Том VII. № 4-2015

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

УЧРЕДИТЕЛЬ:
ООО «Издательский дом Медиа Паблишер»

ГЛАВНЫЙ РЕДАКТОР:
Константин Легков

ИЗДАТЕЛЬ:
Светлана Дымкова

ПРЕДПЕЧАТНАЯ ПОДГОТОВКА:
ООО «H&ES Research»

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

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

Журнал H&ES Research зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия.

ПЛАТА С АСПИРАНТОВ ЗА ПУБЛИКАЦИЮ РУКОПИСИ НЕ ВЗИМАЕТСЯ

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

H&ES Research – один из ведущих рецензируемых научных журналов, в котором публикуются основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук. Журнал освещает достижения и проблемы российских инфокоммуникаций, внедрение последних достижений отрасли в автоматизированных системах управления, развитие технологий в информационной безопасности, исследования космоса, развитие спутникового телевидения и навигации, исследование Арктики. Особое место в издании уделено результатам научных исследований молодых ученых в области создания новых средств и технологий космических исследований Земли.
H&ES Research – научно-технический журнал для специалистов в области современных инфокоммуникационных технологий и автоматизированных систем управления, средств космических исследований Земли и информационной безопасности. В журнале публикуются новости о событиях в вышеуказанных областях, репортажи и интервью ведущих компаний, мнения специалистов, новые технологии, инновационные разработки, оборудование и решения, аналитические статьи, маркетинговые исследования и др.

Журнал входит в систему российского индекса научного цитирования (РИНЦ)

ISSN 2412-1363 (Online)

ISSN 2409-5419 (Print)

Тематика публикуемых статей в соответствии с перечнем групп специальностей научных работников по Номенклатуре специальностей:
- 01.01.00 Математика
- 05.07.00 Авиационная и ракетно-космическая техника
- 05.11.00 Приборостроение, метрология и информационно-измерительные приборы и системы
- 05.12.00 Радиотехника и связь
- 05.13.00 Информатика, вычислительная техника и управление

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

Subject of published articles according to the list of branches of science and groups of scientific specialties in accordance with the Nomenclature of specialties: • 01.01.00 Mathematics • 05.07.00 Aviation, space-rocket hardware • 05.11.00 Instrument engineering, metrology and information-measuring devices and systems • 05.12.00 RF technology and communication • 05.13.00 Informatics, computer engineering and control

H&ES RESEARCH

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

FOUNDER: «Media Publisher», LLC

EDITOR IN CHIEF: Konstantin Legkov

PUBLISHER: Svetlana Dymkova

PREPRESS: «H&ES Research», JSC

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

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

Journal H&ES Research has been registered by the Federal service on supervision of legislation observance in sphere of mass communications and cultural heritage protection. The opinions of the authors don't always coincide with the point of view of the publisher. For the content of ads, the editorial Board is not responsible.

GRADUATE STUDENTS FOR PUBLICATION OF THE MANUSCRIPT WILL NOT BE CHARGED

All authors wishing to post a scientific article in the journal, you must register it according to the requirements and send the materials to your email: HT-ESResearch@yandex.ru. The requirements are available on the website: www.H-ES.ru.

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

WWW.H-ES.RU

HES_Research HES–Research
club55425245

Hi-tech Earth Space RESEARCH

МОБИЛЬНЫЕ ТЕХНОЛОГИИ
ДЛЯ ГОСУДАРСТВА И БИЗНЕСА:
РЕШЕНИЯ ПО БЕЗОПАСНОСТИ

ИНФОФОРУМ
МОБИЛЬНАЯ БЕЗОПАСНОСТЬ

Практическая конференция

- Мобильная безопасность в государственном, корпоративном и массовом секторах
- Риски консьюмеризации и опасности социальных сетей
- Мобильные технологии и преступность: что должен знать пользователь, чтобы защититься
- Защищенная система электронного документооборота на основе мобильных технологий

17•09•2015 | Здание Правительства Москвы
ул. Новый Арбат, 36

Организатор:
Национальный форум
информационной безопасности
«Инфофорум»

infoforum.ru

СОДЕРЖАНИЕ

CONTENTS

Intel и РВК изучат перспективы технического творчества в России

Российская Венчурная Компания (РВК) и корпорация Intel проведут первое исследование цифрового Do-It-Yourself («сделай сам») движения в России. В фокусе внимания – сообщество любителей создания «умных» устройств своими руками и сложившаяся вокруг них экосистема. Применим ли международный опыт к российской действительности? В чем особенности развития отечественного DIY? Организаторы исследования и представители сообщества уверены: российская экосистема имеет серьезный потенциал для развития, но нуждается в стратегической поддержке и самоорганизации.

Intel и РВК объявили о сотрудничестве на первой конференции российских открытых цифровых лабораторий, прошедшей в центре технического творчества Санкт-Петербургского Политехнического университета. Компании представили предварительные данные совместного исследования – обзор мировых практик и первичный анализ российской экосистемы, выполненные компанией «Делойт»*. Итоги проекта, состоящего из нескольких этапов, будут представлены в ноябре текущего года.

Первая конференция цифровых лабораторий, организованная Санкт-Петербургским политехническим университетом, собрала вместе 35 центров молодежного инновационного творчества из 15 городов России. Обсуждение промежуточных выводов исследования с участниками конференции стало важным этапом исследовательского проекта и показало, что представителей экосистемы объединяет общее видение дальнейших путей развития, целей, задач и открытых вопросов, требующих новых форматов взаимодействия.

Итогом конференции стало решение о создании первой в России Ассоциации цифровых лабораторий. Учреждение Ассоциации открытых лабораторий позволит объединить проектные и методические наработки лабораторий и ляжет в основу дальнейшего развития института фаблабов в России. Планируется, что в наблюдательный совет Ассоциации войдут представители РВК, Сколково, Ассоциации инновационных регионов России, Intel и других ведущих российских и международных компаний, активно поддерживающих развитие и популяризацию технического творчества в России.

Современная ИТ-индустрия с интересом наблюдает за ускоряющимся развитием цифровой субкультуры DIY. Как показал предварительный этап исследования, в мире насчитывается порядка 3500 активных сообществ в сфере изобретательства и технического творчества, каждое из которых объединяет в среднем 400 участников и может выпускать от 20 до 30 продуктов в год. Число инновационных производственных лабораторий формата Fab Lab в мире за 2013-2015 годы выросло в 3,5 раза (с 146 до 508) и продолжает расти. Потенциальный объем рынка в данной сфере в 2015 году составит по разным оценкам до 29 млрд долларов, что объясняет заинтересованность крупных представителей ИТ-индустрии в этом направлении.

Деятельность сообществ технических энтузиастов является предметом поддержки со стороны государств, стремящихся достичь или сохранить лидирующие позиции в промышленности и технологиях. В США, Китае, Великобритании, Индии, Пакистане, Бразилии и других странах разработаны стратегии и целевые программы оказания финансовой и иной помощи инноваторам. Только в США суммарный размер грантов, предоставляемых техническим энтузиастам, составляет более 2.5 млрд. долларов. Движение «Сделай сам» (Do-It-Yourself) сегодня – это перспективный рынок и источник человеческого капитала, знаний и компетенций в области практического применения новых технологий.

Как отмечают Intel, РВК и представители российских ЦМИТов, на текущем этапе критически важно обратить внимание индустрии и государства на ключевые точки роста: подготовку и привлечение квалифицированных специалистов и менторов, предоставление доступа к современному оборудованию, популяризацию и информационную поддержку технического творчества, а также выработку стратегического подхода к поддержке технического творчества на федеральном и региональном уровнях – эта задача и станет ключевой для новой Ассоциации. РВК и Intel продолжат исследование и проведут специальное экосистемное мероприятие в конце года, где участники сообщества обсудят итоги проекта, а также прогресс по ключевым направлениям взаимодействия.

XI «Инфофорум-Евразия/Крым»

6–10 июля в Севастополе состоялся 11-й Евразийский форум информационной безопасности и информационного взаимодействия «ИНФОФОРУМ ЕВРАЗИЯ/КРЫМ». Форум традиционно собрал на одной площадке ведущих специалистов в области информационной безопасности из Российской Федерации и зарубежных стран для обсуждения актуальных вопросов международной информационной безопасности и построения безопасного информационного пространства в Российской Федерации и евразийском регионе.

Организаторы форума: Комитет Государственной Думы ФС РФ по безопасности и противодействию коррупции, Некоммерческое партнерство Национальный форум информационной безопасности «ИНФОФОРУМ», при поддержке и участии Аппарата полномочного представителя Президента РФ в Крымском федеральном округе, Аппарата Совета Безопасности РФ; МВД России; ФСБ России, МИД России, Организации договора о коллективной безопасности, Правительства Севастополя, Правительства Республики Крым.

Форум собрал на одной площадке более 300 участников – представителей регуляторов отрасли, федеральных и региональных органов власти, ведущих ИТ- и телекоммуникационных компаний, учреждений науки и образования, общественных организаций.

По региональной составляющей большинство участников представляли различные организации Крымского федерального округа. И это не случайно, ведь одной из главных задач форума было содействие в решении вопросов обеспечения информационной безопасности в ходе продолжающейся интеграции Крыма и РФ.

Также в работе форума приняли участие представители Волгоградской области, Кемеровской области, Самарской области, Республики Коми, Республики Саха (Якутия), Республики Северная Осетия – Алания, Ростовской области, Московской области, Приморского края, Ярославской области, и других регионов.

На повестку Инфофорума в Крыму были вынесены следующие темы:

международное сотрудничество в области кибербезопасности,

безопасность в Интернете: создание государственного сегмента Сети в России,

устойчивость и безопасность сетей связи общего пользования на территории регионов Крыма,

обеспечение информационной безопасности в организациях и на предприятиях и перспективы импортозамещения,

задачи подготовки кадров в области ИБ для нужд Крыма и Севастополя.

Информационная безопасность на международном уровне

Кибервойны становятся реальностью в наши дни. На данный момент около 150 стран мира проводят активные эксперименты в области ведения кибервойн, что может привести к серьезным последствиям. И поэтому вопросы информационной безопасности на международном уровне приобретают особую важность.

Специальный представитель Президента РФ по вопросам международного сотрудничества в области информационной безопасности Андрей Крутских в своем выступлении отметил, что мировому сообществу необходимо договориться об использовании информационно-коммуникационных технологий. По его словам, Россия выработала основные принципы ИКТ-политики. «Базовые основы нашей информационной политики подразумевают, прежде всего, наличие суверенного права каждого государства распоряжаться информационно-коммуникационной инфраструктурой на своей территории и возможность определять политику в сфере информационной безопасности. Второй основной принцип – информационно-коммуникационные технологии могут использоваться только в мирных целях, а не для ведения войны», пояснил Андрей Крутских.

Спецпредставитель Президента также отметил, что данные базовые принципы информационной политики, предложенные Россией, были одобрены экспертами ООН и будут представлены на генеральной ассамблее. «Мы заставили западников пойти на нашу концепцию и доклад на уровне экспертов был принят консенсусом», сказал Андрей Крутских.

В рамках недавнего саммита БРИКС было заключено соглашение о сотрудничестве в области информационной безопасности. Ранее подобное соглашение было заключено странами ШОС. Таким образом, подчеркнул Андрей Крутских, «две трети мира будет связано с Россией одной логикой предотвращения кибервойны».

Кроме этого, стоит напомнить, что в мае Россия заключила уникальное соглашение с Китаем в области сотрудничества по обеспечению международной информационной безопасности. «На очереди еще ряд соглашений, в том числе с западными странами», подытожил Андрей Крутских.

По итогам встречи были намечены шаги по развитию программы «Инфофорум – для регионов России»: создание рейтинга проблем обеспечения информационной безопасности в регионах Российской Федерации и организация стажировок представителей региональных администраций в федеральных органах власти и ведущих ИТ-компаниях.

***

По итогам 11-го Евразийского форума информационной безопасности и информационного взаимодействия «Инфофорум-Евразия/Крым» будет сформирован пакет предложений и рекомендаций по рассмотренным в рамках форума вопросам, который будет направлен в Государственную Думу и органы исполнительной власти.

Пресс-служба Инфофорума.

Подготовлено по материалам ИА «КрымИнформ», ИА «ТАСС», пресс-службы Федерального агентства связи.

Цифровизация российского ТВ-парадоксы, закономерности, прогнозы

В последние несколько лет драйвером роста отрасли платного ТВ является цифровое ТВ. Явное преимущество новых технологий (IPTV, OTT), повсеместная доступность спутникового ТВ, удешевление оборудования цифрового ТВ, а также предоставляемая многими операторами возможность его аренды либо бесплатного использования – все эти факторы способствуют снижению числа аналоговых подключений и активному росту спроса на услуги цифрового вещания.

В ходе опроса операторов платного телевидения, проведённом аналитиками iKS-Consulting при поддержке журнала «Кабельщик» большинство респондентов – 86% – назвали HD наиболее востребованной технологией сегодняшнего телевидения, в то время, как время активного использования 4K и 3D технологии по мнению большинства придёт лишь лет через 5–7 лет.

Проанализировав ответы всех респондентов, принявших участие в этом опросе, iKS-Consulting составил рейтинг востребованности современных ТВ-форматов, где технологиям, получившим максимальное предпочтение в каждой из анкет, присваивался коэффициент 3, наименее конкурентоспособным – 1. Результаты данного ранжирования представлены на рис.1.

Однако, несмотря на растущую популярность цифровых форматов, о полном отказе от аналогового вещания говорить еще рано. По данным iKS-Consulting, к концу 2014 года услугами цифрового ТВ воспользовались 59% от общего числа абонентов платного ТВ.

Согласно результатам вышеупомянутого анкетирования iKS-Consulting и журнала «Кабельщик», в 2014 году за количество аналоговых каналов в базовом пакете операторов ТВ-контента не сократилось, а выросло – в среднем на 21% по отношению к 2013 году, что на фоне общего роста числа используемых в России ТВ-каналов на уровне 42% выглядит весьма внушительно. Лидером в этой «гонке» снова стала HD-технология – ее доля в базовом пакете выросла за год на 67%, тогда как количество подключений цифровых каналов увеличилось на 53%.

Очевидно, что эволюция ТВ-технологий набирает обороты, но процесс этот протекает гораздо медленнее, чем представлялось 3–4 года назад, что и послужило одной из причин переноса полного отказа от аналоговой технологии вещания на конец 2018 г. Подтверждением тому, что это решение оправданно, является тот факт, что при гипотетической доступности цифрового эфирного вещания почти двум третям телевизионных домохозяйств России, реальное количество тех, кто пользуется цифровым эфиром, оценивается в чуть более 10% общей численности телевизионных домохозяйств: до сих пор сказывается отсутствие ресиверов и низкий процент обновления парка телевизоров (рис. 2.1, 2.2).

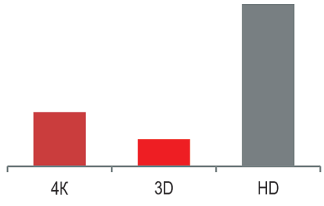


Рис.1. Рейтинг востребованности ТВ-форматов

Оценивая влияние кризиса на рынок ТВ-потребления, iKS-Consulting и журнал «Кабельщик» попросили участников опроса прогнозировать изменение стоимости конечного оборудования в ближайшей перспективе. Подавляющее большинство не реализуем респондентов (75%) предположили, что оно будет дорожать, однако сценарии этого подорожания получили равное число голосов.

Примерно такое же количество (78% респондентов) предположило, что в условиях финансового кризиса не удастся избежать удорожания абонентского обслуживания (рис. 3.1, 3.2).

В условиях недостаточного прогресса цифрового эфирного телевещания, а также низкого уровня цифровизации в лидером цифровизации в России стал сегмент спутникового телевещания, как платного, так

Рис. 2.1. Телевизионные домохозяйства России в разрезе цифровойи аналоговой платформ, 2007–2014 (млн.)

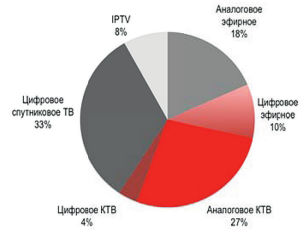


Рис. 2.2. Распределение телевизионных домохозяйств России по типу подключения, 2014 (млн.)

и бесплатного: согласно оценкам iKS-Consulting, на данный сегмент приходится порядка 67% всех цифровых телевизионных домохозяйств страны.

Между тем, как показало специальное исследование iKS-Consulting, количество HD-каналов в базовых пакетах операторов связи растёт куда более активными темпами, чем объём трансляций по цифровой-технологии, хотя на данный момент их количество на порядок меньше.

Самым быстрорастущим сегментом цифрового ТВ является цифровое кабельное ТВ, в котором численность абонентов за год увеличилась более чем на 40%. Связано это, прежде всего, с усилиями игроков по цифровизации своей базы аналогового ТВ, позволяющей, в том числе, увеличить и доходность с одного абонента. Однако, несмотря на бурный рост, на этот сектор рынка цифрового ТВ приходится лишь 14% абонентов. Большую же часть рынка цифрового ТВ занимают спутниковые операторы, которых на текущий момент осталось четыре: «Триколор ТВ», «Орион Экспресс», «НТВ-Плюс» и недавно запустившийся МТС.

Примечательно, что, согласно опросу iKS-Consulting, большинство

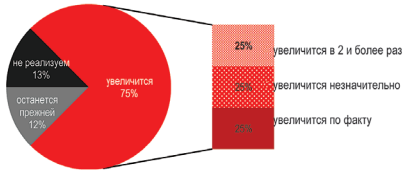


Рис. 3.1. Как будет меняться стоимость конечного оборудования?

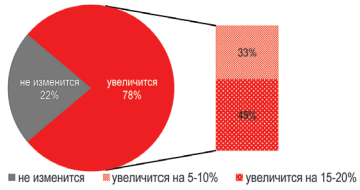


Рис. 3.2. Как изменится абонентская плата?

по-прежнему не пользуется платным контентом вне подписки на услуги платного ТВ. В частности, 63% респондентов подключены к операторам платного ТВ (кабельным, спутниковым и IPTV) – эти данные коррелируются с показателями проникновения платного ТВ среди городского населения. При этом практически у 2/3 пользующихся услугой платного ТВ к ней подключено несколько (более одного) устройств. В среднем же к услуге подключены 2,1 телевизора – следствие того, что большинство операторов платного ТВ предлагают сегодня такой сервис, как multiroom – возможность подключения к услуге нескольких телевизоров в одной квартире (рис. 4).

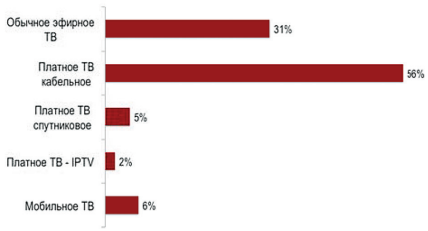


Рис. 4. Какими из следующих услуг вы пользуетесь?

В разрезе используемых устройств наименьший удельный вес респондентов, не пользующихся услугами платного видео-контента, наблюдается среди пользователей планшетных компьютеров – 84% опрошенных против 93% опрошенных в среднем. В целом пользователи мобильных устройств, а также смарт-телевизоров, в большей степени готовы платить за видеоконтент, чем пользователи обычных телевизоров и компьютеров. Ведущая роль спутникового телевидения в процессе цифровизации в России сохранится и в перспективе, причем доля спутниковых подключений будет постоянно увеличиваться. Даже полное отключение аналогового вещания мало изменит сложившуюся конфигурацию – цифровое эфирное телевидение приостановит дальнейшую экспансию спутникового ТВ, однако не развернет ее вспять: опыт стран, уже перешедших на цифровое эфирное телевещание, показывает, что массовой миграции абонентов платных цифровых сервисов в формат DTT не происходит (рис.5).

Участники опроса iKS-Consulting и журнала «Кабельщик» примерно поровну разделились во мнениях относительно вероятности оттока абонентов в строну операторов OTT-сервисов (рис.6).

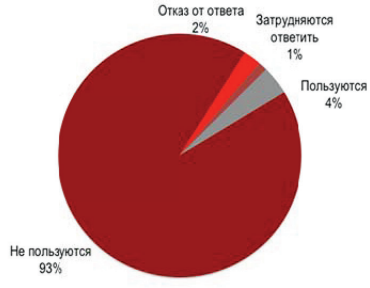
Говоря о развитии цифровых сервисов в России, надо принимать во внимание тот факт, что до сих пор существует достаточно сильная разница в проникновении услуг платного ТВ в разрезе федеральных округов, что обусловлено следующими факторами:

- Наличие или отсутствие в регионе крупных городов с развитой кабельной инфраструктурой
- Полнота охвата спутниковым вещанием в том или ином регионе
- Различия в уровне экономического развития регионов.

Лидерами являются Центр и Северо-Запад: наряду с высоким проникновением темпы прироста здесь меньше, чем в остальных регионах. Быстрее всего численность абонентов платного ТВ увеличивается на рынках Сибири, Дальнего Востока и Юга, поскольку здесь проникновение еще не соответствует среднероссийскому и остается большой потенциал для роста.

Объемы подключения цифрового ТВ растут во всех регионах страны. На Юге наблюдается самое высокое проникновение данной услуги, так как в ЮФО преобладают спутниковые операторы. Самое низкое проникновение цифрового ТВ наблюдается в Сибири. Центральный регион занимает самую большую долю по абонентам цифрового ТВ и по объему выручки от услуги. Рынок здесь формируется в основном крупными операторами («Ростелеком», «Вымпелком», МТС, «Акадо»), которые не практикуют демпинг (рис. 7).

Более высокий, чем в Центре, ARPU имеет место только на Дальнем Востоке. На Юге доходность на абонента – самая низкая.



* не считая платного ТВ

Рис. 5. Пользуетесь ли вы платными сервисами, связанными с видео-контентом? (города России,2013)*

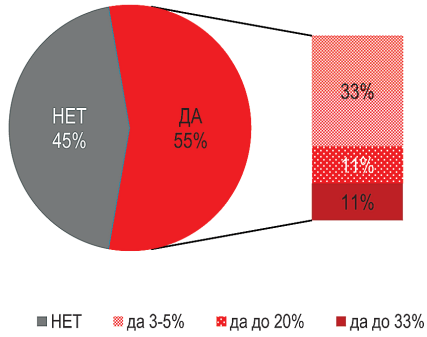


Рис. 6. Следует ли ожидать оттока абонентов в сторону OTT сервисов?

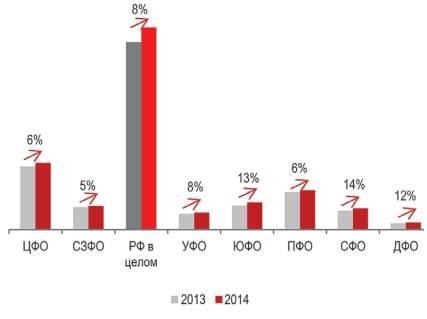


Рис. 7. Темпы роста рынка платного ТВ по ФО, 2014

ИССЛЕДОВАНИЕ ПОТЕНЦИАЛЬНОЙ ПОМЕХОУСТОЙЧИВОСТИ НЕКОГЕРЕНТНОГО ОПТИЧЕСКОГО ЦИФРОВОГО КАНАЛА СВЯЗИ

Федоров
Сергей Евгеньевич,
к.т.н., профессор,
профессор Московского технического университета связи и информатики,
г. Москва, Россия,
fedorovse1@yandex.ru

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

АННОТАЦИЯ

Дана постановка задачи различения оптических цифровых сигналов, сформированных на конечном интервале времени оптическим передатчиком с некогерентным светоизлучающим диодом, применение которого эффективно для волоконно-оптических каналов в автоматизированных системах управления с относительно малой протяженностью кабельных линий связи и с высокими эксплуатационно-техническими требованиями по надежности в сложных условиях их эксплуатации.

При постановке задачи различения оптических цифровых сигналов использовано векторное представление наблюдаемого фотонного процесса, что позволило связать форму сигналов с вероятностным распределением чисел фотонов и фотоэлектронов по модам наблюдаемого процесса. Такой подход позволил найти структуру оптимального приемника, реализующего прием «в целом» в отличие от ранее использованных подходов оптимизации каналов при посимвольном приеме цифровых оптических сигналов.

Для оптического цифрового канала связи с некогерентным источником излучения синтезирован по критерию минимума средней вероятности ошибки оптимальный приемник ортогональных сигналов в усиленном смысле.

Найдено выражение для минимальной средней вероятности ошибки оптимального приема цифровых сигналов исследуемого канала, что позволило определить квантовый предел помехоустойчивости цифрового канала с некогерентной оптической несущей.

Показано, что при переходе исследуемого оптического канала связи в классический канал с гауссовыми ортогональными сигналами полученное выражение для квантового предела помехоустойчивости совпадает с известным в классической теории потенциальной помехоустойчивости выражением для средней вероятности ошибки оптимального приема ортогональных гауссовых сигналов на фоне белого гауссова шума.

При этом подтверждена достоверность полученного аналитического выражения для квантового предела помехоустойчивости исследуемого оптического канала с некогерентным источником излучения.

В качестве практического приложения полученных результатов рассматриваются современные автоматизированные системы управления, для которых достаточно эффективно применение волоконно-оптических каналов со светоизлучающими диодами, которые отличаются от лазерных источников простотой конструкции, высокой надежностью, слабой зависимостью характеристик излучения от температуры и линейной зависимостью выходной оптической мощностью от тока накачки, а также низкой стоимость.

Современный процесс автоматизации технологических процессов и производств предусматривает широкое внедрение автоматизированных систем управления, что приводит к задаче обеспечения передачи и приема больших потоков информации по физическим каналам связи с высокой помехоустойчивостью, надежностью их функционирования и высоким уровнем защиты информации.

Для обеспечения этих технических требований перспективны волоконно-оптические каналы связи, реализующие их потенциальные информационные возможности. Для автоматизированных систем управления с относительно малой протяженностью кабельных линий связи и с высокими эксплуатационно-техническими требованиями, прежде всего, по надежности в сложных условиях эксплуатации, достаточно эффективно применение волоконно-оптических каналов со светоизлучающими диодами.

Действительно, некогерентные источники оптического излучения – светоизлучающие диоды выгодно отличаются от лазерных источников простотой конструкции, высокой надежностью, слабой зависимостью характеристик излучения от температуры и линейной зависимостью выходной оптической мощностью от тока накачки, а также низкой стоимостью [1,2].

При этом в научно-технической литературе [1-4] крайне ограниченно освещены вопросы оценки потенциальной помехоустойчивости оптических каналов с некогерентным оптическим излучателем. Данная работа восполняет ряд пробелов теории потенциальной помехоустойчивости оптических цифровых каналов с учетом квантовой природы некогерентного оптического излучения.

Рассмотрим задачу различения $M<\infty$ равновероятных сигналов, сформированных на конечном интервале времени $[t_0, t_0+T]$ оптическим передатчиком с некогерентным излучателем. Сигналы представим в следующем виде:

$$s_i(t) = S_i(t) \exp(i\omega_0 t) \quad (1)$$

где $S_i(t)$ – комплексная огибающая узкополосного гауссовского процесса со средней частотой ω_0. Все сигналы с равной энергией и нормированы таким образом, что среднее число сигнальных фотонов на интервале $[t_0, t_0+T]$

$$N_s = M_0 \int_{t_0}^{t_0+T} |S_i(t)|^2 dt, \quad i = \overline{1, M}, \quad (2)$$

где знак M_0 означает математическое ожидание.

Среднее значение огибающих сигналов

$$M_0[S_i(t)] = 0, \qquad i = \overline{1, M}, \quad (3)$$

а ширина их спектров ограничена полосой частот F_c.

Прием сигналов проводится на фоне аддитивного гауссова шума

$$u(t) = U(t) \exp(i\omega_0 t)$$

с нулевым средним значением и комплексной огибающей $U(t)$ с шириной спектра $F_ш > F_c$. Среднее число шумовых фотонов $N_ш$ на интервале времени $[t_0, t_0+T]$

$$N_ш = M_0 \int_{t_0}^{t_0+T} |U(t)|^2 dt,$$

Сигналы $s_i(t)$, $i = \overline{1, M}$ и шум статистически независимы.

Принимаемую оптическую аддитивную смесь сигнала и шума представим в виде

$$y(t) = A(t) \exp(i\omega_0 t),$$

где комплексная огибающая принимаемого случайного процесса имеет вид

$$A(t) = S_i(t) + U(t), \qquad i = \overline{1, M}.$$

Для исследуемого канала с некогерентным излучателем синтезируем оптимальный, в байесовском смысле, приемник ортогональных, в усиленном смысле, оптических сигналов $s_i(t)$, $i = 1, M$, для которых выполняется условие

$$\lambda_{ij} = \frac{1}{N_s} \int_{t_0}^{t_0+T} S_i(t) S_i^*(t)\, dt = 0, \quad i \neq j;\ i, j = \overline{1, M}. \quad (4)$$

Здесь знак * означает комплексную сопряженность.

Множество ортогональных сигналов, определенное выражением (4), как показано автором в работе [5], является оптимальным по критерию минимума средней вероятности приема сигналов и обеспечивает минимум средней вероятности ошибки оптимального приема $P^0_{ош}$ произвольных по форме $M<\infty$ некогерентных оптических сигналов $s_i(t)$, $i = \overline{1, M}$, заданных выражениями (1) – (3).

Нахождение этого минимума средней вероятности ошибки оптимального приема ортогональных сигналов определяет потенциальную помехоустойчивость оптического цифрового канала с некогерентным излучателем, что является основной целью данного исследования.

