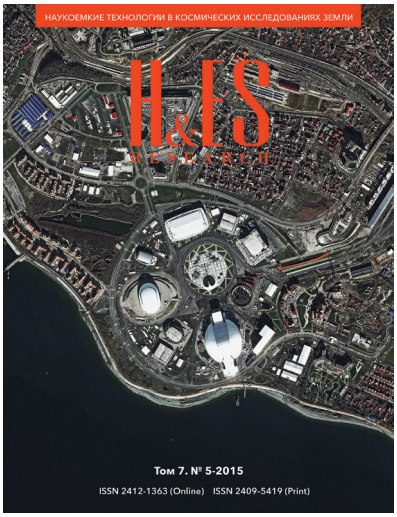

Том VII. № 5-2015

Издается с 2009 года
Издательская лицензия ПИ № ФС 77-60899
Язык публикаций: русский, английский
Периодичность выхода –6 номеров в год
Сайт в Интернете: **www.H-ES.ru**
E-mail: **HT-ESResearch@yandex.ru**

УЧРЕДИТЕЛЬ:
ООО «Издательский дом Медиа Паблишер»

ГЛАВНЫЙ РЕДАКТОР:
Константин Легков

ИЗДАТЕЛЬ:
Светлана Дымкова

ПРЕДПЕЧАТНАЯ ПОДГОТОВКА:
ООО «H&ES Research»

АДРЕС РЕДАКЦИИ:
111024, Россия, Москва,
ул. Авиамоторная, д. 8, офис 512-514

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

Журнал H&ES Research зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия.
Мнения авторов не всегда совпадают с точкой зрения редакции. За содержание рекламных материалов редакция ответственности не несет.
Материалы, опубликованные в журнале – собственность ООО «ИД Медиа Паблишер». Перепечатка, цитирование, дублирование на сайтах допускаются только с разрешения издателя.

ПЛАТА С АСПИРАНТОВ ЗА ПУБЛИКАЦИЮ РУКОПИСИ НЕ ВЗИМАЕТСЯ

Всем авторам, желающим разместить научную статью в журнале, необходимо оформить ее согласно требованиям и направить материалы на электронную почту: **HT-ESResearch@yandex.ru.**
С требованиями можно ознакомиться на сайте: **www.H-ES.ru.**

H&ES Research – один из ведущих рецензируемых научных журналов, в котором публикуются основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук. Журнал 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.
H&ES Research – научно-технический журнал для специалистов в области современных инфокоммуникационных технологий и автоматизированных систем управления, средств космических исследований Земли и информационной безопасности. В журнале публикуются новости о событиях в вышеуказанных областях, репортажи и интервью ведущих компаний, мнения специалистов, новые технологии, инновационные разработки, оборудование и решения, аналитические статьи, маркетинговые исследования и др.

Журнал входит в систему российского индекса научного цитирования (РИНЦ)

ISSN 2412-1363 (Online)

ISSN 2409-5419 (Print)

Тематика публикуемых статей в соответствии с перечнем групп специальностей научных работников по Номенклатуре специальностей:
- 01.01.00 Математика
- 05.07.00 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

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.)

Дизайн и компьютерная верстка: Оксана Иванова
Системный администратор сайта: Вячеслав Косинов
Отдел развития и рекламы: Ольга Дорошкевич

H&ES Research – one of leading reviewed scientific journal in whom the main scientific results of the dissertation on competition of a scientific degree of the doctor and the candidate of science are published. The journal covers achievements and problems of the Russian infokommunikatsiya, 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.

H&ES Research – journal for specialists in the field of modern information and communication technologies and automated systems management means for Space Research of the Earth and information security. The journal publishes news about events in the above areas, reports and interviews of the leading companies, the opinions of experts, new technologies, innovations, products and solutions, analytical articles, market research and others.

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

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.)

Design and computer imposition: Oksana Ivanova
Site's system administrator: Vyacheslav Kosinov
Development and advertizing department: Olga Doroshkevich

H&ES RESEARCH

Vol. VII. № 5-2015

It is published since 2009
Publishing license ПИ № ФС 77-60899
Language of publications:
Russian, English
Periodicity – 6 issues per year
Site on the Internet: **www.H-ES.ru**
E-mail: **HT-ESResearch@yandex.ru**

FOUNDER: «Media Publisher», LLC

EDITOR IN CHIEF: Konstantin Legkov

PUBLISHER: Svetlana Dymkova

PREPRESS: «H&ES Research», JSC

ADDRESS OF EDITION:
111024, Russia, Moscow,
st. Aviamotornaya, 8, office 512-514

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

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. The opinions of the authors don't always coincide with the point of view of the publisher. For the content of ads, the editorial Board is not responsible.

GRADUATE 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.

«H&ES RESEARCH – HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH» JOURNAL

WWW.H-ES.RU

HES_Research HES–Research
club55425245

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

СОДЕРЖАНИЕ

CONTENTS

Анализ использования населением цифрового эфирного телевидения и его влияния на платное телевидение

J'son & Partners Management Consultancy

Компания J'son & Partners Consulting проанализировала возможную степень влияния цифрового эфирного вещания на деятельность операторов платного телевидения в крупных городах России.

Ключевые вопросы исследования

В исследовании дан анализ взаимного влияния российских рынков цифрового эфирного вещания и платного телевидения.

Целью исследования является анализ ожидаемого использования цифрового эфирного вещания и его влияние на потребление населением услуг платного телевидения.

Практическая ценность исследования

Данное исследование дает оценку потенциала роста спроса на услуги цифрового эфирного вещания среди населения крупных городов России и перспектив оттока абонентов российских телекоммуникационных компаний, предоставляющих услуги платного телевидения.

Результаты исследования могут послужить основой в ходе выработки стратегии развития бизнеса участниками рынка.

Целевая аудитория

Результаты исследования и сделанные в нем выводы будут представлять интерес для операторов платного телевидения, телеканалов и исследовательских агентств, а также других компаний, участвующих или потенциально заинтересованных в участии на рынке платного телевидения в России.

Резюме исследования

Цифровое эфирное телевидение (ЦЭТВ) является общедоступным телевидением, сигнал которого транслируется по наземным радиочастотам с использованием мультиплексов в формате DVB-T2.

Платное телевидение (ПТВ) – услуги связи для целей телевизионного вещания, поставщиком которых выступает оператор, предоставляющий возможность просмотра 40 и более телеканалов с использованием технологий аналогового и цифрового кабельного, IPTV, спутникового вещания.

Уровень развития услуги телевещания зависит от многих факторов: особенностей географии, экономики, демографии, мощности передатчиков эфирного вещания и распространения платного телевидения (ПТВ). Проникновение ПТВ в каждом конкретном городе зависит от особенностей городской инфраструктуры, застройки и реально располагаемых доходов населения. Плотно застроенные города характеризуются лучшим покрытием сетей кабельного телевидения, а в регионах с большим частным сектором преобладает спутниковое и эфирное ТВ. Экономическое положение в городе напрямую влияет на платежеспособный спрос населения на развлечения.

С учетом этого эксперты J'son & Partners для анализа влияния развития ЦЭТВ на рынок ПТВ разделили города России на два сегмента. К первому отнесены города с населением 100 000 и более жителей, где качество жизни населения держится на довольно высоком уровне, а услуги ПТВ пользуются большим спросом и имеют широкое распространение. Во второй сегмент входят города со средним и низким уровнем экономического развития и развитости услуг ПТВ.

Анализ данных, предоставленных ФГУП «РТРС» (Российская телевизионная и радиовещательная сеть), показал, что по состоянию на 3-й квартал 2015 года технический охват населения России ЦЭТВ первого мультиплекса составил 90 %. Цифровые телеканалы второго мультиплекса доступны 56,8 % населения страны.

ЦЭТВ распространено неравномерно – в Москве и Санкт-Петербурге технический охват составляет 100 %, тогда как, например, в Магнитогорске и Нижнекамске – 10–12 %. Стоит отметить, что технический охват не показывает фактических зрителей ЦЭТВ, а говорит лишь о возможности населения принимать цифровой сигнал.

Исходя из тенденций на рынке платного телевидения, а также региональных особенностей, в J'son & Partners Consulting определили степень влияния ЦЭТВ на развитие бизнеса операторов платного телевидения и оценили его использование населением городов.

В таких городах, как Казань, Оренбург, Тюмень, население активно пользуется услугой платного телевидения и готово регулярно за нее платить. Это позволяет говорить о минимальном возможном текущем и прогнозируемом (в перспективе 2-3 лет) количестве зрителей ЦЭТВ – не более 3 %.

С другой стороны, в городах с большим частным сектором, исторической неразвитостью ПТВ или низкой финансовой обеспеченностью жителей в перспективе 2-3 лет есть более высокий потенциал роста количества зрителей ЦЭТВ – до 15 % населения. Например, в Твери при относительно высоком уровне распространения ПТВ у населения низкие доходы, что может привести к оттоку абонентов в ЦЭТВ при увеличении знания о наличии в нем бесплатных качественных каналов.

Телевидение в России имеет собственную специфику, которая обусловлена особенностями заселения территории, ситуацией на рынке платного телевидения, сложившимися предпочтениями пользователей. Цифровое эфирное телевидение существует наравне с другими технологиями доставки ТВ-сигнала и, так или иначе, конкурирует за своих абонентов.

Результаты исследования представлены в полной версии отчета: «Развитие цифрового эфирного телевидения в России, 2015–2020 гг.»

Рынок оборудования и перспективы внедрения новых услуг на базе технологии IMS

J'son & Partners Management Consultancy

IMS (IP Multimedia Subsystem) – это стандартизированная архитектура, основанная на IP-протоколе, которая позволяет осуществить конвергенцию устройств фиксированной и мобильной связи, интегрировать различные виды сетей и мультимедиа-приложений.

J'son & Partners Consulting представляет краткие результаты исследования рынка IMS в России и в мире.

Ключевые вопросы исследования

В исследовании анализируются решения крупнейших вендоров, основные проекты внедрения в мире и пилотные проекты в России. Выделены основные глобальные и российские тенденции и прогнозы развития рынка IMS. Основное внимание уделено детальному анализу функционала различных решений, операторских кейсов и возможностей для внедрения операторами сервисов с добавленной стоимостью на основе IMS.

Практическая ценность исследования

• Проведен детальный анализ решений более чем 15 вендоров IMS.

• Проанализирована ситуация на рынке IMS, дана оценка рынка.

• Проанализированы основные проекты IMS в мире, а также состояние и перспективы внедрения этой технологии в России.

Целевая аудитория

Исследование предназначено операторам мобильной и фиксированной связи, производителям оборудования, системным интеграторам, венчурным и инвестиционным фондам, профильным стартапам и исследовательским агентствам.

Резюме исследования

В мире

Первые коммерческие IMS-сети стали появляться в 2004–2005 гг., однако до сих пор не получили массового распространения, несмотря на высокие ожидания. Одной из основных предпосылок для внедрения IMS в настоящее время является необходимость предоставления качественных голосовых услуг в сетях LTE, которые, несмотря на бурный рост в сегменте передачи данных, все еще приносят операторам основную часть доходов. Среди основных новых технологий, которые требуют внедрения, IMS-платформы претендуют на роль новых «генераторов» доходов от голосовых услуг – VoLTE и,в последнее время, VoWiFi (голос поверх Wi-Fi), а также «расширенные» услуги RCS.

Внедрение IMS в инфраструктуре оператора позволяет решить несколько задач продуктового маркетинга одновременно:

• IMS как сервисная платформа позволяет операторам расширить спектр предоставляемых услуг, обогащая пользовательский опыт абонентов и снижая их отток;

• функциональность услуг на базе IMS, описанных утвержденными стандартными спецификациями, успешно конкурирует с возможностями OTT-сервисов, а значит, позволяет оператору удержать свою абонентскую базу от миграции на OTT-сервисы;

• стандартизация услуг позволяет обеспечить возможность общения их пользователей с пользователями аналогичных услуг у других операторов, что повышает проникновение таких услуг в абонентскую базу.

Число коммерческих сетей VoLTE и абонентская база VoLTE в мире стабильно растут – 51 млн абонентов в конце 2014 г., по сравнению с 12 млн абонентов в 2013 г. и 300 тыс. в 2012 г. По прогнозам, абонентская база VoLTE в 2015 г. превысит 100 млн.

Одной из наиболее актуальных технологий является Voice over WiFi (VoWiFi), которую можно рассматривать как эффективный способ расширения покрытия и емкости сети мобильного оператора. Развертывание VoLTE на платформе IMS автоматически дает возможность оператору сотовой связи развернуть эту услугу и для предоставления поверх Wi-Fi.

На восходящий тренд роста проникновения таких услуг указывает поддержка VoWiFi в последнем релизе операционной системы iOS и запуск коммерческих сервисов VoWiFi на базе IMS несколькими операторами.

По прогнозам, доля универсальных операторов, которые к концу 2018 г. будут предлагать коммерческие сервисы VoWiFi, будет составлять в среднем около 70 %, среди мобильных операторов доля таких компаний составит около 53 %.

В России

В России внедрение IMS и соответствующих сервисов в коммерческую эксплуатацию дополнительно сдерживалось нерешенностью ключевых вопросов регулирования в этом сегменте. В этой связи все крупные российские операторы, протестировавшие платформы IMS/VoLTE, ждут положительного решения регулятора, после чего станет возможным внедрение новых технологий и услуг. Минкомсвязи требовалось обновить правила применения абонентского оборудования. Также для запуска VoLTE регулятору было необходимо внести изменения в правила присоединения сетей электросвязи и их взаимодействия, действующие с середины 2000-х гг.

Старые правила, например, запрещали завершение вызовов из сетей передачи данных на телефонную сеть. Одним из важных факторов в регулировании коммуникационных услуг являются требования СОРМ, предъявляемые к любым типам сетей.

В августе 2015 г. «ВымпелКом» и «МегаФон», получив необходимые разрешения от спецслужб, запустили VoLTE в тестовом режиме в Московском регионе. Операторы ожидают разрешительную документацию от Минкомсвязи, после чего будет полностью активизирован функционал сети, отвечающий за обеспечение работы VoLTE. МТС планирует запустить VoLTE до конца текущего года.

В Москве состоялся V Международный конгресс «ЭРА-ГЛОНАСС»

V Международный конгресс «ЭРА-ГЛОНАСС», который состоялся 1 октября в Москве, собрал в Москве более 700 ведущих участников рынка применения навигационно-информационных технологий на транспорте. Организатором мероприятия выступило Некоммерческое партнерство «ГЛОНАСС», федеральный сетевой оператор в сфере навигационной деятельности, единственный исполнитель работ по созданию и внедрению государственной автоматизированной системы экстренного реагирования при авариях «ЭРА-ГЛОНАСС». В Конгрессе приняли участие делегаты из России, стран ЕАЭС, БРИКС и Евро-пейского союза.

Работу Международного конгресса «ЭРА-ГЛОНАСС» открыл Заместитель Председателя Правительства Российской Федерации Дмитрий Рогозин. Он отметил, что «ЭРА-ГЛОНАСС» – это первый в мире государственный проект, в котором спутниковая навигация и возможности других современных технологий: микроэлектроники, сотовой связи и информационных сервисов используются в интересах безопасности людей на автомобильном транспорте. Следующим шагом развития и внедрения навигационных технологий в России должен стать поэтапный переход к рынку беспилотных автомобилей».

Отдельно Дмитрий Рогозин отметил важность импортозамещенияи использования отечественных продуктов и услуг в навигационной сфере:

«Задача перехода российской промышленности на отечественную компонентную базу, в том числе микроэлектронную, является одной из приоритетных. В октябре Президент России провел совещание по микроэлектронике и поручил Правительству Российской Федерации до конца года сформировать план действий и интегрированный государственный заказ на производство микро и радиоэлектроники на территории страны. «ЭРА-ГЛОНАСС» – один из двенадцати проек-тов, которые были выделены как приоритетные для развития применения российской микроэлектроники», – добавил он.

Вице-премьер вручил двум российским компаниям ОАО «АВТОВАЗ» и ООО «Форт-Телеком» первые сертификаты соответствия требованиям Технического регламента Таможенного союза «О безопасности колесных транспортных средств». Система «ЭРА-ГЛОНАСС», устанавливаемая серийно в автомобили Lada Vesta, и устройство вызова экстренных оперативных служб от «Форт-Телеком» первыми успешно прошли все необходимые испытания.

Помощник Президента Российской Федерации Игорь Левитин зачитал приветственное слово Руководителя администрации Президента Российской Федерации Иванова Сер-гея Борисовича. А в своем выступление Игорь Левитин подчеркнул, что за последние несколько лет российский автопарк качественно изменился, улучшились автодороги, но количество аварий и их тяжесть при этом не снизились. Использование технологических возможностей «ЭРА-ГЛОНАСС» и развитие этого инновационного направления будет способствовать профилактике аварийности, повышению уровня безопасности на транспорте, в первую очередь, перевозок детей и пассажирских перевозок.

Также Игорь Левитин добавил, что в целом расширение использования навигационных, информационных и телекоммуникационных технологий на автомобильном транспорте, развитие

технологий беспилотных транспортных средств ведет к революционным изменениям всего транспортного комплекса. «Это потребует от государства серьезного совершенствования законодательства и технического регулирования, разработки и внедрения новых стандартов строительства и эксплуатации автомобильных дорог и всей транспортной инфраструктуры. Мы должны быть к этому готовы, должны и здесь быть первыми в мире, как и в создании таких высокотехнологичных систем, как «ЭРА-ГЛОНАСС» – сказал он.

Заместитель Министра транспорта Российской Федерации Алексей Цыденов отметил, что спектр сервисов, которые могут быть реализованы с использованием инфраструктуры «ЭРА-ГЛОНАСС», очень широк. «С учетом многомиллионного числа автомобилей, которые уже в ближайшие 2-3 года будут оснащены устройствами «ЭРА-ГЛОНАСС», бизнесу следует уже сейчас выстраивать отношения с оператором системы – АО «ГЛОНАСС».

В рамках пленарной сессии перед делегатами Конгресса выступили Директор Департамента информационных технологий и связи Министерства здравоохранения Российской Федерации Елена Бойко, Начальник Управления информационных техно-

логий и связи МЧС России Сергей Власов, Генеральный директор АО «ГЛОНАСС» Андрей Недосеков, Президент Некоммерческого партнерства «ГЛОНАСС» Александр Гурко.

Александр Гурко, Президент НП ГЛОНАСС», отметил: «Мы видим новую миссию Партнёрства – стать эффективной площадкой для развития и внедрения навигационно-информационных технологий на транспорте за счет объединения усилий и ресурсов российских участников рынка и государства. Основные направления нашей работы: формирование нормативной базы и технической политики на национальном и межгосударственном уровне, взаимодействие с институтами развития, организация пилотных проектов, поддержка экспорта технологий ГЛОНАСС».

«В сфере наших интересов: сервисы для водителей, пассажиров, поддержка сервис- и контент-провайдеров, дизайн-центры оборудования, развитие в России технологий V2X и беспилотного транспорта. В этих целях отраслевое представительство в Партнерстве будет расширяться. К операторам связи и навигационным компаниям добавятся автопроизводители, российские компании, развивающие технологии беспилотного транспорта, навигационные компании из стран ЕАЭС и БРИКС», – добавил Александр Гурко.

В рамках Конгресса обсуждались направления развития системы «ЭРА-ГЛОНАСС» и возможности использования ее инфраструктуры в интересах операторов навигационно-информационных систем, сервис-провайдеров, автопроизводителей и страховых компаний. Среди важных вопросов – международное сотрудничество и кооперация в сфере создания и внедрения навигационно-информационных систем, перспективы использования навигационных, информационных и телекоммуникационных технологий на автомобильном транспорте.

85 лет со дня образования Санкт-Петербургского государственного университета телекоммуникаций имени профессора М.А. Бонч-Бруевича

Правительство Российской Федерации особое внимание уделяет сфере информационных технологий, достижения в области телекоммуникаций становятся доступны всё большему количеству граждан. Существующий рынок огромен и требует большего количества высококвалифицированных специалистов. Кроме того, столь стремительное развитие связи ставит перед профессионалами новые задачи.

Сохранение традиций пионеров отрасли и уверенное развитие новейших технологий – вот основные принципы Санкт-Петербургского государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича. 13 октября 2015 г. СПбГУТ, ведущий базовый вуз отрасли, празднует своё 85-летие. Это важное событие для Санкт-Петербурга и связистов всей страны.

История университета начинается с 1930 года – на базе Высших курсов связи было создано специальное высшее учебное заведение по радиотехнике и электросвязи. Чуть позже оно было переименовано в Ленинградский электротехнический институт связи (ЛЭИС). В 1994 году институт получил статус университета.

Вуз носит имя выдающегося радиотехника и блестящего учёного Михаила Александровича Бонч-Бруевича.

На сегодняшний день в СПбГУТ существует девять факультетов, включая факультет повышения квалификации и институт военного образования. Они охватывают широкий спектр научно-образовательных направлений как технических, так и гуманитарных, а также экономических. Существуют филиалы в Смоленске и Архангельске. В СПбГУТ функционируют научно-образовательные центры, научно-исследовательские лаборатории. В университете проходят обучение более 10 000 студентов по программам среднего профессионального и высшего профессионального образования.

«Бонч» – единственный в своем роде университет Северо-Запада, где студенты получают знания и практические навыки в области инфокоммуникаций технологий.

Университет широко известен и в международном научном сообществе. Ежегодно в СПбГУТ проходят различные конференции, форумы, круглые столы с участием российских и зарубежных деятелей. Возглавляет СПбГУТ ректор профессор Сергей Викторович Бачевский.

В Пермском крае обсудят будущее российской промышленности

ПЕРМСКИЙ ИНЖЕНЕРНО-ПРОМЫШЛЕННЫЙ ФОРУМ

Пермский инженерно-промышленный форум состоится 12-13 ноября 2015 года. Масштабное событие соберет руководство страны, представителей федеральных и региональных органов исполнительной власти субъектов Российской Федерации, руководителей крупнейших отечественных предприятий. Цель уникального мероприятия – обсудить пути развития российской промышленности ближайшего будущего, формирование инновационной экономики и подготовку профессиональных кадров для создания «новой экономики».

Организаторы форума получили предварительное согласие принять участие от полномочного представителя Президента в ПФО Михаила Бабича, министра энергетики Александра Новака, министра промышленности Дениса Мантурова, генерального директора федерального космического агентства «Роскосмос» Игоря Комарова и президента Торгово-промышленной палаты РФ Сергея Катырина.

«Сейчас мы можем смело говорить об эпохе новой индустриализации. Пермский край, как регион с серьезной промышленной традицией и большим опытом развития высокотехнологичных отраслей, в полной мере может считаться лидером экономического роста страны. Практические наработки пермских предприятий адаптированы к внедрению и в других регионах. Поэтому второй год подряд столь масштабный форум проходит именно у нас», – говорит губернатор Пермского края Виктор Басаргин.

В рамках форума будут созданы отраслевые площадки, где обсудят оптимизацию технологических процессов. Площадки представят предприятия оборонно-промышленного комплекса Пермского края: ОАО «Мотовилихинские заводы», «Авиадвигатель», «Пермский моторный завод», «Протон-ПМ», НПО «Искра», «Редуктор-ПМ», «Метафракс», «Уралкалий», «Пермская научно-производственная приборостроительная компания» и другие.

В период проведения инженерно-промышленного форума пройдет первый Съезд членов Пермской торгово-промышленной палаты. На мероприятии будет подписано соглашение между ТПП РФ и Пермским краем, которое определит приоритетные направления деятельности на 2016-2017 гг.

13 ноября компания «Уралхим» в рамках конференции «Кадры для Верхнекамской агломерации» представит практику грамотного использования людских ресурсов.

Программу мероприятия наполнит как деловая часть с дискуссиями, круглыми столами, семинарами и конференциями, так и зрелищная часть – полномасштабная битва роботов в соответствии с международным регламентом Battlebots; осмотр экспозиции предприятий Пермского края; финал конкурса по разработке социально-ориентированных приложений на базе открытых данных «Открытый регион. Хакатон».

Пермский инженерно-промышленный форум, организованный Правительством Пермского края при поддержке промышленных предприятий региона, состоится в регионе второй раз. Прошлогодний форум собрал более 4000 участников.

Пресс-центр Пермского инженерно-промышленного форума
Юлия Солдатенко
press@engineerforum.ru

10 инженерных стартапов будут представлены на суд экспертов «Сколково» на форуме в Перми

12 ноября 2015 года, в рамках Пермского инженерно-промышленного форума состоится питч сессия инновационных инженерных стартапов. 10 инженерных стартапов будут представлены на суд экспертов «Сколково». У участников будет всего 90 секунд на то, чтобы убедить представителей фонда и потенциальных инвесторов в практической значимости своих разработок. Инженеры расскажут об уникальности своих замыслов, озвучат потребности в инвестициях, кадрах и партнерах. После презентации мнение о проектах и готовность их поддержать озвучат представители «Российской венчурной компании», инвестиционных фондов и промышленных предприятий.

«Инновационные проекты крайне важны для российской экономики: это и развитие наукоемких технологий, и формирование новых рабочих мест, и инвестиционная привлекательность регионов, – говорит губернатор Пермского края Виктор Басаргин. –Мы уверены, что площадка, которую предоставляет Пермский инженерно-промышленный форум, поможет инноваторам найти и привлечь инвесторов. Реализация подобных проектов положительно скажется на развитии промышленной отрасли страны в целом».

На площадке выступят 10 разработчиков из Москвы, Рязани, Краснодара, Перми, Красноярска.

Среди проектов, которые оценят эксперты, например:

- Промышленные транспортировочные роботы – специальная платформа, автономно осуществляющая перевозку деталей по производственной линии.
- Специальные робототехнические системы, способные передвигаться по сильно пересеченной местности и преодолевать препятствия непредсказуемой конфигурации в условиях катастроф техногенного, военного или природного характера и другие проекты.

Школа мобильной связи «Russian Mobile School 2015»

RMS
Russian Mobile School

С 14 по 17 октября в Санкт-Петербурге во второй раз открыла свои двери школа мобильной связи Russian Mobile School. Мероприятие прошло в Санкт-Петербургском университете телекоммуникаций им. проф. М.А.Бонч-Бруевича (СПбГУТ).

Russian Mobile School — это первая в России школа мобильной связи. Каждый желающий смог пройти цикл лекций, посетить выставки и мастер-классы, на которых профессионалы поделятся своими знаниями и опытом. Главная задача Школы — показать завтрашним выпускникам отрасль изнутри, действительно помочь им сориентироваться в будущей профессии и найти контакты с работодателями. Это проект Романа Андреева (выпускник СПбГУТ, эксперт в области мобильной связи) и Владимира Лаврухина (Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича).

Школа также представила участникам возможность «потрогать руками» реальное оборудование, используемое операторами мобильной связи. Зрителям была продемонстрирована работа различных программных, аппаратных и измерительных средств. Кроме того, на мероприятии осуществлен тестовый запуск собственной 3G сети.

Среди гостей мероприятия были: Тигран Карленович Погосян (старший вице-президент ZTE, бывший заместитель генерального директора по стратегическим проектам «Мегафон»), Валерий Олегович Тихвинский (Заместитель генерального директора ООО «АйКомИнвест» по инновационным технологиям) и другие известные представители из отрасли мобильной связи.

«Нам удалось найти тот формат, которого так не хватает многим учебным заведениям. Во-первых, мы приглашаем выступать только профессионалов и практиков. Во-вторых, мы проводим демонстрации решений и оборудования в формате мастер-классов. Это резко отличает нас от других профессиональных мероприятий, где демонстрации продуктов, зачастую, проводят люди, основная задача которых продать свои решения, а не показать как они работают», — говорит, один из основателей проекта.

Три первых дня Школы были посвящены техническим аспектам работы мобильных сетей. А заключительный день раскрыл секреты трудовых будней в компаниях отрасли мобильной связи.

фото: Светлана Маханькова

О НЕКОТОРЫХ АСПЕКТАХ ПРИМЕНЕНИЯ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ ПРИ ОБОСНОВАНИИ ПЕРЕЧНЯ ХАРАКТЕРИСТИК ИЗДЕЛИЯ, КОНТРОЛИРУЕМЫХ В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ

Новиков
Александр Николаевич,
к.т.н., доцент кафедры
Военно-космической
академии имени А.Ф.Можайского,
г. Санкт-Петербург, Россия,
novalloll@mail.ru

Ключевые слова:
некогерентный оптический излучатель, оптимальный оптический прием, оптимальные оптические цифровые сигналы, синтез оптического приемника, фотоны и фотоэлектроны, минимизация средней вероятности ошибки приема.

АННОТАЦИЯ

В условиях поэтапной модернизации объектов наземной космической инфраструктуры, особое внимание следует уделить совершенствованию измерительных систем и комплексов, применяемых для метрологического обслуживания такого рода изделий. При этом, отсутствие полноценной информации о степени реализуемости режимов и условий проведения контроля параметров и характеристик изделий создает предпосылки для поиска оригинальных подходов в решении оптимизационных задач обоснования перечня измеряемых (контролируемых) параметров изделий.

Представлены результаты исследований особенностей применения методов целочисленной многокритериальной оптимизации при обосновании перечня параметров и характеристик изделия, контролируемых в процессе эксплуатации с использованием нечетких исходных данных о режимах и условиях проведения контроля, а именно, особенностей ранжирования альтернатив с учётом возможных вариантов сочетания различных типов оценок, представленных в детерминированной, стохастической, либо нечёткой формах. Основное внимание уделяется разработке уточняющих положений, касающихся применения метода ранжирования по максимальному удалению с использованием формализованных в нечетком виде исходных данных, позволяющих исключить допущения, обязательные в случае применения традиционных методов ранжирования недоминируемых альтернатив о том, что частные показатели оценивания альтернатив независимы, насколько неравноценны, настолько и несоизмеримы по важности, об аддитивности частных показателей, о неизменности выполнения принципа транзитивности при ранжировании альтернатив. Показано, что применение аппарата теории нечетких множеств существенно дополняет методологию решения задач целочисленной многокритериальной оптимизации. Ряд переменных, отражающих влияние внешних факторов (условий) проведения измерений (контроля) при оценивании показателя результативности контроля параметров изделия, а также компонент затрат на контроль при оценивании показателя экономичности (ресурсоемкости) может на этапе анализа вариантов формирования рационального перечня измеряемых (контролируемых) в процессе эксплуатации параметров изделия оценён лишь приблизительно, с указанием примерного интервала возможных значений и ожидаемого распределения на этом интервале. В такой ситуации нечёткие оценки являются единственно корректной формой отражения реальной неопределённости оценивания значений частных показателей предпочтительности альтернатив (комбинации характеристик).

Согласно основным нормативным документам одной из важных задач на этапе исследований и обоснования разработки сложных технических систем является определение номенклатуры и нормирование параметров изделия, требований к погрешности их измерений (достоверности контроля), а также определение номенклатуры параметров, контролируемых в процессе эксплуатации.

В условиях постоянного роста требований к повышению точности, оперативности, снижению ресурсоемкости измерительных систем и комплексов, применяемых для метрологического обслуживания такого рода изделий, а также отсутствия полноценной апостериорной информации о степени реализуемости режимов и условий проведения контроля параметров и характеристик изделий (особенно, вновь разрабатываемых), возникает необходимость в поиске оригинальных подходов в решении оптимизационных задач обоснования перечня измеряемых (контролируемых) параметров изделий, связанных с применением теории нечетких множеств.

При этом, применимость большинства традиционно используемых методов ранжирования недоминируемых альтернатив, таких как метод лексикографического упорядочения, методы упорядочения с обобщённым критерием, методы упорядочения без обобщённого критерия, исследованных например, в работах [1,2,3] зачастую ограничена предположениями (допущениями) о том, что частные показатели оценивания альтернатив независимы, насколько неравноценны, настолько и несоизмеримы по важности. Кроме того, не всегда обоснованным представляется применение в этих задачах принципа аддитивности частных показателей, так как при его использовании возможна ситуация, что будет признана лучшей альтернатива, набравшая большее суммарное число «баллов» за счёт суммы не самых важных, но многочисленных частных показателей. Не исключена при этом и возможность получения вариантов упорядочений с нарушением принципа транзитивности при ранжировании альтернатив, т.е. может быть, что $a_i \phi a_j$, $a_j \phi a_k$ и $a_k \phi a_i$.

Исходя из этого, рассмотрим альтернативный метод обоснования рационального перечня измеряемых (контролируемых) в процессе эксплуатации параметров изделия, основанный на решении оптимизационных задач.

