. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption. The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy and elasticity. Cloud computing security concerns, especially data security and privacy protection issues, remain the first problem of cloud computing services.
In the actual article we introduce a detailed analysis of the cloud security problem. We investigated the problem from the cloud architecture. Based on this analysis we offers a detailed specification of the cloud security problem and key features that should be covered by any proposed security solution.

Keywords: privacy protection; cloud architecture; cloud computing; cloud computing security; data segregation; data security.

References
1. Wayne Jansen, Timothy Grance. NIST SP 800–144 *Guidelines on Security and Privacy in Public Cloud Computing*, December 09, 2011. 80 p. URL: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494.
2. *Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii* [On information, information technologies and protection of information] Federal'nyy zakon ot 27 iyulya 2006 g. № 149-FZ [Federal law of July 27, 2006 149-FZ] URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108264 (date of access 25.12.2016). (In Russian)
3. FIPS197. Advanced Encryption Standard. Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, November 26, 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (date of access 01.02.2017).
4. U.S. Patent 4,405,829. Cryptographic Communications system and method. Ronald L. Rivest, Adi Shamir, Leonard M. Adleman. Declared 14.12.1977. Published 20.09.1983.
5. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol, Version 1.2 (RFC5246). URL: https://tools.ietf.org/html/rfc5246 (дата обращения 13.12.2016).
6. Li W., Mitchell C.J. (2014) Security Issues in OAuth 2.0 SSO Implementations. In: Chow S.S.M., Camenisch J., Hui L.C.K., Yiu S.M. (eds) Information Security. ISC2014. Lecture Notes in Computer ScienceSpringer-Verlag, 2014. Vol. 8783. Pp. 529–541.

Information about authors:
Sakharov D.V., PhD, associate professor at the Department of Protected communication systems of the St. Petersburg State University of Telecommunications prof. Bonch-Bruevich;
Levin M.V., postgraduate student of the St. Petersburg State University of Telecommunications prof. Bonch-Bruevich;
Fostach E.S., graduate student of the St. Petersburg State University of Telecommunications prof. Bonch-Bruevich;
Vitkova L.A., postgraduate student of the St. Petersburg State University of Telecommunications prof. Bonch-Bruevich.

For citation: Sakharov D.V., Levin M.V., Fostach E.S., Vitkova L.A. Research of mechanisms of the protected access problem to cloud data storage. *H&ES Research*. 2017. Vol. 9. No. 2. Pp. 40–46. (In Russian)

РОССИЙСКАЯ НЕДЕЛЯ
ВЫСОКИХ ТЕХНОЛОГИЙ

ТПП РФ

ufi Approved Event

Expo Rating

СВЯЗЬ

Информационные и коммуникационные технологии

25–28 апреля 2017

В НОВЫЕ СРОКИ

29-я международная выставка

Организатор:

ЭКСПОЦЕНТР МОСКВА

При поддержке:

- Государственной Думы Федерального Собрания РФ
- Министерства связи и массовых коммуникаций РФ
- Министерства промышленности и торговли РФ
- Федерального агентства связи (Россвязь)
- Российской ассоциации электронных коммуникаций (РАЭК)

Под патронатом Торгово-промышленной палаты РФ

Россия, Москва, ЦВК «Экспоцентр»

www.sviaz-expo.ru

Реклама 12+

МОДИФИКАЦИЯ НЕКОТОРЫХ ПРОЦЕДУР АВТОМАТИЧЕСКОГО АНАЛИЗА ДАННЫХ

Моисеев Александр Александрович,
к.т.н., старший научный сотрудник Государственного
Научно-исследовательского института химмотологии,
г. Москва, Россия, slow.coach@yandex.ru

АННОТАЦИЯ

Наиболее значимой составляющей автоматизированной обработки информации является автоматический анализ данных. Наряду с классическими процедурами статистического анализа – факторного, дисперсионного, дискриминантного и др. – он также включает ряд дополнительных процедур, не связанных напрямую со статистическим анализом. К ним, в частности относятся процедуры генетической оптимизации, классификации без учителя путем кластеризации исходной выборки данных, методы адаптации перцептронного классификатора по обучающей выборке, а также процедура нечеткого управления. В настоящее время предпринимаются значительные усилия по объединению подобных процедур в рамках единой интеллектуальной технологии. В рамках этих усилий здесь рассматриваются некоторые модификации указанных процедур путем их существенного упрощения – как идеологически, так и в части реализации. Проведенное рассмотрение показало, что они имеют сравнительно простую основу. Так, генетическая оптимизация была сведена к двухшаговой версии случайного поиска экстремума, шагами в которой является предварительное смешивание результатов первичного поиска, аналогичное скрещиванию, и вторичный случайный поиск в выделенной области, соответствующий мутации. Метод потенциальных функций позволил сравнительно просто реализовать автоматическую кластеризацию входной выборки без ограничений на ее характер. В предложенном алгоритме обучения перцептронного классификатора обработка в ассоциативном нейроне была реализована в виде усреднение сигналов от подключенных рецепторов с вычитанием постоянной величины. Дополнительное использование условия нормировки адаптивных коэффициентов делает ее малосущественной при использовании выбора максимума в качестве решающего правила. Методически несложно реализована процедура обучения алгоритма нечеткого управления, базирующаяся на выравнивании частот реализации управляющих воздействий при использовании эквидистантной выборки входных состояний.

Ключевые слова: автоматический анализ данных; генетическая оптимизация; случайный поиск; скрещивание; мутация; потенциальные функции; кластеризация; перцептрон; классификатор; машинное обучение; нечеткое управление

Для цитирования: *Моисеев А.А.* Модификация некоторых процедур автоматического анализа данных // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 48–53.

Наиболее значимой составляющей автоматизированной обработки информации является автоматический анализ данных. Наряду с классическими процедурами статистического анализа — факторного, дисперсионного, дискриминантного и др. [1] — он также включает ряд дополнительных процедур, не связанных напрямую со статистическим анализом. К ним, в частности относятся процедуры генетической оптимизации, классификации без учителя путем кластеризации исходной выборки данных, методы адаптации перцептронного классификатора по обучающей выборке, а также процедура нечеткого управления. В настоящее время предпринимаются значительные усилия по объединению подобных процедур в рамках единой интеллектуальной технологии [2, 3]. В рамках этих усилий здесь рассматриваются некоторые модификации указанных процедур путем их существенного упрощения — как идеологически, так и в части реализации.

