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.

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

Том VII. № 3-2015

Издается с 2009 года
ISSN 2412-1363 (Online)
ISSN 2409-5419 (Print)
Издательская лицензия ПИ № ФС 77-60899
Язык публикаций: русский, английский
Периодичность выхода – 6 номеров в год
Сайт журнала: **www.H-ES.ru**

УЧРЕДИТЕЛЬ:
ООО «Издательский дом Медиа Паблишер»

ГЛАВНЫЙ РЕДАКТОР:
Константин Легков
HT-ESResearch@yandex.ru

ИЗДАТЕЛЬ:
Светлана Дымкова
HESRes@yandex.ru

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.

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.**

обложка: Оксана Иванова

ТЕМАТИЧЕСКИЕ НАПРАВЛЕНИЯ (Topical Columns)

- **Вопросы развития автоматизированных систем управления** / Automated control systems
- **Физико-математическое обеспечение разработки новых технологий** / Physical and mathematical software development of new technologies
- **Развитие автоматизированных систем управления технологическим процессом** / Development of automated process control systems
- **Вопросы исследования космоса** / Questions of space exploration
- **Телекоммуникационные технологии и технические новинки систем подвижной связи** / Telecommunication technology and technical innovations of mobile systems
- **Перспективы развития единого инфокоммуникационного пространства** / Prospects for unified info communication space
- **Использование радиочастотного спектра в системах подвижной связи** / Use of a radio-frequency range in systems of mobile communication
- **Антенно-фидерное оборудование** / Antenna-feeder equipment
- **Спутниковое телевидение, системы спутниковой навигации, GLONASS, построениенавигационных систем GPS** / Satellite TV, satellite navigation system, GLONASS, GPS navigation systems construction
- **Вопросы развития геодезии и картографии** / Issues of Geodesy and Cartography
- **Информационная и кибербезопасность** / Information and cyber security
- **Вопросы исследования Арктики** / Questions Arctic research
- **Волоконно-оптическое оборудование и технологии** / Fiber-optic equipment and technology
- **Метрологическое обеспечение** / Metrological maintenance
- **Программное обеспечение и элементная база для сетей связи** / Software and electronic components for communication networks
- **Производители, поставщики и дистрибьюторы телекоммуникационного оборудования** / Manufacturers, suppliers and distributors of telecommunications equipment
- **Работа отечественных ассоциаций, региональных и координирующих операторов** / National associations, regional and coordinating operators
- **Правовое регулирование инфокоммуникаций, законодательство в области связи** / Legal regulation of Infocomm, legislation in the communication field
- **Экономика связи, конвергенция сетей, универсальные коммуникации** / Economy of communications, networks convergence, universal communication
- **Выставки, форумы, конференции, семинары, интервью (оригинальные и новые проекты, итоги деятельности, проблемы отрасли и пути их решения и т.д.)** / Exhibitions, forums, conferences, seminars, interview (оригинальные и новые проекты, итоги деятельности, проблемы отрасли и пути их решения и т.д.)

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.

The journal is included in the Russian index of scientific citing.

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

H&ES RESEARCH

It is published since 2009
ISSN 2412-1363 (Online)
ISSN 2409-5419 (Print)
Publishing license ПИ № ФС 77-60899
Language of publications:
Russian, English
Periodicity – 6 issues per year

FOUNDER: «Media Publisher», LLC

EDITOR IN CHIEF:
Konstantin Legkov
HT-ESResearch@yandex.ru

PUBLISHER:
Svetlana Dymkova
HESRes@yandex.ru

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

Hi-tech Earth Space RESEARCH

24-я НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

29 июня – 02 июля

Санкт-Петербург

поселок Репино
загородный клуб
«forRestMix»

МиТСОБИ -2015

ОРГАНИЗАТОРЫ
МОО «Ассоциация Защиты Информации»
ЗАО «НПП «СТЗИ»
ООО «НеоБИТЭ»

СОУЧРЕДИТЕЛИ
Комитет по информатизации и связи
Правительства Санкт-Петербурга
Комитет по науке и высшей школе
Правительства Санкт-Петербурга
ФГАОУ ВО «Санкт-Петербургский
политехнический университет Петра Великого»

ПРИ УЧАСТИИ
Федеральной службы безопасности РФ,
Федеральной службы по техническому
и экспортному контролю,
Управление специальной связи
и информации ФСО России в СЗФО,
Федеральной службы по финансовому мониторингу

ОРГАНИЗАЦИОННАЯ ПОДДЕРЖКА
РОСТЕЛЕКОМ, ЗАО «РНТ»
ЗАО «ГОЛЛАРД», ИКСИ, R-Stale
ЗАО «ИнформИнвестГрупп»
ЗАО «Лаборатория Касперского»
«РЦЗИ «ФОРТ», ОАО «ИнфоТеКС», НИИГлоб
ООО «ИБМ Восточная Европа/Азия»
ЗАО РКСС, ФГУП «НИИ «Квант»

Конференция посвящена проблемам развития новых современных направлений в области защиты компьютерных систем, программно-аппаратного обеспечения безопасности информационных технологий с применением современных зарубежных систем и подготовке специалистов в данном направлении. Особое внимание будет уделено безопасности электронных услуг, предоставляемых населению, облачным системам и Grid- системам и современным проблемам противоборства в киберпространстве. Актуальность данного направления деятельности научных и производственных организаций обусловлена стремительным развитием систем телекоммуникаций и ростом потоков обрабатываемой информации, повышением роли информационных ресурсов в принятии инновационных решений, политической обстановкой, складывающейся как вокруг, так и внутри России.

Формат конференции: пленарные и секционные заседания, круглые столы по тематике, предложенной спонсорами конференции. В ходе проведения конференции будет работать постоянно действующая выставка, на которой будут проводиться презентации продукции участников конференции. К началу конференции Оргкомитет готовит издание программы конференции, включающей материалы докладов и сообщений, с которыми участники конференции выступят на пленарных заседаниях, а также в ходе работы нескольких секций. В рамках конференции состоится финал ежегодного соревнования по кибербезопасности – «NeoQUEST-2015», организованный компанией «НеоБИТ». В «NeoQUEST-2015» кроме соревнования будут представлены практические доклады и конкурсы, освещающие актуальные киберугрозы и способы защиты от них.

Основные направления работы конференции
Ппредполагается роводить заседания по следующим секциям:
Секция 1: «Кибербезопасность высокотехнологических критических систем. Современные угрозы, безопасность программного обеспечения».
Секция 2: «Создание национальной безопасной программной платформы. Доверенная вычислительная среда».
Секция 3: «Безопасность облачны, виртуальных систем и систем с динамической архитектурой».
Секция 4: «Высокопроизводительные средства защиты и обработки сетевой информации. Безопасность Интернет вещей. Обнаружение вторжений».
Секция 5: «Криптографические методы защиты информации».
Секция 6: «Противоборство в киберпространстве».
Секция 7: «Пленум Северо-Западного регионального отделения УМО по образованию в области информационной безопасности». Круглый стол: обсуждаем образовательные стандарты в области информационной безопасности.
Секция 8: NeoQUEST-2015 «Практические аспекты безопасности современных информационных технологий».

По всем вопросам, связанным с участием, просим Вас обращаться к организаторам Конференции:
Савельева Зоя Сергеевна – (812)552-64-80, (812)552-76-32;
Зегжда Петр Дмитриевич – (812) 552-64-89
Факс (812) 552-76-32, E-mail: elena.a@ibks.ftk. spbstu.ru.
Зарегистрироваться для участия в работе конференции можно по адресам: mitsobi.ru /митсоби.рф

СОДЕРЖАНИЕ

НОВОСТИ

Новости науки и техники, события, люди 6

РАДИОТЕХНИКА И СВЯЗЬ

Ершов Г.А., Синицын Е.А., Фридман Л.Б.
Компенсация искажений фазоманипулированного сигнала с целью улучшения характеристик его сжатия 16

АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

Хашагульгов Р.А., Ходор М.А.
Частная авиация – новая угроза безопасности воздушного движения в России 22

ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ

XIX Международный Форум «Инфокоммуникации устойчивого развития» в рамках деловой программы 27-й международной выставки «Связь-Экспокомм-2015» 28

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Курчидис В.А., Попов Т.А., Анисимов О.В.
Предикатная модель схемно-ориентированных запросов обслуживающего персонала в системах информационной поддержки 30

Тарасов А.Г., Дорожко И.В.
Логико-параметрический подход к моделированию живучести автоматизированных систем подготовки и пуска ракет космического назначения в условиях возникновения нештатной ситуации 38

ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ

Буренин А.Н., Легков К.Е.
Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей 46

СПУТНИКОВОЕ ТЕЛЕВИДЕНИЕ

«Космическая связь» вводит в эксплуатацию новый космический аппарат связи и вещания «Экспресс-АМ7» в орбитальной позиции 40° восточной долготы 62

ПУБЛИКАЦИИ НА АНГЛИЙСКОМ ЯЗЫКЕ

Гон Хасон
Причины ложных срабатываний автоматической пожарной системы оповещения и планы по ее усовершенствованию в Корее 64

CONTENTS

NEWS

6 News of science and technology, events, people

RF TECHNOLOGY AND COMMUNICATION

16 **Ershov G.A., Sinitsin E.A., Fridman L.B.**
Distortion compensation of phase-manipulated signal to improve the characteristics of its compression

AVIATION, SPACE-ROCKET HARDWARE

22 **Khashagulgov R.A., Hodor M.A.**
Private aviation is a new threat to security air traffic in Russia

INFOCOMMUNICATION SYSTEMS

28 The XIX International Forum «Infocommunications of a sustainable development» within the business program of the 27th international exhibition «Svyaz-Expokomm-2015»

INFORMATICS, COMPUTER ENGINEERING AND CONTROL

30 **Kurchidis V.A., Popov T.A., Anisimov O.V.**
The predicate model of scheme-oriented queries for staff in information support systems

38 **Tarasov A.G., Dorozko I.V.**
Logically-parametric approach to survivability simulation of automated systems preparation and launching of space rockets in case of emergency

INFORMATION AND CYBERSAFETY

46 **Burenin A.N., Legkov K.E.**
Security issues infocommunication systems and networks for special purposes: the main threats, the ways and means of ensuring comprehensive network security

SATELLITE TELEVISION

62 Space Communication places in operation the new communication and broadcasting spacecraft «Express AM7» at the orbital position of 40 ? east longitude

PUBLICATIONS IN ENGLISH

64 **Kong Ha Sung**
Cause of false positive of automatic fire notification system and improvement plan in Korea

К 70-летию Великой Победы: разработки ученых во время войны

Накануне войны Томск представлял собой один из крупнейших за Уралом научно-образовательных центров страны, здесь находилось 6 вузов, 19 техникумов и ряд научно-исследовательских учреждений. Летом 1941 года этот мощный научный комплекс смог быстро мобилизовать свои ресурсы и перестроить всю деятельность на военные нужды. Ученые Томского государственного университета и других вузов города занялись исследованиями и созданием разработок для армии, промышленных предприятий, транспорта, медицинских учреждений.

Уже через пять дней после начала войны, 27 июня 1941 года, в Томске был создан Томский комитет ученых по содействию промышленности, транспорту и сельскому хозяйству в военное время. Это была первая общественная организация подобного рода в стране, призванная организовать эффективную работу ученых в интересах обороны и тыла.

«Мы, томские ученые, – сказал на городском собрании научных работников 3 июля 1941 года профессор ТГУ, основатель Сибирского физико-технического института Владимир Кузнецов, – должны немедленно организовать единый коллектив, объединенный страстной мыслью –разгромить и уничтожить врага... должны все то, что есть лучшее у нас, отдать Родине».

Председателем комитета стал биолог, создатель учения о фитонцидах профессор ТГУ Борис Токин. Комитет располагался в здании Сибирского физико-технического института при ТГУ (СФТИ). На заседания собирались директора и главные инженеры заводов, профессора томских и эвакуированных в Томск вузов.

Перед учеными была поставлена задача использовать достижения науки для укрепления обороны страны, готовить кадры специалистов, в которых нуждалась армия, оборонные предприятия и транспорт, госпитали.

Научная работа велась по самым разным направлениям:

- военная оптика, акустика;
- исследование бронепробиваемости и бронестойкости;
- создание прочных сплавов, дефектоскопов и многим другим.

Важной частью этой работы была помощь госпиталям в лечении раненых. В условиях войны страна лишилась многих товаров, поступающих из-за рубежа, в том числе лекарственных средств и приборов медицинского назначения. Необходимо было в короткий срок найти им замену, а также создать свои разработки, помогающие спасению людей. Одной из таких разработок стал радиощуп, предназначенный для обнаружения металлических осколков в теле раненых.

Идея использовать электромагнитные явления для обнаружения металлических предметов (пуль, осколков) принадлежала старшему лаборанту Томского индустриального института Петру Одинцову. Реализовал же эту идею доцент Томского государственного университета Борис Кашкин. Прибор был создан под руководством профессора Александра Сапожникова в Сибирском физико-техническом институте при ТГУ и назван искателем Одинцова-Кашкина.

Этот искатель или, как его обычно называли, радиощуп мог легко и нетравматично находить осколки в теле человека во время операции. Первые приборы поступили в томские госпитали уже осенью 1941 года. Кашкин и Сапожников сами были частыми ассистентами на операциях, работая с прибором.

После того, как радиощуп успешно прошел испытания в Томске, его описание было послано в Государственный комитет обороны, в Наркомздрав и в СибВО. В проекте решения бюро Новосибирского обкома ВКП(б) от 5 января 1942 года, в частности, отмечалось: «Изобретенный в Томске радиощуп Кашкина-Одинцова для обнаружения местонахождения металлических включений в теле раненого рекомендовать Наркомздраву использовать во всех госпиталях СССР. Обязать зав. облздравом (т. Лапченко) в течение 2-х месяцев снабдить каждый госпиталь Новосибирской области прибором радиощупом».

Радиощуп благодаря простоте в использовании, небольшому размеру и эффективности стал быстро завоевывать популярность, и не только в Томске. Заказы поступали из самых разных регионов России. Например, командование эвакуационным госпиталем №3284, находящимся в Саратове, в своем запросе от 21 мая 1942 года просило срочно выслать один прибор. В заявке также сообщалось: «Ведущий хирург-консультант эвакоуправления – проф. Э.М. Эйбер берет на себя обязательство, проработав с вашим аппаратом не менее 1000 операций, в самое короткое время дать вам свои наблюдения как обмен опытом».

Заказов было так много, что томский комитет ученых даже обратился к начальнику Санитарного отдела СибВО бригадврачу А.Н. Правдину: «В связи с многочисленными запросами на радиощупы со стороны госпиталей, а также главного сануправления (Москва), просим Вас поставить вопрос перед соответствующими организациями о снабжении мастерских СФТИ нужными материалами для изготовления радиощупов».

В августе 1942 года руководство Томского комитета ученых «в связи с полной апробацией многочисленными хирургами и госпиталями радиощупа» решило просить горком партии поддержать инициативу директора завода №625 о его серийном производстве при научной консультации сотрудников СФТИ.

С 1942 года радиощуп стал активно применяться и на фронте. Благодаря этому изобретению томских ученых было спасено немало жизней.

Искусственный интеллект создается в России

В то время как такие западные гении, как Стивен Хокинг, Элон Маск и Стив Возняк предупреждают человечество о том, что искусственный интеллект вот-вот поработит нас, в России ученые готовы отдать под его контроль боевую технику. Ближайшие 10 лет станут для нашей страны станут поворотными. Во-первых, должен появиться первый боевой робот-аватар. А во-вторых, роботы с развитым искусственным интеллектом.

«ФПИ ставит перед собой задачу создания искусственного интеллекта. Я думаю, что он будет создан в ближайшей перспективе – в течение 7–10 лет. Конструктивная постановка задачи – создание искусственного оператора, который хорошо решает интеллектуальные рациональные задачи и способен заменить человека при решении этих задач», – поделился заместитель гендиректора Фонда перспективных исследований (ФПИ) Сергей Гарбук между выступлениями на конференции «Информационные технологии на службе оборонно-промышленного комплекса». Этот оператор, по словам Гарбука, сможет управлять боевой техникой или выявлять террористов в толпе людей, мог бы выполнять функцию диспетчера аэропорта и так далее.

Замглавы ФПИ отметил, что на данный момент созданные роботы лишены искусственного интеллекта, но ученые близки к его созданию. По сути, это будет «некая информационная система, но выполненная на новых архитектурных принципах».

Сергей Гарбук сказал, что сейчас ФПИ старается проводить постоянно действующий конкурс, на котором будут объявлены интеллектуальные задачи и установлены квалификационные уровни, преодоление которых будет считаться созданием искусственного интеллекта в каком-либо аспекте. «Мы планируем финансировать лучшие проекты. Такие разработки ведутся уже давно, мы хотим их упорядочить», – сказал Гарбук.

Замглавы ФПИ подчеркнул, что в РФ имеется очень серьезная школа исследований по данному направлению, в частности действует Российская ассоциация искусственного интеллекта. В СССР, по словам собеседника журнала, «исследования в этой области начались еще в 1960-е годы и не прекращались никогда». Также он напомнил, что в России имеется очень серьезная математическая школа в области искусственного интеллекта.

Между тем величайшие умы человечества не устают напоминать нам об опасности, которую таит в себе искусственный интеллект. «Уже в ближайшие 100 лет искусственный интеллект превзойдет человеческий, – уверен профессор Кембриджского университета и знаменитый астрофизик Стивен Хокинг. – И до того, как это случится, мы должны сделать все, чтобы цели машин совпадали с нашими». Хокинг считает, что искусственный интеллект должен быть под контролем человека, иначе всем нам придет конец. Билл Гейтс и Элон Маск вторят ему, а сооснователь Apple Стив Возняк и вовсе считает, что человек станет для роботов домашним животным: «Сейчас мы создаем эти умные девайсы, чтобы они заботились о нас, но в итоге они станут более сообразительными и избавятся от человека», – говорил Возняк.

Российские ученые исследуют черные дыры

Роскосмос принял решение о продлении работы российской космической радио-обсерватории «Радиоастрон» до конца 2016 года. Уникальный исследовательский комплекс, который включает спутник «Спектр-Р», получил разрешение на проведение третьей научной программы наблюдений.

Радио-обсерватория «Радиоастрон» была запущена в июле 2011 года с космодрома «Байконур». Она стала первым и наиболее технически совершенным астрофизическим инструментом, который был создан российскими специалистами. Основная цель запуска станции – обеспечение возможности совместной работы с наземной и глобальной сетью радиотелескопов. Вместе с «Радиоастроном» они образуют РСДБ – единый наземно-космический интерферометр со сверхдлинной базой.

Юрий Ковалев, заведующий лабораторией Астрокосмического центра ФИАН, заявил, что текущая открытая программа наблюдений АО2 завершается в июле. Ей на смену придет новый этап изучения радиовселенной, в рамках которого российские специалисты совместно с коллегами из Испании, Японии, США и Нидерландов получат возможность задействовать инструменты «Радиоастрона» для проведения масштабных исследований космоса.

Экспертный совет миссии и руководитель программы, академик Николай Кардашев из АКЦ ФИАН, в течение последних нескольких месяцев занимались отбором проектов, которые будут включены в программу экспериментов АО3. Девять наиболее перспективных направлений – это возможность приблизиться к ядрам далеких галактик, «пощупать» образовавшиеся в них черные дыры и изучить структуру джетов – тонких пучков переработанной материи, выпускаемых сверхмассивными черными дырами.

Навигационный рынок – перезагрузка. Новые маршруты

Как будет развиваться рынок навигации в ближайшем будущем? Произойдет ли перезагрузка? Какие решения идут на замену? Эти и многие другие актуальные вопросы навигационной отрасли обсуждались ведущими экспертами в рамках IX Международного навигационного форума, который прошел 22-23 апреля в Москве, совместно с 7-й Международной выставкой «Навитех-2015».

В IX Международном навигационном форуме приняли участие около 1400 делегатов из 550 компаний из стран Евразийского Экономического Союза, Европейского Союза, БРИКС, включая такие страны, как: Австрия, Белоруссия, Великобритания, Германия, Индия, Италия, Казахстан, Китай, Литва, Нидерланды, Объединенные Арабские Эмираты, Соединенные Штаты Америки, Туркменистан, Франция.

Среди зарегистрированных участников Форума – представители федеральных и региональных органов государственной власти Российской Федерации, представители органов власти стран СНГ, делегаты ведущих российских и зарубежных навигационных, информационных, автомобильных и других компаний, работающих в сфере навигации и смежных отраслях. Форум и Выставка традиционно являются центральными событиями навигационного года в России и странах СНГ.

В начале пленарного заседания прошла церемония награждения премией в области навигации, учрежденной Ассоциацией «ГЛОНАСС/ГНСС-Форум». В этом году в восьмой раз были отмечены заслуги людей, внесших неоценимый вклад в развитие навигационных технологий. В номинации «За вклад в создание и развитие системы ГЛОНАСС» награждены: Лебедкин Геннадий Дмитриевич – профессор Академии проблем безопасности, обороны и правопорядка; Полищук Георгий Максимович – заместитель генерального директора Холдинга «СТК «Союз»; Персев Виктор Степанович – начальник отдела научно-технического и информационного сопровождения программ развития средств КВНО ФГУП ЦНИИмаш; Ельцова Оксана Львовна - внесла большой личный вклад в подготовку федеральной целевой программы «Глобальная навигационная система»; Ревнивых Сергей Георгиевич и Климов Владимир Николаевич – являются авторами идеи создания первой целевой программы создания глобальной навигационной спутниковой системы ГЛОНАСС, принимали активное участие в ее подготовке и реализации. В номинации «За внедрение навигационных технологий» за многолетний добросовестный труд, большие заслуги в научной деятельности и реализации проектов по внедрению навигационных технологий с использованием системы ГЛОНАСС награждены: Ганин Александр Анатольевич – первый заместитель генерального директора ФГУП «Космическая связь»; Лебедев Михаил Григорьевич – советник генерального директора концерна ПВО «Алмаз-Антей»; Шепотько Иван Семенович – ведущий консультант ПАО «НИС».

В рамках пленарного заседания навигационного форума помощник Президента Российской Федерации Левитин Игорь Евгеньевич отметил: «За прошлый год количество навигационных приборов в мире превысило 3,5 млрд., из них 60% используют сигналы российской системы ГЛОНАСС. Это наглядное свидетельство престижа отечественного проекта, подтверждение высокого технологического уровня». Также Игорь Евгеньевич обратил внимание на то, что решение различных актуальных задач открывает новый этап российской и международной навигации.

Министр транспорта Российской Федерации Соколов Максим Юрьевич отметил, что навигационные технологии прочно вошли в нашу повседневную жизнь. ГЛОНАСС-технологии активно используются в государственной сфере, в работе всего транспортного комплекса, всех его отраслей. Системы диспетчеризации и мониторинга, логистики, обеспечения безопасности, интеллектуальные транспортные системы, тахографический контроль работают с применением спутниковой навигации. И это закономерно. По оценкам специалистов, потенциальный экономический эффект, достигнутый от использования навигационных технологий, может составить более половины процента от внутреннего валового продукта страны.

По словам Максима Соколова, главным событием прошедшего года стало решение о вводе в промышленную эксплуатацию с 1 января 2015 года государственной системы

«ЭРА-ГЛОНАСС». Россия не на шаг, а на несколько шагов опередили создание и применение аналогичных систем и в Европе, и в Америке, и в Китае и других странах мира. Создание системы «ЭРА-ГЛОНАСС» является полномасштабным проектом в сфере навигационной деятельности, обеспечения транспортной безопасности и безопасности на транспорте, которая, в первую, очередь направлена на спасение человеческих жизней.

Заместитель Руководителя Федерального Космического Агентства Хайлов Михаил Николаевич рассказал о состоянии и перспективах системы ГЛОНАСС. «Благодаря усилиям федеральных органов и промышленности, мы вышли на полноценную группировку (24 аппарата, используемых по целевому назначению, обеспечивающие предоставление навигационного сигнала ста процентам территории Земного шара), вышли на точность, соизмеримую с системой GPS (2,8 м) и начали летные испытания космического аппарата нового поколения «ГЛОНАСС-К» – констатировал современное состояние группировки Хайлов. По словам Михаила Николаевича, дальнейшие задачи Федерального космического агентства заключаются в поддержании и развитии имеющейся группировки, а именно: развитие орбитального сегмента, развитие наземного сегмента и развитие международного сотрудничества в целях продвижения системы ГЛОНАСС.

«За девять лет наш навигационный форум прошел большой путь: получил статус международного, стал центральным событием навигационной отрасли на пространстве СНГ. Вслед за развитием навигационных технологий ГЛОНАСС изменилась и тематика форума. Сегодня в центре внимания – эффективное использование возможностей навигационных, информационных и коммуникационных технологий на транспорте, в различных отраслях экономики, в интересах всех категорий потребителей, – сказал Александр Гурко, Президент Некоммерческого партнерства «ГЛОНАСС». – «Партнерство из года в год выступает стратегическим партнером Форума и демонстрирует ключевые тенденции рынка в рамках выставки «Навитех». Важнейшее навигационное событие прошедшего года в России – это, безусловно, ввод в эксплуатацию государственной системы «ЭРА-ГЛОНАСС», в основе работы которой – применение технологий ГЛОНАСС. Следующий шаг – использование возможностей «ЭРА-ГЛОНАСС» в интересах российских автомобилистов, федеральных, ведомственных и региональных систем, бизнеса. Именно это станет главным драйвером развития технологий ГЛОНАСС и российского навигационного рынка».

Объем мирового навигационного рынка в 2014 году составил 65 млн евро, к 2020 году эта цифра возрастет практически вдвое – до 100 млрд евро. На данный момент количество навигационного оборудования в мире уже превысило 3, 5 млрд устройств, из которых 2, 5 млрд это смартфоны.

По оценкам аналитиков НП «ГЛОНАСС», основными дайверами мирового развития навигационной отрасли в ближайшие 3-5 лет станет капитализация посредством коммерческих сервисов (информационных, безопасности, платежных, страховых, технической поддержки) возможностей «подключенного (к интернету) автомобиля» (Connected Car); развитие технологий V2X – информационного обмена «автомобиль – автомобиль» V2V, «автомобиль – инфраструктура V2I», «автомобиль – человек» V2P; развитие навигационных технологий в интересах транспортных средств (робомобили, БПЛА) и роботов; технологии единой навигации для потребителя: спутниковой, инерциальной, indoor навигации; технологий навигации повышенной точности и гарантированной надежности.

Дополнительными драйверами для технологий ГЛОНАСС на ближайшие годы, по мнению экспертов, станет оснащение транспорта приборами контроля режима труда и отдыха водителей (тахографами), создание системы возмещения ущерба федеральным дорогам большегрузным транспортом (12-тонники) и экспорт ГЛОНАСС решений в страны Евразийского Экономического Союза, ШОС и БРИКС.

Говоря о развитии системы ГЛОНАСС, нужно заметить, что система обновления карт также усовершенствуется. В рамках круглого стола «Безопасность и навигация: дальше только вместе» с докладом на тему: «Совершенствование системы обеспечения данными ГЛОНАСС государственного топографического мониторинга в интересах формирования ГИС – «Арктика», выступил Ефимов Сергей Анатольевич, Директор научно-технического комплекса, ОАО «НИиП центр «Природа». Он говорил об использовании топографической основы при обновлении карт и новом подходе к определению время обновления той или иной местности. Сергей Анатольевич отметил, что топографический мониторинг состоит из обзорного мониторинга (определение территорий нуждающихся в обновлении по космической съемке) и детального мониторинга (выявление изменений местности). Завершается процесс мониторинга созданием опытного образца. Применение ГЛОНАСС происходит, как на этапе детального мониторинга, так и на этапе полевого дообследования территорий, а также в процессе беспилотной съемки. Крайне важно, что вся информация хранится в базах данных, и есть возможность прослеживать изменения на протяжении многих лет.

В рамках Форума российские разработчики акцентировали внимание на тенденции к объединению, комплексированию различных технологий в рамках создания навигационно-информационных систем.

По мнению директора по маркетингу SpaceTeam® Светланы Хадоновой, классические системы мониторинга транспорта постепенно отходят на второй план. «Заказчиков интересуют комплексные решения, которые позволили бы решать широкий комплекс задач конкретного предприятия: это и обеспечение безопасности перевозок, и обеспечение информационной безопасности, и контроль работы транспорта в режиме реального времени с учетом множества различных параметров,

и помощь в планировании работы, и повышение эффективности работы, и экономия на содержании автопарка и мн. др.». Так, например, для перевозки опасных грузов мы создаем специализированное, заточенное под требования Заказчика, взрывозащищенное устройство с установкой датчиков работы исполнительных устройств, выполняющих, в том числе функции диагностики», – прокомментировала Светлана Хадонова.

На коммерческом рынке появляются многопрофильные навигационные ГЛОНАСС/GPS устройства, совмещающие множество функций, полезных потребителю. Поддержка протокола «ЭРА-ГЛОНАСС», навигация с функцией контроля пробок, видеорегистрация, тахограф, мультимедийный комплекс, мониторинг и диагностика транспортного средства, алкозамок, коммутационное устройство, контроллер для платных дорог в ближайшее время могут быть технически объединены в многопрофильное навигационное устройство и предоставлять потребителю единый телематический сервис.

Развитие навигационных сервисов в интересах массовых потребителей четко прослеживается в сфере позиционирования внутри зданий (indoor-навигации). На круглом столе: «Индор-навигация: потребители в ожидании простых и эффективных решений» Florian Freitag, Руководитель проекта indoo.rs рассказал о реальных кейсах разработанных его компанией, это использование приложений в торговых центрах, аэропортах, офисах и других помещениях для навигации в помещении. Florian сказал, что их проекты нацелены на клиента и могут удовлетворять множество потребностей, таких как сбор аналитики, позиционирование и другие. Технология работает на Wi-Fi, IP – радиосигналах в сочетании с инновационными сенсорами в самих смартфонах, гироскопами всем вместе взятым. Спикер придал особое значение пользе подобных приложений для инвалидов, слепых людей, а также для служб безопасности. Подводя итог выступления, Florian выделил сферы, наиболее активно интересующиеся подобными приложениями: это авиация и розничная торговля.

Навигация внутри помещений относительно новый продукт на российском рынке и на сегодняшний день участники форума отметили, приоритетным направлением для России и российских компаний остается навигационный рынок на автотранспорте, составляя основной эффект (до 80%) от применения технологий спутниковой навигации.

Суперкомпьютер раскрыл тайну укладки ДНК

Суперкомпьютер «Ломоносов», созданный российской компанией «Т-Платформы» для Московского государственного университета (МГУ), обеспечил проведение исследования принципов укладки ДНК. Ученые выполнили моделирование на суперкомпьютере и нашли объяснение форме укладки нитей дезоксирибонуклеиновой кислоты по принципу спагетти.

По словам ученых, в ядре клетки молекула ДНК упаковывается в виде фрактальной глобулы – «комка», в котором не существует узлов, причем структура петель нитей повторяется в крупных и малых масштабах. Если представить, что ДНК – это длинная леска от спиннинга, то, уронив её на пол и потянув за концы, вы без труда распутаете глобулу, так как она состоит из множества свободных петель разного размера. Такой принцип укладки ДНК напоминает брикет лапши «Доширак» и обеспечивает возможность эффективного считывания с нитей информации.

Процесс укладки ДНК протекает под действием ускоренной тепловой диффузии. Аналогичная теория была разработана учеными для звена полимерной цепи, включающей до 250 000 звеньев. Цепь также свернута во фрактальную глобулу. Для исследования явления ученые выполнили моделирование полимерной цепи на суперкомпьютере «Ломоносов» и проанализировали параметры тепловых процессов, происходящих в ней.

В МГУ отмечают, что фрактальную глобулу предсказали ещё в 1988 году физики Александр Гросберг, Сергей Нечаев и Евгений Шахнович. Исследователи назвали её складчатой, однако с переименованием термина его суть не изменилась.

Компьютерное моделирование позволило виртуально «уложить» хроматиновую цепочку во фрактальную глобулу, отслеживая тепловые процессы, происходящие внутри. Ранее исследователям не удавалось получить достоверные результаты моделирования слишком длинных цепочек, так как процесс их прихода в равновесное состояние занимал слишком много времени, а до этого момента исследование тепловой диффузии является нецелесообразным.