Пусть для каждого частного показателя K_v можно указать пороговое значение L_v такое, что альтернативы, оценки которых по показателю K_v ниже, чем L_v, крайне нежелательны. Более предпочтительными считаются альтернативы, оценки которых по частным показателям как можно дальше отстоят от критических значений Lv. Исходя из сущности подхода к ранжированию, данный метод можно назвать методом ранжирования по максимальному удалению от критических значений частных показателей или, сокращённо, методом ранжирования по максимальному удалению (РМУ).

Представим математическую модель, лежащую в основе метода РМУ, в формализованном виде следующим образом.

Пусть альтернативы $A = \{a_1,...,a_n\}$ оцениваются по s частным критериям $K_1,...,K_s$ и $X_{i<s>} = (x_{i1},...,x_{is})$ – вектор оценок альтернативы a_i, $i \in \{1,...,n\}$. Альтернативу a_i будем считать более предпочтительной, чем a_j, если

$$\min\{x_{i1}–L_1,..., x_{is}–L_s\} > \min\{x_{j1}–L_1,..., x_{js}–L_s\}.$$

Тогда выбор наилучшей альтернативы a^* осуществляется как решение задачи

$$a^* = \arg\max_{a_i \in A}\left[\min_{v\in\{1,...,s\}}\{(x_{iv} - L_v)\}\right]. \qquad (1)$$

В работе [4] показано, что задача (1) может быть решена как задача линейного программирования

$$z_{iv} \to \max_{\substack{i\in\{1,...,n\}\\ v\in\{1,...,s\}}} \qquad (2)$$

при ограничениях $x_{iv} – L_v – z_{iv} \geq 0$, $v \in \{1,...,s\}$, $a_i \in$ A.

При небольшом числе альтернатив задача может быть решена непосредственным расчётом значений $\min_v(x_{iv}–L_v)$ и выбором альтернативы с максимальным значением данного критерия.

Обобщим правило (1) на случай, когда частные показатели K_v, $v\in\{1,...,s\}$ различны по важности. В данной постановке это означает, что удаление оценок альтернатив от критических значений по одним частным показателям важнее, чем по другим. Например, для одной группы параметров (характеристик) изделия важнее обеспечить более высокие значения показателей результативности контроля (снижение неопределенности знаний о текущем (перспективном) техническом (функциональном) состоянии по сравнению с показателями оперативности и экономичности (ресурсоемкости) контроля. В то время как для другой важнее обеспечить более высокие значения показателей оперативной готовности и эксплуатационной экономичности по сравнению с требованиями к точности и информативности контроля (достаточными для принятия обоснованного решения только о текущем состоянии изделия (годен/не годен)).

Допустим, что определены значения весовых коэффициентов $\alpha_1,...,\alpha_s$, характеризующих важность удаления оценки альтернативы по каждому из частных показателей. Тогда задача (1) может быть записана в виде:

$$a^* = \arg\max_{a_i \in A}\left[\min_{v\in\{1,...,s\}}\{\alpha_v(x_{iv} - L_v)\}\right]. \qquad (3)$$

Соответственно, задача линейного программирования (2) принимает вид:

$$\sum_{v=1}^{s}\alpha_v z_{iv} \to \max_{i\in\{1,...,n\}} \qquad (4)$$

при ограничениях $x_{iv} – L_v – z_{iv} \geq 0$, $v \in \{1,...,s\}$, $a_i \in A$.

Или, введя функцию $\Phi(a_i) = \sum_{v=1}^{s}\alpha_v z_{iv}$, можно записать:

$$a^* = \arg\max_{a_i \in A} \Phi(a_i) \qquad (5)$$

$$x_{iv} - L_v - z_{iv} \geq 0,\ v \in \{1,...,s\}.$$

Анализ составляющих выражения (5) позволяет выделить следующие аспекты, подлежащие уточнённому исследованию:

1. Выбор способа оценивания значений коэффициентов важности частных показателей α_v, $v \in \{1,...,s\}$.

2. Анализ возможных способов формирования оценок x_{iv}, $i \in \{1,...,n\}$, $v \in \{1,...,s\}$ частных показателей.

3. Исследование способов преобразования частных показателей K_v, $v \in \{1,...,s\}$ к однородным.

4. Анализ способов задания критических значений L_v, $v \in \{1,...,s\}$ частных показателей.

5. Исследование особенностей ранжирования альтернатив с учётом возможных вариантов сочетания различных типов оценок составляющих данного выражения.

В случае если заранее можно строго проранжировать частные показатели по важности, то можно воспользоваться следующим способом оценивания значений коэффициентов α_v.

Пусть частные показатели K_v, $v \in \{1,...,s\}$ представлены в проранжированном виде множеством $K^r_{\{s\}} = \{K^r_1,...,K^r_s\}$. Тогда можно сформировать соответствующее упорядоченное множество из коэффициентов важности $\alpha^r_{\{s\}} = \{\alpha_1,...,\alpha_s\}$.

Допустим, что определены значения коэффициентов сравнительной предпочтительности ρ_{ij} между соседними коэффициентами важности α_i и α_j в упорядоченном множестве $\alpha_{\{s\}}$, такие что $\rho_{ij} = \frac{\alpha_i}{\alpha_j}$, $j = i+1$; $i,j \in (1,...,s\}$.

С учётом этого можно составить следующую систему из $(s+1)$ уравнений с s неизвестными α_i:

$$\begin{cases} \alpha_1 = \rho_{12}\alpha_2, \\ \alpha_2 = \rho_{23}\alpha_3, \\ \quad\vdots \\ \alpha_{s-1} = \rho_{(s-1)s}\alpha_s, \ , \\ \sum\limits_{v=1}^{s} \alpha_v = 1. \end{cases} \qquad (6)$$

Решая (6), имеем:

$$\begin{aligned} &\alpha_s = \left(1 + \rho_{(s-1)s} + ... + \prod_{i=2}^{s-1}\rho_{i(i+1)} + \prod_{i=1}^{s-1}\rho_{i(i+1)}\right)^{-1} = M_s, \\ &\alpha_{s-1} = \rho_{(s-1)s}M_s, \\ &\alpha_{s-2} = \rho_{(s-2)(s-1)}\rho_{(s-1)s}M_s, \\ &\vdots \\ &\alpha_j = \prod_{i=j+1}^{s}\rho_{(i-1)i}M_s, \\ &\vdots \\ &\alpha_1 = \prod_{i=2}^{s}\rho_{(i-1)i}M_s. \end{aligned} \qquad (7)$$

Если при строгом ранжировании частных показателей K_v по важности возникают затруднения, то можно воспользоваться методом, описанным в работе [5]. При этом предполагаются известными значения, принимаемые каждой из n альтернатив по всем частным показателям K_v, $v=\overline{1,s}$, т.е. векторы $X_i = (x_{i1},...,x_{is})$, $i \in \{1,...,n\}$. Кроме того, есть информация о парных сравнениях альтернатив, т.е. для каждой пары альтернатив α_i, α_j известна более предпочтительная.

Тогда, задача отыскания весовых коэффициентов $\alpha_v \geq 0$ формулируется как

$$\sum_{ij \in I} Y_{ij} \to \min \qquad (8)$$

при ограничениях

$$\sum_{v=1}^{s}(x_{iv} - x_{jv})\alpha_v + Y_{ij} \geq 0,$$

$$\sum_{v=1}^{s}\alpha_v = 1, \alpha_v \geq 0,\ Y_{ij} \geq 0,$$

где I – есть множество всех пар индексов i,j, для которых $a_i \phi a_j$.

Данная задача относится к классу задач линейного программирования и при сравнительно небольшом числе альтернатив может эффективно решаться с помощью ЭВМ.

Анализ возможных способов формирования оценок x_{iv}, $i \in \{1,...,n\}$, $v \in \{1,...,s\}$ частных показателей показывает, что в зависимости от количества исходных данных, доступности источников информации, способов получения информации и природы частных показателей K_v оценки x_{iv} могут быть представлены в детерминированной, стохастической, либо нечёткой формах. Детерминированные и стохастические оценки с точки зрения формы представления выражаются в виде точечных, либо интервальных величин. Нечёткие же оценки представляют собой нечёткие множества $\underset{\sim}{x}_{iv}$, определённые на множествах значений частных показателей с помощью так называемых функций принадлежности μ_{iv} в виде:

$$\underset{\sim}{x}_{iv} = \{< x_{iv}, \mu_{iv} >\},\ \mu_{iv} : X_{iv} \to [0;1]. \qquad (9)$$

Нечёткие оценки в ряде случаев являются единственно корректной формой отражения реальной неопределённости оценивания значений частных показателей. В частности, ряд переменных, отражающих влияние внешних факторов (условий) проведения измерений (контроля) при оценивании показателя результативности контроля параметров изделия, а также компонент затрат на контроль при оценивании показателя экономичности (ресурсоемкости) может на этапе анализа вариантов формирования рационального перечня измеряемых (контролируемых) в процессе эксплуатации параметров изделия оценён лишь приблизительно, с указанием примерного интервала возможных значений и ожидаемого распределения на этом интервале.

Как уже было сказано выше, в общем случае частные показатели являются неоднородными, так как измеряют интенсивность свойств различной физической

природы. В этом случае они нуждаются в преобразовании к однородным. Рекомендации, приведенные в работе [6] справедливы для случая, когда частные показатели таковы, что более предпочтительной альтернативе соответствует большее значение показателя. В противном случае преобразование показателей в однородные следует осуществлять с помощью выражений:

$$x'_{iv} = \frac{\overline{x}_v - x_{iv}}{\overline{x}_v} = 1 - \frac{x_{iv}}{\overline{x}_v} \quad , \qquad (10)$$

$$x'_{iv} = \frac{\overline{x}_v - \underline{x}_v - \overline{x_{iv}} + \underline{x_{iv}}}{\overline{x}_v - \underline{x}_v} = 1 - \frac{\overline{x_{iv}} - \underline{x_{iv}}}{\overline{x}_v - \underline{x}_v} \text{ , } v \in \{1,...,s\}. \qquad (11)$$

В большинстве практических случаев измерения значений частных показателей производятся в шкалах отношений, когда преобразования показателей к однородному виду требует знания точечных оценок $\overline{x}_v$. Однако, для некоторых частных показателей, не измеряемых в шкале [0;1], таких, например, как трудоемкость, стоимость, технологическая сложность процедуры контроля, и т.п., трудно задать однозначное значение максимально возможной оценки показателя. В то же время можно указать приближённо область значений, которой $\overline{x}_v$ принадлежит с большей или меньшей уверенностью. В этих случаях целесообразно оценивать в виде нечёткой величины:

$$\underset{\sim}{\overline{x}}_v = \{< \overline{x}_v, \mu_v(\overline{x}_v) >\} \quad , \qquad (12)$$

где $\mu(\overline{x}_v)$ есть функция принадлежности нечёткого множества максимально возможных значений оценки показателя K_v.

С учётом этого обстоятельства преобразование $\overline{x}_{iv}$ к однородному виду производится по формулам:

$$\underset{\sim}{x}'_{iv} = x_{iv} / \underset{\sim}{\overline{x}}_v = \{< x'_{iv}, \mu(x'_{iv}) >\} \quad , \qquad (13)$$

где $x'_{iv} = x_{iv} / \overline{x}_v, \mu(x'_{iv}) = \mu(\overline{x}_v)$;

$$\underset{\sim}{x}'_{iv} = (\overline{x}_{iv} - \underline{x}_{iv}) / (\underset{\sim}{\overline{x}}_v - \underline{x}_v) = \{< x'_{iv}, \mu(x'_{iv}) >\} , \qquad (14)$$

где $x'_{iv} = (\overline{x}_{iv} - \underline{x}_{iv}) / (\overline{x}_v - \underline{x}_v), \mu(x'_{iv}) = \mu(\overline{x}_v)$;

$$\underset{\sim}{x}'_{iv} = 1 - (x_{iv} / \underset{\sim}{\overline{x}}_v) = \{< x'_{iv}, \mu(x'_{iv}) >\} , \qquad (15)$$

где $x'_{iv} = 1 - (x_{iv} / \overline{x}_v), \mu(x'_{iv}) = \mu(\overline{x}_v)$;

$$\underset{\sim}{x}'_{iv} = 1 - [(\overline{x}_{iv} - \underline{x}_{iv}) / (\underset{\sim}{\overline{x}}_v - \underline{x}_v)] = \{< x'_{iv}, \mu(x'_{iv}) >\} , \qquad (16)$$

где $x'_{iv} = 1 - [(\overline{x}_{iv} - \underline{x}_{iv}) / (\overline{x}_v - \underline{x}_v)], \mu(x'_{iv}) = \mu(\overline{x}_v)$.

Примечание. Выражения (10) и (11) получены в предположении, что минимально возможная оценка $\underline{x}_v$ по *v*-му показателю задана в чётком виде (обычно $\underline{x}_v = 0$).

В формулах (10) и (11) не учитывается возможность приближённого оценивания самих значений показателей K_v. Однако, как было сказано выше (9), такие ситуации могут вполне встречаться на практике. Поэтому, обобщим выражения (12) и (13), представив их с учётом нечёткого оценивания значений частного показателя K_v:

$$\underset{\sim}{x}_{iv} = \{< x_v, \mu(x_{iv}) >\}.$$

Имеем:

$$\underset{\sim}{x}'_{iv} = \underset{\sim}{x}_{iv} / \underset{\sim}{\overline{x}}_v = \{< x'_{iv}, \mu(x'_{iv}) >\} , \qquad (17)$$

где $x'_{iv} = x_{iv} / \overline{x}_v, \mu(x'_{iv}) = \sup\limits_{\forall x'_{iv} | x_{iv} / \overline{x}_v = x'_{iv}} \min [\mu(x_{iv}), \mu(\overline{x}_v)]$;

либо

$$\underset{\sim}{x}'_{iv} = 1 - (\underset{\sim}{x}_v / \underset{\sim}{\overline{x}}_v) = \{< x'_{iv}, \mu(x'_{iv}) >\}, \qquad (18)$$

где $x'_{iv} = 1 - (x_{iv} / \overline{x}_v), \mu(x'_{iv}) = \sup\limits_{x'_{iv} | 1 - (x_{iv} / \overline{x}_v) = x'_{iv}} \min [\mu(x_{iv}), \mu(\overline{x}_v)]$.

Выражения для функций принадлежности $\mu(x'_v)$ в формулах (17) и (18) получены с помощью принципа обобщения Л. Заде [7].

Анализ способов задания критических значений L_v, $v \in \{1,...,s\}$ частных показателей также показал, что наиболее корректно оценивать их значения в виде нечётких величин:

$$\underset{\sim}{L}_v = \{< L_v, \mu(L_v) >\} \quad . \qquad (19)$$

Необходимо учитывать, что при работе с неоднородными показателями их критические значения также должны быть подвергнуты преобразованию к значению в однородной шкале:

$$\underset{\sim}{L}'_v = \underset{\sim}{L}_v / \underset{\sim}{\overline{x}}_v = \{< L'_v, \mu(L'_v) >\} \quad , \qquad (20)$$

где $L'_v = L_v / \overline{x}_v, \mu(L'_v) = \sup\limits_{x_v | L_v / \overline{x}_v = x_v} \min [\mu(L_v), \mu(\overline{x}_v)]$;

либо

$$\underset{\sim}{L}'_v = 1 - (\underset{\sim}{L}_v / \underset{\sim}{\overline{x}}_v) = \{< L'_v, \mu(L'_v) >\} , \qquad (21)$$

где $L'_v = 1 - (L_v / \overline{x}_v), \mu(L'_v) = \sup\limits_{x_v | 1 - (L_v / \overline{x}_v) = x_v} [\mu(L_v), \mu(\overline{x}_v)]$.

Сущность преобразования x_v и L_v к однородной шкале показана на рис. 1.

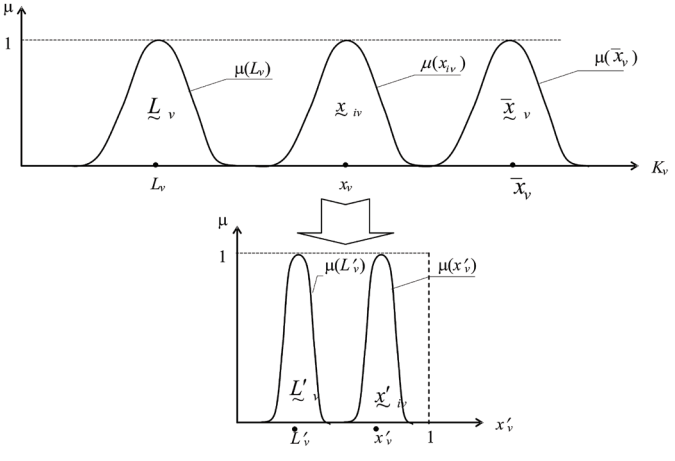

Рис. 1. Преобразование частного показателя к однородному виду

После того, как рассмотрены основные особенности оценивания частных показателей, их критических значений и способы преобразования шкал отношений к однородному виду, исследуем особенности ранжирования альтернатив по правилу (22).

С учётом проведённого анализа в наиболее общей постановке задача выбора наилучшей альтернативы описывается выражением:

$$a^* = \arg\max_{a_i \in A}[\min_{v\in\{1,\dots,s\}}\{\alpha_v(\underset{\sim}{x}'_{iv} - \underset{\sim}{L}'_v)\}], \qquad (22)$$

где $\underset{\sim}{K}'_{iv}$ есть результат приближённого оценивания i-й альтернативы по v-му частному показателю, преобразованному к однородному виду.

Очевидно, что результатом преобразования α_v $(\underset{\sim}{x}'_{iv} - \underset{\sim}{L}'_v)$ будет нечёткое множество $\underset{\sim}{\Delta}_{iv}$ взвешенного нормированного расстояния (удаления) оценки i-й альтернативы по v-му частному показателю от критического значения:

$$\underset{\sim}{\Delta}_{iv} = \{< \delta_{iv}, \mu(\delta_{iv}) >\}, \qquad (23)$$

где $\delta_{iv} = \alpha_v(x'_{iv} - L'_v) = \alpha_v(x_{iv}/\bar{x}_v - L_v/\bar{x}_v)$, либо $\delta_{iv} = (L_v/\bar{x}_v - x_{iv}/\bar{x}_v)$ – в случае, когда лучшей альтернативе соответствует меньшее значение показателя. Функция принадлежности $\mu(\delta_{iv})$ соответственно оценивается выражениями:

$$\mu(\delta_{iv}) = \sup_{\delta_{iv}\left|\alpha_v\left(\frac{x_{iv}}{\bar{x}_v} - \frac{L_v}{\bar{x}_v}\right)=\delta_{iv}\right.} \min \; [\mu(x'_{iv}), \mu(L'_v)], \qquad (24)$$

либо

$$\mu(\delta_v) = \sup_{\delta_{iv}\left|\alpha_v\left(\frac{L_v}{\bar{x}_v} - \frac{x_{iv}}{\bar{x}_v}\right)=\delta_{iv}\right.} \min \; [\mu(x'_{iv}), \mu(L'_v)]. \qquad (25)$$

С учётом (24) задача (25) может быть записана в виде:

$$a^* = \arg\max_{a_i \in A}[\min_{v\in\{1,\dots,s\}} \underset{\sim}{\Delta}_{iv}]. \qquad (26)$$

Таким образом, задача выбора рационального варианта сводится к задаче поиска минимальной нечёткой оценки удаления каждой альтернативы от критического значения по всем частным показателям и, затем, выбора среди таких альтернатив наилучшей по максимальному удалению.

Для ранжирования нечётких множеств можно воспользоваться одним из известных методов, описанных в литературе, например, методом сравнения нечётких подмножеств единичного интервала [8]. Согласно этому методу сравнение нечётких множеств может производиться на основе так называемой функции упорядоченности, представляющей собой скалярное число из единичного интервала.

Пусть A – нечёткое подмножество единичного интервала $\underset{\sim}{A} = \{< x, \mu_{\underset{\sim}{A}}(x) >\}$, x ∈ [0;1].

Определим уровневое множество как

$$A_\alpha = \{x \mid \mu_{\underset{\sim}{A}}(x)\} \geq \alpha \;,$$

где α есть некоторый заданный уровень, 0<α≤1. Пусть $a(\alpha)$ и $b(\alpha)$ есть соответственно левая и правая границы множества A_α. Определим функцию $M(\alpha)$ как среднюю величину интервала $[a(\alpha), b(\alpha)]$, т.е.

$$M(\alpha) = \frac{a(\alpha) + b(\alpha)}{2} \;.$$

Тогда, функция упорядоченности $F(\underset{\sim}{A})$ может быть рассчитана как

$$F(\underset{\sim}{A}) = \frac{\int_0^{\alpha_{max}} M(\alpha)d\alpha}{J} \;. \qquad (27)$$

где $J = 1/d\alpha$.

При практических расчётах задаются некоторым интервалом дискретизации $d\alpha$ множества значений α, так что оно разбивается на конечное число непересекающихся интервалов: $0 < \alpha \leq d\alpha$, $d\alpha < \alpha \leq 2\,d\alpha$,…, $1 - d\alpha < \alpha \leq 1$.

Для каждого j-го интервала находится значение $M_j(\alpha)$, затем рассчитывается приближённое значение $F(\underset{\sim}{A})$:

$$F(\underset{\sim}{A}) \approx \frac{\sum_{j=1}^{J} M_j(\alpha)}{J} \;. \qquad (28)$$

Таким образом, по функции упорядоченности можно проранжировать нечёткие множества $\underset{\sim}{\Delta}_{iv}$ и $\underset{\sim}{\Delta}_{i\,min}$, что позволяет выбрать наиболее предпочтительную альтернативу a^*, то есть определить номенклатуру параметров, контролируемых в процессе эксплуатации.

Литература

1. Кини Р., Райфа Х. Принятие решений при многих критериях: предпочтения и замещения. М.: Радио и связь. 1981. 560 с.

2. Айзерман М.А., Алескеров Ф.Т. Выбор вариантов: основы теории. М.: Наука. 1990. 240 с.

3. Vincke Ph. Outranking approacha. In: T. Gal, T. Stewart, T. Hanne (Eds.) Multicriteria Decision Making: Advances in MCDM models, algorithms, theory and applications, Kluwer. Boston : Academic Publishers. 1999.

4. Сигал И.Х., Иванова А.П. Введение в прикладное дискретное программирование: модели и вычислительные алгоритмы. М.: ФИЗМАТЛИТ. 2002. 240 с.

5. Hokkannen J., Salminen P. ELECTRE Ш and IV Decision Aids in an Environmental Problem // J. of Multi-Criteria Decision Analysis. 1997. Vol. 6.

6. Обработка нечеткой информации в системах принятия решений / А.Н. Борисов, А.В. Алексеев, Г.В. Меркурьева и др. М.: Радио и связь. 1989.

7. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений. М.: Мир. 1976.

8. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей: примеры использования. Рига: Зинатне. 1990. 184 с.

Для цитирования:
Новиков А.Н. О некоторых аспектах применения теории нечетких множеств при обосновании перечня характеристик изделия, контролируемых в процессе эксплуатации // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 12–17.

ON SOME ASPECTS OF APPLYING FUZZY SET THEORY IN SUBSTANTIATING THE LIST OF CHARACTERISTICS OF PRODUCTS CONTROLLED DURING OPERATION

Novikov Alexandr Nikolaevic,
St. Petersburg, Russian, novalloll@mail.ru

Abstract
In the context of a phased modernization of ground infrastructure, special attention should be paid to improving measuring systems and complexes used for the metrological service of such products. At the same time, the lack of full information on the degree of marketability modes and conditions of the control parameters and characteristics of products creates the preconditions for the search of original approaches to solving optimization problems justify the list of measured (controlled) parameters of products. It is presents the results of studies of the application of methods of integral multi-criteria optimization when justifying the list of parameters and characteristics of the product controlled during operation using fuzzy initial data on the conditions and modalities of control, namely the characteristics of the ranking of alternatives taking into account the options for combining different types of evaluations presented in a deterministic, stochastic, or fuzzy forms. The focus is on the development of clarifying the provisions relating to the application of the method of ranking for maximum removal using a formalized in a fuzzy form of raw data to eliminate assumptions required in the case of traditional methods of ranking non-dominated alternatives that private performance evaluation of alternatives are independent, how uneven, so and incommensurable in importance, an additive partial indicators of the continuing implementation of the principle of transitivity in ranking alternatives. It is shown that the application of the theory of fuzzy sets substantially complementary methodology solving the integer multicriterial optimization. A number of variables reflecting the impact of external factors (conditions) measurements (monitoring) when evaluating the performance indicator monitoring parameters of the product, and component inspection costs when evaluating the indicator efficiency (resource consumption) may be at a stage of analysis of options for the formation of a rational list of the measured (controlled) process Operating parameters of the product rated only approximately, with an indication of the approximate range of possible values and the expected distribution in this interval. In this situation, fuzzy evaluations are the only correct form of reflection of real uncertainty estimation values of particular indices of preference alternatives (combinations of characteristics).
Keywords: ranking techniques, fuzzy evaluation, selection of monitored parameters, performance evaluation of alternatives, methods of integral multi-criteria optimization.

References
1. Keeney R., Rife H. Prinyatie resheniy pri mnogikh kriteriyakh: predpochteniya i zameshcheniya. [Decisions multi-criteria: preferences and substitution]. Moscow: Radio i svyaz', 1981. 560 p. (In Russian).
2. Ayzerman M.A., Aleskerov F.T. Vybor variantov: osnovy teorii [The choice of options: the basic theory]. Moscow: Nauka, 1990. 240 p. (In Russian).
3. Vincke Ph. Outranking approacha. In: Gal T., Stewart T., Hanne T. (Eds.) Multicriteria Decision Making: Advances in MCDM models, algorithms, theory and applications, Kluwer. Boston: Academic Publishers, 1999.
4. Segal I.H., Ivanova A.P. Vvedenie v prikladnoe diskretnoe programmirovanie: modeli i vychislitel'nye algoritmy [Introduction to Applied Discrete programming: models and computational algorithms]. Moscow: FIZMATLIT, 2002. 240 p. (In Russian).
5. Hokkannen J., Salminen P. ELECTRE III and IV Decision Aids in an Environmental Problem // J. of Multi-Criteria Decision Analysis. 1997. Vol. 6.
6. Borisov A.N., Alekseev A.V., Merkureva G.V. et al. Obrabotka nechetkoy informatsii v sistemakh prinyatiya resheniy [Processing of fuzzy information in the decision-making systems]. Moscow: Radio i svyaz'. 1989. (In Russian).
7. Zadeh L.A. Ponyatie lingvisticheskoy peremennoy i ego primenenie k prinyatiyu priblizhennykh resheniy [The concept of linguistic variable and its application to the adoption of the approximate solutions]. Moscow: Mir. 1976. (In Russian).
8. Borisov A.N., Krumberg O.A., Fedorov I.P. Prinyatie resheniy na osnove nechetkikh modeley: primery ispol'zovaniya. [Decision-making based on fuzzy models usage examples]. Riga: Zinatne.1990. 184 p. (In Russian).

Information about authors:
Novikov A.N., Ph.D., associate professor, Military Space Academy.

For citation:
Novikov A.N. On some aspects of applying fuzzy set theory in substantiating the list of characteristics of products controlled during operation. H&ES Research. 2015. Vol. 7. No. 5. Pp. 12–17. (in Russian).

ОБОБЩЕННАЯ МОДЕЛЬ ПОТОКА РАЗНОТИПНЫХ ПРОГРАММНЫХ ОШИБОК ДЛЯ ОЦЕНИВАНИЯ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Гусеница Ярослав Николаевич,
к.т.н., преподаватель кафедры метрологического обеспечения вооружения, военной и специальной техники Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург, Россия, yaromir226@mail.ru

Ключевые слова:
командные пункты, сложные военно-технические системы, ограниченный объем испытаний, надежность программного обеспечения, произвольное распределение, разнотипные программные ошибки.

АННОТАЦИЯ

В работе проведен анализ направлений обеспечения требуемого уровня эффективности боевого применения сложных военно-технических систем. Обозначена одна из проблем реализации опытно-конструкторских работ по созданию и модернизации средств вычислительной техники и программного обеспечения командных пунктов сложных военно-технических систем. Данные опытно-конструкторские работы, с одной стороны, позволяют расширить функциональные возможности сложных военно-технических систем, а с другой стороны, приводят к усложнению программного обеспечения командных пунктов. При этом усложнение программного обеспечения становится причиной появления в нем значительного количества программных ошибок, наличие которых приводит к снижению не только уровня надежности программного обеспечения командных пунктов, но и эффективности боевого применения сложных военно-технических систем. Обоснована актуальность задачи оценивания надежности программного обеспечения командных пунктов сложных военно-технических систем при ограниченном объеме испытаний. Проведен анализ существующих моделей надежности программного обеспечения. Выявлены их ограничения и допущения, не позволяющие их использовать для оценивания надежности программного обеспечения командных пунктов сложных военно-технических систем при ограниченном объеме испытаний. Предложена обобщенная модель потока разнотипных программных ошибок, позволяющая компенсировать указанные недостатки. Данная модель является дальнейшим развитием модели Шнейдевинда. Однако предлагаемая модель, в отличие от модели Шнейдевинда, комплексно учитывает ключевые закономерности между программными ошибками, отказами и надежностью программного обеспечения. Во-первых, формализована зависимость надежности программного обеспечения от набора входных данных. Для этого в модели Шнейдевинда конкретизирован коэффициент, характеризующий интенсивность определения программных ошибок, параметрами статической модели Нельсона. Во-вторых, математически описана возможность внесения новых программных ошибок при исправлении обнаруженных, а также формализовано условие того, что не каждая программная ошибка может быть обнаружена и исправлена. Это реализовано путем уточнения коэффициента, характеризующего оставшееся количество программных ошибок, параметрами модифицированной динамической модели Липова. В-третьих, учтена возможность проявления программных ошибок с разной частотой. В результате плотность распределения интервалов времени между проявлением программных ошибок обобщена на случай произвольных распределений. В-четвертых, формализована ситуация, что не каждая программная ошибка может привести к отказу программного обеспечения. Для этого все обнаруженные программные ошибки предлагается разделять на соответствующие типы, отличающиеся друг от друга критичностью последствий проявления в программном обеспечении. Кроме того, поток программных ошибок каждого типа необходимо моделировать отдельно. В результате обобщенная модель потока разнотипных программных ошибок может быть использована для оценивания надежности программного обеспечения командных пунктов сложных военно-технических систем при ограниченном объеме испытаний. Данная модель может быть применена при обосновании внедрения новейших достижений науки и техники в практику создания, отработки и испытаний программного обеспечения командных пунктов сложных военно-технических систем.

Введение

Анализ военных конфликтов последних десятилетий наглядно демонстрирует активное развитие эвентуальным противником не только вооружения, военной и специальной техники, способов и форм их боевого применения, но и новых концепций и сфер ведения войны. Данная тенденция обусловливает появление ранее неизвестных новых внешних угроз национальной обороны Российской Федерации, для парирования которых в настоящее время совершенствуются существующие и создаются новые сложные военно-технические системы.

Материальную основу сложных военно-технических систем составляют вооружение, военная и специальная техника, системы и комплексы военного назначения, энерго-механические и инженерно-технические комплексы, линии энергоснабжения, система боевого управления, представляющие собой совокупность взаимосвязанных технических объектов и персонала, объединенных в единую систему для решения поставленных перед ними задач по предназначению.

В настоящее время обеспечение требуемого уровня эффективности боевого применения сложных военно-технических систем реализуется по нескольким крупным направлениям. Одно из них связано с повышением качества подготовки военных специалистов в области эксплуатации тех или иных компонентов сложных военно-технических систем. По данному направлению основу составляет внедрение тренажерных комплексов и компьютерных обучающих систем в учебный процесс военных специалистов [1, 2].

Еще одним актуальным направлением обеспечения требуемого уровня эффективности боевого применения сложных военно-технических систем является автоматизация всего процесса боевой работы. Это в свою очередь достигается путем внедрения в процесс функционирования сложных военно-технических систем самых современных информационных технологий [3, 4], что объясняет наличие многочисленных опытно-конструкторских работ, направленных на разработку и модернизацию средств вычислительной техники и программного обеспечения командных пунктов сложных военно-технических систем.