Генетическая оптимизация представляет собой модификацию классических генетических алгоритмов поиска экстремума. Ее первым шагом является случайный поиск экстремума, например, максимума, в m — мерном пространстве факторов X. Совокупности случайных точек x_i, $i = 1, \ldots n$, соответствует совокупность x_{ij} их координат, где $j = 1, \ldots m$, а также совокупность y_i значений максимизируемой функции в этих точках. Пусть $\min = \min\limits_i y_i$ — минимальное значение указанной функции на введенной выборке. В качестве первого приближения точки максимума выберем точку с координатами

$$x'_j = \frac{\sum\limits_i x_{ij}\left(y_i - \min\right)^{\alpha}}{\sum\limits_i \left(y_i - \min\right)^{\alpha}},$$

где $\alpha = 1, 2, \ldots$ — параметр элитарности [2], рост которого ведет к быстрому росту вероятности отбора точки максимума практически без изменения. Расчет точки максимума путем использования взвешенного среднего соответствует процедуре скрещивания генетического алгоритма. Точка $x' = (x'_1, \ldots, x'_m)$ определяет центр области мутации $(x'_j - \Delta, x'_j + \Delta)$, $j = 1 \ldots m$, в которой осуществляется дальнейший поиск максимума методом случайного поиска. При этом дополнительно вводится случайная выборка x'_i, $i = 1, \ldots, n'$. Результатом этого поиска является $y' = \max\limits_{x \in \{x', x'_1, \ldots, x'_{n'}\}} y(x)$, а точка x: $y(x) = y'$ соответствует результату мутации для этой итерации.

Полученная таким образом точка максимума заменяет точку минимума в исходной выборке, после чего осуществляется следующая итерация генетической оптимизации. Итерации продолжаются до останова процедуры при выполнении условия $\frac{\max_k - \min_k}{\max_0 - \min_0} < \varepsilon \in (0,1)$, где $\max_k$, $\min_k$ — значения максимума и минимума на k-той итерации, а $\max_0$, $\min_0$ — значения максимума и минимума при первичном случайном поиске.

Преимуществом данной процедуры является ее всеобъемлющий характер, позволяющий осуществлять поиск глобального максимума. Ее основной недостаток — низкая скорость сходимости за счет необходимости перебора всех точек исходной выборки. Вероятно, эту скорость удалось бы повысить, ограничившись случайным поиском в области мутации. Однако при этом существует опасность выплеснуть с водой и ребенка, пропустив точку максимума вне этой области. Поэтому вопрос о коррекции правила останова остается пока открытым.

Модифицированная кластеризация базируется на использовании метода потенциальных функций [4, 5]. Его первым шагом является расчет максимального расстояния Δ между крайними точками исследуемой выборки. В каждой из этих точек формируется потенциал вида

$$\varphi = \frac{1}{1 + \alpha\left(\frac{r}{\Delta}\right)^2},$$

где r — расстояние от крайней точки до данной, α — параметр потенциальной функции. К каждому из исходных кластеров относятся точки, удовлетворяющие условиям отнесения $\varphi_A(r) > 0.9$, $\varphi_B(r) > 0.9$. При добавлении точек в кластер соответствующие потенциалы трансформируются следующим образом:

$$\varphi_A \to \frac{1}{n_A}\sum_{r_i \in A}\varphi\left(r_i\right)$$

$$\varphi_B \to \frac{1}{n_B}\sum_{r_i \in B}\varphi\left(r_i\right)$$

Добавление точек к кластерам A и B завершается, когда в выборке не остается точек, удовлетворяющим условиям $\varphi_A > 0.9$, $\varphi_B > 0.9$.

Из точек, не отнесенных к исходным кластерам, выберем точку C, сумма квадратов расстояний от которой до крайних точек максимальна. Эта точка интерпретируется как зародыш третьего кластера, в который входят точки, оставшиеся вне исходных кластеров и удовлетворяющие условию отнесения $\varphi_C(r) > 0.9$. Как и ранее, добавление точек в кластер будет приводить к трансформации его потенциала: $\varphi_C \to \frac{1}{n_C}\sum\limits_{r_i \in C}\varphi\left(r_i\right)$. Отбор будет проводиться до тех пор, пока не останется точек, удовлетворяющих условию отнесения со скорректированным потенциалом. Эта ситуация отображена на рис. 1.

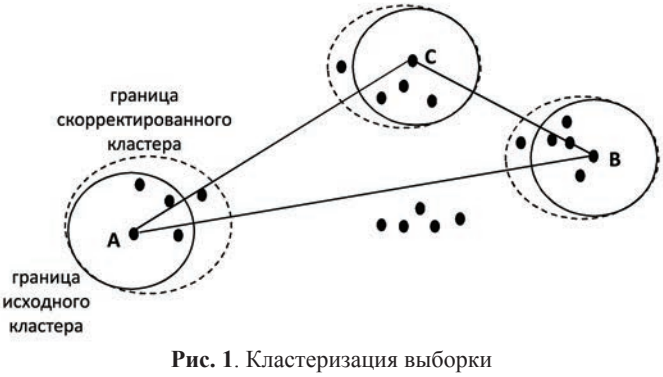


Рис. 1. Кластеризация выборки

Отбор точек, максимально удаленных от крайних, в качестве зародышей кластеров и формирование этих кластеров по описанной методике продолжается до тех пор, пока не останется точек, не отнесенных к кластерам. Преимуществом построенной процедуры кластеризации является е общий характер, позволяющий осуществить кластеризацию без ограничений на кластеризуемую выборку. Недостатком является необходимость выбора параметра настройки α.

Принципиальная схема перцептронного классификатора [5] приведена на рис. 2. Его входами являются рецепторы, формирующие бинарные сигналы $x_1 \ldots x_n$ с одинаковыми коэффициентами усиления $\frac{1}{n}$, линейные функции от которых формируются в ассоциативных нейронах $A_1 \ldots A_k$:

$$y_i = \frac{k}{n} \sum_{x_j \in A_i} x_j - \theta$$

Эти нейроны, таким образом, формируют среднее значение подключенных рецепторов за вычетом параметра классификатора $\theta \in (0,1)$. В свою очередь, выходы ассоциативных нейронов используются для формирования линейных комбинаций $z_i = \sum \lambda_{ij} y_j$ с адаптивными коэффициентами усиления λ_{ij}, выбираемыми по результатам обучения с учителем.

В дальнейшем будем считать, что адаптивные коэффициенты λ_{ij} удовлетворяют условию нормировки $\sum_{j=1}^{k} \lambda_{ij} = 1$, $i = 1,\ldots m$. Их начальным приближением являются случайные величины, равномерно распределенные в интервале (0, 1) и затем скорректированные в соответствии с условием нормировки. Предположим, что для обучения предложен i-тый образ. Если $z_i \neq z_p = z_{max}$, осуществляется следующая коррекция адаптивных коэффициентов:

$$\lambda_{ij} \to a\lambda_{ij}, y_j > 0$$
$$\lambda_{ij} \to \lambda_{ij}, y_j \le 0$$
$$\lambda_{pj} \to \lambda_{pj} / a, y_j > 0$$
$$\lambda_{pj} \to \lambda_{pj}, y_j \le 0$$
$$a > 1$$

Затем скорректированные коэффициенты дополнительно пересчитываются с учетом условия нормировки. Эта операция повторяется с предъявлением i-того образа, пока не будет выполнено условие $z_ш = z_{max}$. После этого для обучения предъявляется следующий образ и описанные выше операции повторяются.