«Ломоносов» показал, что частицы, являющиеся звеньями хроматиновой цепочки, во фрактальной глобуле движутся быстрее, чем в обычной – квадрат теплового смещения растет в степени 0,4, а не в степени 0,25. Вероятно, это и определило выбор метода спагетти в качестве способа укладки ДНК в ядре.

Моделирование на суперкомпьютере «Ломоносов» позволило понять, как именно происходит хранение информации в ДНК и её считывание, а также установить перечень ключевых факторов и процессов, оказывающих на неё влияние. Михаил Тамм, старший научный сотрудник кафедры физики полимеров и кристаллов физического факультета МГУ, отмечает: «Мы сумели оценить тепловую динамику, свойственную этому виду укладки. Проведенное нами компьютерное моделирование хорошо подтвердило теоретический результат. С точки зрения динамики нам бы хотелось разобраться с тем, какие там встроенные характерные времена, какие процессы могут происходить просто за счет теплового движения, а что неизбежно требует привлечения активных элементов, ускоряющих работу ДНК».

Highscreen Pure F – Яркий европейский дизайн в компактном корпусе

Российский бренд Highscreen объявляет о начале продаж нового бюджетного смартфона Highscreen Pure F.

Highscreen Pure F – яркий смартфон в минималистичном и функциональном дизайне. Он создан для того, чтобы дарить радость и позитив. Смартфон поставляется уже с актуальной версией операционной системы Android 5 Lollipop, попробуйте новый интерфейс Material design без лишних надстроек, только «чистый» Android – такова идеология Highscreen.

Highscreen Pure F сильно выделяется среди конкурентов в бюджетном сегменте из-за своего яркого и «свежего» дизайна. Из ключевых характеристик стоит отметить 4-ядерный процессор, MediaTek MTK6582M, 1.3 ГГц, 1 ГБ оперативной и 8 ГБ встроенной памяти расширяемой при помощи карт памяти microSD, а так же FM-радиоприемник работающий при подключенных наушниках. В смартфоне установлен 5 Мп модуль основной камеры и 0.3 Мп модуль фронтальной камеры. Из программных «фишек» стоит отметить «умный» режим энергосбережения и улучшатели звука такие как BesAudEnh и BesLoudness.

Highscreen Pure F доступен в пяти современных, модных цветах, так актуальных летом. Классический чёрный, элегантный белый, яркий оранжевый, насыщенный бирюзовый, жизнерадостный жёлтый – любое из этих исполнений будет поднимать настроение владельцу.

Смартфон уже поступил в продажу в фирменном магазине бренда Highscreen (shop.highscreen.ru), и в магазинах партнёров. Рекомендованная розничная цена смартфона 5490 руб.

Основные технические характеристики смартфона Highscreen Pure F:

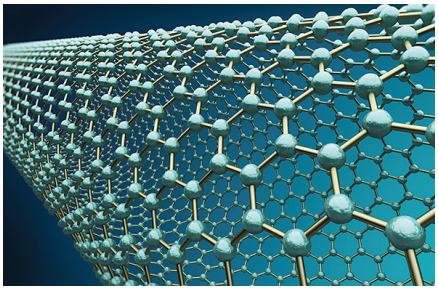
Операционная система	**Android 5**
Дисплей	4.0'', 800x480
Процессор	MediaTek MT6582M, 4 ядра, 1.3 ГГц
Видеопроцессор	Mali-400MP
Размер оперативной памяти	1 ГБ
Размер постоянной памяти	8 ГБ (расширяемая microSD, совместимо с SDHC)
Фронтальная камера	0.3 Мп
Основная камера	5 Мп
Wi-Fi®	IEEE 802.11 b/g/n
Bluetooth	4.0+EDR (A2DP/HID/AP)
Сети	GSM: 850/900/1800/1900 WCDMA: 900/2100 Поддержка двух SIM-карт (Dual SIM Dual Standby)
Датчики	G-сенсор Датчик света Датчик приближения
GPS	Встроенный
Емкость аккумулятора	1500 мАч
Габариты	123.5 x 63.9 x 9.6 мм
Вес	122 г.

Официальный сайт бренда Highscreen:
http://highscreen.ru

Директор по развитию PlanB Group
Олег Михайлов
Тел.: + 7 967 194 44 35
E-mail: planbclub@ya.ru

Маркетолог PlanB Group
Светлана Корнеева
Тел.: +7 917 514 84 00
E-mail: sveta@planb-group.ru

Метод визуализации дефектов на поверхности графена



Российские ученые из Института органической химии имени Зелинского Российской академии наук под руководством профессора Валентина Ананикова разработали эффективный метод визуализации дефектов на поверхности графена и других углеродных материалов, позволяющий за короткое время локализовать тысячи дефектов с помощью стандартной техники микроскопического исследования. Это важно для понимания физико-химических и механических свойств материалов и является одной из основных задач современных нанотехнологий.

Валентин Анаников в 1996 году окончил Донецкий государственный университет. Тогда же поступил в аспирантуру Института органической химии (ИОХ) имени Зелинского РАН. В 1999 году защитил кандидатскую диссертацию, а в 2003 году – докторскую. В 2008 году в возрасте 33 лет был избран член-корреспондентом РАН, став самым молодым членом РАН. В настоящее время руководит отделом в ИОХ РАН и лабораторией Санкт-Петербургского государственного университета, созданной на средства мегагранта.

Метод, предложенный учеными, основан на свойстве наночастиц металлов, которые избирательно адсорбируются по краям дефектов, в результате чего контуры дефектов «прочерчиваются» цепочками металлических наночастиц, и их видно в электронный микроскоп.

С помощью этого подхода химикам удалось установить, что на поверхности углеродных материалов дефекты располагаются не хаотически, а образуют упорядоченные структуры.

Работа выполнена учеными с участием международного исследовательского коллектива, а ее результаты опубликованы в журнале Chemical Science Королевского химического общества Великобритании и отмечены на его обложке.

Экспериментальные исследования свойств графена, проведенные в последнее десятилетие, спровоцировали настоящий «графеновый бум». Сегодня исследования графена и других двумерных материалов на его основе можно условно выделить в отдельную область нанотехнологий.

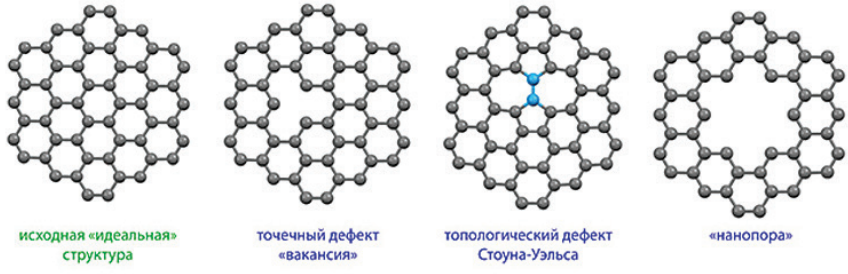
Особенность графена – высокая подвижность носителей заряда. Графен отличается высочайшей теплопроводностью, электропроводностью и способностью изменять эти свойства в зависимости от модификации своей структуры и от природы внешних воздействий. Поэтому графен и его производные часто рассматриваются как перспективные компоненты электронных устройств нового типа и химических сенсоров.

Например, присоединение к плоскости графена различных функциональных групп не только изменяет электронную проводимость этого материала, но и обеспечивает ему избирательное сродство к определенным молекулам из внешней среды, в том числе биологическим. Свойства графена можно изменить и за счет замещения части его атомов углерода на другие атомы, в частности кремний или германий.

Графен – родоначальник целого класса двумерных структур. Условно этот класс разделяют на две группы. К первой группе относятся структуры на основе самого графена, функционализированного графена (то есть модифицированного различными химическими группами), гибридных графеновых материалов (например, гибриды графена и углеродных нанотрубок). Вторая группа – это когда графен выступает в роли только структурного образца, прообраза, но непосредственного отношения к графену эти структуры не имеют. Например, силицен – структурный аналог графена, состоящий не из атомов углерода, а из атомов кремния.

Важнейший способ управления свойствами двумерных материалов и, в частности, графена – направленное введение в их двумерную сетку структурных дефектов. «Идеальный» графен состоит только из строго упорядоченных шестичленных циклов. Однако отклонения от этой идеальности дают возможность регулировать как физические, так и химические свойства графена.

Прямое наблюдение дефектов графена чрезвычайно затруднено. Более того, некоторые дефекты являются динамическими, то есть способны менять свое местоположение и «мигрировать» по поверхности углеродного материала. В результате дефекты могут самоорганизовываться – сливаться или выстраиваться вдоль определенного направления. В работе было показано, что повышенную реакционную способность графеновых дефектов можно использовать для их локализации в пространстве и сортировки по химической активности. Методика поиска графеновых дефектов проста и поэтому эффективна.



Некоторые типы дефектов в графене на примере небольшой нанопластины

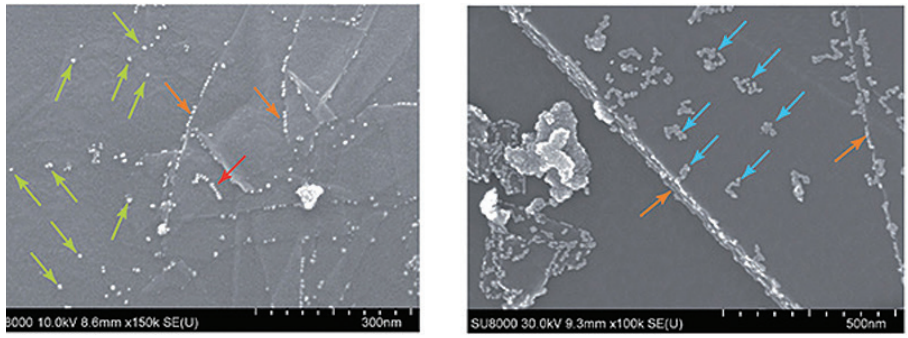
На первой стадии готовится раствор комплекса палладия в органическом растворителе. При небольшом нагревании в этом растворе образуются наночастицы палладия. Добавление углеродного материала приводит к быстрой адсорбции наночастиц палладия на его поверхности, и этот процесс легко контролируется даже визуально: темно-красный раствор превращается в бесцветный.

Затем образец углеродного материала можно исследовать под микроскопом. На микрофотографиях отчетливо видно, что наночастицы группируются на точечных дефектах или выстраиваются в линии вдоль линейных дефектов. Более активные дефекты связываются с наночастицами металла более прочно. Значит, есть возможность не только установить пространственное положение дефектов, но и оценить их химическую активность.

В результате исследований было установлено, что на одном квадратном микрометре поверхности углеродного материала может быть до двух тысяч дефектов (реакционноспособных центров). При этом в некоторых случаях дефекты располагаются по поверхности в виде упорядоченных структур.

Предложенный метод – эффективный инструмент подбора условий для получения графеновых материалов с заданным пространственным расположением дефектов определенной химической активности. А это открывает путь для создания новых типов наноструктурированных катализаторов, в которых молекулы реагентов размещаются не хаотически, а только на выделенных и упорядоченных местах, то есть подвергаются предварительной организации. Это еще один контролируемый способ получения новых графеновых продуктов с заданными свойствами.

«Исследование графеновых систем – чрезвычайно сложная задача на передовом крае современной науки. Провести работу подобного уровня нам удалось только при поддержке Российского научного фонда, обеспечившего достойное финансирование этого проекта», – подчеркнул руководитель работы профессор Анаников.



Электронные микрофотографии с локализацией различных типов дефектов графена с помощью наночастиц палладия: зеленые и синие стрелки указывают на точечные дефекты различных размеров, красные — на линейные дефекты, оранжевые — на ступенчатые переходы между различными листами графена

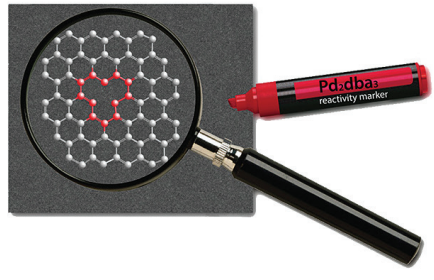
Помимо финансирования самих исследований, для графеновой гонки крайне важен доступ к новейшему оборудованию. Как правило, первыми добиваются успеха научные группы, располагающие уникальными установками. Наши ученые в своей работе использовали целый комплекс из высокопроизводительных установок – синхротрон во Франции, высокоразрешающий электронный микроскоп в Японии и мощнейший суперкомпьютер в Московском государственном университете.

Выполненное на суперкомпьютере молекулярное моделирование – принципиальный момент, поскольку теоретическое исследование представляет независимое доказательство природы наблюдаемых явлений. К счастью для российских ученых, суперкомпьютер МГУ, входящий в верхние строчки мирового рейтинга, обеспечивает такую возможность и делает российскую науку более конкурентноспособной в столь сложной и динамичной области науки.

Дефекты кристаллов – важнейший объект изучения физики и химии твердого тела. От концентрации дефектов напрямую зависят эксплуатационные характеристики изделий. Например, дефекты уменьшают механическую прочность материала, изменяют его токопроводящие свойства. В полупроводниковой промышленности стараются получить кристаллы полупроводниковых материалов с как можно меньшим количеством дефектов.

Если в области материаловедения дефекты играют, скорее, негативную роль и от них стараются по возможности избавиться, то в химии дефекты кристаллов весьма полезны. Так, в гетерогенном катализе химическая реакция происходит на твердой поверхности частицы катализатора, и именно дефекты поверхности зачастую выполняют функцию каталитических центров, то есть мест, где и происходит каталитическая реакция. Поэтому для химии и химической технологии умение контролируемо управлять дефектами поверхности – это путь к созданию катализаторов с заданной каталитической активностью и селективностью (то есть способностью ускорять именно целевую реакцию из всего множества реакций, осуществимых с данным набором реагентов).

Такие каталитические системы активно используются в настоящее время как в крупнотоннажной химической промышленности, так и в тонком органическом синтезе.



Локализация дефектов углеродных наноматериалов, значительно влияющих на их физико-химические и механические свойства – одна из важнейших задач современных нанотехнологий

Россия и 5G

Пропагандируя достижения российской науки, нельзя игнорировать того, что делается в этой сфере за рубежом. В этом отношении для нас очень поучительны регулярно издаваемые за рубежом на протяжении многих лет и бесплатно распространяемые на многих европейских языках издания Еврокомиссии.

Еврокомиссия – Информационная служба ЕС по исследованию и разработкам (CORDIS, Community Research and Development Information Service, cordis.europa.eu/research-eu). Наиболее популярными из этих изданий являются Research*eu Results Magazine и Research*eu Focus Magazine.

Первое издание на протяжении ряда лет отслеживает наиболее важные результаты сетевых исследовательских проектов, выполненных в контексте рамочных программ ЕС по исследованиям и разработкам (FP6, FP7). Эти результаты систематизированы по темам:

- Биология и медицина;
- Социология и гуманитарные науки;
- Энергетика и транспорт;
- Окружающая среда и общество;
- Информационные технологии и телекоммуникации;
- Промышленные технологии;
- Космос;
- Продовольствие и сельское хозяйство.

Концепция «citizen sciences»

Один из последних трендов, который нам удалось уловить, читая регулярно этот журнал, это концепция «Citizen Sciences».

Многие сетевые европейские исследования используют эту концепцию, вовлекая в нее множество волонтеров и любителей науки.

Наиболее мощным европейским проектом в этой области является SOCIENTIZE (Society as Infrastructure for E-science via Technology, Innovation and Creativity, socientize.eu), который выполнялся в рамках FP7-INFRASTRUCTURES-2012-1 и координировался университетом Сарагосы (Испания). Этот проект собрал тысячи волонтеров, учителей, ученых и разработчиков, объединил их навыки, время и ресурсы для цели продвижения научных исследований.

Благодаря инструментам Open source, развитых в рамках этого проекта, волонтеры помогли собрать для ученых исходные данные, которые затем анализировались профессиональными исследователями, или даже самими волонтерами (например, классификация и анализ изображений).

Спектр решаемых задач огромен – от астрономии до социальных наук. Например, эксперимент Saving Energy Home предложил людям предоставить данные о температуре в их домах и за их пределами для того, чтобы построить ясную картину температур в городах всех стран ЕС.

В тоже время испанская сеть GripeNet.es предложила людям сообщать о заболевании гриппом для того, чтобы наблюдать за вспышками заболеваний и предсказывать возможные эпидемии.

Помимо сбора данных, волонтеры помогали в их анализе. Отмечается, что даже самые продвинутые компьютеры не очень хороши для распознавания таких явлений, как солнечные пятна или клетки. Например, после короткого обучения волонтеры могут легко идентифицировать живые и мертвые клетки.

В этой связи проекты Sun4All и Cell Spotting предложили волонтерам классифицировать изображения солнечной активности и раковых клеток с помощью мобильных телефонов или компьютеров.

Проект SOCIENTIZE стоимостью 0,791 млн евро, который объединил организации Испании, Португалии, Австрии и Бразилии, был завершен в октябре 2014 г. и собрал вместе 12000 граждан в различных фазах исследований на протяжении двух лет.

Другой проект EPIWORK (Developing the Framework for an Epidemic Forecast Infrastructure, epiwork.eu) стоимостью 4,85 млн евро (2009-2013 гг.), выполненный в рамках FP7-ICT-2007-3 и объединивший в себе 12 исследовательских команд из 8 стран, разработал систему мониторинга за активностью гриппоподобных болезней, которая получила название Influenzanet. В настоящее время она объединяет 20000 волонтеров из местных сообществ 10 стран ЕС.

Взаимодействие в Influenzanet между исследовательскими командами, национальными институтами здравоохранения и другими партнерами проекта осуществляется через сайт и приложение для мобильных устройств.

5G–беспроводные сети пятого поколения

Второе издание имеет тематический характер и посвящено актуальным темам. Недавно вышел в свет №15 этого издания за 2015 год, с броским названием «Why the EU is betting big on 5G» («Почему ЕС делает большую ставку на 5G»).

Свое обращение к читателям этого выпуска журнала, Günther Oettinger, Commissioner Digital Economy & Society (комиссар Еврокомиссии по делам цифровой экономики и общества) начинает словами: «Следующее, пятое поколение беспроводных сетей (5G) изменит способ, которым мы общаемся, то как мы делаем бизнес, как мы делаем все!». Далее, он отмечает, что влияние 5G будет распространяться далеко за пределы телекоммуникаций. Оно будет стимулировать сдвиги парадигм в ряде существующих отраслей и вызовет появление новых отраслей промышленности и экосистем.

Коммуникационные сети в эпоху 5G также будут играть более важную социальную роль, чем сегодня: объединяя людей, машины и предметы в глобальном масштабе, они будут способствовать предоставлению персонализированных медицинских услуг и поддерживать стареющее общество, помогут оптимизировать транспорт и логистику, улучшат доступ к культуре и образованию для всех, и это может

фактически произвести виртуальную революцию общественных услуг, заключает еврокомиссар.

Предполагается в сотрудничестве с промышленностью запустить 5G Public-Private Partnership (5G PPP). Еврокомиссия выделит 700 млн евро для финансирования в рамках исследовательской и инновационной программы EC Horizon 2020, чтобы ускорить развитие 5G. Также идет работа над созданием соглашений о стратегическом сотрудничестве с ключевыми партнерами по всему миру для достижения общего видения развития мобильных сетей к концу 2015 года. Согласно плану Президента ЕС Juncker, чтобы достичь этого: ЕС должен произвести стратегические инвестиции в инфраструктуру и развитие инновационных услуг. А это возможно, если поддержка со стороны ЕС исследователям будет дополнена поддержкой частных инвестиций в размере 315 млрд евро.

Все вышесказанное позволит обеспечить лидерство ЕС в телекоммуникационных технологиях и стать крупным игроком в эпоху 5G. Это важно, потому что коммуникационная инфраструктура, по мнению европейских экспертов, должна стать самой важной из всех инфраструктур в течение следующего десятилетия, не только для экономики, но и для общества в целом.

Согласно последнему Ericsson's Mobility Report, мобильный трафик возрастет в 1000 раз в течение следующего десятилетия, что окажет огромное воздействие на лежащую в его основе сетевую инфраструктуру. К 2020 г. ожидается свыше 6 млрд владельцев смартфонов и свыше 90% населения старше 6 лет будут иметь мобильные телефоны.

Предполагается, что эра 5G обеспечит повсеместное сетевое подключение (ubiquitous connectivity), что будет выражаться в тысячекратном росте беспроводной мощности, а также организацией мобильной связи для более чем 7 миллиардов человек и 7 триллионов устройств, что в 140 раз больше, чем количество подключенных к Интернету устройств, ожидаемых к 2020 году.

Стратегическое партнерство в развитии 5G-сетей

В качестве стратегических партнеров в развитии пятого поколения беспроводной связи ЕС видит Китай, Японию, Корею и США, которые также признали стратегический характер этой области и инициировали значительные объемы научно-исследовательской деятельности. Правительство Южной Кореи подписало соглашение о сотрудничестве по исследованиям и стандартизации 5G с ЕС в июне 2014 года и планирует инвестировать более 1 млрд евро в исследования, чтобы запустить 5G для населения на зимних Олимпийских играх в Пхенчхане в 2018 году (Winter Olympics in Pyeongchang). Япония, тем временем, в рамках аналогичного партнерства с ЕС, планирует испытать первую массовую сеть 5G на Олимпиаде в Токио в 2020 году (Tokyo Olympics).

Естественно, что в условиях международных санкций ЕС не рассматривает Россию в качестве стратегического партнера в развитии 5G-сетей. В этой связи России следует организовать стратегическое партнерство в развитии таких сетей в рамках БРИКС.

В этой связи следует отметить, что китайская организация The International Mobile Telecommunications 2020 (IMT-2020) Promotion Group, созданная Министерством науки и технологий (MoST) и Национальной комиссией по развитию и реформам (NDRC) для поддержки 5G R&D, работает в рамках программы 863 ЕС.

Население стран БРИКС составляет 40% мирового, а следовательно, эти страны имеют огромный рынок для устройств мобильной связи, кроме того, эти страны имеют хорошие компетенции в области информационно-коммуникационных технологий и программирования.

В рамках такого партнерства Россия могла бы запустить 5G-сеть во время проведения футбольного чемпионата мира в 2018 году. Структуры стран БРИКС, ответственные за научную кооперацию, могли бы задуматься над этими вопросами.

К сожалению, следует отметить, что Россия не была среди лидеров в

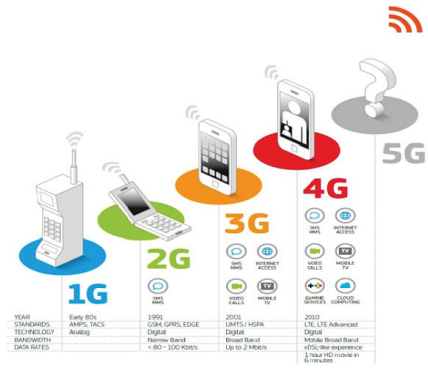


Рис.1. Эволюция сетей мобильной связи

развитии предыдущих поколений беспроводных сетей, эволюция которых показана на рисунке 1, заимствованном нами из рассматриваемого тематического выпуска Research*eu Focus Magazine.

Смотря на этот рисунок, естественно предположить, что в пятом поколении таких сетей, наряду с cloud computing, впервые появится технология ubiquitous computing, будут разработаны и реализованы более совершенные процессоры по распознаванию и оцифровке речевых сигналов, а также изображений.

Например, вы слушаете доклад на конференции – и на вашем смартфоне эта речьпреобразуется в word-документ, вы фотографируете какой-либо документ – и его изображение преобразуется в один из редактируемых форматов на базе, например, программного обеспечения по оптическому распознаванию символов (optical character recognition).

Что из себя в содержательном плане представляют концепция 5G PPP показано на рисунке 2, заимствованного из того же издания.

Рис.2. Иллюстрация к концепции 5G PPP

КОМПЕНСАЦИЯ ИСКАЖЕНИЙ ФАЗОМАНИПУЛИРОВАННОГО СИГНАЛА С ЦЕЛЬЮ УЛУЧШЕНИЯ ХАРАКТЕРИСТИК ЕГО СЖАТИЯ

Ершов
Герман Анатольевич,
к.т.н., начальник научно-технического центра АО «Всероссийский научно-исследовательский институт радиоаппаратуры», г. Санкт-Петербург, Россия, vniira@sp.ru

Синицын
Евгений Александрович,
д.т.н., профессор, начальник научно-исследовательского отдела АО «Всероссийский научно-исследовательский институт радиоаппаратуры», г. Санкт-Петербург, Россия, vniira@sp.ru

Фридман
Леонид Борисович,
к.т.н.,старший научный сотрудник АО «Всероссийский научно-исследовательский институт радиоаппаратуры», г. Санкт-Петербург, Россия, lenya2002@bk.ru

Ключевые слова:
подоптимальный фильтр, доплеровский сдвиг частоты, код Баркера, сжатие фазоманипулированного сигнала, компенсация искажений.

АННОТАЦИЯ

Проведен анализ влияния искажений сигнала с фазовой манипуляцией, выполненной в соответствии с кодом Баркера, на характеристики эффективности его сжатия. При этом рассматривались искажения, вызванные: доплеровским сдвигом частоты сигнала, отражённого от движущегося летательного аппарата; свойствами приемо-передающего тракта радиолокатора.

Предложен фильтр сжатия фазоманипулированного сигнала, обеспечивающий при наличии доплеровского сдвига частоты характеристики эффективности согласованного фильтра сжатия. Предложен подоптимальный фильтр, обеспечивающий при наличии доплеровского сдвига частоты сжатие фазоманипулированного сигнала теоретически с нулевым уровнем боковых лепестков (обусловленным лишь вычислительной погрешностью). С помощью математического моделирования в программной среде «Matlab» проведён анализ характеристик эффективности предложенных фильтров сжатия при различных величинах доплеровского сдвига частоты. Было показано, что использование предложенных фильтров обеспечивает сохранение характеристик эффективности сжатия фазоманипулированного сигнала при наличии доплеровского сдвига частоты.

Выполнен анализ характеристик эффективности сжатия фазоманипулированного сигнала в зависимости от доплеровского сдвига частоты (при заранее неизвестной величине доплеровского сдвига). При этом в качестве характеристик эффективности рассматривались: снижение отношения сигнал-шум из-за наличия доплеровского сдвига; уровень боковых лепестков на выходе фильтра сжатия; расширение основного пика на выходе фильтра сжатия. Даны рекомендации по выбору количества доплеровских каналов (при многоканальной доплеровской обработке) в зависимости от допустимых величин уровня боковых лепестков и снижения отношения сигнал-шум на выходе фильтров сжатия.

Проведён анализ влияния искажений фазоманипулированного сигнала в приемо-передающем тракте радиолокатора с использованием радиолокационных данных, записанных при работе радиолокатора в условиях его штатного функционирования. При этом подоптимальное сжатие радиолокационных данных выполнялось при помощи математического моделирования в программной среде «Matlab». Результаты моделирования показали, что искажения фазоманипулированного сигнала в приемо-передающем тракте радиолокатора привели к образованию боковых лепестков на выходе подоптимального фильтра сжатия на уровне порядка минус 20–27 дБ.

Предложена схема компенсации искажений фазоманипулированного сигнала. Компенсация искажений сигнала позволила снизить пиковый уровень боковых лепестков до уровня минус 45–50 дБ. При этом отношение сигнал/шум не ухудшилось по сравнению с отношением сигнал/шум при отсутствии искажений.

Введение

В радиолокационных станциях, работающих в импульсном режиме, повышение разрешающей способности по дальности (при сохранении энергии сигнала) может быть достигнуто благодаря использованию внутриимпульсной модуляции, в частности, фазовой манипуляции. В настоящее время широкое распространение получили сигналы с фазовой манипуляцией 0-π, выполненной в соответствии с кодами Баркера [1]. Сжатие таких сигналов обычно осуществляется при помощи согласованного (оптимального) фильтра [2]. Уровень боковых лепестков (УБЛ), возникающих на выходе согласованного фильтра, в некоторых случаях оказывается недопустимо высоким. В [3] был предложен подоптимальный фильтр, обеспечивающий сжатие теоретически с нулевым уровнем боковых лепестков (обусловленным лишь вычислительной погрешностью) при незначительной потери мощности для ряда фазоманипулированных (ФМ) сигналов. В частности, для сигнала с фазовой манипуляцией, выполненной в соответствии с тринадцатиэлементным кодом Баркера, уменьшение отношения сигнал-шум (ОСШ) при использовании такого фильтра составляет не более 5 % [3].

Для нахождения подоптимального фильтра в [3] был рассмотрен код фазовой манипуляции, состоящий из n_B элементов (n_B - битный код) длительностью $T_p = n_s T$, где T – период дискретизации сигнала; n_s – количество дискрет в одном элементе кода (бите).

Код Баркера в [3] был представлен как

$$\kappa(n) = h_C(n) * p(n) = \sum_{j=-\infty}^{\infty} p(j)\, h_C(n-j) \qquad (1)$$

где $*$ обозначает свёртку; $n = -\infty, \ldots, \infty$;

$h_C(n) = \sum_{i=0}^{n_B-1} a_i \delta(n - i n_S)$ – импульсная характеристика (ИХ) кодирующего фильтра; $a_i = \pm 1$; $\delta(n)$ – дельта-функция;

$p(n) = \sum_{i=0}^{n_s-1} \delta(i-n)$ – элементарный импульс.

$\kappa(n)$ принимает нулевые значения при $n<0$ и при $n>n_S(n_B-1)$.

ИХ подоптимального фильтра, обеспечивающего сжатие ФМ сигнала теоретически с нулевым уровнем боковых лепестков [3]

$$\lambda(n) = h_{dec}(n) * p(-n) = \sum_{j=-\infty}^{\infty} p(-j)\, h_{dec}(n-j) \qquad (2)$$

где $n = -\infty, \ldots, \infty$, $h_{dec}(n) = F^{-1}\left\{\frac{1}{F\{h_C(n)\}}\right\}$;

F и F^{-1} – операторы соответственно прямого и обратного дискретных преобразований Фурье (ДПФ).