Данные опытно-конструкторские работы, с одной стороны, позволяют расширить функциональные возможности сложных военно-технических систем, а, с другой стороны, приводят к усложнению программного обеспечения командных пунктов. При этом усложнение программного обеспечения становится причиной появления в нем значительного количества программных ошибок, наличие которых приводит к снижению не только уровня надежности программного обеспечения командных пунктов, но и эффективности боевого применения сложных военно-технических систем [5].

Известным способом повышения надежности программного обеспечения командных пунктов сложных военно-технических систем является проведение различных видов контроля и испытаний, которые позволяют получать статистическую информацию о программных ошибках, содержащихся в этом программном обеспечении [6-8]. Наличие и анализ такой информации является необходимым условием в принятии обоснованных решений о возможных сроках доработки программного обеспечения командных пунктов сложных военно-технических систем, а также нужном объеме экономических, временных и людских ресурсов на исправление обнаруженных программных ошибок.

Однако в настоящее время объем испытаний как самих сложных военно-технических систем, так и его компонентов значительно сокращается. Этому способствует высокая стоимость проведения натурных испытаний, ограниченность полигонных испытаний и полная невозможность проведения боевых работ на местах размещения сложных военно-технических систем. Особенно остро данный вопрос стоит при испытании программного обеспечения командных пунктов сложных военно-технических систем, т.к. реализация полного объема испытаний программного обеспечения командных пунктов возможна только до морального устаревания сложных военно-технических систем. Поэтому оценивание надежности программного обеспечения командных пунктов сложных военно-технических систем при ограниченном объеме испытаний является весьма актуальной задачей.

Для решения этой задачи в настоящее время используются модели надежности программного обеспечения. Но анализ этих моделей показывает, что они являются неадекватными реальному процессу функционирования программного обеспечения командных пунктов сложных военно-технических систем. Прежде всего, это связано с тем, что имеющиеся модели надежности программного обеспечения обладают чрезмерным количеством ограничений и допущений. Кроме того в каждой из моделей время безотказной работы программного обеспечения подчиняется какому-либо конкретному закону распределения, который практически невозможно подтвердить в случае неполной статистической информации о программных ошибках.

Все перечисленные выше обстоятельства не позволяют использовать имеющиеся модели для оценивания надежности программного обеспечения командных пунктов сложных военно-технических систем при ограниченном объеме испытаний. Следовательно, выходом из сложившейся ситуации является разработка модели, адекватной реальному процессу функционирования программного обеспечения командных пунктов сложных военно-технических систем.

Адекватность является мерой объективного соответствия модели познаваемому объекту исследования и характеризуется тем, насколько полно в модели отражены основные закономерности предметной области. К основным закономерностям между программными ошибками, отказами и надежностью программного

обеспечения командных пунктов сложных военно-технических систем можно отнести следующие [9]:

1. Надежность программного обеспечения зависит от набора входных данных.

2. Надежность программного обеспечения зависит от длительности испытаний.

3. Надежность программного обеспечения характеризуется частотой проявления программных ошибок. При этом известно, что программные ошибки проявляются с разной частотой. Кроме того несколько программных ошибок могут проявляться одновременно.

4. Число программных ошибок – величина «ненаблюдаемая», наблюдаются не сами программные ошибки, а результат их проявления – отказы. Поэтому не каждая программная ошибка может быть обнаружена и исправлена.

5. Программные ошибки могут компенсировать друг друга, так что после исправления какой-то одной программной ошибки могут быть внесены другие. В итоге уровень надежности программного обеспечения может стать ниже, чем до исправления этой программной ошибки.

6. Не каждая программная ошибка может привести к отказу программного обеспечения. С другой стороны отказ программного обеспечения может быть следствием не одной, а сразу нескольких программных ошибок.

Данные закономерности учитываются в обобщенной модели потока разно-типных программных ошибок. Эта модель является дальнейшим развитием модели Шнейдевинда, которая учитывает вторуюи частично третью (надежность программного обеспечения характеризуется частотой проявления программных ошибок) закономерности между программными ошибками, отказами и надежностью программного обеспечения. Согласно модели Шнейдевинда проявление программных ошибок описывается как неоднородный пуассоновский процесс с экспоненциально затухающей функцией интенсивности, для которого параметр потока программных ошибок определяется формулой (1), а плотность распределения интервалов времени между проявлением программных ошибок – формулой (2) [10]:

$$\omega(t) = \varphi e^{-\psi t}, \tag{1}$$

$$f(t) = \varphi e^{-\psi t + \frac{\varphi}{\psi}(e^{-\psi t} - 1)}, \tag{2}$$

где φ – коэффициент, характеризующий оставшееся количество программных ошибок в программном обеспечении; ψ – коэффициент, характеризующий интенсивность определения программных ошибок в программном обеспечении.

Для того чтобы учесть первую закономерность между программными ошибками, отказами и надежностью программного обеспечения, необходимо конкретизировать коэффициент ψ параметрами статической модели Нельсона:

$$\psi = -\sum_{a=1}^{A} \frac{\ln\left(1 - \sum_{b=1}^{B} p_{ab} y_b\right)}{\Delta t_a}, \tag{3}$$

где A – общее количество прогонов программного обеспечения; B – общее количество наборов входной информации; p_{ab} – вероятность использования b-го набора входной информации на a-м прогоне программного обеспечения; Δt_a – время a-го прогона программного обеспечения; y_b – динамическая переменная, принимающая значение «0», если при b-м наборе входной информации прогон программного обеспечения завершается программной ошибкой, «1» – если при b-м наборе входной информации прогон программного обеспечения завершается правильным результатом, то динамическая переменная принимает значение.

Чтобы учесть четвертую и пятую закономерности между программными ошибками, отказами и надежностью программного обеспечения, необходимо конкретизировать коэффициент φ параметрами модифицированной динамической модели Липова [18]:

$$\varphi = \left(N - (1-\rho)\sum_{j=1}^{i-1} n_j + \sum_{j=1}^{i-1} m_j\right), \tag{4}$$

где n_j – количество обнаруженных и исправленных программных ошибок после (i–1)-го интервала испытания программного обеспечения; m_j – количество обнаруженных и неисправленных программных ошибок после (i–1)-го интервала испытания программного обеспечения; ρ – вероятность внесения новой программной ошибки при исправлении обнаруженной.

Вероятность ρ может быть получена с использованием информации о текучести программного обеспечения автоматизированных систем управления войсками и оружием, которая отражает объем изменений в исходном коде, внесенных за период разработки, производства и сопровождения программного обеспечения. Текучесть программного обеспечения может быть вычислена следующим образом [12]:

$$\hat{\rho} = \frac{L'}{L},$$

где L – количество строк исходного кода в программном обеспечении; L' – количество добавленных, удаленных, измененных строк исходного кода.

Анализ работы [12] показывает, что корреляционный момент между текучестью программного обеспечения и вероятностью внесения программной ошибки составляет $K_{\rho\hat{\rho}}$=0,79 Поэтому вероятность внесения новой программной ошибки при исправлении обнаруженной может быть рассчитана по формуле:

$$\rho = K_{\rho\hat{\rho}} \frac{L}{L'} = 0{,}79 \frac{L}{L'}.$$

Чтобы учесть полностью третью закономерность между программными ошибками, отказами и надежностью программного обеспечения, необходимо плот-

ность распределения (2) обобщить на случай произвольных распределений интервалов времени между проявлением программных ошибок. Для этого предлагается плотность распределения $f(t)$ представить как среднее значение гипердельтной $f_\partial(t)$ и гиперэкспоненциальной $f_\Im(t)$ плотностей:

$$\overline{f}(t)=\frac{f_\partial(t)+f_\Im(t)}{2}\ , \qquad (5)$$

Гипердельтная плотность определяется на основе гипердельтной аппроксимации. В результате плотность распределения $f(t)$ представляется как

$$f_\partial(t)= C_1\delta(t-T_1)+C_2\delta(t- T_2), \qquad (6)$$

где $C_{1,2}=\frac{1}{2}\left(1\pm\frac{3\nu_2\nu_1-\nu_3-2\nu_1^3}{\sqrt{\nu_3^2-6\nu_3\nu_2\nu_1-3\nu_2^2\nu_1^2+4\nu_3\nu_1^3+4\nu_2^3}}\right)$ –

вероятности, удовлетворяющие условию $C_1+C_2=1$;

$T_{1,2}=\frac{\nu_3-\nu_2\nu_1\mp\sqrt{\nu_3^2-6\nu_3\nu_2\nu_1-3\nu_2^2\nu_1^2+4\nu_3\nu_1^3+4\nu_2^3}}{2\left(\nu_2-\nu_1^2\right)}$ –

постоянные параметры;

$\delta(\bullet)$– дельта-функция Дирака.

При этом ν_1, ν_2 и ν_3 являются соответственно первым, вторым и третьим начальными моментами для интервалов времени между проявлением программных ошибок.

Гиперэкспоненциальная плотность может быть получена на основе метода последовательных фаз. В этом случае плотность распределения $f(t)$ представляется суммой двух экспоненциальных плотностей с комплексно-сопряженными параметрами:

$$f_\Im(t)=\left(\frac{\alpha^2+\beta^2}{\beta}\right)e^{-\alpha t}\sin\beta t\,, \qquad (7)$$

где $\alpha=\frac{\nu_1}{2\nu_1^2-\nu_2}$ –1-й комплексно-сопряженный параметр;

$\beta=\frac{\sqrt{3\nu_1^2-2\nu_2}}{\left(2\nu_1^2-\nu_2\right)}$ –2-й комплексно-сопряженный параметр.

Гипердельтная $f_\partial(t)$ и $f_\Im(t)$ гиперэкспоненциальная плотности могут использоваться независимо друг от друга. Однако использование данных плотностей в выражении (5) дает более точные результаты. С учетом этого интенсивность проявления программных ошибок рассчитывается по следующей формуле:

$$\overline{\lambda}(t)=\frac{1}{2}\cdot\left(\frac{C_1\delta\left(t-T_1\right)+C_2\delta\left(t-T_2\right)}{\left(C_1\theta\left(t-T_1\right)+C_2\theta\left(t-T_2\right)\right)-1}+\right.$$
$$\left.+\frac{\alpha e^{-\alpha t}\sin\beta t}{\beta}-e^{-\alpha t}\cos\beta t\right), \qquad (8)$$

где $\theta(\bullet)$ – функция Хевисайда.

Наконец, чтобы учесть шестую закономерность между программными ошибками, отказами и надежностью программного обеспечения, необходимо выполнить соответствующие преобразования.

Во-первых, все программные ошибки следует разделить на определенные типы, представленные в таблице 1 [11].

Таблица 1

Классификация типов программных ошибок

№ п/п	Тип программной ошибки	Описание
1.	Слабый	Нарушение эстетики программного обеспечения
2.	Умеренный	Некорректные выходные данные
3.	Раздражающий	Некорректное выполнение функций
4.	Очень серьезный	Выполнение не требуемых функций
5.	Экстремальный	Некорректные выходные данные при сетевой передаче
6.	Невыносимый	Некорректные выходные данные при записи в базу данных или в файл
7.	Катастрофический	Зависание программного обеспечения
8.	Инфекционный	Зависание операционной системы

Во-вторых, поток программных ошибок каждого k-го типа следует моделировать отдельно [11], т.е. выражение (8) должно быть преобразовано к следующему виду:

$$\overline{\lambda}_k(t)=\frac{1}{2}\cdot\left(\frac{C_1\delta\left(t-T_{1k}\right)+C_2\delta\left(t-T_{2k}\right)}{\left(C_1\theta\left(t-T_{1k}\right)+C_2\theta\left(t-T_{2k}\right)\right)-1}+\right.$$
$$\left.+\frac{\alpha_k e^{-\alpha_k t}\sin\beta_k t}{\beta_k}-e^{-\alpha_k t}\cos\beta_k t\right).$$

В-третьих, для каждого k-го типа программных ошибок необходимо определить критичность последствий их проявления в программном обеспечении. Она определяется через $p_k^{отк}$ условные вероятности отказа программного обеспечения из-за проявления в нем программных ошибок k-го типа. Эти условные вероятности могут быть рассчитаны по экспериментальным данным, полученным в ходе отладки программного обеспечения командных пунктов сложных военно-технических систем [11]:

$$p_k^{отк}=1-\frac{N_k^{отк}}{N_k^{ош}},$$

где $N_k^{отк}$ – количество отказов программного обеспечения, к которым привели программные ошибки k-го типа в ходе отладки; $N_k^{отк}$ – количество программных ошибок k-го типа, обнаруженных в ходе отладки.

Имея значение интенсивности проявления программных ошибок каждого типа и критичности последствий их проявления, может быть рассчитана интенсивность отказов программного обеспечения [11]:

$$\lambda(t) = \sum_{k=1}^{K} \lambda_k(t) p_k^{отк}.$$

Таким образом, обобщенная модель потока разнотипных программных ошибок комплексно учитывает ключевые закономерности между программными ошибками, отказами и надежностью программного обеспечения, что позволяет ее использовать для оценивания надежности программного обеспечения командных пунктов сложных военно-технических систем при ограниченном объеме испытаний. Данная модель может быть применена при обосновании внедрения новейших достижений науки и техники в практику создания, отработки и испытаний программного обеспечения командных пунктов сложных военно-технических систем.

Литература

1. Петрич Д.О., Гусеница Я.Н., Кругляк Ю.Л., Озеров В.А. Автоматизированная система контроля знаний обучающихся в области технического обслуживания компьютерных систем и комплексов // Труды Военно-космической академии имени А.Ф. Можайского. 2014. № 644. С. 219–230.

2. Гусеница Я.Н., Кругляк Ю.Л., Петрич Д.О. Наклонный стенд технического обслуживания и ремонта персонального компьютера // Техника средств связи. 2014. № 3(142). С. 124–128.

3. Разумов А.В., Ермаков С.Г., Петрич Д.О., Гусеница Я.Н. Вычислительная техника цифровой сигнальной обработки измерительных данных в трактах отечественных радиолокационных средств // Вопросы радиоэлектроники. 2011. №1. С. 124–128.

4. Петрич Д.О., Гусеница Я.Н., Завалишин М.А. Научно-методический подход к выбору рационального варианта архитектуры вычислительного комплекса радиолокационной системы специального назначения // Труды Военно-космической академии имени А.Ф. Можайского. 2011. № 632. С. 50–55.

5. Гусеница Я.Н., Завалишин М.А., Пестун У.А. Моделирование информационных средств системы контроля космического пространства, функционирующих в условиях динамически изменяющейся космической обстановки // Труды Военно-космической академии имени А.Ф. Можайского. 2011. № 632. С. 44–49.

6. Пророк В.Я., Гусеница Я.Н., Петрич Д.О. Построение системы контроля и диагностирования комплекса средств автоматизации автоматизированных систем управления войсками и оружием на основе нечетких искусственных нейронных сетей // T-Comm. Телекоммуникации и транспорт. 2013. Т. 7. № 6. С. 67–71.

7. Гусеница Я.Н. Методика верификации программного обеспечения вычислительных комплексов информационных средств контроля космического пространства на этапе проектирования // Труды Военно-космической академии имени А.Ф. Можайского. 2012. № 634. С. 15–20.

8. Гусеница Я.Н. Метод экспертизы программного обеспечения вооружения, военной и специальной техники / Техника средств связи. 2014. № 3(142). С. 118–123.

9. Гусеница Я.Н., Кругляк Ю.Л., Петрич Д.О. О некоторых особенностях надежности программного обеспечения автоматизированных систем управления войсками // Труды Военно-космической академии имени А.Ф. Можайского. 2013. № 638. С. 31–36.

10. Schneidewind N.F. Analysis of Error Processes in Computer Software // Sigplan Not. 1975. Vol. 10. No. 6.

11. Гусеница Я.Н. Модификация динамической модели Липова для оценивания надежности программного обеспечения автоматизированных систем управления войсками и оружием при ограниченном объеме испытаний // Сборник трудов Всероссийской научно-технической конференции «Теоретические и прикладные проблемы развития и совершенствования автоматизированных систем управления военного назначения», т. 1, ч. 2 . СПб.: ВКА имени А.Ф. Можайского. 2014. С. 126–132.

12. Нагаппан Н., Болл Т. Научно обоснованное прогнозирование сбоев // Идеальная разработка ПО. Рецепты лучших программистов; под ред. Э. Орама и Г. Уилсона. СПб.: Питер. 2012. 592 с.

Для цитирования:

Гусеница Я.Н. Обобщенная модель потока разнотипных программных ошибок для оценивания надежности программного обеспечения // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 18–23.

THE TOTAL MODEL OF STREAM WITH SOFTWARE ERRORS OF DIFFERENT TYPES FOR ESTIMATING SOFTWARE RELIABILITY

Gusenitsa Yaroslav Nikolaevich,
St. Petersburg, Russian, yaromir226@mail.ru

Abstract
The article presents of the flow of different types of software errors. This model is a modification of Schneidewind's model. However, the proposed model, in contrast to its prototype, the key allows for complex patterns between software errors, failures and reliability of the software. The formalization software reliability depending on the set of input data is implemented using a Nelson's model. The formalization of the possibility of a new software detected errors when correcting software errors, as well as formalization of the conditions that not every software error can be detected and corrected, implemented using a modified dynamic Lipov's model. The formalization of the situation concludes that not every software error can lead to the failure of software is implemented as follows. Firstly, all the detected software errors are invited to share in the corresponding types, differing criticality effects display in the software. Secondly, the flow of each type of software errors modeled separately. As a result of the generalized model of the flow of different types of software bugs can be used to estimate the reliability of the software command posts complex military-technical systems with limited testing. This model can be applied in justifying the introduction of the latest achievements of science and technology in the practice of creating, processing and testing software command and control centers complex military-technical systems.

Keywords: : command and control, complex military-technical systems, limited testing, software reliability, arbitrary distribution, software errors of different types.

References

1. Petric D.O., Gusenitsa Y.N., Kruglyak Y.L., Ozerov V.A. The automated control system of students' knowledge in the field of maintenance of computer systems and complexes. Military and space akademy named after A.F. Mojaiskiy. 2014. No. 644. Pp. 219–230. (In Russian).
2. Gusenitsa Y.N., Kruglyak Y.L., Petric D.O. The sloping stand for maintenance and repair of personal computers. Tekhnika sredstv svyazi. 2014. No. 3(142). Pp. 124–128. (In Russian).
3. Razumov A.V., Ermakov S.G., Petric D.O. Computers digital signal processing measurement data paths local radar. Voprosyi radioelektroniki. 2011. Pp. 124–128. (In Russian).
4. Petric D.O., Gusenitsa Y.N., Zavalishin M.A. Scientific and methodical approach to the choice of a rational variant of architecture computing complex radar system for special purposes. Military and space akademy named after A.F. Mojaiskiy. 2011. No. 632. Pp. 50–55. (In Russian).
5. Gusenitsa Y.N., Zavalishin M.A., Pestun U.A. Modeling information devices of control of space functioning in a dynamically changing space environment. Military and space akademy named after A.F. Mojaiskiy. 2011. No. 632. Pp. 44–49. (In Russian).
6. Prorok V.Y., Gusenitsa Y.N., Petric D.O. Building a system of monitoring and diagnosing the automated control systems for special purposes based on fuzzy artificial neural networks. T-Comm: Telecommunications and Transport. 2013. Vol. 7. No. 6. Pp. 67–71. (In Russian).
7. Gusenitsa Y.N. Method of verification software computer systems of information devices of control space in the design phase. Military and space akademy named after A.F. Mojaiskiy. 2012. No. 634. Pp. 15–20. (In Russian).
8. Gusenitsa Y.N. Method of software review of weapons, military and special equipment. Tekhnika sredstv svyazi. 2014. No. 3(142). Pp. 118–123. (In Russian).
9. Gusenitsa Y.N., Kruglyak Y.L., Petric D.O. Some features of the software reliability of the automated systems of command and control. Military and space akademy named after A.F. Mojaiskiy. 2013. No. 638. Pp. 31–36. (In Russian).
10. Schneidewind N.F. Analysis of Error Processes in Computer Software. Sigplan Not. 1975. Vol. 10. No. 6.
11. Gusenitsa Y.N. Modification of the dynamic model for evaluating the reliability of Lipova software of the automated systems of command and control and weapons with a limited amount of testing. Proceedings of the All-Russian Scientific and Technical Conference «Theoretical and applied problems of development and improvement of automated control systems for military use». Saint-Petersburg. 2014. Pp. 126–132. (In Russian).
12. Nagapan N., Ball T. Nauchno obosnovannoe prognozirovanie sboev [Science-based forecasting failures]. Ideal'naya razrabotka PO. Retsepty luchshikh programmistov; pod red. E. Orama i G. Uilsona. . SPb.: Piter. 2012. 592 p. (In Russian).

Information about authors:
Gusenitsa Ya.N., Ph.D., lecturer in Department of metrological maintenance, Military Space Academy.

For citation:
Gusenitsa Ya.N. The total model of stream with software errors of different types for estimating software reliability. H&ES Research. 2015. Vol. 7. No. 5. Pp. 18–23. (in Russian).

ОБ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ СЕТЕЙ ОБМЕНА УПРАВЛЯЮЩЕЙ ИНФОРМАЦИЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Щелков
Дмитрий Александрович,
адъюнкт кафедры технологий и средств технического обеспечения и эксплуатации автоматизированных систем управления Военно-космической академии имени А.Ф.Можайского, г. Санкт-Петербург, Россия, Dmitry-Schelkov@yandex.ru

Ключевые слова:
сети обмена управляющей информацией, протокол RIP, алгоритм Беллмана-Форда, протокол OSPF, алгоритм Дейкстры, состояния смежности.

АННОТАЦИЯ

Анализ потоков информации, циркулирующих в различных современных инфокоммуникационных системах и сетях специального назначения (ИКС СН) (в т.ч. в наложенных сетях обмена управляющей информацией автоматизированных систем управления (АСУ) инфокоммуникационной сетью специального назначения), реализующих Internet protocol (IP), показывает наличие значительного числа сообщений различных видов, передаваемых в виде IP-пакетов. Среди многообразия задач, решаемых в процессе функционирования таких сетей, можно выделить основную – обеспечение передачи заданного объема потоков управляющих сообщений с заданной своевременностью, достоверностью при обеспечении требуемого уровня устойчивости в условиях фиксированного уровня ресурсов.

Как правило, сети обмена управляющей информацией АСУ инфокоммуникационными сетями специального назначения строятся путем наложения на некоторую транспортную основу слоя, реализующего Internet protocol (IP) или сочетание IP/MPLS.

Устойчивость информационного взаимодействия должностных лиц пунктов управления в настоящее время приобретает наиболее важное значение, так как процессы передачи информации в IP-сети с применением стандартных протоколов управления и маршрутизации не обеспечивает требуемый ее уровень в реальных условиях эксплуатации.

Традиционное объединение локальных сетей должностные лица пунктов управления АСУ ИКС СН через слабо защищенную внешнюю среду передачи информации в единую сеть с образованием защищённой виртуальной сети, в которой каналы связи интерпретируются с помощью каналов связи реальной сети, не защищают от несанкционированных воздействий через протоколы маршрутизации и управления.

Известные методы снижения возможности несанкционированных воздействий на сеть при использовании в ней простого протокола сетевого управления SNMP рассмотрены в работе.

Поэтому актуальным является рассмотрение возможных вариантов обеспечения устойчивой работы сетей обмена управляющей информацией АСУ инфокоммуникационной сетью специального назначения, реализующих IP на сетевом уровне, при использовании в наложенной IP-сети наиболее часто применяемых протоколов маршрутизации RIP и OSPF.

Протокол RIP (Routing Information Protocol) описан в документе RFC 1058. Протокол RIP относится к классу протоколов IGP. Этот протокол является одним из первых протоколов обмена маршрутной информацией между маршрутизаторами в IP-сети и основывается на использовании алгоритма длины вектора. Впервые протокол RIP появился в 1982 году как часть стека протокола TCP/IP для UNIX. Исторически протокол RIP близко связан с семейством сетевых протоколов фирмы Xerox. Преимуществом протокола RIP является его простота. Недостатком – увеличение трафика за счёт периодической рассылки широковещательных сообщений.

Этот алгоритм основывается на тех же принципах, что и алгоритм Беллмана-Форда, который был применён в первом протоколе маршрутизации для сетей ARPA и исходит из предположения, что каждый маршрутизатор может вычислить самый короткий маршрут и соответствующее расстояние до каждой сети. При применении его в сети каждый маршрутизатор выбирает ближайший соседний маршрутизатор, который расположен на этом самом коротком маршруте до получателя. Выбор осуществляется на основании информации о стоимости путей (выбирается путь с меньшей стоимостью). Стоимость вычисляется по информации, имеющейся в таблицах маршрутизации всех соседних маршрутизаторов. Маршрутизаторы регулярно обмениваются между собой таблицами маршрутизации. Протокол RIP использует в качестве метрики маршрута количество переходов, то есть число маршрутизаторов, которые должен миновать пакет (дейтаграмма), прежде чем он достигнет получателя. Маршрутизаторы с поддержкой протокола RIP всегда выбирают маршрут в сети с наименьшим числом переходов.На рис. 1. представлена метрика протокола RIP.

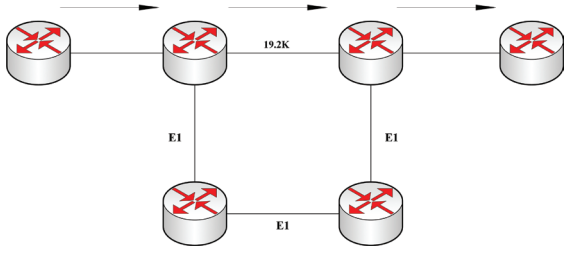

Рис. 1. Метрика протокола RIP

Маршрут с полосой пропускания равной 19,2 Кбит/с включает в себя три перехода. Нижний альтернативный маршрут по каналам связи E1 включает пять переходов. Поскольку выбор маршрута в протоколе RIP основывается на количестве переходов, то в данном случае в таблицу маршрутизации будет записан маршрут с пропускной способностью 19,2 Кбит/с вместо гораздо более быстрых каналов E1.

Протокол RIP предотвращает появление петель в маршрутизации, по которым пакеты могли бы циркулировать неопределенно долго, устанавливая максимально допустимое количество переходов на маршруте от отправителя к получателю. Стандартное максимальное значение количества переходов равно 15. При получении маршрутизатором обновление маршрутов, содержащее новую или измененную запись, он увеличивает значение метрики на единицу. Ограничение в 15 транзитных узлов сужает область применения протокола RIP до сетей, в которых число промежуточных маршрутизаторов не должно превышать 15. Для более масштабных сетей нужно использовать другие протоколы маршрутизации, или разбивать сеть на автономные области.

К появлению новых маршрутов маршрутизаторы RIP приспосабливаются без труда: в очередном сообщении своим соседям они передают новую информацию, так что та постепенно становится известна всем маршрутизаторам сети. А вот к отрицательным изменениям, связанным с потерей какого-либо маршрута, им адаптироваться сложнее. Дело в том, что в формате сообщений протокола RIP нет поля, где бы содержалась информация об отсутствии пути к данной сети. Некоторый маршрут становится недействительным на основании истечения времени жизни маршрута или указания специального расстояния до сети. Для реализации первого механизма каждая запись таблицы маршрутизации, полученная по протоколу RIP, имеет время жизни (TTL). При поступлении очередного сообщения RIP с подтверждением того, что данная запись действительна, таймер TTL устанавливается в исходное состояние, а затем из него каждую секунду вычитается единица. Если за время тайм-аута не придет новое маршрутное сообщение об этом маршруте, то он отмечается как недействительный. Время ожидания связано с периодом рассылки векторов по сети. Период рассылки в RIP равен 30 с., а в качестве тайм-аута принято шестикратное значение периода рассылки. Шестикратный запас времени нужен для уверенности в том, что проблемы заключаются не в потерях сообщений RIP (а это возможно, так как RIP использует транспортный протокол UDP, который не гарантирует доставку сообщений), а в том, что сеть действительно стала недоступна. Если какой-либо маршрутизатор выходит из строя, то через 180 с все порожденные этим маршрутизатором записи станут недействительными у его ближайших соседей. После этого процесс повторится уже для ближайших соседей – они вычеркнут подобные записи через 360 с, так как первые 180 с ближайшие соседи еще передавали сообщения об этих записях. Как видим, сведения о недоступных через отказавший маршрутизатор сетях распространяются по сети не очень быстро, время распространения кратно времени жизни записи, а коэффициент кратности равен количеству транзитных узлов между самыми дальними маршрутизаторами сети. В этом и заключается одна из причин выбора в качестве периода рассылки небольшой величины.

Так как протокол RIP был разработан достаточно давно и практически не изменялся за это время, он обладает определенными недостатками, которые ограничивают его применение в достаточно сложных сетях [2], но в сети обмена управляющей информацией автоматизированных систем управления (АСУ) инфоком-

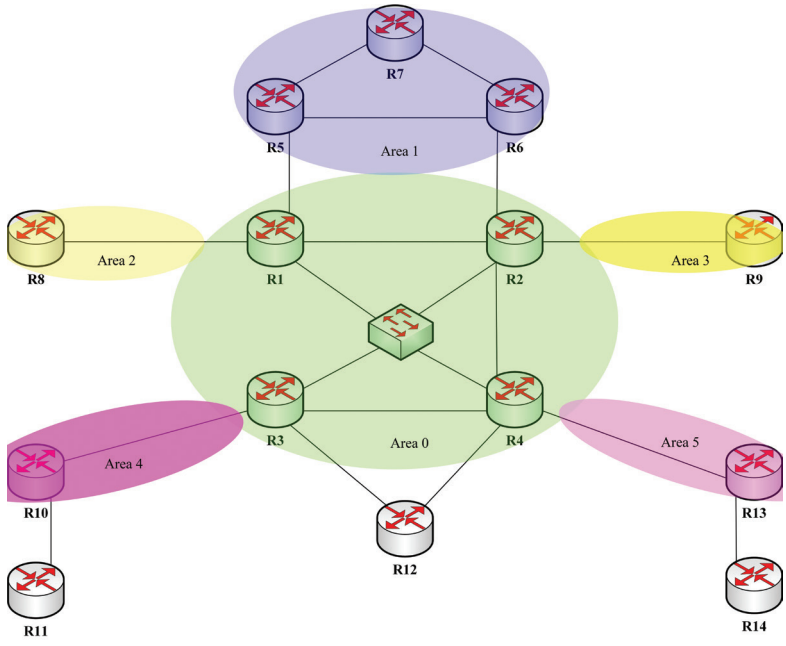

Рис. 2. Разбиение автономной системы на несколько областей

муникационной сетью специального назначения он может быть достаточно хорош.

Существует спецификация протокола OSPF (Open Shortest Path First), которая описана в документе RFC 1247. Протокол OSPF использует деление автономной системы на несколько областей, в каждой из которых работает своя копия протокола. Деление автономной системы на несколько областей позволяет значительно сократить нагрузку на сеть. Пример разбиения системы на области представлен на рис. 2.

Протокол OSPF может вычислять маршруты в сети, работая совместно с другими протоколами обмена маршрутной информацией. Данный протокол основан на алгоритме состояния канала. Суть этого алгоритма состоит в том, что необходимо вычислить кратчайший путь. При этом «кратчайший» не означает, что путь физически самый короткий. Имеется в виду что, информация пройдёт по этому пути быстрее, чем по другим. Маршрутизатор сети, работающий с этим протоколом, отправляет запросы всем соседним маршрутизаторам, находящимся в одном с ним домене маршрутизации, для выявления состояния каналов до них и далее от них. Состояние канала при этом характеризуется несколькими параметрами, которые называются метриками. Метрикой может быть пропускная способность канала, его загрузка на текущий момент, задержка информации при её прохождении по этому каналу и т.д. Обобщив полученные сведения, этот маршрутизатор сообщает их всем соседям. После этого им строится ориентированный граф, который повторяет топологию домена маршрутизации. Каждому ребру этого графа назначается оценочный параметр (метрика) рис. 3.

После построения графа используется алгоритм Дейкстры, который по двум заданным узлам находит набор рёбер с наименьшей суммарной стоимостью, т.е. по сути, выбирает оптимальный маршрут. По совокупной информации (полученной и найденной в результате вычислений) создаётся таблица маршрутизации.