Предъявление образов осуществляется в циклическом порядке, пока персептрон не начнет различать их безошибочно. Это является признаком останова процедуры обучения. Величина θ при описанной организации обучения оказывается не столь существенной, поскольку при выполнении условия нормировки для адаптивных коэффициентов она дает лишь постоянный сдвиг, не влияющий на выбор максимума. Изначально ее можно выбрать, например, равной $\theta = \frac{1}{n}$, а используя ее вариацию в интервале (0, 1), можно добиться линейной сепарабельности распознавания, если последняя имеет место.

Полезным применением процедуры обучения является адаптивная настройка алгоритма нечеткого управления [2, 6]. Его традиционная схема отображена на рис. 3 в предположении, что формируемые управляющие воздействия y_k образуют конечное множество, упорядоченное по возрастанию. Эти воздействия представляют собой выходы процедуры дефуззификации нечетких выводов B_k (термов выходной лингвистической переменной), функции принадлежности которых аппроксимируются гауссовыми формами вида $\mu_{Bk}(y) = \exp\left(-\left(\frac{y - y_k}{\sigma_{yk}}\right)^2\right)$. Величины σ_{yk} выбираются при этом так, чтобы значения «чужих» функций принадлежности в точках y_k были бы <<1. Этому условию удовлетворяет, например выбор σ_{yk} в виде:

$$\sigma_{yk} = \min\left(\frac{y_k - y_{k-1}}{3}, \frac{y_{k+1} - y_k}{3}\right)$$

Таким образом, функции принадлежности нечетких выводов B_k можно считать заданными. В этом случае обучение сводится к выбору функций принадлежности термов

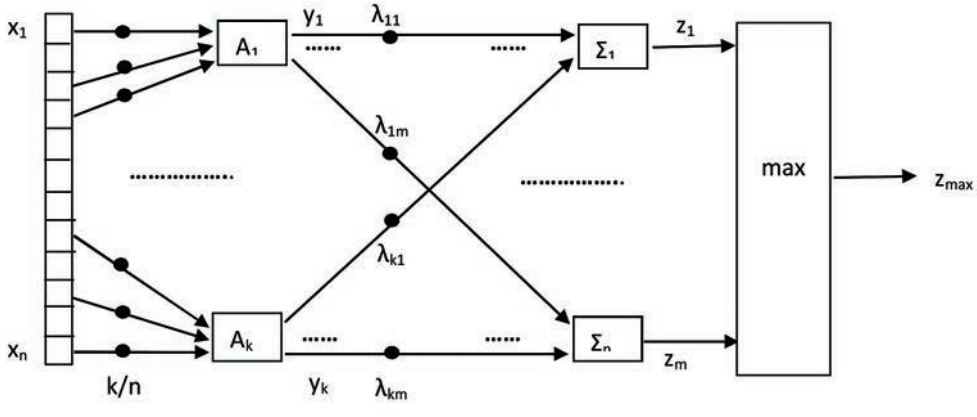


Рис. 2. Перцептронный классификатор

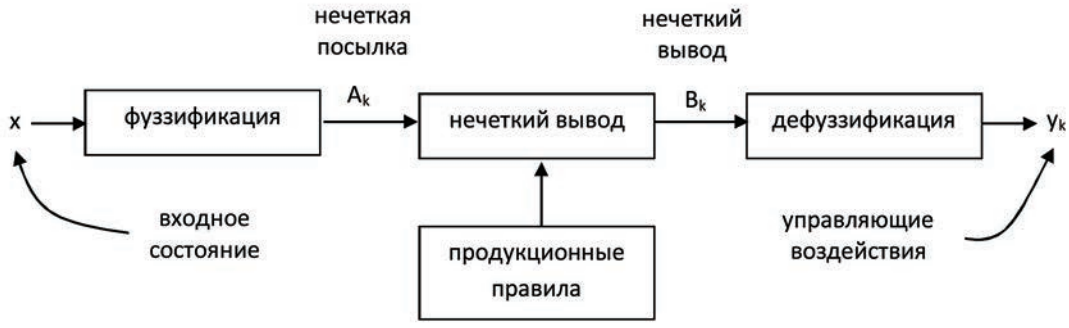


Рис. 3. Нечеткое управление

A_k входной лингвистической переменной. В предположении, что эти функции также аппроксимируются гауссовыми формами $\mu_{Ak}(y) = \exp\left(-\left(\frac{x - x_k}{\sigma_{xk}}\right)^2\right)$, задача их выбора оказывается эквивалентной выбору параметров x_k, σ_{xk}.

Этот выбор подчиним следующим соображениям. Предположим, что входное состояние управляемого объекта финитно и будем в дальнейшем интерпретировать x как относительное отклонение этого состояния от 0, соответствующего уставке регулирования. Поскольку скорость объекта в этой ситуации также ограничена, будем интерпретировать x' как относительную скорость. Типичное поведение x, x' в ситуации регулирования отображено при этом на фазовой диаграмме, приведенной на рис. 4. Из нее видно, что управляющее воздействие определяется по существу только величиной отклонения x. Форма зависимости $y(x)$ управляющих воздействий от состояния также приведена на рис. 4. Априорно она неизвестна, и именно это обуславливает необходимость обучения.

Примем в первом приближении, что центры входных термов $x_1 \ldots x_m$ разделяет область $x \in (-1, 1)$ на равные части. Входные состояния также зададим эквидистантной выборкой $u_1 \ldots u_n$, где $n >> m$. Качественно обработка этой выборки отображена на рис. 5. При правильном выборе $x_1 \ldots x_m$ эквидистантная входная выборка должна порождать равновероятные выборки откликов y. Согласно рисунку этой равновероятности соответствует условие $\frac{\max - \min}{\max} < \varepsilon \in (0,1)$, где max, min — максимальная и минимальная частота одинаковых откликов. Если это условие не выполняется, то интервал на x, соответствующий частотному максимуму, должен сжиматься, а соответствующий частотному минимуму — расширяться. Признаком останова процедуры обучения является приближенное выполнение условии равночастотности откликов.