Сигнал на выходе подоптимального фильтра сжатия

$$w(n) = \lambda(n) * \kappa(n) \qquad (3)$$

ИХ стандартного согласованного фильтра является зеркальным отражением ФМ сигнала, т.е.

$$\mu(n) = \kappa(-n) = h_C(-n) * p(-n), \quad n = -\infty, \ldots, \infty. \qquad (4)$$

Сигнал на выходе согласованного фильтра:

$$w_m(n) = \mu(n) * \kappa(n) = h_C(-n) * p(-n) * h_C(n) * p(n).$$

I. Фильтры сжатия фазоманипулированного сигнала

Доплеровский набег фазы принятого сигнала за время T_p определяется выражением $\Delta\varphi_D = f_D T_p = 2v_R T_p/\lambda_C$, где f_D – доплеровский сдвиг частоты; λ_C – длина волны излучаемого сигнала; v_R – радиальная скорость движения ЛА. Код Баркера с учётом доплеровского сдвига имеет вид

$$\kappa^D(n) = \kappa(n)\exp(jf_D nT). \qquad (5)$$

Найдём ИХ подоптимального фильтра сжатия при наличии доплеровского сдвига частоты. Подставив (5) в (3), получим отклик подоптимального фильтра при наличии доплеровского сдвига частоты

$$w^D(n) = \lambda(n) * \{\kappa(n)\exp(jf_D nT)\}. \qquad (6)$$

Подставив (1), (2) в (6), получим ДПФ сигнала $w^D(n)$:

$$F\{w^D(n)\} = F\{h_{dec}(n)\}\, F\{h_c(n)\exp(jf_D nT)\} \times \times F\{p(n)\}F\{p(-n)\}$$

Выбирая $h_{dec}(n)$ таким образом, чтобы

$$F\{h_{dec}(n)\}\, F\{h_C(n)\exp(jf_D nT)\} = 1,$$

т.е. $$h_{dec}(n) = F^{-1}\left\{\frac{1}{F\{h_C(n)\exp(jf_D nT)\}}\right\} \qquad (7)$$

получим $w^D(n) = p(n) * p(-n)$. (8)

Из (8) следует, что сжатый сигнал $w^D(n)$ соответствует отклику согласованного фильтра на элементарный импульс и не имеет боковых лепестков [3]. Подставив (7) в (2), получим ИХ подоптимального фильтра сжатия при наличии доплеровского сдвига частоты:

$$\lambda(n) = F^{-1}\left\{\frac{1}{F\{h_C(n)\exp(jf_D nT)\}}\right\} * p(-n) \qquad (9)$$

ИХ согласованного фильтра сжатия при наличии доплеровского сдвига частоты найдем, подставив (5) в (4):

$$\mu^D(n) = \kappa^D(-n) = \kappa(-n)\exp(-jf_D nT) = \{h_C(-n) * * p(-n)\}\exp(-jf_D nT)\}. \qquad (10)$$

II. Характеристики эффективности предложенных фильтров сжатия

Анализ характеристик эффективности выполнен с помощью математического моделирования в программной среде «Matlab». При этом рассматривались

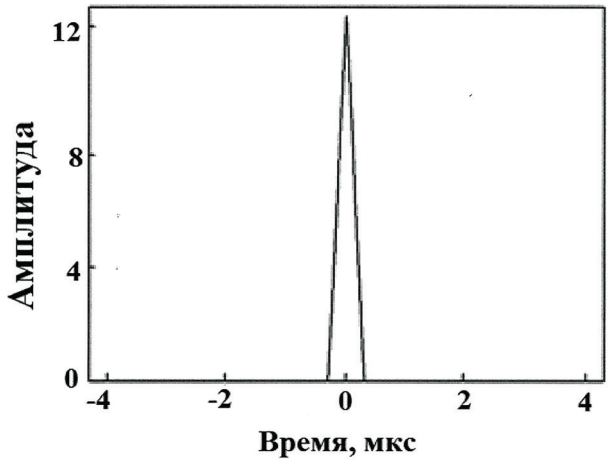


Рис. 1. Результат сжатия фазоманипулированного сигнала предложенным фильтром с импульсной характеристикой (9), при $\Delta\varphi_D = 14{,}4^0$

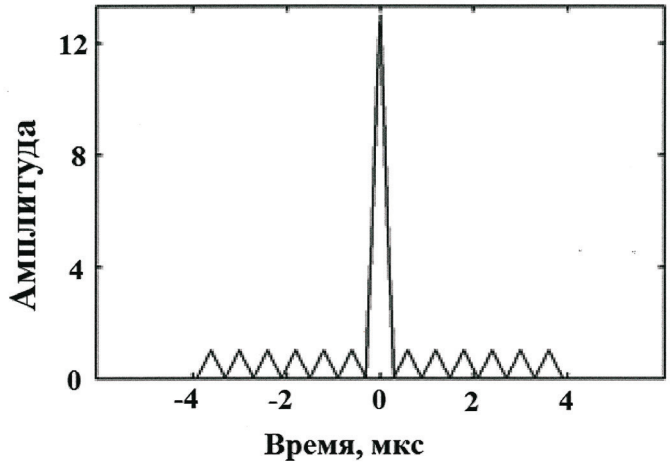


Рис. 2. Результат сжатия фазоманипулированного сигнала предложенным фильтром с импульсной характеристикой (10), при $\Delta\varphi_D = 14{,}4^0$

цифровые сигналы с частотой дискретизации 100 нс, количеством разрядов 32. В качестве излучаемого сигнала рассматривался сигнал с фазовой модуляцией, выполненной в соответствии с тринадцатиэлементным кодом Баркера. Длительность каждого элемента кода T_P =300 нс.

Результаты математического моделирования при различных величинах $\Delta\varphi_D$ показали:

– боковые лепестки на выходе предложенного фильтра сжатия с ИХ (9) отсутствуют (рис. 1);

– ОСШ на выходе предложенного фильтра сжатия с ИХ (9) не снизилось по сравнению с ОСШ на выходе фильтра с ИХ (2) при отсутствии доплеровского сдвига;

– уровень боковых лепестков на выходе предложенного фильтра сжатия с ИХ (10) остается практически тем же, что и при согласованном сжатии кода Баркера без доплеровского сдвига и составляет порядка – 22 дБ (рис. 2);

– ОСШ на выходе фильтра с ИХ (10) не снизилось по сравнению с ОСШ при согласованном сжатии кода Баркера без доплеровского сдвига.

Следовательно, использование фильтров с ИХ (9) и (10) обеспечивает сохранение характеристик эффективности сжатия ФМ сигнала при наличии доплеровского сдвига частоты.

ИХ (9) и (10) рассчитаны на сжатие ФМ сигнала с заранее известной величиной f_D. Однако, радиальная скорость ЛА, а следовательно и величина f_D, как правило, заранее не известны. Более того, одновременно в зону действия радиолокатора могут попадать несколько ЛА, движущихся с разными радиальными скоростями. Для сжатия ФМ сигналов, отражённых от движущихся с произвольными радиальными скоростями летательных аппаратов, требуется использовать несколько доплеровских каналов. Каждый из таких каналов должен быть рассчитан на определённый диапазон радиальных скоростей движения ЛА. Ширину доплеровских каналов следует выбирать, исходя из допустимых величин УБЛ и снижения ОСШ [4], пользуясь таблицей 1. Задавшись допустимыми уровнем боковых лепестков и снижением ОСШ, из таблицы 1 можно получить $\Delta\varphi_D$. Тогда ширина каждого доплеровского канала $\Delta f_D = \dfrac{\Delta\varphi_D}{T_P}$.

Таблица 1

Параметры эффективности сжатия ФМ сигнала в зависимости от доплеровского набега фазы

$\Delta\varphi_D$	Согласованный фильтр			Подоптимальный фильтр		
	Уменьшение ОСШ, дБ	УБЛ, дБ	Расширение основного пика	Уменьшение ОСШ, дБ	УБЛ, дБ	Расширение основного пика (по уровню 3 дБ),%
$0{,}14^0$	0	-22,3	-	0	-52,5	0
$0{,}36^0$	0	-22,3	-	0	-44,3	0
$0{,}72^0$	0	-22,3	-	0	-38,3	0
$1{,}44^0$	0	-22,2	-	0	-32,3	0
$2{,}88^0$	0,16	-22,0	+	0,15	-26,3	0
$4{,}32^0$	0,35	-21,9	+	0,33	-22,7	0
$7{,}20^0$	0,93	-20,8	+	0,99	-18,0	13
$14{,}40^0$	4,3	-2,5	+	4,0	-2,8	35

lII. Компенсация искажений фазоманипулированного сигнала в приемо-передающем тракте радиолокатора

Анализ влияния искажений ФМ сигнала выполнен с использованием радиолокационных данных, записанных при работе радиолокатора в условиях его штатного функционирования. При этом частота дискретизации сигналов составляла 100 нс, количество разрядов – 16. Зондирующим сигналом являлся сигнал с фазовой манипуляцией, выполненной в соответствии с тринадцатиэлементным кодом Баркера, длительность каждого элемента кода нс. Подоптимальное сжатие ФМ сигнала выполнялось в программной среде «Matlab».

Как видно из рисунка 3, наличие искажений ФМ сигнала в приемо-передающем тракте радиолокатора привело к образованию боковых лепестков на выходе подоптимального фильтра сжатия. При этом пиковый УБЛ составил порядка минус 20–27 дБ, что практически соответствует УБЛ при согласованном сжатии данного сигнала. Следовательно, для улучшения характеристик подоптимального сжатия требуется выполнять компенсацию искажений ФМ сигнала.

Коэффициент передачи приемо-передающего тракта радиолокатора (рис. 4) в спектральной области определяется выражением:

$$\dot{H}_{Тр}(\omega) = \dot{H}_{Прч\_1}(\omega)\dot{H}_{УМ}(\omega)\dot{H}_{Прч\_2}(\omega)\dot{H}_{ЦФД}(\omega),$$

где $\dot{H}_{Прч\_1}(\omega)$, $\dot{H}_{Прч\_2}(\omega)$, $\dot{H}_{УМ}(\omega)$, $\dot{H}_{ЦФД}(\omega)$ – соответственно коэффициенты передачи первого и второго преобразователей частоты, усилителя мощности и цифрового фазового детектора; ω - круговая частота.

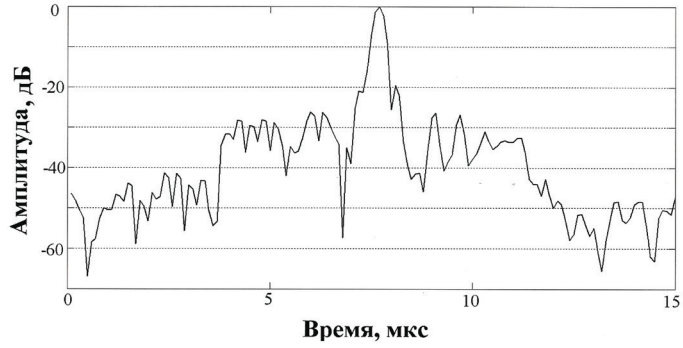


Рис. 3. Отклик подоптимального фильтра сжатия

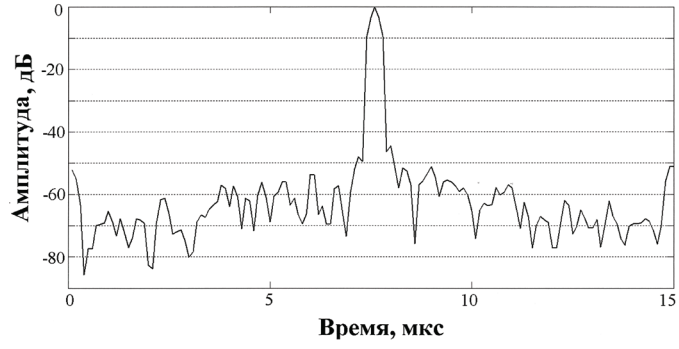


Рис. 5. Отклик подоптимального фильтра сжатия при выполнении компенсации искажений сигнала

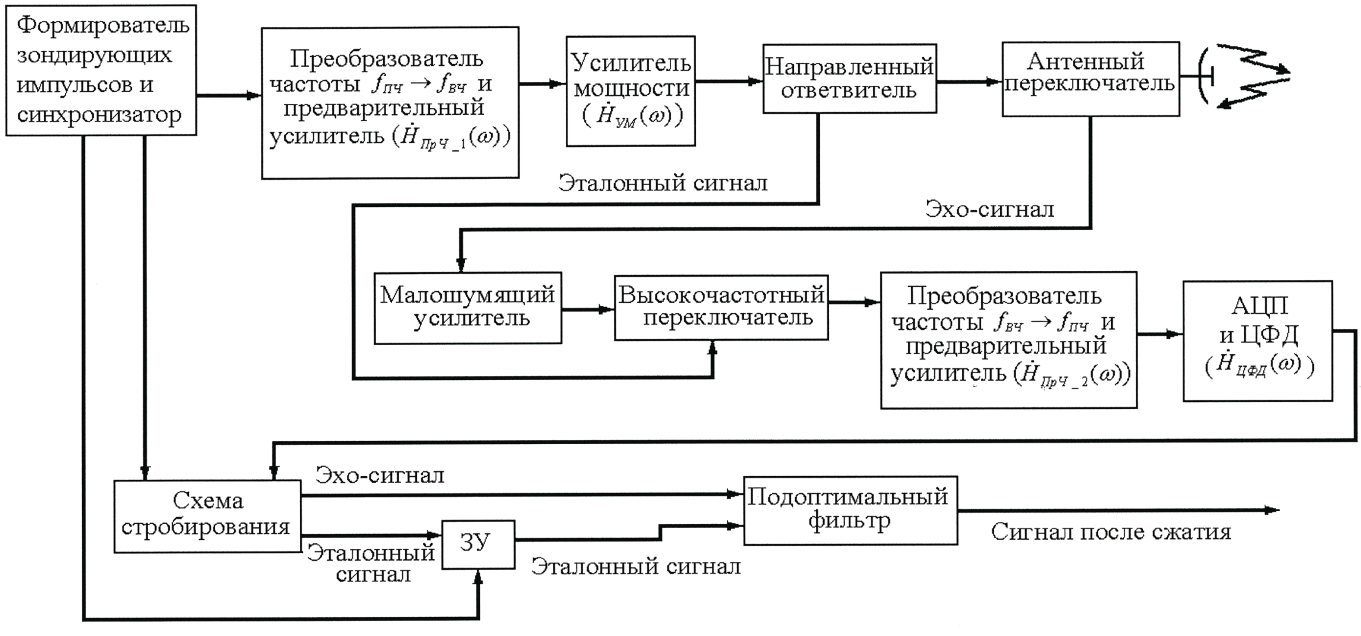


Рис. 4. Структурная схема приемо-передающего тракта радиолокатора при компенсации искажений ФМ сигнала.
АЦП – аналогово-цифровой преобразователь; ЦФД – цифровой фазовый детектор;
ЗУ – запоминающее устройство; $f_{ПЧ}$, $f_{ВЧ}$ – соответственно промежуточная и высокая частоты.

С целью компенсации искажений ФМ сигнала ИХ подоптимального фильтра формируется с использованием зондирующего сигнала, прошедшего через приемо-передающий тракт радиолокатора (рис. 4), что позволяет автоматически подстраивать фильтр сжатия под искажения эхо-сигнала. При этом коэффициент передачи подоптимального фильтра сжатия в спектральной области будет соответствовать спектру эхо-сигнала, т.к. зондирующий и эхо-сигналы проходят через один и тот же приемо-передающий тракт.

Как следует из сравнения рисунков 3 и 5, компенсация искажений ФМ сигнала позволила снизить УБЛ на 23–25 дБ, при этом пиковый УБЛ составил порядка минус 45–50 дБ. Кроме того, результаты моделирования показали, что ОСШ на выходе подоптимального фильтра сжатия при наличии искажений ФМ сигнала не снизилось по сравнению с ОСШ при отсутствии искажений.

IV. Выводы

Предложен фильтр сжатия фазоманипулированного сигнала при наличии доплеровского сдвига частоты. Уровень боковых лепестков и отношение сигнал шум на выходе такого фильтра остаются практически теми же, что и при согласованном сжатии сигнала без доплеровского сдвига.

Предложен фильтр, обеспечивающий сжатие фазоманипулированного сигнала теоретически с нулевым уровнем боковых лепестков (обусловленным лишь вычислительной погрешностью) при наличии доплеровского сдвига частоты. При этом отношение сигнал шум на выходе предложенного фильтра остаётся практически тем же, что и при подоптимальном сжатии сигнала при отсутствии доплеровского сдвига частоты.

Проведено исследование характеристик эффективности сжатия фазоманипулированного сигнала подоптимальным фильтром при компенсации искажений сигнала. Искажения фазоманипулированного сигнала в приемо-передающем тракте радиолокатора привели к образованию боковых лепестков на выходе подоптимального фильтра сжатия на уровне порядка минус 20–27 дБ. Компенсация искажений сигнала позволила снизить пиковый уровень боковых лепестков до уровня минус 45–50 дБ. При этом отношение сигнал/шум не ухудшилось по сравнению с отношением сигнал/шум при отсутствии искажений.

Литература

1. *Barker R.* Group synchronizing of binary digital systems in communications theory. New York, Academic Press. 1953. Pp. 273–287.

2. Теоретические основы радиолокации / Под ред. Я.Д. Ширмана. М.: Советское радио. 1970. 560 с.

3. *Lehtinen M., Damtie B. & Nygren T.* Optimal binary phase codes and sidelobe-free decoding filters with application to incoherent scatter radar. Annales Geophysicae. 2004. Vol. 22. Pp. 1623–1632.

4. *Korshunov A.Y., Sinitsin E.A. & Fridman L.B.* Analysis of influence of Doppler frequency shift on effectiveness of phase-shift keyed signal compression. in proc. 36th International conf. on telecommunications and signal processing (TSP-2013). Rome, Italy. 2013. Pp. 667–671.

5.*Фридман Л.Б., Мазаян Н.Р., Николаев С.Ф., Шильдкрет А.Б.* Сжатие фазоманипулированного сигнала при наличии доплеровского сдвига частоты. Сборник докладов X международной научно-технической конференции «Кибернетика и высокие технологии XXI века». Воронеж. 2009. Т. 2. С. 645–657.

Для цитирования:

Ершов Г.А., Синицын Е.А., Фридман Л.Б. Компенсация искажений фазоманипулированного сигнала с целью улучшения характеристик его сжатия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 16–21.

DISTORTION COMPENSATION OF PHASE-MANIPULATED SIGNAL TO IMPROVE THE CHARACTERISTICS OF ITS COMPRESSION

Ershov German Anatolyevich,
St. Petersburg, Russian, vniira@sp.ru

Sinitsin Evgeniy Aleksandrovich,
St. Petersburg, Russian, vniira@sp.ru

Fridman Leonid Borisovich,
St. Petersburg, Russian, lenya2002@bk.ru

Abstract
Analyzed the influence of phase-shift keyed signal distortion on the effectiveness of signal compression is carried out. The Barker-coded signal is considered as phase-shift keyed signal. The distortions, caused by Doppler frequency shift of signal, reflected from the moving aircraft and by properties of receiving and transmitting path of radar are considered.
The filter for compression of Barker-coded signal is proposed, providing, in the presence of Doppler frequency shift, effectiveness of the matched filter. The mismatched filter is proposed, providing theoretically sidelobe-free compression of Barker-coded signal in the presence of Doppler frequency shift (with sidelobe level, caused only by calculating inaccuracy).
Analysis of effectiveness of Barker-coded signal compression using the proposed filters is carried out for different values of Doppler frequency (by means of mathematical simulation in software environment «MATLAB»). It was shown that usage of the proposed filters provides preserving of effectiveness of phase-shift keyed signal compression in the presence of Doppler frequency shift.
Analysis of effectiveness of phase-shift keyed signal compression with respect to Doppler frequency shift is performed (with a priori unknown values of Doppler shift). Signal-to-noise ratio decrease (caused by Doppler shift), sidelobe level and mainlobe stretching at the compression filter output are considered as effectiveness characteristics. Recommendations are given for choosing of number of Doppler channels (at multi-channel Doppler processing) with respect to allowable values of sidelobe level and signal-to-noise ratio decrease at the compression filters output.
Evaluation of influence of distortions in receiving and transmitting path of radar on the effectiveness of phase-shift keyed signal compression is performed (with usage of radar data, recorded in terms of full-time operation of radar). In this case optimal compression of the radar data was performed by means of mathematical simulation in software environment «MATLAB». Results of mathematical simulation showed that phase-shift keyed signal distortions in receiving and transmitting path of radar caused sidelobes formation on the mismatched filter output at the level of minus 20÷27 dB.
The scheme is proposed for compensation of phase-shift keyed signal distortions. Compensation of signal distortions allowed to reduce sidelobes to the peak level of minus 45÷50 dB. At that, signal-to-noise ratio didn't decrease in comparison with signal-to-noise ratio at the absence of distortions.

Keywords: mismatched filter, Doppler frequency shift, Barker code, compression of Barker-coded signal, distortion compensation.

References
1. *Barker R.* Group synchronizing of binary digital systems in communications theory. New York, Academic Press. 1953. Pp. 273–287.
2. *Shirman Ya.D.* ed. Teoreticheskie osnovy radiolokatsii [Theoretical fundamentals of radiolocation]. Moscow, Sovetskoe radio. 1970. 560 p. (in Russian).
3. *Lehtinen M., Damtie B. & Nygren T.* Optimal binary phase codes and sidelobe-free decoding filters with application to incoherent scatter radar. Annales Geophysicae. 2004. Vol. 22. Pp. 1623–1632.
4. *Korshunov A.Y., Sinitsin E.A. & Fridman L.B.* Analysis of influence of Doppler frequency shift on effectiveness of phase-shift keyed signal compression. in proc. 36th International conf. on telecommunications and signal processing (TSP-2013). Rome, Italy. 2013. Pp. 667–671.
5.Fridman L.B., Mazayan N.P., Nikolaev S.F. & Shildkret A.B. Phase-shift keyed signal compression in the presence of Doppler frequency shift. X mezhdunarodnaja nauchno-tehnicheskaja konferencija «Kibernetika i vysokie tehnologii XXI veka». Voronezh. 2009. Vol. 2. Pp. 645–657. (in Russian).

Information about authors:
Ershov G.A., Ph.D., head of scientific and technical centre, Joint-stock company «All-Russian Research Institute of Radio»;
Sinitsin E.A., Ph.D, professor, head of research department, Joint-stock company «All-Russian Research Institute of Radio»;
Fridman L.B., Ph.D., senior researcher, Joint-stock company «All-Russian Research Institute of Radio».

For citation:
Ershov G.A., Sinitsin E.A., Fridman L.B. Distortion compensation of phase-manipulated signal to improve the characteristics of its compression. H&ES Research. 2015. Vol. 7. No.3. Pp. 16–21. (in Russian).

ЧАСТНАЯ АВИАЦИЯ – НОВАЯ УГРОЗА БЕЗОПАСНОСТИ ВОЗДУШНОГО ДВИЖЕНИЯ В РОССИИ

Хашагульгов
Руслан Абдул-Мажитович,
к.т.н., докторант Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, x.p.a-m@mail.ru,

Ходор
Михаил Александрович,
преподаватель кафедры автоматизированных систем управления противоракетной обороны Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, khodorvvv@mail.ru.

Ключевые слова:
сверхлегкие летательные аппараты, безопасность полетов, летающий автомобиль, маловысотное радиолокационное поле, оптико-электронная система.

АННОТАЦИЯ

Контроль порядка использования летательными аппаратами воздушного пространства одна из важнейших задач решаемых любым суверенным государством. Добычей информации о текущих координатах, параметров движения, государственной принадлежности воздушных объектов возлагается на части и подразделения видов и родов Вооруженных Сил, а также специальные службы гражданской авиации. Концентрация усилий различных ведомств по организации комплексного использования сил и средств, ведения воздушной разведки в районах совместного базирования, представляет собой систему разведки и контроля воздушного пространства государства. В идеальном случае система контроля должна фиксировать, определять параметры всех воздушных объектов во всем диапазоне высот их применения и с любой отражающей поверхностью. В реальности приходится идти на компромисс, обусловленный высокой стоимостью, ограниченными техническими характеристиками радиолокационных средств, требованиями экологической безопасности по их размещению, формируя более качественное радиолокационное поле с важных направлений и менее качественное в глубине страны. Однако стремительное развитие легкомоторной авиации находящейся, в том числе в частном пользовании, ставит перед системой разведки и контроля воздушного пространства задачу по устранению новой угрозы – безопасности воздушного движения над административно-политическими центрами и объектами техногенных катастроф. Ведение разведки на малых и предельно малых высотах не обеспечиваемое традиционными радиолокационными средствами предложено выполнять путем создания подсистемы контроля воздушного пространства важных административно-политических центров и объектов техногенных катастроф на базе оптико-электронных систем обнаружения и выдачи информации, как дополнение к существующей системе контроля. Проанализированы некоторые пути ее построения и технической реализации. Показано, что оптико-электронные системы на современном этапе развития позволяют успешно решать задачи контроля использования воздушного пространства легкомоторной авиацией на малых и предельно малых высотах.

На взгляд рядового российского гражданина, кажется, что самостоятельный воздушный полет – это нечто сложное и недоступное для него. На самом же деле стать пилотом и летать на самолете или вертолете, даже своем собственном, не такая уж и невыполнимая задача. Речь, конечно, идет о малой или сверхлегкой авиации. К огромной радости российских любителей авиации, законодательство нашей страны вполне толерантно регламентирует деятельность малой авиации. Хотя специалисты и говорят, что летные нормы и правила в России имеют завышенные требования, но все должно познаваться в сравнении. Да, в Новой Зеландии, на сверхлегких летательных аппаратах (СЛА) летают все возрастные группы населения с частотой использования россиянами личных автомобилей. Но хорошо уже то, что в России, в принципе, разрешены частные воздушные полеты. Соседи из Украины ждали такого права намного дольше.

Наше законодательство разрешает выполнять частные воздушные полеты почти над всей территорией России. Исключение составляют Москва и ряд правительственных объектов. Для выполнения рейса необходимо только подать заявку уведомительного (даже не разрешительного) характера [1], содержащую информацию о месте взлета и посадки, и все, можно лететь. Запретить полет никто не имеет права.

До 2010 года все полеты осуществлялись в разрешительном порядке под контролем войск ПВО. Разумеется, у гражданских властей нет необходимых специализированных сил и средств контроля. По сути, маршрут полета согласовывается на честном слове, а бесконтрольность, как известно, порождает нарушения.

Глава Московской межрегиональной транспортной прокуратуры Владимир Тюльков заявил журналистам: «Несмотря на принимаемые прокуратурой меры, эксплуатация частной малой авиации часто угрожает безопасности полетов воздушных судов, объектам и людям на земле» [2].

По его словам, на сегодняшний день у правоохранительных органов «нет точных данных по ЦФО о количестве воздушных судов малой авиации, об их размещении, техническом состоянии, возможном использовании, то есть налицо отсутствие контроля над их учетом и полетами».

По словам начальника Северо-Западного межрегионального территориального управления воздушного транспорта Федерального агентства воздушного транспорта (Росавиация) Олега Гринченко «количество воздушных судов возросло в 2,5 раза за последние 3 года. Сейчас у нас в регионе насчитывается около 95 самолетов и 116 вертолетов, а всего – около 300 воздушных судов. Но на фоне роста количества судов и полетов ситуация с безопасностью полетов остается непростой и нельзя сказать, что есть качественное улучшение» [3].

Немало нарушений и на территории двух регионов – Санкт-Петербурга и Ленинградской области. По словам экспертов, это выполнение полетов на незарегистрированных воздушных судах, управление пилотами без допусков, полеты на неисправном судне, полеты без уведомления там, где это необходимо, а также полеты на слишком низких высотах.

По данным МЧС, фиксируется неуклонный рост авиационных происшествий с малыми воздушными судами. В отраслевом же объединении малых авиаторов напоминают о том, что имеет место быть и увеличение числа воздушных судов и пилотов малой авиации, что отражается на статистике происшествий.

Воздушное судно – далеко не автомобиль, его невозможно остановить во время полета и проверить наличие удостоверения у пилота и категорию рейса. К сожалению, встречаются случаи, когда за штурвал СЛА садятся люди, не имеющие никакого летного удостоверения. Самолетом управлять в той или иной мере они, конечно, умеют, но, не желая тратить денежные средства на оплату полетов с инструктором, летного удостоверения не получают. Далеко не каждый любитель авиации способен оплатить минимально требуемое количество часов налета. Встречаются случаи, когда пилот поднимает самолет, находясь в нетрезвом состоянии. Частота происшествий с участием СЛА растет пропорционально популярности и распространенности малой авиации и тут можно только надеяться на сознательность пилотов, которые отвечают не только за свою жизнь, но и за жизнь своих пассажиров и тех, кто находится на земле.

А теперь, сенсация: автомобиль, он же воздушное судно!

Недавно стало известно, что российские конструкторские бюро предложили Минобороны РФ присоединиться к разработке летающих автомобилей. Проекты, носящие названия AVTOL-1 и AVTOL-2, будут реализованы гораздо быстрее при поддержке государства.

Российский проект AVTOL, под руководством инженера Мерзлякова, предусматривает три модификации летающих автомобилей. Так, AVTOL-1 – это аппарат, который может не только ездить по обычным дорогам, но и развивать сверхзвуковую скорость в воздухе. Автомобиль под именем AVTOL-2 может развивать скорость до 800 км/ч, а максимальная скорость модели AVTOL-3 составляет 400 км/ч.

Наибольший интерес для рядовых граждан может представлять, как раз AVTOL-3 конструкторы рассчитывают, что этот аппарат станет многофункциональным и универсальным. Идея разработчиков состоит в том, чтобы дать летающему автомобилю возможность вертикального взлета практически с любой поверхности, к примеру, песчаного покрытия или воды. Использовать транспортное средство можно будет для перевозки грузов или пассажиров.

На данный момент прототипы проходят летные испытания, которые должны завершиться летом 2015 года[4].

Но не только в России разрабатываются подобные проекты. Так, в США «Агентством передовых оборон-

ных исследовательских проектов» (DARPA) проводятся испытания похожего аппарата X-Plane VTOL. Максимальная скорость полета американского прототипа ограничена 700 км/ч. Правда, эксперты отмечают, что испытания пока этой летающей машины пока не принесли никаких впечатляющих результатов.

Кроме того, разработкой летающей машины в США уже давно занимается компания Terrafugia.

Их Transition – автомобиль со складными крыльями, уже сертифицирован для продаж в США. Правда, пока аппарат не так универсален – для взлета ему нужна полоса для разгона.

Первой же летающей машиной в Европе может стать Pegasus. Гибрид автомобиля и ультралёгкого самолёта, по мнению разработчиков, обязательно превратится в транспорт нового поколения.

Изобретатели готовятся вскоре завершить все испытания и приступить к серийному производству и продаже. Первую тестовую модель Pegasus разрабатывают в соответствии со строгими европейскими требованиями в сфере безопасности, для чего приглашаются инженеры из авиации.

Скорость аппарат развивает невысокую – 60–80 км/ч. Максимальное время в полете составляет три часа.

У голландских изобретателей – другая концепция. В отличие от российских американских и французских разработчиков, они совместили автомобиль не с самолетом, а с вертолетом. Аппарат получил соответствующее название – Helicycle Pal-V.

Это чудо техники представляет собой трехколесную капсулу с двумя посадочными местами, большим хвостом и винтом как у вертолета. И хвост, и винт складываются, и вертолет превращается в машину.

До «сотни» на земле Helicycle Pal-V разгоняется всего за 8 секунд. Бака топлива хватает либо на 1300 км, если использовать его как машину, либо на 350 при движении по воздуху.

Представители компании поговаривают, что у них уже есть внушительный список потенциальных клиентов.

А это означает, что в недалеком будущем численность парка СЛА совершит головокружительный скачок. Количество таких «воздушных судов» будет исчисляться не сотнями, а тысячами! Как ГИБДД будет осуществлять свои функции в отношении участников дорожного движения, способных мгновенно переквалифицироваться в участников воздушного движения? А диспетчерские службы? Они не будут обладать даже теми крохами информации об использовании воздушного пространства, которые получают в уведомлении в настоящее время. Ведь гибриды «автомобиль-воздушное судно» не будут нуждаться в специально оборудованном месте взлета и посадки, а большинство из них изначально не оборудуются бортовыми ответчиками. При этом возможно как преднамеренное отключение бортовых ответчиков (воздушный терроризм), так и непреднамеренное в силу технических неисправностей.

В таких условиях радиотехнические войска будут не в состоянии отследить и контролировать всех участников воздушного движения.

Специалисты ПВО хорошо знают, что дежурное (некогда сплошное, всевысотное, многочастотное, с одно-, двукратным перекрытием) радиолокационное поле над Россией давно приобрело очаговый характер. В пределах оставшихся зон радиолокационного наблюдения в лучшем случае обеспечивается обнаружение целей на средних и больших высотах. Развертывание же новых РЛС маловысотного поля - дело весьма дорогое, а в местах с большой плотностью населения, кроме того, вызывает серьезное противодействие со стороны экологических организаций.

Сокращение подразделений и средств радиолокационной разведки привело к тому, что над территорией РФ сегодня существуют открытые участки государственной границы и внутренних районов страны.

Проблема усугубляется и высокой вероятностью применения низколетящих малозаметных целей, что требует уплотнения боевых порядков РЛС традиционного парка и увеличения затратности содержания сплошного маловысотного радиолокационного поля (МВРЛП). Для создания сплошного дежурного круглосуточного МВРЛП высотой от 25 метров (высота пролета крылатой ракеты или самолета сверхлегкой авиации) по фронту всего 100 километров требуется не менее двух РЛС типа КАСТА-2Е2 (39Н6) [5].

Но в соответствии с федеральным законом «О санитарно-эпидемиологическом благополучии населения» от 30 марта 1999 года № 52-ФЗ [6] установлены нормы излучений, которые носят обязательный характер на всей территории России. Мощность излучения любой из известных РЛС ПВО многократно превышает эти нормы. Также нужно учесть, что РЛС типа КАСТА-2Е2 (39Н6), потребляемая мощность каждой из которых составляет 23 кВт, являются одними из самых менее энергозатратных. С учетом средней стоимости электроэнергии в ценах 2015 года только стоимость поддержания этого участка МВРЛП составит не менее трех миллионов рублей в год. При подсчете необходимо учесть и стоимость затрат всей инфраструктуры обеспечения функционирования данных средств, от персонала до регламентных работ.