Протокол OSPF состоит из трёх внутренних подпротоколов: Hello, Exchange, Flooding. Периодически маршрутизаторы сети обмениваются между собой сообщениями подпротокола Hello. Важным процессом в протоколе OSPF является установка связей между маршрутизаторами. Протокол OSPF имеет несколько состояний. Самое простое состояние, при котором не происходит обмен между соседними маршрутизаторами, обычно наблюдается сразу после подключения к сети маршрутизатора, работающего под управлением протокола OSPF, или после возникновения нарушения в работе. Следующее состояние называется

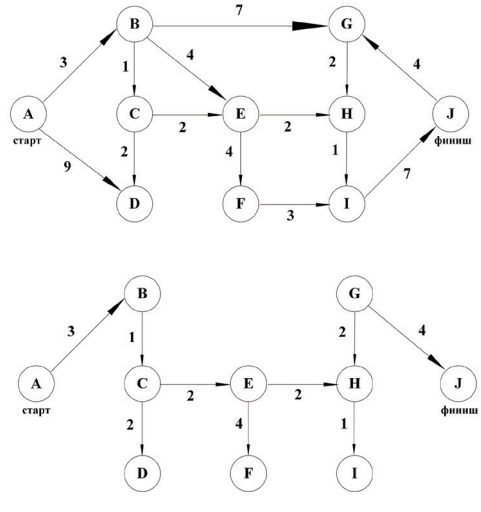

Рис. 3. Оценочные параметры рёбер графа

состоянием инициализации. В ходе данного состояния маршрутизатор OSPF посылает Hello пакеты для установки связи между соседними устройствами. В состоянии двусторонней связи каждый маршрутизатор OSPF пытается установить связь со всеми своими соседями, это происходит также с помощью пакета Hello. В данном пакете передаётся список всех известных соседних маршрутизаторов. Если маршрутизатор принимает пакет Hello и «видит» в этом пакете свой идентификатор, то считается что состояние двухсторонней связи установлено. После установления связей маршрутизаторы переходят в послестартовое состояние. Это состояние представляет собой первый этап формирования отношений смежности, на котором необходимо определить, какой маршрутизатор должен быть ведущим и какой — ведомым. Ведущим становится маршрутизатор с наибольшим идентификатором. Ведущий маршрутизатор управляет процессом обмена данными, устанавливая и наращивая начальный порядковый номер базы данных. Ведущий и ведомый маршрутизаторы представлены на рис. 4.

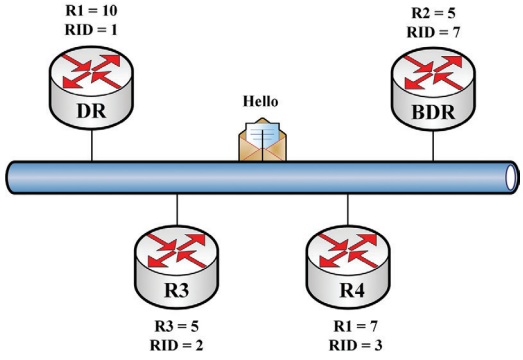

Рис. 4. Ведущий и ведомый маршрутизаторы

В следующем состоянии происходит обмен информации о состоянии каналов. После получения маршрутизатором такой информации он сравнивает её со своей базой данных и если такая информация отсутствует, то маршрутизатор запрашивает полную информацию о данном канале. В следующем состоянии, которое называется состоянием загрузки, передача пакетов базы данных должна быть завершена, а соседнему устройству переданы пакеты запросов состояния каналов (Link-State request – LSR), содержащие требование передать более свежие анонсы, которые еще не были получены в состоянии обмена. В результате выполнения этих запросов передаются анонсы LSA, позволяющие завершить обмен информацией о маршрутах. После того как каждый маршрутизатор имеет свою таблицу смежных маршрутизаторов, считается что установлено состояние полной смежности. В данном состоянии маршрутизаторы приступают к нормальной работе.

В целом протокол OSPF и многие другие (IGRP, EIGRP, EGP, BGP, IGMP, DVMRP, MOSPF, PIM) подходят для современных больших, динамически изменяющихся сетей. Однако, ориентировка этих протоколов на открытую сеть типа Интернет, предполагающая фактически знание на каждом маршрутизаторе всей структуры сети и возможность влияния на процессы маршрутизации извне, являются существенными недостатками. Поэтому применение их в сетях обмена управляющей информацией АСУ инфокоммуникационной сетью специального назначения, реализующих Internet protocol нежелательно по причинам невозможности обеспечения требований по качеству и безопасности.

Поэтому необходимы дополнительные приемы, разработаны алгоритмы усовершенствования, основанные на изменении формирования метрик при составлении матрицы маршрутов в маршрутизаторах сетей обмена управляющей информацией АСУ инфокоммуникационной сетью специального назначения. Эти алгоритмы должны учитывать особенности применяемых протоколов как IP, так RIP и OSPF. Эти алгоритмы, очевидно можно использовать. Причем процедуры формирования метрики можно распространить на каждый из доменов маршрутизации, что позволит организовать псевдоключевые зоны на сетевом уровне IP-сети. Эти алгоритмы должны быть встроены в стандартные протоколы маршрутизации (RIP и OSPF). Процедуры формирования метрики могут носить различный характер, определяемый степенью ее адекватности реальным процессам передачи информации в сети. Важно только то, чтобы они существенно отличались от применяемых в протоколах. При этом могут быть рекомендованы достаточно известные методы управления и формирования метрики [5].

Так, например, в процедуре вычисления метрики протокола RIP, в котором учитывается величина длины пути в числе транзитов $R_l = \sum r_i$, можно так изменить параметр r_i, чтобы он каким либо образом учитывал уровень нагрузки (или задержки пакета), т.е. $r_{in} = r_i + \Delta r_i$, причем $\Delta r_i = f(r_{zi})$ или $\Delta r_i = f_1(\rho_i)$.

Аналогично, в процедуре вычисления метрики протокола OSPF, в котором учитывается пропускная способность исходящих из узлов сети трактов $P_l = \sum y(p_i)$, можно также изменить параметру $y(p_i)$, чтобы он определенным образом учитывал уровень нагрузки (или задержки пакета), т.е. $y_n(p_i) = y(p_i) + y(\Delta p_i)$, причем $y(\Delta p_i) = f_y(t_{zi})$ или $y(\Delta p_i) = f_{y1}(\rho_i)$.

Вопросы учета степени влияния добавок Δr_i от величин t_{zi} или ρ_i являются достаточно сложными и требуют отдельных исследований. Важно, что такой подход позволяет учесть данные параметры, устранить недостатки приведенных известных протоколов и повысить показатели передачи в сети обмена управляющей информацией АСУ.

Литература

1. Буренин А.Н., Легков К.Е. К вопросу управления современными инфокоммуникационными сетями, функционирующими в условиях интенсивных воздействий // Сборник трудов Северо-Кавказского филиала Московского технического университета связи

и информатики. Часть 1. Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2014. С. 101–103.

2. Легков К.Е., Буренин А.Н. Модели организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями // Наукоемкие технологии в космических исследованиях Земли.2012. Т. 4. № 1. С. 14–16.

3. Буренин А.Н., Легков К.Е. Эффективные методы управления потоками в защищённых инфокоммуникационных сетях // Наукоемкие технологии в космических исследованиях Земли.2010. Т. 2. № 2. С. 29–34.

4. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. СПб.: БХВ-Петербург. 2000. 512 с.

5. Буренин А.Н. Об управлении маршрутизацией на основе модифицированных адаптивных методов // Техника средств связи. Сер. ТПС. 1991. № 7. С. 51–59.

Для цитирования:
Щелков Д.А. Об устойчивости функционирования сетей обмена управляющей информацией автоматизированных систем управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 24–28.

ABOUT THE SUSTAINABILITY OF EXCHANGE NETWORKS OF MANAGEMENT INFORMATION AUTOMATED SYSTEMS MANAGEMENT INFO-COMMUNICATION NETWORKS SPECIAL PURPOSE

Shchelkov Dmitry Aleksandrovich,
St. Petersburg, RussianDmitry-Schelkov@yandex.ru

Abstract
The analysis of flows of information circulating in various modern infocommunication system and networks (ICN SP) (including in the imposed networks of an exchange of operating information of automatic control system (ACS) an infocommunication network of a special purpose), realizing IP, shows existence of considerable number of messages of the different types transferred in the form of IP of packages.
Among variety of the tasks solved in the course of functioning of such networks, it is possible to allocate the main - ensuring transfer of the set volume of flows of operating messages with the set timeliness, reliability when providing demanded level of stability in the conditions of the fixed level of resources.
As a rule, networks of an exchange of operating information of ACS infocommunication networks of a special purpose are under construction by imposing on some transport basis of the layer realizing IP or a combination of IP/MPLS.
Stability of information interaction of officials of points of management gets now most importance as information transfer processes in an IP network with application of standard protocols of management and routing level demanded it in actual practice does not provide operation.
Traditional association of the ACS ICN SP local networks through poorly protected environment of information transfer in a uniform network with formation of the protected virtual network in which communication channels are interpreted by means of communication channels of a real network, do not protect from unauthorized influences through routing and management protocols.
Known methods of decrease in possibility of unauthorized impacts on a network when using in it the simple protocol of network management of SNMP are considered in work.
Therefore consideration of possible options of ensuring steady work of networks of an exchange by operating information of ACS by an infocommunication network of the special purpose, realizing IP at network level is actual, when using in the imposed IP network of most often applied protocols of routing of RIP and OSPF.
Keywords: the network exchange control information, RIP, the algorithm of Bellman-Ford, OSPF, Dijkstra's algorithm, the state of the adjacency.

References
1. Burenin A.N., Legkov K.E. To a question of management of the modern infocommunication networks functioning in the conditions of intensive influences. In collection of works of the North Caucasian branch of the Moscow technical university of communication and informatics. Part 1. Rostov-on-Don.: PTs SKF "University" MTUSI. 2014. Pp. 101–103. (in Russian).
2. Legkov K.E., Burenin A.N. Models of the organization of the information managing director of a network for management system the modern infocommunication networks. H&ES Research. 2012. Vol. 4. No.1. Pp. 14–16. (in Russian).
3. Burenin A.N, Legkov K.E. Effective methods of control over flows on the protected infocommunication networks. H&ES Research. 2010. Vol. 2. No. 2. Pp. 29–34. (in Russian).
4. Olifer V. G., Olifer N. A. Novye tekhnologii i oborudovanie IP-setey [New technologies and equipment of IP networks]. SPb. BHV Petersburg. 2000. 512 p. (in Russian).
5. Burenin A.N. About management of routing on the basis of the modified adaptive methods. Tekhnika sredstv svyazi. Ser. TPS. 1991. No. 7. Pp. 51–59. (in Russian).

Information about authors:
Shchelkov D.A. post-graduate student of the Department automated systems of control, Military Space Academy.

For citation:
Shchelkov D.A. About the sustainability of exchange networks of management information automated systems management info-communication networks special purpose. H&ES Research. 2015. Vol. 7. No. 5. Pp. 24–28. (in Russian).

СВЯЗЬ

10–13.05

2016

Международная выставка информационных коммуникационных технологий

ЭКСПОЦЕНТР

Организатор: ЗАО «Экспоцентр»

При поддержке:
- Министерства связи и массовых коммуникаций РФ
- Министерства промышленности и торговли РФ
- Федерального агентства связи (Россвязь)
- Правительства Москвы

Под патронатом
Торгово-промышленной палаты РФ

12+

Реклама

Россия, Москва, ЦВК «Экспоцентр»

www.sviaz-expo.ru

Мобильная спутниковая связь и спутниковый интернет: тенденции формирования нового рынка

J'son & Partners
Management Consultancy

Введение

По оценкам International Telecommunications Union, более чем половина населения Земли не имеет доступа в Интернет, а компания Iridium оценивает, что только 10% поверхности планеты, включая моря и океаны, обеспечено беспроводной (мобильной) связью, которая основывается на наземной инфраструктуре. В этом смысле Россия, как крупнейшая по территории страна, – очень привлекательный рынок для спутниковых услуг, так как значительная часть ее территории мало населена и не охвачена мобильной связью.

Услуги спутниковой телефонной связи, а позднее и спутникового интернет для частных потребителей, существуют уже около 20 лет и за все это время они не смогли составить значимой конкуренции услугам на базе сотовой связи и мобильному интернет, оставаясь нишевыми предложениями для потребителей в отдаленных районах, работающих в специфических условиях, а так же для обеспеченных потребителей. Спутниковая телефонная связь стала синонимом «богатства», так как стоимость минуты соединения стоила намного выше тарифа в сотовых сетях, сюда же следовало добавить необходимость покупки дорогого спутникового телефона и тарифный план как правило включал высокую абонентскую плату и активацию. Вместе с тем, развитие телекоммуникаций последних лет и феномен конвергенции технологий позволил разработчикам космических спутников, операторам спутниковой связи, а так же инновационным технологическим компаниям и венчурным фондам взглянуть по-новому на рыночные возможности спутниковой связи и интернет и уже в настоящий момент предложить решения позволяющие в среднесрочной перспективе начать конкурировать на рынке сотовой связи и мобильного интернет.

В данном обзоре будут рассмотрены мировые тенденции формирования нового сегмента рынка телекоммуникаций – доступной широким слоям потребителей мобильной спутниковой связи и спутникового интернет, которые к 2020 году могут превратиться в огромный многомиллиардный международный рынок. В обзоре не рассматриваются другие технологии и рынки спутниковой связи. Например, стационарной спутниковой связи, рынки корпоративной и промышленной спутниковой связи (морские перевозки, нефте- и газодобыча и т. п.) и рынки спутниковых M2M услуг.

1. Понятие подвижной спутниковой связи и спутникового интернет в контексте общего рынка связи

Современный рынок услуг связи для частных потребителей включает следующие суб рынки:

- Рынок проводной связи и ШПД интернет, Wi-Fi точки подключения;
- Рынок сотовой связи и мобильного интернет (2G, 3G, LTE);
- Рынок спутниковой связи и интернет (на базе спутниковых телефонов, стационарных спутниковых тарелок и оборудования).

Новый сегмент рынка зарождается на базе конвергенции технологий всех трех рынков: рынка спутниковой связи, «последней мили» на базе Wi-Fi и рынка мобильной связи, так как для связи может почти любой современный смартфон (рис. 1).

Рис. 1. Формирование нового сегмента рынка

2. Объем и динамика рынка мобильной спутниковой связи в мире

По оценкам Satellite Industry Association в 2014 году доходы мирового спутникового рынка составили 201 млрд долл. с потенциалом роста до 250 млрд долл. к 2020 году. Принимая во внимание многие оценки (SIA, TIA и SpaceWorks) мирового рынка телекоммуникаций в 2014 году в диапазоне 4,6–5 трлн долл. с ежегодным ростом в 4–7 %, получается, что мировой спутниковый рынок составляет 4% доходов всего рынка телекоммуникаций. На долю спутниковых услуг приходится сейчас более 60% доходов спутникового рынка.

Доходы рынка от мобильных (подвижных) космических услуг (mobile satellite services – MSS) включающих мобильную спутниковую связь и мобильный спутниковый интернет оцениваются в 1,4 % доходов от спутниковых услуг (табл. 1).

Основной объем рынка как в производстве спутников, их запусках, так и в доходах от спутниковых услуг приходится на США, которые занимают 44 % всего мирового рынка (109 млрд долл. в 2013 году). Далее идут рынки Азии (55 млрд долл.) и Западной Европы (35 млрд долл.). Компании из США построили 27% всех спутников в мире и получили до 70 % всех доходов от их продажи. Более 65 % всех заказов новых спутников направляются в США, 4 % – в Россию. В общем количестве спутников, находящихся сейчас на орбите (1084 спутника), 41% составляют спутники США и 10% спутники России (рис. 2).

Рис. 2. Доля MSS в общих доходах спутникового рынка в мире 2014 году

По данным SIA и SwissQuote в 2013 году в функциональной структуре спутников до 40 % занимали коммерческие спутники связи, которые генерировали до 30 % всех доходов спутникового рынка. По оценкам Sandler Research в среднесрочной перспективе до 2018 года среднегодовой рост спутникового рынка (CAGR) оценивается в 8.05% и главным драйвером этого роста будет сектор коммерческих спутников.

Следует отметить, что традиционные космические спутники могут быть размером с автобус и весить несколько тонн, что объясняет их огромную стоимость разработки и вывода на орбиту. К тому же половину их веса составляет жидкое топливо, иногда более 2 тонн, для выполнения маневров в космосе. Поэтому основной современный интерес для реализации коммерческих услуг на базе MSS представляет сегмент «малых спутников» связи имеющих массу менее 500 кг. Подобные спутники отличаются значительно меньшей стоимостью разработки и запуска чем традиционные и позволяют организовать достаточную космическую группировку в сжатые сроки (табл. 2).

Таблица 1

Мировой спутниковый рынок млрд долл.

Доходы рынка	2010	2011	2012	2013	2014
Всего	168	177,4	188,8	195,2	201
Спутниковые услуги, в т.ч:	99,2	107,8	113,5	118,6	123
• **Спутниковая голосовая связь**	0,7	0,7	0,7	0,8	0,9
• **Спутниковый интернет**	1,6	1,7	1,8	1,8	1,9

Таблица 2

Классификация малых спутников связи и их рыночная стоимость, долл.

Размерность	Вес, кг	Стоимость, $
мини-	100-500	от 10 млн
микро-	10-100	1-10 млн
нано-	1-10,0	0,1-1 млн
пико-	0,1-1	до 0,1 млн
фемто-	до 0,1	до 0,1 млн

По данным SpaceWorks в 2014 году было запущено 158 малых спутников, в том числе 107 коммерческих, что превзошло оценки аналитиков, показав прирост в 72 % к 2013 году. Около половины всех новых запусков спутников в 2013 году производилась на малую околоземную орбиту. Значительная часть малых спутников используется в целях связи (22 %), науки и дистанционного зондирования Земли.

Принимая во внимание опубликованные планы ряда компаний США, выходящих на спутниковый рынок (см. Таблицу 8) и инвестирующих в настоящий момент миллиарды долларов в проекты по выводу сотен и тысяч малых спутников к 2020 году, можно ожидать, что это будет год массовых запусков огромных группировок малых спутников связи (рис. 3).

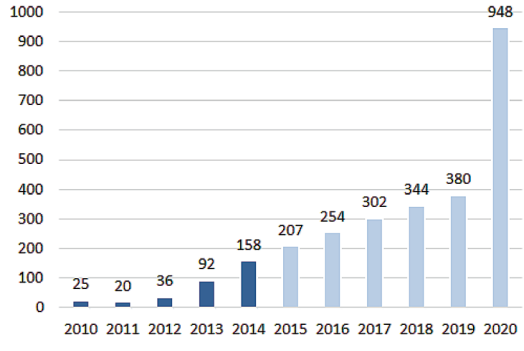

Рис. 3. Динамика запусков малых спутников в мире и прогноз до 2020 года, единиц

Существенное увеличение запусков в 2020 году связано с заявленными планами компаний по массовым запускам.

По оценкам SpaceWorks в период 2014–2016 годов коммерческие спутники будут составлять более половины (56 %) всех новых запусков малых спутников, а на долю спутников связи будет приходится до 9 % запусков. Основной прирост прогнозируется в сегменте наноспутников весом от 1 до 10 кг. Данная пропорция может сильно измениться к 2020 году, когда коммерческие спутники связи будут составлять подавляющую часть запускаемых малых спутников (рис. 4).

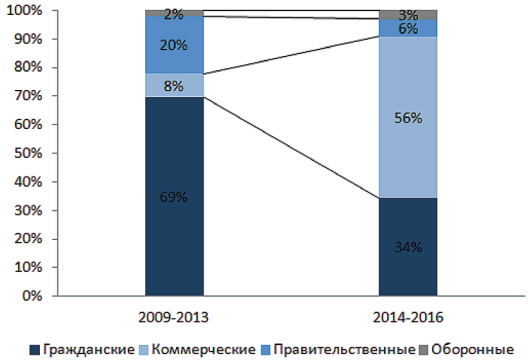

Рис. 4. Структура запусков нано-и микро-спутников по назначению, в мире

Доходы от продажи спутникового абонентского оборудования в мире выросли в 2013 году на 22 % по всем сегментам рынка – спутниковое ТВ, спутниковое радио, фиксированный интернет и услуги MSS.

3. Рынок мобильной спутниковой связи в общей структуре рынка связи

По данным ITU, GSMA, Informa и других агентств в 2014 году мировой рынок сотовой связи и мобильного интернет оценивается в более чем 1 трлн долл. с числом подписчиков (сим карты) в 7,2 млрд. единиц.

Это намного превышает размер рынка спутниковых MSS – 1,96 млрд долл. и 2,9 миллионов абонентов.(табл. 3).

Таблица 3

Статистика рынка мобильной связи в сравнении с рынком спутниковых MSS, 2014 год

Рынок	Размер рынка, млрд $	CAGR,%	Абоненты, млн.
Сотовая связь	1000	2,90%	7229
Мобильный интернет	210	16,9%	2530
Спутниковые мобильные услуги (MSS)	1,96	5%	2,9

Основным двайвером роста рынка телекоммуникаций будут пользователи мобильного интернет с CAGR 19 %, тогда как рост в сегменте спутниковых MSS прогнозируется в 5 %. Если эти темпы роста сохранятся, то к 2020 году в мире будет около 6 миллионов абонентов MSS (табл. 4).

Доходы на абонента (ARPU) спутниковых операторов более чем в пять раз выше, чем у сотовых операторов (табл. 5).

Таблица 4

Прогноз рынка мобильной связи и спутниковых MSS в 2020 году, млн абонентов

Сегмент рынка	2014	2020	CAGR,%
Сотовая связь	7229	9200	4%
Мобильный интернет	2530	5900	19%
Спутниковые мобильные услуги (MSS)	2,9	5,99	5%

Таблица 5

Статистика MSS-бизнеса спутниковых операторов и среднего счета на абонента (ARPU) мобильных операторов, 2014 год

Оператор	Выручка MSS, млн $	Абоненты MSS, млн	ARPU MSS, $ в мес
Thuraya	140,42	0,26	53
Globalstar	69,82	0,10	58
Iridium	309,42	0,38	68
Inmarsat	387,60	0,38	85
Средневзвешенное по группе	-	-	68
Verizon Wireless	-	-	19
AT&T	-	-	15
Sprint Nextel	-	-	17
T-Mobile USA	-	-	15
Среднемировой показатель по сотовым операторам	-	-	12

4. Тенденции развития рынка спутниковой связи и интернет

4.1. Ключевые направления развития рынка

К тенденциям спутникового рынка последних лет следует отнести:

- Существенное удешевление разработки и вывода на орбиту новых спутников;
- Снижение веса и размера спутников позволяет запускать единовременно большее их количество. Средний вес малых спутников уменьшается на 8 % ежегодно при этом их функциональные возможности возрастают;
- Стандартизация платформ и серийное производство спутников (платформы SSTL, стандарты Cubesat, PocketQub);
- Использование промышленных электронных компонентов при строительстве спутников, а не специальных «космических»;
- Появление частных космических грузовых перевозчиков, которые повышают конкуренцию в отрасли и снижают цену доставки на орбиту;
- Повышение интереса крупных компаний к производству малых спутников (Boeing, EADS) и выход на рынок малых спутников развивающихся стран (Перу, Эквадор, Вьетнам);
- Повышение интереса к малой орбите;
- Вывод спутников на более низкую орбиту обеспечивает более высокую скорость передачи сигнала от земли к спутнику и обратно, а так же меньшую задержку сигнала;
- Околоземная орбита является исчерпаемым ресурсом. Диапазон 600-1000 км является наиболее популярным и от этого наиболее загруженным. Накапли-

ваются будущие риски эксплуатации спутников и их вывода с орбиты после окончания срока их службы;

• Возможность получения глобального покрытия Земли средствами большого числа малых спутников;

• Партнерства корпораций из различных сфер обеспечивают эффект синергии в космических проектах, увеличивают скорость и качество разработки спутников и снижают стоимость проекта;

• Активное привлечение венчурных инвестиций показывает сохраняющийся интерес к отрасли. Венчурные фонды США вкладывают миллиарды долларов в новые проекты. Большое чисто проектов со сроком реализации в 2020 году;

• Рост числа малых спутников, разрабатываемых в университетах (рост на 16 % ежегодно), способствует повышению качества подготовки кадров;

• Существенное увеличение рынка космических услуг, появление компаний реализующих новые бизнес модели, например, таких как «превратить спутниковую связь в транспорт по предоставлению мобильных услуг с использованием обычного смартфона» (табл. 6).

Таблица 6

Ключевые факторы, влияющие на развитие спутникового рынка в России

Драйверы рынка	Барьеры рынка
Значительная часть малонаселенных районов не охвачена мобильной связью	Высокая роль государства в отрасли
Увеличение предложения средств выведения малых спутников (новые ракеты)	Неразвитый рынок коммерческих космических услуг
Постепенное развитие частного сектора и рост числа университетских малых спутников (Dauria Aerospace, Спутникс, Техком, Геоскан)	Низкий уровень частных инвестиций, в том числе венчурных
Активные разработки перспективных малых спутников в классах нано- и микро-размера	Отставание российской компонентной базы от мировой
Снижение себестоимости малых спутников за счёт разработки стандартизованных платформ и серийного производства (платформы Карат, ТаблетСат и др.)	
Снижение стоимости терминального оборудования	
Появление компаний реализующих новые бизнес модели	

4.2. Активность спутниковых операторов на рынке услуг MSS

Ключевой активностью спутниковых операторов является обновление их спутниковых группировок, которые работают на орбите уже многоие годы и технологически устарели в сравнении со стремительно улучшающимися возможностями сотовых и проводных сетей данных. Например, в то время как в сотовых сетях уже возможен просмотр потокового видео высокого качества на экране смартфона, спутниковые операторы могут предложить пользователям услуг MSS обмен текстовыми сообщениями, работу с e-mail и просмотр веб страниц на скоростях сравнивых с коммутируемым доступом. Так, Iridium и Inmarsat уже начали обновление своих группировок спутниками второго поколения со значительно улучшенными характеристиками скорости передачи данных (например, у Iridium Global Xpress скорость передачи на абонентское устройство возрастет с сегодняшних 384 бит/с до 5 Мбит/с; у Inmarsat Next с 2,4 Кбит/с до 1,5 Мбит/с.

Параллельно вся большая четверка спутниковых операторов расширяет портфель абонентского оборудования, чтобы с одной стороны увеличить абонентскую базу, в том числе среди абонентов массового рынка, а с другой, чтобы повысить ARPU среди существующих абонентов. В портфеле операторов появились спутниковые Wi-Fi хотспоты (у Thuraya это адаптер для смартфона) позволяющие пользоваться спутниковой голосовой связью и интернет на многих современных смартфонах (имеющем Wi-Fi и позволяющих устанавливать специальное мобильное приложение оператора), которое выступает управляющим интерфейсом между смартфоном и технической частью спутникового хотспота (табл. 7). По оценкам Northern Sky Research, к 2022 году в мире будет продано до 150 тысяч спутниковых Wi-Fi хотспотов или 2,5% от числа пользователей услуг спутниковых MSS (табл. 7).

4.3. Инвестиции в отрасль спутниковой связи

По оценкам Inmarsat выход на международный спутниковый рынок нового оператора может занять не менее 6 лет и будет сопряжен со следующими барьерам:

• Огромные капитальные вложения необходимые для построения спутниковой сети и последующего обновления спутников (срок их эксплуатации ограничен);

• Необходимость приобретения прав на частоты в современном черезвычайно занятом частотном спектре;

• Необходимость получения позиции на орбите, которая является исчерпаемым ресурсом;

• Необходимость лицензирования услуг и абонентского оборудования в глобальном масштабе;

• Необходимость развития дистрибуции улуг и абонентского оборудования в глобальном масштабе;

• Поддержание доверия потребителей и рыночной репутации, на что требуется длительное время.

Новые компании, выходящие на рынок спутникового интернет и связи, уже заявили о привлечении более 17 млрд долл. инвестиций, запланировав вывести на орбиту более 5000 спутников связи, и планируют начать оказание услуг на массовом рынке в ближайшие несколько лет. Основной пик запусков спутников запланирован на 2020 год.

Кроме того, существующие спутниковые операторы Iridium и Inmarsat обновляют свои спутники связи более современными аппаратами второго поколения, инвестируя в это совокупно 4,5 млрд.долл на период до 2017 года. Общий объем инвестиций до 2020 года среди указанных компаний может превысить 22 млрд долл.

• **O3b Networks**

Инвестиции в размере 1,2 млрд долл., а также кредит в размере 465 млн долл. Стоит отметить, что в том числе в проекте венчурно участвует Google с инвестициями в 1 млрд долл (табл. 8).

Компания основана в 2007 году. Первый плановый запуск спутников был намечен на 2010 год, но

Таблица 7

Абонентское MSS-оборудование спутниковых операторов – Wi-Fi хотспоты (и приставка)

				
Название продукта	**Thuraya SatSleeve**	**Globalstar Sat-Fi**	**Iridium Go!**	**Inmarsat IsatHub**
Тип	Телефонный адаптер	Wi-Fi хотспот	Wi-Fi хотспот	Wi-Fi хотспот
Цена, долл.	789$	999$	875$	1300$
Размер, Вес, грамм	Мобильный 220	Стационарный 1065	Мобильный 305	Портативный 900
Батарея питания Время разгов/ожид	Встроенная 3ч/36ч	Внешний источник питания	Встроенная 7ч/16ч	Встроенная 2,5ч/8ч
Скорость передачи данных из сети	9,6 Кбит/с	9,6 Кбит/с	Сейчас 2,4 Кбит/с В Iridium Next до 1,5 Мбит/с	Сейчас 384/240 Кбит/с В Inmarsat Global Xpress до 5Мбит/с
Функции:				
• **Wi-Fi / Подключений**	нет	да, 8	да, 5	да, 10
• **Голос**	+	+	+	+
• **Интернет (IP)**	нет	нет	нет	+
• **SMS**	+	нет	+	+
• **E-mail**	+	+	+	+
• **Социальные сети**	+	нет	+	+
• **SOS сигнал**	+	нет	+	Нет
• **Caller ID**	Нет	+	+	Нет
• **Ipv65**	Нет	Нет	+	+
Особенности:	Не универсален: работает только с моделями Iphone и Samsung Galaxy	Высокое качество голоса, но обрывы соединения, включает одну внешнюю антенну и кабель,	GPS tracking, IPv65, Платформа разработчиков приложений, высокое качество голоса, но обрывы	Стандартный IP, не поддерживает Windows и Blackberry, нет порта Ethernet

был отложен до 2013 года, когда компания вывела на среднюю (8000 км) орбиту 4 спутника (вес каждого 700 кг). В 2014 году компания вывела еще 8 спутников из запланированной группировки, доведя общее число на орбите до 12 спутников. Спутники работают в Ка-диапазоне с производительностью 10 Гбит/с и задержкой доставки сигнала в 150 мс. Компания планирует увеличивать группировку до 210 спутников, запуская спутники поэтапно каждый год, пропорционально увеличению спроса.

Компания планирует обслуживать в первую очередь мобильных операторов и сервис-провайдеров, приземляя их трафик и предоставляя услуги голоса и интернет, а также массовых потребителей «…которые лишены доступа к интернет в силу их географического, политического или экономического положения».

Запуск первых 12 спутников состоялся в 2013–2014 годах.

• **Iridium Next**

Инвестиции в размере 2,9 млрд долл.

Компания обновляет свою существующую группировку спутников, выводя на малую орбиту 66 (без учета еще 6 запасных аппаратов) новых спутников весом 860 кг каждый, которые обеспечат покрытие всей поверхности Земли. Планируется обеспечение скорости в L-диапазона до 1,5 Мбит/с и до 8 Мбит/с в более высокоскростном Ка-диапазоне, что намного превосходит существующие параметры сети компании. Существующие абоненты смогут пользоваться услугами на базе новых спутников без необходимости покупки нового абонентского оборудования.

Таблица 8

Заявленные инвестиции и планы компаний по запуску новых спутников

Компания	Инвестиции, млрд.долл.	Количество спутников	Год запуска
O3b Networks	1,665	120	2013-2020+
Iridium Next	2,9	66	2015-2017
Inmarsat Global Xpress	1,6	4	2015-2016
OneWeb (WorldVu)	2,0-3	648	2018-2020
Yaliny	0,001+(0,99 план)	135	2018-2019
LeoSat	2,5-3	120-140	2019-2020
SpaceX	10	4000	2020
ВСЕГО	21,6-23,2	5113	-

Запуск спутников и обновленных услуг в 2015–2017 годах.

• **Inmarsat Global Xpress**

Ивестиции в размере 1,6 млрд долл.