Синтез оптимального приемника

Для оптического канала связи с некогерентным источником излучения синтезируем по критерию минимума средней вероятности ошибки оптимальный приемник ортогональных сигналов в усиленном смысле, что позволит в дальнейшем определить квантовый предел помехоустойчивости цифрового канала с некогерентным оптическим излучателем.

Для этого с использованием результатов работы [5] определим среднее число шумовых фотонов в каждой

из M ортонормированных мод разложения огибающей A(t), в виде

$$N_{\text{ш}j} = M_0 [\,|u_j|^2\,], \quad j = \overline{1, M}.$$

В силу равномерности спектральной плотности мощности шума число шумовых фотонов в каждой из M мод одинаковое:

$$N_{\text{шп}} = N_{\text{ш}j}, \quad j = \overline{1, M}.$$

При передаче ортогонального сигнала $s_i(t)$, $i=\overline{1, M}$, число фотоэлектронов, инициируемое i-ой ортогональной модой, согласованной с i-м сигналом, определяется распределением Бозе-Эйнштейна вида

$$P_s(k_i \,|\, s_i) = (1 - v_s)\, v_s^{k_i}, \quad i = \overline{1, M}, \tag{5}$$

где

$$v_s = \frac{\alpha N_S + \alpha N_{\text{шп}}}{\alpha N_S + \alpha N_{\text{шп}} + 1},$$

где $P_s(k_i \,|\, s_i)$ – вероятность наблюдения k фотоэлектронов в i-ой моде, а коэффициент α определяет квантовую эффективность фотодетектора.

В каждой из M – 1 остальных мод содержатся только шумовые фотоны, поэтому число инициируемых ими шумовых фотоэлектронов подчиняется распределению Бозе-Энштейна вида:

$$P_{\text{ш}}(k_n) = (1 - v_{\text{ш}})\, v_{\text{ш}}^{k_n}, \quad n \neq i, \tag{6}$$

$$v_{\text{ш}} = \frac{\alpha N_{\text{шп}}}{\alpha N_{\text{шп}} + 1}.$$

Функция правдоподобия для некогерентных ортогональных сигналов с учетом выражений (5) и (6) и на основании результатов работы [5], можно представить в следующем виде:

$$P(k_1, k_2, \ldots, k_M | s_i) = \\ = (1 - v_s)\, v_s^{k_i} (1 - v_{\text{ш}})^{M-1} \prod_{n \neq i}^{M} v_{\text{ш}}^{k_n}. \tag{7}$$

Отсюда получим отношение правдоподобия для сигналов $s_i(t)$ и $s_j(t)$ в виде

$$\frac{P(k_1, k_2, \ldots, k_M | s_i)}{P(k_1, k_2, \ldots, k_M | s_j)} = \left(\frac{v_s}{v_{\text{ш}}}\right)^{k_i - k_j}, \quad i \neq j.$$

С учетом того, что $v_s > v_{\text{ш}}$ при любых значениях N_S и $N_{\text{шп}}$ следует достаточно очевидный вывод. Максимум функции правдоподобия $P(k_1, k_2, \ldots, k_M \,|\, s_i)$ для i-го сигнала достигается при максимальном числе фотоэлектронов, инициируемых i-ой модой.

Таким образом синтезирован оптимальный оптический приемник M ортогональных в усиленном смысле сигналов, заданных на конечном интервале времени длительностью T. Алгоритм работы приемника основан на счете числа фотоэлектронов, инициируемых каждой ортогональной модой, например, на каждом из неперекрывающихся подинтервалах длительностью $\tau = \frac{T}{M}$, и выборе того сигнала, номер которого равен номеру моды – номеру подинтервала, где число фотоэлектронов максимально. В случае неединственности максимума решение может быть произвольное, в том числе рандомизированное.

Квантовый предел помехоустойчивости канала связи

Теперь определим квантовый предел помехоустойчивости цифрового канала с некогерентным оптическим излучателем. Для этого заметим, что средняя вероятность правильного приема равновероятных ортогональных сигналов

$$P^0_{\text{пр}} = 1 - P^0_{\text{ош}} = \frac{1}{M} \sum_{i=1}^{M} P\{a_i | s_i\},$$

где $P\{a_i \,|\, s_i\}$ – условная вероятность правильного решения a_i при условии, что передан сигнал $s_i(t)$. При этом в силу равноудаленности ортогональных сигналов с равным средним числом сигнальных фотонов, определенным выражением (2), можно записать

$$P^0_{\text{пр}} = P\{a_i \,|\, s_i\}, \quad i = \overline{1, M}.$$

Для определенности будем полагать, что передавался сигнал $s_1(t)$. Тогда средняя вероятность правильного приема ортогональных сигналов синтезированным оптическим приемником может быть представлена в виде

$$\begin{aligned} P^0_{\text{пр}} &= M_0 \Big\{ P[k_i < k_1, i = \overline{2, M}] \\ &+ \frac{1}{2} C^1_{M-1} P[k_1 = k_2; \quad k_i < k_1, i = \overline{3, M}] \\ &+ \frac{1}{3} C^2_{M-1} P[k_1 = k_2 = k_3; \quad k_i < k_1, i = \overline{4, M}] \\ &+ \frac{1}{M} C^{M-1}_{M-1} P[k_1 = k_2 = k_3 = \cdots = k_M] \Big\}. \end{aligned} \tag{8}$$

Здесь $M_0\{*\}$ – математическое ожидание относительно распределения случайной величины k_1, которое определено выражением (4); $P[*]$ – условная вероятность при фиксированном числе фотоэлектронов k_1; $C_{M\text{-}1}$ – коэффициент, являющийся числом сочетаний, равным числу способов, которым можно выбрать n мод с k_1 фотоэлектронами из M – 1 мод, инициирующих только шумовые фотоэлектроны.

Заменяя для упрощения записи k_1 на k и замечая, что для одной моды

$$P(k_i < k) = \sum_{i=0}^{k-1} P_{\text{ш}}(l) = 1 - v_{\text{ш}}^k, \qquad i = \overline{2, M},$$

представим выражение для средней вероятности правильного приема (7) в следующем виде:

$$P_{\text{пр}}^{0} = M_0 \left\{ (1 - v_{\text{ш}}^{k})^{M-1} + \frac{1}{2} C_{M-1}^{1} P_{\text{ш}}(k)(1 - v_{\text{ш}}^{k})^{M-2} + \frac{1}{3} C_{M-1}^{2} P_{\text{ш}}^{2}(k)(1 - v_{\text{ш}}^{k})^{M-3} + \cdots + \frac{1}{M} C_{M-1}^{M-1} P_{\text{ш}}^{M-1}(k) \right\}. \quad (9)$$

Используя выражение (6) и формулу бинома Ньютона, выражение (9) можно преобразовать к виду

$$P_{\text{пр}}^{0} = \frac{1}{M(1 - v_{\text{ш}})} M_0 \left\{ \sum_{l=1}^{M} (-1)^{l} C_{M-1}^{l} (v_{\text{ш}}^{l} - 1) v_{\text{ш}}^{k(l-1)} \right. \quad (10)$$

Вычисляя математическое ожидание в выражении (10) относительно распределения числа фотоэлектронов (5), можно получить

$$P_{\text{пр}}^{0} = \frac{1}{M} \frac{1 - v_s}{1 - v_{\text{ш}}} \sum_{l=1}^{M} (-1)^{l} C_{M}^{l} \frac{v_{\text{ш}}^{l} - 1}{1 - v_s v_{\text{ш}}^{l-1}}.$$

Отсюда искомая минимальная средняя вероятность ошибки представляется в виде

$$P_{\text{ош}}^{0} = \frac{1}{M} \frac{1 - v_s}{1 - v_{\text{ш}}} \sum_{l=2}^{M} (-1)^{l} C_{M}^{l} \frac{1 - v_{\text{ш}}^{l}}{1 - v_s v_{\text{ш}}^{l-1}}. \quad (11)$$

Выводы

Таким образом, для оптического цифрового М-ичного канала с некогерентным излучателем синтезирован по критерию минимума средней вероятности ошибки оптимальный приемник ортогональных в усиленном смысле сигналов и получено аналитическое выражение (11), определяющее квантовый предел помехоустойчивости приема цифровых сигналов.

Полученный квантовый предел помехоустойчивости позволяет оценить потенциальную помехоустойчивость цифрового волоконно-оптического канала с некогерентным излучателем, например, со светоизлучающим диодом.

Следует отметить, что при $N_{\text{шп}} \gg 1$ исследуемый оптический канал связи переходит в классический канал с гауссовыми ортогональными в усиленном смысле сигналами, различаемыми на фоне белого гауссова шума. Действительно, в этом случае

$$v_{\text{ш}}^{l} = \left(1 - \frac{1}{\alpha N_{\text{шп}} + 1}\right) \approx 1 - \frac{1}{\alpha N_{\text{шп}}},$$

а отношение сигнал/шум

$$\frac{N_s}{N_{\text{шп}}} = \frac{E_s}{N_0},$$

где E_s – энергия сигналов; N_0 – односторонняя спектральная плотность мощности белого шума. В результате выражение (11) преобразуется в известное в классической теории потенциальной помехоустойчивости [6,7] выражение

$$P_{\text{ош}}^{0} = \frac{1}{M} \sum_{l=2}^{M} (-1)^{l} C_{M}^{l} \left[(l-1) \frac{E_s}{N_0} - l \right]^{-1}$$

для средней вероятности ошибки оптимального приема М ортогональных гауссовых сигналов на фоне белого гауссова шума. Этот предельный переход подтверждает достоверность найденного квантового предела помехоустойчивости исследуемого оптического канала.

Литература

1. Фриман Р. Волоконно-оптические системы связи / Пер. с англ. М.: Техносфера. 2006. 496 с.

2. Бейли Д., Эдвин Р. Волоконная оптика: Теория и практика / Пер. с англ. М.: КУДИЦ-ОБРАЗ. 2006. 320 с.

3. Гауэр Дж. Оптические системы связи / Пер. с англ. М.: Радио и связь. 1989. 504 с.

4. Гальярди Р.М., Карп Ш. Оптическая связь. Связь. 1978. 424с.

5. Федоров С.Е. Синтез оптического цифрового канала связи для автоматизированных систем управления // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 2. С. 48–52.

6. Финк Л.М. Теория передачи дискретных сообщений. Изд. 2-е, перераб., доп. М.: Советское радио. 1970. 728 с.

7. Коржик В.И., Финк Л.М. Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. М.: Связь. 1975. 272 с.

Для цитирования:

Федоров С.Е. Исследование потенциальной помехоустойчивости некогерентного оптического цифрового канала связи // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 10–14.

STUDY OF POTENTIAL NOISE INCOHERENT OPTICAL DIGITAL COMMUNICATION CHANNEL

Fedorov Sergey Evgenevich,
Moscow, Russian,
fedorovse1@yandex.ru

Abstract
The formulation problem of distinguishing an optical digital signal generated on a finite time interval optical transmitter with non-coherent light emitting diode, the use of which effectively for fiber optic channels in automated control systems with a relatively small length of cable communication lines and high operational and technical requirements for reliability under difficult operating conditions.
In formulating the problem of distinguishing optical digital signals used vector representation of the observed photon process, allowing to bind a form of signals with probabilistic distribution of the numbers of photons and photoelectrons according to the fashion of the monitored process. This approach allowed us to find the structure of the optimal receiver that implements the admission in large in contrast to the previously used approaches of optimization of character-by-character channels when receiving digital optical signals.
For optical digital communication channel with non-coherent source of radiation synthesized according to the criterion of minimum average error probability of the optimal receiver orthogonal signals in the strong sense.
The obtained expression for the minimum average error probability for optimal reception of digital signals channels that allowed us to determine the quantum limit of noise immunity of the digital channel with non-coherent optical carrier.
It is shown that the transition of the investigated optical communication channel in the classical Gaussian channel with orthogonal signals obtained an expression for the quantum limit of noise immunity coincides with the known in the classical theory of potential noise immunity expression for the average probability of error for optimal reception of orthogonal Gaussian signals in white Gaussian noise.
This confirmed the accuracy of the analytical expressions for the quantum limit of noise immunity of the investigated optical channel with non-coherent radiation source.
As a practical application of the obtained results are considered modern automated control systems, which is enough for effective use of fiber-optic channels with light-emitting diodes, which are different from laser sources, simplicity of design, high reliability, a weak dependence of the emission characteristics on the temperature and the linear dependence of the output optical power from the pump current, and low cost.
Keywords: incoherent optical emitter; an optimal optical reception; optimum optical digital signals; synthesis optical receiver; photons and photoelectrons; minimization of the average error probability of reception.

References
1. Freeman R. Volokonno-opticheskie sistemy svyazi [Fiber-optic communication systems]. Trans. angl. M.: Tekhnosfera. 2006. 496 p. (In Russian).
2. Bailey D., Edwin R. Volokonnaya optika: Teoriya i praktika [Fiber optics: Theory and practice]. Trans. angl. M.: KUDITS-OBRAZ. 2006. 320p. (In Russian).
3. Gower J. Opticheskie sistemy svyazi [Optical communications systems] /TRANS. angl. M.: Radio i svyaz. 1989. 504 p. (In Russian).
4. Gagliardi R.M., Karp S. Opticheskaya svyaz. Svyaz. [Optical communications. Connection]. 1978. 424 p. (In Russian).
5. Fedorov S.E. Synthesis of optical digital communication channel for automated control systems. H&ES Research. 2015. Vol. 7. No.2. Pp. 48–52. (in Russian).
6. Fink L.M. Teoriya peredachi diskretnykh soobshcheniy [Theory of transmission of discrete messages]. Ed. 2-e, Rev., extra-M.: Sovetskoe radio. 1970. 748 p. (In Russian).
7. Korzhik, V.I., Fink, L.M. Pomekhoustoychivoe kodirovanie diskretnykh soobshcheniy v kanalakh so sluchaynoy strukturoy [Noiseless coding discrete messages in channels with random structure]. M: Svyaz. 1975. 272 p. (In Russian).

Information about authors:
Fedorov S.E., Ph.D, professor, professor Moscow Technical University of Communication & Informatics.

For citation:
Fedorov S.E. Study of potential noise incoherent optical digital communication channel. H&ES Research. 2015. Vol. 7. No. 4. Pp. 10–14. (in Russian).

ITU Kaleidoscope 2015

Trust in the Information Society

Barcelona, Spain, 9-11 December 2015

Papers submission: 6 July 2015

Organized by:

ITU

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

АРХИТЕКТУРНЫЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Голубинцев Александр Владимирович,
аспирант Северо-Кавказского филиала Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия, galex@mail.ru

Мясникова Анна Ивановна,
аспирант Северо-Кавказского филиала Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия, man@yandex.ru

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

Ключевые слова:
взаимодействие открытых систем, архитектура, автоматизированная система управления, интерфейс, системы управления.

АННОТАЦИЯ

На современном этапе бурного развития информационных и телекоммуникационных технологий, перехода к концепции Глобальной информационной инфраструктуры наиболее актуальным является вопрос создания и управления современными инфокоммуникационными системами и сетями специального назначения (ИКС СН). Так, наряду с системными и функциональными принципами организации автоматизированных систем управления (АСУ) инфокоммуникационных сетей специального назначения (ИКС СН) чрезвычайно важны также архитектурные принципы. Под архитектурой АСУ ИКС СН рассмотрим ее формализованное описание, отражающее входящие в нее компоненты, их назначение и взаимосвязи друг с другом и определяемое принципами построения АСУ ИКС СН, а также протокольной моделью взаимодействия ее удаленных элементов. Методологической основой построения архитектуры АСУ ИКС СН являются принципы эталонной модели взаимодействия открытых систем (ЭМ ВОС), формирования профиля ВОС, концепции Глобальной информационной инфраструктуры, принципов сетей нового поколения (NGN), концепций сетевой службы (NMS и TMN) и др. Различают физическую, информационную, функциональную и логическую архитектуры автоматизированной системы управления ИКС СН. Физическая архитектура автоматизированной системы управления – составляющая архитектуры АСУ ИКС СН, которая представляет собой ее физическую основу, описывает номенклатуру подсистем, комплексов средств автоматизации, коммутации-маршрутизации, их привязку друг к другу, организацию информационных соединений, характеристику стыков и интерфейсов. Информационная архитектура АСУ ИКС СН, в рамках которой осуществляется обмен данными по управлению, основана на некой модели управления, использует объектно-ориентированный подход и оказывает непосредственное влияние на спецификацию интерфейсов.

Появление логической архитектуры было обусловлено тем, что задачи управления ИКС СН и сетевого управления достаточно сложны и многоплановы. Для упрощения управления и разграничения полномочий между различными участниками процесса управления функциональные возможности элементов и подсистем АСУ вместе с необходимой информацией могут быть разбиты на ряд логических уровней.

В основу логической архитектуры АСУ ИКС СН положена стандартная ЭМ ВОС, в соответствии с которой различные средства автоматизации, информационные и телекоммуникационные комплексы АСУ должны строиться в виде открытых систем.

Наряду с системными и функциональными принципами организации автоматизированных систем управления информационных систем специального назначения (АСУ ИКС СН) чрезвычайно важны также архитектурные принципы [1, 2].

Будем понимать под архитектурой АСУ ИКС СН ее формализованное описание, отражающее входящие в нее компоненты, их назначение и взаимосвязи друг с другом и определяемое принципами построения АСУ ИКС СН, а также протокольной моделью взаимодействия ее удаленных элементов. Методологической основой построения архитектуры АСУ ИКС СН являются принципы эталонной модели взаимодействия открытых систем (ЭМ ВОС), формирования профиля ВОС, концепции Глобальной информационной инфраструктуры, принципов сетей нового поколения (NGN), концепций сетевой службы (NMS и TMN) и др. Будем различать физическую, информационную, функциональную и логическую архитектуры автоматизированной системы управления ИКС СН [2, 3]. .

Физическая архитектура автоматизированной системы управления – составляющая архитектуры АСУ ИКС СН, которая представляет собой ее физическую основу, описывает номенклатуру подсистем, комплексов средств автоматизации, коммутации-маршрутизации, их привязку друг к другу, организацию информационных соединений, характеристику стыков и интерфейсов. Фактически физическая архитектура АСУ ИКС СН описывает физические соединения с помощью сети обмена данными управления (управляющая сеть), различных центров управления АСУ ИКС СН (рис. 1).

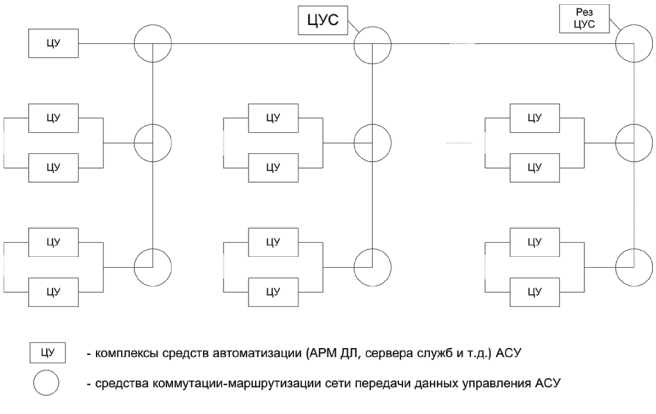


Рис. 1. Упрощенная физическая архитектура АСУ ИКС СН

С технологической точки зрения управление ИКС СН представляет собой обработку информации, поступающей от ее элементов специализированными программными приложениями комплексов средств автоматизации АСУ ИКС СН. Для обеспечения обработки информации необходимо осуществлять информационный обмен между многочисленными устройствами и оборудованием АСУ ИКС СН. Поэтому в настоящее время управление инфокоммуникациями реализуется на базе распределенных по средствам автоматизации программных приложений. Информационная архитектура АСУ ИКС СН, в рамках которой осуществляется обмен данными по управлению, основана на некой модели управления, использует объектно-ориентированный подход и оказывает непосредственное влияние на спецификацию интерфейсов.

Ключевыми элементами информационной архитектуры являются информационные элементы, модели взаимодействия элементов и собственно информационные модели [4]. При этом информационные элементы с точки зрения объектно-ориентированного подхода моделируются как управляющие и управляемые объекты.

Описание управляемого объекта является наиболее существенной частью информационной архитектуры АСУ ИКС СН и осуществляется обычно с помощью контура управляемого объекта [4]. В этом контуре указаны характеристики объекта, доступные для управления, в частности (рис. 2):

– атрибуты, которые описывают свойства объекта;

– операции, которые могут выполняться на объекте;

– поведение или режим работы объекта, которые задаются согласно операции;

– сообщения или уведомления, которые выдаются объектом.

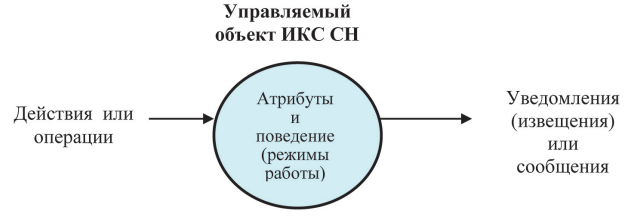


Рис. 2. Описание управляемого объекта ИКС СН

Описание объектов управления достаточно абстрактно и может относиться к самым разнообразным элементам ИКС СН. Управляемый объект наиболее точно характеризуется своим состоянием и взаимоотношениями с другими объектами. Эти характеристики представлены в атрибутах управляемого объекта, доступ к которым можно получить с помощью операций, выполняемых по команде управляющего объекта. При описании объекта управления определяется набор уведомлений, которые посылает управляемый объект для оповещения управляющей системы о событиях, связанных с данным объектом.

Для описания синтаксиса данных, передаваемых между управляющим и управляемым объектами ИКС СН, используется специальный метаязык описания данных [3, 4]. Для описания семантики операций над атрибутами и объектами применяются шаблоны поведения объектов, которые обычно записываются на естественном языке. Управляемый объект может быть создан или удален внешними командами, если это раз-

решено должностными лицами (ДЛ) соответствующего центра управления. Заданный объект может наследовать все операции, уведомления и поведение других объектов. При определении новых объектов предполагается, что стандартные определения при возможности используются повторно. Это один из сложных аспектов моделирования объектов управления. Различные наборы инструментальных средств моделирования упрощают такую задачу. Управление объектом осуществляется с помощью модели взаимодействия агент-менеджер (рис. 3).

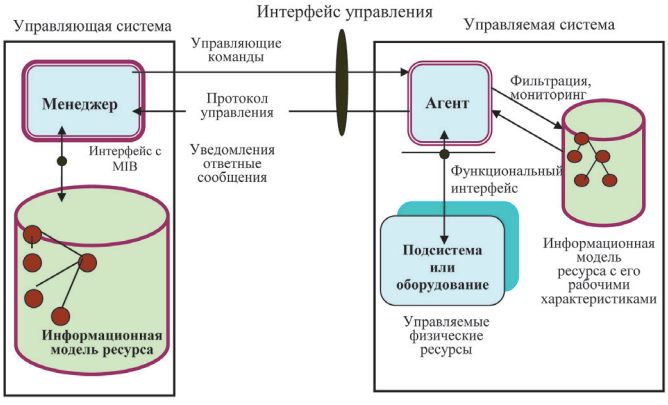


Рис. 3. Взаимодействие менеджера и агента в информационной архитектуре АСУ ИКС СН

Программное приложение в средствах автоматизации, которое выдает команды управления и принимает уведомления, является программой-менеджером. Приложение, установленное на элементе ИКС СН, выполняющее управляющие команды и посылающее уведомления от имени управляемых объектов, является программой-агентом.

Менеджер устанавливает взаимосвязь с агентом для осуществления управляющего взаимодействия. Возможное нарушение такой взаимосвязи может быть обнаружено обеими сторонами.

Как только связь между менеджером и агентом установлена, может начаться обмен управляющей информацией. Программа-менеджер может потребовать выполнения операций «Создать» (CREATE), «Удалить» (DELETE), «Выполнить» (ACTION) в отношении управляемых объектов в целом, а также операций «Получить» (GET) и «Установить» (SET) относительно атрибутов управляемых объектов, согласно руководства по определению управляемых объектов (GDMO). В итоге, получив команду начать ту или иную операцию, программа-агент выполняет требуемое действие на управляемом объекте и посылает менеджеру сообщение о результатах или подтверждение, о выполнении операции.

Программа-агент выступает своего рода посредником между менеджером и управляемым ресурсом. При этом агент с помощью функционального интерфейса взаимодействует с управляемыми физическими ресурсами. Описание ресурсов агент поддерживает с помощью информационной модели управляемого ресурса. В этой модели отражаются рабочие характеристики ресурса, на которые можно воздействовать или которые можно контролировать в процессе управления. С другой стороны, менеджер также поддерживает информационную модель управляемого ресурса, т.е. информационные модели агента и менеджера в основном одинаковые.

Информационная модель менеджера может быть более точна в силу того, что информация менеджера является «очищенной», обработанной, нормализованной, упорядоченной. Это происходит благодаря агенту, который фильтрует поток данных в сторону менеджера от незначительных ошибок, искажений.

Кроме того, информационная модель менеджера включает модели нескольких ресурсов, т.е. модель менеджера более глобальна, чем модель агента. Модель агента часто называют базой данных управляющей информации (Management Information Base или MIB).

Менеджер также поддерживает MIB, но база данных менеджера вторична по отношению к базе данных. Для обновления своей базы данных менеджер всегда запрашивает агента. В MIB хранятся атрибуты управляемых объектов, описания классов, которые соответствуют элементам сети. MIB является абстрактным описанием характеристик управляемых ресурсов, т.е. оборудования и подсистем связи, и позволяет хранить описание действий (операций управления), которые можно осуществлять над управляемыми объектами. Другими словами, MIB позволяет программным приложениям управления (в первую очередь агенту, затем менеджеру) получать информацию об управляемых объектах.

Управляемые объекты могут самостоятельно выдавать уведомления о своем состоянии при наступлении некоторых событий, которые признаны, например, аварийными, т.е. уведомления обычно означают, что на объекте управления произошло что-либо, представляющее интерес – создание, удаление объекта или изменение значений его атрибутов. Агенты доставляют уведомления менеджеру либо непосредственно, либо через дискриминаторы передачи событий. Дискриминаторы являются управляемыми объектами, фильтрующими события, поступающие от агентов. Фильтрация гарантирует прием менеджером информации только о событиях, представляющих интерес, или согласно приоритету сообщения. Например, сообщения о критических неисправностях или угрожающих состояниях будут направлены менеджеру в первую очередь, а сообщения о незначительных неисправностях смогут поступить только после отработки сообщения о критических неисправностях.

Другой важный аспект управления в АСУ ИКС СН состоит в том, что передача управляющих команд основана на модели асинхронной передачи сообщений. Все операции, осуществляемые над управляемым объек-

том, могут быть разделены на четыре примитива (или типа): запросы, ответы, подтверждения и указания. Эти примитивы используются следующим образом:

– чтобы выполнить операцию, менеджер посылает управляющую команду (сообщение-запрос);

– когда такое сообщение поступает агенту, оно принимается как сообщение-указание;

– агент выполняет требуемое действие и может послать сообщение-ответ;

– сообщение-ответ принимается менеджером как сообщение-подтверждение.

Агент посылает ответное сообщение, если в исходном запросе затребовано подтверждение. В целом информационная модель управления в АСУ ИКС СН представляет собой информационную конструкцию, которая поддерживается функциональными блоками менеджеров и распределенными знаниями по управлению, которые могут быть распределены по нескольким центрам (пунктам) управления.

Информационная модель управления представляет собой абстрактное описание сетевых ресурсов, доступных для управления, и соответствующих операций управления, определяет стандарты для содержания информационного массива, который появляется в ходе управления системой связи и сетевого управления. Информационная модель относится к прикладному уровню модели ВОС, поэтому при ее разработке требуется организовать взаимодействие с другими приложениями 7-го уровня модели, которые используются для хранения, поиска и обработки информации. С учетом использования технологии «агент-менеджер» функциональная архитектура имеет вид, представленный на рис. 4.

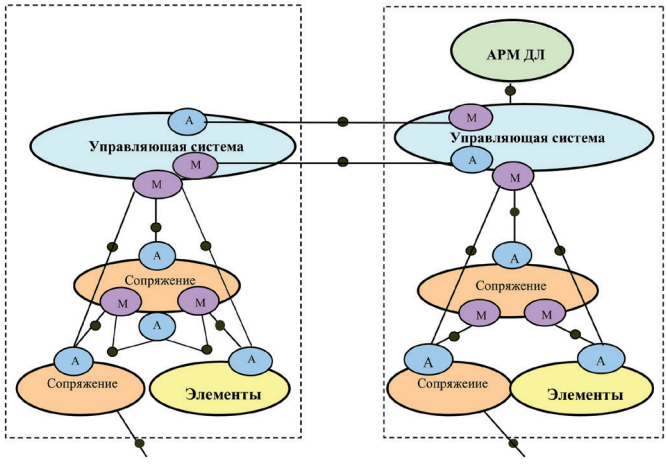


Рис. 4. Функциональная архитектура АСУ ИКС СН
М – менеджеры, А – агенты

В рамках АСУ ИКС СН всегда существует определенная иерархия «обязанностей», связанных с управлением теми или иными объектами системы или сетей связи. Такая иерархия может быть описана с помощью термина «уровень управления» и соответственно архитектура, которая описывается с помощью уровней, называется логической многоуровневой архитектурой АСУ ИКС СН.

Появление логической архитектуры было обусловлено тем, что задачи управления ИКС СН и сетевого управления достаточно сложны и многоплановы. Для упрощения управления и разграничения полномочий между различными участниками процесса управления функциональные возможности элементов и подсистем АСУ вместе с необходимой информацией могут быть разбиты на ряд логических уровней.