Таким образом, налицо дисбаланс потребностей и возможностей субъектов эволюции использования воздушного пространства.

Проблема контроля использования воздушного пространства СЛА в пределах важных административно-политических центров и объектов техногенных катастроф может быть решена путем использования систем и средств дающих наибольший удельный вклад в эффективность информационного обеспечения на единицу суммарных затрат на всех этапах жизненного цикла этих систем и средств. В настоящее время эту роль могут выполнять оптико-электронные системы (ОЭС) обнаружения и автосопровождения целей.

Наибольшее развитие такие ОЭС получили в системах управления корабельным оружием, где решены вопросы обеспечения кругового пассивного обзора в инфракрасном спектре длин волн, автоматического обнаружения нескольких целей, автосопровождения нескольких целей одновременно без прекращения пассивной локации окружающего пространства. Обеспечивается выполнение всех задач ОЭС, связанных с целеуказанием: определение координат целей и параметров их движения, информационный взаимообмен в режиме реального времени с системами управления оружием. Учитывая погрешность стабилизации, которая на подобных ОЭС не превышает 1 угловой минуты, и качество современных оптических каналов, удается в дневных и ночных условиях точно наводиться на быстродвижущиеся наземные, надводные и воздушные цели на расстоянии до 20 км [7]. Данные ОЭС даже несколько избыточны в плане наличия блоков гироскопической стабилизации, применение которых не обязательно на стационарных объектах.

Определение пространственных координат сетью стационарных ОЭС может производиться включением в состав аппаратуры лазерного дальномера, либо триангуляционным методом.

Триангуляционный метод основан на измерении угловых направлений на объект минимум в двух приемных пунктах, разнесенных на некоторое расстояние, называемое базой (рис. 1).

При определении пространственных координат объекта достаточно точно измерить азимуты β_1 и β в двух пунктах и угол места ε_1 в одном либо, наоборот, углы места ε_1 и ε_2 в двух пунктах и азимут β_1 в одном.

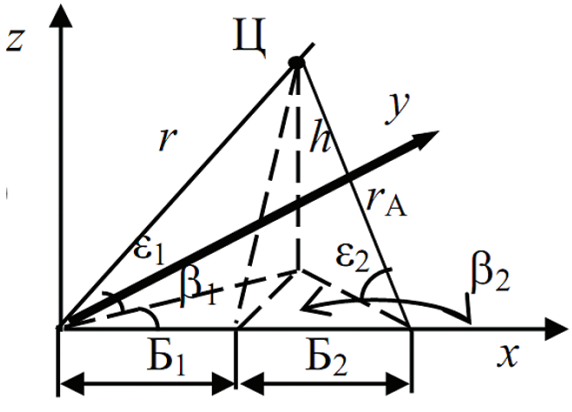


Рис.1. Пояснение триангуляционного метода определения координат в пространстве

Местоположение источника излучения соответствует точке пересечения трех поверхностей положения – трех плоскостей. Дальность до объекта r рассчитывается по измеренным углам и известной базе, например, из соотношений:

$$r\cos\varepsilon_1 \cdot \cos\beta_1 + r_A \cdot \cos\varepsilon_2 \cdot \cos(180^\circ - \beta_2) = Б_1 - Б_2 = Б,$$
$$r\cos\varepsilon_1 \cdot \sin\beta_1 = r_A \cdot \cos\varepsilon_2 \cdot \sin(180^\circ - \beta_2) = h,$$

откуда исключая $r_A \cos\varepsilon_2$, получаем:

$$r = \frac{Б}{\cos\varepsilon_1 \cdot (\cos\beta_1 - \sin\beta_1 \cdot \mathrm{ctg}\beta_2)}$$

Создание подсистемы контроля воздушного пространства важных административно-политических центров на базе ОЭС обеспечит решение задач обнаружения СЛА, получения координатной и некоординатной информации о СЛА их идентификации.

Для размещения ОЭС могут использоваться как охраняемые высотные здания подразделений и частей МО и других ведомств РФ, научных организаций, предприятий, высотные линии электропередач, вышки телевизионных и сотовых ретрансляторов.

Связанные в единую систему и обеспеченные автоматизацией обработки и выдачи информации потребителю ОЭС позволят в полной мере использовать их преимущества в высокой разрешающей способности определения координат СЛА, низком энергопотреблении, электромагнитной безопасности.

Литература

1. Постановление Правительства РФ от 11.03.2010 N 138 «Об утверждении Федеральных правил использования воздушного пространства Российской Федерации».

2. http://ria.ru/defense_safety/20100209/208399106.html (дата обращения 25.05.2015).

3. http://www.rosbalt.ru/piter/2014/01/14/1220731.html (дата обращения 25.05.2015).

4. http://focusgoroda.ru/materials/2014-04-08/3205.html (дата обращения 25.05.2015).

5. http://www.pro-pvo.ru/articles/18242 (дата обращения 25.05.2015).

6. http://правовед.org/zakon/federalnyi-zakon-rf-ot-30-marta-1999-goda-№-52-fz-«o-sanitarno-epidemiologicheskom-blagopoluch (дата обращения 25.05.2015).

7. http://npo-karat.ru (дата обращения 25.05. 2015).

Для цитирования:
Хашагульгов Р.А-М., Ходор М.А. Частная авиация – новая угроза безопасности воздушного движения в России // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 22–26.

PRIVATE AVIATION IS A NEW THREAT TO SECURITY AIR TRAFFIC IN RUSSIA

Khashagulgov Ruslan Abdoul-Mazhitovich,
St. Petersburg, Russian, x.p.a-m@mail.ru
Hodor Mikhail Aleksandrovich,
St. Petersburg, Russian, khodorvvv@mail.ru

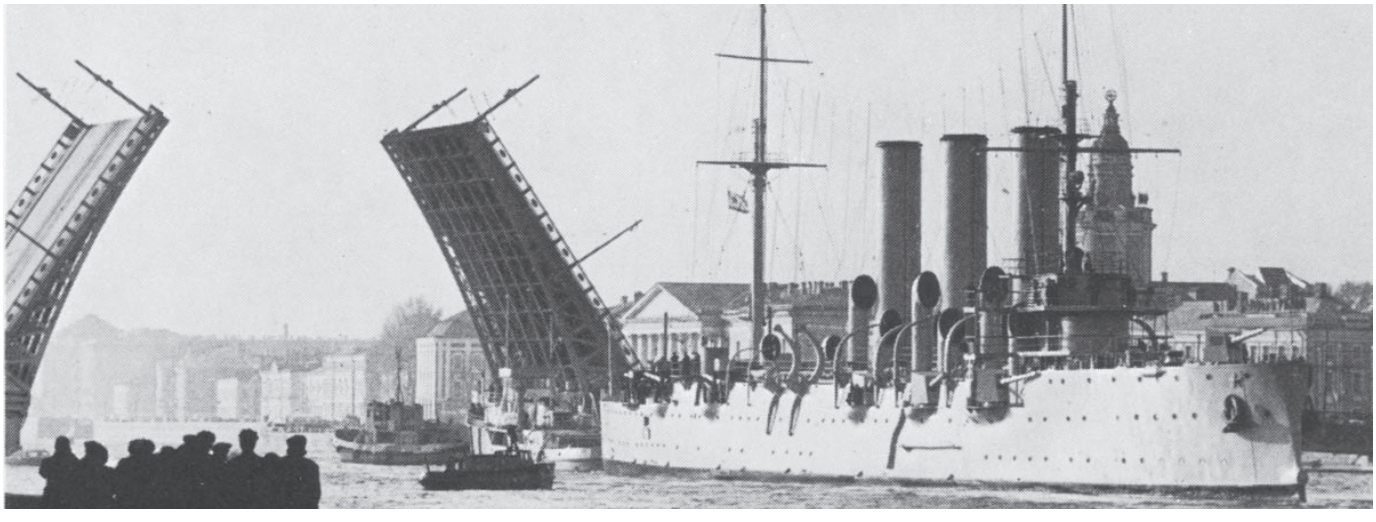
Abstract
Control procedures for using aircraft airspace is one of the major problems solved by any sovereign state. Gathering information about the current coordinates, motion parameters, the nationality of the aircraft assigned to the objects and units of species and genera of the Armed Forces, as well as special services to civil aviation. Concentration of efforts of various departments of the organization of complex use of forces and means of conducting aerial reconnaissance in areas of co-location, is a system of investigation and control of the airspace of the State. Ideally, the monitoring system should record, to determine the parameters of air targets at all altitudes of their application and from any reflecting surface. In reality, have to compromise due to the high cost, limited technical characteristics of radar, the environmental safety requirements for their placement, creating a better radar field with critical areas and less quality in the hinterland. However, the rapid development of light aircraft located, including private use, poses intelligence system and airspace control problem to address a new threat - the safety of air traffic over administrative and political centers and objects man-made disasters. Reconnaissance on small and extremely low altitudes not provide traditional radar facilities offered to perform by creating subsystem control the airspace of important administrative and political centers and objects man-made disasters on the basis of optoelectronic detection systems and delivery of information, in addition to the existing control system. We analyzed some ways its construction and technical implementation. It is shown that the optical-electronic systems at the present stage of development to meet the challenges of control of airspace use light aircraft at low and extremely low altitudes.

Keywords: aircraft, ultralight aircraft, flight safety, flying car, low-altitude radar field, opto-electronic system.

References
1. The Government decree on 11/03/2010 N 138 «On approval of Federal rules of use of airspace of the Russian Federation». (in Russian).
2. http://ria.ru/defense_safety/20100209/208399106.html (date of access 25.05.2015).
3. http://www.rosbalt.ru/piter/2014/01/14/1220731.html (date of access 25.05.2015).
4. http://focusgoroda.ru/materials/2014-04-08/3205.html (date of access 25.05.2015).
5. http://www.pro-pvo.ru/articles/18242 (date of access 25.05.2015).
6.http://правовед.org/zakon/federalnyi-zakon-rf-ot-30-marta-1999-goda-№-52-fz-«o-sanitarno-epidemiologich-eskom-blagopoluch (date of access 25.05.2015).
7. http://npo-karat.ru (date of access 25.05.2015).

Information about authors:
Khashagulgov R.A-M., Ph.D., doctoral student, Military space Academy;
Hodor M.A., lecturer in Department of Automated systems control, Military Space Academy.

For citation:
Khashagulgov R.A-M., Hodor M.A. Private aviation is a new threat to security air traffic in Russia. H&ES Research. 2015. Vol. 7. No.3. Pp. 22–26. (in Russian).



ВУС

Военно-учетный стол

Программный комплекс

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

Воинский учет в организациях:

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

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

• Создание и печать отчетных документов по установленным формам в 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

XIX Международный Форум «Инфокоммуникации устойчивого развития» в рамках деловой программы 27-й международной выставки «Связь-Экспокомм-2015»

Форум МАС проходил в знаменательный год 150-летия Международного союза электросвязи (МСЭ), 70-летия Организации Объединенных Наций, 120-летия открытия радио А.С. Поповым, 70-летия Победы в Великой Отечественной войне. В этот год вступает в действие новый глобальный договор – «Регламент международной электросвязи», «Дубайский план действий» МСЭ, рассчитанный на период до 2020 года и принятый Всемирной конференцией по развитию электросвязи (с участием делегации России), знаменующие окончание эры традиционной телефонно-телеграфной связи.

В 2015 году завершается первый этап реализации задач стратегического документа ООН «Цели развития тысячелетия», принятого мировыми лидерами в 2000 году и включающего задачу обеспечения повсеместного доступа к информационно-коммуникационным технологиям. Так совпало, что именно в этом году количество контрактов на подвижную связь достигнет численности населения Земли.

Все эти события послужили поводом для всесторонней публичной оценки на Форуме МАС роли инфокоммуникаций, их значения в общественном развитии, как одной из важнейших составляющих национальной и глобальной инфраструктуры.

Термин «устойчивое развитие» отражает одну из актуальнейших общемировых задач, решаемых в наше время, направленной на обеспечение высокого качества жизни для людей нынешнего и будущих поколений, переход от во многом угрожающего планете интенсивного индустриального развития к новой модели цивилизации, способной противостоять надвигающемуся системному кризису в экономике, экологии и социуме – к информационному обществу, обществу знаний.

Как сказал в своем приветствии форуму Генеральный секретарь МСЭ, академик МАС Хоулинь Чжао: «Сегодня мы живем в быстро развивающемся мире, в котором эффективность экономики, государственного управления и качество жизни населения во все большей степени определяются уровнем распространения информационных/коммуникационных технологий (ИКТ), позволяющих реализовать преимущества информационного общества».

По данным МСЭ к началу года более 40 %, или 3 млрд. населения в мире уже пользуются широкополосным доступом. К 2017 году такая возможность будет у каждого второго жителя Земли. Уровень проникновения подвижного ШПД в 2014 г. в мире был 32%, в развитых странах 84 %, в России – около 65%.

Но по мере роста использования электросвязи/ИКТ, возникают и новые риски, новые проблемы, которые нашли свое отражение в докладах и выступлениях форума.

В приветственных выступлениях члена Совета Федерации Федерального Собрания Российской Федерации Н.Ф. Пожиткова, Председателя Ассоциации Содействия ООН, ректора МГИМО (У) МИД России А.В. Торкунова, председателя Профсоюза работников связи России А.Г. Назейкина, Министра Правительства Москвы, руководителя департамента информационных технологий А.В. Ермолаева, генерального директора ИК РСС Н.Н. Мухитдинова и в докладах на пленарном заседании Президента МАС А.П. Оситис, администратора по программам зонального отделения МСЭ А.Л. Унтилы, руководителя отдела общегородского видеонаблюдения Департамента информационных технологий города Москвы Д.А. Головина, исполнительного директора МОКС «ИНТЕРСПУТНИК» В.С. Вещунова, проектного менеджера по работе с Телекомом Кластера «Космические технологии и телекоммуникации» Фонда «Сколково» М.А. Жаренова,

рассматривались ряд системных проблем современного развития телекоммуникаций и связанные с этим вопросы.

Конкретные проблемы и пути их решения рассматривались на заседаниях в формате круглого стола.

Комплекс вопросов, связанных проблемами телеком-операторов, перехода к сетям нового поколения обсуждался в ходе работы круглого стола «Создание цифровых коммуникаций в интересах устойчивого развития государства, общества, личности в мире и в Российской Федерации». Операторы вынуждены сегодня изменять не только технологии, но и свои бизнес-модели. В условиях конкуренции со стороны ранее не связанных с ними бизнесов, решать проблемы диверсификации, предоставления новых услуг, в неприемлемой, по общему мнению, ситуации отсутствия единой государственной концепции построения и развития национальной сети менять технологии, переходить к сетям последующих поколений, в т.ч. на базе технологий программно-конфигурируемых сетей и виртуализации сетевых функций. На круглом столе обсуждались вопросы отсутствия отраслевой системы технологического регулирования в части: проектирования, строительства, эксплуатации, межотраслевого взаимодействия и взаимосвязи межотраслевых нормативов и сводов правил, отсутствие в Градостроительном кодексе РФ требований к строительству и эксплуатации инфокоммуникационных сетей и многие другие вопросы.

Вызывает озабоченность состояние мелкого и среднего бизнеса. В отрасли связи России 92% составляют доходы нескольких крупных компаний и лишь 8% – мелких и средних.

Большое внимание Форума было уделено такой важной, актуальной сегодня теме, как «Импортозамещение». В этой связи Форум обратил особое внимание на необходимость кардинального расширения поддержки отраслевой отечественной науки и отечественных разработок в условиях актуализации вопросов импортозамещения. Также было отмечено, что необходимо разработать нормативно-правовые акты, определяющие развитие электросвязи /ИКТ в России в части создания отечественного оборудования. Для академии тема импортозамещения не новая. Вопросами производства современного высокотехнологичного оборудования инфокоммуникаций МАС занимается постоянно. На осень этого года намечено проведение очередной международной конференции по этому вопросу.

Одним из ключевых приоритетов в работе связистов становится обеспечение информационной безопасности. С развитием новых сетей и информационных технологий вопросы укрепления доверия, надежности и безопасности при использовании электросвязи/ИКТ выходят на первый план. Круглые столы «Проблемы достоверности идентификации субъектов и объектов при развитии инфокоммуникаций нового поколения», «Безопасность контента» были посвящены этим проблемам.

Традиционными для Форумов МАС являются вопросы инновационного развития в разных секторах инфокоммуникаций. Не была нарушена эта традиция и в этот раз, о чем свидетельствуют публичные обсуждения, организованные по проблемам развития цифрового телевидения; сетей 5G; магистральных кабельных линий и сетей.

Результаты и предложения состоявшихся обсуждений обобщены в Решении Форума МАС'2015, которое будет размещено на сайте МАС.

Международная общественнаяакадемия связи
(МАС)
тел.: (495) 742-53-53, 742-17-72,
факс (495) 742-75-46,
e-mail: info@ita.org.ru
URL: www ita.org.ru

ПРЕДИКАТНАЯ МОДЕЛЬ СХЕМНО-ОРИЕНТИРОВАННЫХ ЗАПРОСОВ ОБСЛУЖИВАЮЩЕГО ПЕРСОНАЛА В СИСТЕМАХ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ

Курчидис
Виктор Александрович,
д.т.н., профессор, профессор кафедры автоматики (и вычислительных средств) Военно-космической академии имени А.Ф. Можайского, г. Ярославль, Россия, idahmer2@yandex.ru

Попов
Тимур Александрович,
заместитель начальника научно-исследовательского отдела Военно-космической академии имени А.Ф. Можайского г. Ярославль,Россия, popov_ta@mail.ru

Анисимов
Олег Витальевич,
к.т.н., доцент, доцент кафедры автоматики (и вычислительных средств) Военно-космической академии имени А.Ф. Можайского, г. Ярославль, Россия, qwaker@inbox.ru

Ключевые слова:
информационная поддержка, электрическая схема, предикатная модель, радиоэлектронная аппаратура, техническая эксплуатация, схемно-ориентированный запрос.

АННОТАЦИЯ

Одним из путей повышения эффективности решения задач эксплуатации сложных технических комплексов является использование средств автоматизации. Существующие средства автоматизации, не предоставляют обслуживающему персоналу возможности по формированию запросов на получение требуемой информации в виде фрагментов электрических схем с использованием понятий и терминов предметной области в рамках синтаксиса естественно-подобного языка.

Работа посвящена разработке предикатной модели запросов, ориентированных на использование понятий и терминов предметной области при формировании целевых условий со стороны обслуживающего персонала для представления запрашиваемых фрагментов схем. Такие запросы в работе названы схемно-ориентированными. Предлагается свойства элементов, участвующих в определении условий, формально записывать в форме отношений между предметными понятиями. Выявлены основные отношения, которые соответствуют структурным элементам электрической схемы и определены во фреймовой концептуальной модели радиоэлектронной аппаратуры.

Определены задаваемые обслуживающим персоналом условия, которым должны удовлетворять элементы электрических схем, отображаемые в виде графических фрагментов. Обосновано использование логики предикатов первого порядка в рамках синтаксиса естественного языка для формирования целевых условий запросов в терминах и понятиях электрических схем радиоэлектронной аппаратуры. Предлагаемая формализованная структура схемно-ориентированных запросов позволяет согласовать предикатные формулы со структурой предложений естественного языка.

Предложенная предикатная модель характеризуется тем, что такие запросы формируется на основе предложений на естественно-подобном языке. При этом имеется возможность использовать в запросах термины и понятия предметной области, а также производить согласование используемых слов по падежам и формам единственного/множественного числа.

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. Это способствует повышению уровня автоматизации систем информационной поддержки обслуживающего персонала и сокращению времени решения прикладных задач технической эксплуатации изделий радиоэлектронной аппаратуры сложных технических комплексов.

Введение

Эксплуатация сложных технических комплексов требует от обслуживающего персонала навыков как по использованию радиоэлектронной аппаратуры этих комплексов по назначению, так и ее техническому обслуживанию и восстановлению, что связано с необходимостью поддержания таких комплексов в работоспособном состоянии. Важную роль в процессе восстановления радиоэлектронной аппаратуры играют средства информационной поддержки, предоставляющие обслуживающему персоналу доступ к эксплуатационной документации (комплект электрических схем, руководства по эксплуатации, нормативно-справочная информация и т.п.). Организация таких средств в виде автоматизированных систем информационной поддержки (СИП) является одним из путей повышения эффективности деятельности обслуживающего персонала благодаря расширению возможностей по извлечению, анализу и предоставлению разнородной информации.

В современных СИП для извлечения информации, необходимой при выполнении операций восстановления РЭА, обслуживающий персонал формирует запросы, имеющие определенную формализованную структуру. Учитывая, что современные СИП построены на основе реляционных или объектно-реляционных баз данных и систем управления, для определения необходимой информации используются процедурные и/или декларативные языки запросов, использующие выражения реляционной алгебры и/или формулы реляционного исчисления [2]. Примерами современных языков запросов являются формальные языки, такие как SQL, DBE, XQuery, XPath, LinQ и другие.

Такие запросные языки являются универсальными с точки зрения формирования разнообразных запросов в терминах баз данных. Однако они не позволяют в структуре запросов учитывать особенности концептуального представления терминов и понятий для конкретных предметных областей. Поэтому для развития средств автоматизации в предметной области технического обслуживания и восстановления РЭА необходимо создавать языки запросов для СИП, которые позволяют использовать систему терминов и понятий, сложившуюся в нормативной и эксплуатационной документации, а также в практике эксплуатации РЭА. Структура таких языков в значительной степени определяется информационным ресурсом, с которым работает обслуживающий персонал.

Важным информационным ресурсом при выполнении операций по восстановления являются электрические схемы РЭА, которые позволяют обслуживающему персоналу на основе графического представления получать подробную информацию об электрических элементах РЭА и связях между ними. Наличие электрических схем в комплекте эксплуатационных документов на РЭА регламентировано существующими стандартами [ГОСТ 2.601-2006, ГОСТ 2.701-2008].

Автоматизированные средства информационной поддержки ОП в существующих СИП могут обеспечивать использование целого ряда распространенных способов и приемов работы со схемами, таких, как предоставление схем, предоставление дополнительной информации для схемных элементов, выделение фрагментов схем и т.д. При этом обслуживающий персонал, имея определенное представление о способе решения прикладной задачи восстановления РЭА, формулирует конкретную цель в предметных понятиях и терминах электрических схем. Эта цель должна быть отражена в запросе обслуживающего персонала и направлена на определение одного или нескольких фрагментов схем, которые содержат необходимую техническую информацию.

Повышение гибкости и эффективности способов работы ОП со схемами при восстановлении РЭА может быть обеспечено путем совершенствования средств формирования запросов за счет использования в запросах конструкций на естественно-подобном языке [1]. Это обеспечивает грамматическое и терминологическое согласование содержания запроса с представлением ОП о цели и способах решения задач восстановления РЭА. При этом появляется возможность полностью формировать запросы на основе естественно-подобного языка и учитывать условия, определяемые целью запроса, а также автоматизировать операции формирования и представления обслуживающему персоналу схемных фрагментов. Это приводит к возможности перехода в современных СИП к высокоуровневым концептуальным интерфейсам, обеспечивающим совместное использование речевых, текстовых и схемно-графических технологий при работе обслуживающего персонала с электрическими схемами радиоэлектронной аппаратуры.

Такой подход к автоматизации СИП, в первую очередь, требует решения задачи определения и формализация структуры запросов, которые обеспечивают обслуживающему персоналу возможность описания цели и условий на естественно-подобном языке с использованием терминов и понятий предметной области, необходимых для формирования и представления фрагментов электрических схем при восстановлении РЭА. Решение сформулированной задачи в литературе отсутствует, в данной работе для таких запросов используется название «схемно-ориентированный запрос» (СОЗ).

Определение и формализация структуры СОЗ связана с разработкой модели СОЗ, которая должна с одной стороны использовать термины и понятия, связанные со структурными элементами электрических схем, а с другой стороны отражать отношения между этими элементами, представленные на основе естественного языка.

В данной работе решение научной задачи по разработке модели СОЗ осуществляется за счет решения двух частных задач: формализованного описание структуры схемно-ориентированного запроса и пред-

ставление схемно-ориентированного запроса на естественно-подобном языке.

Формализованное описание структуры схемно-ориентированного запроса

Схемно-ориентированный запрос в терминах электрических схем в целом должен соответствовать общепринятой структуре запроса [2]:

<Запрос> = <Команда> <Данные>.

Информационная поддержка обслуживающего персонала на основе СОЗ направлена на управление визуальным представлением графических фрагментов электрических схем и определяется полем <Данные> запроса. При таком способе организации информационной поддержки поле <Команда> у всех запросов может основываться на использовании, по крайней мере, двух команд, которые могут быть ассоциированы, например, со словом «Показать» и «Скрыть». Цель запроса с командой «Показать» состоит в определении схемных фрагментов с необходимой информацией для визуального представления. Запроса с командой «Скрыть» используется для скрытия схемных фрагментов, соответствующих требуемым условиям, при визуальном отображении схем РЭА.

Поле <Данные> определяет задаваемые обслуживающим персоналом условия, которым должны удовлетворять элементы электрических схем, отображаемые в составе визуальных графических фрагментов. Условия определения множества элементов схемы, могут задаваться непосредственно свойством (совокупностью свойств) одного элемента x схемы либо опосредованно через другие элементы y, z и т.д., имеющие связи не только с элементом x, но и между собой.

Формально множество Q_1 целевых элементов схемы, определяемых на основе свойств одного элемента можно определить следующим образом:

$$Q_1 = \{x \mid Y_1(x)\} \quad (1)$$

где $У_1(x)$ обозначает условия, которым должен удовлетворять элемент x электрической схемы.

В свою очередь, условие $У_1(x)$ может определяться одним свойством $P(x)$ либо совокупностью свойств элемента x электрической схемы:

$$У_1(x) = \varphi_1(P_{11}(x), P_{12}(x), \ldots). \quad (2)$$

В случае, когда условие для определения элементов x могут задаваться опосредованно через свойства других элементов у электрической схемы, множество Q_2 целевых элементов схемы определяется следующим образом:

$$Q_2 = \{x \mid \exists y\, Y_2(x, y)\} \quad (3)$$

В общем случае условие $У_2(x, y)$ может определяться не только свойствами элемента x, но и свойствами элемента y, а также свойствами элемента x, связанными с другими элементами y:

$$У_2(x, y) = \varphi_2(P_{21}(x), P_{22}(x), \ldots, (P'_{21}(y), P'_{22}(y), \ldots, P''_{21}(x, y), P''_{22}(x, y), \ldots). \quad (4)$$

Условия для определения целевых элементов x схемы могут задаваться опосредованно через свойства не одного, а нескольких других элементов y, z электрической схемы:

$$Q_3 = \{x \mid \exists y\, \exists z\, Y_3(x, y, z)\} \quad (5)$$

При этом не только элемент x может определяться опосредованно через элемент y, но и элемент y может опосредованно определяться через элемент z. В этом случае условие $У_3(x, y, z)$ будет определяться не только свойствами элемента x, но также свойствами элементов y и z; свойствами элемента x, связанными с элементами y и z; свойствами элемента y, связанными с элементом z.

Формально свойства элементов, которые участвуют в определении условий, целесообразно записывать в форме отношений вида $\alpha R \beta$ или $R(\alpha,\beta)$. В этой записи α и β являются предметными понятиями, которые соответствуют структурным элементам x, y, z электрической схемы и определены во фреймовой концептуальной модели ФМ РЭА, предложенной в работе [5], а R определяет вид (название) отношения между элементами этой модели. В такой форме записи эти отношения являются высказываниями, которые могут быть истинными или ложными, так что формулы φ_1, φ_2 и φ_3, которые определяют условия $У_1(x)$, $У_2(x,y)$ и $У_3(x,y,z)$, являются логическими формулами.

Человеку условия удобно выражать в виде суждений, используя форму высказываний о свойствах и отношениях структурных элементов электрических схем. Такие высказывания основываются на использовании понятий предметной области и могут иметь два значения истинности (истина или ложь). Примерами таких высказываний могут быть: «блок имеет разъем», «ячейка выполняет функцию» и т.п. Поскольку элементы отношений могут быть предметными переменными, использование только логики высказываний может быть не достаточно для определения сложных условий $У_1(x)$, $У_2(x,y)$ и $У_3(x,y,z)$. Поэтому при формировании условий на основе отношений целесообразно использовать предикатную форму записи, которая основывается на логике предикатов первого порядка. Использование языка предикатов позволяет создавать сложные высказывания, которые при формальной записи используют операции алгебры логики (и, или, не) и кванторы существования и общности [4-6].

Предметные понятия, используемые в записи предикатных выражений, могут являться предметными переменными или предметными константами. В качестве предметных переменных выступают понятия, определяемые слотами фреймовой модели ФМ РЭА, описанной в работе [5], а в качестве предметных констант – значения соответствующих слотов.

При таком подходе к формализации структуры СОЗ все свойства схемных элементов x, y и z, которые определяются условиями разных видов $У_1(x)$, $У_2(x,y)$и $У_3(x,y,z)$, целесообразно записывать в форме предикатов на основе необходимых отношений R_1, R_2, R_3 и т.д. В результате будет сформирована предикатная модель схемно-ориентированных запросов. В такой модели собственно условие может быть представлено в виде составной формулы на основе операций алгебры логики. Например, в случае, когда условие определяется свойствами одного схемного элемента x (выражение 2), составная формула может иметь вид:

$$У_1(x) = R_{11}(x)\& \overline{R}_{12}(x) \vee R_{13}(\mathrm{x}, y), \qquad (6)$$

где отношения R_{11}, R_{12}, R_{13}, – унарные отношения, отражающие свойства элемента x.

В случае, когда условие определяется двумя элементами x и y (выражение 4), составная формула может иметь вид:

$$У_2(x, y) = R_{21}(x)\& \overline{R}_{22}(x, y) \vee R_{23}(\mathrm{x}, y), \qquad (7)$$

где R_{21} – унарное отношение, отражающее свойства элемента x, а R_{22} и R_{23} – бинарные отношения между элементами x и y.

Аналогично можно записать логическую формулу для условий с большим числом учитываемых схемных элементов. Множество элементов Q, составляющих цель запроса, с использованием исчисления предикатов может определяться предикатным выражением, которое формируется с использованием кванторов. Например, применительно к множеству Q_1 предикатное выражение имеет вид: $\forall x\ Y_1(x)$. Этот предикат определяет множество Q_1, как совокупность элементов x, в которой для всех x выполняется условие $У_1(x)$. Применительно к множеству Q_2 предикатное выражение имеет вид: $\forall x\ \exists y\ Y_2(x, y)$. Этот предикат определяет множество Q_2, как совокупность элементов x и y, в которой для всех x выполняется условие $Y_2(x, y)$. Аналогично записывается предикат, определяющий множество элементов Q_3.

В предикатной модели СОЗ с помощью формул логики предикатов предлагается записывать собственно условия, а запрос представлять в виде предложений, которые используют предикатные формулы и понятия есте-ственного языка. При этом использование понятий русского языка ограничивается, с одной стороны, предикатной формой записи, а, с другой стороны, требованием их согласования с позиций грамматических правил естественного языка.

При таком подходе к определению структуры запроса поле <Данные> в СОЗ предлагается формировать на основе языка логики предикатов. Это позволяет в рамках общей предикатной модели СОЗ, с одной стороны, логически связать в запросе понятия и отношения предметной области, а, с другой стороны, предоставляет возможность использовать простые синтаксические структуры естественного языка, в частности, вида «подлежащее-сказуемое-дополнение».

Ниже развитие способов использования языковых синтаксических средств направлено на формирование сложных схемно-ориентированных запросов, которые в целом соответствуют правилам естественного языка.

Представление схемно-ориентированного запроса на естественно-подобном языке

Предикатный язык формирования схемно-ориентированных запросов основывается на использовании двух языковых элементов – термов и предикатов. Термы определяют понятия и объекты предметной области, которые определяются используемой концептуальной моделью предметной области. При использовании фреймовой модели ФМ РЭА, как концептуальной модели РЭА, в качестве термов целесообразно использовать типы структурных элементов схемы (блок, ячейка, разъем, цепь прохождения сигнала и т.д.) и значения их атрибутов (маркировка, название, позиционное обозначение и т.д.), а также функциональные элементы модели (функциональные задачи, выполняемые функции) и значения их атрибутов (имя функциональной задачи, имя выполняемой функции и т.д.).