Inmarsat так же обновляет свою существующую группировку спутников на более современную второго поколения – Global Xpress. Компания уже вывела на геостационарную орбиту 2 спутника из 4 планируемых в декабре 2013 года и феврале 2015 года и планирует запустить оставшиеся во втором полугодии 2015 года и в конце 2016 года. Спутники, работающие в Ка-диапазоне, разработаны на основе стандартов платформы Boeing 702HP и будут обеспечивать скорости передачи до 50 Мбит/с от спутника и до 5 Мбит/с к спутнику. Каждый спутник размером с двухэтаж-

ный автобус и весом 6,1 тонн расчитан на работу в течение 15 лет.

Запуск 4 спутников и оказание услуг в конце 2016 году.

• **OneWeb ltd. (ранее WorldVu)**

Инвестиции в размере 2-3 млрд долл., полученные от Virgin Group и Qualcomm.

Компания планирует обеспечить спутниковым интернет «сотни миллионов потенциальных пользователей в местах без ШПД интернета» посредством вывода на малые орбиты в 800 км и в 950 км группировки из 648 миниспутников. Каждый спутник будет весить до 158 кг и стоить 350 тыс. долл. Планируется серийное производство, чтобы снизить общую стоимость проекта. Запуски будут производится в период 2019–2020 годов.

Компания приобрела широкий спектр частот в Ku-диапазоне у компании SkyBridge (которая не смогла реализовать ранее аналогичный проект по спутниковому интернет и запуску 360 малых спутников) и по состоянию на январь 2015 года является единственной компанией, получившей лицензию от International Telecommunications Union среди тех компаний, кто еще не вывел спутники на орбиту.

В штате компании уже работают 30 человек инженерных специальностей.

Запуск спутников и услуг план планируется в 2018–2020 годах.

• **Yaliny**

Компания привлекает дополнительные инвестиции и для реализации всего проекта требуется около 1 млрд долл.

Компания планирует создать необходимую инвраструктуру для предоставления услуг спутниковой связи, а так же, во вторую очередь, спутникового интернет. Компания, образована россиянами и имеет центры разработки как в России, так и в США. В настоящее время штат компании насчитывает 50 человек. Компания получила частные инвестиции в размере 1 млн долл., и на данном этапе она разрабатывает и тестирует прототип спутника.

Планируется группировка из 135 спутников весом 570 кг на малой орбите и сроком эксплуатации 5-7 лет. Пользоваться услугами связи и интернет можно будет практически с любого современного смартфона подключенного к портативному спутниковому Wi-Fi хотспорту Yaliny с заявленной ценой около 100 долл. и тарифом на безлимитную голосовую связь за 10 долл. в месяц. Сеть компании будет рассчитана на подключение до 25 млн пользователей голосовых услуг.

Запуск спутников и услуг планируется в 2018–2019 годах, но полное финансирование еще не привлечено.

• **Leosat LCC**

Инвестиции в проект на уровне 2,5–3 млрд долл.

Компания планирует вывести на среднюю орбиту 1800 км группировку из 120–140 спутников Ka-диапазона и обеспечить глобальное покрытие Земли высокоскоростным интернет по доступной цене. Планируется обеспечить соединение в режиме точка-точка без приземления сигнала, в зашифрованном виде, с низкой задержкой менее 50 мс и скоростями до 1,2 Гбит/с. Предполагается использовать специальное вновь разработанное спутниковое абонентское оборудование. Компания планирует сфокусироваться на следующих сегментах рынка: морской транспорт, нефте- и газодобыча, передача трафика для сотовых операторов в режиме 4G, корпоративные спутниковые сети и как резервный канал ШПД для массовых пользователей.

Запуск спутников и услуг в 2019–2020 году.

• **SpaceX**

Инвестиции в проект на уровне 10 млрд долл. на период до 2020 года, в том числе в проекте венчурно участвуют Google и Fidelity Investments с инвестициями в 1 млрд долл.

В январе 2015 года основатель компании SpaceX, специализируйшейся на частных коммерческих космических грузоперевозках на базе собственных ракет носителей Falcon, а так же создающая элеметны солнечных батарей, объявил новую инициативу компании по разработке и запуску собственной группировки спутников для предоставления доступного по цене спутникового интернет в любой точке планеты, для сельских и развивающихся регионов, за исключением полярных областей.

Запланирована группировка из 4000 микроспутников на малой орбите до 1100 км, которые будут произведены на специально построенном заводе в Сиэтле (США) и выведены на орбиту с использованием ракет носителей компании. Для управления спутниками может быть задействована собственная система навигации и управления полетами, которая уже используется компанией для ракет Falcon. В качестве альтернативы получению частот для спутников рассматривается реализация оптическо-лазерной передачи данных. Стоимость абонентских терминалов планируется компанией в диапазоне 100–300 долл.

В штат компании уже набрано 60 инженеров, а в ближайшие 2–3 года общий штат компании может составить не менее 1000 сотрудников.

«Чтобы построить первый город на Марсе нам [SpaceX] необходимо много денег. Данный проект [спутниковый интернет] позволит нам заработать эти деньги» – объявил Элан Маск, основатель компании SpaceX, на презентации спутникового проекта.

Запуск спутников и услуг в 2020 году.

• **Венчурные инициативы Google**

Венчурные инвестиции на уровне 1 млрд долл. в совместный проект с компанией SpaceX.

Венчурные инвестиции на уровне 1 млрд долл. в компанию O3b Networks.

Посредством участия в венчурных проектах компания планирует обеспечить спутниковым интернет отдаленные районы Земли для увеличения числа пользователей ее основных сервисов. Данные проекты будут реализован наряду с существующими проектами

венчурного подразделения GoogleX по обеспечению покрытием отдаленных регионов Земли высокоскоростным интернетом с использованием воздушных шаров и дирижаблей на высотах до 32 км (Project Loon) и беспилотных дронов на солнечных батареях.

Запуск спутников – до 2020 года.

5. Выводы

Стремительное развитие телекоммуникационных технологий и компонентной базы, снижение веса, размера и стоимости спутников, снижение стоимости их вывода на орбиту, возможность организации глобального покрытия планеты в сжатые сроки, позволили спутниковым операторам, разработчикам спутниковой инфраструктуры и коммерческим и инвестиционным компаниям по-новому взглянуть на перспективы рынка спутниковой связи и интернет запуская новые амбициозные много миллиардные проекты.

Современный мировой спутниковый рынок оценивается в 201 млрд.долл. При этом на долю спутниковых услуг приходится более 60% доходов рынка. Услуги подвижной спутниковой связи и интернет (MSS) занимают в общей структуре 1,4% доходов рынка или 2,8 млрд долл. и будут расти в среднем минимум на 5% в год в ближайшие 5 лет. Количество пользователей спутниковых услуг MSS возрастет с сегодняшних 2,9 млн. до почти 6 млн. пользователей.

К концу этого рассматриваемого периода, в 2019–2020 годах, ожидается выход на спутниковый рынок сразу нескольких новых игроков, ориентированых главным образом на массового потребителя, которые вероятно существенно изменят расстановку сил на рынке. Уже сейчас совокупные инвестиции в построение новых спутниковых группировок из тысяч спутников заявлены на уровне более 21 млрд долл. Крупные компании в числе Google, Virgin Group, Qualcomm, SpaceX обозначили свое участие самостоятельно, либо венчурно, в спутниковых проектах с одинаковыми целями: обеспечить новых потребителей, отдаленные и неохваченные связью районы Земли доступным спутниковым интернет и связью. Одни – с целью увеличения числа пользователей своих основных сервисов, другие – для получения прямого дохода от спутниковых услуг.

Существующие спутниковые операторы Iridium и Inmarsat осуществляют обновление своих группировок запуская спутники второго поколения, которые должны обеспечить существенный рост скорости передачи данных и качество услуг конечных пользователей.

Все операторы большой четверки расширили портфель своего абонентского оборудования для массового рынка портативными спутниковыми Wi-Fi хотспотами (Thuraya запустила приставку), которые позволят получать услуги спутниковой связи используя обычный современный смартфон. Данная тенденция является новым направлением развития, который будут усиливать и развивать вновь создаваемые компании все больше приближая спутниковую связь к массовому потребителю.

Лидером на спутниковом рынке является США. На их долю приходится большая часть производимых и запускаемых спутников (41%), большая часть всех доходов мирового рынка от спутниковых услуг (44%) и они сохранят и упрочат это лидерство в анализируемой перспективе. Учитывая специфику спутниковых технологий он смогут предоставлять услуги спутниковой связи и интернет в любой точке планеты и любому потребителю.

ВУС

Военно-учетный стол

Программный комплекс

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

Воинский учет в организациях:

• Ведение электронных Картотек организаций, филиалов и граждан (по Т-2 и Т-2 ГС);

• Документы необходимые для ведения ВУ в организации (приказ, план работы, журнал проверок, расписки о приеме документов ВУ и др.);

• Создание и печать отчетных документов по установленным формам в соответсвии с Инструкцией ГШ ВС РФ по ведению ВУ в организациях;

• Генерация документов по бронированию.

Первичный воинский учет в органах местного самоуправления:

• Ведение Картотеки организаций зарегистрированных на территории ОМСУ;

• Построение и управление картотекой граждан пребывающих в запасе и призывников в ОМСУ;

• Создание отчетных форм документов и других данных в соответствии с Методическими рекомендациями ГШ ВС РФ по ведению первичного ВУ в ОМСУ;

• Распределение организаций ведущих учет ГПЗ по видам экономической деятельности, формам собственности и численности работающих в ней граждан.

Учет и Бронирование в Межведомственных комиссиях:

• Организация картотеки различных органов РФ от правительства до организации включительно с различными формами учета и отчетности, ведение структуры подчиненности;

• Автоматический расчет форм №6,формы №18 расчет и обобщение суммарной формы №6 за все подотчетные объекты;

• Анализ обеспеченности трудовыми ресурсами;

• Ведение перечня должностей и профессий по бронированию граждан;

• Определение сотрудников подлежащих бронированию, бронирование сотрудников в соответствии с ПДП;

• Заполнение, передача, сбор и обобщение форм ГД.

НПЦ ИРС

Научно-производственный центр
Информационных региональных систем

npcirs.ru

ПРЕДМЕТНАЯ ОБЪЕКТНАЯ ГРАФИЧЕСКАЯ МОДЕЛЬ ЭЛЕКТРИЧЕСКИХ СХЕМ РАДИОЭЛЕКТРОННОЙ АППАРАТУРЫ

Курчидис Виктор Александрович,
д.т.н., профессор, профессор кафедры автоматики (и вычислительных средств) Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, idahmer2@yandex.ru

Анисимов Олег Витальевич,
к.т.н., доцент, доцент кафедры автоматики (и вычислительных средств) Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, qwaker@inbox.ru

Попов Тимур Александрович,
заместитель начальника научно-исследовательского отдела Ярославского высшего военного училища противовоздушной обороны, г. Ярославль, Россия, popov_ta@mail.ru

Ключевые слова:
электрическая схема, фреймовая модель, предметная объектная модель, графическая объектная модель, паттерн, восстановление радиоэлектронной аппаратуры.

АННОТАЦИЯ

Эксплуатация современных сложных технических комплексов требует от обслуживающего персонала не только навыков по использованию изделий по назначению, но и их техническому обслуживанию и восстановлению в связи с необходимостью поддержания таких систем в работоспособном состоянии. Это определяет важную роль, которая отводится системам информационной поддержки обслуживающего персонала для решения совокупности задач технической эксплуатации с использованием комплекта электрических схем радиоэлектронной аппаратуры.

Одним из направлений развития средств автоматизации в части информационной поддержки обслуживающего персонала при использовании электрических схем является совершенствование средств автоматизации, связанных с предоставлением необходимых схемных фрагментов для извлечения требуемой технической информации в процессе восстановления радиоэлектронной аппаратуры. Развитие соответствующих средств представляет собой актуальную научную задачу, решение которой позволяет использовать концептуальные интерфейсы при построении систем информационной поддержки процесса восстановления радиоэлектронной аппаратуры.

В работе рассматривается решение задачи по преобразованию фреймовой модели, формирующей представление элементов электрических схем в понятиях и терминах предметной области, в графическое описание. Предлагаются две модели: предметная объектная модель радиоэлектронной аппаратуры и графическая объектная модель электрических схем, совместное применение которых направлено на обеспечение согласования графического представления элементов радиоэлектронной аппаратуры на схемах с предметными понятиями, что необходимо для организации высокоуровневых интерфейсов обслуживающего персонала.

Предлагаемые формальные модели радиоэлектронной аппаратуры и электрических схем позволяют создавать высокоуровневые информационные интерфейсы обслуживающего персонала на основе естественно-подобных языков для систем автоматизации технической эксплуатации. Это способствует повышению уровня автоматизации систем информационной поддержки обслуживающего персонала и сокращению времени решения прикладных задач технической эксплуатации изделий радиоэлектронной аппаратуры сложных технических комплексов.

Полученный результат целесообразно рассматривать в качестве методологической основы построения концептуальных интерфейсов на основе естественно-подобных языков для систем информационной поддержки обслуживающего персонала в процессе технической эксплуатации радиоэлектронной аппаратуры.

Комплекты электрических схем на радиоэлектронную аппаратуру (РЭА) являются одним из основных информационных ресурсов, используемых обслуживающим персоналом при восстановлении зенитного ракетного вооружения. При выполнении операций по восстановлению РЭА обслуживающий персонал работает с фрагментами электрических схем, содержащих необходимую техническую информацию. Предоставление соответствующих фрагментов электрических схем осуществляется на системы информационной поддержки (СИП) по запросам обслуживающему персоналу (ОП). Основой для представления в СИП электрических схем в терминах и понятиях предметной области может выступать фреймовая модель ФМ РЭА, описанная в работе [1].

Фреймовая модель, обеспечивая высокоуровневое описание РЭА, не содержит средств, которые предназначены для графического представления РЭА в виде электрической схемы. В данной работе для устранения указанного недостатка ФМ предлагается разработать две модели: предметную объектную модель РЭА (ПОМ) и графическую объектную модель электрических схем РЭА (ГОМ). Совместное применение этих моделей направлено на обеспечение согласования графического представления элементов РЭА на схемах с предметными понятиями, что необходимо для организации высокоуровневых интерфейсов ОП.

Формирование моделей ПОМ и ГОМ представляет собой самостоятельную задачу, которая требует учета и взаимного согласования целого ряда следующих аспектов:

предметного представления РЭА в виде фреймовой ФМ РЭА,

графического представления электрических схем РЭА в графических системах,

графического представление электрических схем в соответствии с правилами ЕСКД,

соответствия принципам объектно-ориентированного подхода.

Решение рассматриваемой задачи, с одной стороны, требует выделения из фреймовой модели ФМ РЭА элементов, имеющих законченный предметный смысл (блок, ячейка, разъем, маркировка, позиционное обозначение и т.п.), а с другой стороны, выделения на электрической схеме РЭА графических элементов, несущих смысловую предметную нагрузку.

В соответствии с принципами объектно-ориентированного подхода [2] выделение таких элементов целесообразно выполнять в виде объектов, что определило название обоих вышеназванных моделей.

Формирование предметной объектной модели радиоэлектронной аппаратуры

Построение предметной объектной модели (ПОМ) начинается с формирования фреймов-прототипов, определяющих на основе ФМ РЭА структуру классов, являющих основой для формирования множества объектов, соответствующих представлению радиоэлектронной аппаратуры в ФМ РЭА [1]. Исходными данными для этого является множество фреймов, образующих фреймовую модель ФМ РЭА. Каждый из фреймов необходимо поставить в соответствие одному из трех типов фреймов: фрейм-экземпляр Φ^1, фрейм-роль Φ^2 или фрейм-сценарий Φ^3. В соответствии с этим целесообразно определить три типа фреймов-прототипов $\Phi^1_П$, $\Phi^1_П$ и $\Phi^1_П$ (рис. 1).

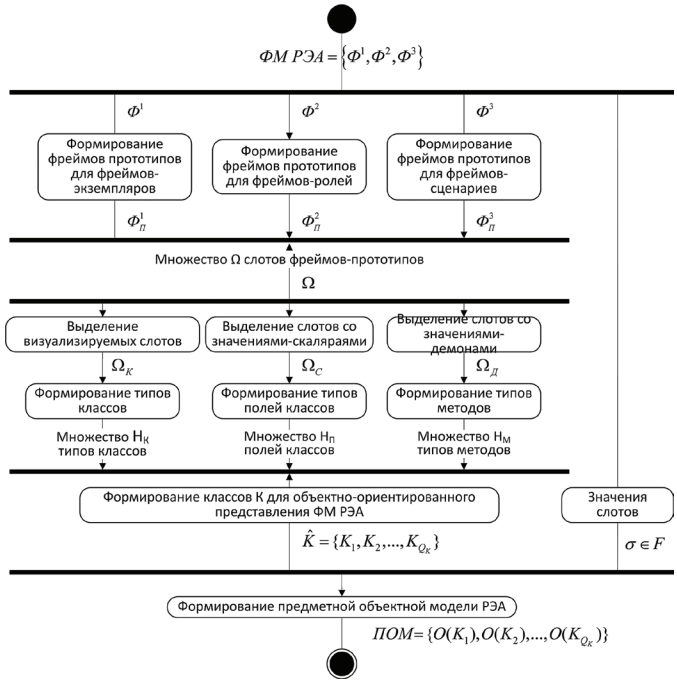

Рис. 1. UML-представление способа формирования предметной объектной модели РЭА

Для формирования множеств фреймов-прототипов $\Phi^i_П$ (i = 1,2,3) производится разбиение множеств Φ^i (i = 1,2,3) по группам фреймов (блок, разъем, контакт, функция, сигнал, цепь и т.д). Далее для каждой группы фреймов k определяется соответствующий фрейм-прототип $F^i_{Пк}$ путем объединения слотов всех фреймов k-ой группы: $F^i_{Пк} \in \Phi^i_П (i = 1,2,3;\ k = 1,2,\ ...,\ \xi_{Пi})$. Количество создаваемых фреймов-прототипов и количество слотов в них определяется общей структурой фреймовой модели ФМ РЭА.

Ниже в таблице 1 продемонстрировано применение такого подход на примере формированию фрейма-прототипа $F^1_{П(Ячейка)}$ для описания предметного понятия «Ячейка» соответствующего схемного элемента «Ячейка».

На основе совокупности фреймов-прототипов $\Phi^1_П$, $\Phi^1_П$ и $\Phi^1_П$ формируется объединенное множество $\Omega = \{\sigma_1, \sigma_2, ..., \sigma_M\}$ слотов по следующему правилу:

$$\Omega = \sigma(\Phi^1_П) \cup \sigma(\Phi^2_П) \cup \sigma(\Phi^3_П) \qquad (1)$$

где $\sigma(\Phi^i_П)$ – набор всех слотов фреймов-прототипов $\Phi^i_П$.

Таблица 1

Фреймы ячеек РЭА				Фрейм-прототип «Ячейка»
Я05А	**ДЩ2**	**Я11А**	**...**	$F^1_{П(Ячейка)}$
Имя фрейма	Имя фрейма	Имя фрейма	...	Имя фрейма
Название	Название	Название	...	Название
Маркировка	Маркировка	Маркировка	...	Маркировка
Позиционное обозначение	Позиционное обозначение	Позиционное обозначение	...	Позиционное обозначение
Уровень	Уровень	Уровень	...	Уровень
Индикатор	-	-	...	Индикатор
Разъем	Разъем	Разъем	...	Разъем
Обозначение цепи	Обозначение цепи	Обозначение цепи	...	Обозначение цепи

Дальнейший анализ совокупности слотов Ω направлен на их классификацию в соответствии с принципами объектно-ориентированного подхода. Для этого множество Ω разбивается на три подмножества:

Ω_B – совокупность слотов, которые имеют визуализируемое представление на электрических схемах (надпись, позиционное обозначение, маркировка, разъем, ячейка и т.д.),

Ω_C – совокупность слотов-скаляров, которые не используются при визуализации электрических схем (тип сигнала, название функции, название функциональной задачи и т.д.),

$\Omega_Д$ – совокупность слотов, значениями которых являются демоны (демон ЦПС, демон ЦЗС и т.д [1]).

Следуя принципам объектно-ориентированного подхода, на основе множества слотов Ω_B целесообразно сформировать совокупность H_K типов классов. Множество слотов Ω_C определяет совокупность $H_П$ полей классов, а множество слотов-демонов $\Omega_Д$ – совокупность H_M типов методов классов.

Проведенная классификация упорядочивается представлением, определяемым фреймовой модель ФМ РЭА, которое для каждого типа класса определяет соответствующие поля и методы, задающие структуру каждого типа класса. Это позволяет сформировать множество классов $\hat{K}=\{K_1, K_2, ..., K_{Q_K}\}$, которые определяют предметное описание РЭА, соответствующее объектно-ориентированному подходу к декомпозиции ФМ РЭА.

Для формирования предметного объектно-ориентированного представления РЭА с каждым фреймом $F \in ФМ\ РЭА$ сопоставляются соответствующие классы $K(F) \subseteq \hat{K}$ и производится заполнение полей этих классов значениями, определяемыми слотовой структурой фрейма F. В результате на основе каждого из классов $K_j \in \hat{K}$ формируется множество объектов $O(K_j)$, которые в совокупности образуют предметную объектную модель (ПОМ), адекватную фреймовой модели РЭА:

$$ПОМ = O(K_1) \cup O(K_2) \cup, ..., O(K_{Q_K}). \quad (2)$$

Каждое множество $O(K_j)$ определяет не только некоторый набор объектов, но также и предметное значение этого объекта в соответствии с типом класса. Учитывая, что в этой записи $O(K_j)$ является множеством объектов, целесообразно использовать другую форму записи ПОМ, отражающую объектное представление ФМ РЭА:

$$ПОМ=\{o_1, o_2, ..., o_m\}, \quad (3)$$

При этом m обозначает общее число различных созданных объектов $o_m=\overline{1,m}$ в модели ПОМ, так, что $m=cardinal(\bigcup_{j=1}^{Q_1} O(K_j))$, где *cardinal* – количество элементов множества.

Таким образом, использование двух форм (2) и (3) записи ПОМ определяет не только объектное представление, но также задает соответствие между объектами модели и предметными понятиями, связанными с этими объектами. Предлагаемый способ представления фреймовой модели ФМ РЭА при использовании средств автоматизации обеспечивает возможность работать с объектами в терминах предметной области. Однако этого недостаточно для определения графического представления элементов, определяемых соответствующими предметными схемными понятиями, так, что требуется разработка графической объектной модели электрических схем РЭА.

Формирование графической объектной модели электрических схем радиоэлектронной аппаратуры

В СИП для представления электрических схем используются базовые графические элементы, которые предоставляются графическими системами средств автоматизации и которые в соответствии с ГОСТ 27459-87 и ГОСТ 27817-88 называются примитивами вывода (ГП). Например, в графической системе Microsoft Visio такими базовыми элементами является надпись, линия, прямоугольник, отрезок и т.д [3].

Правила построения электрических схем S, изложенные в нормативных документах ЕСКД, являются основой для определения множества примитивов вывода $ГП(S) \in ГП$, которые целесообразно использовать при визуализации электрических схем РЭА в СИП.

Для визуализации электрических схем ниже предлагается использовать объектное представление схемных элементов на основе паттернов. В литературе термином «паттерн» обозначают повторяющийся шаблон, образец [4]. Термин «паттерн» широко используется в графике, математике, программировании [4–6]. Паттерн следует рассматривать как шаблон (виджет), предназначенный для визуального представления предметных понятий, соответствующих структурным элементам на электрических схемах. Использование паттернов позволяет обеспечить согласование объектов ПОМ РЭА с примитивами вывода, определяемыми возможностями графической системы СИП.

При определении паттернов необходимо каждое предметное понятие, определяющее поле класса, представить в виде объекта, который выступает в качестве основы для формирования графических единиц визуализации схемных объектов. В соответствии с этим всякий паттерн формально можно представить в виде двухэлементного кортежа:

$$\pi = \langle O(\pi), ГП(S) \rangle . \quad (4)$$

В структуре (4) паттерна π одновременно отражены два аспекта схемных элементов – предметный и графический. Предметный аспект в структуре паттерна представляется набором $ГП(\pi)$ объектов ПОМ, а графический – набором примитивов вывода.

Паттерны формируются для каждого типа схемных элементов с учетом их предметного объектного описания в ПОМ и используемых графических примитивов вывода. Например, такие объекты ПОМ, как «Маркировка», «Позиционное обозначение», «Название» и другие, которые на электрических схемах представляются в виде надписей, целесообразно представить в виде графического примитива $ГП_{Текст}$. Такие объекты, как «Кабель» и «Шлейф», на электрических схемах представляются в виде линий, и их можно представить в виде графического примитива $ГП_{Линия}$. Объекты типа «Блок» и «Ячейка» на электрических схемах визуально представляются в виде прямоугольника и для таких объектов целесообразно использовать примитив вывода $ГП_{Прямоугольник}$.

Разнообразие графических примитивов определяется видом и сложностью визуализируемого объекта. При этом одни и те же примитивы могут использоваться при построении паттернов разных объектов. С другой стороны, создание паттернов объектов может требовать использования собственных уникальных графических примитивов вывода. Таким образом, для каждого объекта ПОМ должны быть определены соответствующие графические примитивы вывода. Совокупность всех различных используемых графических примитивов вывода образует графическую объектную модель электрических схем $ГОМ = \{ГП_1, ГП_2, ..., ГП_L\}$.

Определяя графические примитивы вывода, соответствующие объектам ПОМ, можно сформировать множество паттернов, совокупность которых образует предметно-ориентированное графическое описание $\hat{\pi} = \langle \pi_1, \pi_2, ..., \pi_B \rangle$ радиоэлектронной аппаратуры, которое целесообразно представить в виде предметно-графической объектной модели ПГОМ. Эта модель образуется объединением моделей ПОМ и ГОМ, что формально можно записать следующим образом:

$$ПГОМ = \langle ПОМ, ГОМ \rangle. \quad (5)$$

Паттерны можно комбинировать для представления фрагментов электрических схем. При этом предлагается использовать иерархический принцип структуризации паттернов, означающий, что во всяком паттерне можно использовать графические примитивы структурных схемных элементов, являющихся классами ПОМ, которые имеют собственные паттерны.

На рис. 2 иллюстрируется принцип формирования паттерна «Ячейка» $\pi_{ячейка}$ в соответствии с описанием схемного элемента «Ячейка», приведенным в ПОМ (Таблица 1). Предметную объектную основу паттерна «Ячейка» составляют такие объекты, как: название (O_1), позиционное обозначение (O_2), маркировка ячейки (O_3), маркировка разъема (O_4), разъем (O_5), название индикатора (O_6), индикатор (O_7). Графическую объектную основу паттерна «Ячейка» составляют графические примитивы для представления паттернов схемных элементов «Разъем» ($ГП_{Разъем}$) и «Индикатор» ($ГП_{Индикатор}$), а также графические примитивы текст ($ГП_{Текст}$) и прямоугольник ($ГП_{Прямоугольник}$).

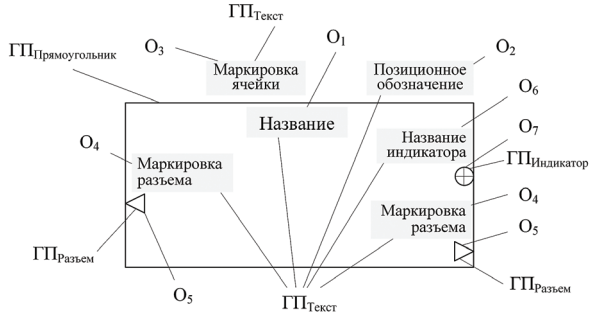

Рис. 2. Элементы графического паттерна «Ячейка»

В соответствии в иерархическим принципом структуризации паттернов, сформулированным выше, в паттерне «Ячейка» использованы два графических примитива $ГП_{Разъем}$ и $ГП_{Индикатор}$, соответствующих структурным схемным элементам «Разъем» и «Индикатор», которые являются классами ПОМ. Это означает, что каждый из этих структурных схемных элементов имеет собственный паттерн (рис. 3).

Подобным образом могут быть сформированы и структурированы паттерны для других понятий. В качестве примера ниже приведен паттерн «Цепь» (рис. 4), в котором также используются графические примитивы элементов электрических схем, имеющих собственные паттерны.

Предоставление обслуживающему персоналу возможности работать с электрическими схемами в понятиях и терминах предметной области следует рассматривать, как эффективный путь развития средств автоматизации СИП. Совместное применение моделей ПОМ и ГОМ в форме предметной графической модели ПГОМ позволяет согласовать графическое представление и понятийное описание электрических схем РЭА для использования в системах информационной поддержки ОП. Представленные модели ПОМ и ГОМ в совокупности определяют набор средств, которые хорошо согласуются с принципами объектно-ориентированного подхода к описанию информационно-программных компонентов современных систем автоматизации.

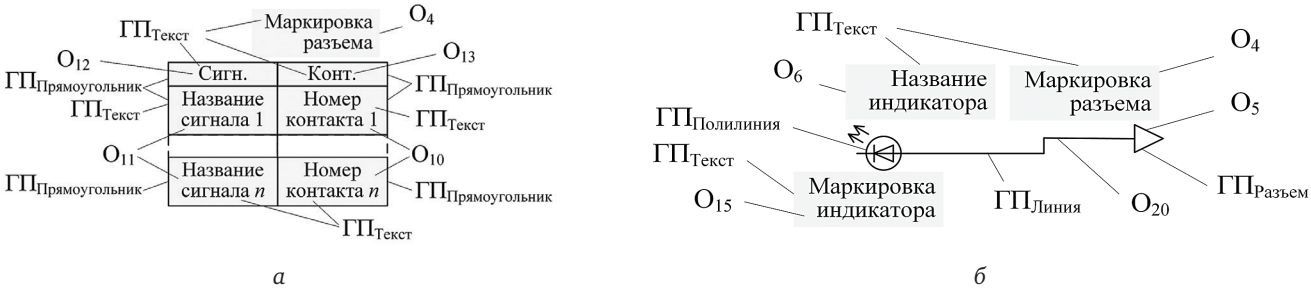

Рис. 3. Графические паттерны для схемных элементов «Разъем» (*а*) и «Индикатор» (*б*)

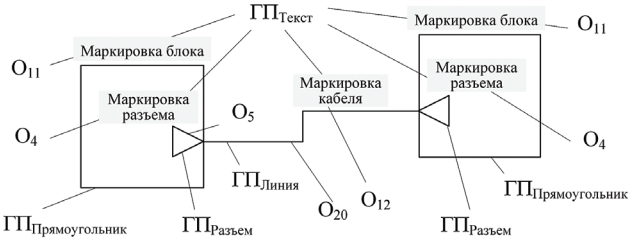

Рис. 4. Графический паттерн «Цепь»

Разработанные модели ПОМ и ГОМ можно рассматривать, как основу для организации интеллектуализированных интерфейсов в СИП, которые обеспечивают обслуживающему персоналу новые возможности по извлечению и предоставлению технической информации при работе с электрическими схемами в процессе восстановления РЭА. Особенностью предлагаемых интерфейсов является их высокая информативность за счет использования высокоуровневых понятий предметной области, что позволяет сократить число запросов ОП к СИП, а, соответственно время восстановления РЭА за счет уменьшения времени на извлечение требуемой технической информации.

Литература

1. Анисимов О.В., Курчидис В.А., Попов Т.А. Концептуальное представление электрических схем радиоэлектронной аппаратуры на основе фреймовой модели // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 2. С. 20–28.

2. Грэди Буч и др. Объектно-ориентированный анализ и проектирование с примерами приложений (3-е издание).: Пер. с англ. М.: Вильямс. 2010. 720 с.

3. Леонтьев Б. Microsoft Visio 2002 Professional. Построение проектов, диаграмм и бизнес-схем в ОС Microsoft Windows XP. М.: СОЛОН-Р. 2002. 512 с.

4. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж. Приемы объектно-ориентированного проектирования. Паттерны проектирования. СПб: «Питер». 2007. 366 с.

5. Фримен Э., Фримен Э., Сьерра К., Бейтс Б. Паттерны проектирования // O'Relly. СПб: «Питер». 2007. 656 с.

6. Patterns of Enterprise Application Architecture. Martin Fowler. Addison-Wesley. Boston. 2002. 560 p.

Для цитирования:
Курчидис В.А., Анисимов О.В., Попов Т.А. Предметная объектная графическая модель электрических схем радиоэлектронной аппаратуры // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 38–43.