Функциональные возможности АСУ ИКС СН в связи с различием управляемых объектов могут быть разбиты на следующие уровни (рис. 5):

– элементы системы и сетей связи – управление элементами (УЭ);

– сети связи и телекоммуникационные сети – управление сетями;

– услуги связи, предоставляемые пользователям и прикладным процессам – управления услугами.

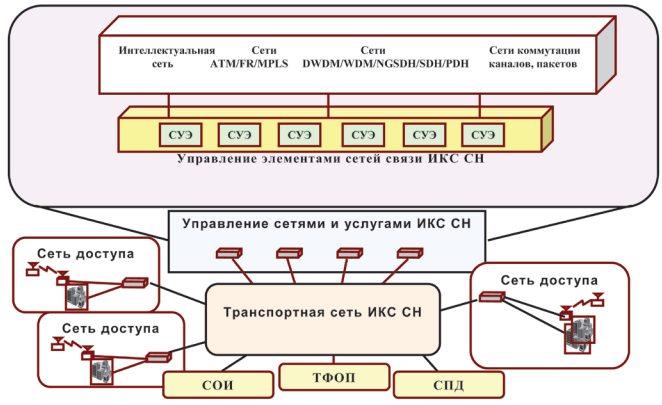


Рис. 5. Уровни архитектуры
автоматизированной системы управления ИКС СН

Исходя из целевого предназначения АСУ, автоматизированное управление ИКС СН и сетями в ее составе осуществляется с помощью управляющих прикладных процессов, программно реализующих задачи следующих ранее рассмотренных подсистем управления (рис. 6):

– организационного;

– оперативно-технического;

– технологического.

Логическая АСУ ИКС СН – составляющая архитектуры АСУ, представляющая собой многоуровневую логическую модель взаимодействия функционально независимых логических элементов системы управления, образующих в своей совокупности соответствующие логические подсистемы:

– обработки информационных потоков управления с целью предоставления необходимого спектра телекоммуникационных услуг комплексам средств автоматизации (КСА) и ДЛ органов управления (серверная подсистема услуг, подсистема услуг);

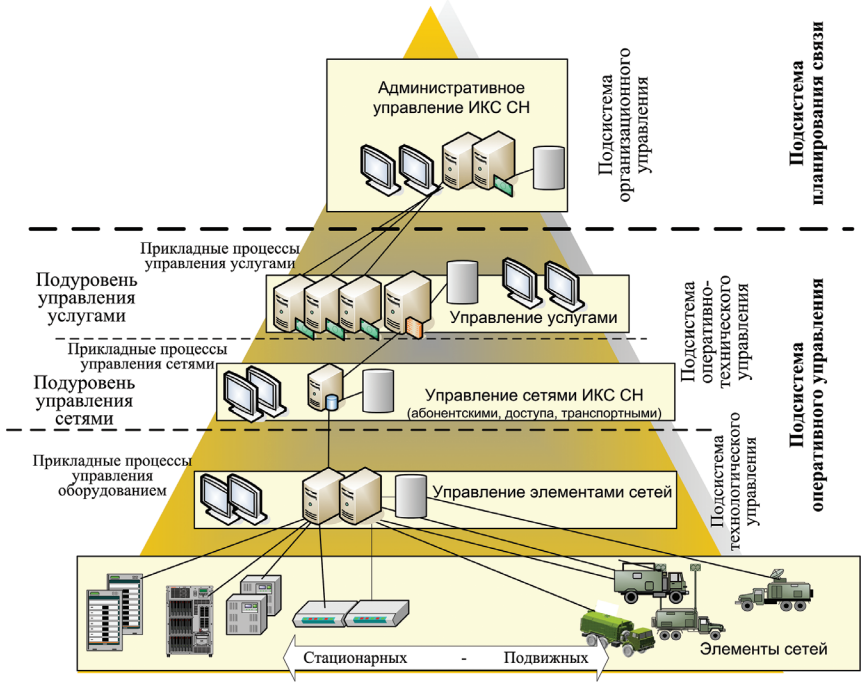


Рис. 5. Архитектура подсистем АСУ ИКС СН

– обмена информацией управления (данными управления), обеспечивающую транспортные функции при организации информационного взаимодействия центров управления ИКС СН и телекоммуникационными сетями (сеть управления, сеть передачи данных управления);

– клиентская или терминальная подсистема, обеспечивающая доступ ДЛ органов управления ИКС СН и сетями связи к ресурсам и услугам служб управления и прикладным процессам поддержки процессов управления;

– служб и услуг управления, обеспечивающая процессы управления ИКС СН и сетями в ее составе.

Ключевым понятием в логической архитектуре АСУ является понятие профиля и стэка протоколов. Будем понимать под профилем протоколов АСУ ИКС СН набор базовых стандартов и других спецификаций, определяющих совокупность услуг, доступных прикладным процессам управления и ДЛ органов управления связью в конкретных условиях ее функционирования. Профиль протоколов АСУ состоит из базового набора открытых (общедоступных) согласованных стандартов и спецификаций, определяющих различные услуги в эталонной модели АСУ, ограниченных конкретной функциональной средой (группой сред) функционирования. Он охватывает широкий круг прикладных областей, в которых заинтересованы различные службы управления. Стандарты и спецификации профиля АСУ ИКС СН определяют форматы данных управления, интерфейсы, протоколы или комбинацию этих элементов. Стэк протоколов в составе профиля – набор рекомендаций и специальных базовых стандартов и спецификаций, определяющих отдельную, относительно функционально независимую группу услуг в логической модели АСУ.

В основу логической архитектуры АСУ ИКС СН целесообразно положить стандартную модель взаимодействия открытых систем (ВОС), в соответствии с которой различные средства автоматизации, информационные и телекоммуникационные комплексы АСУ должны строиться в виде открытых систем [5]. При этом АСУ ИКС СН (как и все взаимодействующие с ней системы управления) следует создавать для интеллектуальной и инфокоммуникационной поддержки выполнения прикладных процессов управления и деятельности ДЛ органов управления ИКС СН, а элементы АСУС должны представляться в виде совокупности взаимодействующих открытых систем (терминальных, серверных, коммутационных, управляющих).

В архитектурном плане, каждая терминальная подсистема любой АСУ, представляющая собой, либо комплекс средств автоматизации (КСА) определенного центра управления соответствующего министерства, ведомства или корпорации, либо КСА центров управления ИКС СН или телекоммуникационной сетью, центров других информационных систем и т.д., должна состоять из прикладных процессов, для выполнения которых она создана, и области взаимодействия, предназначенной для обеспечения связи прикладных процессов управления друг с другом и передачи информации во внешнюю среду (рис. 7).

Учитывая особенности современных и существующих сетей связи, область прикладных процессов

должна опираться на три поддерживающих стэка протоколов, используемых как семиуровневую модель OSI (МСЭ-Т), четырехуровневую модель подобную сети Internet (TCP/IP), так и специальную модель. Центры управления АСУ отличаются тем, что их область взаимодействия предназначена для поддержки прикладных процессов управления системой и сетями связи (серверы управления). Логическая архитектура типового серверного комплекса АСУ ИКС СН приведена на рис. 8.

Логическая архитектура комплексов подсистемы обмена информацией (транспортной подсистемы) АСУ отличается от логических архитектур терминальных и серверных комплексов. Ограниченное применение конкретного комплекса подсистемы в рамках сети управления определяет его специфическую логическую архитектуру как элемента сети, обеспечивающей транспортные функции при организации информационного взаимодействия центров управления связью и телекоммуникационными сетями (сеть управления, сеть передачи данных управления).

Логическую архитектуру АСУ ИКС СН можно представить в виде совокупности взаимодействующих между собой различных элементов и логических подсистем: центров управления, комплексов технических средств (КТС) сетей передачи данных (СПД) и систем обмена информацией (СОИ), сетей телефонной и телеграфной связи, а также центров и систем управления взаимодействующих систем связи.

Нормативно-правовой базой для профиля протоколов АСУ служит Госпрофиль РФ, на основе которого можно, добавляя новые протоколы, обеспечивающие требуемые услуги, гарантирующие надежную передачу данных между оконечными средствами АСУ, передачу данных управления, способную поддерживать многие виды приложений АРМ ДЛ и их функциональные среды, обеспечить возможность запросов стандартных прикладных программ, функционирующих через стандартные сети управления.

Профиль обеспечивает как надежные межконцевые услуги, благодаря которым должностные лица органов управления или КСА АСУ ИКС СН могут использовать и применять свои собственные прикладные программы, реализующие прикладные процессы административного управления (планирование связи), управления транспортной сетью (структурой сети, потоками, ошибками, отказами, безопасностью), услугами связи, телекоммуникационными сетями и вторичными сетями связи, сетями доступа (структурой сетей, информационными потоками, сбойными ситуациями и ошибками передачи, отказами оборудования и программных средств, безопасностью), управления сетевыми узлами и оборудованием узлов, управления эффективностью использования имеющихся сетевых ресурсов и поддержкой новых служб.

Для обеспечения ДЛ органов управления связью возможностью реализации эффективных управленческих технологий и повышения эффективности функционирования, имеющихся телекоммуникационных сетей (в том числе сети управления), профиль дополнен протоколами, установленными рекомендациями МСЭ-Т, содержащими пять спецификаций, определяющих работу аудиокодеков, видеокодеков, протокол сигнализации RAS (регистрации, подтверждения и состояния), протокол сигнализации (установление и разрыв соединения между терминалами), протокол управления мультимедийной конференцией, а также протоколы RTP (Real-time Transport Protocol) – доставки адресатам аудио- и видеопотоков в масштабе реального времени при работе с IP-сетями управления, и RTCP (Real-Time Transport Control Protocol) – управления передачей в режиме реального времени (комплекс стандартов RFC).

Рис. 7. Архитектура терминального комплекса КСА АСУ ИКС СН

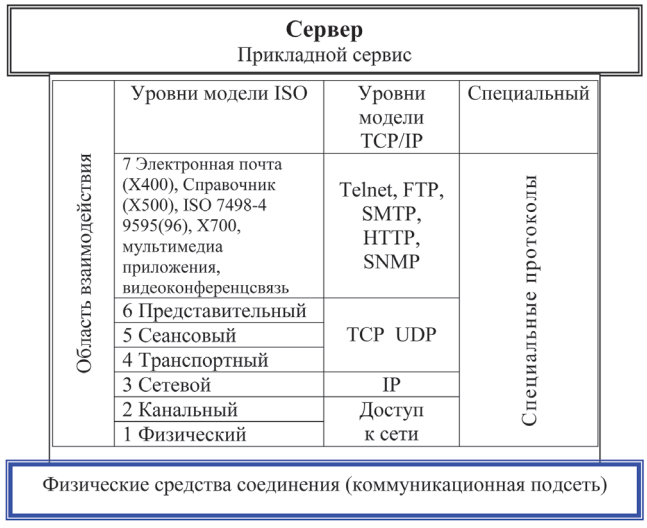


Рис. 8. Архитектура серверного комплекса АСУ ИКС СН

Организация совместного функционирования центров управления АСУ в едином процессе управления ИКС СН или сетями связи предусматривает эффективный обмен информацией управления. При этом, в архитектурном плане, различают три категории

команд, обеспечивающих обмен информацией управления, конкретные содержание которых определяется протоколом управления:

– управляющие воздействия;
– управляющая информация;
– уведомление о событиях.

Обмен информацией при взаимодействии КСА центров управления АСУ рассматривается как двухстороннее взаимодействие, в котором стороны выполняют роли инициатора и ответчика (клиент-сервер) для каждого единичного акта обмена информацией. Инициатор формирует управляющее воздействие, т.е. выдает запрос на определенную функцию управления, а ответчик формирует ответ на управляющий запрос. Деятельность по передаче информации управления реализуется в запросах на определенную информацию, выдаваемых инициатором, и в ответах, формируемых ответчиком. Уведомления о событиях формируются и посылаются инициатором. Если требуется подтверждение на прием такого уведомления, то оно формируется ответчиком в виде информационного ответа.

Так как в основе архитектурного построения АСУ закладывается, уже рассмотренная фундаментальная схема взаимодействия агент-менеджер [1, 2, 4, 5], при которой определенный агент является неким посредником между управляемым ресурсом и прикладной управляющей программой – менеджером данного связного ресурса, то особенности построения и функционирования системы, сетей связи и систем управления ими, приводят к необходимости использования одного и того же типа менеджера для управления различными связными ресурсами. Для этого в рамках соответствующих агентов АСУ обычно создается адекватная модель управляемого ресурса, в которой отражаются только те параметры ресурса, которые необходимы для его контроля и управления.

Литература

1. Буренин А.Н. Системно-архитектурные вопросы построения автоматизированных систем управления связью // Телекоммуникационные технологии. 1996. № 1. С. 97–112.

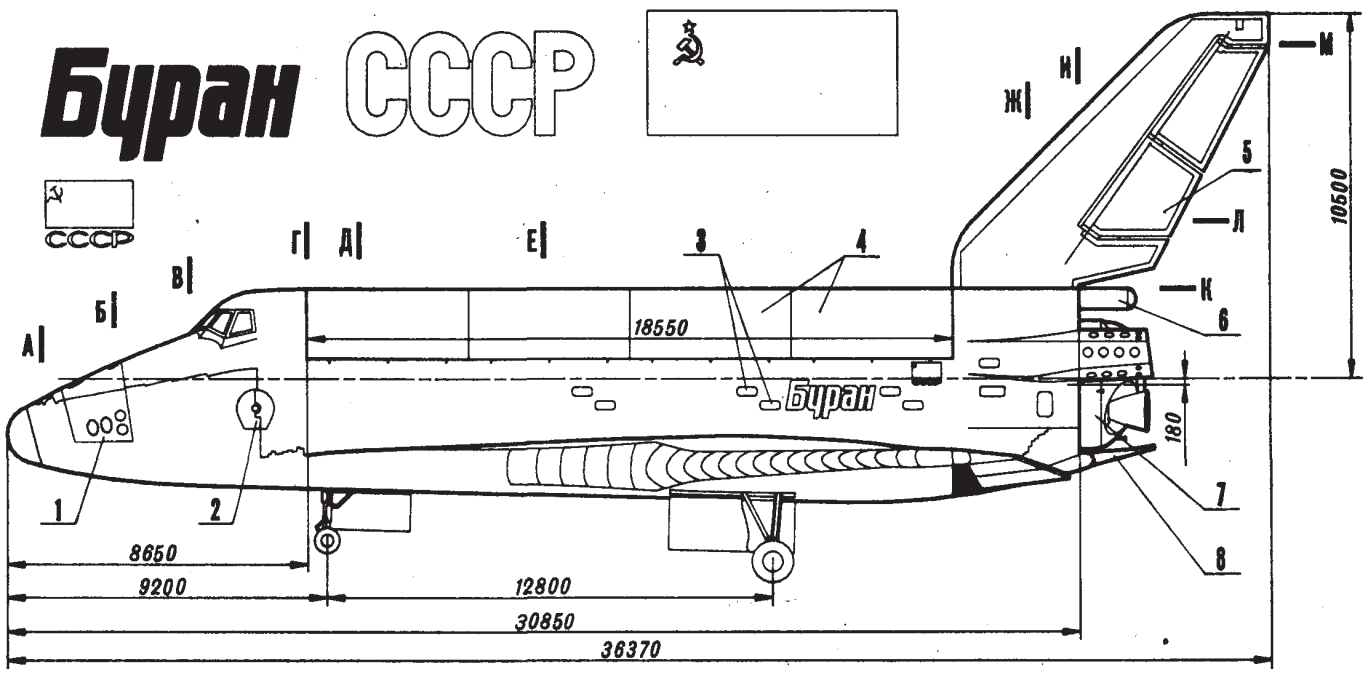
2. Буренин А.Н., Легков К.Е. Современные инфокоммуникационные системы и сети специального назначения. Основы построения и управления: Монография. М.: Медиа-Паблишер. 2015. 348 с.

3. Кульгин М. Архитектура технологии ATM // Byte Россия. 1998. № 3. С. 60–67.

4. Гребешков А.Ю. Стандарты и технологии управления сетями связи. М.: Эко-Тренд. 2003. 288 с.

5. Буренин А.Н., Легков К.Е. Особенности архитектур функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 5. № 3. С. 12–17.

Для цитирования:
Голубинцев А.В., Мясникова А.И., Легков К.Е. Архитектурные принципы организации автоматизированных систем управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 16–23.



ARCHITECTURAL PRINCIPLES OF ORGANIZATION AUTOMATED CONTROL SYSTEMS OF INFOCOMMUNICATION NETWORKS SPECIAL PURPOSE

Golubintsev Alexander Vladimirovich,
Rostov-on-Don, Russian, *galex@mail.ru*

Myasnikova Anna Ivanovna,
Rostov-on-Don, Russian, *man@yandex.ru*

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

Abstract
At the present stage of rapid development of information and telecommunication technologies, the transition to the concept of Global information infrastructure the most pressing issue is the creation and management of modern communication systems and networks (ICN SP). So, along with system and functional organization principles of the automated control systems (ACS) information and communication networks for special purposes (ICN SP) is also extremely important architectural principles. Under the ACS architecture ICN SP consider its formal description, reflecting the constituent components, their purpose and relationship to each other and defined by the principles of ACS ICN SP, and Protocol interaction model her deleted items. The methodological basis for the architecture of ACS ICN SP are the principles of the reference model of open systems interconnection (OSI), the profile formation OSI, the concept of Global information infrastructure, principles of next generation networks (NGN), concepts of network service (NMS and TMN), etc. There are physical, informational, functional and logical architecture of an automated control system ICN SP. The physical architecture of the automated control system component architecture ACS ICN SP, which represents its physical basis, describes the range of subsystems, systems automation, switching-routing them to bind to each other, the organization of information compounds, characterization of joints and interfaces. Information architecture ACS ICN SP, in which there is an exchange of management based on a governance model that uses object-oriented approach and has a direct impact on the specification of interfaces.
The emergence of the logical architecture was due to the fact that the management tasks ICN SP and network management is quite complex and multifaceted. For ease of management and the division of powers between the different actors of the process control functionality of elements and subsystems of the ACS along with the necessary information can be broken down into a number of logical layers.
The basis of the logical architecture of ACS ICN SP based on standard OSI, in accordance with which various means of automation, information and telecommunications control systems installed must be constructed in the form of open systems.

Keywords: open systems, architecture, automated management system, interface, control system.

References
1. Burenin A.N. System-architectural issues of building automated control systems communication. Telekommunikatsionnye tekhnologii. 1996. No. 1. Pp. 97–112. (In Russian).
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], M.: Media Publisher, 348 p. (In Russian).
3. Kuligin M. the Architecture of the ATM technology. Byte Russia. 1998. No. 3. Pp. 60–67. (In Russian).
4. Grebeshkov A.Yu. Standarty i tekhnologii upravleniya setyami svyazi [Standards and technology network management]. M.: Eko-Trend. 2003. 288 p. (In Russian).
5. Burenin A.N., Legkov K.E. Features of the architectures of the functioning, monitoring and management of field components of modern communication networks. H&ES Research. 2013. Vol. 5. No. 3. Pp. 12–17. (In Russian).

Information about authors:
Golubintsev A.V., post-graduate student of North-Caucasus branch of the Moscow technical University of communications and Informatics;
Myasnikova A.I., post-graduate student of North-Caucasus branch of the Moscow technical University of communications and Informatics;
Legkov K.E., Ph.D., deputy head of the Department automated systems of control, Military Space Academy.

For citation:
Golubintsev A.V., Myasnikova A.I., Legkov K.E. Architectural principles of organization automated control systems of infocommunication networks special purpose. H&ES Research. 2015. Vol. 7. No. 4. Pp. 16–23. (in Russian).

LTE: есть куда расти

Агентство TelecomDaily подвело итоги развития LTE-сетей в России по состоянию на 1 квартал 2015 года.

Всего в России установлено уже 44,3 тыс. базовых станций LTE, что на 275% больше по сравнению с 1 кварталом 2014 года (около 16 тыс. станций) и на 5,5% больше в сравнении с 4 кварталом 2014 (рис. 1).

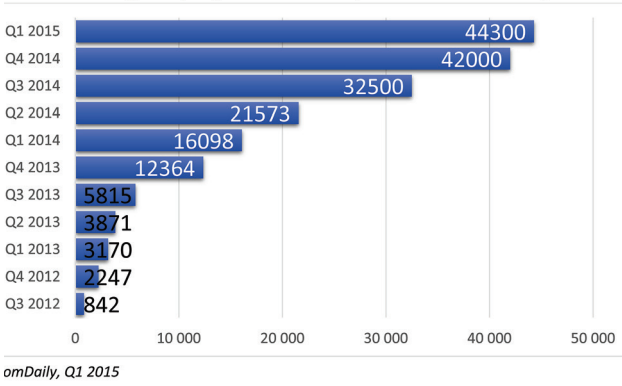


Рис. 1. Количество действующих базовых станций LTE в России по кварталам

По итогам 1 квартала 2015 года, больше всего базовых станций LTE в России насчитывалось у компании «МегаФон» – 18,6 тыс. У компании МТС – 15,7 тыс. станций, у «Билайн» – 8,2 тыс. станций, ещё 1,8 тыс. станций построено другими операторами связи, в частности, «Ростелеком» и «Вайнах Телеком».

Официально кроме «Мегафона» другие операторы «большой тройки» не раскрывают абсолютные значения по количеству LTE-станций, а озвучивают только темпы роста. Например, МТС за 2014 год построил 8937 базовых станций, что больше, чем у любого из конкурентов. Это, впрочем, легко объясняется тем, что за год МТС запустила LTE в 61 регионе РФ, то есть увеличила количество регионов с покрытием LTE в 5 раз. «Билайн» вообще оперирует лишь относительными понятиями, заявляя о приросте количества базовых станций LTE год к году на 430%: разумеется, столь впечатляющие показатели можно объяснить в первую очередь эффектом «низкой базы» (рис. 2, 3).

При этом «Билайн» и МТС совместно построили 3 тыс. базовых станций в рамках соглашения о совместном использовании сети радиодоступа (RAN Sharing). Это позволяет снизить капитальные затраты и более эффективно использовать ограниченный частотный ресурс. RAN Sharing используют и другие операторы при строительстве сетей LTE.

Покрытие LTE в России

В условиях экономического кризиса темпы запусков новых сетей LTE в регионах замедлились: операторы предпочитают развивать покрытие в уже запущенных областях, в первую очередь тех, где имеется платежеспособный спрос на услуги связи четвертого поколения. Это всего 4 субъекта федерации, объединенные в две лицензионные зоны: Москва с Московской областью и Санкт-Петербург с Ленинградской областью.

Тем не менее, операторы активно строят сети LTE. Наибольшее проникновение (100%) обеспечено ими в южном и приволжском федеральных округах, далее с 94% следует Сибирский федеральный округ. Покрытие в 93% обеспечено в Северо-западном, Северо-кавказском и Уральском федеральном округах, 90% – в Центральном и 84% – в Дальневосточном. В Крымском федеральном округе уровень проникновения LTE-связи составляет 0%.

Лидером по количеству запущенных регионов является МТС: сети оператора присутствуют в 77 субъектах федерации. В 2015 году МТС запустил в эксплуатацию сети LTE в Краснодарском крае и Кемеровской области (запуск на базе RAN Sharing с «Билайн»). Причём с первым регионом связана интересная история: ранее в Краснодарском крае действовал мораторий на строительство сетей LTE до 2016 года, пролоббированный «МегаФоном», построившим масштабную сеть в Сочи к Олимпийским играм 2014 года. Однако конкурентам удалось в судебном порядке оспорить законность данного моратория, и он был отменен для всего региона,

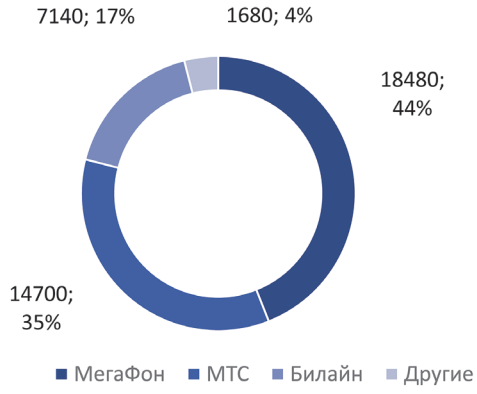


Рис. 2. Доли операторов по количеству базовых станций LTE Q4 2014

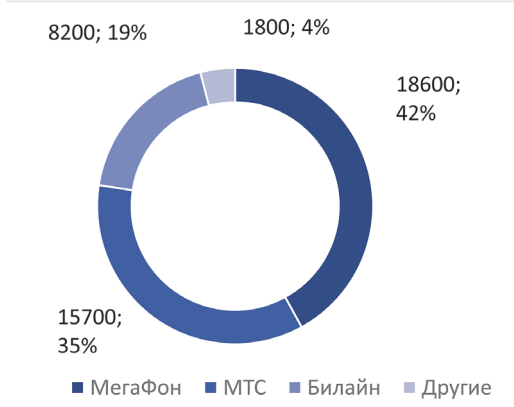


Рис. 3. Доли операторов по количеству базовых станций LTE Q1 2015

кроме собственно города Сочи, где «МегаФон» остается монополистом.

«МегаФон» занимает второе место по количеству запущенных LTE-сетей в регионах, присутствуя в 74 субъектах федерации. В 2015 году LTE от «МегаФон» появилось в Забайкальском крае и Республике Коми, а также в коммерческую эксплуатацию запущена сеть в Удмуртской республике, легализованная ещё в 2014 году.

«Билайн» пока существенно отстает от конкурентов и работает на базе LTE только в 49 регионах, поэтому в 2015-ом году он, вероятно, станет лидером по количеству новых запусков. В 2015 году оператор уже запустил LTE-сети в Челябинской области и Красноярском крае, Ханты-Мансийском автономном округе и Северной Осетии.

Перспективы LTE-Advanced

В развитии сетей связи четвертого поколения (4G) мобильные операторы планомерно переходят от технологии LTE к LTE-Advanced (LTE-A): за счёт агрегации частот в одном или разных диапазонах можно существенно увеличить пиковые пропускные способности сети, а в случае с разными диапазонами еще и стабилизировать покрытие.

Первым LTE-Advanced (Cat. 6, 300 Мбит/сек) запустил весной 2014 года «МегаФон» – сначала в Москве, затем в Санкт-Петербурге. Оператор в дополнение к собственным 2x10 МГц использует частоты 2x30 МГц приобретенного ранее «Скартела» (все в Band 7, 2600 МГц), а также начинает экспериментировать с рефармингом диапазона 1800 МГц, используемого сетями GSM: это стало возможным после введения законодательного принципа «технологической нейтральности», который ранее эффективно использовался в первую очередь для недопущения развития «Tele2», в итоге проданного «Ростелекому». Всего LTE-A у «МегаФон» работает в четырех регионах: помимо двух столиц это Челябинск и Ростов-на-Дону (здесь сеть тестируется).

Коммерческая сеть LTE-Advanced 5+10 МГц (Band 20 + Band 7) работает у «Вымпелкома» в Москве, по три несущих (5 МГц в Band 20, 5 в Band 3 и 10 в Band 7) намеревается в этом году агрегировать МТС – а в середине апреля было агрегировано и вовсе 40 МГц в Башкирии.

Пока, однако, эти эксперименты – скорее, лишь повод для громких заявлений о собственной «инновационности»: на деле же проникновение поддерживающих эти технологии абонентских терминалов исчисляется сотыми долями процента. В 2015-м году ассортимент поддерживающих LTE-A гаджетов должен расшириться, поскольку поступят в продажу новые флагманские смартфоны, поддерживающие LTE вплоть до Cat.9 и даже Cat.10. Но такие устройства доступны лишь в аппаратах верхней ценовой категории, которые по понятным причинам сейчас имеют весьма ограниченный спрос. Тем не менее, наличие на массовом рынке 60 моделей LTE-A устройств вместо нескольких не может не сказаться на проникновении услуг такого типа.

Между тем, внедрение LTE-A дает всем абонентам рост средних скоростей интернет-доступа благодаря модернизации оборудования и транспортной сети под LTE-A. В частности, в Москве у «МегаФона» средняя скорость 4G в течение 2014 года увеличилась на 25% (с 15 МБит/сек на начало года до 19 МБит/сек на конец) и продолжает расти, в течение января и февраля 2015 она составила уже порядка 20 МБит/сек (данные технической дирекции «МегаФон»). А согласно ежеквартальному исследованию удовлетворенности клиентов CSI (Consumer Satisfaction Index) по столичному филиалу «МегаФона», количество удовлетворенных пользователей по атрибуту «мобильный интернет со смартфона» в 4 квартале 2014 выросло на 4% по отношению к 4 кварталу 2013. Это самый высокий показатель по «большой тройке» (44% пользователей удовлетворены качеством интернет-доступа «МегаФон»).

Покупка пакетов большего объема приводит к удешевлению удельной стоимости мегабайта для клиента. В течение 2014 средняя стоимость 1 Мб снизилась с 11 копеек до 8 коп за счет роста потребления трафика и покупки клиентами пакетов большего объема (более

крупный опт). Среднее потребление трафика на LTE-абонента составляет 2,6 ГБ.

Операторы получают больше дохода за счет того, что базовые станции с поддержкой LTE-A пропускают на 25% больше трафика, чем обычные базовые станции с поддержкой только LTE за счет более современного оборудования. также они обеспечивают разгрузку 3G- и 4G-сетей для основного ядра абонентов: в LTE-A мигрируют в первую очередь «тяжелые» абоненты, потребляющие большие объемы трафика. обновление базовых станций до уровня LTE и LTE-A проводится в рамках текущей модернизации оборудования 2G и 3G. При этом средняя цена базовой станции с LTE+LTE-A не отличается от цены базовой станции LTE. основная инвестиция в частотный ресурс уже сделана.