Фреймовая модель ФМ РЭА позволяет определить только понятия, используемые в схемно-ориентированных запросах. Для определения множества предикатов, необходимо проанализировать отношения между предметными переменными, ассоциированными с понятиями ФКМ РЭА, и представить их в виде терминов естественного языка, которые используются для описания этих отношений.

Анализ ФМ РЭА показывает, что предметное понятие «блок», как предикатная переменная, участвует, по крайней мере, в шести базовых отношениях, которые могут быть определены через языковые термины естественного языка: «соединен с», «входит в», «имеет», «содержит», «выполняет», «влияет на». Это позволяет зафиксировать все базовые отношения $R(\alpha, \beta)$, связывающие предикатную переменную α =«блок» с другими предикатными переменными β, и представить их в виде фрагмента семантической сети (рис. 1).

Аналогичный анализ, выполненный для всех предикатных переменных, позволяет сформировать полный граф семантической сети и определить множество языковых понятий, ассоциированных с предикатами R в модели СОЗ:

R = {«входит в», «содержит», «соединяет», «соединен с», «связан с», «проходит через», «имеет», «влияет на», «зависит от», «выполняет»}.

Использование названных элементов языка, позволяет, применяя формализм языка логики предикатов, создать основу представления запросов в виде совокупности простых предложений естественного языка, содержащих термины и понятия электрических схем. Такие простые предложения имеют базовую предикативную форму в естественном языке. Примерами

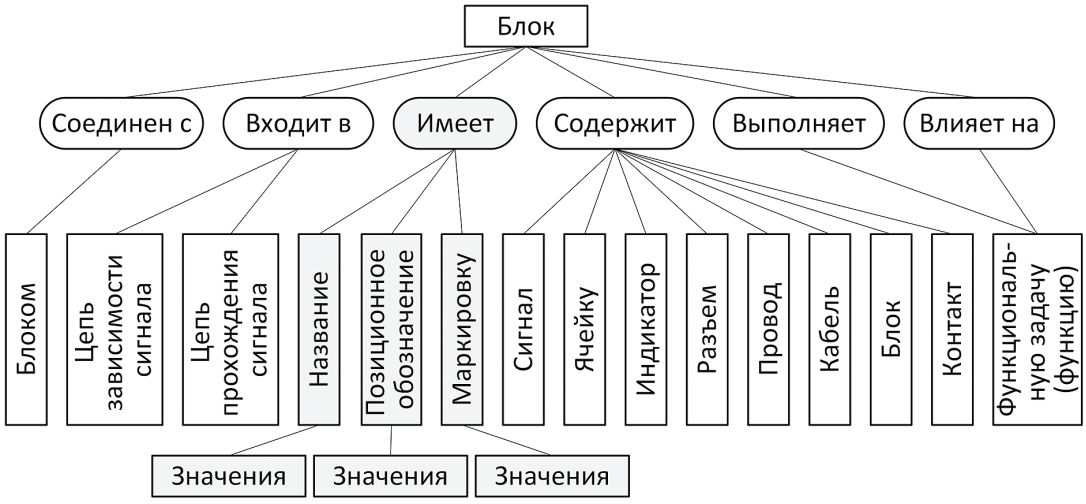


Рис.1. Фрагмент семантической сети для предикатной переменной <блок>

таких предложений могут быть следующие: «блок содержит ячейку», «ячейка входит в блок», «блок выполняет функцию» и т.п.

Следует отметить одну особенность в записи предикатных форм в таких простых предложениях, связанную с использованием предикатных констант. Эти константы в соответствии с фреймовой моделью ФМ РЭА [5] определяют уникальные значения свойств структурных элементов электрических схем. Наличие конкретного значения свойства всякого элемента определяется использованием предиката «имеет», например, «ячейка имеет название Я5», «блок имеет позиционное обозначение У2» и т.п. В этом случае целесообразно использовать сокращенную языковую запись в предложениях, которая соответствует унарной форме записи $R(x)$ отношения, например, «ячейка Я5», «блок А1» и т.п. С учетом этого замечания допустимы следующие предложения в структуре запроса: «блок содержит ячейку Я5», «ячейка входит в блок ФР1», «сигнал зависит от сигнала В», «цепь сигнала соединяет блоки А и блоки В», и т.п.

Эти же простые предложения можно записать как с использованием причастного оборота (например, «блок, содержащий ячейку Я5»; «ячейка, входящая в блок ФР1»; сигнал, не зависящий от сигнала В; цепь сигнала, соединяющая блоки А и В), так и используя придаточный определительный оборот с союзным словом «который» (например, блок, который содержит ячейку Я5; ячейка, которая входит в блок ФР1; сигнал, который не зависит от сигнала В; цепь сигнала, которая соединяет блоки А и В). В таком случае использование одноместной формы записи отношений для определения значения свойств элементов позволяет сократить длину предложения в запросе. Так, предложение «Блок, который содержит ячейку, имеющую позиционное обозначение У2», может быть представлено в сокращенной форме: «Блок, который содержит ячейку У2».

С формальной точки зрения предложение «Блок, который содержит ячейку У2» используя предикатную модель схемно-ориентированного запроса можно записать следующим образом:

У(блок, ячейка, У2) = содержит (блок, ячейку) & имеет(ячейка, название) & есть(название, У2).

В соответствии с правилами формирования условий вида (6) и (7) каждое последующее предложение в запросе направлено на уточнение свойств термов, используемых в предыдущих предложениях. Поэтому объединение в структуре запроса нескольких простых предложений в сложное предложение можно осуществлять с использованием, например, наречий. В частности, предлагается использовать наречие «причем», так, что использование данного наречия требует представления присоединяемого простого предложения в базовой предикативной форме.

Использование перечисленных правил и приемов формирования предложений позволяет определить структуру поля «Данные» схемно-ориентированного запроса, которая в целом будет соответствовать грамматическим требованиям построения предложений на естественном языке. Использование естественного языка в структуре предложений запроса позволяет производить согласование используемых слов по падежам, а также использовать формы множественного/единственного числа, что удобно с точки зрения голосового формирования этих запросов обслуживающим персоналом. Учитывая, что использование команды «показать» также синтаксически согласуется с предлагаемой структурой предложения, следует отметить, что, в целом структура запросов является грамматически корректной конструкцией естественного языка.

Описанные выше правила определяют общую структуру схемно-ориентированного запросов в виде предложений на естественно-подобном языке. В качестве примеров запросов, соответствующих этим правилам, могут служить следующие предложения: «Показать блок, который содержит ячейку, которая включает разъем Ш1»; «Показать ячейку, которая входит в цепь прохождения сигнала А1, причем ячейка содержит разъем Ш1»; «Показать блоки».

Использование предикатной модели схемно-ориентированных запросов в системах информационной поддержки требует разработки правил построения предложений языка схемно-ориентированных запросов на основе теории формальных грамматик. Использование в запросах естественно-подобного языка, сопряженного с определенной предметной областью, определяет необходимость описывать в этих правилах не только синтаксис предложений, но также и множество смыслов предложений с точки зрения предметной области, т.е. семантику языка.

Заключение

Для повышения гибкости и эффективности способов работы ОП с электрическими схемами при восстановлении РЭА предлагается использовать схемно-ориентированные запросы. Такие запросы предоставляют обслуживающему персоналу возможность использовать естественно-подобный язык для описания целевых условий определяющих в терминах и понятиях предметной области, фрагменты электрических схем, которые необходимо формировать для визуального представления.

Предлагаемая предикатная модель схемно-ориентированных запросов формально основывается на использовании логики предикатов. Языковая структура схемно-ориентированных запросов определяется совокупностью грамматических правил, позволяющих формировать запросы в виде предложений на естественно-подобном языке с использованием терминов и понятий электрических схем. Использование естественного языка в структуре предложений запросов позволяет производить согласование используемых слов по падежам, а также использовать формы множественного/единственного числа.

Использование предлагаемой модели определяет направление развития архитектуры систем информационной поддержки, связанное с использованием концептуальных интерфейсов, обеспечивающих совместное использование речевых, текстовых и схемно-графических технологий при работе обслуживающего персонала с электрическими схемами РЭА.

Использование естественно-подобных языков способствует повышению информационной емкости запросов и, соответственно, сокращению общего числа запросов, которое необходимо формировать обслуживающему персоналу для получения требуемой информации. Наибольший эффект сокращение числа запросов дает в процессе восстановления РЭА, который характеризуются многократностью формирования запросов со стороны обслуживающего персонала и циклическим характером выполняемых операций.

Формализация и общая логика предложенной структуры схемно-ориентированного запроса являются основой для программной реализации соответствующего интерпретатора запросов, как компонента систем информационной поддержки. Внедрение в системы информационной поддержки соответствующих программных средств позволяет повысить уровень автоматизации процессов технической эксплуатации и сократить время восстановления РЭА за счет уменьшения времени на извлечение требуемой технической информации по запросам обслуживающего персонала.

Литература

1. *Анисимов О.В.* Направления совершенствования систем информационной поддержки обслуживающего персонала при технической эксплуатации систем специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2014. Т.6. № 5. С. 44–52.

2. *К. Дж. Дейт.* Введение в системы баз данных. СПб.: Вильямс. 2006. 1328 с.

3. *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.

4. *Колмогоров А.Н, Драгалин А.Г.* Математическая логика. М.: КомКнига, 2006. 240 с.

5. *Анисимов О.В., Приветень А.С., Курчидис В.А.* Структура метода формирования онтологии предметной области технической эксплуатации радиоэлектронной аппаратуры // Наукоемкие технологии в космических исследованиях Земли. – 2014. Т.6. № 3. С. 26–30.

6. *Анисимов О.В., Приветень А.С.* Эффективность информационной поддержки обслуживающего персонала в цикле восстановления радиоэлектронных средств // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 1. С. 26–29.

Для цитирования:

Курчидис В.А., Попов Т.А., Анисимов О.В. Предикатная модель схемно-ориентированных запросов обслуживающего персонала в системах информационной поддержки // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 30–36.

THE PREDICATE MODEL OF SCHEME-ORIENTED QUERIES FOR STAFF IN INFORMATION SUPPORT SYSTEMS

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

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

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

Abstract
One way of raising efficiency in solving problems of complex technical systems operation while using the automation equipment. Existing automation equipment, maintenance personnel do not provide opportunities to build queries to obtain the required information in the form of electrical schemes fragments using concepts and terms within the subject area of this natural language syntax.
The work is dedicated to the development of predicate query models, focused on the use of concepts and terms in the field of the formation of the target conditions by staff to represent the requested schema fragments. Such requests are referred to 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. For the formation of targeted query conditions and concepts in terms of the electrical circuits of electronic equipment is justified use of the first-order predicate logic within the syntax of natural language. The offered formalized structure of the scheme-oriented requests allows coordinating the predicate formulas with the structure of the natural language sentences.
Proposed 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.
The obtained result is appropriate to consider as a methodological basis for constructing conceptual interfaces based on natural-like language systems for service personnel information support in the technical exploitation of electronic equipment. This increases the level of information support automation for service personnel and reducing the solution of applied problems of technical operation of radio-electronic equipment in complex technical systems.

Keywords: information support, technical maintenance, electronic devices, electric scheme, predicate model, scheme-oriented query.

References

1. *Anisimov O.B.* The directions of improvement of systems of information support of the service personnel at technical operation of systems of a special purpose. H&ES Research. 2014. Vol. 6. No. 5. Pp. 44–52. (in Russian).
2. Date. C. Vvedenie v sistemy baz dannykh [An introduction to Database System]. SPb.: Vilyams. 2008. 1328 p. (in Russian).
3. *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).
4. *Kolmogorov A.N., Dragalin A.G.* Matematicheskaya logika [The mathematical logic]. Moscow: ComKniga. 2006. 240 p. (in Russian).
5. *Anisimov O.V., Priveten A.S., Kurchidis V.A.* Structure of the method of forming domain ontology technical operation radio-electronic equipment. H&ES Research. 2014. Vol. 6. No. 3. Pp. 26–30. (in Russian).
6. *Anisimov O.V., Priveten A.S.* Information support of scheme request for the personnel in the recovery cycle of radio-electronic devices. H&ES Research. 2013. Vol. 5. No. 1. Pp. 26–29. (in Russian).

Information about authors:
Kurchidis V.A., Ph.D., professor, professor Automation (and computing devices), Military Space Academy;
Popov O.V., deputy head of Department scientific research, Military Space Academy;
Anisimov O.V., Ph.D., associate professor, docent Automation (and computing devices), Military Space Academy.

For citation:
Kurchidis V.A., Popov O.V., Anisimov O.V. The predicate model of scheme-oriented queries for staff in information support systems. H&ES Research. 2015. Vol. 7. No.3. Pp. 30–36. (in Russian).

КРЫМСКИЙ ТРАНСПОРТНЫЙ ФОРУМ

25-26 июня 2015, г. Алушта, Крым

РЕГИСТРАЦИЯ УЧАСТНИКОВ:

+7 (495) 646-01-51
+7 (812) 448-08-48

www.crimtrans.ru

В ПРОГРАММЕ:

- Развитие транспортной инфраструктуры Крыма и изменение грузопотоков в регионе
- Посещение объектов транспортной инфраструктуры Крыма

www.crimtrans.ru

КЛЮЧЕВЫЕ ТЕМЫ:

- Транспортная инфраструктура Республики Крым: вопросы, решения и пути развития
- Порты Азово-Черноморского бассейна: переориентирование грузопотоков?
- Железнодорожная логистика: инфраструктурные проекты
- Свободная экономическая зона в Крыму: новые возможности

Генеральный интернет-партнёр: IQtrans

Генеральное информационное агентство: ТАСС — Информационное агентство России

Официальный информационный партнёр: РЖД ПАРТНЕР

Эксклюзивный информационный партнёр: Транспорт России

Отраслевой информационный партнёр: ТРАНСПОРТ

Информационная поддержка: T•Comm

Организатор Форума: icf Международные конференции

ЛОГИКО-ПАРАМЕТРИЧЕСКИЙ ПОДХОД К МОДЕЛИРОВАНИЮ ЖИВУЧЕСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ПОДГОТОВКИ И ПУСКА РАКЕТ КОСМИЧЕСКОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ ВОЗНИКНОВЕНИЯ НЕШТАТНОЙ СИТУАЦИИ

Тарасов
Анатолий Геннадьевич,
к.т.н., докторант Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, Atol-77@mail.ru

Дорожко
Игорь Владимирович,
к.т.н., преподаватель кафедры автоматизированных систем подготовки и пуска ракет космического назначения Военно-космической академии имени А.Ф. Можайского г. Санкт-Петербург, Россия, Doroghko-Igor@yandex.ru

Ключевые слова:
автоматизированная система управления, нештатная ситуация, безопасность, логико-графическая модель, робототехнический комплекс.

АННОТАЦИЯ

Постановка проблемы: активное внедрение автоматизированных систем в процессы управления и, соответственно, сокращение эксплуатирующего персонала, с одной стороны, и принципиальная ограниченность привлечения персонала для устранения нештатных ситуаций с позиций безопасности, с другой стороны, требуют решения задачи автоматизации процесса устранения неисправности для обеспечения необходимого уровня оперативности и безопасности технологических процессов в целях повышения эффективности. Целью работы является разработка функциональной модели системы комплексного контроля и обеспечения живучести автоматизированной системы управления, позволяющей оптимизировать управление в случаях возникновения нештатных ситуаций и ликвидации последствий аварий. Результаты: сформулированы этапы анализа технологических процессов в виде логико-параметрического мониторинга состояния элементов системы на основе данных распределённых программно-аппаратных средств (датчики, измерители, резидентные модули и т.д.) и приведен пример ее решения при реализации процесса заправки керосином блока «И» ракеты космического назначения «Союз-2». В качестве модели предлагается логико-графическая модель «дерево функционирования» с учетом изменения состояния объекта при воздействии опасных факторов. Сущность предложенной функциональной модели системы комплексного контроля и обеспечения живучести состоит в оперативной идентификации нештатных ситуаций и синтезе робототехнических систем и комплексов для их устранения. Новизна подхода состоит в том, что при управлении технологическими процессами концепция «приемлемого» риска реализуется для всех возможных состояний объекта, а именно безопасного, опасного, аварийного. Практическая значимость: сформулирована общая постановка задачи синтеза системы контроля и обеспечения живучести с использованием робототехнических систем и комплексов. Приводится пример модели процесса заправки керосином блока «И» ракеты космического назначения «Союз-2». Для рассмотренного примера определены интегральные риски реализации нештатных ситуаций с использованием аппарата байесовских сетей доверия.

Введение

Анализ функционирования современных автоматизированных систем управления технологическими процессами (АСУ ТП) показывает, что в процессе проектирования не предусматривается их участие в устранении нештатных (НшС) и аварийных ситуаций, а закладываются лишь различные блокировки с целью предотвращения эскалации данных ситуаций. Устранение нештатных и аварийных ситуаций обеспечивается силами эксплуатирующего персонала (ЭП) без участия либо с минимальным участием АСУ ТП в целях обеспечения необходимой безопасности. Таким образом, возникает противоречие между обеспечением безопасности в штатном и нештатном режимах работы АСУ, поскольку в первом случае уменьшается количество ЭП, а во втором – увеличивается.

Алгоритм управления безопасностью подготовки ракеты космического назначения (РКН) в нештатных ситуациях базируется на принципе своевременного обнаружения причин, оперативного предотвращения перехода штатных ситуаций в нештатные или аварийные; а также выявления факторов риска, прогнозирования основных показателей «живучести» объекта в течение заданного периода его эксплуатации как основы обеспечения гарантированной безопасности в динамике функционирования, устранения причин возможного перехода работоспособного состояния объекта в неработоспособное состояние на основе системного анализа многофакторных рисков нештатных ситуаций.

Функциональная модель системы контроля и обеспечения живучести автоматизированной системы подготовки и пуска ракеты космического назначения

В процессе разработки системы управления объектом необходимо учесть все возможные факторы при реализации технологического процесса с целью минимизации возможного ущерба. Практика показывает, что крупные аварии, как правило, характеризуются комбинацией случайных событий, возникающих с различной частотой на разных стадиях возникновения и развития аварии (отказы оборудования, ошибки ЭП, нерасчетные внешние воздействия, разрушение, выброс, пролив вещества, рассеяние веществ, воспламенение, взрыв и т.д.). Поэтому для выявления причинно-следственных связей между этими событиями предлагается на основе логико-графических методов анализа «деревьев отказов» и «деревьев событий» разрабатывать для объекта управления логико-графическую модель «дерево функционирования» с учетом изменения состояния объекта при воздействии ОФ.

Для построения «дерева функционирования» каждый элемент системы необходимо рассматривать как потенциальный источник исходного события аварии. Затем определяются последствия отказов каждого элемента системы, ошибок ЭП, а также совместные отказы элементов и ошибки ЭП (инициирующие события). На следующем шаге определяются предельные значения параметров системы, выход за которые приводит

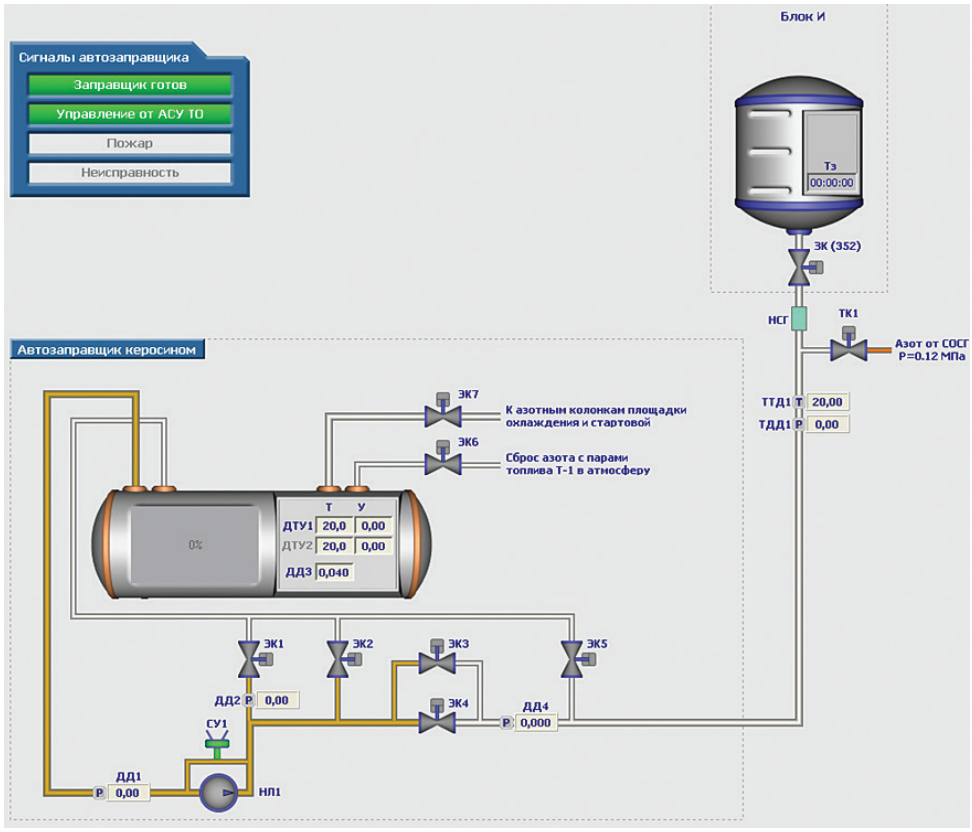


Рис. 1. Функциональная схема системы заправки керосином блока «И» РКН «Союз-2»

к возникновению аварийных ситуаций (последствия инициирующих событий). Далее рассматриваются возможные варианты развития аварийных ситуаций (эскалация). По результатам определения инициирующих событий и их последствий разрабатывается решение о применимости сценариев защиты с целью недопущения возникновения аварийных ситуаций и их дальнейшей эскалации. Затем разрабатываются требования к средствам защиты и восстановления системы, ликвидации последствий аварий в случае их возникновения. Дополнительно могут быть определены ограничения от требуемого качества процесса функционирования с целью достижения результата для обеспечения необходимых требований живучести.

Модель «дерево функционирования» для системы заправки керосином блока «И» (СЗК И) РКН «Союз-2», функциональная схема которой представлена на рис.1, в режиме заправки бака может быть представлена следующим образом (рис. 2).

Для построения «дерева функционирования» из анализа особенностей конструкции агрегатов и объекта системы заправки были определены следующие предельные (критические) значения давления и температуры в баках и магистралях:

– давление в автозаправщике: 10 кПа ≤ ДД3 ≤ 50 кПа;

– давление в магистралях:

ДД2 ≤ 980 кПа и 100 кПа ≤ ДД4 ≤ 650 кПа;

– температура в магистрали: 15 оС ≤ ТТД1 ≤ 35 оС.

Выход данных параметров за указанные пределы характеризует наступление опасной операции, причем показания приборов должны быть установившимся, для чего устанавливаются временные интервалы, в течение которых должны фиксироваться критические значения параметров. Установившиеся критические параметры характеризуют наступление отказов систем и агрегатов, а кратковременные выходы параметров за предельные значения свидетельствуют о сбоях в работе систем и агрегатов.

Переходы между различными состояниями представляют собой логические и параметрические критерии возможности возникновения аварийных ситуаций и состоят из инициирующих событий, последствий и эскалации аварийных ситуаций, которые для системы заправки керосином представлены на рис. 3.

Инициирующее событие (причина) Y_{12i}	Последствия Y_{23i}	Эскалация Y_{34i}	Ущерб
Отказ ЭК7 (открыт), ЭК4 (БР) и ЭК3 (МР) (закрыт)	Превышение давления ДД3 > 50кПа в теч. 5 сек.	Взрыв автозаправщика	Загрязнение окружающей среды, пожар
Отказ ЭК4 (БР), ЭК2 и ЭК3 (МР) (закрыт), насос НЛ1 включен	Превышение давления ДД2 > 980кПа или ДД4> 650кПа в теч.10с	Взрыв заправочных магистралей	Загрязнение окружающей среды, пожар
Отказ ЭК7 (закрыт), ЭК6 (открыт), насос НЛ1 включен	Понижение давления ДД3 < 10кПа в теч. 5с.	Деформация автозаправщика	Загрязнение окружающей среды, пожар
Отказ ЗК (открыт), СИУЗ, насос НЛ1 включен	Достижение аварийного уровня заправки	Взрыв блока «И»	Загрязнение окружающей среды, пожар
Отказ ЗК (закрыт), насос НЛ1 включен	Понижение давления ДД4 < 30кПа в теч. 10с	Утечка керосина через стыковочные разъемы	Загрязнение окружающей среды, пожар

Рис. 3. Переходы между состояния и их условия для системы заправки керосином

Анализ причинно-следственных связей необходим для выработки защитных мер (блокировок) с целью парирования отказов (Y21i) и предотвращения эскалации опасной ситуации (Y32i) в случае ее возникновения. Защитные меры могут быть реализованы в автоматизированной системе управления технологическими процессами, противоаварийной автоматической защите (ПАЗ) (предохранительные клапаны, мембраны), физических барьерах защиты (обвалование, огнезащитные покрытия, взрывоустойчивое исполнение и т.п.).

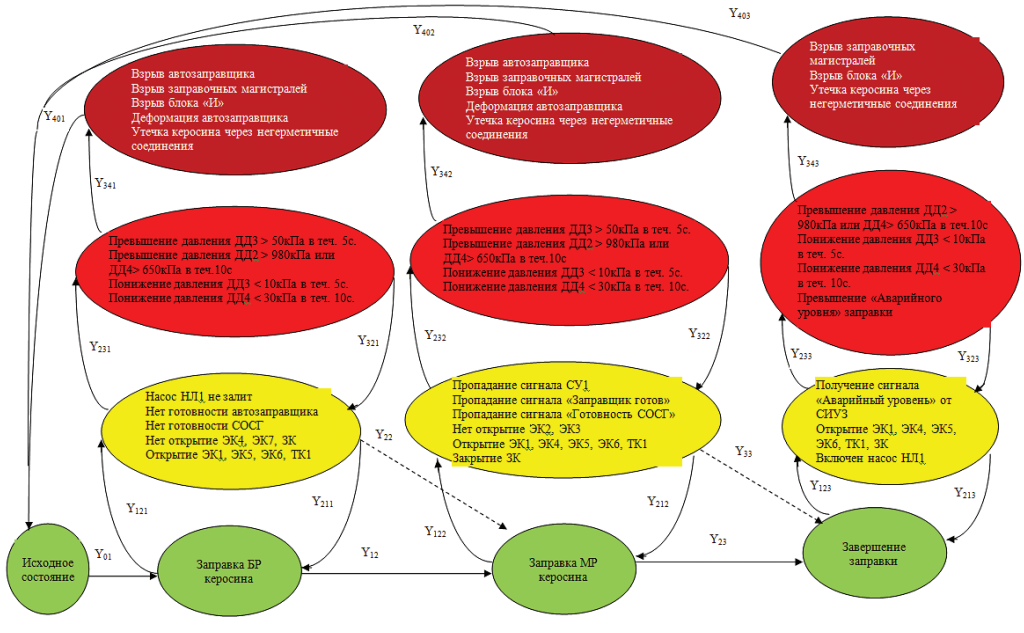


Рис. 2. «Дерево функционирования» системы заправки керосином

Из анализа представленных опасных событий следует, что в качестве защитных мер необходимо отключать насос НЛ1 и открывать/закрывать клапаны в случае фиксации последствий отказов оборудования.

Переходы Y22 и Y33 характеризуют свойство живучести [1] СЗК И, которая заключается в возможности сохранять и восстанавливать способность к выполнению основных функций в заданном объеме при изменении структуры системы и (или) алгоритмов и условий ее функционирования вследствие непредусмотренных регламентом штатной работы опасных факторов. В качестве опасных факторов могут выступать отказы элементов системы, в том числе ошибки обслуживающего персонала, входящего в состав системы (изменение свойств системы), а также изменение условий функционирования системы (изменение свойств среды).

Переходы Y401, Y402 и Y403 определяют способность СЗК И к ликвидации последствий аварий и восстановлению исходного состояния агрегатов и оборудования.

Для определения интегральных рисков реализации нештатных ситуаций в работе использован аппарат байесовских сетей доверия. Разработанная в среде GeNIe модель СЗК И (рис. 4) учитывает влияние всех органов управления (ЭК1-ЭК7, ЗК, ТК1, насос НЛ1) на состояние системы (безопасное, опасное, аварийное).

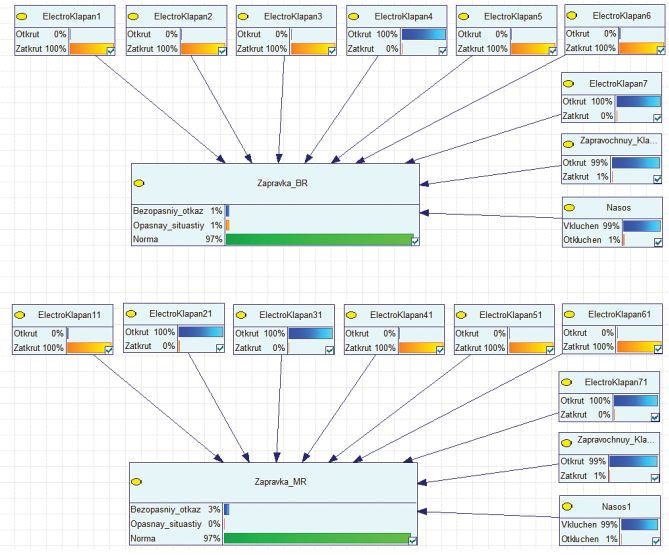


Рис. 4. Модель СЗК И в среде GeNIe

Разработка данной модели представляет собой трудоемкую процедуру, даже для относительно несложной системы СЗК И, органы управления которой могут находиться в двух состояниях (клапаны – открыт/закрыт, насос – включен/выключен), необходимо рассмотреть 210=1024 возможных состояний. С другой стороны, когда решаются вопросы безопасности эксплуатации, которые затрагивают здоровье и жизни ЭП, сохранение окружающей среды, вопросы трудоемкости уходят на второй план. Детальный перебор всех возможных состояний объекта управления позволяет исключить возникновение непредусмотренных по причине отказов оборудования и ошибок оператора ситуаций, что позволяет повысить достоверность защитных мер. Вследствие этого «дерево функционирования» целесообразно разрабатывать на этапе проектирования или модернизации АСУ ТП для выработки необходимых защитных мер с целью обеспечения безопасности ЭП и живучести АСУ.

Для эксплуатирующей организации «дерево функционирования» будет полезно при разработке организационных мер (инструкции, приказы и т.п.) с целью обеспечения безопасности ЭП при возникновении НшС, а также для анализа достоверности и полноты логико-параметрических критериев возможности возникновения аварийных ситуаций и достаточности средств для парирования отказов, предотвращения эскалации опасной ситуации, обеспечения живучести и восстановления исходного состояния в случае возникновения НшС, заложенных в процессе проектирования или модернизации.

Анализ раздела «ДЕЙСТВИЯ ОПЕРАТОРА ПРИ НЕШТАТНЫХ И АВАРИЙНЫХ СИТУАЦИЯХ» руководства оператора автоматизированного рабочего места СЗК И показал, что в документации отсутствуют указания оператору в режиме заправка на случай открытия клапанов ЭК5 и ЭК6, а также при выходе значения температуры в магистрали 15oC ≤ ТТД1 ≤ 35oC за предельные значения. Данные результаты подтверждают актуальность исследований.

Применение защитных мер не обеспечивает полного исключения возможности возникновения аварийной ситуации, в связи с чем при проектировании АСУ ТП необходимо разрабатывать средства ликвидации последствий аварий и восстановления объектов эксплуатации. Таким образом, для обеспечения необходимой безопасности ЭП АСУ ТП необходимо разрабатывать средства аварийной блокировки, ликвидации последствий аварий и восстановления, которые целесообразно выделить в систему контроля и обеспечения живучести (СКОЖ). Учитывая опасные факторы, в условиях которых необходимо проводить восстановление объектов и ликвидацию последствий аварий в качестве средств СКОЖ целесообразно применять автоматизированные и робототехнические системы и комплексы [2], так как привлечение ЭП с позиций безопасности не приемлемо.