Проведенное рассмотрение показывает, что рассмотренные алгоритмы автоматического анализа имеют сравнительно простую основу. Так, генетическая оптимизация представляет собой двухшаговую версию случайного поиска экстремума, шагами в которой является предварительное смешивание результатов первичного поиска, аналогичное скрещиванию, и вторичный случайный поиск в выделенной области, соответствующий мутации. Метод потенциальных функций позволяет сравнительно просто реализовать автоматическую кластеризацию входной выборки без ограничений на ее характер. В Предложенном алгоритме обучения перцептронного классификатора обработка в ассоциативном нейроне представляет собой усреднение сигналов от подключенных рецепторов и вы-

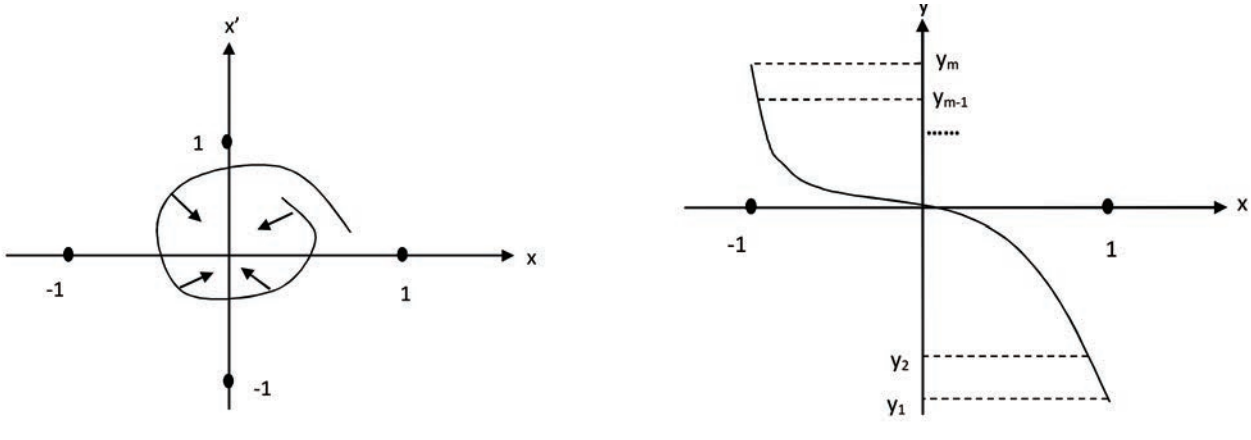


Рис. 4. Динамика регулирования и управляющие воздействия

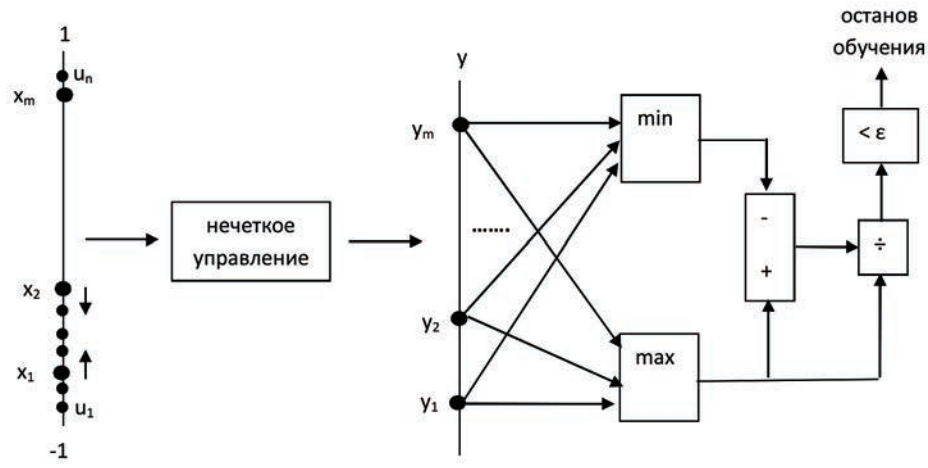


Рис. 5. Обучение нечеткого управления

читание постоянной величины. Дополнительное использование условия нормировки адаптивных коэффициентов воспроизводит эту величину на выходе, что малосущественно при использовании выбора максимума в качестве решающего правила. Методически несложной является и процедура обучения алгоритма нечеткого управления, базирующаяся на выравнивании частот реализации управляющих воздействий при использовании эквидистантной выборки входных состояний.

Литература

1. Статистические методы для ЭВМ / под ред. К. Энслейна, Р. Рэлстона, Г. Уилфа. М.: Наука, 1986. 464 с.

2. *Рутковская Д.*, *Пилиньский Р.*, *Рутковский Л.* Нейронные сети, генетические алгоритмы и нечеткие системы. М.: Телеком, 2006. 452 с.

3. *Роштейн А. П.* Интеллектуальные технологии идентификации. Винница: Универсум, 1999. 320 с.

4. *Айзерман М. А.*, *Браверман Э. М.*, *Розеноэр Л. И.* Метод потенциальных функций в теории обучения машин. М.: Наука, 1970. 384 с.

5. *Вапник В. Н.*, *Червоненкис А. Я.* Теория распознавания образов (статистические проблемы обучения). М.: Наука, 1974. 416 с.

6. *Цыпкин Я. З.* Адаптация и обучение в автоматических системах. М.: Наука, 1968. 400 с.

SOME PROCEDURES MODIFICATION OF AUTOMATIC DATA ANALYSIS

Alexander A. Moiseev,
Moscow, Russia, slow.coach@yandex.ru

ABSTRACT
Automatic data analysis is most substantial component of computer – aided data processing. Along with classical procedures of statistical analysis – factor's, dispersion's, discriminates ones – it includes also some additional procedures not related directly with statistical analysis. Particularly, these are procedures of genetic optimization, classification by means of starting sample clasterization, some method of perceptron adaptation on teaching sample, some procedures of fuzzy control. Now performed essential facilities to consolidate such procedures in form of united intellectual technology. In the framework of these facilities here considered some modifications of these procedures by means of their simplification – ideologically and practically. Performed some algorithms consideration of data analysis, that's shown their base simplicity. Genetic optimization were transformed to two – step version of stochastic search, whose steps are preliminary mixing of primary search results (interpreted as crossing) and secondary stochastic search (interpreted as mutation). Potential function method allowed implementing the simple procedure of clasterization without any additional requirements to input sample. Learning algorithm of perceptron's classifier was used the preliminary averaging in secondary neurons with any constant subtraction. Additional adaptive coefficients normalizing does it insufficient at maximization used as decisive function. Fuzzy control learning were developed that's based on control transactions frequencies equalization at equidistant sample of input states.

Keywords: data analysis; genetic optimization; stochastic search; crossing, mutation; potential functions; cauterization; perceptron; classifier; machine learning; fuzzy control.