Между тем, важно понимать, что рефарминг диапазона 1800 МГц пока проводится в экспериментальном и демонстрационном порядке: если отдать из него более 5 МГц под LTE, возникнут сложности с обеспечением емкости для абонентов GSM – напомним, пока 50% абонентов имеют простые телефоны с поддержкой только GSM 900/1800.

Технология VoLTE

В долгосрочной перспективе голосовой мобильный трафик всё же уйдет в VoLTE: то есть будет передаваться по пакетной сети без переключения в канальную. Сейчас LTE-абонент для совершения голосового вызова принудительно переключается в сеть GSM или UMTS, а после – переключается обратно. Это снижает количество успешно совершенных вызовов и приводит к неоправданному расходу энергии мобильных терминалов. Технически вся «большая тройка» уже готова запустить VoLTE в любой момент; тестовые звонки были совершены еще 2-3 года назад, а недавно «Билайн» продемонстрировал VoLTE в коммерческой сети: конечно, опять же в первую очередь в PR-целях.

Запустить VoLTE мешает неготовность СОРМ: система еще не готова к анализу и прослушиванию пакетного голоса. по имеющимся данным, к лету 2015 года завершатся испытания обновленной сорм, и регулятор сразу после этого разрешит использование VoLTE. Однако массового спроса на VoLTE ждать тоже не следует: далеко не все LTE-терминалы поддерживают передачу голоса в LTE. Опять же, речь идёт о моделях верхней ценовой категории, при этом в ряде случаев в партиях для российского рынка поддержка VoLTE отключена по умолчанию, и для ее использования потребуется обновление программного обеспечения.

Смарфтоны с LTE

Длительное время, большой проблемой в продвижении технологии LTE в России было недостаточное количество устройств и их ценовые характеристики. За 4 квартал 2014 года и 1 квартал 2015 года, все это вышло на иной уровень, когда появился и выбор и приемлимые стоимостные характеристики (рис. 4).

Для понимания, в 1квартале 2014 года в России было всего доступно 120 моделей с поддержкой LTE, тогда как по итогам 1 квартала 2015 года их количество составило уже 420 моделей.

Стоимость устройств с поддержкой LTE, также значительно изменилась, но уже в сторону снижения. Средняя цена смартфона с LTE упала с 22 000 рублей до 16 400 рублей. При этом, на рынке, существует достаточно большое количество устройств представлено в ценовой категории от 8 000 до 12 000 рублей. А самые доступные LTE-смартфоны и планшеты стоят дешевле 6 тысяч рублей. В 1 квартале 2015 года рост продаж LTE-устройств (смарфтоны, планшеты) в целом составил порядка 7% (реализовано почти 1 млн. устройств), в деньгах – около 19%.

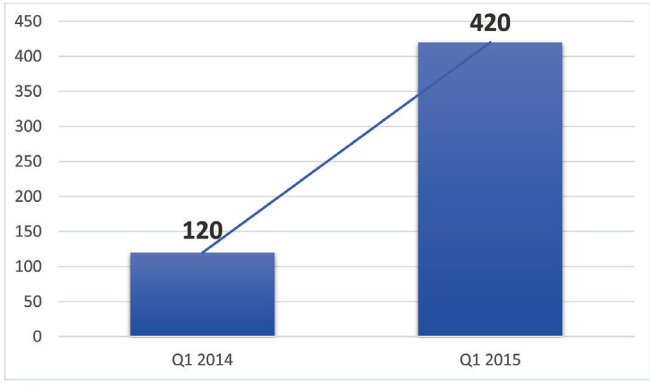


Рис. 4. Количество моделей мобильных LTE-устройств, доступных в России

Устройства LTE формируют уже фактически 45% рынка в денежном выражении.

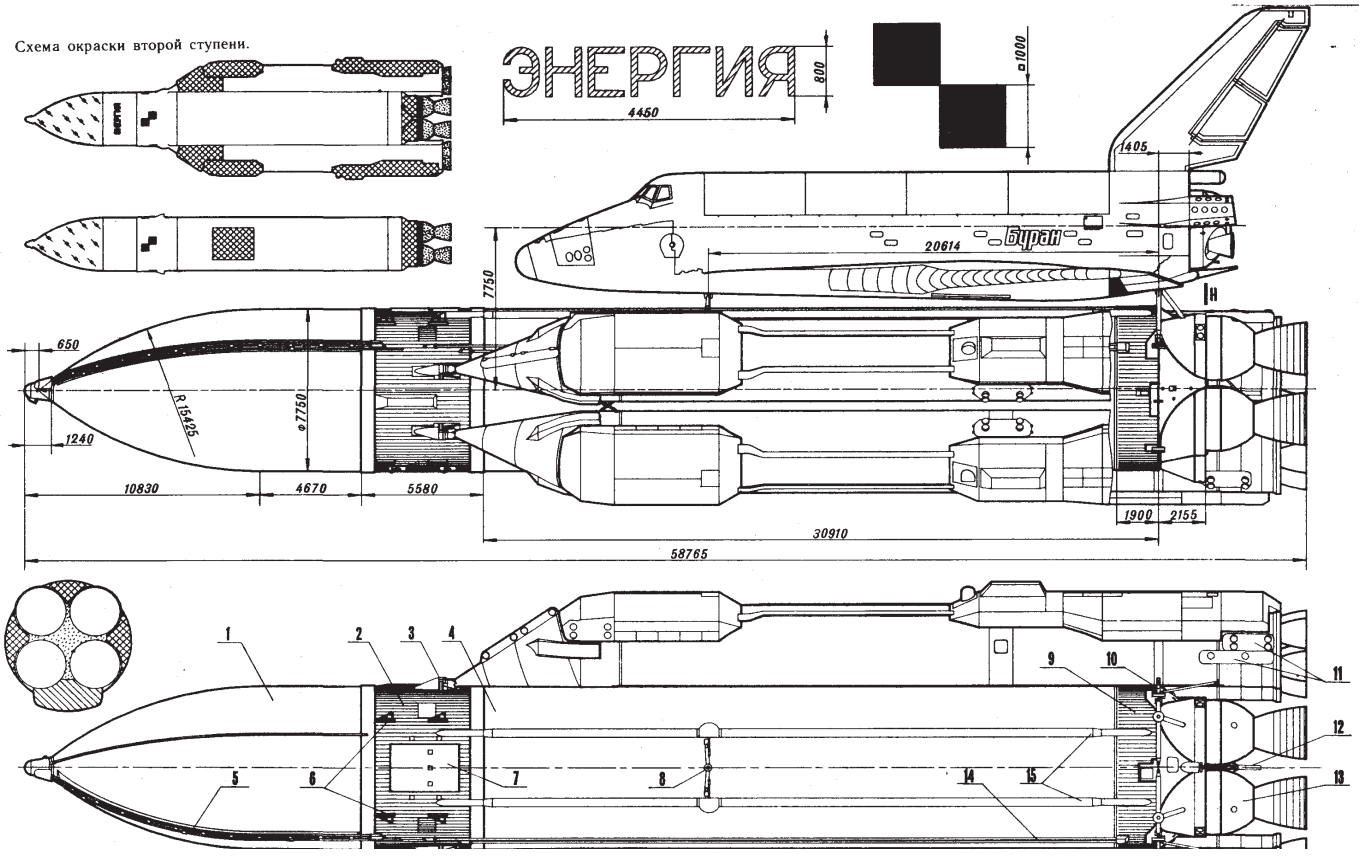
Свыше 85% LTE-устройств и в натуральном, и в денежном выражении – это смартфоны. Продажи «умных» телефонов с поддержкой 4G за первые 3 месяца увеличились на 28 % в штуках до 865 тыс. устройств, в деньгах – на 40% до 21,5 млрд. рублей. Таким образом, даже на фоне снижающегося рынка смартфоны с LTE остаются одной из немногих категорий, растущих двузначно.

Перспективы LTE

LTE длительное время развивался очень медленно из-за отсутствия достаточного количества устройств и их высокой стоимости, что сказывалось на подключениях, ввиду высокого «входного билета». Сейчас, практически во всех регионах РФ, спрос на мобильные устройства с поддержкой LTE значительно увеличился, что операторам позволяет набирать абонентские базы. Можно утверждать, что 2 половина 2015 года и 1 половина 2016 года будут очень активными на число подключаемых абонентов и технология LTE сможет занять значительную долю в общей динамике продаж. Главная задача операторов, поддерживать и оптимизировать собственные сети, чтобы не снижать скоростных характеристик. На 1 квартал 2015, по данным TelecomDaily, число активных абонентов LTE в России составляет порядка 13 млн., а по итогам всего 2015 года превысит отметку в 20 млн.

В целом в 2015 году проникновение услуг мобильной связи 4G (LTE) будет расти во всех регионах РФ, а «Билайн» должен будет активно включиться в гонку со своими основными конкурентами, что не исключает сотрудничества «большой тройки» в рамках RAN Sharing. За первые 4 месяца 2015 года были осуществлены 9 новых запусков LTE-сетей операторами в разных регионах РФ, и до конца года их количество будет исчисляться десятками.

Качественно новых уровень потребления услуг LTE в России может быть достигнут не ранее 2016 года и далее за счёт органического роста в силу озвученных выше факторов: завершение строительства сетей LTE крупнейшими игроками, увеличения проникновения устройств с поддержкой LTE и LTE-A среди массовых пользователей, роста спроса на большие объемы мобильного трафика данных.



СПОСОБ ФОРМИРОВАНИЯ СХЕМНЫХ ФРАГМЕНТОВ ПО ГОЛОСОВЫМ ЗАПРОСАМ ОБСЛУЖИВАЮЩЕГО ПЕРСОНАЛА В СИСТЕМАХ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ

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

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

Ключевые слова:
электрическая схема, голосовой запрос, схемно-ориентированный запрос, паттерн, восстановление радиоэлектронной аппаратуры.

АННОТАЦИЯ

В существующих системах работа с комплектом электрических схемам базируются на традиционных запросных методах предоставления информации из структурированных массивов и баз данных. Используемые методы обладают недостаточной информативностью, так как не позволяют в структуре запросов учитывать особенности концептуального представления электрических схем в терминах и понятиях предметной области. Это приводит к необходимости формирования большого числа запросов для извлечения требуемой технической информации из электрических схем и негативно отражается на времени восстановлении радиоэлектронной аппаратуры.

Повышение эффективности работы обслуживающего персонала со схемами при восстановлении радиоэлектронной аппаратуры может быть обеспечено путем совершенствования средств формирования запросов за счет использования в запросах терминов и понятий электрических схем на основе конструкций естественно-подобного схемно-ориентированного языка запросов. Использование естественно-подобного языка обеспечивает возможность предоставления обслуживающему персоналу средств голосового ввода схемно-ориентированных запросов. Учитывая, что голосовой процессор преобразует запрос тестовую форму с сохранением языковой структуры запросов, именно текстовые запросы выступают основой для решения задачи формирования схемных фрагментов.

Предлагается способ интерпретации текстовых схемно-ориентированных запросов обслуживающего персонала, направленный на выполнение автоматического анализа условий, определяемых обслуживающим персоналом в запросах, и подготовки графических фрагментов электрических схем, содержащих требуемую техническую информацию, для визуализации.

В качестве формальной основы способа интерпретации предлагается использовать совокупность моделей, представляющих в структурированной форме исходные данные для описания схемно-ориентированных запросов и электрических схем. Разнообразие используемых моделей позволяет при интерпретации отразить предметный, языковой и графический аспекты представления радиоэлектронной аппаратуры, которые тесно связаны между собой при визуализации фрагментов электрических схем.

Способ интерпретации схемно-ориентированных запросов предлагается реализовать в виде трех последовательных процедур, назначение каждой из которых определяется общей задачей интерпретации: грамматический анализ схемно-ориентированных запросов, предметная интерпретация предложения запроса, формирование графического контекста для средств визуализации.

Предложенный способ позволяет автоматизировать операции предоставления обслуживающему персоналу схемных фрагментов, содержащих необходимую техническую информацию, по голосовым запросам. Формализация и общая логика предложенной структуры способа интерпретации являются основой для его программной реализации, что позволяет повысить уровень автоматизации процессов технической эксплуатации и сократить время восстановления радиоэлектронной аппаратуры за счет уменьшения времени на извлечение требуемой технической информации по запросам обслуживающего персонала.

Одним из основных информационных ресурсов, используемых обслуживающим персоналом при восстановлении сложных технических комплексов, является комплект электрических схем на радиоэлектронную аппаратуру (РЭА). При выполнении операций по восстановлению РЭА обслуживающий персонал работает с фрагментами электрических схем, содержащих необходимую техническую информацию. Предоставление соответствующих фрагментов электрических схем в процессе восстановления РЭА по запросам обслуживающему персоналу (ОП) возлагается на системы информационной поддержки (СИП).

В существующих СИП работа с комплектом электрических схемам базируются на традиционных запросных методах предоставления информации из структурированных массивов и баз данных, основанных на использовании формальных языков, таких как SQL, XQuery, XPath, LinQ. Такие запросные языки являются универсальными с точки зрения формирования разнообразных запросов, однако они не позволяют в структуре запросов учитывать особенности концептуального представления электрических схем в терминах и понятиях предметной области. Следствием этого является недостаточно высокая информативность использующихся в СИП запросных методов, что приводит к необходимости формирования большого числа запросов для извлечения требуемой технической информации из электрических схем и негативно отражается на времени восстановлении РЭА [8].

Повышение эффективности способов работы ОП со схемами при восстановлении РЭА может быть обеспечено путем совершенствования средств формирования запросов за счет использования в запросах терминов и понятий электрических схем на основе конструкций естественно-подобного языка, который в работе [5] назван схемно-ориентированным языком запросов (СОЯЗ). Использование естественно-подобного языка обеспечивает возможность предоставления обслуживающему персоналу средств голосового ввода схемно-ориентированных запросов (СОЗ). Особенностью использования голосовых схемно-ориентированных запросов СОЗГ состоит в том, что в СИП с помощью голосового процессора осуществляется промежуточное преобразование СОЗГ в тестовые запросы СОЗТ с сохранением языковой структуры запросов. При этом текстовые запросы СОЗТ выступают основой для решения задачи формирования схемных фрагментов, удовлетворяющих условиям СОЗ.

Поскольку при такой организации обработки запросов языковую основу определяет СОЯЗ, то решение названной задачи требует создания интерпретатора текстовых схемно-ориентированных запросов обслуживающего персонала, что связано с необходимостью разработки соответствующего способа интерпретации и его реализации в виде программного продукта. С прикладной точки зрения способ интерпретации схемно-ориентированных запросов предназначен для выполнения автоматического анализа условий, определяемых обслуживающим персоналом в запросах, и подготовки графических фрагментов электрических схем, содержащих требуемую техническую информацию, для визуализации.

Принцип интерпретации схемно-ориентированных запросов

Функционально преобразование для реализации предлагаемого способа интерпретации СОЗ на основе комплекта электрических схем S может быть представлено в виде оператора $И$, применение которого к запросу со стороны обслуживающего персонала обеспечивает автоматическое формирование графического контекста $ГК_{СОЗ} = И(S, СОЗТ)$ в виде набора паттернов для визуализации соответствующего схемного фрагмента $СФ_{СОЗ}$ (рис. 1).

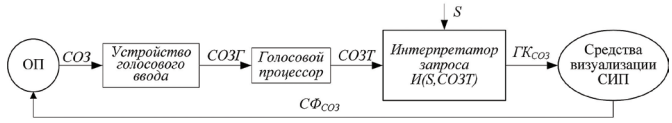


Рис. 1. Принцип интерптетации схемно-ориентированных запросов обслуживающего персонала

В качестве формальной основы способа интерпретации СОЗ целесообразно использовать следующую совокупность моделей, представляющих в структурированной форме исходные данные для описания СОЗ и электрических схем S:

предикатная модель ПМ СОЗ [5], определяющая формальную структуру запроса;

синтаксис G и семантика ω языка СОЯЗ [5], определяющие правила формирования СОЗ на естественно-подобном языке;

фреймовая модель ФМ РЭА [6], обеспечивающая концептуальное представление электрических схем РЭА в предметных понятиях;

предметно-графическая объектная модель ПГОМ [7],которая определяет набор паттернов, предназначенных для визуализации схемных фрагментов, и представляет собой объединение предметной объектной модели ПОМ РЭА и графической объектной модели ГОМ электрических схем РЭА.

Разнообразие используемых моделей позволяет при интерпретации отразить как предметный, так и графический аспект представления РЭА, который тесно связан с визуализацией электрических схем средствами отображения информации в СИП.

Алгоритмически предлагаемый способ интерпретации СОЗ целесообразно реализовать в виде последовательности процедур, назначение каждой из которых определяется общей задачей интерпретации (рис. 2):

грамматический анализ СОЗТ для выделения команды запроса $К_{СОЗ}$ и предложения запроса $П_{СОЗ}$;

предметная интерпретация $ПИ_{СОЗ}$ предложения $П_{СОЗ}$ запроса;

формирование графического контекста $ГК_{СОЗ}$ схемного фрагмента $СФ_{СОЗ}$.

На рисунке 2 показана соответствующая последовательность операций, выполняемых над исходным запросом СОЗТ, который обслуживающий персонал формирует на языке СОЯЗ, а также распределение по операциям используемых моделей, выступающих в качестве информационных ресурсов.

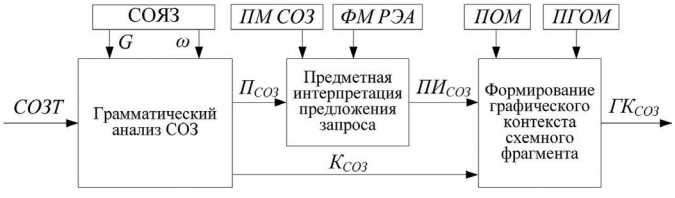


Рис. 2. Структура способа интерпретации схемно-ориентированных запросов обслуживающего персонала

Грамматический анализ схемно-ориентированных запросов

Цель грамматического анализа состоит в определении принадлежности предложений запроса языку СОЯЗ. В соответствии со сложившимися принципами теории формальных языков [4] при выполнении грамматического анализа необходимо последовательно провести операции лексического, синтаксического и семантического анализа текстового СОЗ (рис. 3). При этом правила выполнения этих операций определяются формальными моделями грамматики G и семантики ω языка СОЯЗ.

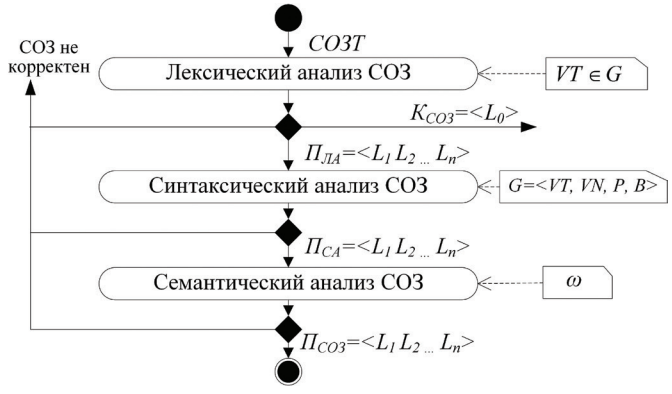


Рис. 3. Структура процедуры грамматического анализа схемно-ориентированного запроса

С точки зрения лексического анализа всякий СОЗ представляется в виде цепочки лексем $<L_0\ L_1\ \ldots\ L_n>$. Лексический анализ направлен на распознавание лексем в структуре СОЗ и выполняется на основе словаря терминов, определяемых множеством VT терминальных символов грамматики G. Выделение и анализ лексем $L_i \in СОЗ$ в контексте запроса является операцией обработки тестовых строк и осуществляется путём отождествления лексем с терминальными символами грамматики G. Например, в запросах $СОЗ_1$=«Показать блок, который содержит ячейку, причем ячейка содержит разъем Ш1» или $СОЗ_2$ =«Скрыть цепь 27 вольт, которая связана с блоком Б1», лексемами являются все слова, разделенные пробелами.

После выполнения лексического анализа запрос логически делится на две части: командную часть запроса $К_{СОЗ} = <L_0>$ и предложение $П_{ЛА} = <L_1\ L_2\ \ldots\ L_n>$, определяющее условия запроса. В вышеприведенных примерах лексемой L_0 являются слова «показать» или «скрыть». Лексема L_0 после выполнения лексического анализа непосредственно передается в процедуру формирования графического контекста в качестве команды для управления визуализацией.

Синтаксический анализ проводится на основе грамматического разбора лексически корректного предложения $П_{ЛА} = <L_1\ L_2 \ldots L_n>$ для проверки соответствия структуры предложения правилам грамматики G. Совокупность синтаксических правил определяется грамматикой $G=<VT, VN, P, B>$ [5], в которой множество правил вывода P задано в форме РБНФ. Поскольку грамматика G является контекстно-свободной, то для выполнения процедуры грамматического разбора можно использовать известные методы теории формальных языков (дерево вывода, магазинный автомат), представленные в литературе [1; 2; 3; 4].

Для синтаксически корректных предложений $П_{ЛА} = <L_1 L_2 \ldots L_n>$ должен выполняться семантический анализ, который основан на применении семантических правил $\omega_1, \omega_2 \in \omega$, определенных в [5]. Особенности структуры этих правил обуславливают следующих порядок их применения к предложениям $П_{СА}$: первым применяется правило ω_1, а вторым – ω_2. Учитывая, что в работе [5] данные правила задаются в табличном виде, выполнение семантического анализа осуществляется путём последовательного анализа цепочек лексем предложения $П_{СА}$ на соответствие правилам ω_1 и ω_2. Сематический анализ завершает процедуру грамматического анализа. В результате выполнения грамматического анализа осуществляется структуризация СОЗ и подтверждение грамматической корректности предложения $П_{СОЗ}$.

Предметная интерпретация предложения запроса

После проведения грамматического анализа СОЗ формальная предикатная структура предложения $П_{СОЗ}$ скрыта в контексте запроса из-за использования конструкций естественно-подобного языка. Поэтому для предметной интерпретации предложения запроса $П_{СОЗ}$ предлагается выполнить последовательность операций, показанных на рис. 4.

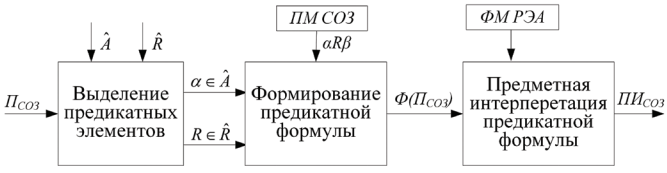


Рис. 4. Процедура формирования предикатной формулы предложения схемно-ориентированного запроса

Вначале производится выделение предикатных элементов в структуре предложения $П_{СОЗ}$. Для этого устанавливается соответствие лексем $L_n \in П_{СОЗ}$ элементам множеств понятий $\hat{A}$ и отношений $\hat{R}$, определяемых фреймовой моделью ФМ РЭА и предикатной моделью ПМ СОЗ соответственно. После этого каждой лексеме ставится в соответствие либо некоторый элемент множества $\hat{A}$, либо некоторое отношение из множества $\hat{R}$. Далее в соответствие с предикатной моделью ПМ СОЗ осуществляется формирование элементарных предикатных выражений (предикатов) в виде xR_1y, yR_2z, ..., где $x, y, z \in \hat{A}$, а $R_i \in \hat{R}$. При этом одновременно на основе анализа лексем определяются символы логических операций, использованных в предложении $П_{СОЗ}$.

Элементарные предикатные выражения используются для формирования предикатной формулы $Ф(П_{СОЗ})$, которая в формальном виде представляет условие $У_{СОЗ}$, определяющее свойства требуемого схемного фрагмента в запросе ОП.

Предикатная формула $Ф(П_{СОЗ})$ формируется на основе предикатной формы $Е(П_{СОЗ})$, которая отражает структуру условия $У_{СОЗ}$. Предикатная форма $Е(П_{СОЗ})$ определяет предикатную структуру предложения $П_{СОЗ}$ и образуется путем конкатенации элементарных предикатов на основе логической операции «и»: $Е(П_{СОЗ}) = Е_{СОЗ}(x, y, z, ...) = (xR_1y)(yR_2z)...$.

Так, для предложения $П_{СОЗ_1}$ = «блок, который содержит ячейку, причем ячейка содержит разъем Ш1», полученного в результате грамматического анализа приведенного выше запроса $СОЗ_1$, предикатная форма имеет вид:

$$\begin{gathered} Е(П_{СОЗ_1}) = Е_{СОЗ}(x, y, z, w) = \\ = (x_{блок} R_{содержит} y_{ячейку}) * (x_{блок} R_{содержит} z_{разъем}) * \\ * (z_{разъем} R_{имеет} w_{маркировку}) * (w_{маркировка} R_{есть} Ш1) \end{gathered} \quad (1)$$

В этой записи $x_{блок}$, $y_{ячейку}$, $z_{разъем}$, $w_{маркировка}$ являются переменными величинами предметной области, а величина $Ш1$ является предметной константой.

Каждый элементарный предикат в форме $Е(П_{СОЗ})$ представляет собой элемент условия $У_{СОЗ}$. Для формирования предикатной формулы $Ф(П_{СОЗ})$ необходимо в предикатной форме $Е(П_{СОЗ})$ применить кванторы общности и существования по отношению к переменным величинам x, y,... предметной области, как описано в [5]. Соответственно этому в общем виде предикатную формулу $Ф(П_{СОЗ})$, определяющую формальную запись условий $У_{СОЗ}$, можно записать в виде:

$$У_{СОЗ} \to Ф(П_{СОЗ}) \to (\forall x)(\exists y)(\exists z)...((xRy)(yRz)...). \quad (2)$$

В такой записи переменная x является основной, а переменные y, z, … – альтернативными. Фактически $Ф(П_{СОЗ})$ можно рассматривать как шаблон, который может быть составлен по предикатной форме $Е(П_{СОЗ})$. С точки зрения программной реализации предлагаемого способа интерпретации этот шаблон определяет структуру информационных запросов (в частности, SQL-запросов, LinQ-запросов) к структурированным данным, представляемым фреймовой моделью ФМ РЭА.

Применительно к предикатной форме $Е(П_{СОЗ_1})$ для предложения $СОЗ_1$ соответствующая предикатная формула $Ф(П_{СОЗ_1})$, на основании которой может производиться предметная интерпретация запроса $СОЗ_1$, имеет следующий вид:

$$\begin{gathered} У_{СОЗ_1} \to Ф(П_{СОЗ_1}) \to \\ (\forall x_{блок})(\exists y_{ячейку})(\exists z_{разъем})(\exists w_{маркировка}) \\ ((x_{блок} R_{содержит} y_{ячейка})(y_{ячейка} R_{содержит} z_{разъем}) \\ (z_{разъем} R_{имеет} w_{маркировкf}) * (w_{маркировка} R_{есть} Ш1)) \end{gathered} \quad (3)$$

Полученная запись (3) является математической конструкцией, которая определяет предикатную формулу условий $Y_{СОЗ_1}$, определяющих свойства требуемого схемного фрагмента на естественно-подобном языке в предложении $П_{СОЗ_1}$ запроса $СОЗ_1$.

Предметная интерпретация предикатной формулы $Ф(П_{СОЗ})$ определяется носителем интерпретации, в качестве которого выступает фреймовая модель ФМ РЭА. При этом результатом предметной интерпретации предикатной формулы $Ф(П_{СОЗ})$ является множество всех структурных схемных элементов, определяемых значениями основной предметной переменной x, для которых наборы значений предметных альтернативных переменных y, z,…определяют множество истинности предикатного выражения $Ф(П_{СОЗ})$.

Таким образом, предметная интерпретация предикатной формулы $Ф(П_{СОЗ})$ формально может быть записана в виде множества $ПИ_{СОЗ} = \{x | \exists y \exists ... Y(x, y, ...)\}$которое определяет совокупность всех схемных элементов, удовлетворяющих условию $Y_{СОЗ}$. Например, в предположении, что предметной интерпретацией запроса $СОЗ_1$ являются блоки А1 и Б4, множество $ПИ_{СОЗ_1}$ представляется в виде: $ПИ_{СОЗ_1}$ = {"*блок* А1", "*блок* Б4"}.

Схемные элементы, входящие в множество $ПИ_{СОЗ}$, выступают в качестве информационной основы для процедуры формирования графического контекста $ГК_{СОЗ}$ схемного фрагмента $СФ_{СОЗ}$, который соответствует условиям $Y_{СОЗ}$, определенным ОП в СОЗ.

Формирование графического контекста схемного фрагмента

Необходимость выполнения процедуры формирования графического контекста $ГК_{СОЗ}$ схемного фрагмента объясняется тем, что множество предметных понятий, определяющих структурные схемные элементы множе-

ства $ПИ_{СОЗ}$, получаемые после процедуры предметной интерпретации запроса, не может непосредственно использоваться графическими системами. Рассматриваемая процедура завершает процесс интерпретации СОЗ и фактически определяет предметно-графический интерфейс, позволяющий перейти от понятийного контекста, представленного в $ПИ_{СОЗ}$, к графическому контексту $ГК_{СОЗ}$, который предназначен для визуализации схемного фрагмента $СФ_{СОЗ}$ средствами графической системы СИП (рис. 5).