Использование моделей динамической обработки данных логико-параметрического мониторинга состояния элементов системы на основе данных распределённых программно-аппаратных средств (датчики, измерители, резидентные модули и т.д.) и расчёт значений интегрального риска реализации НшС является базисом для синтеза системы комплексного контроля и обеспечения живучести интегрированных АСУ. Функциональная модель системы комплексного контроля и обеспечения живучести АСУ представлена на рис. 5.

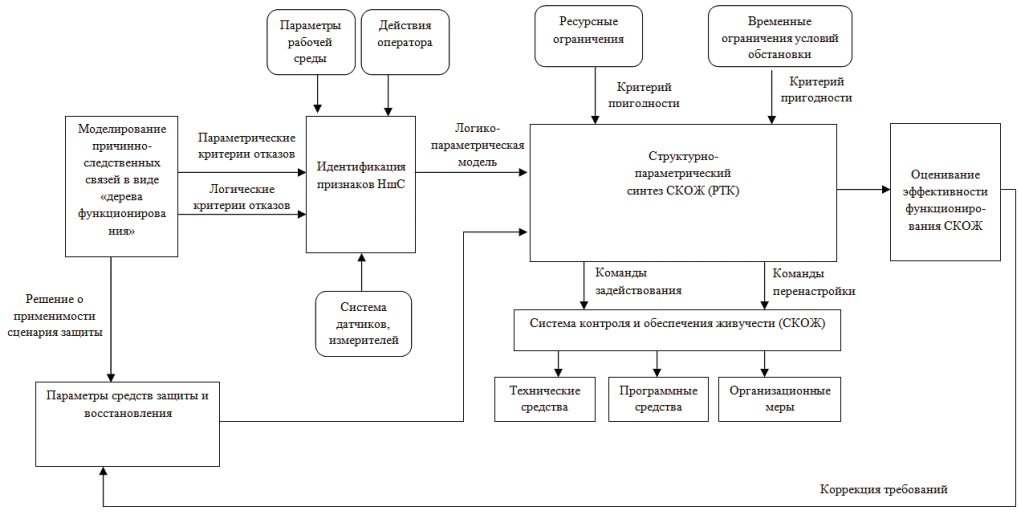


Рис. 5. Функциональная модель системы контроля и обеспечения живучести АСУ

Внедрение робототехнических систем и комплексов в структуру АСУ ТП образует дополнительный уровень [3], а структурно-параметрический синтез средств обеспечения живучести, их оптимизация и оценивание эффективности будут реализовываться на верхнем уровне АСУ. Под роботом будем понимать автономное техническое устройство (средство), заменяющее человека при выполнении целевых задач путем автоматического воспроизведения в той или иной степени его разумного поведения в изменяющихся условиях функционирования за счет наличия информационно-измерительной (сенсорной), управляющей, исполнительной (двигательной) и коммуникационной (связной) систем, а также активного взаимодействия с внешней средой.

Робототехническая система (РТС) подготовки и пуска (ПП) РКН – система, состоящая из роботов, предназначенная для автоматического или автоматизированного (интерактивного) выполнения задач в процессе подготовки и пуска РКН.

Робототехнический комплекс (РТК) ПП РКН – управляемая и контролируемая подсистемой управления (оператором, их группой и т.д.) автоматизированная система с динамично формируемыми и изменяющимися в соответствии с решаемыми задачами и условиями обстановки составом и связями между входящими в него РТС и роботами ПП РКН, предназначенная для выполнения тяжелых и опасных для человека операций на ракетно-космическом комплексе (РКК) в ходе ПП РКН в обычных условиях обстановки, при возникновении нештатных ситуаций (НшС), аварий и катастроф, а также ликвидации их последствий.

В соответствии с веденным понятием структурно-функциональная схема робота будет выглядеть следующим образом (рис. 6).

Модели применения РТК ПП РКН могут быть внешними и внутренними. Внешняя модель применения РТК ПП РКН описывает его функционирование как кибернетической системы, состоящей из трех подсистем (рис. 7):

1. Системы и агрегаты технологического оборудования (ТО) и технических систем (ТхС) стартового комплекса (СК) и РКН.

2. Автоматизированная система подготовки и пуска (АСПП).

3. РТК ПП РКН.

Если обозначить через

Э – модель показателя эффективности применения РТК ПП РКН;

W(t) – модель внешних воздействий на объекты ракетно-космического комплекса (РКК) (на рис. 7 обозначены «1»);

U(t) – модель воздействий управляющей системы на объекты РКК (на рис. 7 обозначены «2»);

Z(t) – модель воздействий РТК ПП РКН на ТО и ТхС СК и РКН (на рис. 7 обозначены «3»);

Y(t) – модель ответных реакций РТК ПП РКН, ТО и ТхС СК и РКН на указанные воздействия (на рис. 7 обозначены «4»), то символьное представление общей

$$U(t) = F(Z(t), W(t), Э);$$
$$Z(t) = f(U(t), W(t));$$
$$Y(t) = \varphi(Z(t)).$$

модели применения РТК ПП РКН будет задаваться с помощью соотношений

Внутренняя модель применения РТК ПП РКН как составные части включает в себя модели роботов и РТС ПП КА, объединенные функциональными связями друг с другом. Ее символьное представление аналогично приведенному для внешней модели.

Предлагаемый подход к моделированию применения РТК ПП РКН предопределяет два вида показателей

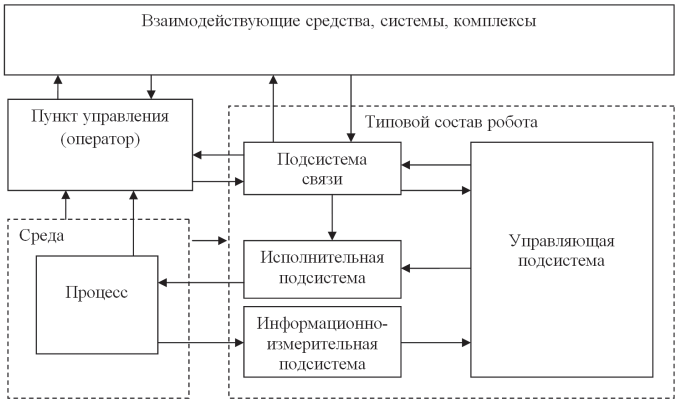


Рис. 6. Структурно-функциональная схема робота

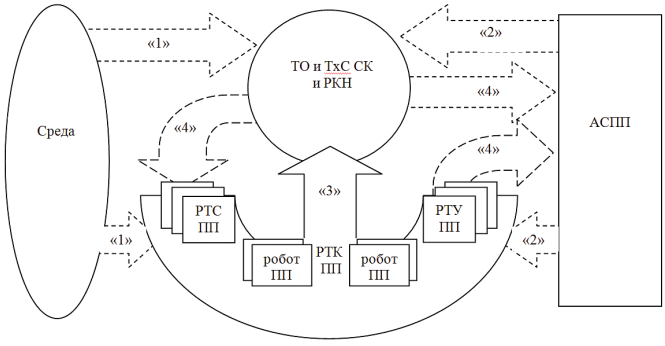


Рис. 7. Графическое представление внешней модели применения РТК ПП РКН

эффективности (ПЭ): внешние (основные) и внутренние. Оценивание эффективности применения РТК ПП РКН основывается на принципе выявления соответствующего как внешнего, так и внутреннего ПЭ в строгом соответствии с целью применения РТК. При этом он должен описываться какой-либо вероятностной характеристикой в связи с тем, что ущерб, который может быть причинен в результате НшС, аварии или катастрофы является случайной величиной, а на функционирование РТК ПП РКН в целом, а также роботов и РТС ПП воздействует множество случайных факторов.

В связи с основным предназначением РТК ПП РКН является выполнение операций на РКК в экстремальных условиях и ликвидация последствий Ншс, аварии или катастрофы, то целью его применения является предотвращение или понижение ущерба от их проявлений. В зависимости от выполняемой РТК ПП РКН задачи в качестве предотвращенного ущерба могут выступать сохраненные в результате его применения объекты РКК, личный состав и техника, время, на которое сокращена подготовка РКН к запуску при возникновении НшС и ряд других.

При проектировании РТК необходимо учитывать опыт разработок зарубежных специалистов [4-6], которые опережают нас в настоящее время в области практических разработок и применения РТК.

Заключение

Предлагаемая в статье логико-параметрическая модель «дерево функционирования» сложной технической системы позволяет повысить достоверность оценок интегральных рисков реализации нештатных ситуаций за счет максимального учета состояний агрегатов и оборудования системы. «Дерево функционирования» с учетом трудоемкости процедуры построения целесообразно разрабатывать на этапе проектирования систем. Новизна подхода состоит в том, что при управлении технологическими процессами концепция «приемлемого» риска реализуется для всех возможных состояний объекта, а именно безопасного, опасного, аварийного.

Литература

1. *Черкесов Г. Н.* Методы и модели оценки живучести сложных систем. М.: Знание. 1987. 32 с.

2. *Тарасов А. Г.* Перспективы создания робототехнических средств и комплексов подготовки и пуска ракет космического назначения // Наукоемкие технологии в космических исследованиях Земли. 2014. Т. 6. № 6. С. 72–75.

3. *Тарасов А. Г.* Системная согласованность управления безопасностью и живучестью в автоматизированной системе подготовки и пуска ракет космического назначения // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 1. С. 42–47.

4. *Sturges, Robert H., Jr.* Practical Field Robotics: a System Approach. John Wiley & Sons, Ltd. Published. 2015. 213 p.

5. *Kanabe C., Hopkins M. and Hong D.* Team CHARLI: RoboCup 2012 Humanoid AdultSize League Winner, in RoboCup 2012, Lecture Notes in Computer Science (eds X. Chen, P. Stone, L.E. Sucar and T. Van der Zant), Springer. 2012. Pp. 59–64.

6. *Benedettell D.* Creating Cool MINDSTORMS NXT robots. 2008. 596 p.

Для цитирования:

Тарасов А.Г., Дорожко И.В. Логико-параметрический подход к моделированию живучести автоматизированных систем подготовки и пуска ракет космического назначения в условиях возникновения нештатной ситуации // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 38–44.

LOGICALLY-PARAMETRIC APPROACH TO SURVIVABILITY SIMULATION OF AUTOMATED SYSTEMS PREPARATION AND LAUNCHING OF SPACE ROCKETS IN CASE OF EMERGENCY

Tarasov Anatoly Gennadevich, St. Petersburg, Russian, Atol-77@mail.ru

Doroghko Igor Vladimirovich, St. Petersburg, Russian, Doroghko-Igor@yandex.ru

Abstract

Statement of the problem - the active introduction of automated systems management processes and the limited involvement of staff to address emergency situations from the standpoint of safety. This requires solving the problem of automating the process of troubleshooting to ensure the necessary level of efficiency and safety of production processes in order to improve efficiency. Objective: development of functional model in integrated control system and ensure the survivability of the automated control system to optimize control in cases of emergency situations and liquidation of consequences of accidents. Results: stages formulated analysis in the form of logic-parametric monitoring the status of system components based on distributed software and hardware (sensors, meters, resident modules, etc.) and is an example of the implementation of its decision of kerosene refueling unit «I «space rocket» Soyuz-2». Proposed logical-graphic model «tree operation» with the state of the object changes when exposed to dangerous factors. Essence of the proposed functional model is the rapid identification of emergency situations, and synthesis of robotic systems and complexes for their elimination. Novelty of this approach is that during workflow control concept «acceptable risk» realizes for all possible object conditions: safety, unsafe, dangerous. Practical significance: a general statement of control system synthesis problem and survivability provision using robotic systems and complexes. An example of a process model kerosene refueling unit «I» space rocket «Soyuz-2». For example considered integral identified risks of the emergency situations, using bayesian network trust-model.

Keywords: computer-based system, emergencies, safety, logic-graphic model, robotics complex.

References

1. *Cherkesov G.N.* Metody i modeli otsenki zhivuchesti slozhnykh sistem [Metody and model of an assessment of survivability of difficult systems]. Moscow: Znanie. 1987. 32 p. (In Russian).
2. *Tarasov A.G.* Prospects of creation of robotic tools and systems training and startup space rockets. H&ES Research. 2014. Vol. 6. No. 6. Pp. 72–75. (In Russian).
3. *Tarasov A.G.* The system consistency management safety and survivability in the automated system preparation and launch of space rocket // H&ES Research. 2015. Vol. 7. No. 1. Pp. 42–47. (In Russian).
4. *Sturges, Robert H,* Jr. Practical Field Robotics: a System Approach. John Wiley & Sons, Ltd. Published. 2015. 213 p.
5. *Kanabe C., Hopkins M. and Hong D.* Team CHARLI: RoboCup 2012 Humanoid AdultSize League Winner, in RoboCup 2012, Lecture Notes in Computer Science (eds X. Chen, P. Stone, L.E. Sucar and T. Van der Zant), Springer, 2012. Pp. 59–64.
6. *Benedettelli D.* Creating Cool MINDSTORMS NXT robots. 2008. 596 p.

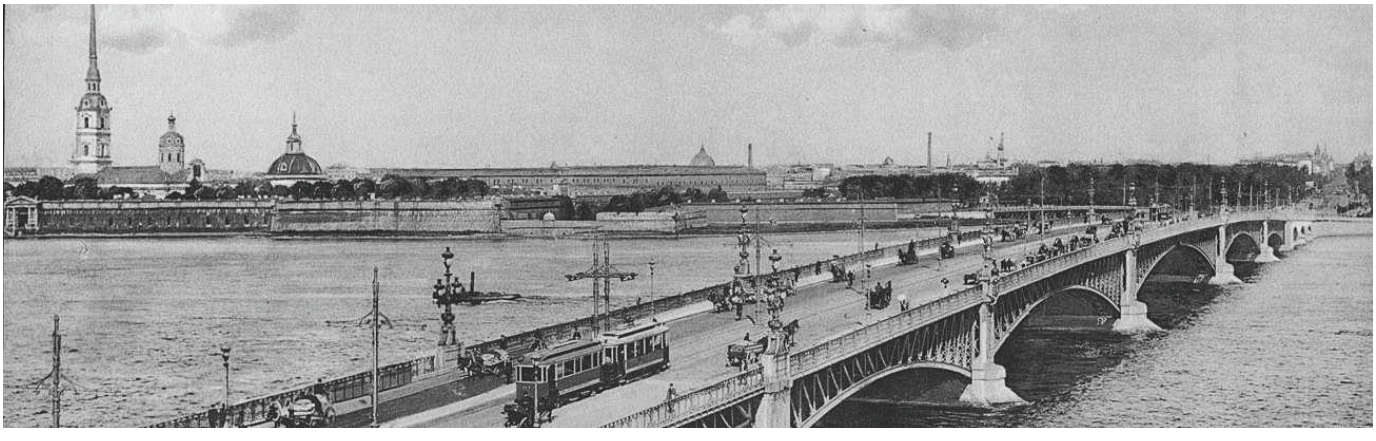
Information about authors:

Tarasov A.G., Ph.D., doctoral student, Military Space Academy;

Doroghko I.V., lecturer in Department of Automated systems preparation and launching of space rockets, Military Space Academy.

For citation:

Tarasov A.G., Kurchidis V.A. Logically-parametric approach to survivability simulation of automated systems preparation and launching of space rockets in case of emergency. H&ES Research. 2015. Vol. 7. No. 3. Pp. 38–44. (in Russian).



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.

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

ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ: ОСНОВНЫЕ УГРОЗЫ, СПОСОБЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ СЕТЕЙ

Буренин
Андрей Николаевич,
к.т.н., доцент, главный специалист ОАО «Научно-исследовательский институт «Рубин», г. Санкт-Петербург, Россия, konferencia_asu_vka@mail.ru

Легков
Константин Евгеньевич,
к.т.н., заместитель начальника кафедры технологий и средств технического обеспечения и эксплуатации автоматизированных систем управления Военно-космической академии имени А.Ф. Можайского, г. Санкт-Петербург, Россия, constl@mail.ru

Ключевые слова:
инфокоммуникационные системы, телекоммуникационные и информационные услуги, разрушающие и информационные воздействия, проблемы обеспечения безопасности, угрозы безопасности.

АННОТАЦИЯ

В настоящее время гарантированное обеспечение требуемых телекоммуникационных и информационных услуг должностным лицам органов управления для нужд обороны, безопасности и обеспечения правопорядка связано с вопросами комплексного решения сложных задач организации, проектирования, эксплуатации, обеспечения безопасности функционирования и управления инфокоммуникационными системами и сетями специального назначения, развернутыми в рамках соответствующих ведомственных и межведомственных систем связи.

Это предполагает решение достаточно сложных технических и теоретических задач, в которых были бы получены предложения и рекомендации по организации современных инфокоммуникационных систем и сетей специального назначения, функционирующих в условиях целого комплекса разрушающих и информационных воздействий.

Происходящие в последние годы процессы интенсивной интеграции различного рода сетей передачи данных, речи, видео со средствами и приложениями пользователей, а также необходимость поддержки средств мультимедиа и информационных технологий на узлах ведомственных центров автоматизированных и информационных систем, ставят принципиально новые задачи по созданию, эксплуатации инфокоммуникационных систем и сетей специального назначения, а также по организации эффективного управления этими сетями. При этом практически отсутствуют работы, в которых бы рассматривались проблемы организации, создания, эксплуатации и управления современными инфокоммуникационными системами и сетями вообще и специального назначения, в частности.

При решении задач организации управления современной инфокоммуникационной сетью специального назначения необходимо учитывать требования по обеспечению безопасности, так как существует достаточно большая вероятность преднамеренного неправомерного вторжение в сеть из внешней среды, которое выполняется как с целью несанкционированного использования ресурсов (для хищения информации), так и с целью нарушения её работоспособности. Поэтому, без использования соответствующих средств защиты информации и реализации соответствующих механизмов защиты функционирование инфокоммуникационной системы специального назначения невозможно.

В силу выше изложенных соображений рассмотрение и исследование вопросов безопасности современных инфокоммуникационных систем специального назначения является весьма актуальным.

Основные проблемы обеспечения безопасности функционирования инфокоммуникационных систем и сетей специального назначения

С учетом требований по обеспечению безопасности инфокоммуникационная система специального назначения (ИКС СН) – технологическая система, предназначенная для предоставления санкционированных информационных и телекоммуникационных услуг пользователям министерств и ведомств, передачи по защищенным линиям связи конфиденциальной информации пользователей и служб (информационных и телекоммуникационных), доступ к которым осуществляется с использованием средств вычислительной техники.

В настоящее время термин «инфокоммуникационная система и сеть» специального назначения обозначает сеть обмена разного вида сообщениями, интегрирующую в себе информационную вычислительную сеть ведомственных или корпоративных органов управления и телекоммуникационную сеть. При этом сама телекоммуникационная сеть все более и более превращается в совокупность защищенных специализированных сетей обмена данными, техническую основу которых составляют защищенные линии связи и специализированные средства, управляющие обработкой информации, предназначенной для пересылки по сети и предоставления информационных услуг и услуг электросвязи. Элементами инфокоммуникационных систем специального назначения является специализированная защищенная инфокоммуникационная сеть и система управления ею, построенная на принципах создания автоматизированных систем управления (АСУ) сложными системами.

Инфокоммуникационные системы и сети специального назначения, используемые для нужд управления государством, обеспечения его обороны, безопасности и охраны правопорядка, являются объектом повышенного внимания средств противодействия и подавления противника (как информационных, так и разрушающих).

Безопасность инфокоммуникационной системы специального назначения характеризует ее способность противодействовать определенному множеству угроз, преднамеренных или непреднамеренных дестабилизирующих воздействий на входящие в состав ИКС СН средства (коммутационной и серверное оборудование, на программный продукт), линии и каналы связи, цифровые тракты и технологические процессы (протоколы), которые могут привести к ухудшению качества услуг, предоставляемых пользователям министерств и ведомств.

С точки зрения анализа проблем обеспечения безопасности функционирования ИКС СН, следует различать информационную безопасность ресурсов, имеющихся в сети, и безопасность функционирования самой ИКС СН [1, 2].

Информационная безопасность ресурсов. Ресурсы (активы) – это объекты, являющиеся принадлежностью государства, ведомства, корпорации, органа управления или иного субъекта права и, в той или иной мере, подлежащие защите.

По существующим взглядам к информационным ресурсам ИКС СН относятся:

– сведения об пользователях министерств и ведомств базы данных;

– информация управления;

– данные, содержащие информацию пользователей (обеспечение доступности и целостности);

– программное обеспечение технических средств связи, средств и систем управления сетями ИКС СН;

– сведения о прохождении, параметрах, загрузке (использовании) линий и каналов связи сетей в составе ИКС СН;

– обобщенные сведения о местах дислокации узлов ИКС СН, установленном сетевом и серверном оборудовании;

– сведения, раскрывающие структуру используемых механизмов обеспечения безопасности сети электросвязи.

В качестве ресурсов, подлежащих защите в ИКС СН, следует определить важные средства и данные для обеспечения эффективного информационного обмена в конкретной ведомственной или корпоративной системе управления. При этом [3, 4] следует разделять аппаратные, аппаратно-программные, информационные ресурсы и персонал (рис.1).

Рис.1. Ресурсы, подлежащие защите в ИКС СН

Аппаратные (аппаратно-программные) ресурсы включают телекоммуникационные и серверные средства, средства управления и средства обеспечения безопасности.

Информационные ресурсы включают данные, хранящиеся в ИКС СН и её элементах, данные, циркулирующие в системах обмена данными ИКС СН и данные по средствам обеспечения безопасности.

Персонал является важнейшим ресурсом ИКС СН, подлежащим защите и контролю.

Под информационной безопасностью ИКС СН понимается состояние защищенности ее информационных ресурсов, то есть способности противостоять различным воздействиям на них.

Наличие возможности воздействия на защищаемые информационные ресурсы ИКС СН, способного прямо или косвенно нанести ущерб информационной безопасности, является угрозой безопасности ИКС СН.

Реализация угрозы возможна при наличии уязвимости ИКС СН – присущему автоматизированной системе и/или персоналу свойству, которое может привести к реализации угрозы.

Для обеспечения информационной безопасности ресурсов ИКС СН необходима координация функционирования значительного числа средств и способов защиты различного назначения, в той или иной мере компенсирующих наличие уязвимостей.

В отличие от информационной безопасности ресурсов, описывающей их состояние, условия и возможности воздействия нарушителей на локальные объекты ИКС СН и её элементы, сетевая безопасность характеризует свойство сети в целом обеспечивать безопасное функционирование всей ведомственной системы управления, являющейся «заказчиком» для ИКС СН.

Основными особенностями обеспечения сетевой безопасности являются необходимость её контроля в масштабе близком к масштабу реального времени, рассредоточение объектов контроля в пространстве, часто на значительных расстояниях, а также централизация системы управления сетевой безопасностью.

В то время как безопасность ресурсов ИКС СН, в значительной мере, может быть обеспечена локальными средствами, сетевая безопасность предполагает обязательное использование специальной системы управления безопасностью, замыкающей на себя объекты и линии коммуникаций всей сети.

Основными задачами сетевой безопасности являются [4]:

– реализация актуальной политики безопасности данной сети на основе выявления угроз, уязвимостей, анализа рисков и мониторинга функционирования сети;

– управление конфигурацией средств и объектов доступа к информационным и телекоммуникационным ресурсам и разграничением доступа пользователей в соответствие с установленными полномочиями;

– управление средствами криптографической защиты;

– управление средствами протоколирования событий безопасности;

– проведение плановых и событийных аудитов ресурсов и средств обеспечения безопасности ИКС СН;

– мониторинг безопасности функционирования ИКС СН (включая обнаружение вторжений).

При решении различных задач обеспечения информационной безопасности используются понятия модели ИКС СН, модели атак, модели нарушителя, а также общей схемы атак, подробно рассмотренные в предыдущих статьях авторов [5].

На основе общей схемы атак производится анализ защищенности ИКС СН, а также определяются «узкие» места сети, на основе чего вырабатываются рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности.

Объекты общей схемы атак подразделяются на базовые объекты и составные, причем вершины графа задаются с использованием базовых объектов, а для формирования различных последовательностей действий нарушителя базовые объекты связываются в общей схеме атак с помощью линий. К базовым объектам общей схемы атак на ИКС СН относятся объекты, принадлежащие к таким типам как АРМ, сервер, коммутатор, маршрутизатор и «атакующее действие». Множество объектов, принадлежащих множеству «атакующие действия» состоит из всех различимых элементарных действий нарушителя.

Атакующие действия разделяются на следующие классы:

– действия по получению информации о ИКС СН и ее элементах, т.е. разведывательные действия;

– подготовительные действия (в рамках уже имеющихся у нарушителя полномочий), служащие для создания условий реализации атакующих действий последующих классов;

– действия, направленные на нарушение конфиденциальности;

– действия, направленные на нарушение целостности;

– действия, направленные на нарушение доступности;

– действия, приводящие к получению противником прав локального пользователя;

– действия, приводящие к получению противником прав администратора.

В целом атакующие действия целесообразно разделить также на две большие группы [6 – 10]:

– действия, использующие различные уязвимости программного и аппаратного обеспечения, например, используются уязвимости в сервисе ОС семейства Linux, позволяющие нарушителю получить права администратора на атакуемом элементе ИКС СН;

– действия легитимного пользователя сети (в том числе действия по использованию утилит получения информации об элементах мультисервисной сети, такие как «удаление файла в записи об этом элементе», «остановка сервиса такой-то службы» и т.п.).

К составным объектам общей схемы атак относятся объекты типов «трасса», «угроза» и «общая схема», при этом под трассой атаки понимается совокупность связанных вершин общего графа атак (АРМ, серверов, коммутаторов, маршрутизаторов и атакующих действий), первый элемент трассы – соответствует первоначальному положению нарушителя, а последний не имеет исходящих дуг. В такой трактовке под угрозой

понимается множество различных трасс атак, имеющих одинаковые начальную и конечную вершины.

Разделение атакующих действий по заданным выше классам соответствует классификации угроз в соответствии с известными типами:

– основные угрозы – угрозы нарушения конфиденциальности, целостности, доступности;

– дополнительные угрозы – угрозы получения информации о мультисервисной сети связи (АРМ, серверах, коммутаторах, маршрутизаторах), угрозы получения нарушителем прав локального пользователя или прав администратора.

Однако обычно при успешной реализации нарушителем разведывательных действий в ИКС СН не происходит нарушения ни конфиденциальности, ни целостности, ни доступности информационных ресурсов сети.

Основные угрозы безопасности ИКС СН и типовые информационные воздействия

С точки зрения государства безопасность представляет собой состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз [1, 2].

Согласно положениям Доктрины информационной безопасности России информационная безопасность представляет собой состояние защищенности информационной среды общества от внутренних и внешних угроз, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Термин «безопасность информации» определяет состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

В качестве угроз безопасности ИКС СН рассматриваются потенциально или реально существующие воздействия, которые могут привести (приводят) к некоторому «ущербу».

В общем виде ущербом для ИКС СН может быть:

– «ознакомление» – случайные или намеренные действия, приводящие к изменению состояния информации по отношению к субъекту, не имеющему непосредственного отношения к данной информации;

– «искажение» – противоправные действия, приводящие к значительному или полному разрушению информационных ресурсов»;

– «разрушение» – противоправное действие, приводящее к изменению или разрушению информации.

Эти угрозы, в первую очередь, влияют на безопасность «информационной» составляющей ИКС СН. Для «телекоммуникационной» составляющей ИКС СН, помимо указанных угроз, существуют угрозы создания условий отказа функционирования (в том числе преднамеренного) и подмены источника передачи.

В связи с этим, в качестве цели защиты целесообразно сформулировать требования обеспечения конфиденциальности, целостности и доступности информационной среды функционирования ИКС СН.

Конфиденциальность: свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

Целостность: свойство сохранять правильность и полноту ресурсов (активов).

Доступность: свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного индивидуума, логического объекта или процесса.

До настоящего времени для общей характеристики угроз безопасности автоматизированных систем использовали понятия «несанкционированный доступ – НСД», «побочные электромагнитные излучения и наводки – ПЭМИН», а также «технические каналы утечки информации – ТКУИ».

Для характеристики возможных воздействий в настоящее время, помимо известных терминов – НСД и ПЭМИН, используют также термины «компьютерная атака» и «программно-аппаратное воздействие».

Термин «компьютерная атака» определяет целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения сетевой безопасности и/или безопасности информации в этих системах и сетях.

Термин «программно-аппаратное воздействие» в семантическом плане является более широким и, помимо целенаправленного воздействия, определяет также случайные и неквалифицированные воздействия на указанные средства, комплексы, сети и системы.

Следует подчеркнуть, что значительную часть угроз, определяемых в качестве НСД к АС и НСД к информации в ИКС СН, в настоящее время целесообразно включать в состав «компьютерных атак». Однако часть этих угроз, по-прежнему, должны определяться как самостоятельные способы реализации угроз. Такой же подход следует также принять для технических каналов утечки информации (ТКУИ) и для ПЭМИН.

Под утечкой информации понимается неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к ней или получения защищаемой информации иностранными разведками и другими заинтересованными субъектами (заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо).

Технический канал утечки информации – путь утечки информации от объекта защиты, образуемый совокупностью объекта защиты, физической среды и средства технической разведки.

Под утечкой информации по каналам ПЭМИН по-

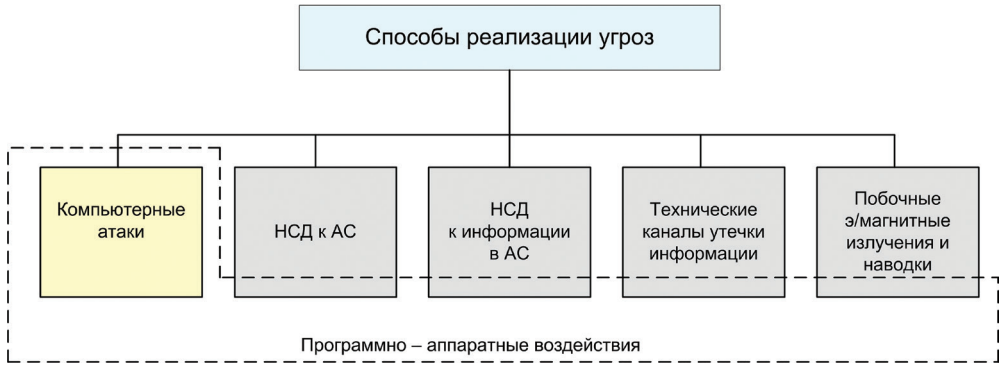


Рис. 2. Способы реализации угроз в ИКС СН

нимается возможность доступа к информации в ИС, осуществляемого путем перехвата и соответствующей обработки побочных (паразитных, непреднамеренных) излучений технических средств, используемых для сбора, обработки, хранения и обмена информацией.

Технические каналы утечки и каналы ПЭМИН в настоящее время достаточно изучены. Однако эти способы получили дальнейшее развитие и «компьютеризировались». Сейчас достаточно «заразить» нужный компьютер специальной программой-закладкой («троянский «конь») любым из известных способов (по технологии вирусов: через компакт-диск с презентацией, интересной программой или игрушкой, дискету с драйверами, а если компьютер в локальной сети - то и через сеть). Программа ищет необходимую информацию на диске и путем обращения к различным устройствам компьютера вызывает появление побочных излучений. Например, программа-закладка может встраивать сообщение в композитный сигнал монитора, при этом пользователь даже не подозревает, что в изображения на мониторе вставлены конфиденциальные текстовые сообщения или изображения. С помощью разведывательного приемника обеспечивается перехват паразитного излучения монитора и выделение требуемого полезного сигнала.

Технология скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств была практически опробована в ходе экспериментальных исследований в США ещё в 1998 году.

Таким образом, для характеристики возможных воздействий на ИКС СН, способы реализации угроз в настоящее время могут быть представлены, как показано на рис. 2, а обобщенные группы угроз безопасности информации для ИКС СН (рис. 3).

Источниками угроз безопасности ИКС СН являются:

– субъекты (нарушители), осуществляющие умышленные незаконные действия в отношении средств ИКС СН и информации, циркулирующей в информационных системах;

– субъекты (нарушители), создающие непреднамеренные угрозы безопасности системы и информации, обрабатываемой и хранящейся в системах обработки информации;

– технические аварии (отказы оборудования, внезапное отключение электропитания, протечки и т.п.);

– стихийные бедствия (пожары, наводнения и т.п.) и чрезвычайные ситуации.