References
1. Enslein K., Ralston A., Wilf M.S. (Eds.). *Statistical methods for digital computers*. NewYork, Wiley, 1977, 464 p.
2. Rutkowskaya D., Pilin'skiy R., Rutkovskiy L. *Neyronnye seti, geneticheskiye algoritmy i nechetkiye sistemy* [Neuron's nets, genetic algorithms and fuzzy systems]. Moscow, Telecom, 2006. 452 p. (In Russian)
3. Rotshtein A. *Intellektualnye technologii identifikatsii* [Intellectual identification technologies]. Vinnitsa, Universum, 1999. 320 p. (In Russian)
4. Aizerman M., Braverman E.M., Rozenoer L.I. *Metod potentsialnych functsij v teorii obucheniya mashin* [Potential functions method in machine learning theory]. Moscow, Nauka, 1970. 384 p. (In Russian)
5. Vapnik V., Chervonenkis A.Ya. *Teoriya raspoznavaniya obrazov* (*statisticheskiye problem obucheniya*) [Image recognition theory (statistical learning problems)]. Moscow, Nauka, 1974. 416 p. (In Russian)
6. Tsypkin J. Adaptatsiya i obucheniye v avtimaticheskich sistemach [Adaptation and learning in control systems]. Moscow, Nauka, 1968. 400 p. (In Russian)

Information about author:
Moiseev A. A., PhD, senior researcher of the State institute of himmotology.

For citation: Moiseev A. A. Some procedures modification of automatic data analysis. *H&ES Research*. 2017. Vol. 9. No. 2. Pp. 48–53. (In Russian)

AUTONOMOUS DEFINITION OF REFERENCE AZIMUTHS WITH USE OF THE EQUIPMENT OF CONSUMERS OF SPACE NAVIGATION SYSTEMS

Chernov Ivan Vladimirovich,
postgraduate student, Military Space Academy,
St. Petersburg, Russia, 4ern86@bk.ru

ABSTRACT
Among in geodesic devices in family of high-precision gyrotheodolites (gyrocompasses) there were devices allowing to make definition of astronomical azimuths with the standard deviation (SD) 1–1,5". Values of the astronomical azimuths defined from standard deviation exceeding accuracy the devices by 3–5" [1] are necessary for calibration of such devices that is with standard deviation it is not worse 0,5".
At the heart of creation and periodical control's of bases of calibration of gyrotheodolites (gyrocompasses) lies the astronomical method of definition of an azimuth. The essence of this method consists in the determination of the azimuth of the stellar body and the simultaneous measurement of a horizontal angle between the sun and the local subject. For high-precision definition of an astronomical azimuth, the way through the sentinel sentry of the Polaris star is usually used. The program of definition of an azimuth with an accuracy of 1" has to be carried out this way within not less than two evenings and must consist of 18 receptions in direct and 18 receptions in the opposite direction. Besides for calcula-tion of the azimuths defined with SD 1" value of astronomical latitudes have to be known no more than with a mistake 3". Definition of a personal instrumental difference of observers is also necessary.To receive an astronomical azimuth with SD 0,5" it is necessary to make the observations consisting of several programs of definition of an azimuth with SD 1" different theodolites (the corresponding accuracy), different observers.
Thus, the astronomical method of high-precision determination of coordinates and azimuths is rather composite in realization and demands the considerable time and strongly depends on weather conditions that can be critical at problem solving of geodetic support. As can be seen in addition to the complexity, the astronomical method does not provide required accuracy for to create bases of calibration modern gyrotheodolite.
Currently in solving problems topogeodetic and navigation software is widely used satellite equipment receiving signals from GLONASS and NAVSTAR systems. This article examines the possibility of using such equipmentfor expeditious creating of polygons for calibration modern means of autonomous orientation (gyrotheodolite, gyrocompass).

Keywords: the azimuth; autonomous orientation; high-precision orientation; operative orientation; gyrotheodolite; gyrocompass.

For citation: Chernov I. V. Autonomous definition of reference azimuths with use of the equipment of consumers of space navigation systems. *H&ES Research*. 2017. Vol. 9. No. 2. Pp. 54–58. (In Russian)

Calculation of length of the orientable direction for achievement of the required accuracy of orientation

The idea of a method of definition of an azimuth with use of the equipment of consumers of space navigation systems (EK SNS) consists in the solution of the inverse geodetic task of a difference of coordinates of points received by the relative method of space geodesy.

At realization of the relative method of space geodesy are performed synchronous measurements of pseudo-ranges to observed satellites not less than on two points. From the received data are calculated the difference between the spatial rectangular coordinates ΔX, ΔY, ΔZ these points, which are then considered to be the measured values. The differences of coordinates turn out in common terrestrial coordinate system.

To calculate geodetic azimuths, on coordinates of point B, L, H$^{\gamma}$ with the measured differences of coordinates ΔX, ΔY, ΔZ calculates coordinates, B, L other points wich fix the these directions. And only now from the solution of the inverse geodetic task (IGT) of the received coordinates of points geodetic azimuths of the directions are calculated. For finding of a geodetic azimuth pass from a space geocentric conception of systems coordinates to topocentric horizontal system Y', X', Z'. Then the geodetic azimuth of A can be calculated from the equation

$$A = arctg\left(\frac{\Delta Y'}{\Delta X'}\right) \tag{1}$$

where $\Delta Y'$, $\Delta X'$ — increments in a topocentric horizont system coordinates.

Let's assume that arguments of a formula (1) are independent. Then, using the equation of an standard deviation of function of independent arguments [2], we will receive expression of SD of calculation of an azimuth

$$m_A^2 = \left(\frac{\partial A}{\partial \Delta X}\right)^2 m_{\Delta X}^2 \rho^2 + \left(\frac{\partial A}{\partial \Delta Y}\right)^2 m_{\Delta Y}^2 \rho^2, \tag{2}$$

where m_A — SD of definition of an azimuth; $m_{\Delta X}$, $m_{\Delta Y}$ — SD of definition of increments of coordinates; ρ – the number of seconds in a radian (206265). Let's find partial derivatives of this equation

$$\frac{\partial A}{\partial \Delta X} = \frac{-\Delta Y}{\Delta X^2 + \Delta Y^2} \tag{3}$$

$$\frac{\partial A}{\partial \Delta Y} = \frac{\Delta X}{\Delta X^2 + \Delta Y^2}$$

After substitution of partial derivatives in an assumption formula we will receive:

$$m_A^2 = \left(\frac{-\Delta Y}{\Delta X^2 + \Delta Y^2}\right)^2 m_{\Delta X}^2 \rho^2 + \left(\frac{\Delta X}{\Delta X^2 + \Delta Y^2}\right)^2 m_{\Delta Y}^2 \rho^2 \tag{4}$$

Let SD of definition of increments on abscissa axes and ordinates be equal to m_{Δ}, then the equation (4) will take a form

$$m_A^2 = m_{\Delta}^2 \rho^2 \frac{\Delta X^2 + \Delta Y^2}{\left(\Delta X^2 + \Delta Y^2\right)^2} \tag{5}$$

After apparent simplifications we will receive

$$m_A^2 = \frac{m_{\Delta}^2 \rho^2}{\Delta X^2 + \Delta Y^2} \tag{6}$$

In a denominator of this equation a square of length of the orientable direction D specified on the horizon plane. Therefore,

$$m_A = \frac{m_{\Delta} \rho}{D} \tag{7}$$

Considering that accuracy of definition of increments of coordinates of the modern EK SNS makes about 2 mm+0,5 mm*D-km and using a formula (7), perhaps a priori to calculate SD of definition of a geodetic azimuth depending on length of the orientable direction. Results of calculation saregivenin fig. 1.