SUBJECT OBJECT GRAPHICAL MODEL OF ELECTRIC SCHEMES RADIO ELECTRONIC EQUIPMENT

Kurchidis Victor Aleksandrovich,
Yaroslavl, Russian, idahmer2@yandex.ru

Anisimov Oleg Vitalyevich,
Yaroslavl, Russian, qwaker@inbox.ru

Popov Timur Aleksandrovich,
Yaroslavl, Russian, popov_ta@mail.ru

Abstract
One of the ways of improving the efficiency of solving problems in exploitation of complex technical systems is the use of automation. The existing means of automation do not provide service personnel with opportunities to build requests for the required information in the form of fragments of electrical schemes using concepts and terms in the subject domain within the syntax of natural-like language.
The work is dedicated to the development of the predicate model of requests, focused on the use of concepts and terms in the subject domain in the formation of the target conditions by service personnel to represent the requested fragments of schemes. Such requests are called in the scheme-oriented. It is offered to record the properties of elements, which are involved in the determination of the conditions, in the form of the relationship between the subject terms. The basic relationship that corresponds to the structural elements of the electrical schemes and are defined in framing conceptual model of radio-electronic equipment are reveled. The conditions asked by service personnel, which must correspond to the elements of electric schemes that are displayed in the form of widgets, are defined. The use of first-order predicate logic within the syntax of natural language is proved to form the target conditions of the requests in terms and concepts of electrical schemes of electronic equipment. The offered formalized structure of the scheme-oriented requests allows coordinating the predicate formulas with the structure of the natural language sentences.
The offered predicate model is characterized by requests that are formed based on the sentences in the natural-like language. In this case, it is possible to use those terms and concepts in the subject domain in requests, as well as to produce coordination of the used words in cases and single/plural forms.
This result is reasonable to consider as a methodological basis for constructing conceptual interfaces based on natural-like language for systems of information support for service personnel in the technical exploitation of electronic equipment. This increases the level of automation of information support for service personnel and reduces the time of solving the applied problems of technical exploitation of radio-electronic equipment in complex technical systems.

Keywords: Electrical scheme, frame model, subject object model, graphic object model, pattern, recovery of radio electronic equipment.

References

1. Anisimov O.V., Kurchidis V.A., Popov T.A. Conceptual representation of electrical schemes electronics based on frame model. H&ES Research. 2015. Vol. 7. No. 2. Pp. 20–28. (in Russian).
2. Grady B. & [et al]. Ob'ektno-orientirovannyy analiz i proektirovanie s primerami prilozheniy (3-e izdanie) [Object-Oriented Analysis and Design with Application'/3rd ed]. Moscow: Viliams. 2010. 720 p. (in Russian).
3. Leontiev B. Microsoft Visio 2002 Professional. Postroenie proektov, diagramm i biznes-skhem v OS. Microsoft Windows XP. [Microsoft Visio 2002 Professional. Construction projects , diagrams and business schemes in the OS Microsoft Windows XP]. Moscow: SOLON-R. 512 p. (in Russian).
4. Gamma E., Helm R., Johnson R., Vlissides J. Priemy ob'ektno-orientirovannogo proektirovaniya. Patterny proektirovaniya [Design Patterns: Elements of Reusable Object-Oriented Software]. SPb: Piter. 2007. 366 p. (in Russian).
5. Freeman E., Freeman E., Sierra K., Bates B., Robson E., Patterny proektirovaniya /O'Relly [Design Patterns / O'Relly]. SPb: Piter. 2007. 656 p. (in Russian).
6. Martin Fowler, 2002, Patterns of Enterprise Application Architecture. Addison-Wesley. Boston. 560 p.

Information about authors:

Kurchidis V.A., Ph.D., professor, professor Automation (and computing devices), Yaroslavl higher military shcool of air defense;
Anisimov O.V., Ph.D., associate professor, docent Automation (and computing devices), Yaroslavl higher military shcool of air defense;
Popov O.V., deputy head of Department scientific research, Yaroslavl higher military shcool of air defense.

For citation:
Kurchidis V.A., Anisimov O.V., Popov O.V. Subject object graphical model of electric schemes radio electronic equipment. H&ES Research. 2015. Vol. 7. No. 5. Pp. 38–43. (in Russian).

ИССЛЕДОВАНИЕ РАСПРЕДЕЛЕННОЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ АДАПТИВНОГО ДЕЙСТВИЯ

Виткова
Лидия Андреевна,
аспирант Санкт-Петербургского Государственного университета телекоммуникаций имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия
lidia@iskin.spb.ru

Ключевые слова:
распределенная компьютерная система, сеть однозначного отождествления, искусственная иммунная система, система предотвращения вторжений, IDS, IPS, GRID, Botnet, экспертная система.

АННОТАЦИЯ

Рассматривается возможность применения алгоритмов искусственных иммунных систем для создания распределенной сети. Описывается базовый механизм защиты иммунитета человека. Далее анализируются существующие технологии, которые были основаны на механизмах иммунитета. Выбираются системы предотвращения вторжений, как отправную точку. Для этого дается краткий обзор алгоритмов распределенных, параллельных вычислений.

Работа состоит из нескольких разделов; при этом раздел «анализ» посвящен анализу существующих решений, а также поиску путей для децентрализации компьютерных сетей и их защите. В рамках эксперимента разрабатывалась программа управления для архитектора распределенной сети. Программный продукт работает как в Windows, так и в Unix системах.

Прогнозируется, что в сети будет функционировать алгоритм индексационных серверов первого и второго правового уровня доступа, каждый из которых отвечает за обновление и взаимодействие с другими подсетями. Один из серверов становится привилегированным и получает доступ к экспертным системам.

Для защиты канала связи в процессе обновления предлагается использовать защищенное соединение SSL, а для защиты системы в целом использовать метод стеговложения. Для стего преобразований оптимален исполнимый файл формата ELF. Избыточность можно использовать для скрытого вложения информации в исполняемый код, не нарушая при этом функциональность.

Несмотря на большое количество исследований и работ в данной области, автор видит потребность в новых алгоритмах взаимодействия, протоколах и адаптивных способах защиты подсетей. Существующие алгоритмы распределенных компьютерных сетей используют протокол P2P, что делает архитектуру менее гибкой и накладывает собственные ограничения. В данном случае требуется внедрение собственного опросного протокола по аналогии с алгоритмом master browser в среде Windows.

Введение

Масштабное распространение сетевых технологий и устройств в современном обществе требует поддержания высокого уровня информационной безопасности. При этом, несмотря на развитие новых технологий, и алгоритмов защиты наблюдается рост успешности сетевых атак. Современные системы обнаружения (IDS) и предотвращения (IPS) вторжений фокусируются на гарантированном выявлении и блокировке вредоносной сетевой активности в реальном времени, аналогией IDSи IPS систем стала иммунная система человека, так как это, прежде всего:

– высокий уровень защиты от патогенов;

– самоорганизуемая система;

– распределенный и децентрализованный механизм управления с возможностью адаптации.

Необходимо отметить, что системы обнаружения вторжений по-прежнему не в состоянии эффективно работать с динамичными и более сложными компьютерными системами. Именно поэтому были успешно реализованы алгоритмы искусственных иммунных сетей в рамках проектов по предотвращению вторжений, то есть IPS системы. Отметим, что при делении на виды IPS используется классификация, наследованная от систем обнаружения вторжений, и таким образом продукты делятся на «сетевые» и «хостовые» [1].

Сегодня сетевая IPS является неким программно-аппаратным устройством или программой, которая работает на пути сетевого трафика. Главная задача – это защита хостов сети от атак путем анализа проходящего трафика и его блокировки в случае угрозы. При этом хостовая IPS привязана к одному конкретному хосту и также анализирует трафик, следит за приложениями и активируемыми системными вызовами. Успешных реализаций довольно много, есть коммерческие продукты, но также доступны и бесплатные решения для самостоятельной настройки и доработки. Примером такого продукта является «SELinux» с исходным кодом, доступным для скачивания.

В данной работе рассматривается задача построения IPS системы, в которой будет реализован один из механизмов иммунной системы, а именно – распределенное управление, децентрализация и адаптация. Автор видит актуальность решения данной задачи в том, что количество хостов в сетях в какой-то момент времени становится настолько большим, что централизованность системы защиты уже сама по себе является одним из ее самых уязвимых мест. В рамках разрабатываемого проекта учитывается потребность в автономности, самоадаптивности, самоконтроле и само-исцелении системы защиты в пределах подсетей и хостов.

Анализ

Человеческая иммунная система является многогранной сетью из органов и клеток, которая отвечает за реализацию двух следующих основных механизмов защиты организма от патогенов. Во-первых, это врожденный иммунитет, а во-вторых – работа адаптивной иммунной системы. Более того, иммунная защита имеет многоуровневую архитектуру. Первым и самым элементарным барьером является кожа, вторым – физиологические реакции (pH, температура). Как только возбудитель проникает через барьеры и попадает в организм, это приводит к обратной реакции системы врожденного и приобретенного иммунитета. Алгоритм распознавания иммунной системы лежит в основе большинства существующих разработок в сфере информационной безопасности. В рамках текущего проекта производится выбор наиболее успешных алгоритмов и их последующая адаптация.

Для решения подобных задач в рамках информационной безопасности или децентрализации, ряд исследователей прилагал большие усилия, стремясь повысить гибкость, масштабируемость систем обнаружения и предотвращения вторжений. Жизнеспособными аналогиями иммунной системы являются алгоритмы агентных сетей и отрицательного отбора. Агентные технологии были применены в системах обнаружения неисправностей сетей в 2007-2010 [2], в GRID вычислениях и в системах тестирования [3]. А алгоритмы отрицательного отбора используются для обнаружения аномалий и вторжений [4, 5], а также в других проектах по компьютерной безопасности [6].

Обратим внимание на то, что в процессе разработки агентных сетей более детально обсуждались вопросы параллельности, распределенности вычислений и программирования. В теоретической части работы автор отталкивается от того, что параллельное и распределенное вычисленияи другие процессы в сетях как базовые понятия не являются эквивалентами. Параллельность процессов обработки данных означает, что процессы выполняются одновременно, а распределенность – что они осуществляются удаленно друг от друга и не обязательно являются параллельными процессами [7].

В процессе анализа было выделено два решения: сети GRID и Botnet-ы. Но «ГРИД-вычисления» (GridComputing) – это форма сетевого вычисления, при помощи которой объединяют все компьютеры распределенной компьютерной сети (РКС) в единую вычислительную машину. Это позволяет исследователям распределять и перераспределять ресурсы между пользователями в соответствии с их возможностями и доступностью. В основе решения лежит аналогия распределенности в иммунной системе, но данный алгоритм разрабатывался больше для параллельного программирования, чем для децентрализации как таковой.

Таким образом, в рамках работы по поиску оптимального алгоритма автор больше уделил внимания реализованным злоумышленниками сетям Botnet. Известно, что по своей сути Botnet – это именно РКС, которая состоит из некого количества удаленных хостов с запущенным на них автономным программным обеспечением. В более ранних решениях Botnet были

централизованными, и лишь в дальнейшем произошло обновление до децентрализованного алгоритма.

Структура таких сетей такова, что каждый хост поддерживает соединение с другим хостом; при этом в Botnet системах отсутствует явный (видимый) центральный сервер, который бы управлял распределенной сетью. В основу данного алгоритма была положена архитектура P2P. И одним из первых решений, использующих P2P сети, стал Botnet Storm. Он появился в поле зрения вирусных аналитиков в 2007 году. В нем для построения и децентрализации сети был использован опросный протокол overnet и новый механизм обновления ПО. Важно, что именно последний и стал той «ахиллесовой пятой», который позволил остановить Botnet Storm [8]. Таким образом, необходимость защиты пакетов обновления от перехвата, модификации и копирования также актуальна.

Сегодня помимо чистых P2P-сетей существуют и гибридные. В таких сетях используются хосты (сервера) для координации работ, поиска или предоставления информации о ПК в сети и их статусе (on-line, off-line и т.д.). Гибридные сети успешно сочетают скорость централизованных сетей и надёжность децентрализованных благодаря гибридным схемам с независимыми индексационными серверами, синхронизирующими информацию между собой. При выходе из строя одного или нескольких серверов сеть продолжает функционировать.

В рамках проекта по разработке распределенной сети однозначного отождествления расставим следующую очередность решения задач: 1) сравнительный анализ готовых успешных решений и алгоритмов; 2) разработка архитектуры и прототипа системы; 3) подготовка панели управления для ПО; 4) внедрение механизмов защиты от перехвата, копирования и модификации; 5) разработка системы взаимодействия подсетей и хостов; 6) разработка алгоритма взаимодействия баз данных подсетей и хостов.

Рассмотрим далее прототип реализации программы ЭВМ для панели управления (настройки).

Синтез

Рассмотрим существующие системы предотвращения вторжений (рис. 1).

Схема на рис. 1 состоит из следующих элементов:

1. AD, Network, IM, End point, Program Sniffer & Mirror Switch –элементы сети;

2. Data Base, Center– элемент серверных станций;

3. Alert & Program Center –элемент ПО;

4. Sys Admin & Sec. Officer –элемент управления.

Системы действительно устойчивы, но весь модуль управления остается под контролем человека и под его ответственностью, таким образом, исключая любую децентрализованность и адаптивность (которая необходима в современных системах). Возможно функционирование подсетей в рамках существующих, переданных в пользование баз данных, но при столкновении с модифицированным вирусом или сложной сетевой

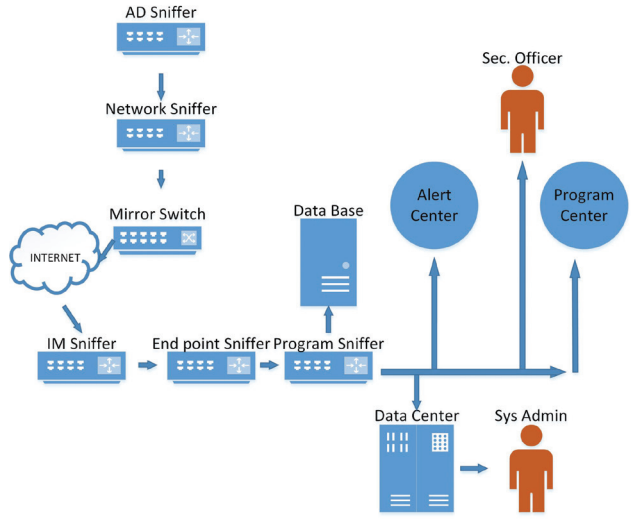

Рис. 1. Схема систем предотвращения вторжений

атакой система сможет только выявить нездоровую активность и сообщить об этом в центр управления. Скорость ответа зависит от качества (и, соответственно, стоимости) продукта. В случае защиты юридических лиц, обновления могут прийти быстро, в случае физических лиц решение, возможно, будет получено в следующем обновлении программного продукта.

Возможным решением данной задачи станет внедрение политики индексационных серверов, которые работают по алгоритму клиент-серверной архитектуры. Но при этом некий индексационный сервер или мастер сервер задается путем выборов. В дальнейшем он обменивается отчетами и обновлениями с другими серверами. При достижении допустимой границы нагрузки или при переходе в режим off-line одного из серверов сети, происходят перевыборы. При этом с экспертными базами данных обмениваться информацией смогут только избранные сервера по защищенному соединению. Алгоритм их взаимодействия является следующим:

– между компьютерами участниками системы проводятся «выборы»;

– после выбора индексационного сервера первого типа выбираются ноль или больше индексационных серверов второго типа, которые будут обслуживать клиентов;

– после прохождения всех выборов каждый узел с запущенной службой Server объявляет себя индексационному серверу первого типа, чтобы тот включил его в общий список компьютеров;

– когда все узлы объявят себя индексационному серверу первого типа, то тот в свою очередь сформирует список индексационных серверов второго типа для участников сети;

– компьютер произвольно выбирает один из индексационных серверов второго типа и обменивается с ним служебной информацией в рамках обеспечения безопасности сети однозначного отождествления.

Для защиты процесса обновления автор предлагает использовать метод стеговложения. Для преобразований оптимален исполнимый файл, например, формата ELF. Главное его преимущество состоит в том, что процессоры семейства x86 имеют избыточность набора инструкций, которая можно использовать для скрытого вложения информации в исполняемый код [9].

В процессе разработки будем отталкиватьсяот разработки необходимого для архитектора РКС функционала по проектированию и согласованию внешних модулей в системе. Следующая панель управления, показанная на рис. 2, позволит действовать упорядоченно от общих задач к деталям.

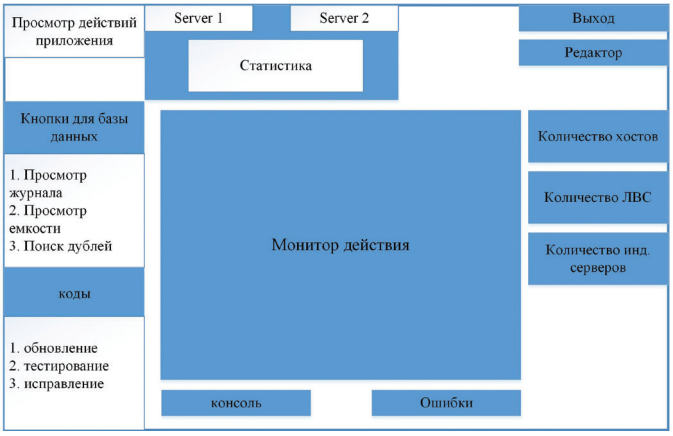

Рис. 2. Пример панели управления архитектора сети

Разработка

Для разработки панели управления использовался язык программирования C++. В результате была написана программа для ЭВМ, которая относится к области информационной безопасности в современных вычислительных сетях. Основное назначение программы следующее:

1. Контроль экспертной системы.
2. Базовая эмуляция процесса управления над экспертной системой.
3. Поддержка и обеспечение экспертной системы необходимыми элементами.
4. Настройка конфигурации в проектируемой области.

На начальном этапе работы над проектом был создан прототип программы управления для архитектора децентрализованной сети. Прототип прошел тестирование и отладку, а его исходный код находится в процессе регистрации программы ЭВМ. Панель управления адаптирована под операционные системы Windows и Unix.

Выводы

Динамичность современных сетевых технологий требует нестандартных подходов и децентрализации управления, создания распределенных компьютерных систем. В рамках проекта автор использует аналогию с иммунной системой человека, а именно алгоритм распределенного управления. Несмотря на большое количество исследований, и работ в данной области автор видит уязвимые места, а именно потребность в новых алгоритмах взаимодействия, протоколахи адаптивных способах защиты подсетей.

Литература

1. Томилин В. Безопасность сетей гарантируют системы предотвращения вторжений [Электронный ресурс]. http://www.cnews.ru/reviews/free/security2007/articles/networks.shtml (дата обращения 31.07.2015).

2. Al-Kasassbeh M., Adda M. Network fault detection with Wiener filter-based agent. Journal of Network and Computer Applications. 2009. Vol. 32. No. 4. Pp. 824–833.

3. Ilarri S., Mena E., Illarramendi A. A system based on mobile agents to test mobile computing applications. Journal of Network and Computer Applications. 2009. Vol. 32. No. 4. Pp. 846–865.

4. Boukerche A., Machado R.B, Juca KRL, Sobral JBM, Notare MSMA. An agent based and biological inspired real-time intrusion detection and security model for computer network operations. Computer Communications. 2007. Vol. 30. Pp. 2649–2660.

5. Tarakanov A.O. Immunocomputing for intelligent intrusion detection. IEEE Computational Intelligence Magazine. 2008. Vol. 3. No. 2. Pp. 22–30.

6. Harmer P., Williams P., Gunsch G., Lamont GB.An artificial immune system architecture for computer security applications. IEEE Transactions on Evolutionary Computation. 2002. Vol. 6. No. 3. Pp. 252–280.

7. Таненбаум Э., М. ванн Стеен. Распределенные системы. Принципы и парадигмы.: Питер. 2003. 880 с.

8. Топ 10-ботнетов [Электронный ресурс] // Хакер. 2014. No. 9. https://xakep.ru/2014/09/09/top-10-botnets (дата обращения 12.06.2015).

9. Штеренберг С.И., Виткова Л.А., Просихин В.П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации. СПб.: СПбГУТ. 2014. Vol. 4. No. 8. С. 126–133.

Для цитирования:

Виткова Л.А. Исследование распределенной компьютерной системы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 44–48.

STUDY ON DISTRIBUTED COMPUTER SYSTEMS ADAPTIVE ACTIONS

Vitkova Lydia Andreevna,
St. Peterburg, Russia, lidia@iskin.spb.ru

Abstract
The possibility of applying algorithms of artificial immune systems to create a distributed network. It describes the basic mechanism of protection of human immunity. Further analysis of existing technologies is done, which in their design were based on the mechanisms of immunity. The author chooses the intrusion prevention system as a starting point. A brief overview of distributed algorithms, parallel computing is given.
The work consists of several sections; «methodology» section describes analysis of existing solutions as well as finding ways to decentralize computer networks to protect them. As part of the experiment developed management software for distributed network architect. Also part of the code is presented. The software product runs in Windows, and Unix systems.
It is predicted that the network will function algorithm for indexing servers first and second legal access level, each of which is responsible for updating and interaction with other subnets. One of the servers becomes the preferred and has access to expert systems.
A secure connection SSL is proposed to use in order to protect the communication channel in the update process and to protect the system as a whole to use the method implantation of steganography. For optimal conversions steganography executable file format is used, ELF. Redundancy can be used for embedding hidden information into executable code without disrupting the functionality.
Despite the large amount of research and work in this field, the author thinks of the necessity for new mechanisms for cooperation, protocols and adaptive methods of protection subnets. Existing algorithms for distributed computer networks use the protocol P2P, making architecture less flexible and impose its own limitations. In this case, the introduction of their own interrogation protocol similar to the algorithm master browser among Windows is needed.

Keywords: distributed computer system, artificial immune system, intrusion prevention system, IDS, IPS, GRID, Botnet, expert system.

References

1. Tomilin V. Network security guarantees system intrusion prevention. http://www.cnews.ru/reviews/free/security2007/articles/networks.shtml (date of access 31.07.2015). (in Russia).
2. Al-Kasassbeh M., Adda M. Network fault detection with Wiener filter-based agent. Journal of Network and Computer Applications. 2009. Vol. 32. No. 4. Pp. 824–833.
3. Ilarri S., Mena E., Illarramendi A. A system based on mobile agents to test mobile computing applications. Journal of Network and Computer Applications. 2009. Vol. 32. No. 4. Pp. 846–865.
4. Boukerche A., Machado R.B, Juca KRL, Sobral JBM, Notare MSMA. An agent based and biological inspired real-time intrusion detection and security model for computer network operations. Computer Communications. 2007. Vol. 30. Pp. 2649–2660.
5. Tarakanov A.O. Immunocomputing for intelligent intrusion detection. IEEE Computational Intelligence Magazine. 2008. Vol. 3. No. 2. Pp. 22–30.
6. Harmer P., Williams P., Gunsch G., Lamont GB.An artificial immune system architecture for computer security applications. IEEE Transactions on Evolutionary Computation. 2002. Vol. 6. No. 3. Pp. 252–280.
7. Tanenbaum E, M. van Steen. Raspredelennye sistemy [Distributed systems]. Printsipy i paradigmy: Piter. 2003. 880 p. (in Russia).
8. Top 10 botnets. Khaker. 2014. No. 9. https://xakep.ru/2014/ 09/09/top-10-botnets/(date of access 12.06. 015). (in Russia).
9. Shterenberg S.I., Vitkova L. A., Procain V.P. The technique of applying the concept of adaptive self-developing system. Informatsionnye tekhnologii i telekommunikatsii.. SPb.: SPbGUT. 2014. Vol. 4. №8. Pp. 126–133. (in Russia).

Information about authors:
Vitkova L.A., post-graduate student St. Petersburg state University of telecommunications.

For citation:
Vitkova L.A. Study on distributed computer systems adaptive actions. H&ES Research. 2015. Vol. 7. No. 5. Pp. 44–48. (in Russian).

НАВИТЕХ

N 55°44.984’ E 37°32.762’

10–13.05 2016

8-я международная выставка

ЭКСПОЦЕНТР

Навигационные системы, технологии и услуги

Организатор:
ЗАО «Экспоцентр»

При поддержке:

- Ассоциации «ГЛОНАСС / ГНСС – Форум»
- НП «ГЛОНАСС»

Под патронатом
Торгово-промышленной палаты РФ

12+ Реклама

Россия, Москва, ЦВК «Экспоцентр»

www.navitech-expo.ru

ОБЩЕЕ ПРЕДСТАВЛЕНИЕ ПРОЕКТА АДАПТИВНОЙ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ A_RPA

Штеренберг Станислав Игоревич,
аспирант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, shterenberg.stanislaw@yandex.ru

Ключевые слова:
искусственный интеллект, адаптивные системы, программы управления, программирование, базы данных.

АННОТАЦИЯ

Для современного информационного общества настает период, когда понятие машина и искусственный интеллект (ИИ) представляет собой что-то общее. Вернее сказать было бы, что системы принятия решений, логические языки программирования и многое другое из ряда изучения о ИИ теперь не изучаются отдельно, а представляют собой единый объект для изучения. Общий ход написания и создания ИИ также более не сводится к единообразному компилированию или отладке конечной программы. Важно понимать, что построение интеллектуальных систем производится при помощи различных инструментов. Однако все сборное, должно представлять единое. В части аннотации уже напрашивается тогда мысль, что системы ИИ будут неким подобием биоаналогии современного мира. Проводится некая аналогия и сравнение с биологическим представлением, но по большей части следует сказать, что если и будет создан полноценный ИИ, то он принципиально будет отличаться от того, что нам будет известно до того времени. О том как проектируется и создается современная адаптивная интеллектуальная система и будет раскрыто в работе.

Анализируя историю ИИ, можно выделить такое обширное направление как моделирование рассуждений. Многие годы развитие этой науки продвигалось именно по этому пути, и сейчас это одна из самых развитых областей в современном ИИ. Моделирование рассуждений подразумевает создание символьных систем, на входе которых поставлена некая задача, а на выходе ожидается ее решение. Как правило, предложенная задача уже формализована, то есть переведена в математическую форму, но либо не имеет алгоритма решения, или этот алгоритм сложный, трудоемкий и т.д. В это направление входят: доказательство теорем, принятие решений и теория игр, планирование и диспетчеризация, прогнозирование.

Таким образом, на первый план выходит инженерия знаний, объединяющая задачи получения знаний из простой информации, их систематизацию и использование. Достижения в этой области затрагивают почти все остальные направления исследования ИИ. Здесь также необходимо отметить две важных подобласти. Первая из них – машинное обучение – касается процесса самостоятельного получения знаний интеллектуальной системой в процессе ее работы. Вторая связана с созданием экспертных систем – программ, использующих специализированные базы знаний для получения достоверных выводов относительно произвольной проблемы.

Большие и интересные достижения имеются в области моделирования биологических систем. Сюда можно отнести несколько независимых направлений. Нейронные сети используются для решения нечетких и сложных проблем, таких как распознавание геометрических фигур или кластеризация объектов. Генетический подход основан на идее, что некоторый алгоритм может стать эффективным, если отберет лучшие характеристики в других алгоритмов («родителей»). Относительно новый подход, где ставится задача создания автономной программы – агента, который сотрудничает с окружающей средой, называется агентный подход. А если правильно заставить большое количество «не очень интеллектуальных» агентов сотрудничать вместе, то можно получить коллективный «муравьиный» интеллект.

Что наиболее важно и с чего стоит начать построение системы искусственного интеллекта ИИ? Как автор, я бы ссылался сначала на общую схему, где будет описан поэтапный разбор конструирования всех элементов системы. Общий проект имеет самоназвание и именнуется как A_RPA (лат. – rationabile progressio aggredi [умеренная программа для решения]) – проект объединяющий в себе несколько программных средств, аппаратно-программных средств и все ЭВМ включенные в одну локальную вычислительную сеть (ЛВС). Цель A_RPA обеспечить адаптивную защиту выделенной ЛВС.

Однако, в целом, вся адаптивная система не будет ограничиваться одной лишь защитой ЛВС. Среди списка ее задач будет следующее:

1. Содержание гибкой базы данных (знаний), накопление информации;

2. Саморазвитие, реализация адаптивных функций;

3. Успешная защита от:

• НСД;

• нарушения целостности;

• нарушения конфиденциальности.

4. Успешная «проактивная» защита:

• Преследование нарушителя, «заброс» вредоносных файлов;

• содержание вредоносных элементов;

• шифрование файлов;

• создание стеганограм.

Упоминается представление роевогопринципа роевого интеллекта (далее РИ). Известно, что системы роевого интеллекта, как правило, состоят из множества агентов (боидов) локально взаимодействующих между собой и с окружающей средой. Идеи поведения, как правило, исходят от природы, а в особенности, от биологических систем.

Каждый боид следует очень простым правилам и, несмотря на то, что нет какой-то централизованной системы управления поведения, которая бы указывала каждому из них на то, что ему следует делать, локальные и, в некоторой степени, случайные взаимодействия приводят к возникновению интеллектуального глобального поведения, неконтролируемого отдельными боидами. Точное определение роевого интеллекта всё еще не сформулировано. В целом, РИ должен представлять собой многоагентную систему, которая бы обладала самоорганизующимся поведением, которое, суммарно, должно проявлять некоторое разумное поведение.

Здесь важно упоминание метода роя частиц (далее МРЧ) при построении. МРЧ оптимизирует функцию, поддерживая популяцию возможных решений, называемых частицами, и перемещая эти частицы в пространстве решений согласно простой формуле. Перемещение подчиняется принципу наилучшего найденного в этом пространстве положения, постоянно изменяется при нахождении частицами выгодных положений.

Далее можно задействовать следующий прием – Искусственный алгоритм пчелиной семьи (АВС). Данный алгоритм роя на основе мета-эвристического алгоритма было введено Карабогом в 2005 году. Он имитирует поведение кормовых медоносных пчел. Алгоритм АВС состоит из трех этапов: рабочей пчелы, пчелы-надзирателя, и пчелы-разведчика. Пчелы используют алгоритм локального поиска в окрестности решения, выбранные на основе детерминированного отбора рабочими пчелами и вероятностного отбора пчелами-надзирателями. Пчела-разведчик выполняет отказ от истощенных источников питания в кормовом процессе. По этой аналогии решения, которые не полезны больше для поиска решения отбрасываются, и добавляются новые решения (по аналогии с исследованием новых регионов в поиске источников).

Данные два метода плавно перетекают в следующий, где принципиально важно реализовывать искусственную иммунная система (ИИС) – это адаптивная вычислительная система, использующая модели, принципы, механизмы и функции, описанные в теоретической иммунологии, которые применяются для решения прикладных задач.

Несмотря на то, что природные иммунные системы изучены далеко не полностью, на сегодня существуют по меньшей мере три теории, объясняющие функционирование иммунной системы и описывающие взаимодействие ее элементов, а именно: теория отрицательного отбора, теория клональной селекции и теория иммунной сети. Они легли в основу создания трех алгоритмов функционирования ИИС.

Таким образом – весь проекта A_RPA решено складывать из следующих частей:

1. *Medic_RPA (Санитар)* – данное программное предназначенное для восстановления и поддержки всего ПО «A_RPA». Включает в себя следующие возможности:

• создание резервных копий;

• шифрование данных;

• встроенный стегокодер.

2. *Worker_RPA (Рабочий)* – специальное программное обеспечения для осуществления поисковой работы общего ИИ. Включает в себя:

• универсальный и совершенствуемый поисковик, самодописывающий инструкции поиска;

• анализатор + синхронизатор (для БД) выбранной/найденной информации;

• поисковик по заданным критериям. Умение искать информацию по системе уже знакомых понятий (к примеру поиск аналогов микроконтроллерных устройств для внедрения в мат. плату, или поиск синхронизируемых компонентом).

3. *Solder_RPA (Солдат)* – главная причина создания A_RPA в целом, инструмент защиты и атаки. Включает следующие элементы:

• антивирус (карантинная область, удаление вредоносных кодов);

• шпион – перехватчик информации (принцип DLP-систем, различных снифферов и кейлогиров);

• бекдор – важный инструмент для реализации скрытного захода не только на удаленные машины, но и на рабочие станции ЛВС;

• дешифратор – использование набора известных методов криптоанализа и стегоанализа (может разделяться на два элемента);

• заразитель – элемент подбора вирусных атак для контратаки нарушителя. Должен будет включать в себя знания о различных типах вирусов и элементов их рассылки (спам).