Необходимо различать внешние и внутренние источники угроз безопасности ИКС СН.

Внешний источник – это субъект (физическое лицо, организация, служба иностранного государства и т.п.), не входящий в состав персонала ИКС СН (то есть не являющийся должностным лицом), деятельность которого направлена на нанесение ущерба безопасности сети и/или информации, циркулирующей на объектах сети, или объект, функционирование которого может принести к ущербу безопасности ИКС СН.

Внутренний источник угрозы (часто употребляется термин «инсайдер») – это субъект из состава персонала объекта ИКС СН, деятельность которого направлена на нанесение ущерба безопасности сети, или непреднамеренные действия которого способствуют нанесению такого ущерба или элемент объекта ИКС СН, функционирование которого может принести к ущербу безопасности функционирования инфокоммуникационной сети.

Основными объектами воздействия для угроз являются:

– средства информатизации (помещения, средства вычислительной техники, автоматизированные системы (подсистемы), сети, средства и системы связи и передачи данных);

– конфиденциальная информация, циркулирующая в системах электронного документооборота в процессе информационного взаимодействия;

– общесистемные и прикладные программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение);

– средства защиты информации;

– средства контроля эффективности защиты информации

– персонал.

Рис. 3. Группы угроз безопасности информации для ИКС СН

За основу классификации угроз безопасности сетей электросвязи целесообразно взять классификацию, установленную ГОСТ Р 51275 -2006, в соответствии с которой угрозы могут быть классифицированы:

– по природе возникновения: объективные (естественные) или субъективные (искусственные);

– по источнику возникновения: внешние или внутренние.

Источником угроз безопасности сетей электросвязи могут быть: субъект, материальный объект или физическое явление.

Внутренними объективными являются следующие факторы.

1. Передача сигналов:

а) по проводным линиям связи;

б) по оптико-волоконным линиям связи;

в) в диапазоне радиоволн и в оптическом диапазоне длин волн.

2. Излучения сигналов, функционально присущие техническим средствам (ТС):

а) излучения акустических сигналов:

сопутствующие работе технических средств обработки и передачи информации (ТС ОПИ);

сопутствующие произносимой или воспроизводимой ТС речи;

б) электромагнитные излучения и поля:

излучения в радиодиапазоне;

излучения в оптическом диапазоне.

3. Побочные электромагнитные излучения:

а) элементов (устройств) ТС ОПИ;

б) на частотах работы высокочастотных генераторов устройств, входящих в состав ТС ОПИ:

модуляция побочных электромагнитных излучений информативным сигналом, сопровождающим работу ТС ОПИ;

модуляция побочных электромагнитных излучений акустическим сигналом, сопровождающим работу ТС ОПИ;

в) на частотах самовозбуждения усилителей, входящих в состав ТС ОПИ.

4. Паразитное электромагнитное излучение:

а) модуляция паразитного электромагнитного излучения информационными сигналами;

б) модуляция паразитного электромагнитного излучения акустическими сигналами.

5. Наводка:

а) в электрических цепях ТС, имеющих выход за пределы контролируемых зон;

б) в линиях связи:

вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

вызванная внутренними емкостными и (или) индуктивными связями;

в) в цепях электропитания:

вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

вызванная внутренними емкостными и (или) индуктивными связями;

3) через блоки питания ТС;

г) в цепях заземления:

вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию;

вызванная внутренними емкостными и (или) индуктивными связями;

обусловленная гальванической связью схемной (рабочей) «земли» узлов и блоков ТС;

д) в технических средствах, проводах, кабелях и иных токопроводящих коммуникациях и конструкциях, гальванически не связанных с ТС, вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

6. Наличие акустоэлектрических преобразователей в элементах ТС.

7. Дефекты, сбои и отказы, аварии ТС и систем.

8. Дефекты, сбои и отказы программного обеспечения ОИ.

Внешними объективными являются следующие факторы.

1. Явления техногенного характера:

а) непреднамеренные электромагнитные облучения ОИ;

б) радиационные облучения ОИ;

в) сбои, отказы и аварии систем обеспечения ОИ.

2. Природные явления, стихийные бедствия:

а) термические факторы (пожары и т.д.);

б) климатические факторы (наводнения и т.д.);

в) механические факторы (землетрясения и т.д.);

г) электромагнитные факторы (грозовые разряды и т.д.);

д) биологические факторы (микробы, грызуны и т.д.);

е) химические факторы (химически агрессивные среды и т.д.).

Субъективными внутренними факторами, воздействующими на безопасность защищаемой информации являются следующие факторы.

1. Разглашение защищаемой информации лицами, имеющими к ней право доступа, через:

а) лиц, не имеющих права доступа к защищаемой информации;

б) передачу информации по открытым линиям связи;

в) обработку информации на незащищенных ТС обработки информации;

г) опубликование информации в открытой печати и других средствах массовой информации;

д) копирование информации на незарегистрированный носитель информации;

е) передачу носителя информации лицам, не имеющим права доступа к ней;

ж) утрату носителя информации.

2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, путем:

а) несанкционированного изменения информации:

б) несанкционированного копирования защищаемой информации.

3. Несанкционированный доступ к информации путем:

а) подключения к техническим средствам и системам;

б) использования закладочных средств (устройств);

в) использования программного обеспечения технических средств через:

маскировку под зарегистрированного пользователя;

дефекты и уязвимости программного обеспечения;

внесение программных закладок;

применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

г) хищения носителя защищаемой информации;

д) нарушения функционирования ТС обработки информации.

4. Недостатки организационного обеспечения защиты информации при:

а) задании требований по защите информации (требования противоречивы, не обеспечивают эффективную защиту информации и т.д.);

б) несоблюдении требований по защите информации;

в) контроле эффективности защиты информации.

5. Ошибки обслуживающего персонала ОИ при:

а) эксплуатации ТС;

б) эксплуатации программных средств;

в) эксплуатации средств и систем защиты информации.

Внешними субъективными факторами являются следующие факторы.

1. Доступ к защищаемой информации с применением технических средств:

а) разведки:

радиоэлектронной;

оптико-электронной;

фотографической;

визуально-оптической;

акустической;

гидроакустической;

технической компьютерной;

б) съема информации.

2. Несанкционированный доступ к защищаемой информации путем:

а) подключения к техническим средствам и системам;

б) использования закладочных средств (устройств);

в) использования программного обеспечения технических средств через:

маскировку под зарегистрированного пользователя;

дефекты и уязвимости программного обеспечения;

внесение программных закладок;

применение вирусов или другого вредоносного программного кода (троянские программы, клавиатурные шпионы, активное содержимое документов);

г) несанкционированного физического доступа;

д) хищения носителя информации.

3. Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

4. Действия криминальных групп и отдельных преступных субъектов:

а) диверсия в отношении объекта;

б) диверсия в отношении элементов объекта.

5. Искажение, уничтожение или блокирование информации с применением технических средств путем:

а) преднамеренного силового электромагнитного воздействия:

по сети электропитания на порты электропитания постоянного и переменного тока;

по проводным линиям связи на порты ввода-вывода сигналов и порты связи;

по металлоконструкциям на порты заземления и порты корпуса;

посредством электромагнитного быстроизменяющегося поля на порты корпуса, порты ввода-вывода сигналов и порты связи;

б) преднамеренного силового воздействия различной физической природы;

в) использования программных или программно-аппаратных средств при осуществлении:

компьютерной атаки;

сетевой атаки;

г) воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

В процессе обеспечения безопасности конкретной ИКС СН необходимо выявление всех возможных угроз ее инфокоммуникационной структуре.

Полное множество угроз безопасности не поддается формализации. Это связано с тем, что архитектура современных ИКС СН, используемые технологии обработки, хранения и передачи информации подвержены большому количеству объективных и субъективных дестабилизирующих воздействий. Но чем больше будет выявлено возможных угроз безопасности, тем точнее будет оценено состояние безопасности сети электросвязи.

К основным возможным угрозам безопасности ИКС СН могут быть отнесены следующие угрозы:

– уничтожение информации и/или других ресурсов;

– искажение или модификация информации;

– мошенничество;

– кража, утечка, потеря информации и/или других ресурсов;

– несанкционированный доступ;

– отказ в обслуживании.

Каждая выявленная угроза в соответствии с выбранной методикой оценки рисков должна ранжироваться по вероятности своего возникновения для последующего анализа рисков и оценки величины возможного ущерба сети электросвязи от реализации угроз [5 – 13].

Угрозы безопасности ИКС СН реализуются нарушителями безопасности через выявленные уязвимости инфокоммуникационной структуры сети, в которую они могут быть внесены на технологическом и/или эксплуатационном этапах ее жизненного цикла. Угрозы безопасности могут изменяться. Уязвимость может существовать на протяжении всего срока эксплуатации сети электросвязи или конкретного протокола, если она своевременно не устраняется разработчиком или по его представлению службами эксплуатации оператора связи.

В целях учета всех возможных сфер проявления угроз для каждой конкретной ИКС СН разрабатывается модель угроз безопасности.

Модель угроз безопасности ИКС СН представляет собой нормативный документ, которым должен руководствоваться заказчик при задании требований к безопасности ИКС СН, и разработчик, создающий эту сеть и службы обеспечения информационной безопасности при ее эксплуатации.

Модель угроз должна включать:

– описание ресурсов инфокоммуникационной структуры (объектов безопасности) ИКС СН, требующих защиты;

– описание источников формирования дестабилизирующих воздействий и их потенциальных возможностей;

– стадии жизненного цикла ИКС СН, в том числе определяющие ее технологический и эксплуатационный этапы;

– описание процесса возникновения угроз и путей их практической реализации.

В качестве приложения модель угроз безопасности должна содержать полный перечень угроз и базу данных о выявленных нарушениях безопасности ИКС СН с описанием обстоятельств, связанных с обнаружением нарушений.

В соответствии с разработанной моделью угроз оценивается опасность угроз для каждой группы идентифицированных ресурсов инфокоммуникационной структуры ИКС СН и услуг связи и определяются возможные меры обеспечения безопасности для противодействия каждой конкретной угрозе.

Программно-аппаратные воздействия (ПАВ) на ИКС СН можно классифицировать также, как классифицируются угрозы, т.е. это будут действия, направленные на нарушение конфиденциальности (несанкционированное чтение), целостности (несанкционированная модификация), доступности (несанкционированное уничтожение или блокирование доступа) защищаемой информации в ИКС СН.

Однако, специфика ПАВ на современные ИКС СН такова, что каждое из них, как правило, сопровождается реализацией этих трех угроз одновременно на разные виды и типы хранимой и передаваемой информации. Поэтому в данном подразделе приводятся описания наиболее часто применяемых противником ПАВ.

Можно разделить действия нарушителей в перспективной ИКС СН на активные и пассивные. К пассивным действиям можно отнести не только анализ сетевого трафика при подготовке атак, но и хищение конфиденциальной информации, передаваемой по сетям ИКС СН в виде файлов или потоков. В случае приложений потокового вещания предусматриваются меры защиты от несанкционированного копирования и нарушения, из-за хищения контента, авторских прав контентодержателя, но далеко не всегда этот вид услуг защищен от несанкционированного подслушивания/подсматривания без сохранения потока. К активным воздействиям относятся модификация или подмена информации, а также порождение паразитной сетевой информации с целью понижения или полной утраты работоспособности узлов ИКС СН.

Модификация потоков информации (требований и услуг) в перспективной ИКС СН. В результате селекции потока перехваченной информации и его анализа можно распознавать тип передаваемых файлов (исполняемый или текстовый). Соответственно, в случае обнаружения текстового файла или файла данных появляется возможность модифицировать проходящие через ложный объект данные. Особую угрозу эта функция представляет для перспективных ИКС СН при обработке конфиденциальной информации.

Другим видом модификации может быть модификация передаваемого кода. Ложный объект, проводя семантический анализ проходящей через него информации, может выделять из потока данных исполняемый код.

Чтобы определить, что передается по сетям ИКССН – код или данные, необходимо использовать определенные особенности, свойственные реализации сетевого обмена в конкретной ИКС СН или некоторые особенности, присущие конкретным типам исполняемых файлов в конкретной операционной системе прикладного сервера или абонентского терминала ИКС СН.

При внедрении разрушающих программ исполняемый файл модифицируется по вирусной технологии: к исполняемому файлу одним из известных способов дописывается тело внедряемой программы и изменяется точка входа так, чтобы она указывала на начало внедренного кода. Описанный способ, в принципе, ничем не отличается от стандартного заражения исполняемого файла вирусом, за исключением того, что файл заражен вирусом в процессе доставки. Такое возможно лишь при использовании системы воздействия, построенной по принципу «ложный объект».

В качестве примеров можно привести вариант использования ложного объекта для создания сетевого червя – наиболее сложного на практике удаленного воздействия в ИКС СН, или внедрение программ – сетевых шпионов.

В случае, когда происходит модификация исполняемого кода с целью изменения логики его работы, воздействие требует предварительного исследования работы исполняемого файла.

Подмена информации. Если модификация информации приводит к ее частичному искажению, то подмена – к полному ее изменению. При возникновении в ИКС СН определенного контролируемого ложным объектом события одному из участников обмена посылается заранее подготовленная дезинформация. При этом такая дезинформация в зависимости от контролируемого события может быть воспринята либо как исполняемый код, либо как данные. Ложный объект контролирует событие, которое состоит в подключении пользователя министерства и ведомства к серверу ИКС СН. Он ожидает, например, запуска соответствующей программы входа в систему обслуживания ИКС СН. Исполняемый файл при запуске программы на сервере, передается на рабочую станцию. Вместо того, чтобы выполнить данное действие, ложный объект передает на рабочую станцию код заранее написанной специальной программы - захватчика паролей. Эта программа выполняет визуально те же действия, что и настоящая программа входа, после чего полученные сведения посылаются на ложный объект, а пользователю выводится сообщение об ошибке. При этом пользователь, посчитав, что он неправильно ввел пароль (пароль обычно не отображается на экране), снова запустит программу подключения к ИКС СН и со второго раза получит доступ. Результат такой атаки – получение имя и пароля пользователя, сохраненные на ложном объекте.

Отказ в обслуживании. Сетевая операционная система функционирует на каждом из объектов территориально распределенной ИКС СН. Одной из основных задач, возлагаемых на нее, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в ИКС СН каждый пользователь или приложение должны иметь возможность санкционировано подключиться к любой службе ИКС СН и получить в соответствии со своими правами удаленный доступ к его ресурсам и услугам. Обычно в ИКС СН возможность предоставления удаленного доступа реализуется следующим образом: на объекте сети в среде сетевой операционной системы запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта.

Программы-серверы входят в состав информационных и телекоммуникационных служб предоставления удаленного доступа. Задача сервера состоит в том, чтобы, находясь в памяти операционной системы объекта ИКС СН, постоянно ожидать получения запроса на подключение от удаленного объекта. В случае получения подобного запроса сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет.

По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты ИКС СН. В этом случае непосредственно система сетевого управления обрабатывает приходящие извне запросы на создание виртуального канала и передает их в соответствии с идентификатором запроса (порт или сокет) прикладному процессу, которым является соответствующий сервер. Очевидно, что возможно иметь только ограниченное число открытых виртуальных соединений и отвечать лишь на ограниченное число запросов. Эти ограничения зависят от различных параметров ИКС СН в целом, основными из которых являются быстродействие серверов сетевых приложений, объем их оперативной памяти и пропускная способность канала связи (чем она выше, тем больше число возможных запросов в единицу времени возможно).

Основная проблема состоит в том, что при отсутствии статической ключевой информации в ИКС СН, идентификация запроса возможна только по адресу его отправителя. Если в ИКС СН не предусмотрено средств аутентификации адреса отправителя, то есть ее инфраструктура позволяет с одного объекта системы передавать на другой атакуемый объект бесконечное число анонимных запросов на подключение от имени других объектов, то в этом случае будет иметь успех удаленная атака типа «Отказ в обслуживании». Результат применения этой удаленной атаки – нарушение на атакованном объекте работоспособности соответствующей службы предоставления доступа и услуги, то есть невозможность получения доступа с других объектов ИКС СН, то есть отказ в обслуживании.

Другая разновидность этой типовой удаленной атаки состоит в передаче с одного адреса такого количества запросов на атакуемый объект, какое позволит трафик превратить в направленный «шторм» запросов. Если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из информационных или телекоммуникационных служб ИКС СН, так и полная их остановка из-за невозможности заниматься ничем другим, кроме обработки запросов.

Третьей разновидностью атаки «Отказ в обслуживании» является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы.

Атака «Отказ в обслуживании» является активным воздействием, осуществляемым с целью нарушения работоспособности элементов и даже целых компонент ИКС СН, безусловно, относительно цели атаки. Она яв-

ляется воздействием без обратной связи, как межсегментным, так и внутрисегментным, осуществляемым на базовой и инфраструктурном уровнях модели ИКС СН.

Нарушители безопасности ИКС СН.
Особенности моделей нарушителя для ИКС СН

Для ИКС СН характерно наличие как нарушителей безопасности, так и противника (в особые периоды функционирования сети). Однако в данном разделе не будут рассматриваться отдельно действия этих групп, так как в значительной мере поведение их схоже.

Нарушителем безопасности (нарушителем) ИКС СН является физическое или юридическое лицо, преступная группа, процесс или событие, производящие преднамеренные или непреднамеренные воздействия на инфокоммуникационную структуру ИКС СН, приводящие к нежелательным последствиям для интересов пользователей министерств и ведомств информационными и телекоммуникационными услугами, операторов связи и/или органов государственного управления.

Нарушителями безопасности ИКС СН могут быть [1, 2, 4, 5, 10 – 13]:

– террористы и террористические организации;

– конкурирующие организации и структуры;

– спецслужбы иностранных государств и блоков государств;

– криминальные структуры;

– взломщики программных продуктов, использующихся в инфокоммуникационных сетях;

– бывшие сотрудники организаций;

– недобросовестные сотрудники и партнеры;

– пользователи инфокоммуникационными услугами и др.

Характеристика направлений противодействия нарушителям описывается политикой безопасности, представляющей собой совокупность документированных правил, процедур, практических приемов или руководящих принципов в области обеспечения безопасности, которыми должен руководствоваться оператор связи.

Для учета всех возможных воздействий нарушителей и определения его категории разрабатывается модель нарушителя безопасности ИКС СН, под которой понимается абстрактное (формализованное или неформализованное) описание нарушителя политики безопасности.

Задача построения модели нарушителя безопасности ИКС СН состоит в определении:

– штатных объектов и элементов ИКС СН, к которым возможен доступ;

– субъектов, допущенных к работе с оборудованием ИКС СН в период ее проектирования, разработки, развертывания и эксплуатации;

– перечня соответствия объектов доступа субъектам, которые могут быть потенциальными нарушителями.

При определении потенциального нарушителя и составлении его модели исходят из того, что нарушитель может быть как законным пользователем услуг ИКС СН (принадлежать к персоналу, непосредственно работающему с абонентскими терминалами), так и посторонним лицом, пытающимся непосредственно или с помощью имеющихся у него технических и программных средств получить доступ к информационным ресурсам и инфраструктуре ИКС СН.

Воздействия нарушителей, в основном, направлены на ухудшение качественных характеристик функционирования ИКС СН и могут осуществляться, как правило, путем поиска и использования эксплуатационных и технологических уязвимостей. Воздействия могут осуществляться:

– по каналам абонентского доступа, в том числе и беспроводным;

– по внутренним линиям связи;

– с рабочих мест систем управления и технического обслуживания;

– по не декларированным каналам доступа.

При этом могут использоваться как штатные, так и специальные средства.

Воздействия нарушителей могут носить как непреднамеренный (случайный), так и преднамеренный характер.

Непреднамеренные (случайные) воздействия могут быть спровоцированы недостаточной надежностью средств связи и автоматизации ИКС СН, ошибками обслуживающего персонала, природными явлениями и другими объективными дестабилизирующими воздействиями.

Преднамеренные воздействия могут быть активными, пассивными и не преследующими никаких целей.

Активные действия нарушителя предусматривают вмешательство в работу ИКС СН, нарушение режимов ее функционирования и снижение качества обслуживания вплоть до полного прекращения предоставления услуг связи пользователям.

Пассивные действия нарушителя предполагают нанесение вреда пользователю информационных и телекоммуникационных услуг путем использования выявленных уязвимостей ИКС СН, но не наносящие прямого вреда самой ИКС СН. Целью таких действий могут являться:

– перехват персональных данных пользователей (например, паролей для регистрации терминалов);

– перехват данных о финансовых сделках с целью нанесения ущерба бизнесу;

– наблюдение за выполняемым процессом (подготовка для новых атак - активных действий);

– поиск идеологических, политических выгод;

– шантаж, вымогательство.

Действия, не преследующие целей (хулиганство) не ставят перед собой цели нанесения вреда конкретному физическому объекту или лицу.

Важнейшие особенности модели нарушителя безопасности ИКС СН определяются её назначением.

Исходя из общего контекста проблемы (рис. 4), безопасность связана с защитой активов (ресурсов)

от угроз, классифицированных на основе потенциала злоупотребления защищаемыми активами. В сфере безопасности ИКС СН во внимание также следует принимать все разновидности угроз, но наибольший вес должен придаваться тем из них, которые связаны с действиями человека и функционированием ИКС СН.

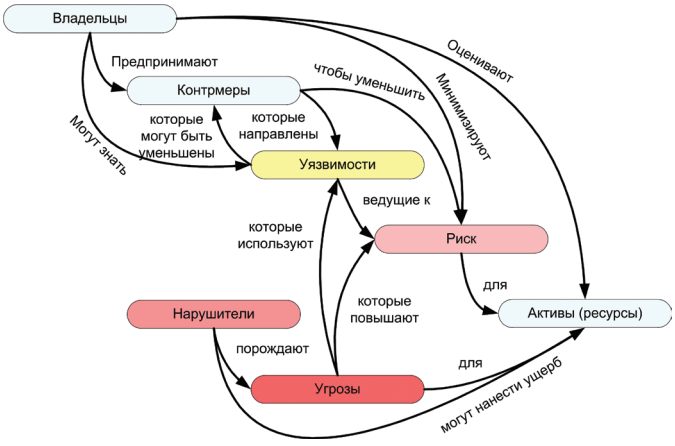


Рис. 4. Общий контекст безопасности

При разработке модели нарушителя ИКС СН, как обычно, должны учитываться:

– предположения о категориях лиц, к которым может принадлежать нарушитель;

– тип нарушителя;

– предположения о мотивах действий нарушителя (преследуемых нарушителем целях);

– предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);

– ограничения и предположения о характере возможных действий нарушителей;

– характер информационных угроз.

Именно характер информационных угроз, точнее та их часть, которую уделяют сетевым угрозам, для модели нарушителя безопасности ИКС СН должна прорабатываться особенно тщательно.

Основная проблема при этом состоит в том, что способы воздействия на сетевые элементы ИСК СН постоянно развиваются. Появляются новые технологии и протоколы. Постоянно растет квалификация пользователей. Растет быстродействие специализированных процессоров, используемых для анализа и дешифровки сетевого трафика. Следствием этого является необходимость отражения в модели нарушителя безопасности ИКС СН категорий лиц и процессов, имеющих возможность отслеживать нештатные ситуации в работе сетей ИКС СН, перегрузки и атаки. Другими словами, в модели нарушителя безопасности ИКС СН должны быть описаны категории объектов, имеющих отношение к мониторингу функционирования инфокоммуникационных сетей, АСУ связью и коммуникационных сетей управления сетевой безопасностью.

Основные способы и средства обеспечения безопасности ИКС СН

Основными целями обеспечения безопасности сетей ИКС СН:

– достижение устойчивого функционирования и успешного выполнения ИКС СН заданных функций в условиях возможных воздействий, способных привести к нарушению конфиденциальности, целостности, доступности или подотчетности;

– обеспечение доступности информационных и телекоммуникационных услуг, особенно услуг экстренного обслуживания в чрезвычайных ситуациях, в том числе и в случае террористических актов.

Особенностью ИКС СН является то, что они предназначены для обеспечения функционирования систем управления министерств и ведомств, а следовательно должны функционировать с необходимой эффективностью в чрезвычайных условиях, в том числе в особых условиях.

Основными задачами обеспечения безопасности ИКС СН являются:

– своевременное выявление, оценка и прогнозирование источников угроз безопасности, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития ИКС СН на всех уровнях иерархии и при взаимодействии с единой сетью электросвязи России (международном, междугороднем, зоновом, местном, на уровне пользования услугами связи и т. д.);

– выявление и устранение уязвимостей в средствах связи и ИКС СН в целом;

– предотвращение, обнаружение угроз безопасности, пресечение их реализации и своевременная ликвидация последствий возможных воздействий нарушителей, в том числе и террористических действий;

– организация системы пропуска приоритетного трафика по ИКС СН в случае чрезвычайных ситуаций, организация бесперебойной работы международной аварийной службы;

– совершенствование и стандартизация применяемых мер обеспечения безопасности ИКС СН.

Содержание указанных задач должно учитываться при планировании мер обеспечения безопасности функционирования ИКС СН в связи с тем, что часть телекоммуникационных ресурсов для ведомств может арендоваться у ЕСЭ РФ.

Как было отмечено выше, безопасность ИКС СН характеризует способность ИКС СН противодействовать определенному множеству угроз, преднамеренных или непреднамеренных дестабилизирующих воздействий на входящие в состав средства, линии связи и технологические процессы (протоколы), что может привести к ухудшению качества услуг, предоставляемых ИКС СН.

Безопасность ИКС СН интегрирует в себе безопасность сетей и безопасность информационных систем (принадлежащих системе управления ведомства и АСУ ИКС СН). Следовательно, обеспечение безопасности

ИКС СН включает в себя обеспечение безопасности ИКС СН и безопасности информации.

Согласно положениям защита информации представляет собой деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

При этом следует различать правовую, техническую, криптографическую и физическую защиту.

Правовая защита информации включает в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации заключается в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации осуществляется с помощью ее криптографического преобразования.

Физическая защита информации осуществляется путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

К объектам защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

По другим взглядам к основным методам защиты информации относятся организационные, физические, технические и программно-аппаратные методы.

Организационные методы включают:

– создание подразделений по защите информации;

– организация контроля выполнения мероприятий защиты;

– организация учета носителей и технических средств обработки информации;

– организация разграничения доступа к информации;

– организация обучения персонала вопросам защиты информации;

– разработка инструкций по защите информации.

Физические методы включают:

– организацию пропускного режима;

– физическую охрану;

– инженерную охрану;

– техническую охрану;

– пожарную охрану;

– охранное телевидение.

Технические методы предусматривают:

– защиту информации от подслушивания;

– защиту информации от перехвата;

– защита информации от подсматривания;

– технический контроль состояния защиты информации;

– стандартизацию способов и средств защиты информации;

– выявление специальных технических средств;

– сертификацию средств защиты информации.

В качестве программно-аппаратных методов используются:

– межсетевое экранирование;

– антивирусная защита;

– система обнаружения вторжений;

– создание VPN;

– криптография;

– стеганография;

– система анализа защищенности;

– идентификация;

– аутентификация.

Таким образом, синтезируя оба подхода, в общем случае способы (методы) обеспечения безопасности ИКС СН могут быть представлены рис. 5.

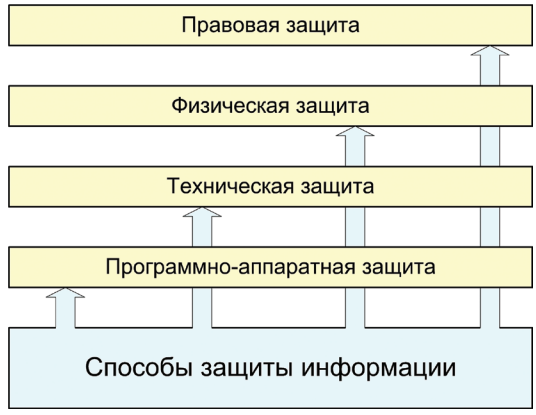


Рис. 5. Основные способы обеспечения безопасности ИКС СН

Современная трактовка состава средств обеспечения безопасности ИКС СН представлена на рис. 6. В качестве основных групп средств обеспечения безопасности ИКС СН следует определить:

– правовые, нормативно-технические и организационные средства;

– технические и программно-аппаратные средства;

– редства управления безопасностью.

Правовые, нормативно-технические и организационные средства предназначены для нормативно-правового, нормативно-технического и организационного регулирования отношений в области обеспечения безопасности ИКС СН. В качестве средств регулирования выступают законодательные и нормативные акты госу-

дарственных органов власти и ведомственных органов управления. На базе нормативных актов формируются органы, обеспечивающие контроль, управление и сертификацию средств обеспечения безопасности ИКС СН.

Выбор технических и программно-аппаратных средств защиты инфокоммуникационных сетей специального назначения должен осуществляться на основе разрабатываемой политики безопасности.

Политика безопасности представляет собой совокупность документированных правил, процедур, практических приемов или руководящих принципов в области обеспечения безопасности ИКС СН, которыми руководствуется ведомство в своей деятельности.

Основное содержание политики безопасности ИКС СН должна составлять модель защиты, представляющая собой порядок использования мер по исключению (минимизации) рисков для идентифицированных активов (ресурсов) ИКС СН на базе моделей нарушителя и угроз.

Технические и программно-аппаратные средства обеспечения безопасности ИКС СН включают средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации и сети.

Технологической реализацией политики безопасности ИКС СН должна быть система управления безопасностью, создаваемая на основе средств управления безопасностью. В качестве методологической основы создания системы управления безопасностью целесообразно использовать стандарты по управлению информационной безопасностью (ГОСТ Р ИСО/МЭК 17799–2005).

Современный подход к обеспечению комплексной безопасности ИКС СН. Этапы создания системы обеспечения комплексной безопасности ИКС СН

В последнее время появились тенденции создания систем обеспечения так называемой комплексной безопасности. В таких системах, кроме обеспечения безопасности сетей ИКС СН и информационной безопасности, в состав «мониторируемых» объектов включают системы контроля физического доступа на объекты, системы пожаротушения, видеонаблюдения, контроля инженерных сетей и т.п.

По сути, эти тенденции означают желание свести воедино потоки разноплановой информации, относящиеся к безопасности ИКС СН, что позволит более оперативно принимать эффективные решения по защите функционирования соответствующей системы управления.

В соответствие с действующими нормативными документами, такими как ГОСТ Р 52448–2005 и ГОСТ Р ИСО/МЭК 17799–2005 на всех этапах проектирова-

Рис. 6. Средства обеспечения безопасности ИКС СН

ния, строительства, реконструкции, развития и эксплуатации сетей ИКС СН и сооружений связи к ним должны предъявляться требования по обеспечению безопасного их функционирования, сопоставимые с возможными воздействиями нарушителя на инфокоммуникационную структуру ИКС СН и ожидаемым ущербом от данных воздействий.

Требования по обеспечению безопасности конкретной сети ИКС СН и ИКС СН в целом должны формироваться с учетом целей, функций и задач решаемых оператором связи, условий ее использования в общей системе связи государства, специфики используемой технологии передачи информации, потенциальных угроз безопасности и возможных воздействий нарушителя, реальных проектных и эксплуатационных ресурсов и существующих ограничений на функционирование сетей ИКС СН, а также требований и условий взаимодействия с другими ведомственными сетями и сетями ЕСЭ РФ.

Требования по обеспечению безопасности ИКС СН включают:

– организационные требования безопасности;

– технические требования безопасности;

– функциональные требования безопасности;

– требования доверия к безопасности.

Организационные требования безопасности содержат общие организационные, административные положения и процедуры по осуществлению мероприятий политики безопасности ДЛ по безопасности ИКС СН.

Технические требования безопасности определяют требования к электропитанию, заземлению, к конструкции средств связи, к линейно-кабельным сооружениям связи, к прокладке линий связи и др., влияющие на обеспечение безопасности и устойчивости функционирования сетей ИКС СН.

Функциональные требования безопасности и требования доверия к безопасности содержат требования, определенные ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 соответственно, которые для сетей и средств ИКС СН должны реализовываться на всех этапах ее жизненного цикла.

Требования к информационной безопасности определяются с помощью систематической оценки рисков. Решения о расходах на мероприятия информационной безопасности должны приниматься, исходя из возможного ущерба, нанесенного в результате нарушений информационной безопасности. Методы оценки риска могут применяться как для всего силового ведомства, так и для какой-либо его части, отдельных информационных систем, определенных компонентов где это практически выполнимо и целесообразно.