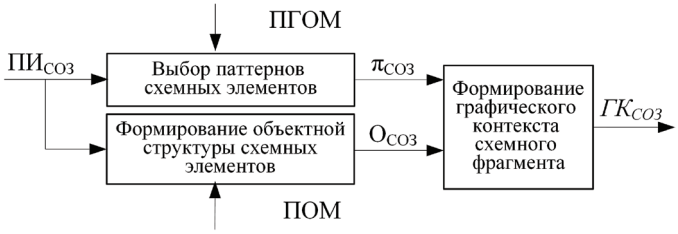


Рис. 5. Структура процедуры формирования графического контекста схемного фрагмента

В качестве основы рассматриваемой процедуры предлагается использовать две объектные модели разработанные в работе [7]: предметно-ориентированную модель РЭА (ПОМ) и предметно-графическую объектную модель электрических схем РЭА (ПГОМ). Эти модели образуют информационный ресурс для реализации процедуры и отражают предметный и схемно-графический аспекты, определяющие содержание СОЗ.

В структуре процедуры выделяются три операции, представленные на рисунке 5:

выбор паттернов схемных элементов, определяющих формируемый схемный фрагмент $СФ_{СОЗ}$,

формирование объектной структуры схемных элементов, входящих в фрагмент $СФ_{СОЗ}$,

формирование графического контекста $ГК_{СОЗ}$ схемного фрагмента $СФ_{СОЗ}$.

Операция выбора паттернов основана на сопоставлении типов схемных элементов множества $ПИ_{СОЗ}$ объектам ПГОМ и отборе множества паттернов $\pi_{СОЗ} \subseteq ПГОМ$ по признаку совпадения типов. Применительно к $ПИ_{СОЗ_1}$ множество $\pi_{СОЗ_1}$ содержит один паттерн $\pi_{блок} \in ПГОМ$, так как "*блок А1*" $\rightarrow \pi_{блок}$ и "*блок Б4*" $\rightarrow \pi_{блок}$, причем выбранный паттерн $\pi_{блок}$ определяет графическое представлению схемного элемента «блок» в комплекте электрических схем РЭА. При этом следует отметить, что паттерны множества $\pi_{СОЗ}$ определяют все графические шаблоны, необходимые для формирования требуемого схемного фрагмента $СФ_{СОЗ}$.

Операция формирования объектной структуры схемных элементов основана на сопоставлении элементов множества $ПИ_{СОЗ}$ объектам ПОМ и опреде-

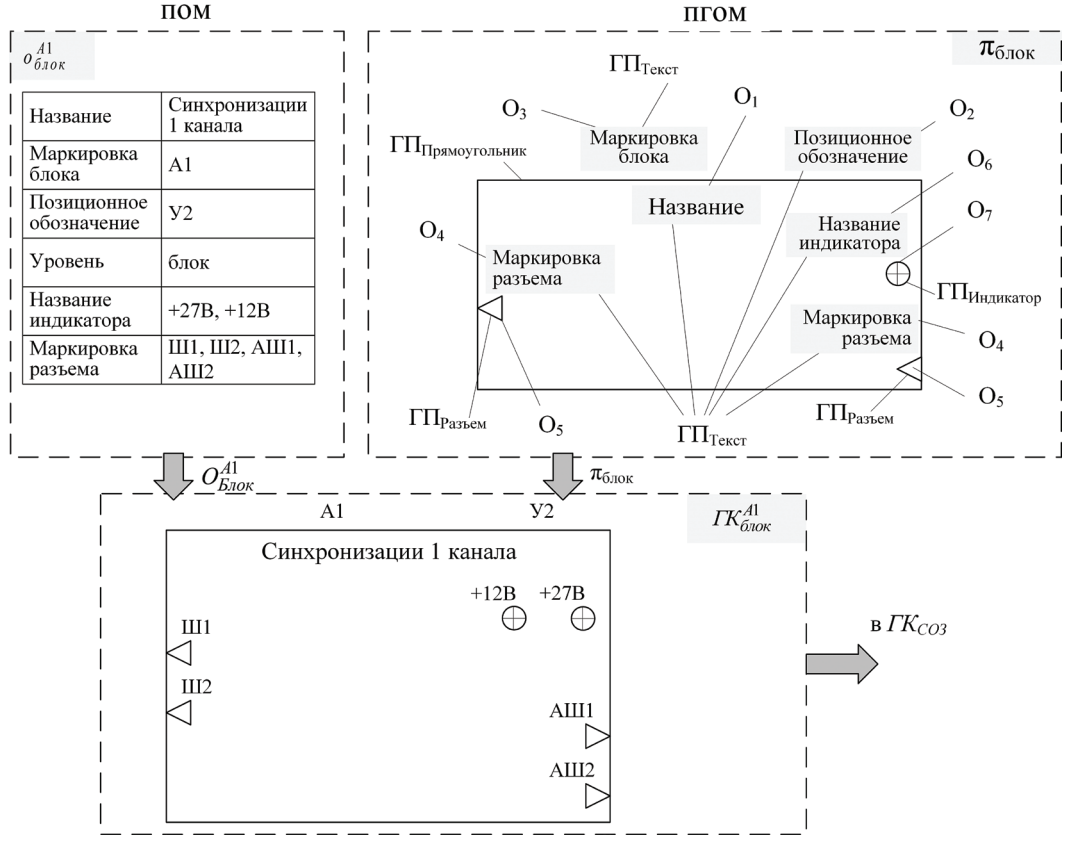


Рис. 6. Принцип формирования графического контекста

лении множества соответствующих объектов $O_{СОЗ}$, являющихся подмножеством объектов ПОМ. Применительно к $ПИ_{СОЗ_1}$ множество $O_{СОЗ_1}$ должно содержать два объекта $o^{А1}_{блок}$, $o^{Б4}_{блок} \in ПОМ$, содержащих свойства соответствующих схемных элементов, таких, что "*блок А*1" $\rightarrow o^{А1}_{блок}$ и "*блок Б*4" $\rightarrow o^{Б4}_{блок}$. В общем случае модель ПОМ полностью характеризует свойства всех объектов $o \in O_{СОЗ}$.

Формирование графического контекста $ГК_{СОЗ}$ основывается на совмещении двух представлений $\pi_{СОЗ}$ и $O_{СОЗ}$ требуемого схемного фрагмента. Контекстная структура каждого формируемого паттерна $\pi \in \pi_{СОЗ}$ образуется путем заполнения всех предметных элементов паттернов значениями свойств из соответствующих объектов $o \in O_{СОЗ}$ и тем самым осуществляется конфигурирование контекстной и графической структуры. При этом контекстная структура формируемых паттернов схемных элементов определяется выбранными правилами размещения графических примитивов *ГП* на основе соответствующего паттерна-шаблона. Интегрированные таким образом данные полностью определяют графический контекст $ГК_{СОЗ}$, достаточный для визуализации схемного фрагмента $СФ_{СОЗ}$ с помощью графических средств СИП.

Принцип формирования графического контекста $ГК^{А1}_{блок}$ для гипотетического блока А1 иллюстрируется на рисунке 6. В соответствии с изложенным выше подходом при формировании графического контекста $ГК^{А1}_{блок}$ используются объект $o^{А1}_{блок}$, представляющий блок А1 в модели ПОМ, а также паттерн $\pi_{блок}$, определяющий шаблон для графического представления блоков.

Аналогичным образом формируется графический контекст для схемных элементов других типов (цепь, ячейка, разъем и т.п.) в составе множества $ПИ_{СОЗ}$. В результате формируется полный графический контекст $ГК_{СОЗ}$, определяющий требуемый схемный фрагмент для визуализации.

Заключение

Предложенный способ позволяет автоматизировать операции предоставления обслуживающему персоналу схемных фрагментов, содержащих необходимую техническую информацию, по голосовым запросам. Особенностью предлагаемого способа является использование совокупности предметных и графических моделей в качестве информационного ресурса, что позволяет совместить два соответствующих аспекта представления электрических схем РЭА.

Функционально предложенный способ формирования схемных фрагментов реализует преобразование голосового схемно-ориентированного запроса на естественно-подобном языке в графический контекст для отображения фрагмента электрических схем средствами визуализации СИП. Предлагаемый способ следует рассматривать как мультимедийный интерфейс ОП в СИП, что хорошо согласуется с современными направлениями развития средств автоматизации.

Формализация и общая логика предложенной структуры способа являются основой для его программной реализации, как компонента систем информационной поддержки. Реализация способа в значительной степени определяется используемыми средствами визуализации, на основе которых создается графическое представление электрических схем РЭА в СИП.

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. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. М.: Мир, 1978. Т.1. 612 с. Т. 2. 487 с.

2. Грис Д. Конструирование компиляторов для цифровых вычислительных машин. М.: Мир. 1975. 544 с.

3. Сеймур Гинзбург. Математическая теория контекстно-свободных языков. М.: Мир, 1970. 326 с.

4. Системное программное обеспечение / А.В. Гордеев, А.Ю. Молчанов. СПб.: Питер. 2004. 736 с.

5. Анисимов О.В., Попов Т.А. Структура схемно-ориентированных запросов для систем информационной поддержки процесса восстановления радиоэлектронной аппаратуры // Вестник ЯЗРИ ПВО. Ярославль. 2015. № 1.

6. 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.

7. Курчидис В.А., Анисимов О.В., Попов Т.А. Формирование предметно-ориентированного графического описания радиоэлектронной аппаратуры // Вестник ЯЗРИ ПВО. Ярославль. 2015. № 2.

8. Рыбакин А.А., Курчидис В.А., Анисимов О.В. Метод формирования виртуальных документов для информационного обеспечения ОП при эксплуатации вооружения. Вестник ВУНЦ ВВС «ВВА» . Ярославль. 2012.

Для цитирования:

Анисимов О.В., Курчидис В.А., Попов Т.А. Способ формирования схемных фрагментов по голосовым запросам обслуживающего персонала в системах информационной поддержки // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 28–34.

METHOD OF FORMING SCHEMATICS FRAGMENTS A VOICE QUERY SERVICE PERSONNEL FOR INFORMATION SUPPORT SYSTEMS

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

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

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

Abstract
The work with a set of electrical schemes in existing systems is based on traditional interrogation methods of information providing from the structured arrays and databases. The used methods are not sufficiently informative, as they do not allow the structure queries to take into account the peculiarities of the conceptual representation of electric schemes in terms of the subject area. This leads to the need forming a large number of requests for retrieval of the requested technical information from the electrical schemes and has a negative time effect relative to recovery of electronic equipment. The efficiency improving of the staff work with the schemes when restoring electronic equipment is based on improved means of queries forming. It is suggested in requests to use the terms and concepts of electrical schemes based on the design of naturally-like circuit-oriented language. The use of natural-like language provides the possibility for the staff to apply the voice input means of circuit-oriented queries.
The interpreting method is offered for voice scheme oriented queries of staff . It is aimed to implementing of automatic analysis of the conditions, defined in staff queries, and preparing the graphic elements of electrical schemes containing the required technical information for visualization.
A formal basis of the method of interpretation is a set of models representing structured data source for describing of scheme-oriented applications and electrical schemes. A variety of used models helps the method to reflect the subject, linguistic and graphical aspects of the submission of electronic equipment, which are closely related with the visualization of the electrical schemes fragments.
The interpretation of scheme oriented queries is implemented in the form of three consecutive procedures. The purpose of each procedure is defined by a common task of interpretation: grammatical analysis of scheme oriented queries, substantive interpretation of the query suggestions, the forming of a graphics context for rendering capabilities. The voice processor translates the query in a text form with preservation of the linguistic structure of queries. The named procedures are applied to requests in text form.
The proposed method allows to automate the operation of providing the staff for the scheme fragments that contain the necessary technical information in voice queries. The general formalization logic and proposed method of interpretation are the basis for its software implementation. Application of the proposed method allows to increase the automation level of technical exploitation processes and reduce the time of recovery of electronic equipment by reducing the time to retrieve a staff by the required technical information.

Keywords: electrical scheme, voice query, scheme-oriented query, pattern, recovery of radio electronic equipment..

References
1. Aho A., Ulman J. Teoriya sintaksicheskogo analiza, perevoda i kompilyatsii [The theory of parsing, translation and compiling]. Moscow: Mir. 1978. Vol. 1. 612 p. Vol. 2. 478 p. (in Russian).
2. Gries D. Konstruirovanie kompilyatorov dlya tsifrovykh vychislitel'nykh mashin [Compiler Construction for Digital Computers]. Moscow: Mir. 1975. 544 p. (in Russian).
3. Ginsburg S. Matematicheskaya teoriya kontekstno-svobodnykh yazy'kov [The Mathematical Theory of Context-free Languages]. Moscow: Mir, 1970. 326 p. (in Russian).
4. Gordeev A.V., Molchanov A.Yu. Sistemnoe programmnoe obespechenie [System Software]. Sankt Peterburg: Piter. 2004. 736 p. (in Russian).
5. Anisimov O.V., Popov T.A. The structure of the shemes-oriented requests for information systems support for the recovery of electronic equipment. Vestnik YaZRI PVO. Yaroslavl. 2015. No. 1. (in Russian).
6. 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).
7. Anisimov O.V., Kurchidis V.A., Popov T.A. 2015, Formation of the domain-specific graphic description of electronic equipment. Vestnik YaZRI PVO. Yaroslavl. Vol. 2. (in Russian).
8. Ribakin A.A., Kurchidis V.A., Anisimov O.V. The method of formation of virtual documents to inform the staff in the operation of weapons. Vestnik VUNTs VVS «VVA». Yaroslavl. 2012. Vol. 2. (in Russian).

Information about authors:
Anisimov O.V., Ph.D., associate professor, docent Automation (and computing devices), Military Space Academy;
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.

For citation:
Anisimov O.V., Kurchidis V.A., Popov O.V. Method of forming schematics fragments a voice query service personnel for information support systems. H&ES Research. 2015. Vol. 7. No. 4. Pp. 28–34. (in Russian).

ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ
ИМЕНИ А.Ф. МОЖАЙСКОГО

25 ноября 2015

САНКТ-ПЕТЕРБУРГ

ВСЕРОССИЙСКАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ПРОБЛЕМЫ РАЗВИТИЯ И СОВЕРШЕНСТВОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ВОЕННОГО НАЗНАЧЕНИЯ

nauka-i-asu.ru

konferencia_asu_vka@mail.ru

при информационной
поддержке научно-технического
журнала H&ES Research

ТРЕБОВАНИЯ К АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ФОРМИРОВАНИЯ И ВЕДЕНИЯ ФЕДЕРАЛЬНОГО РЕЕСТРА ДОКУМЕНТОВ ОБ ОБРАЗОВАНИИ

Исаева
Людмила Николаевна,
к.т.н., доцент кафедры информационной безопасности и автоматизации ФГОБУ ВПО Московский технический университет связи и информатики, г. Москва, Россия
isaeva@homologation.ru

Раев
Константин Валерьевич,
магистрант кафедры информационной безопасности и автоматизации ФГОБУ ВПО Московский технический университет связи и информатики, г. Москва, Россия
raevkv@outlook.com

Ключевые слова:
документ об образовании, документ об обучении, реестр документов об образовании, АИС ФРДО, «открытый» web-сервер, «закрытый» web-сервер.

АННОТАЦИЯ

В соответствии с Федеральным законом от 29.12.2013 № 273-ФЗ «Об образовании в Российской Федерации», Федеральная служба по надзору в сфере образования и науки (Рособрнадзор) организует формирование и ведение федерального реестра документов об образовании и (или) квалификации, документов об обучении. Выполнение данной функции на современном уровне требует разработки автоматизированной системы формирования и ведения федерального реестра документов об образовании (АИС ФРДО, система).

Частично базовые компоненты автоматизированной системы к настоящему моменту уже реализованы в рамках первой очереди автоматизированной системы поддержки процессов предоставления государственной услуги «Предоставление информации о документах об образовании (среднее, начальное и высшее профессиональное образование) и проверке подлинности бланков документов об образовании (среднее, начальное и высшее профессиональное образование)» в электронном виде. Однако, требуется развитие указанной автоматизированной системы в части комплексного обеспечения процессов формирования и ведения федерального реестра документов об образовании, а также обеспечения защиты телекоммуникационных каналов при формировании федерального реестра.

Целью работы является разработка требований к модернизации системы, в части автоматизации следующих процессов:

– сбор сведений о документах об образовании из образовательных организаций по электронным каналам связи, с применением технологий электронной подписи;

– учет и хранение сведений о документах об образовании;

– предоставление доступа к хранящимся в системе данным для подтверждения наличия сведений о выданных документах.

Проанализирован опыт построения информационных систем, автоматизирующих процессы сбора и хранения сведений о документах об образования на государственном уровне.

По результатам анализа установлены основные требования к информационной безопасности информационных систем подобного класса, требования к архитектуре системы, требования к структуре и составу подсистем.

Результаты работ использованы при формировании технического задания на модернизацию автоматизированной системы формирования и ведения федерального реестра документов об образовании.

Введение

В последнее время в Российской Федерации актуальной становится проблема фальсификации документов о высшем образовании. У работодателей, органов государственной власти и различных органов и организаций отсутствуют инструменты для осуществления оперативной проверки достоверности сведений об образовании, представляемых гражданами.

На сегодняшний день органы и организации, которым необходимо осуществить процедуру проверки подлинности документов об образовании того или иного гражданина, вынуждены осуществлять запрос указанных сведений в письменном виде непосредственно в образовательные организации, выдавшие документ об образовании гражданину.

Вместе с тем, необходимо учитывать, что за период с 1991 г. множество образовательных организаций уже прекратило свою деятельность, и сведения о выданных ими документах переданы в архивные органы.

Таким образом, актуальна задача создания на государственном уровне единого реестра обо всех выданных на территории Российской Федерации документов об образовании и развитии соответствующей автоматизированной системы.

Анализ текущей ситуации учета документов об образовании и опыта построений аналогичных систем

В ходе работ по исследованию бизнес-процессов представления образовательными организациями сведений о документах об образовании и (или) квалификации, документах об обучении в Рособрнадзор, а также анализа международного опыта построения систем хранения сведений по выпускникам образовательных организаций, была спроектирована модель процесса сбора документов об образовании (рис. 1), а также были сформированы базовые требования к автоматизированной системе формирования и ведения федерального реестра документов об образовании, в том числе требования к компонентам системы и её функционированию.

Требования к автоматизированной системе

Автоматизированная информационная система должна обеспечить функционирование полностью электронной схемы сбора сведений из образовательных организаций и сервисов, обеспечивающих предоставление доступа к хранящимся в системе данным для подтверждения наличия в системе сведений о выданных документах для формирования и ведения федерального реестра документов об образовании.

Особенное внимание при проектировании указанной системы, необходимо уделить вопросам информационной безопасности, с учетом того, что в системе планируется хранить и использовать массивы персональных данных выпускников образовательных организаций Российской Федерации.

В ходе разработки требований к системе сделан вывод, что для обеспечения безопасности и разграничения доступа к данным в рамках системы необходимо обеспечить функционирование двух web-серверов – «открытого» и «закрытого». «Открытый сервер» предназначен для предоставления доступа к хранящимся в системе данным для проверки наличия сведений о выданных документах об образовании, с автоматическим протоколированием запросов. «Закрытый» сервер пред-

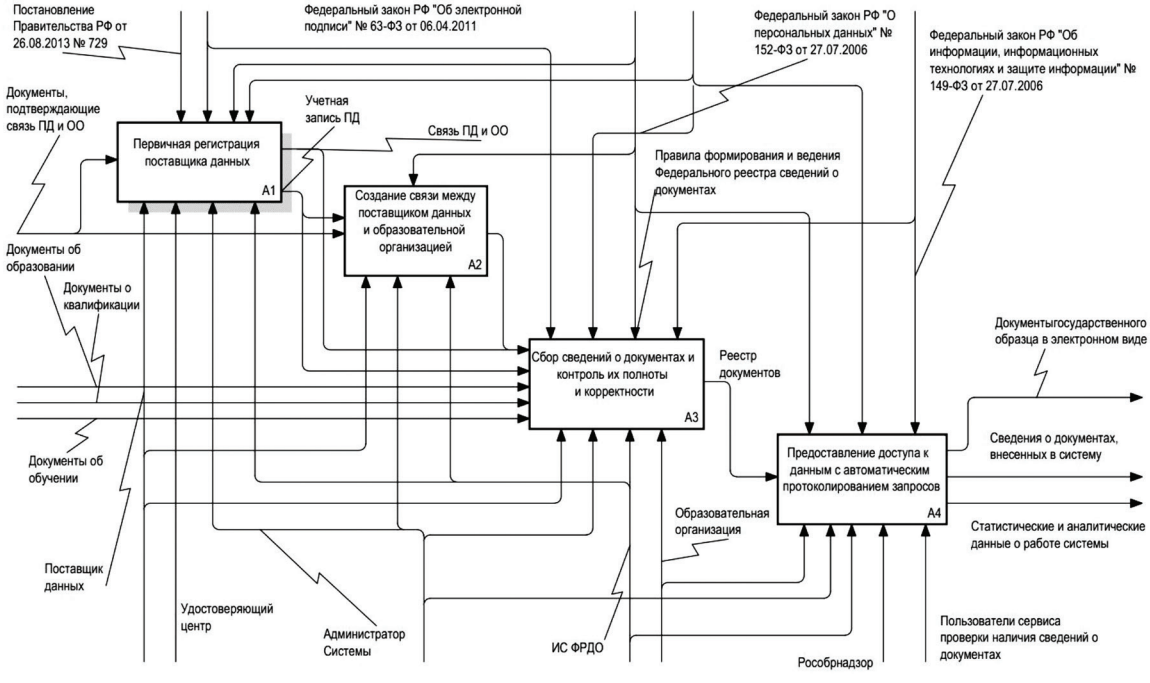


Рис. 1. Модель процесса сбора документов об образовании

назначен для сбора сведений от поставщиков данных, а также для учета и хранения сведений о документах.

Система должна располагаться на серверах оператора за сертифицированным брандмауэром и состоять из следующих пяти блоков:

– «открытый» web-сервер (для проверки наличия сведений о документах об образования без регистрации пользователей);

– «закрытый» web-сервер (остальные подсистемы: сбор сведений о документах, учет и хранение документов и т.д.);

– сервер базы данных, обеспечивающий хранение сведений о выданных документах, выделение необходимых структур внешней памяти, управление транзакциями, журнализацией и репликацией данных;

– сервер приложений, обеспечивающий предоставление сервисов для функционирования подсистем информационной системы;

– сервер проверки подписей, обеспечивающий проверку наличия и достоверности электронной подписи в составе пакета сведений о выданных документах (прямой связи между Удостоверяющим центром Рособрнадзора и сервером проверки подписей нет, сервер проверки подписей должен иметь выход в Интернет для получения сведений об аннулировании сертификатов).

Доступ пользователей системы к «открытому» серверу, а также передача данных, должны осуществляться по сети Internet по открытому трафику.

Доступ пользователей системы к «закрытому» серверу, а также передача данных, должна происходить по внутренней сети VipNet, оператора системы. Предлагаемая архитектура системы приведена на рис. 2.

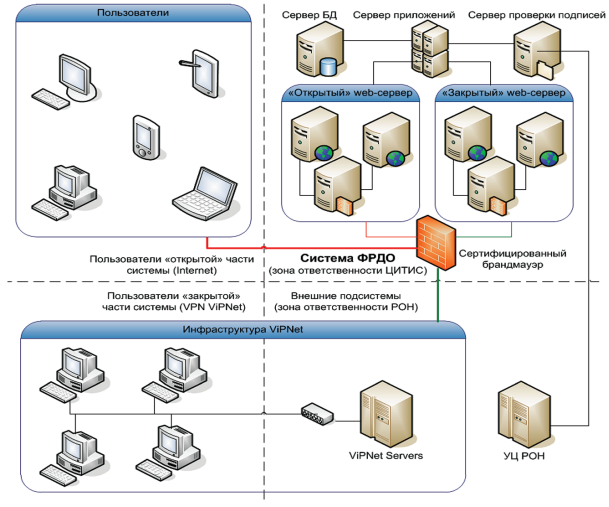


Рис. 2. Предлагаемая архитектура системы

Кроме того, при разработке требований и анализе угроз информационной безопасности, также было установлено, что для повышения безопасности системы функционирование «открытого» и «закрытого» серверов должно выполняться под управлением единого сервера приложений, предоставляющего не связанные между собой сервисы отдельно для «открытого» и «закрытого» серверов.

Система должна иметь централизованную базу хранения информации, а также функционал ввода-вывода данных, предусматривающий web-интерфейс для работы пользователя с ними.

Система должна поддерживать разграничение прав доступа пользователей к объектам и функциональным возможностям подсистем, входящих в состав АИС ФРДО, в соответствии с ролевой моделью. Для получения прав доступа к функциональным возможностям подсистемы сбора сведений из организаций по закрытому каналу, пользователю необходимо иметь сертификат ключа проверки ЭП, выдаваемый аккредитованным удостоверяющим центром.

В системе должен быть реализован принцип однократного ввода информации и механизмы, предотвращающие дублирование информации, нарушение целостности информации.

В АИС ФРДО должна использоваться современная и интуитивно понятная навигация, позволяющая пользователям ориентироваться в функциональных возможностях системы, быстро находить и усваивать нужную информацию.

Для обеспечения возможности подписания сведений о документах непосредственно в интерфейсе браузера при работе в «закрытой» части системы, на клиентском рабочем месте должен быть установлен браузер MicrosoftInternetExplorer 10+ и специализированный плагин для ЭП. Для обеспечения возможности подписания сведений о документах вне интерфейса браузера при работе в «закрытой» части портала, на клиентском рабочем месте может быть установлен альтернативный браузер (Firefox, Safari, Chrome или Opera) и утилита VipNetCryptoFile. Остальные предусмотренные функции системы должны выполняться во всех перечисленных веб-браузерах.

Используемое системное программное обеспечение, а также разработанное программное обеспечение по работе с АИС ФРДО, должно обеспечивать защиту информации от несанкционированного доступа, работу с базой данных только авторизованных клиентов в рамках заданных прав доступа к функциональным возможностям и разделам системы.

Подсистемы АИС ФРДО

Сформированы требования к составу системы, в том числе определены основные подсистемы (компоненты системы):

1. Подсистема «Профессиональное образование», предназначенная для учета и обработки заявлений на предоставление информации о документах об профессиональном образовании государственного образца.

2. Подсистема предоставления государственных услуг на базе сведений федерального реестра, предназначенная для приема, обработки и регистрации электронных и традиционных (бумажных) обращений

за предоставлением сведений из федерального реестра документов об образовании;

3. Подсистема, обеспечивающая сбор сведений из образовательных организаций высшего образования по электронным каналам связи, с применением технологий электронной подписи (функционирует на «закрытом» сервере приложений).

4. Подсистема, обеспечивающая сбор сведений из профессиональных образовательных организаций, общеобразовательных организаций и организаций, ведущих образовательную деятельность, по электронным каналам связи, с применением технологий электронной подписи (функционирует на «закрытом» сервере приложений).

5. Подсистема, обеспечивающая учет и хранение сведений о документах об образовании и (или) о квалификации, документах об обучении (функционирует на «закрытом» сервере приложений).

6. Подсистема, обеспечивающая возможность предоставления доступа к хранящимся в системе данным для подтверждения наличия в системе сведений о выданных документах, а также возможность предоставления доступа к этим сведениям физическим лицам в части, касающейся выданных им документов (функционирует на «открытом» сервере приложений).

7. Подсистема информационной безопасности, предназначенная для обеспечения выполнения требований законодательства и уполномоченных органов к средствам защиты информации и персональных данных в рамках системы.

С четом того, что предлагаемое решение является многокомпонентным необходимо также использовать базовые требования к способам и средствам связи для информационного обмена между компонентами системы.

Информационный обмен между компонентами системы также должен осуществляться через общий доступ к таблицам баз данных системы.

Информационный обмен между компонентами «открытой» части АИС ФРДО, включая сервер БД, сервер приложений в части сервисов открытой части, «открытый» веб-сервер, и пользователями сервиса проверки наличия сведений о документе в системе должен осуществляться по внутренним сетям телекоммуникации с обеспечением удаленного доступа к системе. Выбор протоколов сетевого взаимодействия должен осуществляться с учетом требований к скорости, надежности и безопасности информационного взаимодействия.

Информационный обмен между компонентами «закрытой» части АИС ФРДО, включая сервер БД, сервер приложений в части сервисов закрытой части, «закрытый» веб-сервер, и пользователями организаций – поставщиков данных должен осуществляться по сети VipNet с обеспечением удаленного доступа к системе.

Необходимо также учитывать, что в связи с тем, что предлагаемое решение планируется использовать на федеральном уровне, должны быть разработаны базовые требований к характеристикам взаимосвязей создаваемой системы со смежными системами федерального уровня и уровня субъектов Российской Федерации.

Система должна обеспечивать взаимодействие со смежными системами по локальной сети и внешней сети телекоммуникации (Интернет).

При взаимодействии Системы со смежными системами должны использоваться следующие форматы:

– структурированные сообщения в формате XML;

– структурированные данные в формате CSV.

Взаимодействие может осуществляться по протоколу SOAP, через файловую систему или с помощью прямого обращения к базе данных.

Подсистема предоставления доступа к хранящимся в АИС ФРДО данным для подтверждения наличия сведений о выданных документах должна быть разработана с учетом возможности последующей интеграции с официальным сайтом Рособрнадзора.

Заключение

Разработанные базовые требования к автоматизированной информационной системе формирования и ведения федерального реестра об образовании могут быть использованы при формировании технического задания и технического проекта на модернизацию системы.

Использование разработанных требований также допустимо на этапе разработки комплекта документов (модель угроз, модель нарушителя) для прохождения процедуры сертификации программного обеспечения автоматизированной системы формирования и ведения федерального реестра документов об образовании.