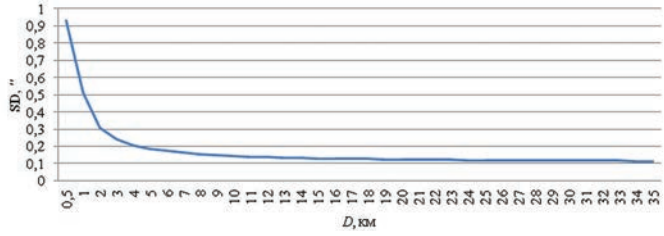


Fig. 1. The expected SD of definition of geodetic azimuths depending on the distance D between points installations of EK SNS antennas given on the horizon plane

The analysis of the received results allows to draw a conclusion that application of the relative method of space geodesy without use of reference points (a land initial geodetic basis) allows to define geodetic azimuths with CD 0,5-0,3″ with a length of orientable direction about 1000-2000 m. Now we will consider a problem of the choice of the orientable directions.

The choice of an azimuth of the orientable direction for achievement of the required accuracy

To increase accuracy and efficiency of the considered method, we will accept a hypothesis of equal influence in the same instant of various sources of mistakes on observed datas for any receiver in the local area (10–30 km) [4]. Then generally, when the zenith distance of the orientable direction will not be equal 90°, there will be a dependence of an error of orientation δA the directions from errors of definition of geodetic coordinates ΔB and ΔL. This dependence is described by the equation [1]

$$\delta A = \left(\Delta B \ \sin A - \Delta L \ \cos A \ \cos B\right) \ \text{ctg}\, z \tag{8}$$

where z — zenith distance of the orientable direction; B, L – the geodetic width and longitude of point from which the azimuth is defined.

From (8) it is visible what δA also depends on an azimuth, a slope angle of the orientable direction and width.rom a formula (8) it is visible that even at errors, in the linear measure of the reaching 15 m, the difference (δA) between any azimuths from a set of the received vectors, will not exceed 0,1″ at slope angles of the orientable direction less than 5 °. Besides, at the latitude of Moscow at orientation of the direction, the close to

$\pi/3 + \pi n$, size $\delta A \approx 0$. For definition of a condition of the choice of the direction at the arbitrariest width we will equate expression (8) to zero

$$\Delta B \ \sin A - \Delta L \ \cos A \ \cos B = 0 \quad (9)$$

having accepted $\Delta B = \Delta L$ we will receive

$$\sin A = \cos A \ \cos B \quad (10)$$

Let's divide both parts of equality into cos$A$

$$A = \operatorname{arctg}\left(\cos B\right) + \pi n \quad (11)$$

The received expression is a direction choice rule at the arbitrariest width when determining azimuths of the directions with application of EK SNS without use of an initial geodetic basis under a condition $\Delta B = \Delta L$. In a case $\Delta B \neq \Delta L$ expression (11) will take a form.

$$A = \operatorname{arctg}\left(\left(\frac{\Delta L}{\Delta B}\right)\cos B\right) + \pi n \quad (12)$$

Let by means of EK SNS coordinates with an accuracy of 0,1 m will be received. Having accepted a confidence interval 2,5 m we will receive that with probability 0,98 [2] $\Delta L \in$ [-0,25, 0,25], $\Delta B \in$ [-0,25, 0,25].

In this case $\max \Delta L/\Delta B \to \infty$ that will not allow to define a direction choice rule at the arbitrariest width when determining azimuths of the directions with application of EK SNS without use of an initial geodetic basis. Then, having brought in ΔL and ΔB equal mistakes which considerably (much) will exceed values ΔL and ΔB, we will receive $\Delta L \in$ [-0,25, 0,25], $\Delta B \in$ [-0,25, 0,25]. In this case $\max \Delta L/\Delta B \approx 1{,}05$. Results of calculations for a formula (11) and (12) are given in the fig. 2.

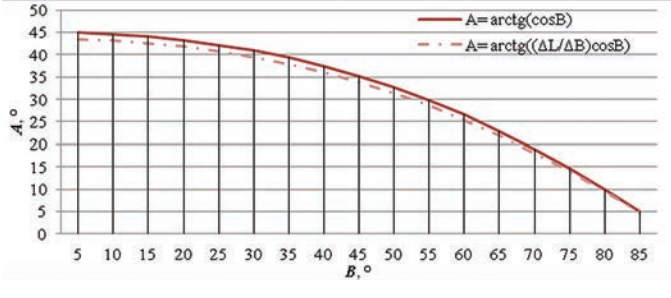


Fig. 2. Results of calculation of azimuths zero δA for a slope angle of the orientable direction equal 5°

From results of calculation of azimuths zero δA (fig. 2) can draw a conclusion that for an exception of azimuthal distortions at independent definition of a high-precision azimuth with application of EK SNS it is necessary to design geodetic network proceeding from the rule (11).

Thus, in case of high-precision orientation and excess of a slope angle of the orientable direction at a size of 5 ° and more (orientation in the mountain area) needs to be considered δA. When using of the offered orientation method the account δA is impossible as the geodetic basis necessary for calculation of sizes ΔB and ΔL geodetic coordinates is not used. However there is an opportunity to compensate δA by the choice of the direction of the close to $A = \operatorname{arctg}(\cos B) + \pi n$. In this case the orientable direction will be almost completely saved from influence of systematic errors of orientation, the bound to lack of an initial geodetic basis. Further from this direction in the way "in all combinations" or the directions in the way of "circular receptions" the geodetic azimuth can be transferred by a goniometry method with initial to any direction.