Итак, мы разобрали три компонента софта A_RPA. Принципиально выделить, что два компонента Worker_RPA и Solder_RPA нуждаются в наличие стойкой и гибкой Базы Данных, откуда будут браться основные элементы взаимодействия с адаптивной системы. Однако об устройстве базы данных мы поговорим позже. Прежде надо разобрать еще один элемент, наиболее важный для всей системы.

4. *Cerebro_RPA (мозг)* – Центральный аппарат системы, элемент управление сложной системы поведения A_RPA. Чтобы три основных компонента функционировали совместно со всей системой необходимы модули синхронизации и инсталяции ПО на Рабочие станции и Сервера. Помимо этого, поскольку Cerebro_RPA – центральная интеллектуальная система, то она должна быть выделена на отдельную машину. Cerebro_RPA должен быть создан первым и обязан обладать следующими компонентами.

• Распознаватель. Иными словами – система «свой-чужой». Необходимый компонент для определения программ в ЛВС, вредоносных систем, а также гарантированная защита от НСД. Здесь и может быть впервые употреблен термин - самомодифицирующийся код RPA (или SM_Code_RPA). Поскольку в создании самомодификации есть определенные опасности, то применимо широкое знание цифровой стеганографии. Важно наличие элементов защиты во всех приложениях A_RPA.

• Синхронизатор, который будет содержать в себе основную часть команд для перечисленных ранее компонентов A_RPA. Важный элемент, поскольку над всей системой нужен тотальный контроль. Однако, команды могут впоследствии изменяться. О процедурах саморазвития системы мы поговорим позже.

• Стратегический комплекс. Как учтено во многих компьютерных играх, симуляторах и прочих тренажерах, там имеется некий ИИ, которых обладает своей стратегией, своей динамикой действий против пользователя и игрока. Этот элемент не менее важен для всей системы A_RPA, поскольку деятельность защиты и атаки будет осуществляться против пользователя. Добро пожаловать в игру!

• Система «Вопрос-ответ». Один из элементов обучения системы A_RPA. На самом деле здесь наблюдается прямое взаимодействие с пользователем. Оператор – первичный наставник молодого саморазвивающегося искусственного интеллекта. Помимо этого, при помощи компонента Worker (и дальнейших его модификаций), будет осуществлен элемент визуального наблюдения, что дополнительно обучит адаптивную систему.

FORUM – проект базы данных для программного модуля A_RPA. Данная база данных должна подходить под общий принцип работы проекта RPA, а также следовать следующей принципам построения:

1. Машинное обучение. Так как раздел машинного обучения, с одной стороны, образовался в результате разделения науки о нейросетях на методы обучения сетей и виды топологий архитектуры сетей, а с другой, вобрал в себя методы математической статистики, то указанные ниже способы машинного обучения исходят из нейросетей. То есть базовые виды нейросетей, такие как перцептрон и многослойный перцептрон (а также их модификации) могут обучаться как с учителем, без учителя, с подкреплением, и активно. Но некоторые нейросети и большинство статистических методов можно отнести только к одному из способов обучения. Поэтому если нужно классифицировать методы машинного обучения в зависимости от способа обучения, то, касательно нейросетей, некорректно их относить к определенному виду, а правильнее классифицировать алгоритмы обучения нейронных сетей. Имеется множество объектов (ситуаций) и множество возможных ответов (откликов, реакций). Существует некоторая зависимость между ответами и объектами, но она неизвестна. Известна только конечная совокупность прецедентов – пар «объект, ответ», называемая обучающей выборкой. На основе этих данных требуется восстановить зависимость, то есть построить алгоритм, способный для любого объекта выдать достаточно точный ответ. Для измерения точности ответов определённым образом вводится функционал качества. Данная постановка является обобщением классических задач аппроксимации функций. В классических задачах аппроксимации объектами являются действительные числа или векторы. В реальных прикладных задачах входные данные об объектах могут быть неполными, неточными, нечисловыми, разнородными. Эти особенности приводятк большому разнообразию методов машинного обучения.

2. Квазибиологическая парадигма. Отличается от понимания искусственного интеллекта по Джону Маккарти, когда исходят из положения о том, что искусственные системы не обязаны повторять в своей структуре и функционировании структуру и протекающие в ней процессы, присущие биологическим системам. Сторонники данного подхода считают, что феномены человеческого поведения, его способность к обучению и адаптации есть следствие именно биологической структуры и особенностей её функционирования. Сюда можно отнести несколько направлений. Нейронные сети используются для решения нечётких и сложных проблем, таких как распознавание геометрических фигур или кластеризация объектов. Генетический подход основан на идее, что некий алгоритм может стать более эффективным, если позаимствует лучшие характеристики у других алгоритмов («родителей»). Относительно новый подход, где ставится задача создания автономной программы – агента, взаимодействующей с внешней средой, называется агентным подходом.

Важнейшими элементами базы знаний являются инженерия знаний и представление знаний. База данных для A_RPA строится с применением знаний:

1. Семантическая сеть – информационная модель предметной области, имеющая вид ориентированного графа, вершины которого соответствуют объектам предметной области, а дуги (рёбра) задают отношения между ними. Объектами могут быть понятия, события, свойства, процессы. Таким образом, семантическая сеть является одним из способов представления знаний. В названии соединены термины из двух наук: семантика в языкознании изучает смысл единиц языка, а сеть в математике представляет собой разновидность графа – набора вершин, соединённых дугами (рёбрами), которым присвоено некоторое число. В семантической сети роль вершин выполняют понятия базы знаний, а дуги (причем направленные) задают отношения между ними. Таким образом, семантическая сеть отражает семантику предметной области в виде понятий и отношений.

2. Фреймы, как способ представления знаний. Фрейм – это модель абстрактного образа, минимально возможное описание сущности какого-либо объекта, явления, события, ситуации, процесса.

Помимо теоретических основ, важно применить практическую модель. База данных для адаптивной системы должно включать в себя структуру, по которой будет строиться для системы A_RPA основной способа подбора и использования текущей информации. База данных должна быть расширяемой, а также ограниченной к использованию. Желательно, чтобы как можно быстрее информация из базы данных обработалась непосредственно элементом A_RPA – Cerebro. будет забито в систему обработки знаний. Даже теоретически пока что нельзя предугадать, что будет забито в систему обработки знаний. Однако, на ранних этапах важно выделить, какая информация будет обрабатываться ИИ A_RPA.

База данных A_RPA может быть не написана на первой стадии, однако под ее размер должно быть выделено довольно большое пространство.

Таблица 1

Представление ячеек базы данных

Сектор (table_type_1)	**Модуль (table_type_2)**	**Значение (table_type_3)**	**Примечание**
Jornal	Solder		*Ввод и вывод информации, обработка кодов и действий программы*
	Worker		
	Medic		
	Cerebro		
SM_Code_RPA	Stego_Option	About_ef_embedding_in_file	*Информация о ходе вложения в файлы*
		File_type_information	*Информация об использованных форматах файлов*
	Function_Option		*Дополнительные опции для действий SM_Code_RPA*
Search_result	`WWW_search_result	Microkontroller_info	*Элементы, найденные на страницах веб, по сопоставлению с микроконтроллерными устройствами*
		Другое…	
	Local_Network_result	Microkontroller_info	*Элементы, найденные на устройствах, по сопоставлению с микроконтроллерными устройствами*
		Soft_info	*Элементы ПО, найденные на устройствах, по сопоставлению с остальным ПО*
		Другое…	
Combat_sector	Antivirus_sector_signature		*данные по защите информации*
	Attack_element		*данные по атакующим и вредоносным элементам*
Strategic_department	Location	Microkontroller_info	*Информация о местоположении A_RPA на платах*
		Drawings	*Планы аудиторного комплекса*
	Build		*Информация о наличие софта поддержки*
	Rush		*Планирование атаки*
	Defend		*Планирование защиты*
	Digital_device		*Информация о наличие внешних цифровых устройств*

Программа управления REX – примитивная и простая в использовании, она должны быть единственным связующим элементом между A_RPA и пользователем. В задачи REX входит следующее:

1. Непосредственное управление серверами и рабочими станциями.

2. Отслеживание действий работы A_RPA, а также SM_Code_RPA.

3. Общение с компонентом Cerebro и координация его действий.

4. Администрирование проектом A_RPA.

Для более детального представления работы ПУ REX, разберем скриншот прототипа (рис. 1).

На скриншоте цифрами отмечены следующие элементы:

1. Соединение с базой данных. Контроль и настройка конфигурации, работа в формах БД (Ниже отображены элементы для добавления знаний в базу знаний).

2. Соединение с базой журналов. Отображение действий кодов и их функций.

3. Настройка политики безопасности рабочих месте (+ режим сервера).

4. Настройки параметров соединения в ЛВС.

5. Просмотр и настройка конфигурации работы серверов (Server 1 – сервер, где установлен A_RPA; Server 2 – серверный компьютер, где планируется разворачивание базы данных {временно можно жесткий диск}).

6. Отображение информации о рабочих состояний имеющихся серверов и рабочих станций, а также сведения о работе ЛВС.

7. Графический режим с представлением текущих баннеров, на которых отображается всё действие происходящее в сети (надо проработать материал в различных средах графических режимов {применение MathCath, 3D MAX, AutoCAD}). Также я доступ на управление окном Cerebro.

8. Диалоговая строка общения и прописка дополнительных команд Cerebro.

9. Элементы связанные с ассемблерными формами обработки программ Solder, Worker & Medic. Ниже результат обработки из диалогового окна и из дочерних элементов.

10. Браузерная строка. Для обработки поисковых алгоритмов по веб-ресурсам, результаты работы скриптов.

11. Выбор режима работы программы:

– Admin – Возможность активировать все кнопки (нужна система идентификации и аутентификации);

– User – Не возможности работать с областями 1, 6, 7, 8, 10.

12. Элемент предназначенный для активации самостоятельной работы A_RPA. Подается сигнал для передачи управления Cerebro, он блокирует кнопки ПУ REX и переводит его в режим User. Далее Cerebro автономен и управляет остальными компонентами A_RPA.

SM_Code_RPA – элемент программы A_RPA, а именно самомодифицирующийся код, который может быть доступен для использования Cerebro и оператором (им, на ранних стадиях обучения). Особенность самомодифицирующегося кода в его стегонаграфических преобразованиях, то есть в возможности оставаться незамеченным для системы и наиболее успешно сохраняться в файловых структурах. SM_Code_RPA в дополнение обладает механизмом самодописания или самомодификации, чем скорее напоминает полиморфные компьютерные вирусы. Однако элемент скрытности и развития иллюстрирует аналогию с бионическими системами, где каждая живая клетка стремиться выжить и защититься. Такой уклад и такая возможность позволят RPA защититься от тотального уничтожения и активироваться в системе вновь.

Подробнее о самомодификации можно объявить следующее:

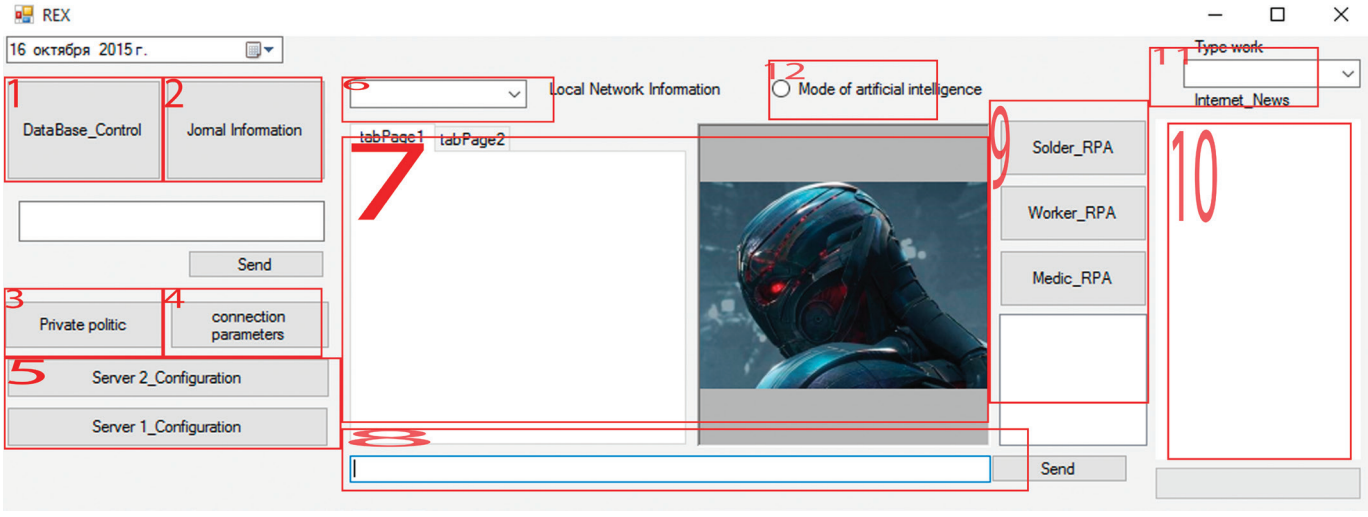

Рис. 1. Скриншот прототипа REX

Самомодифицирующийся код встречается в вирусах, защитных механизмах, сетевых червях, кряках и прочих программах подобного типа. И хотя техника его создания не представляет большого секрета, качественных реализаций с каждым годом становится все меньше и меньше. Окутанный мраком тайны, окруженный невообразимым количеством мифов, загадок и легенд, самомодифицирующийся код постепенно уходит в прошлое. Рассвет эпохи самомодификации уже позади. Во времена неинтерактивных отладчиков типа debug.com и пакетных дизассемблеров типа Sourcer самомодификация действительно серьезно затрудняла анализ, однако с появлением IDA PRO и Turbo-Debugger все изменилось. Самомодификация не препятствует трассировке, и для отладчика она полностью прозрачна. Со статическим анализом дела обстоят несколько сложнее. Дизассемблер отображает программу в том виде, в котором она была получена на момент снятия дампа или загрузки исходного файла, рассчитывая на то, что ни одна из машинных команд не претерпит изменений в ходе своего выполнения. В противном случае реконструкция алгоритма будет выполнена неверно, и хакерский корабль при спуске на воду даст колоссальную течь. Однако, если факт самомодификации будет обнаружен, скорректировать дизассемблерный листинг не составит большого труда.»

Потому, единственно важным остается то, чтобы самомодифицирующийся код дополнительно скрыть и задать параметры автоматического самодописания в файлы. Использование самомодифицирующегося кода с формальной точки зрения вполне законно. Однако следует помнить, что злоупотребление им отрицательно влияет на производительность защищаемого приложения. Кодовый кэш первого уровня доступен только на чтение, и прямая запись в него невозможна. При модификации машинных команд в памяти, в действительности модифицируется кэш данных! Затем происходят экстренный сброс кодового кэша и перезагрузка измененных кэш-линеек, на что расходуется достаточно большое количество процессорных тактов.

Таким образом, можно сделать вывод по каким критериям будет строиться весь прототип ИИ RPA:

1. Наличием гибкой и расширяющейся базы данных.
2. Процедуры поиска и сбора информации:
• Обработка файловых структур;
• Внешние данные (поле иформации).
3. Система резервирования данных.
4. Наличие стеганографических преобразований в системе для обеспечения скрытности.

Вкратце моя идея будет звучать именно так: мы создаем программу, которая в своих ресурсах содержит компилятор и собственный код. Вследствие некоторого воздействия извне или необходимости изменить саму себя, программа пытается улучшить свою новую копию или приспособить ее к новым условиям среды. Для этого она достает из ресурсов компилятор (он уже может присутствовать в операционной системе, тогда этот пункт можно упустить) и собственный исходный код. После этого исходный код модифицируется соответственно к новым условиям и компилируется (при этом в ресурсы попадает новый исходный код и тот же компилятор). После удачной компиляции родительская программа загружает в память машины свою новую версию и завершается сама. Таким образом, программа-потомок начинает функционировать вместо родительской программы и, в случае надобности, цикл самомодификации повторяется, то есть программа-потомок стает родительской программой для нового потомка.

Вы спросите, для чего это все нужно?

1. Циклическое усовершенствование программы или ее алгоритма. Программа модифицирует себя, решает некоторую эталонную задачу и оценивает результат. На основе результата принимается решение о новом цикле модификации.

2. В случае вирусной программы такой подход может использоваться для модификации своего кода при переходе на новую машину и обхода, таким образом, антивирусов. При этом можно как менять уже существующий код, так и добавлять новый, который не несет смысловой нагрузки.

3. Программа может запоминать конкретного пользователя и подстраиваться под него. Например, можно экспериментировать с цветами и формой окна и спрашивать пользователя о приемлемом для него варианте или анализировать наиболее часто используемые пользователем функции программы. В случае оператора типа switch() может иметь смысл наиболее часто используемые варианты выбора передвигать вверх для того, что бы пытаться избежать проверок тех вариантов выбора, которые практически не используются.

4. Программа может попытаться найти в сети Интернет исходный код нового решения какой-то из своих функций, загрузить его, соответствующим образом изменить свой код с учетом новой реализации данной функции и попробовать откомпилировать и проверить работу новой копии. Таким образом можно создать программу, которая со временем будет сама находить лучшие решения проблем и использовать их в своей роботе.

Итак, теперь мы перейдем к построению алгоритма реализации разрабатываемого средства защиты информации. Перейдем к обозначению следующих обязательных действий:

1. Передача самомодифицирующегося кода в основной код исполнимого файла любого формата.

2. Стеганографическое сокрытие передаваемого файла с невозможностью его дальнейшего обнаружения.

3. Распространения самомодифицирующегося кода после команды оператора по всему приложению.

4. Реализация иммунной адаптивной защиты приложения.

5. Реализация возможности накопления «знания» в базу данных о всевозможных типах атаки нарушителей.

6. Реализация принятия решения о контратаки нарушителя.

7. Последующая реализация адаптивной интеллектуальной системы для автоматизации защиты приложений.

И последние комплектующие проекта A_RPA.

SERVER I – некая комплектующая машина оператора, где должны быть обязательно по минимуму следующие элементы:

1. Среда разработки (язык C#, Assembler).

2. Среда визуального/графического представления (AutoCath, 3D MAX, Corel Draw).

3. Системные требования минимальны: 2,2 Гц, 6 Гб ОЗУ, 1 Тб.

SERVER II – на первых стадиях развития хранилище, место хранения базы знаний RPA. Скорее всего внешний HDD от 4 Тб данных.

SERVER I размещает в себе компоненты программы A_RPA: Cerebro, Worker, Solder, Medic. SERVER II содержит базу знаний – FORUM. ПУ REX должен размещаться отдельно на рабочей станции администратора комплекса. Дополнительно должны иметься тестовые рабочие станции, не более двух для отработки системы удаленного взаимодействия и защиты. Подключение к интернету на ранних стадиях опасно для «жизни» кода (рис. 2).

Без преувеличения можно сказать что проект разрабатывается весьма активно, но в одиночку. Как видно из рис. 2 уже ведутся программные реализации базы данных (папка Forum), ПУ REX (Rex_using_program), SM_Code_RPA (Cerebro with him hands and self-modify code – папка SM_Code_RPA). Как видно по проекту, сердце первоначального ИИ будет строиться от папки SM_Code_RPA. здесь будут протекать многие жизненно важные инструкции для Cerebro. Диалоговые окна и базовые функции строятся на языках C#/C++, а системные данные и способы вложения реализуются по большей части на языке Ассеблера. Следует заметить, что соединение с базой данных осуществляться первоначально будет не на выделенном сервере или HDD, а допускается возможность размещение базы данных на SERVER I. Также первично разрешается скрестить компоненты ПУ REX и SM_Code_RPA на одной машине тоже.

Общая компоновка кодов осуществляется временно в Visual Studio (рис.3).

Выводы

Общая структура A_RPA иллюстрирует в некотором смысле систему роевого интеллекта, причем здесь наблюдается сочетание МРЧ и АВС методов в одном, потому что данная даптивная система имеет на вооружение несколько компонентов программы с разными функциями. Первоначально A_RPA разрабатывается как система защиты информации. Здесь важно наличие программы управления над ресурсами адаптивной системы ИИ. Такую функцию исполнить программа REX, которая важна на ранних стадиях разработки ИИ, потому что первичные элементы обучения могут быть «прописаны» только со стороны человеческого фактора.

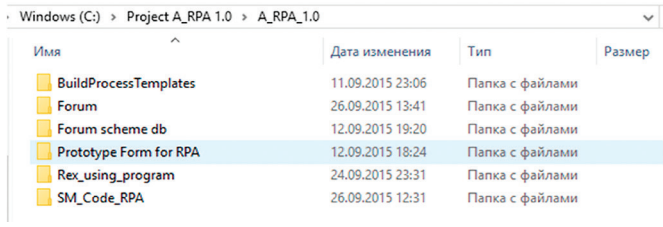

Рис. 2. Ход разработки проекта A_RPA_1.0

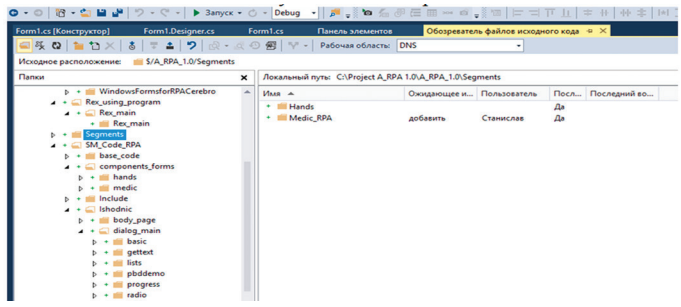

Рис. 3. Ход проекта A_RPA_1.0

Можно более чем подвести один итог: проект A_RPA несет в себе наследования целого ряда биоаналогий (роевый интеллект, машинное обучение, взаимодействие с оператором через программу управления), а также создается в целях адаптивности систем защиты информации и несет в себе особенности экспертных систем (системы, которые могут заменить человека).

Литература

1. Миллер П. Роевой интеллект: Муравьи, пчелы и птицы способны многому нас научить// National Geographic Россия. 2007. № 8. С. 88–107.

2. RPA (rationable progressimo aggredi) (лат.), Свидетельство о государственной регистрации программы для ЭВМ №2015611539. Дата поступления 02 декабря 2014 г. Зарегистрирована в Реестре программ для ЭВМ 30 января 2015 г., Правообладатель: ФГОБУ ВПО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича». Авторы: Штеренберг С.И., Андрианов В.И., Липатников В.А., Костарев С.В.

3. Denning D. E. An intrusion detection model // IEEE Trans. on Software Engineering. 1987, SE-13. Pp. 222–232.

4. Красов А.В., Штеренберг С.И., Верещагин А.С. Разработка методов защиты от копирования ПО на основе цифровых водяных знаков внедряемых в исполнимые и библиотечные файлы. // Актуальные проблемы инфокоммуникаций в науке и образовании. 2013. С. 847-852.

5. Штеренберг С.И., Андрианов В.И. Варианты модификации структуры исполнимых файлов формата PE. // Новосибирск: Перспективы развития информационных технологии. 2013. С. 134–143.

Для цитирования:
Штеренберг С.И. Общее представление проекта адаптивной интеллектуальной системы A_RPA // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 50–57.

OVERVIEW OF PROJECT ADAPTIVE INTELLIGENT SYSTEMS A_RPA

Shterenberg Stanislav Igorevich,
St. Petersburg, Russian, shterenberg.stanislaw@yandex.ru

Abstract
For the modern information society comes a time when the concept of the machine and artificial intelligence (AI) represents something in common. Or rather it would be that the decision-making system, logic programming languages and more out of the study of AI now not studied separately, and represent a single object for study. The general course of writing and creating AI also no longer be reduced to a uniform compiling or debugging the final program. It is important to understand that the construction of intelligent systems is carried out using different tools. However, all teams must submit one. As part of the annotations already it arises then the idea that AI systems will be something like biosimilars modern world. This presents a certain analogy and comparison with the biological performance, but for the most part it must be said that if there will be a full set of AI, it will be fundamentally different from what we know up to that time. About how to design and create a modern and adaptive intelligent system will be described.
Analyzing the history of AI, we can distinguish such a vast area as the simulation argument. For many years the development of this science progressed along this path, and now it is one of the most developed areas in the modern AI. Modeling reasoning involves creating symbolic systems, which are set at the entrance of a certain task, and the output is expected solution. As a rule, the proposed task has been formalized, that is translated into a mathematical form, but does not have a solution algorithm, and this algorithm is complex, time-consuming, etc. In this direction are: theorem proving, decision-making and game theory, planning and scheduling, forecasting.
Thus, at the forefront of knowledge engineering, bringing together the problem of obtaining knowledge from simple information, their systematization and use. Achievements in this area affect almost all other areas of AI research. It is also necessary to note two important subregions. The first of them - machine learning - Regarding the process of self-learning intelligent system during operation. The second involves the creation of expert systems - programs that use specialized knowledge to obtain reliable conclusions about any problems.
Large and interesting achievements are in the modeling of biological systems. These include multiple independent directions. Neural networks are used to solve the fuzzy and complex issues such as the recognition of geometric shapes or clustering of objects. The genetic approach is based on the idea that an algorithm could be effective if the best characteristics will select other algorithms ("parents"). A relatively new approach, which seeks to create a stand-alone program - an agent who is working with the environment, called the agent-based approach. And if the right to make a large number of "not very intelligent" agents work together, you can get a collective "ant" intelligence.

Keywords: search engine, database, SQL, direct search, inverted file.

References
1. Miller P. swarm intelligence: Ants, bees and birds can teach us a lot. National Geographic Rossiya. 2007. No 8. Pp. 88-107. (In Russian).
2. RPA (rationable progressimo aggredi) (Lat.), Certificate of state registration of the computer №2015611539. Date Added December 2, 2014 registered in the Register of Computer Programs January 30, 2015, Copyright: FGOBU VPO "Saint-Petersburg State University of Telecommunications. prof. Bonch-Bruevich." Authors: Shterenberg S.I. Andrianov V.I., Lipatnikov V.A. Kostarev S.W. (In Russian).
3. Denning D.E. An intrusion detection model. IEEE Trans. on Software Engineering. 1987. SE-13. Pp. 222-232.
4. Krasov A.V. Shterenberg S.I., Vereshchagin A.S. Development of methods of copy protection software based on digital watermarking implemented in executable and library files. Aktual'nye problemy infokommunikatsiy v nauke i obrazovanii. 2013. Pp. 847-852. (In Russian).
5. Shterenberg S.I., Andrianov V.I. Options for modifying the structure of executable files format PE. Novosibirsk: Perspektivy razvitiya informatsionnykh tekhnologii. 2013. Pp. 134-143. (In Russian).

Information about authors:
Shterenberg S.I., postgraduate student, Federal State Educational Budget-Financed Institution of Higher Vocational Education The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.

For citation:
Shterenberg S.I. Overview of project adaptive Intelligent systems A_RPA. H&ES Research. 2015. Vol. 7. No. 5. Pp. 50–57. (in Russian).

МЕТОДИКА НАХОЖДЕНИЕ ВЕЛИЧИНЫ НАИБОЛЕЕ ВЫГОДНОГО КОНТЕЙНЕРА В ФОРМАТАХ ИСПОЛНЯЕМЫХ ФАЙЛОВ

Шариков
Павел Иванович,
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, jotass@rambler.ru

Ключевые слова:
скрытие информации, стеганография в исполняемых файлах, контейнеры, выбор выгодного контейнера, portable executable.

АННОТАЦИЯ

Рассмотрена такая проблема, как выбор методики нахождения величины наиболее выгодного контейнера в форматах исполняемых файлов. Рассматривается, от чего зависит надежность стегосистемы и ее устойчивость к стегоанализу. Выявлены основные критерии выдвигаемые контейнеру в формате исполняемого файла. Проанализированы возможные типы контейнеров, а также способы их использования, трудности при работе с ними. Указаны эффективные возможности использования определенных типов контейнеров и их положительные стороны при вложении информации в них. Описан и аргументирован выбор определенного типа контейнеров. Обращено отдельное внимание способам выбора контейнера. Дано пояснение каждому способу, описаны эффективные возможности использования контейнеров отобранных с помощью каждого из рассматриваемых способов. Указаны основные трудности при использовании того или иного способа отбора контейнера. Сделан выбор, в рамках проблемы в пользу одного из способов и приведена аргументация выбора с эффективной реализацией данного способа. Также, приведено распределение контейнеров по типу организации. Описаны плюсы и минусы использования каждого из типов организации. Приведено предположение о соотношении количества информации вкладываемой в контейнер от выбора типа контейнера. Сделан выбор в пользу одного из типов организации контейнеров. Приведено рассуждение его выгодности и эффективности использования, при вложении информации по сравнению с другими. Представлен график, отображающий еще одну зависимость в файлах цифрового формата. На графике показана зависимость надежности системы от объема встраиваемых данных. При рассмотрении указанного графика сделан вывод и описание для достижения оптимальной зависимости надежности системы от объема встраиваемых данных. Соединив все аспекты выбора контейнера, найдено решение, связанное с выбором наиболее выгодного контейнера и сделан рисунок, который схематично показывает цепочку рассуждений в данной статье. В итоге сделан вывод по работе, собрана вся информация за время исследования и представлена методика для успешного скрытия сообщения в исполняемый файл.

Для начала необходимо обозначить объект для методики. За объект выбирается контейнер, то есть элемент интерфейса программы, который содержит или может содержать в себе другие элементы интерфейса. Контейнер объединяет все эти элементы в одно целое, так называемую группу, и отвечает за отображение этих элементов и предоставления возможности по управлению ими. С помощью стеганографических методов, возможно, передавать секретные сообщения, которые встраиваются в контейнеры, так, что сам факт передачи такого сообщения обнаружить невозможно. Разумеется, при использовании контейнеров для передачи секретных сообщений и просто для вложения информации (скрытия) от посторонних глаз есть свои плюсы и минусы. При встраивании сообщений происходит нарушение естественности контейнера и изменению некоторых его свойств.

Таким образом, надежность стегосистемы и вероятность обнаружения самого факта передачи скрытого сообщения напрямую зависит от выбора контейнера. Известно, что контейнер в программировании – это структура, которая позволяет инкапсулировать в себе типы данных различного типа. Наиболее известными контейнерами являются те, которые построены на основе шаблонов. Хотя существуют и решения в виде библиотек файлов. До стегокодера – контейнер пустой, после – заполненный. Существует два основных типа контейнеров: фиксированный и потоковый. При использовании потоковых контейнеров существенную трудность составляет синхронизация начала скрытого сообщения. Также существуют методы, использующиеся для контейнеров с произвольным доступом. Такие методы предназначены для работы с файлами фиксированной длины (программы, графические, звуковые файлы). В таком случае размер файла и его содержимое известно заранее [1–2].

Теперь отвлечемся и рассмотрим более детально использование контейнеров с произвольным доступом. При заранее известном размере файла и его содержимом, вытекает условие, при котором использование контейнеров фиксированной длины имеет смысл и большую вероятность сокрытия вложения. Данное условие можно сформулировать следующим образом. Контейнер с вложением и контейнер без вложения должны быть не различимы, т.е. абсолютно одинаковы, по объему занимаемой памяти. Так как мы рассматриваем в качестве контейнера некоторую программу (а точнее ее исполняемый код), то утверждение можно задать, исходя из наших потребностей. Контейнер с вложением и контейнер без вложения должны быть абсолютно одинаковы, по объему занимаемой памяти. Важный элемент вложения – у файла не должен меняться размер. Если это программный продукт имеющий интерфейс и визуализационную составляющую, то изменения затронувшие контейнер должны быть незаметны для человека. В идеале даже при использовании программных средств. Также, в работе программы не должно произойти видимых изменений или изменений функционала программы при ее работе. Целостность и функции программы должны остаться без изменений [3].

Недостаток таких контейнеров в том, что они обладают гораздо меньшими размерами, чем потоковые. Преимуществом данных контейнеров является тот факт, что они могут быть заранее оценены с точки зрения эффективности выбранного стеганографического преобразования. В непрерывном потоке данных наибольшую трудность для получателя составляет сложность определения момента начала скрытого сообщения.

Несмотря на недостаток контейнеров с произвольным доступом, свой выбор останавливаем на них. Это связано с тем, что данные контейнеры встречаются повсеместно. В них проще отследить начало скрытого сообщения, в отличие от потоковых контейнеров. Несколько небольших контейнеров с произвольным доступом имеют большую эффективность и ценность для вложения информации, нежели потоковые контейнеры. Контейнер с произвольным доступом наиболее приемлем.