Литература

1. Национальный центр по статистике образования США – официальный сайт. http://nces.ed.gov/ipeds (дата обращения 16.10.2014).

2. Федеральная служба по надзору в сфере образования и науки – официальный сайт. http://obrnadzor.gov.ru (дата обращения 16.10.2014).

3. Трутнев Д.Р. Архитектуры информационных систем. Основы проектирования: учеб. пособие. СПб.: НИУ ИТМО. 2012. 66 с.

4. Стратегия информационной безопасности Российской Федерации до 2020 года от 13 мая 2009 года.

5. Советов Б.Я., Яковлев С.А. Моделирование систем: учебник для вузов. 5-е изд. М.: Высшая школа, 2007. 343 с.

Для цитирования:

Исаева Л.Н., Раев К.В. Требования к автоматизированной системе формирования и ведения федерального реестра документов об образовании // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 36–40.

REQUIREMENTS FOR AN AUTOMATED SYSTEM OF CREATING AND MAINTAINING THE FEDERAL REGISTER OF DOCUMENTS ON EDUCATION

Isayeva Lyudmila Nikolaevna, Moscow, Russian, isaeva@holologation.ru

Raev Konstantin Valeryevich, Moscow, Russian, raevk@outlook.com

Abstract

According to Federal Law On Education in the Russian Federation dated 29.12.2013 No. 273-FL, Federal Education and Science Supervision Service (Rosobrnadzor) organizes the creating and maintenance of the Federal Register of documents on education and (or) qualification, documents on training. Performing this function up-to-date requires the development of formation and maintenance automated system the Federal Register of Documents on Education. (AIS FRDO, system).

By this moment basic components of an automated system have been partially implemented in the first phase of the automated system of supporting the processes of granting State Service «Provision of information about documents on education (secondary, primary and higher education) and authentication of document forms about education (secondary, primary and higher professional education)» into electronic form.

However, the development of specified automated system as a part of complex support formation and maintenance processes of of the Federal Register Educational Documents and telecommunication channels protection during the formation of the Federal Registry is required.

The goal of this work is to develop requirements for system upgrades concerning automation of the following processes:

– gathering information about documents on educationfrom educational organizations using electronic communication channels with the use of electronic signature technologies;

– recording and storage of information about documents on the education;

– providing access to the storing data in the system in order to confirm the stock of information on the documents given.

The experience of building information systems automatingthe process of recording and storing information about documents on education at the national level has been analyzed. According to the analysis the basic requirements for information security system of such levels, the requirements for architecture system, requirements for the structure and composition of subsystems are set.

The results of the work have been used in the formation of technical specifications for the modernization of the automated system of creating and maintaining the Federal Register of documents on education.

Keywords: a document on education, documents on training, the registry of documents on education, AIS FRDO, «open» web server, «closed» web server.

References

1. National Center for Education Statistics (USA) – official website. http://nces.ed.gov/ipeds (accessed 16.10.2014).
2. Federal Education and Science Supervision Service– official site. http://obrnadzor.gov.ru (accessed 16.10.2014).
3. Trutnev D. R. Information Systems Architecture. Design basics: training manual. SPb.: NIU ITMO. 2012. 66 p. (in Russia).
4. Information Security Strategy of the Russian Federation until 2020, 13 May, 2009. (in Russia)
5. Sovetov B.Ya., Yakovlev S. A. System Modelling. Moscow: Vysshaya shkola. 2007. 343 p. (in Russia).

Information about authors:

Isayeva L.N., Ph.D., docent department of Information security and automation, Moscow Technical University of Communications and Informatics.

Raev K.V., master's degree student, Moscow Technical University of Communications and Informatics.

For citation:

Isayeva L.N., Raev K.V. Requirements for an automated system of creating and maintaining the federal register of documents on education. H&ES Research. 2015. Vol. 7. No. 4. Pp. 36–40. (in Russian).

V МЕЖДУНАРОДНЫЙ КОНГРЕСС ЭРА-ГЛОНАСС

«СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И КОМФОРТА НА ДОРОГАХ»

1 ОКТЯБРЯ 2015

Москва, ЦМТ
(Центр Международной Торговли)

Ключевые темы Конгресса:

- ЭРА-ГЛОНАСС – новый этап развития проекта
- Навигационно-информационные услуги в каждый автомобиль
- Безопасность и эффективность на основе новых технологий – объединяя страны и транспортные потоки
- Нормативное обеспечение функционирования и развития «ЭРА-ГЛОНАСС»
- Роли и задачи государства и бизнеса в развитии и внедрении новых навигационных и информационных технологий на автомобильном транспорте (технологии V2X, беспилотные транспортные средства)
- Навигация повышенной точности и надежности на автомобильном транспорте: новые требования и новые технические возможности
- Новые технологии в сфере персональных пассажирских перевозок

В конгрессе примут участие

- Представители федеральных органов исполнительной власти и органов власти субъектов Российской Федерации
- Представители Республики Беларусь, Республики Казахстан, Китайской народной республики, Европейского Союза
- Российские и мировые автопроизводители
- Ведущие разработчики и производители автомобильного оборудования
- Операторы связи и сервис-провайдеры информационно-навигационных и телекоммуникационных услуг
- Российские и зарубежные эксперты

Организатор

Некоммерческое партнерство "ГЛОНАСС"
Федеральный сетевой оператор

+7 (495) 641 57 17

office@proconf.ru | www.congress-era-glonass.ru

ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ: УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ 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 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

Основой создания подсистем комплексной безопасности инфокоммуникационных сетей специального назначения (ИКС СН) являются комплексы средств защиты информации. Состав комплексов вытекает из особенностей построения ведомственных или корпоративных ИКС СН и составляющих их подсистем, а также понятия «защищенной» системы – ИКС СН, обеспечивающей устойчивое выполнение целей функционирования в рамках заданного перечня угроз безопасности и действий противника или нарушителя.

С точки зрения управления безопасностью ИКС СН под компьютерной атакой (КА) понимается целенаправленное воздействие на компьютерные системы, комплексы, средства и сети ИКС СН с целью организации доступа (канала утечки информации) к компьютерным ресурсам или их блокирования, модификации, уничтожения. Кроме того, термин «компьютерная атака», подразумевает, что запуск программ для получения неавторизованного доступа к компьютеру осуществляется именно людьми, хотя отдельные их составляющие могут осуществляться в автоматизированном режиме.

Особенностями современных ИКС СН являются их корпоративный характер, невозможность повсеместного применения аппаратуры шифрования, а также использование для их нужд ресурсов из состава Единой сети электросвязи России. Эти особенности определяют специфику проведения компьютерных атак против систем управления ИКС СН и должны учитываться при организации управления безопасностью.

Телекоммуникационные и информационные элементы – сервера, накопители информации, коммутаторы, маршрутизаторы, мультиплексоры и т.д., а также элементы подсистем обеспечения информационной безопасностью могут быть объектами компьютерных атак, как и любые терминальные средства пользователей министерств и ведомств. Фактически любой элемент ИКС СН, имеющий в своем составе вычислительную среду с выполняемым в ней программным обеспечением и с возможностью сетевого доступа к ней потенциально является объектом КА.

Следует отметить, что с точки зрения злоумышленника целенаправленное воздействие на ИКС СН в первую очередь целесообразно осуществлять на наиболее критичные объекты, в качестве которых в первую очередь необходимо определить информационные ресурсы систем управления ИКС СН, в т.ч. входящих в них подсистем управления отдельными элементами ИКС СН и средствами обеспечения информационной безопасности.

Еще несколько лет назад под управлением безопасностью большинство специалистов понимали только управление программными (или аппаратными) решениями по безопасности. Однако с начала XXI века мир безопасности кардинально изменился. Причиной этому стал набравший силу процессный подход к управлению информационной безопасностью в соответствии со стандартами ISO 27001/ISO 17799. Основы этого подхода, примененные к задачам управления безопасностью вообще (сетевой и информационной), позволяют решить концептуальные проблемы управления безопасностью сложных инфокоммуникационных сетей специального назначения [1-3].

Учитывая важность рассматриваемых вопросов, специалистам сегодня крайне важно говорить на одном языке и однозначно трактовать используемые термины. В связи с этим следует подчеркнуть, что защиту информации следует рассматривать как процесс, который не ограничивается и не может ограничиваться конкретными техническими решениями. Соответственно, правильное толкование такого широкого термина как управление безопасностью – это управление процессом обеспечения сетевой и информационной безопасности в инфокоммуникационных системах и сетях специального назначения (ИКС СН) в соответствии со стандартом ISO 27001.

Следовательно, система управления безопасностью ИКС СН – часть АСУ ИКС СН, основанная на анализе рисков и предназначенная для создания, внедрения, выполнения, мониторинга, пересмотра, поддержания и повышения уровня сетевой и информационной безопасности ИКС СН. Она должна затрагивать организационную структуру, политики, планы действий, распределение ответственности, осуществление на практике, процедуры, процессы и ресурсы. В рамках процесса, безусловно, могут применяться (или не применяться) те или иные технические решения, позволяющие реализовывать те или иные управляющие воздействия [4].

Комплекс контроля функционирования сетей в составе ИКС СН и АСУ ИКС СН, их систем защиты предназначен для адаптивной реализации политик безопасности в части автоматизированных средств анализа состояния сетей ИКС СН, сети управления, отражения атак и восстановления прикладных систем. Адаптивное управление должно использовать тенденции развития методов предотвращения и отражения атак, связанные с формированием систем защиты и контроля.

В целом вопросы обеспечения и управления безопасностью регламентированы целом рядом стандартов ISO 7498-2, ISO 10164-7, 10164-8, 10164-9, ISO/IEC 17799:2000 и рекомендациями МСЭ-Т X.800, M.3016.0 – M.3016.4, Y.2701 и др.

Безопасность ИКС СН обеспечиваются рядом встроенных механизмов (рис. 1). Так встроенный механизм «Нотаризация» (удостоверение) гарантирует, что третье лицо для гарантии правильности информации использует не только ее содержание, но также сведения об источнике информации, хронометраже и доставке адресату.

Рис. 1. Встроенные механизмы безопасности

Механизм «Управление маршрутизацией в контексте безопасности» содержит правила, которые позволяют при передаче требований, пакетов (сообщений) избегать определенных подсетей, направлений или трактов передачи информации с целью обеспечения требуемого уровня безопасности.

Механизм «Управления доступом» используется, чтобы предотвратить несанкционированный доступ к ресурсу ИКС СН (если доступ запрещен) или предотвратить использование его несанкционированным способом.

Механизм «Аутентификация обмена» используется тогда, когда идентичность лица или прикладного процесса должна быть проверена раньше, чем предоставлен доступ к определенному ресурсу сети.

Механизм «Целостность данных» используется, чтобы гарантировать, что данные при обмене, взаимодействии или просто чтении не будут разрушены или изменены несанкционированным способом.

Механизм «Цифровая сигнатура» (или уникальный набор байтов) используется для гарантии того, что получатель данных – именно тот, кому адресованы данные, и что блок данных не был изменен или поврежден. Часто для этого применяются криптографические методы защиты информации в протокольном блоке (PDU).

Механизм «Заполнение трафика» использует специальные биты, октеты или другие блоки данных, которые добавляются в конце протокольных блоков (PDU).

Механизм «Шифрование» используется для закрытия данных или другой информации криптографическими методами.

Как эти механизмы, так и архитектура подсистемы управления безопасностью (рис. 2) должны учитываться при организации процессов управления безопас-

ностью ИКС СН [4, 5], которые целесообразно свести к двум компонентам (рис. 3).

Рис. 2. Архитектура подсистемы управления безопасностью ИКС СН

Рис. 3. Компоненты общей задачи управления безопасностью ИКС СН

Первый компонент обеспечивает управления средствами как специфическим оборудованием с оценкой его состояния и заданием целесообразных режимов работы с гарантированием заданных установок по параметрам безопасности (рис. 4).

Второй компонент осуществляет контроль выполнения правил безопасности, выработку управления в соответствии с отклонением правил от заданных и включает определенные процессы (рис. 5).

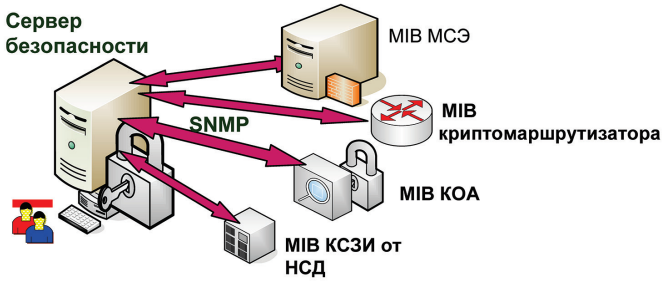


Рис. 4. Управление средствами обеспечения безопасности ИКС СН

Таким образом, целесообразно все средства управления безопасностью ИКС СН свести в группы (рис. 5), и привязать разработку моделей управления (для тех задач, которые удается формализовать и которые возможно автоматизировать) к этим группам.

Так, задачи проведения аудита, управления политиками безопасности для ИКС СН достаточно трудно поддаются формализации и автоматизации, поэтому их решение, как правило, осуществляется с привлечением ДЛ по безопасности ПУ АСУ ИКС СН, в то время как задачи управления рисками безопасности, управления инцидентами и процессами обнаружения атак целесообразно формализовать и в максимальной степени автоматизировать в рамках подсистем управления рисками и инцидентами [4, 5].

В качестве методической основы создания такой системы целесообразно выбрать теорию управления информационными рисками. Основные положения этой теории позволяют взаимоувязано рассматривать зависимость ресурсов системы от угроз, уязвимостей и уровня приемлемости риска реализации угроз в системе. При этом под угрозой понимается совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба ИКС СН или ее системе управления.

Под риском понимается вероятность причинения вреда информационным и телекоммуникационным ресурсам ИКС СН, системе управления ИКС СН. Другими словами риск – вероятный ущерб, который понесет ИКС СН при реализации угроз безопасности, зависящий от защищенности сетей ИКС СН.

Под уязвимостью понимаются недостатки подсистемы управления ИКС СН или её элементов, которые дают возможность преднамеренно или непреднамеренно оказать на неё негативное воздействие (логика взаимосвязи названных элементов приведена на рис. 6).

Уместность предлагаемого подхода для управления безопасностью ИКС СН, иллюстрируется следующим. Любые приемы и методы, реализуемые в системах безопасности ИКС СН, требуют сбалансированной политики безопасности, так как неоправданное ужесточение требований к безопасности, может привести не к повышению защищенности, а к ослаблению системы защиты. Это напрямую связано с категорией «риск».

К наиболее распространенным и универсальным сценариям нарушения безопасности, использующим сами средства защиты, можно отнести следующие:

– на уровне предотвращения угрозы атак действия приводят к событию, которое является более уязвимым (нештатным) по сравнению с плановой работой ИКС СН. Например, перезагрузки приложения, переинициализация подсистемы безопасности для запуска паразитной программы или использование штатного механизма смены паролей для атак на подсистему аутентификации, и т.п. Или же действие приводит к «Отказу в обслуживании», например,

Рис. 5. Управление процессами обеспечения безопасности ИКС СН

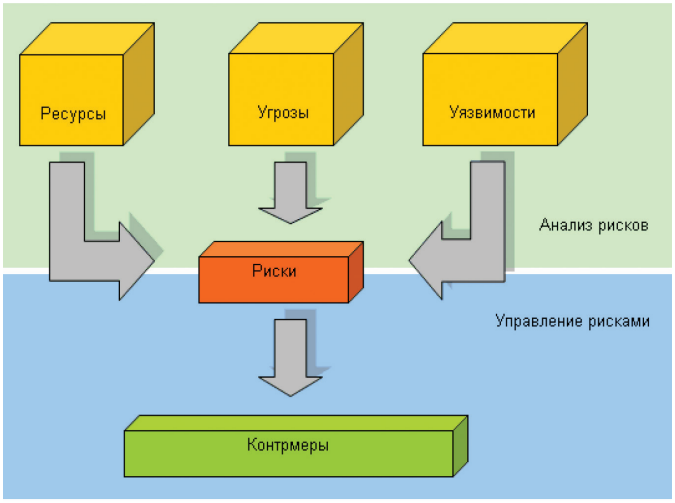


Рис. 6. Взаимосвязь понятий управления рисками безопасности в ИКС СН

использование шифрования трафика для атак отказа в обслуживании;

– на уровне затруднения реализации угрозы, действие приводит к установке таких атрибутов безопасности, которые являются неприемлемыми для пользователей ИКС СН, что приводит к отключению или фактическому сведению на нет системы защиты (например: неправильная политика разграничения доступа и выработки паролей – установка минимальной длины пароля для атак на криптографическую подсистему);

– на уровне обнаружения угроз система безопасности имеет такие расплывчатые признаки угрозы, что ее постоянное срабатывание приводит к ее полному отключению;

– на уровне противодействия атакам система безопасности реализована так, что, при угрозе потери информации из-за исчерпания ресурса, она останавливает функционирование сетей ИКС СН и оказывается уязвимой к DoS-атакам, или же при активном противодействии предусмотрено блокирование или даже уничтожение атакующей системы, без детектирования возможной подмены IP-адреса, что может на время «информационно уничтожить» саму ИКС СН или блокировать ресурсы ее администрирования и не дать возможность противодействовать другим атакам;

– на уровне системы регистрации используются значительные ресурсы, из-за чего происходит отказ (например – переполнение файла регистрации событий, приводящее к DoS-атаке);

– на уровне восстановления после атаки система безопасности восстанавливает «ядро» сетей ИКС СН из некоего резервного источника, что способствует запуску на реально работающей ИКС СН внедренного в ее резервные копии ПО «трояна».

Модель управления рисками включает в себя четыре основных процесса: идентификацию, анализ, планирование и контроль рисков.

Управление рисками – это процессы, связанные с идентификацией, анализом рисков и принятием решений, которые обеспечат максимизацию положительных и минимизацию отрицательных последствий наступления рисковых событий в ИКС СН. Процесс управления рисками должен включать выполнение следующих процедур:

– планирование управления рисками – выбор подходов и планирование деятельности по управлению рисками в ИКС СН и в каждой ее сети;

– идентификация рисков – определение рисков, способных повлиять на ИКС СН и АСУ ИКС СН, и документирование их характеристик;

– качественная оценка рисков – качественный анализ рисков и условий их возникновения с целью определения их влияния на функционирование ИКС СН и АСУ ИКС СН;

– количественная оценка – количественный анализ вероятности возникновения и влияния последствий рисков на ИКС СН и АСУ ИКС СН;

– планирование реагирования на риски – определение процедур и методов по ослаблению отрицательных последствий рисковых событий и использованию возможных преимуществ;

– мониторинг и контроль рисков – мониторинг рисков, определение остающихся рисков, выполнение плана управления рисками в ИКС СН и АСУ ИКС СН, оценка эффективности действий по минимизации рисков.

Деятельность органов управления по реализации управления рисками и составляет подсистему управления рисками.

На основе вышесказанного может быть дано более строгое определение.

Управление рисками – это совокупность процедур и действий, которые позволяют должностным лицам подсистемы управления безопасностью ИКС СН выявлять, оценивать, отслеживать и устранять риски до или во время их превращения в проблемы информационной безопасности.

Цели и задачи управления рисками могут варьироваться в зависимости от звена управления, но должны быть четко определены на этапе построения ИКС СН и АСУ ИКС СН.

При создании подсистемы управления рисками необходимо построить модель анализируемой информационной системы. Модель должна включать: виды ценной информации, объекты ее хранения; группы

пользователей и виды доступа к информации, средства защиты (включая политику безопасности) и виды угроз.

Планирование управления рисками представляет собой процесс принятия решений по применению и планированию управления рисками для конкретного звена управления. Он может включать в себя решения по организации, кадровому обеспечению процедур управления рисками в ИКС СН, выбор предпочтительной методологии, источников данных для идентификации риска, временной интервал для анализа ситуации. Важно спланировать управление рисками, адекватное как уровню и типу риска, так и важности проекта для сетей и служб ИКС СН и её элементов.

Успех деятельности подсистемы управления рисками во многом определяется полнотой выявления потенциальных рисков на начальном этапе. Очень важно при этом иметь детальный план функционирования ИКС СН и АСУ ИКС СН в условиях применения с разбиением задач на подзадачи. Имея полное представление о функционировании ИКС СН и АСУ ИКС СН, эксперты могут провести анализ рисков для всех стадий действий.

При рассмотрении рисков должны быть решены две задачи:

– определение возможных сценариев, соответствующих данному риску;

– определение вероятности для каждого из этих сценариев.

Следует, однако, помнить, что любая числовая мера неопределенности является ограниченной – лишь само распределение дает исчерпывающую характеристику риска для ИКС СН и АСУ ИКС СН. Поэтому при выборе в качестве такой меры той или иной числовой характеристики распределения следует учитывать особенности конкретной задачи управления рисками.

Таким образом, с учетом отмеченных трудностей и в зависимости от особенностей конкретных рисков можно рекомендовать три метода измерения рисков:

– вероятностный метод. Этот метод наиболее предпочтителен при условии, что доступна достаточно надежная информация о всех сценариях и их вероятностях;

– приближенный вероятностный метод. Если по каким-либо причинам невозможно определить искомое распределение вероятностей для множества всех сценариев, то можно попытаться упростить это множество сценариев в расчете на то, что полученная (хотя и грубая) модель окажется практически полезной;

– косвенный (качественный) метод. Если точное или приближенное применение вероятностной модели оказывается практически невозможным, значит «прямое» (количественное) измерение рисков невозможно. В этом случае следует ограничиться измерением каких-либо других показателей, которые косвенно характеризуют рассматриваемый риск и в то же время доступны для практического измерения. Обычно этот метод дает лишь качественную оценку риска, но за неимением лучшего этот подход в ряде случае оказывается единственно возможным.

Для ранжирования рисков по значимости целесообразно ввести понятие ожидаемой величины риска (ОВР), которая вычисляется как произведение вероятности возникновения риска на оценку последствий возможной его реализации.

Оцененные риски группируют по степени их значимости и определяют тот набор рисков, который будет контролироваться в ходе функционирования ИКС СН.

Качественная оценка рисков – это процесс представления качественного анализа идентификации рисков и определения рисков, требующих быстрого реагирования. Такая оценка рисков позволяет определить степень важности риска и выбрать способ реагирования. Доступность сопровождающей информации помогает легче расставить приоритеты для разных категорий рисков. Качественная оценка рисков – это оценка условий возникновения рисков и определение их воздействия на ИКС СН и АСУ ИКС СН стандартными методами и средствами. В течение всего жизненного цикла ИКС СН и АСУ ИКС СН необходимо производить периодическую переоценку рисков.

Количественная оценка рисков определяет вероятность возникновения рисков и влияние последствий рисков на ИКС СН и АСУ ИКС СН, что помогает должностным лицам принимать верные решения и избегать неопределенностей.

Оценка рисков позволяет определить:

– вероятность достижения целей функционирования ИКС СН;

– степень воздействия риска на ИКС СН и АСУ ИКС СН и объемы непредвиденных затрат и материалов, которые могут понадобиться;

– риски, требующие скорейшего реагирования и большего внимания, а также влияние их последствий на функционирование ИКС СН.

Планирование реагирования на риски – это разработка методов и технологий снижения отрицательного воздействия рисков на функционирование ИКС СН. Планирование включает в себя идентификацию и распределение каждого риска по категориям. Стратегия планирования реагирования должна соответствовать типам рисков, наличию ресурсов и временным параметрам.

Контроль процесса подразумевает постоянное наблюдение за факторами возникновения рисков и уведомление ответственных должностных лиц об их появлении, а также отслеживание соответствия последовательности действий как ранее запланированной реакции на риск.

Изменения в ходе функционирования ИКС СН и системы защиты информации могут повлечь за собой появление новых рисков и устранение старых, поэтому контроль предполагает также отслеживание возможных изменений. Выходные данные этого процесса поступают на вход процесса идентификации рисков. Например, планируется свернуть один из узлов доступа к транспортной сети ИКС СН, что приводит к утрате актуальности рисков, связанных с ним.

Мониторинг и контроль позволяют следить за идентификацией рисков, определять остаточные риски, обеспечивать выполнение плана рисков и оценивать его эффективность с учетом понижения риска. Значения показателей рисков, связанные с выполнением условий плана, фиксируются. Мониторинг и контроль позволяют сопровождать процесс функционирования ИКС СН на всех стадиях.

Качественный контроль базовых процессов в ИКС СН поставляет информацию, помогающую принимать эффективные решения для предотвращения возникновений рисков. Для обладания полной информацией необходимо взаимодействие между всеми органами управления, обслуживающими эти процессы.

Цель мониторинга и контроля – выяснить, что:

– система реагирования на риски внедрена в соответствии с планом;

– реагирование достаточно эффективно или необходимы изменения;

– риски изменились по сравнению с предыдущим значением;

– усилилось влияние рисков;

– приняты необходимые меры;

– воздействие рисков оказалось запланированным или явилось случайным результатом.

Контроль может повлечь за собой выбор альтернативных стратегий, принятие корректив, в функционировании АСУ ИКС СН, системы безопасности и комплекса контроля за их функционированием с целью достижения базового плана обеспечения качества функционирования ИКС СН, ее подсистем и сетей. Между названными подсистемами, их должностными лицами должно быть постоянное взаимодействие, все изменения и явления должны фиксироваться. Необходимо регулярное составление отчетов по состоянию качества контролируемых процессов – должна быть разработана соответствующая документированная процедура.

В настоящее время управление рисками относится к наиболее актуальным и динамично развивающимся направлениям в области защиты информации. Его основная задача – объективно идентифицировать и оценить наиболее значимые для качества функционирования ИКС СН информационные риски, в т.ч. для АСУ ИКС СН и самой подсистемы защиты информации, а также адекватность используемых средств контроля рисков для увеличения эффективности решения стоящих задач.

Поэтому под термином «управление рисками» целесообразно понимать системный процесс идентификации, контроля и уменьшения информационных рисков в ИКС СН в соответствии с определенными ограничениями действующей нормативно-правовой базы в области защиты информации и собственной политики безопасности.

Учитывая сложность контроля и обеспечения безопасности в такой сложной многоуровневой системе, какой является ИКС СН, могут быть предложены следующие выражения для оценки рисков, учитывающие все компоненты и уровни ИКС СН:

$$\mathrm{Risk}_{IL} = \frac{1}{N_{IL}} \sum_{i}^{N_{IL}} \sum_{j}^{D_{IL}} \frac{z_{ILj} C^{i}_{urk} P^{i}_{ILugrk}}{V^{i}_{IL_{sk}}} \tag{1}$$

$$\mathrm{Risk}_{MWL} = \frac{1}{N_{MWL}} \sum_{i}^{N_{MWL}} \sum_{j}^{D_{MWL}} \frac{z_{MWLj} C^{i}_{urk} P^{i}_{MWLugrk}}{V^{i}_{MWL_{sk}}} \tag{2}$$

$$\mathrm{Risk}_{BL} = \frac{1}{N_{BL}} \sum_{i}^{N_{BL}} \sum_{j}^{D_{BL}} \frac{z_{BLj} C^{i}_{urk} P^{i}_{BLugrk}}{V^{i}_{BL_{sk}}}. \tag{3}$$

Полученные оценки рисков для каждой уровневой сети ИКС СН сравниваются с заданной допустимой границей:

$$\begin{aligned} &\mathrm{Risk}_{IL} \le \omega_{IL} R_{\text{кр}} \\ &\mathrm{Risk}_{MWL} \le \omega_{MWL} R_{\text{кр}} \\ &\mathrm{Risk}_{BL} \le \omega_{BL} R_{\text{кр}} \\ &R_{\text{кр}} = \mathrm{sup}\mathrm{Risk}_{IKNSN} \end{aligned} \tag{4}$$

По результатам сравнения делаются соответствующие выводы, и решается задача по изменению правил безопасности в ИКС СН.

Международный стандарт ISO 27001:2005 обращает особое внимание на необходимость создания процедуры управления инцидентами информационной безопасности – очевидно, что без своевременной реакции на инциденты безопасности и устранения их последствий невозможно эффективное функционирование подсистемы управления безопасностью ИКС СН.

Управление инцидентами – одна из важнейших процедур управления безопасностью ИКС СН. Прежде всего, важно правильно и своевременно устранить последствия инцидента, а также иметь возможность проконтролировать, какие действия были выполнены для этого. Необходимо также расследовать инцидент, что включает определение причин его возникновения, виновных лиц и конкретных дисциплинарных взысканий. Далее, как правило, следует выполнить оценку необходимости действий по устранению причин инцидента, если нужно – реализовать их, а также выполнить действия по предупреждению повторного возникновения инцидента. Кроме этого, важно сохранять все данные об инцидентах безопасности, так как статистика инцидентов безопасности помогает осознавать их количество и характер, а также изменение во времени. С помощью информации о статистике инцидентов можно определить наиболее актуальные угрозы для ИКС СН, АСУ ИКС СН и, соответственно, максимально точно планировать мероприятия по повышению уровня их защищенности.

Как правило, процедура управления инцидентами разрабатывается в рамках общей системы управления безопасностью ИКС СН. На данном этапе важно, что-

бы все должностные лица органов управления ИКС СН понимали, что обеспечение безопасности в целом и управление инцидентами в частности являются важнейшими целями функционирования АСУ ИКС СН.