Calculation of time of observations by the equipment of consumers of space navigation systems for achievement of the required accuracy of positioning and orientation

Phase ambiguities are allowed for obtaining coordinates at development of geodetic networks by the relative method of space geodesy. A disambiguation is called definition of the complete number of cycles bearing (lengths of waves) between the antenna and the satellite (searching of the whole value of number of lengths of waves).For measurements in the mode this whole value decides on post-processing (PP) which is used for definition of location with an accuracy at the level of centimeter during computerizing. For measurements in real time which are used for definition of location with an accuracy at the level of centimeter this whole value is defined during the process called by initialization. The resolving time of phase ambiguities of t0 for the modern satellite geodetic receivers (EK SNS) from 5 seconds to 10 minutes [5].

After permission of phase ambiguities of EK SNS receives the solution of a navigation task (a phase method) with an interval of one second and more (intervals turn out less than 1 second by interpolation between one-second observations).

Accuracy of obtaining coordinates (SD) in the absolute mode of positioning for EK SNS deviation 5 m [5] today. This deviation is caused by the equivalent bias of pseudo-range (UERE) and a steric geometrical factor (PDOP) [3].Considering above described, it is possible to write down $Ri = [X, Y, Z] + \Delta i = [X_i, Y_i, Z_i]$ where $\Delta = f$ (UERE, PDOP); X, Y, Z — coordinates of the EK SNS installation; X_i, Y_i, Z_i — the coordinates of the EK SNS installation received during an era of $i \in [1, N]$, – the number of measurements (eras).

The true deviation Δ will include ⌂ casual and δ a systematic component. Let the provision of EK SNS concerning Earth be constant, and the size δ can be neglected. Then, the unbiased deviation of calculation of average coordinates will be compensated. In case of the normal distribution law of a deviation ⌂ the expectation of the M random value of R coincides with its arithmetic average

$$M(R) = \bar{R} = \frac{[R]}{N} \quad (13)$$

Having accepted that SD of determination of coordinates in the absolute mode of positioning for EK SNS will deviation $m_{Ri} = 9{,}8$ m, we will receive SD of an arithmetic average R (13) on

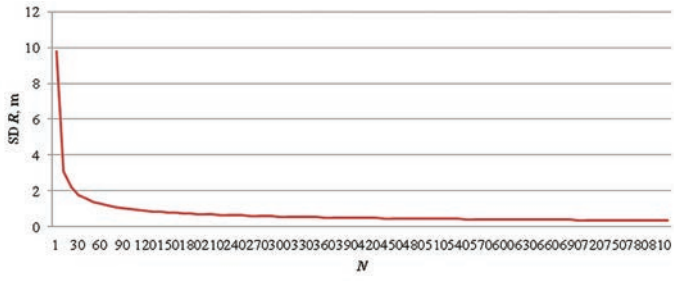


Fig. 3. The expected SD of the average coordinates received with application of an absolute method of positioning

$$m_{\bar{R}} = \frac{m_{Ri}}{\sqrt{N}} \quad (14)$$

Visualization of the given dependence is presented in fig. 3.

Using dependence (14), it is not difficult to write down a formula of time spent for achievement of the given SD of determination of coordinates

$$T = t_0 + tN, N = \left(\frac{m_{Ri}}{m_{\bar{R}}} \right)^2 \quad (15)$$

where T — time spent for achievement of the set SD of determination of coordinates, t — time of one solution of a navigation problem of $t = t_i – t_i – 1$; t_0 — a resolving time of phase ambiguities.

The least interval of the solution of a navigation problem of to deviations one second. Proceeding from a formula (15), time of observations for achievement of the required accuracy of determination of coordinates will make: 12 min. – 1 m; 17 min. – 0,5 m, 3 h – 0,5 m.

In the given calculations systematic components of definitions of pseudo-range (UERE) and systematic components of the deviations caused by a steric geometrical factor (PDOP) are not considered. For increase in accuracy of definitions in the specified conditions it is expedient to apply PPP (Precise Point Positioning) to post-processing.

As so with accumulation of number of measurements coordinates of points are specified, also their differences will be specified, i.e. increments of coordinates, application of averaging of coordinates and increments allows to solve a problem of a high-precision binding of the fixed object on a daily interval of observations and to solve a problem of high-precision definition of an azimuth without use of an initial land geodetic basis, i.e. is autonomously.

Technique of use of the equipment of consumers of space navigation systems for independent definition of reference azimuths

Based on explained above it is possible to present a technique of application of EK SNS for independent definition of azimuths with the required accuracy.

The first step of a technique — "Calculation of length of the orientable direction for achievement of the required accuracy of orientation". Knowing the required SD of definition of an azimuth m_A and accuracy of definition of increments of coordinates of m_Δ, the distance (the basic line) on which is calculated by a formula (7) it is necessary to carry EK SNS antennas.

The following step — "The choice of an azimuth of the orientable direction for decrease in influence of an deviation of determination of coordinates". Knowing EK SNS installation site width, the azimuth with which the orientable direction has to coincide is calculated by a formula (11).

The third step is "Calculation of time of observations of EK SNS for achievement of the required accuracy of positioning and orientation". The formula (15) is used for calculations.

Observations with application of EK SNS are carried out according to the user's guide, but when keeping an indispensable condition — observations on points of the orientable direction have to be simultaneous.

Processing of observed datas is carried out in conclusion of a technique. Calculation of coordinates of point from which the azimuth according to an absolute method of positioning is defined is carried out. The received coordinates are used as initial for determination of coordinates by the relative method of space geodesy. The azimuth and zenith distance of the direction pay off with use of the received coordinates.

After the solution of IGT the zenith distance of z of the orientable direction is estimated. In case z exceeds 5 °, both coordinates of both points change at the equal size (which is much surpassing accuracy of obtaining coordinates) and IGT is solved once again. The second decision is made by total.

The offered technique will allow to apply EK SNS to independent definition of reference azimuths with the required accuracy, due to installation of rules of projection of situation on zenith distance, an azimuth and length of the reference direction, will also allow to define necessary time of observations.

References

1. Gusenitsa Y.N., Malakhov A.V. Simulation model of reconfigurable metrological complexes functioning in the conditions of information uncertainty on the receipt of measurement funds for metrological service. *Uchenye zapiski Komsomolsk-na-Amure Gosudarstvennyy tekhnicheskiy universitet* [Scholarly Notes of Komsomolsk-na-Amure State Technical University. Engineering and Natural Sciences]. 2016. No. III-1(27). Pp. 32–46. (In Russian).