При этом все используемые средства связи и автоматизации должны быть сертифицированы в соответствующей системе сертификации, а пользователи и технический персонал ИКС СН должны быть соответствующим образом отобраны и подготовлены.

В целом, системный подход к обеспечению комплексной безопасности ИКС СН позволяет выделить три этапа создания системы обеспечения комплексной безопасности (рис.7):

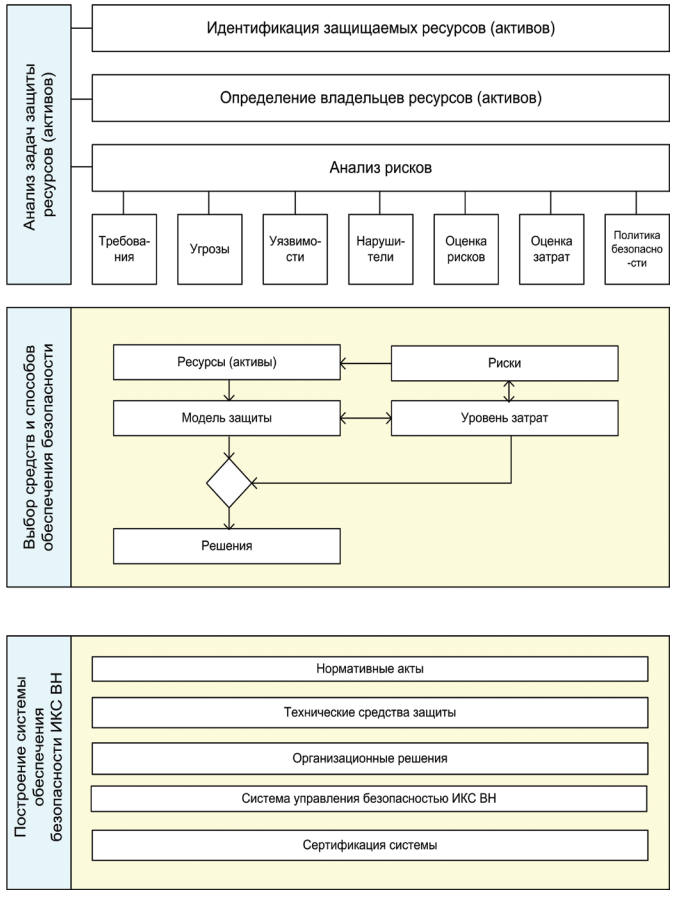


Рис. 7. Этапы создания системы обеспечения безопасности ИКС СН

– этап анализа задач защиты ресурсов (активов);

– этап выбора средств и способов обеспечения безопасности;

– этап построения системы обеспечения безопасности ИКС СН.

Этап анализа задач защиты ресурсов (активов) должен включать подэтапы идентификации защищаемых ресурсов, определения владельцев ресурсов и анализа рисков.

Основное содержание этапа выбора средств и способов обеспечения безопасности состоит в обосновании рациональности решений, обеспечивающих реализацию политики безопасности ИКС СН с приемлемым уровнем затрат. Такие решения получаются в результате итеративных процедур, позволяющих взвесить риски для различных активов с уровнем затрат на противодействие им.

Этап построения системы обеспечения безопасности ИКС СН включает:

– формирование (разработку) нормативных актов для обеспечения функционирования системы безопасности;

– создание технической архитектуры системы, распределение и монтаж на объектах технических средств защиты;

– принятие организационных решений по структуре подразделений, обеспечивающих функционирование системы безопасности;

– принятие организационных и технических решений по структуре системы управления безопасностью;

– сертификация системы обеспечения безопасности ИКС СН.

Литература

1. Доктрина информационной безопасности Российской Федерации: Утверждена Президентом Российской Федерации Пр-1895 от 09 сентября 2000 г.

2. *Буренин А.Н., Легков К.Е.* Современные инфокоммуникационные системы и сети специального назначения. Основы построения и управления: Монография. М.: ООО «ИД Медиа Паблишер», 2015. 348 с.

3. *Mitra D., Ramakrishman K.G.* Technics for traffic engeniring of multiservice in priority networks. BLTJ. 2001. Vol. 1. Pp. 123–130.

4. *Зима В.М., Молдовян А.А., Молдовян Н.А.* Безопасность глобальных сетевых технологий. СПб.: СПбУ, 1999. 368 с.

5. *Буренин А.Н., Легков К.Е.* Некоторые модели управления безопасностью инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. №4. С. 46–50.

6. *Котенко И. В., Степашкин М. В., Богданов В. С.* Анализ защищенности компьютерных сетей на различных этапах проектирования и эксплуатации // Изв. вузов. Приборостроение. 2006. Т. 49. № 5. С. 3–8.

7. *Tishkov A., Kotenko I.* Security Checker Architecture for Policy-based Security ManagementLectureNotes in Computer Science. Springer-Verlag. 2005. Vol. 3685. LNCS. Pp. 460–465.

8. The Third International Workshop «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-05). 2005.

9. *Gorodetski V., Karsayev O., Kotenko I., Khabalov A.* Software Development Kit for Multi-agent Systems Design and Implementation. Lecture Notes in Artificial Intelligence. SpringerVerlag. 2002. Vol. 2296. Pp. 121–130.

10. *Gorodetski V., Kotenko I.* Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool. Recent Advances in Intrusion Detection.Fifth International Symposium. RAID 2002. Zurich, Switzerland. October 2002. Proceedings. Lecture Notes in Computer Science. Vol. 2516. Pp. 219–238.

11. *Kotenko I.* Teamwork of Hackers-Agents: Modeling and Simulation of Coordinated DistributedAttacks on Computer Networks. Lecture Notes in Artificial Intelligence, Springer-Verlag. 2003. Vol. 2691. P. 464.

12. *Gorodetsky V., Kotenko I., Karsayev O.* The Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning. The International Journal of Computer Systems Science &Engineering. 2003. Vol. 18. № 4. Pp. 191–200.

13. *Kotenko I. V.* Modeling and Simulation of Attacks for Verification of Security Policy and Vulnerability Assessment. Seventh International Symposium on Recent Advances in Intrusion Detection. RAID 2004. Abstract and Poster sessions. Sophia-Antipolis. French Riviera. France. 2004. Pp. 533–543.

Для цитирования:
Буренин А.Н., Легков К.Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 46–61.

SECURITY ISSUES INFOCOMMUNICATION SYSTEMS AND NETWORKS FOR SPECIAL PURPOSES: THE MAIN THREATS, THE WAYS AND MEANS OF ENSURING COMPREHENSIVE NETWORK SECURITY

Burenin Andrey Nikolaevich,
St. Petersburg, Russian, konferencia_asu_vka@mail.ru

Legkov Konstantin Evgenyevich,
St. Petersburg, Russian, constl@mail.ru

Abstract
Currently the guaranteed support of the required telecommunication and information services users special controls for defense, safety and support of a law enforcement issues related to the complex solution of difficult problems of the organization, design, maintenance, safety of functioning and control of infocommunication systems and special purpose networks within appropriate departmental and interdepartmental communications. It assumes the decision sufficiently complex technical and theoretical challenges in which sentences and recommendations

about the organization of modern infocommunication systems and special purpose networks functioning in a whole range of information and destructive influences.
Occurring in recent years, intensive integration processes various kinds of data communication networks, voice, video and applications with the means of the users, as well as the need to support multimedia and information technology at the sites of departmental centers and automated information systems, set new objectives foe the creation, operation of communication systems and special purpose networks, as well as on the organization of effective management of these networks. At the same time there are practically no publications that have addressed the problems of organization, creations, maintenance and control of the modern infocommunication systems and networks generally and special purpose, in particular.
When solving problems of the organization management of modern information and communication network special purpose it is necessary to consider the requirements for security, as there is rather high probability of an intentional invasion of the privacy the network from the external environment, which is performed for the purpose of unauthorized use resources (information theft), and the purpose of its performance. Therefore, without appropriate means of information protection and implementation of appropriate mechanisms to protect the functioning of information and communication systems for special purposes impossible.
In virtue of the above stated considerations, the consideration and study of security issues of modern communication systems for special purposes is very important.

Keywords: infocommunication systems, telecommunications and information services, destructive and informational influence, the problems of security, security threats.

References

1. Doctrine of information security of the Russian Federation: It is approved as the President of the Russian Federation D –1895 from 09 september 2000.
2. *Burenin A.N., Legkov K.E.* Sovremennye infokommunikatsionnye sistemy i seti spetsial nogo naznacheniya. Osnovy postroeniya i upravleniya: Monografiya. [Modern infocommunication systems and special purpose networks. Basics of creation and control]. Moscow: Media Publisher, 2015. 348 p. (In Russian).
3. *Mitra D., Ramakrishman K.G.* Technics for traffic engeniring of multiservice in priority networks. BLTJ. 2001. Vol. 1. Pp. 123–130.
4. *Zima B.M., Moldovyan A.A., Moldovyan N.A.* Bezopasnost global nykh setevykh tekhnologiy [Safety of global network technologies]. SPb.: SPbU. 1999. 234 p. (In Russian).
5. *Burenin A.N., Legkov K.E.* Some models of security management infocommunication networks of the special purpose. H&ES Research. 2013. Vol. 5. No. 4. Pp. 46–50. (in Russian)
6. *Kitten of I.V., Stepashkin M.V., Bogdanov V.S.* The analysis of security of computer networks at various stages of their life cycle. Priborostroenie. 2006. Vol. 49. № 4. Pp. 3–8. (In Russian).
7. *Tishkov A., Kotenko I.* Security Checker Architecture for Policy-based Security Management. LectureNotes in Computer Science. Springer-Verlag. 2005. Vol. 3685. LNCS. Pp. 460–465.
8. The Third International Workshop «Mathematical Methods, Models and Architectures for Computer Networks Security» (MMM-ACNS-05). 2005.
9. *Gorodetski V., Karsayev O., Kotenko I., Khabalov A.* Software Development Kit for Multi-agent Systems Design and Implementation. Lecture Notes in Artificial Intelligence. SpringerVerlag. 2002. Vol. 2296. Pp.121–130.
10. *Gorodetski V., Kotenko I.* Attacks against Computer Network: Formal Grammar-based Framework and Simulation Tool. Recent Advances in Intrusion Detection. Fifth International Symposium. RAID 2002. Zurich, Switzerland. October 2002. Proceedings. Lecture Notes in Computer Science. Vol. 2516. Pp. 219–238.
11. *Kotenko I.* Teamwork of Hackers-Agents: Modeling and Simulation of Coordinated DistributedAttacks on Computer Networks. Lecture Notes in Artificial Intelligence, Springer-Verlag. 2003. Vol. 2691. P. 464.
12. *Gorodetsky V., Kotenko I., Karsayev O.* The Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning. The International Journal of Computer Systems Science & Engineering. 2003. Vol. 18. № 4. Pp. 191–200.
13. *Kotenko I.V.* Modeling and Simulation of Attacks for Verification of Security Policy and Vulnerability Assessment. Seventh International Symposium on Recent Advances in Intrusion Detection. RAID 2004. Abstract and Poster sessions. Sophia-Antipolis. French Riviera. France. 2004. Pp. 533–543.

Information about authors:

Burenin A.N., Ph.D., associate professor, chief specialist of JSC «Research Institute «Rubin» ;
Legkov K.E., Ph.D., deputy head of the Department Technologies and technical means the provision and operation of automated systems of control, Military Space Academy.

For citation:
Burenin A.N., Legkov K.E. Security issues infocommunication systems and networks for special purposes: the main threats, the ways and means of ensuring comprehensive network security. H&ES Research. 2015. Vol. 7. No. 3. Pp. 46–61. (in Russian).

«Космическая связь» вводит в эксплуатацию новый космический аппарат связи и вещания «Экспресс-АМ7» в орбитальной позиции 40° восточной долготы

Космическая связь
Федеральное государственное унитарное предприятие

24 апреля 2015 года ФГУП «Космическая связь» (ГП КС) начинает предоставлять услуги связи и вещания в орбитальной позиции 40° восточной долготы с использованием нового космического аппарата «Экспресс-АМ7», который успешно прошел программу летных испытаний и принят в эксплуатацию. Зоны обслуживания «Экспресс-АМ7» охватывают Россию, Европу, Ближний Восток, Африку южнее Сахары, а также Южную Азию.

Новый телекоммуникационный КА «Экспресс-АМ7» тяжелого класса создавался по заказу ГП КС компанией Aribus DS в рамках Федеральной космической программы Российской Федерации на 2009-2015 годы и ФЦП «Развитие телерадиовещания в Российской Федерации на 2009–2015 годы». КА «Экспресс-АМ7» оснащен 80 мощными транспондерами и 9 антеннами C-, Ku- и L-диапазонов частот, срок службы космического аппарата составляет 15 лет.

«Начало работы данного аппарата – это очередной большой шаг к полному устранению информационного неравенства между нашими согражданами и повышению стабильности работы всей системы телерадиовещания Российской Федерации. Также предоставляемый ресурс позволит нашему подведомственному предприятию повысить эффективность работы в новых экономических условиях», – отметил руководитель Россвязи Олег Духовницкий.

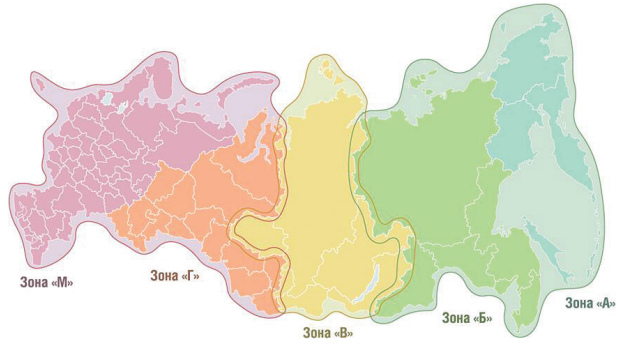
Космический аппарат «Экспресс-АМ7» предназначен для трансляции телевизионных пакетов программ в рамках ФЦП, обеспечения президентской, правительственной и специальной связи, предоставления услуг фиксированной спутниковой связи в интересах государственных и коммерческих заказчиков.

Российские и зарубежные пользователи получают новые возможности организации широкополосного доступа в Интернет, создания корпоративных сетей, в том числе на основе VSAT-технологий, услуг телерадиовещания и мультимедиа. Космический аппарат «Экспресс-АМ7» позволит мобильным операторам создавать сети привязки удаленных базовых станций сотовой связи, что повысит уровень проникновения и расширит линейку услуг связи в труднодоступных и удаленных регионах.

«В преддверии праздника Великой Победы ГП КС начинает трансляцию пакета федеральных программ, а также первого и второго мультиплекса на вещательные зоны М и Г Российской Федерации (европейская часть и Урал) с использованием самого современного космического аппарата – «Экспресс-АМ7». Ввод в эксплуатацию «Экспресс-АМ7» позволит ГП КС укрепить позиции компании на российском и зарубежных рынках, а также выйти на новые для предприятия быстрорастущие рынки Африки и Южной Азии», – подчеркивает генеральный директор ГП КС Юрий Прохоров.

Финансирование создания «Экспресс-АМ7» осуществлялось с привлечением ресурсов Внешэкономбанка. Общая стоимость проекта составила порядка 152,8 млн. евро.

В рамках создания КА «Экспресс-АМ7» была реализована программа подготовки российских специалистов РКК «Энергия» и ФГУП НИИР. Обучение, организованное Airbus DS совместно с ГП КС, проводилось как в России, так и на производственных площадках во Франции, и охватывало все аспекты телекоммуникационных программ: управление проектами, гарантия и стандарты качества, проектирование и создание космической платформы и полезной нагрузки, проведение испытаний полезной нагрузки и космического аппарата. В обучении и стажировках приняло участие более 40 специалистов РКК «Энергия» и ФГУП НИИР.



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

CAUSE OF FALSE POSITIVE OF AUTOMATIC FIRE NOTIFICATION SYSTEM AND IMPROVEMENT PLAN IN KOREA

Kong Ha Sung,
Ph.D., associate professor, lecturer in Kyungil University, Seoul, Korea
kiu119@naver.com

Keywords: *Automatic fire notification system, fire detector, example of false positive, case study, fire safety warden.*

ABSTRACT

The study found out the cause of false positive and suggested improvement plan for case study for decreasing false positive of automatic fire notification system in Korea. The main cause of false positive was negligence of management of fire safety warden, dust invasion inside of smoke detector, not handling with care of automatic fire notification system of user, not considering installation place of fire detector. For preventing false positive, firstly, fire safety education strengthening for fire safety warden, secondly, providing penalty and intensive for fire safety warden for a thorough inspection of fire protection, thirdly, setting period of use of smoke detector, fourthly, fire safety education & training strengthening of user, lastly, keeping thoroughgoing supervision of fire protection system constructor.

In this study, we have searched for improvement plan after investigating the fundamental cause of malfunction (false operation) visiting to directly to an on-the-spot and surveying with the fire fighting targets as the center that malfunction of the automatic fire notification system of apartment area, factory area, and hospital area in the big cities such as Seoul, Daegu, Gyeongbuk province, and Busan occur frequently from Jan. 5th., 2015 to Jan. 13th., 2015 on the basis of an on-the-spot survey for the purpose of improvement so that all automatic fire notification systems in Korea may be not malfunctioned.

1. Malfunction cases of automatic fire notification systems.

1.1. «A» super high-rise apartment.

In this building the fires have broken out frequently 25 times in 2014 for various reasons why the inadaptable smoke detectors were installed at a location where fall under the influence of strong wind with the target of super high-rise apartment buildings that malfunction of the smoke detector have occurred unusually frequently in 2014 as a 51 storied super high rise apartment building where 288 households dwell in.[1-2]

1.2. «A» factory.

In this building as a factory building that a gross floor area is 72,000 square meters and have 250 employees and manufacture the outer cases, because there are a working area together with welding area where machine equipments are not only operated fully for 24 hours and is full of smoke usually, but also temperature and humidity are high, 8 times malfunctions have been occurred in 2014.

1.3. «B» factory.

In this building as a factory building that a gross floor area is 3000 square meters and have 42 employees and manufacture automotive parts, on account of not only malfunction of a smoke detector due to the fumes of petroleum oil stove in a office within factory, but also on account of a transmitter breakage due to the fault of a forklift driver, 3 times malfunctions of a smoke detector have been occurred in 2014 since completion of factory building.

1.4. «C» factory.

This factory of a factory site of 660–1320 square meters together with 20 other companies are contiguous in an area, and just only one transmitter are connected with 20 smoke detectors of 20 companies, and a firefighting control center is designated to be in charge of fire management. On account of a defective smoke detector, malfunctions of a smoke detector have been occurred 3 times in 2014.[3-4]

1.5. «A» welfare center for the elderly.

As the elderly medical welfare facility that a gross floor area is 1,097 square meters, and the number of persons to be accommodated is 74, and have 16 staffs, this building that 5 and 6 story have been extended have accommodated elderly stroke patients, dementia patients and also senior citizens. By the way, malfunction has been occurred by pressing down a transmitter in the process of a collapse of products that have been stacked aside a transmitter and also malfunction that has been occurred on account of the water leak in alarm check valve have occurred 3 times in 2014.

1.6. «A» hospital.

As a geriatric hospital and nursing home that a gross floor area is 4,300 square meters, and the number of persons to be accommodated is 125, and have 125 staffs and as a building that have been completed in March, 2008, during the sweet potatoes baking in a microwave oven that has been equipped on corridors and wards of every floor of the hospital that the smoke detectors have been equipped, malfunction that has

been occurred because deep smoke flowed into the smoke detector have occurred 2 times in 2014.

1.7. «A» senior care center.

Not only as a in-home care facilities for the elderly that a gross floor area is 1,000 square meters, and the number of persons to be accommodated is 49, and have 15 staffs, but also as a building that have been completed in 1997, malfunctions of a smoke detector has occurred 3 times in 2014 not only because water flowed into a differential smoke detector and area of contact point of a smoke detector was corroded, but also because a fire safety warden opened the smoke detector. [5-6]

2. Cause of malfunction of automatic fire notification system and improvement plan in Korea.

Cause of malfunction of automatic fire notification system and improvement plan that arranged on the basis of an on-the-spot survey for facilities that a lot of malfunctions of the automatic fire notification system are occurred are as follows.

2.1. Negligence of the fire safety warden

Main cause of malfunction is due to carelessness. In case of management for petroleum oil stove, because moisture have flown into a differential detector due to negligence of management of the fire fighting safety warden in

Table 1

Cause of malfunction of automatic fire notification system and improvement plan

Facility name	The number of malfunction yearly	Cause	Improvement plan
«A» Super high-rise apartments	27 times	The lack of consciousness for preservation and caution of user's automatic fire notification system	Reinforcement for user's fire safety education & training
		Non-consideration for installation Environment of the smoke detector	Thoroughgoing supervision against the supervision company for fire-fighting facilities
«A» Factory	8 times	Non-consideration for installation Environment of the smoke detector	Thoroughgoing supervision against the supervision company for fire-fighting facilities.
«B» Factory	3 times	Negligence of management of the fire safety warden	Reinforcement for user's fire safety education & training.
		The lack of consciousness for preservation and caution of user's automatic fire notification system	Reinforcement for user's fire safety education & training.
«C» Factory	3 times	Dust invasion within the smoke detector	Durability period settings of the smoke detector
«A» Welfare center for the elderly	3 times	Negligence of management of the fire safety warden.	Penalty against the fire safety warden or incentive offer.
		The lack of consciousness for preservation and caution of user's automatic fire notification system.	Reinforcement for user's fire safety education & training.
«A» Hospital	2 times	The lack of consciousness for preservation and caution of user's automatic fire notification system.	Strengthening for user's fire safety education & training.
«A» Senior care center	3 times	Negligence of management of the fire safety warden.	Penalty against the fire safety warden or incentive offer.

Data Source: data to be cited from Cheon Il Ryeon etc.(2014) [7]

senior care center, insufficient inspection for fire protection system such as an alarm check valve in «A» welfare center for the elderly, and inadequate education for users, a receiving sensor that receive a sudden signal of fire hazard was malfunctioned. strengthening for user's fire safety education & training that is based on the functional checklist for operation of Korea Fire Safety Association that take charge of practical education so that a receiving sensor that receive a sudden signal of fire hazard may not be malfunctioned is necessary and also penalties and incentives offer against the fire safety wardens so that may inspect thoroughly the fire protection system is necessary. [8]

2.2. Dust invasion within the smoke detector

The malfunctioned cause of the automatic fire notification system in «C» factory was because of dust that have been stacked within the deteriorated smoke detector. Because the internal cleaning within the smoke detector is difficult structurally even though a fire safety warden clean the smoke detector periodically, malfunction occurrence probability is to heighten as time went on after installing the smoke detector. [9] In comparison, in case of Japan, the smoke detector is replaced regularly by designating an maximum durability term of the smoke detector as 10 years. On the contrary, in Korea, durability term criteria of the smoke detector is not designated. [10] Therefore, hereafter the regular replacement of the smoke detector by designating durability term criteria in order to decrease malfunction of the smoke detector.

2.3. The lack of consciousness for preservation and caution of user's automatic fire notification system

On account of smoking at the bottom of a fire protecting shutter in «A» super high-rise apartment, transmitter breakage due to fault of forklift driver in "B" factory and due to the collapsing of products that have been stacked aside a transmitter in «A» welfare center for the elderly, and due to using microwave ovens, the smoke detector and a transmitter that transmit a sudden signal of fire hazard was malfunctioned. It is necessary that strengthen the fire safety education & training that is aimed at consciousness for preservation and caution of user's automatic fire notification system so that the smoke detector or a transmitter are not malfunctioned.

2.4. Non-consideration for installation Environment of the smoke detector

The fraudulent construction work that did not consider an on-site situation of fire-fighting facilities construction corporation cause malfunction of the smoke detector and a transmitter. [11] On account of not only installation of the maladjusted smoke detector and a transmitter that wind effects on a super high-rise apartment were not considered, but also non-installation of the adaptable smoke detector at a place where temperature and humidity within «A» factory are high, malfunction of the automatic fire notification system have been occurred. It is necessary that supervise thoroughgoingly a fire fighting facilities supervision corporation that supervise fire-fighting facilities construction work corporation so that fire-fighting facilities construction work corporation may install the smoke detectors and transmitters suitable to installation environment.

In conclusion, in order to prevent malfunction of the smoke detector and a transmitter, improvement such as safety education that are aimed at fire safety wardens of Korea Fire Safety Association that carry out practical education for fire fight safety and management, penalty and incentive offer for fire safety wardens so as to inspect thoroughgoingly fire fighting facilities, setting up durability term of the smoke detector, reinforcement of fire fighting safety education & training about consciousness for preservation and caution of user's automatic fire notification system, and the thoroughgoing supervision against a fire fighting facilities supervision corporation so as to install the smoke detector suitable to an on-the-spot situation.

References

1. *Lee Bok Young, Jung Kil Sun, Lee Byung Kon* (2003), “A Study on Response Characteristics of Ionization Smoke Detector Influenced by Air Stream”, Journal of Korean Institute of Fire Science & Engineering, Vol. 17, No. 2, pp.6-9.

2. *Park Sang Tae, Lee Bog Young, Ahn Ja Son* (2002), “Experimental Study on the Responsiveness of Ionization Smoke Detector followed by the Change of air currents”, Proceedings of Fall Annual Conference, Korean Institute of Fire Science & Engineering, pp. 164-169.

3. *Hong Sung Ho, Chol Moon Soo, Park Sang Tae, Baek Dong Hyun*(2012), “A Study on the Reliability Test for Smoke Detection Chamber of Smoke Detector”, Proceedings of Spring Annual Conference, Korean Institute of Fire Science & Engineering, pp. 389-392.

4. *Baek Won Don, Kin Shi Kuk, Ok Kyung Jea, Lee Chun Ha, Jee Seung Wook*(2008), “A Study on the Response Characteristics Depending on Service Life of Ionization Smoke Detector”, Journal of Korean Institute of Fire Science & Engineering, Vol. 22, No. 4, pp. 61-64.

5. *Kook Hyeong Ho, Jo Dae Ho, Kong Ha Sung* (2008), “A Study on Efficient Improvement Ways of Fire Protection Management System”, Journal of Korean Institute of Fire Science & Engineering, Vol. 22, No. 1, pp. 115-127.

6. *Kwak Chang Sik, Woo Seong Cheon, Chae Jin*(2010), “The Improvement of the Specific Target for Fire Fighting of Fire Safety Grade System”, , Journal of Korean Institute of Fire Science & Engineering, Vol. 24, No. 2, pp. 167-168.

7. Cheon Il Ryeon etc.(2014), “The Study on Unwanted Alarm and Countermeasure of Fire Detect Receiving System of Automatic Fire Notification System”, Human Resources Development Service of Korea Research Reports, pp. 87-91.

8. Korea Ministry of Government Legislation(2013), “notice about Self-check of Fire Protection System [Form 2]”, Seoul: Korea Ministry of Government Legislation, p. 17.

9. *Son Young Jin, Lee Young ll, Lee Sang Hyeon* (2008), “Research on the Reliability Improvement of Automatic Fire Alarm System”, Journal of Korean Institute of Fire Science & Engineering, Vol. 22, No. 4, pp. 43.

10. Fire Alarm Association in Japan(2009), “Practical Manual of Automatic Fire Detection System: Focus on Fire Detector”, Tokyo: Fire Alarm Association in Japan, pp. 50-70.

11. *Ryu Ho Cheol* (2014), “Analysis on Activation Characteristic of Heat Detectors in a Compartment Fire”, Journal of the Korean Society of Disaster Information, Vol. 10, No. 4, p. 601.

For citation:
Kong Ha Sung. Cause of false positive of automatic fire notification system and improvement plan in Korea. H&ES Research. 2015. Vol. 7. No.3. Pp. 72–75.

ПРИЧИНЫ ЛОЖНЫХ СРАБАТЫВАНИЙ АВТОМАТИЧЕСКОЙ ПОЖАРНОЙ СИСТЕМЫ ОПОВЕЩЕНИЯ И ПЛАНЫ ПО ЕЕ УСОВЕРШЕНСТВОВАНИЮ В КОРЕЕ

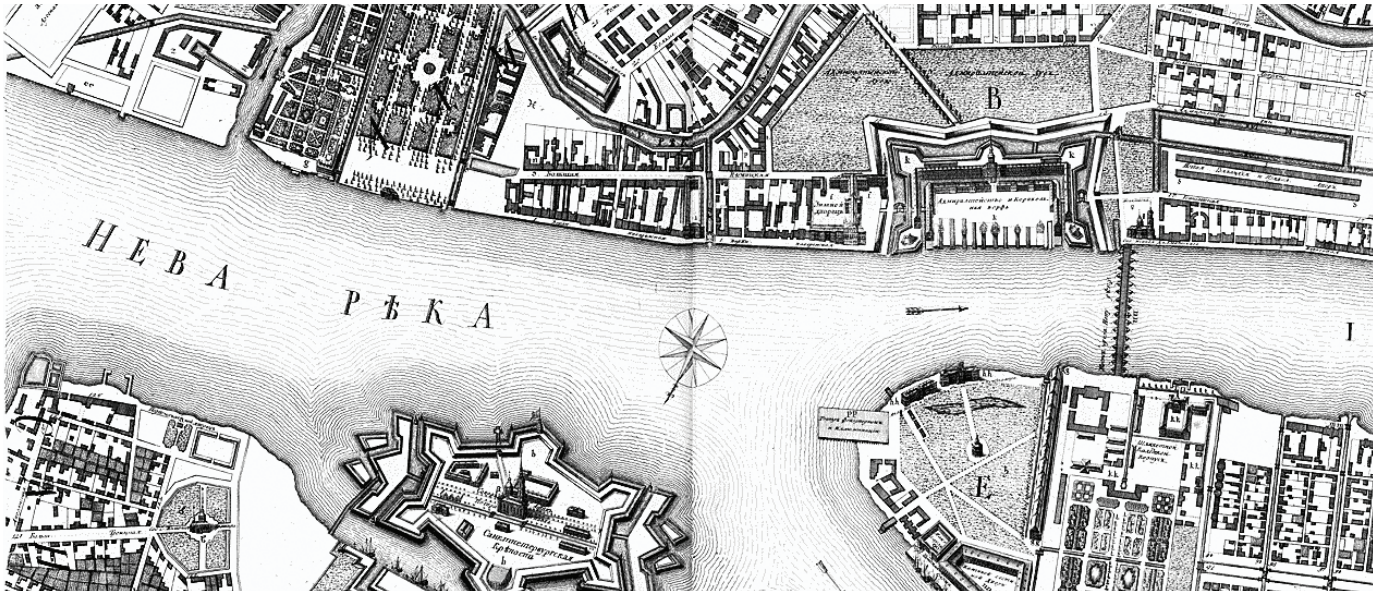
Гон Хасон, г. Сеул, Корея, kiu119@naver.com

Аннотация
Исследование выявило причины ложных срабатываний. Предложен план по усовершенствованию системы для снижения ложных срабатываний при работе автоматической пожарной системы оповещения в Корее.
Основной причиной ложных срабатываний была халатность руководства управления пожарной безопасности, загрязнение внутри детектора дыма, невыполнение профилактических работ по обслуживанию автоматической пожарной системы оповещения пользователя, неверное местоположение датчиков пожарной безопасности. Для предотвращения ложных срабатываний требуется, во-первых, обучение руководства для укрепления пожарной безопасности, во-вторых, наложение штрафных санкций для руководства и проведение тщательного обследования противопожарной защиты, в-третьих, установление срока использования детектора дыма, в-четвертых, проведение обучения и тренингов по пожарной безопасности среди пользователей и, наконец, проведение профилактических работ по поддержанию системы противопожарной защиты в рабочем состоянии.

Ключевые слова: автоматическая пожарная система оповещения, пожарный датчик, пример ложных срабатываний, начальник службы пожарной безопасности.

Информация об авторе:
Гон Хасон, магистр технических наук, доцент, преподаватель Университета Кенил.

Для цитирования:
Гон Хасон. Причины ложных срабатываний автоматической пожарной системы оповещения и планы по ее усовершенствованию в Корее. Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 72–75.



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 Microsoft Equation или Math Type. 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.