Необходимые нормативные документы по управлению инцидентами должны описывать:

– определение инцидента безопасности, перечень событий, являющихся инцидентами;

– порядок оповещения должностных лиц о возникновении инцидента (необходимо определить формат отчета, а также отразить контактную информацию лиц, которых следует оповещать об инциденте);

– порядок устранения последствий и причин возникшего инцидента;

– порядок расследования инцидента (определение причин инцидента, виновных в возникновении инцидента, порядок сбора и сохранения улик);

– порядок определения дисциплинарных взысканий;

– порядок реализации необходимых корректирующих и превентивных мер.

Определение перечня событий, являющихся инцидентами, – важный этап разработки процедуры управления инцидентами. Следует отметить, что все события, которые не войдут в указанный перечень, будут рассматриваться как штатные (даже если они несут угрозу безопасности ИКС СН). В частности, инцидентами безопасности могут быть:

– отказ в обслуживании сервисов, средств обработки информации, оборудования ИКС СН;

– нарушение конфиденциальности и целостности ценной информации;

– несоблюдение требований к информационной безопасности, принятых в системе управления (нарушение правил обработки информации);

– незаконный мониторинг информационной системы специального назначения;

– использование вредоносных программ;

– компрометация информационной системы (например, разглашение пароля пользователя).

В качестве примеров инцидентов можно привести такие события, как неавторизованное изменение данных в распределенной базе данных, оставление терминала незаблокированным без присмотра, пересылка конфиденциальной информации с помощью открытой почты.

В общем случае инцидент безопасности определяется как единичное, нежелательное или неожиданное событие безопасности (или совокупность таких событий), которое может угрожать безопасности ИКС СН или АСУ ИКС СН (ISO/IEC TR 18044:2004).

Важно отметить, что процедура управления инцидентами тесно связана со всеми другими процедурами управления безопасностью. Поскольку инцидентом, в первую очередь, является неразрешенное событие, оно должно быть кем-то запрещено, следовательно, необходимо наличие документов, четко описывающих все действия, которые можно выполнять в ИКС СН и которые выполнять запрещено.

Важно, чтобы были предусмотрены такие процедуры, как мониторинг событий, своевременное удаление неиспользуемых учетных записей, контроль и мониторинг действий пользователей, контроль над действиями системных администраторов и пр.

Для описания процедуры управления инцидентами безопасности используется классическая модель непрерывного улучшения процессов, получившая название от цикла Шухарта-Деминга – модель PDCA (Планируй, Plan – Выполняй, Do – Проверяй, Check – Действуй, Act). Стандарт ISO 27001 описывает модель PDCA как основу функционирования всех процессов системы управления информационной безопасностью. Естественно, что и процедуры управления инцидентами в ИКС СН должны подчиняться модели PDCA.

Обнаружение и регистрация инцидента может быть осуществлено пользователем или должностным лицом АСУ ИКС СН. Как правило, должностные лица знают, что следует делать в случае обнаружения инцидентов, чего не всегда можно сказать о пользователях. Для пользователей должна быть разработана специальная инструкция, в которой необходимо описать, в каком виде пользователь должен сообщить о возникновении инцидента, координаты ответственных лиц, а также перечень действий, которые могут выполняться самостоятельно. Отчет должен содержать подробное описание инцидента, перечисление должностных лиц и пользователей, вовлеченных в инцидент, фамилию лица, зафиксировавшего инцидент и дату возникновения и регистрации инцидента.

Требуется разработать инструкцию для специалиста по защите информации, в обязанности которого входит регистрация инцидента. Такая инструкция может содержать, например, правила и срок регистрации инцидента, перечень необходимых первоначальных инструкций для лица, обнаружившего инцидент, и, кроме того, описание порядка передачи информации об инциденте соответствующему должностному лицу, порядок контроля за устранением последствий и причин инцидента.

Инструкция по устранению причин и последствий инцидента должна включать описание общих действий, которые необходимо предпринять (конкретные действия для каждого вида инцидента определять трудоемко и не всегда целесообразно), а также сроки, в течение которых следует устранить последствия и причины инцидента. Сроки устранения последствий и причин инцидента зависят от уровня инцидента. Следует разработать классификацию инцидентов – определить количество уровней критичности инцидентов, описать инциденты каждого уровня и сроки их устранения. В документе должно быть определено, какие события следует считать инцидентами и описать уровни инцидентов.

Таким образом, инструкция по устранению последствий и причин инцидента может включать: описание действий, предпринимаемых для устранения послед-

ствий и причин инцидента, сроки устранения и указание на ответственность за несоблюдение инструкции.

Расследование инцидента безопасности в ИКС СН включает в себя определение виновных в его возникновении, сбор доказательств и улик инцидента, определение соответствующих дисциплинарных взысканий. Инструкция по расследованию инцидентов должна описывать: действия по расследованию инцидента (в том числе определение виновных в его возникновении), правила сбора и хранения улик и правила внесения дисциплинарных взысканий.

После устранения последствий инцидента и восстановления нормального функционирования ИКС СН и АСУ ИКС СН, возможно, потребуется выполнить действия по предотвращению повторного возникновения инцидента. Для определения необходимости реализации таких действий следует провести анализ рисков, в рамках которого определяется целесообразность корректирующих и превентивных действий.

Для того чтобы процедура управления рисками выполнялась правильно и эффективно, все эти этапы должны непрерывно и последовательно повторяться. Через определенное время необходимо заново пересмотреть перечень событий, определенных в качестве инцидентов, форму отчета и пр., внедрить обновленную процедуру в информационную систему, проверить ее функционирование, эффективность и реализовать превентивные действия. Таким образом, цикл модели PDCA будет непрерывно повторяться, и гарантировать четкое функционирование процедуры управления инцидентами и, главное, ее постоянное улучшение.

Необходимо подчеркнуть, что управление инцидентами не предупреждает нанесение ущерба ИКС СН и АСУ ИКС СН (как правило, ущерб, связанный с инцидентом, уже нанесен), однако расследование инцидента и своевременное внедрение превентивных и корректирующих мер снижает вероятность его повторения (и, следовательно, вероятность повторения нанесения ущерба).

В процессе функционирования ИКС СН любое событие, которое не позволяет сетям в ее составе функционировать с заданными параметрами в течение определенного периода времени, может интерпретироваться как отказ и должно повлечь за собой выполнение комплекса мероприятий по восстановлению. При этом следует подчеркнуть, что в силу специфичности роли, какую играют в ведомственных или корпоративных системах управления ИКС СН, их восстановлению должно быть уделено особое внимание.

Управление восстановлением ИКС СН и сетей в ее составе после программно-аппаратных воздействий является составной частью процесса восстановления нормального функционирования ведомственных или корпоративных систем управления в целом.

Конкретное содержание процессов восстановления, в основном, будет зависеть от характера воздействий и объектов ИКС СН, против которых эти воздействия были направлены, т. е. определяется возможными угрозами информационной и системной безопасности ИКС СН. Поэтому, оценив соответствующие риски безопасности, может быть проведена предварительная работа по возможным процедурам восстановления функционирования ИКС СН и выработке тех управляющих воздействий, которые должны реализовать эти процедуры в требуемой последовательности за заданное время.

Анализ характера возможных программно-аппаратных воздействий и объектов ИКС СН, против которых эти воздействия могут быть направлены, позволяют предположить, что с точки зрения восстановления подсистем и сетей ведомственных или корпоративных ИКС СН основную роль играют процессы восстановления программного обеспечения (ПО) и используемых данных.

Для этого в подсистеме управления безопасности должны быть предусмотрены должностные лица, организующие реализацию процедур восстановления ПО и данных.

Важнейшим элементом при восстановлении ПО является восстановление операционных систем (ОС). При этом следует учитывать, что в ИКС СН, АСУ ИКС СН, в сетях ИКС СН, в отдельных комплексах (средствах) могут использоваться различные ОС.

Для обеспечения восстановления ОС в них должны быть предусмотрены так называемые «контрольные точки восстановления». В качестве точек восстановления выступают копии важнейших системных файлов (данные реестра, загрузочные и защищенные файлы, данные о настройках и т. д.). Создание точек восстановления должно осуществляться автоматически всякий раз, когда в ИКС СН происходит событие, способное негативно влиять на работу ОС объектов (установка нового ПО или драйверов, выполнение процедуры обновления и т.д.).

Следует подчеркнуть, что пользоваться системой восстановления нужно только в тех случаях, когда нет другого способа восстановить работоспособность ИКС СН. В ходе сбоя при установке нового программного оборудования для восстановления ОС иногда достаточно просто вернуться к предыдущему состоянию системы.

Восстановление работоспособности ОС можно также осуществить при помощи архивных копий основных системных файлов или копий жестких дисков. Восстановление из архива может быть осуществлено как в текущем сеансе работы подсистем ИКС СН, так и до запуска (при их аварийном отказе).

В подсистеме управления безопасностью должна быть предусмотрена процедура переустановки ОС.

Восстановление данных после успешных программно-аппаратных воздействий должно предусматривать комплекс мер по минимизации ущерба и последствий совершенных атак с помощью систем:

– повышения надежности на основе систем частичного резервирования или внесения избыточности на уровне данных;

– полного резервирования на уровне аппаратного обеспечения за счет дублирования наиболее критичных устройств или их компонент, а также на уровне

сервисов или приложений за счет дублирования программ и процессов;

– восстановления за счет создания резервных копий информационных объектов жизненно необходимых для бесперебойной работы приложений ИКС СН, то есть контрольных точек, фиксирующих состояние информационных объектов различных приложений.

Литература

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

2. Mitra D., Ramakrishman K.G. Technics for traffic engeniring of multiservice in priority networks // BLTJ. 2001. Vol. 1. Pp. 123-130.

3. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. СПб.: СПбУ, 1999. 234 с.

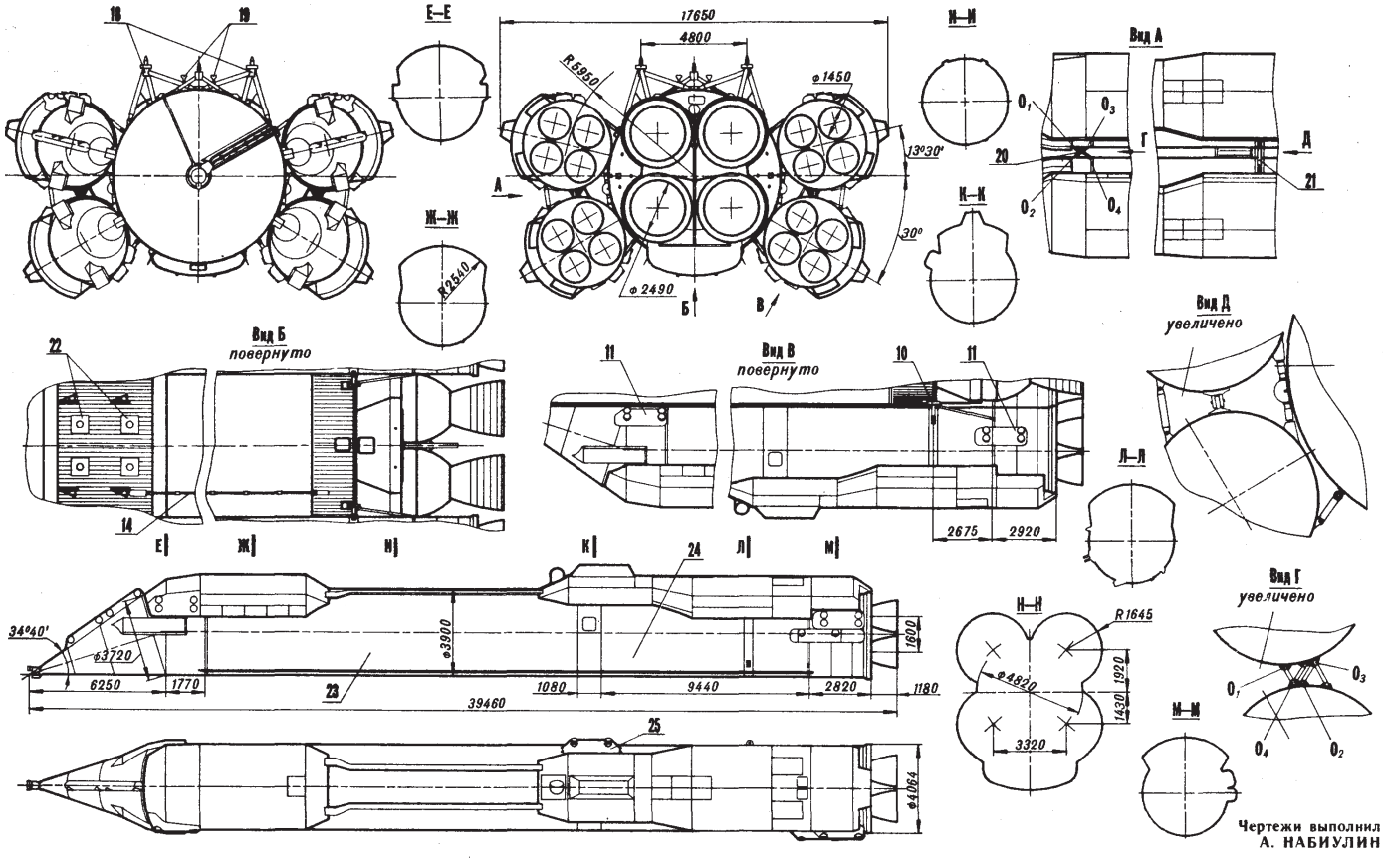
4. Буренин А.Н., Курносов В.И. Теоретические основы управления современными телекоммуникационными сетями. М.: Наука. 2011. 464 с.

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

Для цитирования:

Буренин А.Н., Легков К.Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: управление безопасностью сетей // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 42–51.



SECURITY ISSUES OF INFOCOMMUNICATION SYSTEMS AND SPECIAL PURPOSE NETWORKS: NETWORKS SECURITY MANAGEMENT

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

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

Abstract
The basis for the creation of are subsystems complex security infocommunication networks for special purposes (ICN SP) of means are the complexes information protection. The composition of the complexes follows from the features of construction of departmental or corporate ICN SP components and their subsystems, as well as the concept of "protected" system – ICN SP, ensuring sustainable implementation of objectives within a given list of security threats and actions of the enemy or intruder.
From the point of view security management ICN SP under computer attack (CA) refers to the targeting of computer systems, systems, tools and networks ICN SP for the purpose of access (channel information leakage) to computing resources or their blocking, modification, destruction. In addition, the term «computer attack» implies that the running programs to gain unauthorised access to the computer is done by people, although some of their components can be implemented in an automated mode.
Features modern ICN SP are their corporate nature, the impossibility of a universal application of the encryption equipment, and use for their needs resources from Unified telecommunication network of Russia. These features determine the specifics of carrying out cyber attacks against control systems ICN SP and should be considered when the organization's safety management.
Telecommunications and information elements – servers, storage devices, switches, routers, multiplexers, etc., as well as elements of subsystems ensure information security can be targets of computer attacks, like any terminal users ' funds of ministries and agencies. In fact, any element ICN SP, having in its composition a computing environment to run in it's own software and network access is potentially an object of the CA.
It should be noted that from the point of view of the attacker targeting of ICN SP in the first place should be the most critical objects, which you first need to identify the information resources management systems ICN SP, including constituent subsystems control the individual elements of ICN SP and means of ensuring information security.

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

References
1. The doctrine of information security of the Russian Federation: Approved by the President of the Russian Federation D-1895 from 09 September 2000. (In Russian).
2. Mitra D., Ramakrishman K. G. Technics for traffic engeniring of multiservice in priority networks. BLTJ. 2001. Vol. 1. Pp. 123–130.
3. Zima V.M., Moldovyan A.A., Moldovyan N.A. Bezopasnost' global'nyh setevyh tehnologij [The global security network technologies]. SPb.: SPbU, 1999. 234 p. (In Russian).
4. Burenin A. N., Kurnosov V. I. Teoreticheskie osnovy upravleniya sovremennymi telekommunikacionnymi setyami. [Theoretical bases of management of modern telecommunications networks]. Moscow: Nauka. 2011. 464 p. (In Russian).
5. Burenin A. N., Legkov K. E. Some models security management info-communication networks. H&ES Research. 2013. Vol. 5. No. 4. Pp. 46–50. (In Russian).
6.Burenin A.N., Legkov K.E. Sovremennye infokommunikatsionnye sistemy i seti spetsial'nogo naznacheniya. Osnovy postroeniya i upravleniya [Modern infocommunication systems and special purpose networks. Basics of creation and control]. Moscow: Media Publisher. 2015. 348 p. (In Russian).

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 automated systems of control, Military Space Academy.

For citation:
Burenin A.N., Legkov K.E. Security issues of infocommunication systems and special purpose networks: networks security management. H&ES Research. 2015. Vol. 7. No. 4. Pp. 42–51. (in Russian).

МЕТОДИКА ПОСТРОЕНИЯ ПОИСКОВОЙ СИСТЕМЫ ДЛЯ ПРИМИТИВНОЙ ПРОГРАММЫ АДАПТИВНОГО ДЕЙСТВИЯ

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

Ключевые слова:
поисковая система, база данных, SQL, прямой поиск, инвертированные файлы.

АННОТАЦИЯ

Интересная проблематика с которой сталкивается современное информационное общество – это устойчивые алгоритмы с автономными программами. Вокруг таких программ строятся смелые предположения и фантастические теории. В исследовании будут разобраны способы и методы по части использования поисковых систем для автоматизированных программ.

Существует распространенное убеждение, что каждое новое поколение программ совершеннее предыдущего: раньше все было несовершенно, зато теперь повсюду царит чуть ли не искусственный интеллект. Иная точка зрения состоит в том, что «все новое – это хорошо забытое старое». Скорее всего, применительно к поисковым системам, истина лежит где-то посередине. Разобрав теоретическое описание, также следует коснуться практического применения изученных методик. Предлагается применить полученные знания в реализации программного модуля «Fithicus». Данный алгоритм разрабатывается на кафедре защищенных систем связи СПбГУТ им. профессора М.А. Бонч-Бруевича. В работе предлагается также прибегнуть к использованию реляционных баз знаний. На основе их применения будут построены специальные схемы результатов работы базы данных до и после применения модуля «Fithicus», который включает в себя особый алгоритм для функционирования поисковой системы. Данный модуль можно использовать с различными системам предотвращения утечек информации (DLP-системы). Можно утверждать, что на сегодняшний день это один из наиболее эффективных инструментов для защиты конфиденциальной информации и актуальность подобных решений будет со временем только увеличиваться.

Также следует отметить, что полученные результаты рассматриваются в рамках примитивных адаптивных систем, пример одной из которых рассматривается в исследовании.

Построенный программный модуль успешно внедрен в предложенную проектную подсистему, где планируется выполнение основных функций адаптивной программы. В конце практической реализации выявлены характеристики работы предложенной методологии и практической реализации.

Введение

Как и любая программа, поисковая система оперирует со структурами данных и исполняет алгоритм. Есть четыре класса поисковых алгоритмов. Три алгоритма из четырех требуют «индексирования», предварительной обработки документов, при котором создаются вспомогательный файл, сиречь «индекс», призванный упростить и ускорить сам поиск [2,3] (пример алгоритма инвертированных файлов – рис. 1).

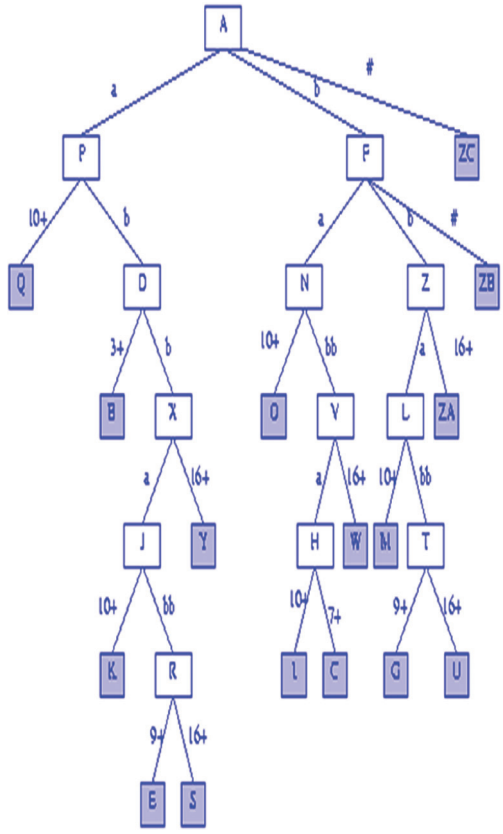


Рис. 1. Алгоритм инвертированных файлов

Основной принцип работы алгоритмов инвертированных файлов такой же, как у алгоритмов сигнатурного поиска антивирусов. Как антивирус сканирует файл в поисках участков данных, совпадающих с известными фрагментами кода вирусов, так и алгоритмы инвертированных файлов, использующиеся в программах для восстановления данных, считывают информацию с поверхности диска в надежде встретить знакомые участки данных. Заголовки многих типов файлов содержат характерные последовательности символов. К примеру, файлы в формате JPEG содержат последовательность символов «JFIF», архивы ZIP начинаются с символов «PK», а документы PDF начинаются с символов «%PDF-» [4].

Некоторые файлы (к примеру, текстовые и HTML файлы) не обладают характерными сигнатурами, но могут быть определены по косвенным признакам, т.к. содержат только символы из таблицы ASCII.

Для восстановления файла мало найти его начало, нужно также определить его конец. Конец файла можно найти, зная размер и адрес начала файла. Размер файла определяется либо анализом заголовка (ZIP, JPEG, AVI и т.п.), либо считыванием и анализом секторов диска, идущих сразу за заголовком. К примеру, концом текстового или HTML файла алгоритм будет считать первый же сектор, который будет содержать символы, не входящие в таблицу ASCII.

В вырожденном случае предварительный этап индексирования отсутствует, а поиск происходит при помощи последовательного просмотра документов. Предлагается воспользоваться так называемым *прямым поиском*.

```
char* strstr (char *big, char *little)
{
        char *x, *y, *z;
        for (x = big; *x; x++)
        {
                for (y = little, z = x; *y;
                        ++y, ++z)
                {
                        if (*y != *z)
                                break;
                }
                if (! *y)
                        return 0;
}
```

Листинг 1. Программная реализация прямого поиска

Здесь показан показан пример выполнения некоторой функции **big**, где сначала просматривают слева направо и для каждой позиции x запускают последовательное сравнение с искомой подстрокой **little**. Для этого, двигая одновременно два указателя **y** и **z**, попарно сравнивают все символы. Если пользователь успешно дошел до конца искомой подстроки, значит она найдена [5].

Методология

Методы, используемые для построения поисковых систем не могут обходится без гибких систем баз данных и баз знаний (рис. 2). Для поиска и запроса, данные приводятся в таблицах, которые связаны друг с другом. Это означает, что, как и в веб-поисках, были записаны, в качестве первичного набора информации, ссылки на страницы, которые можно сортировать по тому, как они связывают друг с другом. Для этого примера предлагается использовать извлечение известного IMDB. Использование файлов общих данных и IMDbPY, делает возможной связь с базой данных на объем 5GB+.

Благодаря реляционной базе данных легко создать полнотекстовых поиск таблицы с использованием расширений FTS4. Можно воспользоваться информацией реляционной базы данных, чтобы создать схему всех результатов и связывая их вместе (рис. 3).

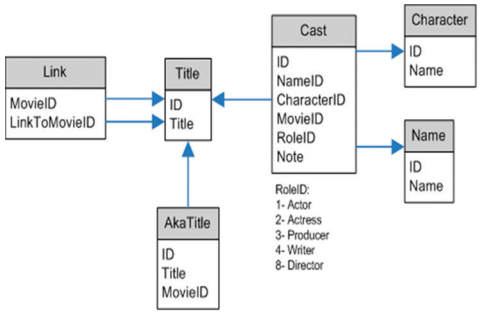


Рис. 2. Сортировка типов данных в реляционной базе данных

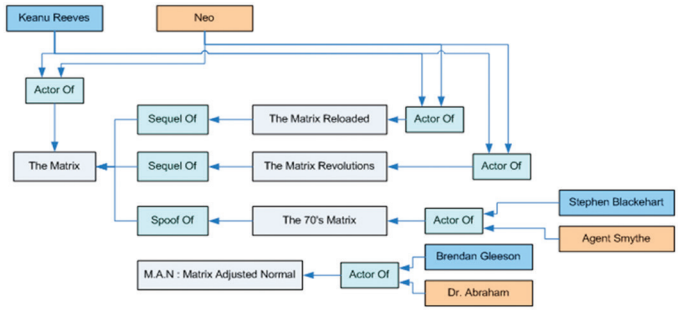


Рис. 3. Схема результатов работы реляционной базы данных поисковой системы

Из этого графика, есть возможность вычислить оценку релевантности на основе различных ссылок.

Самый походящий алгоритм для программ адаптивного действия – это алгоритм «Fithicus», который подходит для примитивных программ адаптивного действия. Принцип работы алгоритма может успешно реализовывать себя по части программ перехвата информации, например DLP-системы (рис. 4). Рекомендуется использовать систему DLP, потому что данная система предотвращает передачу и получение конфиденциальной или другой нежелательной информации. На первой стадии перехвата осуществляется при помощи следующих типов поисковиков:

– фразовый поиск;
– поиск по словарю;
– поиск похожих по содержанию документов;
– поиск по атрибутам документов;
– поиск нераспознанных документов;
– поиск по регулярным выражениям;
– поиск по цифровым отпечаткам;
– сложные запросы.

Также DLP-система оптимизирует загрузку каналов и экономит трафик, а также в комплекте системы есть контроль присутствия работников на рабочем месте [6].

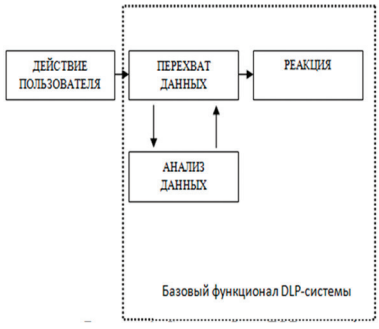


Рис. 4. Схема работы DLP-системы

По большей части модуль «Fithicus» включает в себя приведенную выше методологию и работу предложенной базы данных (рис. 5). Специальных одноименный модуль «Fithicus» был разработан, чтобы демонстрировать преимущества динамической схемы реляционной базы данных. Однако, на первичном этапе тестирования «Fithicus» предназначен, чтобы забить статический набор (Наиболее часто используемые статистические функции встроены в основное ядро программы, то есть эти функции доступны с момента запуска программы. Другие более специализированные функции входят в дополнительную подпрограмму, называемую пакетом анализа). Для каждого узла, он вычисляет две оценки: «Власть» определяет сколько узлов были связаны , и «концентратор» определяет сколько узлов ссылок связаны с другими данными.

Поисковой алгоритм «Fithicus» выполняет текст запроса в 4 последовательных шагов (рис. 6):

1. Текст запроса передается в полнотекстовый поиск в базе данных. (Здесь все сделано с помощью FTS extension of SQLite).

2. Список записей преобразуется в схеме и программа соединяет их вместе.

3. Если максимальное количество узла схемы не достигнуто, создается второе поколение данных.

4. Значения ХИТЫ (Fithicus) вычисляются для каждого узла схемы и лучший результат будет в последствии извлечен.

Для повышения производительности, исходная база данных восстанавливается в отдельную SQLite базу данных, которая позволяет программе легко определить полный текст результатов и связывает узел вместе.

В «main_xxx» – глобальные таблицы, используемые в программе, имеют следующие пункты:

1. «Main_domain» и «Main_DomainMetadata» описывают содержания и отношения различных областей (сбор поиска данных).

2. Main_Master содержит всю уникальную ItemID во всех областях. Эта таблица позволяет находить домен, который связан с данной ItemID. Это также хорошее место, чтобы добавить статические оценки.

3. Main_FullText содержит все для поиска строк во всех областях. С SQLite каждая запись может быть связана только с одним значением называется «DocID». По этой причине, мы дописываем дополнительную таблицу, чтобы связать запись обратно в своей области.

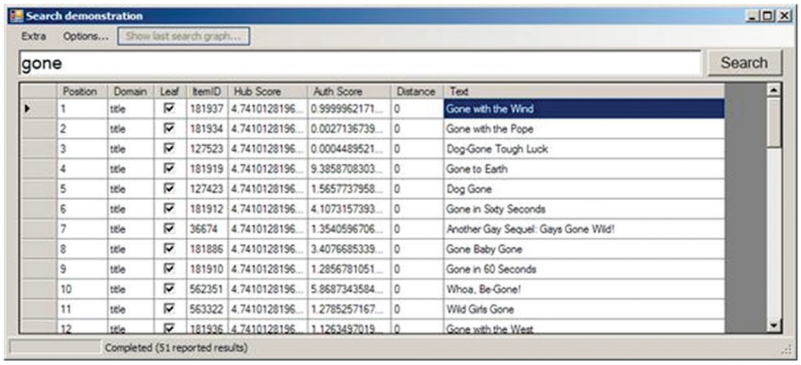


Рис. 5. Работа поискового модуля «Fithicus»

Каждый домен содержится в своей таблице. Очевидно, что для поиска текст хранится в качестве идентификатора. В зависимости от метаданных, внешние идентификаторы (ссылка MovieID и NameID) являются ItemIDs.

Эта структура позволяет реализовать большую часть добычи базы данных непосредственно в SQL. Используя таблицу метаданных, программа может создавать два выборочных запроса, чтобы получить все связи пунктов, а также, чтобы получить все входящие ссылки.

Реализация

Внедрение модуля «Fithicus» было произведено по определенной схеме (рис. 7). Стрелками указано, в каком направлении и между какими компонентами передаются данные.

Опишем по шагам цикл обработки одного поискового запроса.

1. Веб-страница формирует get-запрос, содержащий текст запроса, заданного пользователем системы.