2. Rusyaeva E.A. *Teoriya matematicheskoj obrabotki geo-dezicheskih izmerenij. CHast' 1. Teoriya oshibok izmerenij* [The theory of mathematical processing of geodetic measurements. Part 1. Theory of measurement errors]. Moscow: Moskovskiy gosudarstvennyy universitet geodezii i kartografii Publ., 2016. 56 p. (In Russian)

3. Antonovich K.M. *Ispolzovanie sputnikovyx radionavigacionnyx sistem v geodezii* [The use of satellite navigation systems in geodesy]. In 2 vol. Moscow, Kartgeotsentr, 2006. 360 p. (In Russian)

4. Astapovich A.V., Bogachev A.N., Makarov S.A. *Teoriya matematicheskoj obrabotki izmerenij. Part 2. Metod nai-*

men'shih kvadratov [The theory of mathematical processing of measurements. Part 2: Method of least squares]. St. Petersburg: Voenno-kosmicheskaya akademiya imeni A.F. Mozhayskogo-Publ., 2014. 102 p. (In Russian)

5. Precision of GLONASS/GPS navigation definitions. *Russian system of differentional correction and monitoring*. URL: http://www.sdcm.ru/smglo/ (date of access 16.01.2017). (In Russian)

АВТОНОМНОЕ ОПРЕДЕЛЕНИЕ ЭТАЛОННЫХ АЗИМУТОВ С ПРИМЕНЕНИЕМ АППАРАТУРЫ ПОТРЕБИТЕЛЕЙ КОСМИЧЕСКИХ НАВИГАЦИОННЫХ СИСТЕМ

Чернов Иван Владимирович,
адъюнкт Военно-космической академия имени А.Ф. Можайского,
г. Санкт-Петербург, Россия, 4ern86@bk.ru

АННОТАЦИЯ

Среди геодезических приборов в семействе высокоточных гиротеодолитов (гирокомпасов) уже появились приборы позволяющие производить определение астрономических азимутов со средней квадратической ошибкой (СКО) 1–1,5". Для эталонирования таких приборов необходимы значения астрономических азимутов определённых со СКО превышающей точность эталонируемых приборов в 3–5 раз [1], то есть с СКО не хуже 0,5".

В основе создания и периодического контроля баз эталонирования гиротеодолитов (гирокомпасов) лежит астрономический метод определения азимута. Сущность этого метода состоит в определении азимута светила и одновременном измерении горизонтального угла между светилом и местным предметом. Для высокоточного определения астрономического азимута обычно используется способ по часовому углу Полярной звезды. Программа определения азимута этим способом с точностью 1" должна выполняться в течение не менее двух вечеров и состоять из 18 приёмов в прямом и 18 приёмов в обратном направлении. Кроме того для вычисления азимутов, определяемых с СКО 1", значение астрономических широт должны быть известны с ошибкой не более 3". Кроме того необходимо определение личной инструментальной разности наблюдателей. Для получения астрономического азимута с СКО 0,5" необходимо производить наблюдения состоящие из нескольких программ определения азимута с СКО 1" разными теодолитами (соответствующей точности), разными наблюдателями.

Таким образом, астрономический метод высокоточных определений координат и азимутов является достаточно сложным в реализации и требует значительного времени и сильно зависит от метеорологических условий, что может быть критичным при решении задач геодезического обеспечения. Как видно помимо трудоёмкости, астрономический метод не обеспечивает требуемые для создания баз эталонирования современных гиротеодолитов точности.

В настоящее время при решении задач топогеодезического и навигационного обеспечения широко используется спутниковая аппаратура (АП КНС), принимающая сигналы от навигационных систем ГЛОНАСС и NAVSTAR. В настоящей статье рассматривается вопрос о возможности применения такой аппаратуры при оперативном создании полигонов эталонирования современных средств автономного ориентирования (гиротеодолитов, гирокомпасов).

Ключевые слова: азимут; автономное ориентирование; высокоточное ориентирование; оперативное ориентирование; гиротеодолит; гирокомпас.

Для цитирования: *Чернов И. В.* Автономное определение эталонных азимутов с применением аппаратуры потребителей космических навигационных систем // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 54–58.

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 содержимого;
- 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.

НПЦ ИРС
Научно-производственный центр
Информационных региональных систем
▸ npcirs.ru

Телефон: 8(800)100-40-90
E-mail: administrator@npcirs.ru

Предоставляемая для публикации статья 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 научно-теоретический уровень публикуемого материала.

1. **Статья подготавливается** в редакторе MS Word. **Шаблон статьи можно скачать на сайте журнала www. h-es.ru.**

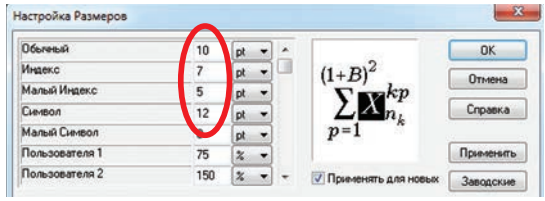
2. **Объём статьи** без аннотации — от 10 до 20 тыс. знаков. Рисунки и таблицы в объеме статьи не учитываются.

3. **Объем аннотации** 250-300 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** (не менее пяти), разделенных точкой с запятой.

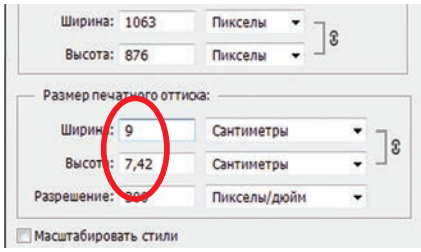
5. Фамилия, имя, отчество, ученая степень, звание, должность и полное название организации — места работы, город, страна, адрес электронной почты и почтовый адрес каждого автора полностью.

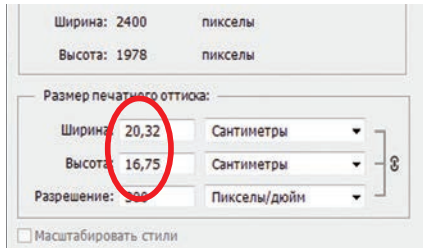
6. **Формульные выражения** выполняются в редакторе Math Type. Формулы нумеруются в круглых скобках, источники — в прямых. Нумерация формул и приведение в списке источников, на которые нет ссылок по тексту, не допускается. Длина формулы в одну строчку 8–9см. В формулах использовать только буквы латинского 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 четкие 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 *.tif 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** не менее пяти наименований, для статей – с указанием страниц, для книг — с указанием общего числа страниц в книге, для интернет-сайта — с указанием даты обращения. 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 7.05-2008. Образец оформления списка литературы размещен на сайте журнала.

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.

10. Статья предоставляется в электронном виде, единым файлом, имеющим следующую структуру: заглавие статьи, сведения об авторах, ключевые слова, аннотация, текст статьи (включая иллюстрации, таблицы и формулы), пристатейный список литературы, англоязычный блок. Также представляется отдельная папка с экспортированными изображениями рисунков в формате TIFF, по требованиям указанным в п.7.

11. 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.

Редакция принимает к публикации статьи на английском языке.

Внимание! Редакция оставляет за собой право отклонить представленные материалы, оформленные не по указанным правилам.