При использовании контейнеров имеющих фиксированную длину корреспондент заранее знает размер файла и может выбрать скрывающие биты в подходящей псевдослучайной последовательности [4].

Но контейнеры фиксированной длины имеют ограничение по объему, следовательно, скрываемое сообщение может попросту не поместиться в файл-контейнер. С другой стороны, контейнеры фиксированной длины наиболее распространены и доступны, что делает их использование на практике более обоснованным. Проще и удобнее будет рассматривать случайный контейнер. Случайным контейнером может оказаться абсолютно любой исполняемый файл, любого размера. Начиная от файла-запуска какого-либо небольшого приложения, заканчивая полноценными программами и их средами выполнения. Таким образом, мы не будем поставлены в жесткие рамки, и вправе будем выбирать любой интересующий нас контейнер. Проще говоря, при таком подходе подойдет любой контейнер, который выберем мы или в зависимости от ситуации выберут нам.

Также, существуют способы отбора контейнера. Методы суррогатной криптографии, селективной и конструирующей [5].

Суррогатная стеганография
или безальтернативная

Возможности выбора контейнера не существует по каким-либо причинам. Для сокрытия сообщения выбирается любой первый попавшийся контейнер, который может не подходить для скрываемого сообщения. Биты контейнера заменяются битами скрываемого сообщения так, что данное изменение незаметно. Главный недостаток данного метода заключается в том, что имеется возможность скрывать лишь незначительное количество данных.

Селективная стеганография

При использовании селективной стеганографии генерируется большое количество различных контейнеров, с целью последующего выбора наиболее подходящего контейнера из всех имеющихся для вложения в него конкретного сообщения. Наиболее часто выбор контейнера происходит путем сравнения хеш-функции сообщения и хеш-функции контейнера. Если хеш-функции совпали, то поиск наиболее удобного контейнера для вложения считается законченным и выбирается данный контейнер.

Конструирующая стеганография

Предельный случай. В данном способе отбора контейнера более детальный отбор проходит не контейнер, а скрываемое сообщение. Сообщение подбирается таким образом, чтобы при вложении его в контейнер оно минимально изменяло модель первоначального шума. Однако, чаще всего сама система генерирует контейнер. Шум контейнера моделируется скрываемым сообщением. В качестве примера может послужить какая-либо система, которая в качестве контейнера генерирует фрактал Мандельброта.

В зависимости от ситуации могут использоваться разные способы отбора контейнера. Можно предположить, что высокоэффективным методом будет конструирующая стеганография. В данном методе при использовании процедур, которые кодируют скрываемое сообщение под шум и сохраняют модель первоначального шума, вполне вероятно, обнаружить скрываемое сообщение гораздо сложнее, чем в других методах. Очевидно, что метод селективной стеганографии самый затратный по времени и ресурсам. Для сообщения небольшого объема совершенно не годится. Наконец, метод суррогатной стеганографии. Но у него имеется минус, по сравнению с остальными методами, в том, что он зачастую не позволяет вложить сообщение целиком в контейнер, он имеет преимущество в скорости. Такой контейнер подойдет для небольших вкладываемых сообщений, при которых не будет значительных искажений контейнера.

Исходя из того, что несколько контейнеров с небольшим количеством информации лучше, чем один большой, следует вывод, что способ суррогатной стеганографии наиболее применим. Имеется способ, который основывается на том, что ветвления кода программы можно записывать в различном порядке. При различных порядках записи ветвления кода программы, получается различный занимаемый объем памяти кодом. Таким образом, если при одном из ветвлений кода программа занимает меньшее количество памяти, а ее функционал остается неизменным, можно в освободившиеся биты программы осуществить вложение необходимой нам информации.

Контейнеры можно разделить по типу организации. По типу организации существует два вида контейнеров: систематические и несистематические. В систематических контейнерах существует возможность указать определенные места стеганограммы, места, где находятся информационные биты самого контейнера и шумовые биты, которые предназначены и используются для скрываемой информации. В несистематических контейнерах такое разделение невозможно, чтобы выделить или узнать скрытую информацию будет необходимо обработать содержимое всей стеганограмы полностью.

Стоит принять во внимание, что при сокрытии информации в контейнере, происходит нарушение структуры или искажение ее статистических свойств искажение. Все это необходимо учитывать, так как от этого зависит уменьшение демаскирующих признаков.

Методы, которые используют специальные свойства форматов представления файлов, следует выделить в отдельную группу:

1. Зарезервированные для расширения поля компьютерных форматов файлов, которые обычно заполняются нулями и не учитываются программой.

2. Специальное форматирование данных (смещение слов, предложений, абзацев или выбор определенных позиций букв).

3. Использование незадействованных мест на магнитных носителях.

4. Удаление идентифицирующих заголовков для файла.

Для большинства современных методов, которые используются для скрытия сообщений в файлах цифрового формата, имеет место зависимость надежности системы от объема встраиваемых данных, представленная на рис. 1.

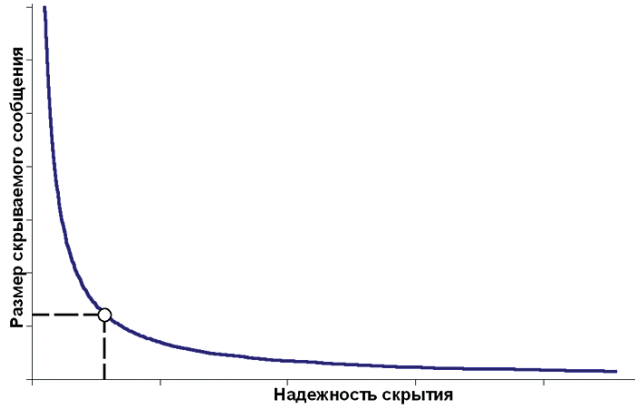

Рис. 1. Диаграмма оптимальных характеристик контейнера стеговложения

Из рисунка 1 следует, что надежность системы сильно снижается при увеличении объема встраиваемых данных [6].

Таким образом, можно смело озвучивать, что вывод сделанный ранее о том, что несколько небольших контейнеров с малым количеством информации намного надежнее и эффективнее одного-двух больших

по объему контейнеров и с большим количеством информации в них.

Ограничивая степень ухудшения качеств контейнера, которые может воспринять человек, можно добиться при стеганографической обработке контейнера либо высокой устойчивости скрываемых данных к модификации или анализу, либо высокого уровня встраиваемых данных. Одновременно данных параметров достичь не удастся, ни в коем случае. При увеличении одного из показателей непременно будет происходить спад другого.

Имея в наличие многие аспекты выбора контейнера, мы можем прийти к решению проблемы выбора величины наиболее выгодного для скрытия данных в исполняемом файле. Все рассуждение схематично показано на рисунке 2 [7].

Рис. 2. Схема, иллюстрирующая выбор идеального контейнера

Вывод

В данной статье были приведены различные способы использования стегоконтейнеров. Исходя из разобранных способов, следует выделить следующую методику. Для того чтобы успешно скрыть сообщение в исполняемый файл необходимо:

– Раздробить сообщение на несколько сообщений небольшого размера/длины.

– Выбрать количество случайных контейнеров фиксированной длины равное количеству частей сообщения.

– Контейнеры обязательно должны быть систематическими, чтобы мы легко могли указать шумовые биты, предназначенные для скрываемой информации.

– Произвести в каждом из контейнеров семантическую замену значимых структурных элементов среды.

Таким образом, разделяя сообщение на несколько, мы увеличиваем количество скрываемых данных, тем самым повышая степень устойчивости контейнера.

Такой подход хорошо применим к ООП, где каждый класс это отдельный файл в который можно вложить данные.

Также, стоит учитывать, что огромное количество контейнеров небольшого размера не принесет желаемых результатов, как показано на рис. 1, и, стоит выбирать оптимальное решение, при выборе между скрываемыми данными и степенью устойчивости сигнала-контейнера.

Литература

1. Intel 64 and IA-32 Architectures Software Developer's Manual. Volume 2A: Instruction Set Reference, A-M: Intel Corp. 2008. 764 p.

2. Intel 64 and IA-32 Architectures Software Developer's Manual. Volume 2B: Instruction Set Reference, N-Z: Intel Corp. 2008. 524 p

3. Ingemar J. Cox. Digital Watermarking and Steganography, Second Edition: Morgan Kaufmann. 2008. 593 p.

4. Красов А.В., Штеренберг С.И., Верещагин А.С. Разработка методов защиты от копирования ПО на основе цифровых водяных знаков внедряемых в исполнимые и библиотечные файлы // Сборник: Актуальные проблемы инфокоммуникаций в науке и образовании. Материалы конференции: сборник научных статей. 2013. С. 847–852.

5. Штеренберг С.И., Виткова Л.А., Андрианов В.И. Методы использования пустых секций исполнимого файла для стеговложения саморазвивающегося кода в распределенной системе однозначного отождествления // Системы управления и информационные технологии. 2015. Т. 59. № 1.1. С. 189–194.

6. Штеренберг С.И., Андрианов В.И. Варианты модификации структуры исполнимых файлов формата PE // Перспективы развития информационных технологий. 2013. № 16. С. 134–143.

7. Штеренберг С.И. Анализ современных методов стеганографии применительно к цифровым носителям // Сборник: Актуальные проблемы инфокоммуникаций в науке и образовании. Материалы конференции: сборник научных статей. 2014. С. 925–932.

Для цитирования:
Шариков П.И. Методика нахождение величины наиболее выгодного контейнера в форматах исполняемых файлов // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 58–62.

METHODS OF FINDING THE VALUE OF THE MOST PROFITABLE CONTAINER FORMATS OF EXECUTABLE FILES

Sharikov Pavel Ivanovich,
St. Petersburg, Russian, Jotass@rambler.ru

Abstract
The describes a problem, as the choice of method for finding the value of the most profitable container formats of executable files. We consider, on which depends the reliability stegosystem and its resistance to steganalysis. In the article the basic criteria put forward by the container in the format of the executable file.
The possible types of containers, as well as how to use them, difficulties in dealing with them. Said effective possible use of certain types of containers and their positive aspects of the embedding information in them. It described and argued to select a certain type of containers. Paid special attention to methods for selection of containers. Explanation is given for each method are described efficient possible use of containers selected by each of the methods considered. Make a choice, within the framework of the problem, in favor of a way of reasoning and choice refer to the effective implementation of this method.
Also, given the distribution of containers by type of organization. We describe the pros and cons of using each type of organization. Powered assumption that the ratio of the amount of information deposited in a container on the choice of the type of container. To opt for one of the types of organization containers. Powered argument profitability and efficiency of its use, at an investment information than others. Is a graph showing another relationship in digital format files. The graph shows the reliability of the system from the scope of the embedded data. When considering this schedule concluded and description for optimum reliability of the system depending on the amount of embedded data.
Combining all aspects of the selection of the container solution is found associated with the selection of the most profitable container and made a drawing that schematically shows the line of reasoning in this article. As a result of the conclusion of the whole work, all the information collected during the study, and provides a methodology to successfully hide the message in an executable file.
Keywords: information hiding, steganography in executable files, containers, container profitable choice.

References
1. Intel 64 and IA-32 Architectures Software Developer's Manual. Volume 2A: Instruction Set Reference, AM: Intel Corp., 2008. 764 p.
2. Intel 64 and IA-32 Architectures Software Developer's Manual. Volume 2B: Instruction Set Reference, NZ: Intel Corp., 2008. 524 p.
3. Ingemar J. Cox. Digital Watermarking and Steganography, Second Edition: Morgan Kaufmann, 2008. 593 p.
4. Krasov A.V. Shterenberg S.I., Vereshchagin A.I. Development of methods of copy protection software based on digital watermarking implemented in executable and library files. In: Actual problems of info-communications in science and education materials of the conference: a collection of scientific articles. 2013. Pp. 847–852. (In Russian).
5. Shterenberg S.I., Vitkova L.A., Andrianov V.I. Methods of using the empty sections of executable code for stegovlozheniya self-developing in a distributed system unambiguous identification. Sistemy upravleniya i informatsionnye tekhnologii. 2015. T. 59. No 1.1. Pp. 189-194. (In Russian).
6. Shterenberg S.I. Andrianov V.I. Options for modifying the structure of executable files format PE. Perspektivy razvitiya informatsionnykh tekhnologiy. 2013. No. 16. Pp.134–143. (In Russian).
7. Shterenberg S.I. Analysis of modern methods of steganography applied to digital media. In: Actual problems of info-communications in science and education materials of the conference: a collection of scientific articles. 2014. Pp. 925–932. (In Russian).

Information about authors:
Sharikov P.I., student, Federal State Educational Budget-Financed Institution of Higher Vocational Education The Bonch-Bruevich Saint-Petersburg State University of Telecommunications.

For citation:
Sharikov P.I. Methods of finding the value of the most profitable container formats of executable files. H&ES Research. 2015. Vol. 7. No. 5. Pp. 58–62. (in Russian).

ITU Kaleidoscope 2015

Trust in the Information Society

Barcelona, Spain, 9-11 December 2015

Papers submission: 6 July 2015

Organized by:

ITU

150 1865 2015

In partnership with:

早稲田大学 WASEDA University

I.E.E.E.J

EURAS

Universidad del País Vasco Euskal Herriko Unibertsitatea

COM SYS

RWTH AACHEN UNIVERSITY

Hosted by:

UAB Universitat Autònoma de Barcelona

METHODOLOGICAL APPROACHES TO FORMALIZE MANAGEMENT INFOCOMMUNICATION SYSTEMS AND NETWORKS OF SPECIAL PURPOSE

Burenin Andrey Nikolaevich,
Ph.D., associate professor, chief specialist of JSC «Research Institute «Rubin», St. Petersburg, Russian, konferencia_asu_vka@mail.ru

Legkov Konstantin Evgenyevich,
Ph.D., deputy head of the Department automated systems of control, Military Space Academy, St. Petersburg, Russian, constl@mail.ru

Keywords: *functioning, infocommunication networks of a special purpose, information influence, management, architectural construction.*

ABSTRACT

Now in the conditions of extension the nomenclature of communication services, customers of telecommunication and infocommunication networks of a special purpose interests first of all their quality and quantitative indices. The main quality and quantitative indices are: the guaranteed quality of service «from the end – in the end», availability of service, existence of a stable continuous communication, mobility, universality of the equipment access, a guarantee of compatibility various standards, possibility of support individual settings and a profile of the consumer services. Therefore effective decisions in the field of management such networks are most important.

The functioning of modern infocommunication system and networks of special purpose (ICN SP) with high quality indicators can be achieved only when all tasks of management. The ever-increasing complexity of organization of various networks included in the ICN SP (personal and facility network, access network, transport network multi-level, network services application level) leads to extremely complicated procedure of decision-making and development of control actions in the development and creation of powerful automated control systems (ACS) ICN SP. So the article, to enable extensive automation of management procedures ICN SP and creation on this basis of the special software complexes of means ACS ICN SP, consistent sets out rather strict methodological approaches to the formulation and management of ICN SP, allowing to develop an appropriate algorithmic support of automated control systems ICN SP.

Currently within departmental communication systems of special purpose creates a number of information systems and telecommunication networks that form in their entirety by the information communication system or the special-purpose network (ICN SP), which is actually information and telecommunication the core of the relevant system connection, and provide users with requested services. [1, 2].

The functioning of the departmental ICN SP with high quality indicators in the conditions of enough rigid requirements of the special users of information systems and Executive bodies, is possible only if the solution of complex management tasks assigned to management information system ICN [3 – 5].

The increased complexity of telecommunication networks, which are part of the departmental ICN (subscriber network, site network, access network, transport network, network services, each network level), and processes of their functioning, increasing the number of used telecommunication and information technology, potential errors in their implementation, and therefore in the provision of services and opportunities opposing parties on the implementation of the various influences on the network, necessitate the development and implementation of sufficiently powerful automated subsystems for monitoring, planning and operational management, which, in turn, significantly increases quality performance of each network, determine critical network resources and prepare data for selection of adequate programme management.

When the various tasks of ensuring management ICN SP are solves, that uses different approaches to the formalized representation of the processes of functioning and management, which can serve as the mathematical theory of control processes of a General type [6].

In the description of various dynamical systems, which, of course, is the inhomogeneous ICN SP, are most often used either linear vector and matrix differential equations, or equations reduced to linear.

Let the operation of the heterogeneous ICN SP is described by vector-matrix equation of the form:

$$\frac{dx(t)}{dt} = Ax(t) + f(t), \quad (1)$$

where $f(t)$ – is some vector function describing deterministic perturbations, including management ICN SP.

In this case $x(t=0)=x_0$, the initial state ICN SP is quite fixed.

Stable steady-state operation ICN SP characterizes the case when the matrix A is constant. This case is extremely important for practice is the aim control ICN SP.

The solution of equation (1) has the following form:

$$x(t) = y(t) + \int_0^t K(t-s) f(s) \quad . \quad (2)$$

In this case, $y(t)$ is a solution of the homogeneous equation and such a representation is a systematic study of the forms of solving various classes of linear functional equations for which a solution is obtained either in the form of (2), or in a more General form:

$$x(t) = y(t) + \int_0^t K(t,s) f(s) \quad . \quad (3)$$

Here it should be noted the important issue of stability of both linear and nonlinear ICN SP. Currently, however, it is not possible to establish a link between like-minded theories of management and sustainability, as the results in the area in which these theories overlap very little.

In General it can be shown that the study of a number of control processes ICN SP leads to the problem of determining such a vector function $f(t)$ that minimizes the functional

$$\Phi(t) = \int_0^t [x(t) - x_0]\, dt + a_1 \int_0^t f(s)\, ds . \quad (4)$$

In (4) a_x is a nonnegative constant, and the variable $x(t)$ associated with the function $f(t)$ equation (2) or (3).

In this case, the control problem can be described as follows. Consider first ICN SP, defined in any time moment the state vector $x(t)$. Suppose that you want to hold in some initial state x_0.

If ICN SP operates in isolation (all by myself), it describes a homogeneous vector equation

$$\frac{dx(t)}{dt} = Ax(t) \quad (5)$$

If this continues, $x(t=0)=x_0$ the initial state ICN SP is fixed.

We agree that we will estimate the deviation from the desired state ICN SP for the time interval [0, T] by means of the functionality

$$\Phi_1(t) = \int_0^T [x(t) - x_0]\, dt \quad (6)$$

Let's call it the price deviations from the desired state ICN SP. We agree also to be a means of price control ICN SP over the same time period, the functional

$$\Phi_2(t) = a_1 \int_0^T f(s)\, ds . \quad (7)$$

The functionals (6) and (7) are quadratic, and the measure of price control will be determined by the price deviation.

If you choose $f(t)$ to minimize the total price deviations from the desired state ICN SP for the time interval [0, T], we arrived at the formulated above problem of control.

Using classical methods for solving obtained linear equation of Euler, which gives the opportunity to use the theory of Hilbert space to display basic properties of the solution, which in General are common for problems of the above type, when a vector function $x(t)$ and the function $f(t)$ are related by equations of the form (2) or (3).

Considered still ICN SP can be called deterministic, in the sense that the behavior of the network in the future is completely determined by its condition at the moment. For the formation of the General approach it was necessary. However, the real ICN SP function in more complex random or even hostile environment.

Let us now consider the more General case, when ICN SP be the impact that is not fully known and may not be taken into account. As examples, we show interference, informational influence, terrorist acts, etc.

One (but not the only, as will be shown below) the path in order to bypass the "ignorance" of the important processes is the introduction of the notion of random function. The notion of helping the formulation of the problem in any case, regardless of whether one believes the designer and official control in fact, it is this influence that accidentally.

Assume, in view of the above, that ICN SP is described by a linear vector equation of the form

$$\frac{dx(t)}{dt} = Ax(t) + f(t) + r(t), \quad (8)$$

where $r(t)$ – is some random vector function characterizing the influence ICN SP.

This means that for any value of t the vector $r(t)$ is a vector random variable with distribution dependent on t.

In such a case defined above the functional (4) is itself a random variable. In order to formulate the minimization problem, we must introduce some mean value functional (4). The simplest of all the averages is the expected value and to solve the problem for this case, it is necessary to determine, due to the linearity of equations (2) and quadratic functional (4), only the expected value as a function of time and the correlation function $R[r(s), r(t)]$.

However, for many generated ICN SP the solution of problems of management it is impossible to implement classical methods. For ICN SP such that the functional that should be minimized linearly f, but the function itself $f(t)$ imposed linear constraints. As a rule, problems of this kind arise in special conditions ICN SP and here the main mathematical

tool is a Lemma the Neyman–Pearson [6], and the applied methods use the properties of the spaces of moments.

In many cases the functioning of the real ICN SP in the special conditions of typical tasks that are neither linear nor sufficiently nonlinear to allow unfettered use of classical methods. To these problems, it is advisable to apply certain combined methods related to determining the minimum on all features $y(t)$ functional

$$\Phi(y) = \int_0^T F(x, y)\, dt \ . \qquad (9)$$

In (9) vector function $x(t)$ and function $y(t)$ the associated differential equation

$$\frac{dx(t)}{dt} = G[x(t), y(t)],\ x(t=0)=x_0,\ 0 \le y(t) \le x(t) \qquad (10)$$

Given in (10), the constraint is usually greatly complicates the solution of the problem, however, is the most natural for the description of different multi-stage processes, and its presence leads to the combination of equations of Euler and imposed inequalities.

For the vast majority of ICN SP function $F(x, y)$ and $G[x(t), y(t)]$ you can specify is quite simple, thus minimizing the function $y(t)$ has a fairly simple structure:

$$y(t) = \begin{cases} 0 & if \ \ 0 \le t \le T_1 \\ y^*, 0 < y^* < x & if \ \ T_1 \le t \le T_2 \\ x & if \ \ T_2 \le t \le T \end{cases} \qquad (11)$$

The values T_1 and T_2 in the General case depend on the values and functions $F(x, y)$ and $G[x(t), y(t)]$.

For each value $t > 0$ there is a linear mapping ρ^* that transforms the vector-function $f(t)$ in the n-dimensional vector with the i-th component equal to

$$\int_0^T \exp[-l_i s] \sum_j a_{ij} f_j(s)\, ds \ . \qquad (12)$$

From (12) it follows that the required time will be the smallest value $t > 0$ at which the set $X_0=\{x_0\}$ itself contains a vector $y(t=0)$, since this vector when $t > t^*$ belongs to a set $X_0=\{x_0\}$, then it needs to be at zero distance from the set $X(t^*)=\{x(t^*)\}$. But since many $X_0=\{x_0\}$, due to a known fact from the theory of Banach spaces, is closed, the set of vector functions $f(t)$ can be topologized so that it is compact, and that each consider the mapping ρ^* was continuous.

If $f^*(t)$ satisfies the ratio $\rho^* f^*(t) = -y(0)$, therefore there are some constants $\theta_1, \ldots, \theta_n$, not all zero, for which the function $f^*(t)$ maximizes the expression

$$\sum_i \theta_i \int_0^{t^*} \exp[-l_i s] \sum_j a_{ij} f_j(s)\, ds \ = \ = \sum_i \int_0^{t^*} \Big(\sum_i \theta_i a_{ij} \exp[-l_i s]\Big) f_j(s)\, ds \ . \qquad (13)$$

It is obvious that the maximum of the expression (13) equal

$$\sum_i \int_0^{t^*} \Big(\sum_i \theta_i a_{ij} \exp[-l_i s]\Big)\, ds \ . \qquad (14)$$

Often functioning ICN SP in the special conditions suggests that extraneous factors it can no longer be regarded as a random function, and it is reasonable to consider them as a kind of hostile to the aims of the network operation. Thus, when in the process of solving tasks of management tend to minimize the measure of price divergence, the opposing side tries to maximize. However, despite the diametrically opposed actions of the parties, to explore and solve problems in which control actions and destructive effects oppose each other, to a certain extent easier. The equation describing ICN SP under these conditions, takes the form:

$$\frac{dx(t)}{dt} = Ax(t) + f(t) + g(t)\ , \qquad (15)$$

where $g(t)$ – is some non-random vector function characterizing the influence ICN SP of the opposing side that may change.

In such stochasticity is introduced by means of the theory of Borel and von Neumann [7], created specifically to research and solve General classes of problems of this kind.

Often in the practical solution of control problems ICN SP the use of the above methods is difficult and perhaps the use of methods based on providing indicators in the form of probabilistic measures of control definition, or providing an extremum of the mathematical expectation of some functional, or performance quantiles, which are also dependent on many random and non-random parameters ICN SP.

$$\Phi^*(y) = M[\Phi(y, Param\ ICN)]. \qquad (16)$$

$$P[\Phi(y, Param\ ICN)] > \Phi_z] \ge P_z\,. \qquad (17)$$

The latter, defined by expression (17), is used most often because it allows to use probabilistic-temporal characteristics of the ICN SP.

Thus, for various kinds of ICN SP and different conditions of their functioning, it is advisable to use those or other methods of solving problems of management presented in this article.

Reference

1. The RF law "On communications", 2007, ed.

2. The conceptual provisions of multiservice communication networks of the Russian Federation. 2001.

3. Burenin A.N. Problemy sistemno-arkhitekturnogo postroeniya avtomatizirovannoy sistemy upravleniya sistemoy svyazi obshchego pol'zovaniya [The problems of system-architecture design of the automated system management system public communications]. Telekommunikatsionnye tekhnologii. 2001. No.1. Pp. 83–94.

4. Burenin A.N., Kurnosov V.I. Teoreticheskie osnovy upravleniya sovremennymi telekommunikatsionnymi setyami [Theoretical bases of management of modern telecommunications networks]. Moscow: Nauka. 2011. 464 p.

5. Legkov K.E., Burenin A.N. Arkhitektura sistem upravleniya sovremennykh infokommunikatsionnykh setey spetsial'nogo naznacheniya [The architecture of the control systems of modern communication networks]. H&ES Research. 2013. Vol. 5. No. 6. Pp. 42–46.

6. Bellman R., Glicksberg I., Gross O. Nekotorye voprosy matematicheskoy teorii protsessov upravleniya [Some problems of mathematical theory of control processes]. Moscow, Izdatel'stvo inostrannoy literatury. 1962. 336 p.

7. Wiener N. Kibernetika, ili upravlenie i svyaz' v zhivotnom i mashine. [Cybernetics, or control and communication in the animal and the machine]. Moscow: Sovetskoe radio. 1958. 567 p.

For citation:
Burenin A.N., Legkov K.E. Methodological approaches to formalize management infocommunication systems and networks of special purpose. H&ES Research. 2015. Vol. 7. No. 4. Pp. 64–67.

МЕТОДИЧЕСКИЕ ПОДХОДЫ К ФОРМАЛИЗАЦИИ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СИСТЕМАМИ И СЕТЯМИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Буренин Андрей Николаевич,
г. Санкт-Петербург, Россия, konferencia_asu_vka@mail.ru

Легков Константин Евгеньевич,
г. Санкт-Петербург, Россия, constl@mail.ru

Аннотация
В настоящее время в условиях расширения номенклатуры услуг связи, заказчиков телекоммуникационных и инфокоммуникационных сетей специального назначения интересует прежде всего их качественные и количественные показатели. Основными качественными и количественными показателями являются: гарантированное качество услуги «из конца - в конец», доступность услуги, наличие устойчивой постоянной связи, мобильность, универсальность оборудования доступа, гарантия совместимости различных стандартов, возможность поддержки индивидуальных настроек и профиля потребителя услуг. Поэтому эффективные решения в области управления такими сетями наиболее важны.
Функционирование современных инфокоммуникационных систем и сетей специального назначения (ИКС СН) с высокими качественными показателями может быть обеспечено только при решении комплекса задач управления ими.
Постоянно возрастающая сложность организация различных сетей, входящих в состав инфокоммуникационной системы специального назначения (абонентские и объектовые сети, сети доступа, многоуровневая транспортная сеть, сети услуг прикладного уровня) приводит к тому, что чрезвычайно усложняются процедуры принятия решений и выработки управляющих воздействий при разработке и создании мощных автоматизированных систем управления (АСУ) ИКС СН.
Для обеспечения возможности осуществления широкой автоматизации процедур управления ИКС СН и создания на этой основе специального программного обеспечения комплексов средств автоматизации АСУ ИКС СН, последовательно излагаются достаточно строгие методические подходы к постановке и решению задачи управления ИКС СН, позволяющие в последствии разработать соответствующее алгоритмическое обеспечение АСУ ИКС СН.

Ключевые слова: функционирование, инфокоммуникационные сети специального назначения, информационное воздействие, управление, архитектурное построение.

Информация об авторе:
Буренин А.Н., к.т.н., доцент, главный специалист ОАО «Научно-исследовательский институт «Рубин»;
Легков К.Е., к.т.н., заместитель начальника кафедры автоматизированных систем управления Военно-космической академии имени А.Ф. Можайского.

Для цитирования:
Буренин А.Н., Легков К.Е. Методические подходы к формализации управления инфокоммуникационными системами и сетями специального назначения. Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 64–67.

ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ МАТЕРИАЛОВ

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.
2. Формульные выражения выполняются в редакторе Math Type. Также в отдельной папке должны содержаться экспортированные изображения формул в формате TIFF (качество изображений не менее 300 dpi). Названия файлов должны соответствовать номерам формул в статье (Например: Формула 1.tif).
3. Объём статьи с аннотацией – от 10 до 20 тыс. знаков. Рисунки и таблицы в объеме статьи не учитываются.
4. Объем аннотации 250-300 слов. Аннотация должна быть информативной (не содержать общих слов), 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.
5. Ключевые слова (не менее пяти).
6. Фамилия, имя, отчество, ученая степень, звание, должность и полное название организации - места работы, город, страна, адрес электронной почты и почтовый адрес каждого автора полностью.
7. 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). Образец оформления списка литературы размещен на сайте журнала.

8. Формулы нумеруются в круглых скобках, источники – в прямых. Нумерация формул и приведение в списке источников, на которые нет ссылок по тексту, не допускается.
9. На английском языке предоставляется: название статьи, фамилия, имя, отчество, город, страна и электронный адрес всех авторов полностью, аннотация, ключевые слова и списки литературы (по стандарту Harvard).

В конце размещается полная информация об авторах (возможно размещение кратких автобиографий): фамилия, инициалы, должность, ученая степень, ученое звание, место работы (организация) и другие данные с надписью (Information about authors).

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 и формул в формате TIFF, по требованиям указанным в п.2. Тексты в рисунках должны быть читаемы.
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.

MANUSCRIPT REQUIREMENTS

Format

1. All files should be submitted as a Word document.
2. Articles should be between 15000 and 20000 characters (incl. spaces).
3. Article Title to be submitted in native language and English. A title of not more than eight words should be provided.

Author Details (in English and native language)

Details should be supplied on the Article Title Page including:

* Full name of each author
* Position, rank, academic degree
* Affiliation of each author, at the time the research was completed
* Full postal address of the affiliation
* E-mail address of each author
* Structured Abstract (in English and native language)
* Abstract should be: informative (no general words), original, relevant (reflects your papers key content and research findings); structured (follows the logics of results presentation in the paper), concise (between 250 and 300 words).
* Purpose (mandatory)
* Design/methodology/approach (mandatory)
* Findings (mandatory)
* Research limitations/implications (if applicable)
* Practical implications (if applicable)
* Social implications (if applicable)
* Originality/value (mandatory)

It is appropriate to describe the research methods/methodology if they are original or of interest for this particular research. For papers concerned with experimental work describe your data sources and data procession technique. Describe your results as precisely and informatively as possible. Include your key theoretical and experimental results, factual information, revealed interconnections and patterns. Give special priority in your abstract to new results and long-term impact data, important discoveries and verified findings that contradict previous theories as well as data that you think have practical value.

Conclusions could be associated with recommendations, estimates, suggestions, hypotheses described in the paper.

Information contained in the title should not be dublicated in the abstract. Try to avoid unnecessary introductory phrases (e.g. the author of the paper considers).

Use the language typical of research and technical documents to compile your abstract and avoid complex grammatical constructions. The text of the abstract should include key words of the paper.

Keywords (in English and native language)

Please provide up to 5 keywords on the Article Title Page, which encapsulate the principal topics of the paper.

Figures

All figures should be of high quality, legible and numbered consecutively with arabic numerals. All figures (charts, diagrams, line drawings, web pages/screenshots, and photographic images) should be submitted in electronic form preferably in color as separate files, that match the following parameters: TIFF format (quality of figures not less than 300 dpi).

References

References to other publications must be in Harvard style and carefully checked for completeness, accuracy and consistency.