2. Контроллер (Controller) модуля «Fithicus» разбивает запрос на термины, формирует поисковую команду – объект, содержащий список терминов и параметры необходимого поиска.

3. ExtendedSearcher получает от системы полнотекстового поиска Apache Lucene ранжированный список сообщений, удовлетворяющих запросу.

4. ExtendedSearcher получает от Хранилища (Storage) данные о каждом сообщении из списка, фигурирующего на предыдущем шаге.

5. ExtendedSearcher изменяет порядок ранжирования сообщений в соответствии с одним из алгоритмов комбинирования различных признаков ранжирования.

6. ExtendedSearcher возвращает список результатов Контроллеру.

7. Контроллер помещает результаты на страницу и возвращает браузеру пользователя HTML-код.

Необходимо установить критерии адаптивности для нашей программы. Адаптивность позволяет при ограниченных затратах на организацию систем защиты информации обеспечить заданный уровень безопасности информационной системы за счет оперативной реакции на изменение множества угроз. С другой стороны, не менее важным качеством является возможность фиксации в системе защиты информации накопленного опыта в виде информационных полей.

В соответствии с заданием на проектирование систем защиты информации выбирается структурная модель систем информационной безопасности в виде иерархии уровней механизмов защиты, а опыт экспертов информационной безопасности (операторов) представляется матрицами экспертных оценок (базы

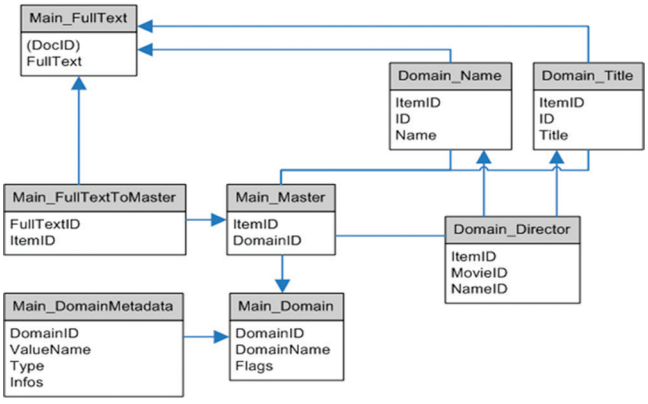


Рис. 6. Модернизированная схема результатов работы реляционной базы с применением алгоритма «Fithicus»

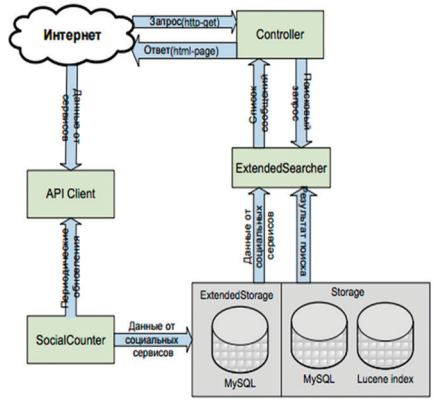


Рис. 7. Схема работы адаптивной подсистемы с применением модуля «Fithicus»

данных) и системами правил логического вывода (базы знаний) для классификации:
1. Угроз по признакам атак;
2. Механизмов защиты на множестве известных угроз.

Важными характеристиками работы программы с модулем «Fithicus» являются:
1. Время обработки отдельного запроса.
2. Количество одновременно обрабатываемых запросов в секунду.
3. Потребление ресурсов сервера (в основном, оперативной памяти).

Эти характеристики были измерены с помощью инструментов Jakarta JMeter и profiler4j, представляющих функции измерения производительности и профилирования программы соответственно.

Профилирование приложений позволяет обнаруживать узкие места приложений и определить время выполнения конкретных функций. В данном случае профилирование позволит узнать, сколько времени тратится непосредственно на функциональную часть работы системы (исключая время на передачу запросов и рендеринг), а также на те функции, которых не было в исходной системе.

Тестирование производилось на машине со следующими характеристиками: CPU Intel Core i7, ОЗУ 8 Гб DDR3, HDD 1000гб. Результаты тестирования представлены в табл. 1.

Таблица 1

Производительность работы системы

Среднее время обработки одного запроса	0,19 сек
Среднее время обработки одного запроса (исходная система)	0,12 сек
Среднее количество запросов в секунду	10,5
Среднее количество запросов в секунду (исходная системы)	16,6
Потребление оперативной памяти	1,2 Гб
Потребление оперативной памяти (исходная система)	1,3 Гб

Отметим, что ухудшение производительности системы естественным образом связано с ее усложнением и выполнением дополнительных операций. В процессе разработки акцент делался больше на гибкость модели данных и реализации, чем на минимизацию количества дополнительных действий. Поэтому для получения значений счетчиков социальных сервисов требуются дополнительные обращения к базе и объектно-реляционное преобразование полученных данных, что занимает дополнительное время.

Заключение

Наиболее эффективными признаками для увеличения качества поиска среди рассмотренных систем являются признаки, основывающиеся на анализе ссылочной структуры веб-интерфейсов. Но в коллекциях, не обладающих данной структурой, можно получить улучшение качества поиска с использованием других признаков, подсчитываемых для целого документа или некоторых его атрибутов.

Модуль поиска «Fithicus» позволяет системам адаптивного действия легче и быстрее подхватывать новую информацию и типы данных. Однако такой модуль требует соответствующих затрат, которые компенсируются гибкостью и надежностью автоматизированного поиска.

Литература

1. Bharat K., Broder A., Henzinger M., Kumara P. and Venkatasubramanian S. The Connectivity Server: Fast Access to Linkage Information on the Web. WWW7. 1998.

2. Brin S., Page L. The Anatomy of a Large-Scale Hypertextual Web Search Engine. WWW7. 1998.

3. Broder A., Glassman S., Manasse M. Syntactic Clustering of the Web. WWW6. 1997.

4. Алгоритм восстановления данных по файловым «сигнатурам» [Электронный ресурс]. http://hetmanrecovery.com/ru/recovery_news/recovering-information-with-signature-search.htm (дата обращения 20.07.2015).

5. Стратегия поиска в автоматизированных информационных системах [Электронный ресурс]. http://www.referat.wwww4.com/view-text-17428 (дата обращения 20.07.2015).

6. Левцов В.И. Контроль подмены символов в системах борьбы с утечками конфиденциальных данных // Информационная безопасность. 2009. № 5. С. 28–29.

Для цитирования:

Штеренберг С.И. Методика построения поисковой системы для примитивной программы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 52–57.

METHODOLOGY CONSTRUCTION OF SEARCH SYSTEM FOR PRIMITIVE PROGRAM OF ADAPTIVE ACTION

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

Abstract
Interesting issues facing the modern information society – a stable algorithms with autonomous programs. Such programs are built around bold assumptions and fantastic theories. This article will be discussed ways and methods of use of the search engines for automated programs.
There is a widespread belief that every new generation of programs of the previous perfect. They say that before everything was perfect, but now reigns throughout almost artificial intellect. Another view is that «everything is new is well forgotten old». May be that with regard to search engines truth lies somewhere in between.
Having examined the theoretical description, we should also touch on the practical application of the studied methods. It is proposed to apply the knowledge gained in the implementation of the program module «Fithicus». The algorithm developed at the Department of protected systems of communications SUT them. prof. M.A. Bonch-Bruevich.
The paper also proposed to resort to the use of relational database knowledge. On the basis of their applications will be built special schemes the results of the database before and after the application module «Fithicus», which includes a special algorithm for operation of a search engine.
This module can be used with various systems, data leak prevention (DLP system). It can be argued that today it is one of the most effective tools to protect confidential information, and the relevance of such solutions will only increase.
It should also be noted that the results obtained are discussed in the framework of the primitive adaptive systems, one example of which is considered in this article.
Built software module successfully implemented in the proposed design subsystem, which is planned to perform the basic functions of the Adaptive Program. After practical realization will identify performance characteristics of the proposed methodology and implementation.

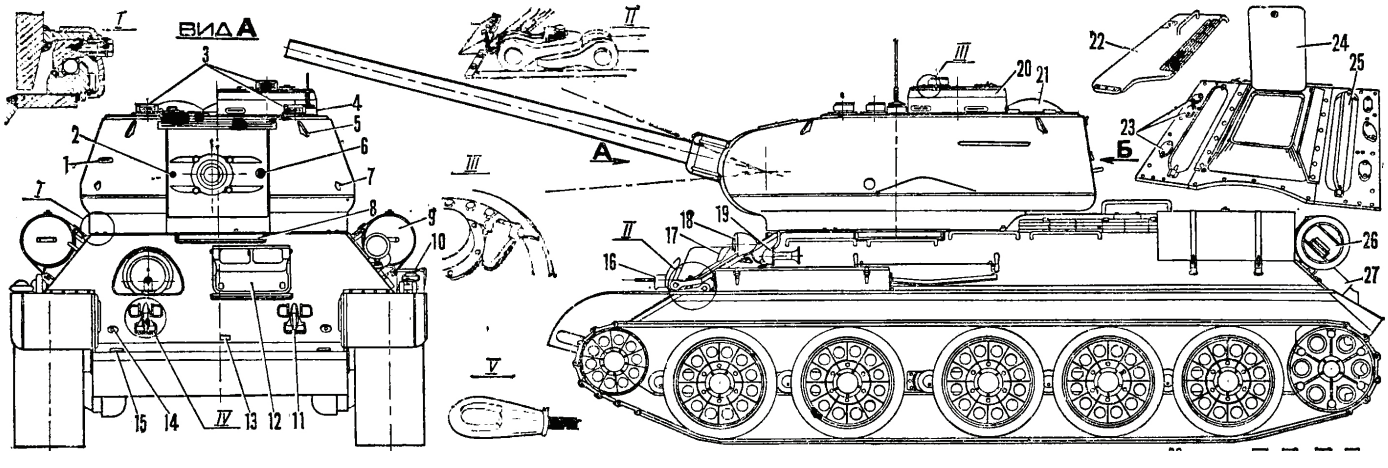
Keywords: search engine, database, SQL, direct search, inverted file.

References

1. Bharat K., Broder A., Henzinger M., Kumara P. and Venkatasubramanian S. The Connectivity Server: Fast Access to Linkage Information on the Web. WWW7. 1998.
2. Brin S., Page L. The Anatomy of a Large-Scale Hypertextual Web Search Engine. WWW7. 1998.
3. Broder A., Glassman S., Manasse M. Syntactic Clustering of the Web, WWW6. 1997.
4. The algorithm of file recovery «signatures» [Electronic resource]. http://hetmanrecovery.com/ru/recovery_news/recovering-information-with-signature-search.htm (date of assess 20.07.2015).
5. Search Strategy in automated information systems [Electronic resource]. http://www.referat.wwww4.com/view-text-17428 (date of assess 20.07.2015).
6. Levtsov V.I. Control of the substitution symbols in the systems against leaks of confidential data. Information Security. 2009. № 5. Pp. 28–29. (In Russian).

Information about authors:
Shterenberg S.I., post-graduate student, Saint-Petersburg State University of Telecommunications.

For citation:
Shterenberg S.I. Methodology construction of search system for primitive program of adaptive action. H&ES Research. 2015. Vol. 7. No. 4. Pp. 52–57. (in Russian).



Ежегодный отчет Cisco по информационной безопасности показывает: разрыв между восприятием информационной безопасности и реальностью растет

Ключевые слова:
Cisco, информационная безопасность, ежегодный отчет Cisco по информационной безопасности, уязвимости, средства защиты.

60% опрошенных компанией Cisco обновляют программное обеспечение (ПО) несвоевременно, и только 10% пользователей браузера IE используют его последнюю версию. Тем не менее 90% респондентов уверены в своей информационной безопасности.

Компания Cisco опубликовала очередной ежегодный отчет по информационной безопасности, подтверждающий тезис о том, что для защиты от киберугроз организациям необходимо задействовать силы всех сотрудников. Злоумышленники все лучше используют уязвимости в средствах защиты от таких угроз, чтобы скрыть свою вредоносную деятельность. Соответственно, службы информационной безопасности (ИБ) должны постоянно улучшать методы своей работы. Это тем более важно, если учесть геополитическую ангажированность злоумышленников и противоречивые требования, зачастую накладываемые местным законодательством по защите цифровой информации, местонахождению данных и шифрованию.

«Чтобы обеспечить информационную безопасность, необходимо задействовать всех сотрудников, от совета директоров до рядовых пользователей, – заявил старший вице-президент, главный директор компании Cisco по ИБ Джон Н. Стюарт (John N. Stewart). – Раньше мы опасались DOS-атак, а сейчас беспокоимся еще и о сохранности данных. Раньше мы опасались кражи интеллектуальной собственности, а теперь — полного отказа служб, имеющих критически важное значение. Злоумышленники действуют все искуснее, используя уязвимости нашей защиты и маскируя свою деятельность. Системы информационной безопасности должны обеспечивать защиту в течение всего цикла атаки, поэтому приобретать нужно только те технологии, которые разрабатывались с учетом данного фактора. Отказоустойчивость должна стать важной частью работы веб-сервисов. Чтобы защитить свое будущее, все вышесказанное нужно применять уже сейчас. Это требует беспрецедентных в истории индустрии усилий».

Злоумышленники

Киберпреступники расширяют арсенал методов своей деятельности и совершенствуют их для проведения скрытых атак. Служба информационной безопасности Cisco выявила три наиболее актуальные тенденции:

• «Спам на снегоступах»: злоумышленники распространяют спам небольшими порциями с большого количества IP-адресов, что позволяет успешно избегать обнаружения. При этом зараженные компьютеры могут быть использованы и для других атак.

• Секретные веб-эксплойты. Широко распространенные наборы эксплойтов быстро нейтрализуются службами безопасности. Чтобы не привлекать внимания, киберпреступники используют менее распространенные эксплойты. Такой механизм работы отслеживать сложнее, что позволяет пользоваться им постоянно.

• Сочетания вредоносных техник. Технологии Flash и JavaScript, например, всегда были небезопасными. Успехи в разработке механизмов защиты и обнаружения заставили злоумышленников разработать средства, которые используют уязвимости Flash и JavaScript одновременно. Распределение эксплойта между двумя файлами – Flash и JavaScript – делает его менее заметным для защитных устройств и затрудняет его анализ через реверс-инжиниринг.

Пользователи

Пользователи оказались между молотом и наковальней: будучи жертвами, они, сами того не зная, помогают вести кибератаки. Исследования, проведенные в 2014 г. службой ИБ Cisco, показали, что теперь злоумышленни-

ки преимущественно атакуют не только серверы и операционные системы, но и данные пользователей через браузеры и электронную почту. Из-за пользователей, загружающих данные с зараженных веб-страниц, количество атак через Silverlight возросло на 228%, а количество спама и рекламных вирусов – на 250%.

Защитники

В исследовании под названием Cisco Security Capabilities Benchmark участвовали руководители служб информационной безопасности 1700 организаций из США, Бразилии, Великобритании, Германии, Италии, Индии, Китая, Австралии и Японии. Вывод неутешителен: руководители стали чаще переоценивать свои возможности по обеспечению ИБ. Например, более 75% респондентов считают, что их системы информационной безопасности очень, а то и чрезвычайно надежны. При этом менее 50% опрошенных уделяют внимание таким стандартным средствам устранения уязвимостей, как регулярное обновление и безопасная настройка ПО. К примеру, Heartbleed стала крупнейшей уязвимостью прошлого года, и тем не менее 56% используемых версий OpenSSL старше 4 лет. Очевидно, что службы ИБ не занимаются обновлением ПО.

Таким образом, вопросам информационной безопасности нужно уделять больше внимания, даже если те, кто за нее отвечает, убеждены, что все в порядке.

«Злоумышленники все лучше и лучше используют уязвимости в системах защиты, – говорит ведущий инженер подразделения Cisco по разработке решений ИБ Джейсон Брвеник (Jason Brvenik). – Мы обнаружили, что для 56% установленных версий OpenSSL все еще актуальна уязвимость Heartbleed, а в крупномасштабных атаках используется лишь один процент всех высококритичных на конкретный момент времени уязвимостей. Несмотря на это, более половины опрошенных представителей служб безопасности не применяет стандартные средства защиты – например, обновление ПО и его безопасную настройку. Даже используя лучшие технологии ИБ, нужно безупречно выстраивать рабочие процессы, чтобы защитить организации и пользователей от изощренных атак и вредоносных кампаний».

В целом результаты проведенного компанией Cisco исследования показывают, что в постановке задач информационной безопасности и управлении ее приоритетами пришло время проявить себя руководству компаний. «Манифест информационной безопасности»от Cisco, представляющий собой формализованный набор основных принципов построения модели корпоративной безопасности, имеет целью помочь руководству, службам ИБ и пользователям понять и нейтрализовать современные киберугрозы. Он может помочь организациям действовать в вопросах информационной безопасности динамичнее, гибче и прогрессивнее злоумышленников. Принципы же таковы:

1. ИБ должна поддерживать бизнес.
2. Механизмы ИБ должны быть удобны и способны работать в условиях существующей архитектуры.
3. ИБ должна быть незаметной, но информативной.
4. ИБ должна давать возможность вести наблюдение и предпринимать необходимые меры.
5. ИБ должна рассматриваться как комплекс человеческих факторов.

Ежегодный отчет Cisco по информационной безопасности на 2015 год — одно из наиболее серьезных отраслевых исследований. В нем рассматриваются самые свежие сведения об угрозах ИБ, собранные экспертами Cisco, и он содержит отраслевые оценки, тенденции и выводы, касающиеся тех проблем в области информационной безопасности, которые могут возникнуть в 2015 году. В отчете использованы данные исследования Cisco Security Capabilities Benchmark, в рамках которого было изучено множество организаций и то, как эти организации оценивают состояние своей информационной безопасности. В отчете уделено также внимание геополитическим тенденциям, мировым событиям, связанным с требованиями к местонахождению данных, и вопросу вынесения проблем ИБ на уровень высшего руководства компаний.

Дополнительная информация
Александр Палладин, глава пресс-службы Cisco
в России/СНГ
тел. (985) 226-3950
Справочная информация общего характера –
по телефону
(495) 961-1410

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ КОСМИЧЕСКИХ ИССЛЕДОВАНИЙ В РОССИИ

Мясникова
Анна Ивановна,
аспирант Северо-Кавказского филиала Московского технического университета связи и информатики, г. Ростов-на-Дону, Россия, man@yandex.ru

Ключевые слова:
космические исследования, запуски, космонавтика, космическая индустрия, программа развития.

АННОТАЦИЯ

Было время, когда, космонавтика была зоной абсолютной гордости нашей страны: первый спутник, полет Юрия Гагарина, первый выход в космос Алексея Архиповича Леонова. Казалось, что выигранная тогда космическая гонка — это не только вполне резонный повод гордиться своей страной и достижениями своей страны, но ещё и нечто достигнутое навсегда. После того как у нас поменялись обстоятельства жизни, выяснилось, что далеко не навсегда. И как космонавтика была в конце 50-х, 60–70 годы скорее поводом для гордости, так последнее время для людей не очень посвящённых она скорее повод для расстройства: неисправности, аварии, отставание в развитии космической индустрии.

Существует мнение, что нет какой-то более или менее единой точки зрения внутри страны на то, что же в нашей космонавтике происходит: мы должны собраться, ощетиниться, сосредоточиться, и улететь на Марс; для полёта на Марс у нас нет достаточного количества ресурсов. Есть мнение, что мы выигрываем борьбу за рынок коммерческих запусков, однако сам по себе рынок коммерческих запусков — это самое неинтересное, что есть в космонавтике вообще.

Проект развития космодрома «Восточный» в настоящее время не оправдывает возложенных на него надежд. Считалось, что это будет не просто космодром, а это будет некий центр притяжения экономических, интеллектуальных и прочих сил, который двинет вперед развитие всего Дальнего Востока, чуть ни всей Сибири. В последнее время данный космодром связан больше с экономическими преступлениями, чем с экономическим и интеллектуальным развитием. По планам «Ангара– 5» должна полететь в 2018 году, «Ангара –7» — в 2020 году, а по информации из средств массовой информации эти данные постоянно ставятся под сомнения. Таким образом, нет сколько-нибудь ясного понимания о том, что происходит в современной космической отрасли.

Статья подготовлена по материалам выступлений заседания Никитского клуба о российской космонавтики.

В ближайшее время завершается официальное формирование программы развития космонавтики на следующие десять лет – с 2016 по 2025 годы [1]. В этой области сделано за последние годы гораздо меньше, чем хотелось и планировалось. Тем не менее, заниматься космической отраслью, не будучи оптимистом, невозможно.

Существуют три главные задачи, которые все страны, занимающиеся фундаментальной наукой в космосе, пытаются решить в начале XXI века: вопросы происхождения Вселенной и новая физика, жизнь во Вселенной (экзопланеты) и Земля как космическая экосистема – взгляд на землю из космоса (рис. 1). Сделано много открытий о том, как образовалась Вселенная, а в последнее время обнаружено, что расширение Вселенной происходит с ускорением. В природе существует какая-то совершенно новая субстанция, называемая тёмной энергией, которая, в отличие от гравитации, расталкивает вещество [2].

Рис. 1. Задачи космических исследований

Ещё одно совершенно потрясающее открытие сделано буквально в последние годы. Обнаружено уже почти две тысячи экзопланет, то есть множество планетных систем у других звёзд. Многие из них совершенно не похожи на нашу Солнечную систему, тем не менее, уже обнаружены планеты – кандидаты на то, что они могут быть обитаемыми. Некоторые из них сравнимы по размерам с нашей Землей, и их иногда называют суперземлями.

Исходя из результатов космических исследований можно сказать, что Земля в каком-то смысле находится в центре всех космических событий. На неё влияет не только Солнце, на неё влияют вспышки далёких сверхновых звёзд, влияет движение всей нашей планетной системы через межзвёздную среду.

Всё, на чём основывается наша цивилизация, – технологии, электроника, биохимия и атомная техника, – наследство, которое мы проедаем, доставшееся нам из прошлого, начиная с Максвелла, Эйнштейна, всей физики, созданной в конце XIX – начале XX веков: теория электромагнетизма, теория относительности, квантовая теория. Не надо никого убеждать, что каждое из этих открытий дало очень много. Телефоны, вся полупроводниковая техника, не говоря уже вообще о радио и телевидении, – результаты открытий, которые сделаны нашими предшественниками. Но в каком-то смысле этот этап завершился, нужен следующий качественный сдвиг для понимания природы, какие-то новые открытия. И мы их можем получить, делая очень дорогостоящие, сложные эксперименты на громадных установках типа Большого адронного коллайдера, или в космосе, потому что именно на галактических масштабах можно обнаружить проявления этих новых законов природы.

Во многих явлениях возникает ещё одна странная и пока непонятная субстанция, называемая тёмной энергией, неизвестная нам форма материи (рис. 2).

После теории эфира, пришла теория электромагнетизма, и у человечества началась другая жизнь.

Рис. 2. Исследование Вселенной и новая физика

Открытия, которые кажутся сейчас абстрактными, рано или поздно скажутся. Это не просто абстрактное знание, все эти эффекты могут оказаться важными и для Земли. Наша Земля находится где-то на краю нашей Галактики (рис. 3), в центре Галактики происходят очень мощные процессы, обнаружена массивная

чёрная дыра, выделяется громадная энергия. Землю спасает то, что она находимся на обочине нашей Галактики. Излучения, которые приходят из космоса, очень влияют на изменчивость и эволюцию человечества. Мутации, необходимые для эволюции, возникают, в частности, из-за частиц галактических космических лучей – частиц, ускорившихся в глубинах Галактики или даже в галактиках, соседних с ней.

Климатические изменения, дождеобразование тоже инициируются потоками галактических космических лучей – центров формирования капель дождя. Современная космическая наука старается все эти вещи изучать.

Земля укутана достаточно плотной атмосферой и её ионизованной внешней зоной – ионосферой, кроме того есть дополнительный зонтик, созданный магнитным полем, отклоняющий враждебные заряженные частицы. Узенькая полоска – длины электромагнитных волн, различных электромагнитных излучений, приходящих из космоса воздействуют на Землю во всем спектре: длинноволновые радиоволны, самое коротковолновое жёсткое гамма-излучение, рентгеновское излучение, находящееся фактически на границе с ультрафиолетом (рис. 4). Есть два окна, в которых мы можем узнавать что-то новое о Вселенной: очень узкий интервал света – весь видимый нашим глазом цветовой спектр, от красного до фиолетового, всего несколько сотен нанометров и окно, через которое проникает радиоизлучение, где оно не отражается довольно мощной земной ионосферой. Радиоастрономия потому и начала развиваться раньше других наук, потому что после Второй мировой войны, до начала космической эры, получали знания о Вселенной с помощью радиометодов.

После того как человек вышел в космос, все эти завесы сняты и в настоящее время проводятся эксперименты во всех диапазонах длин волн. На высотах уже в несколько сотен километров видимы практически все космические излучения. Солнце, как его можно увидеть глазами – это массивный однородный диск, иногда только на нём появляются солнечные пятна (рис. 5). Это то, что человечество знало до начала космической эры. О пятнах знали, конечно, много, их считали, нашли 11-летние солнечные циклы. Солнце при этом выглядит спокойным и вполне уравновешенным.

Совершенно другая картина видна в рентгене и в ультрафиолетовом свете: Солнце «дышит» на масштабе десятков сотен секунд, то есть производит совсем другое впечатление. Таким образом целесообразно все эксперименты делать именно в космосе.

В программу развития космонавтики на 2016–2025 гг. входят условно четыре направления [3-5] (рис. 6). Первое направление – это планеты и исследования Солнечной системы, прежде всего Луна, Марс, кометы, астероиды. Второе направление – это внеатмосферная астрономия, которая в нашей стране оказалась развита хуже, были потеряны очень многие тех-

Рис. 3. Земля как космическая экосистема

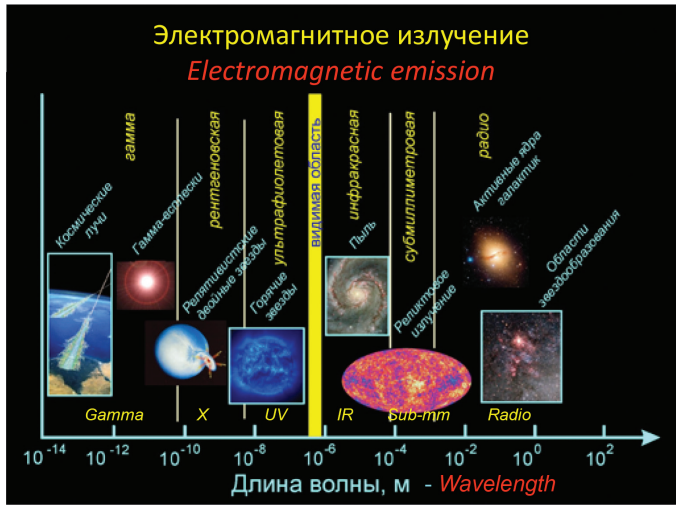


Рис. 4. Электромагнитное излучение

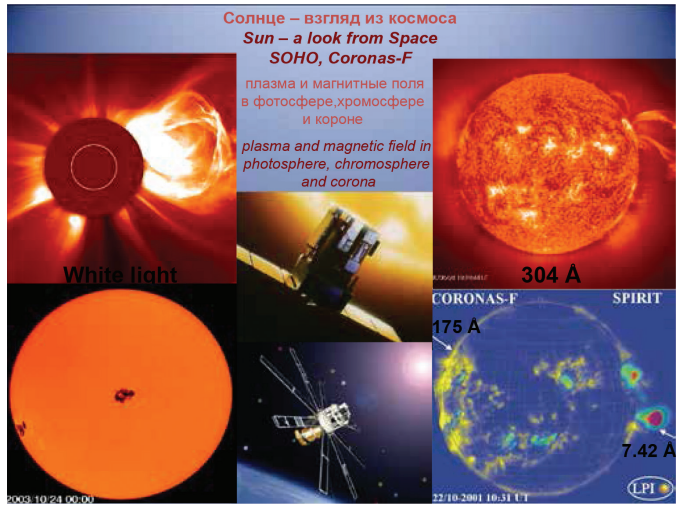


Рис. 5. Солнце – взгляд из космоса

нологии. Сейчас в космосе работает пока только один российский научный аппарат – «Спектр-Радиоастрон» (работает в радиодиапазоне), большой космический интерферометр. С опозданием примерно на 10–12 лет в этом десятилетии готовятся к запуску два проекта: астрономические исследования в рентгеновском и ультрафиолетовом диапазонах – два больших проекта из этой же серии «Спектр».

Третье направление: солнце постоянно излучает поток горячей плазмы, и поэтому возникают важные задачи исследований космической плазмы и солнечно-земных связей. В ближайшее десятилетие готовятся несколько интересных проектов на эту тему. И, конечно, для пилотируемой космонавтики важно четвертое направление – исследование проблем космической биологии и медицины (эти вопросы рассматриваются Институтом медико-биологических проблем).

В наше сложное время российские ученые все-таки сумели «пробиться» на зарубежные космические аппараты. Очевидно, что это не очень просто: надо сделать конкурентоспособный прибор, пройти жёсткий конкурсный отбор. В настоящее время российские приборы работают около Марса, Луны и Венеры, готовятся лететь и на Меркурий (рис. 7).

Сейчас российские приборы успешно и долго работают на «чужих» спутниках: уже больше десяти лет дает интересные результаты прибор HEND на американском аппарате MarsOdyssey, почти столько же – на европейском аппарате MarsExpress, сходные приборы работают почти десять лет и на VenusExpress. На поверхности Марса знаменитый марсоход Curiosity тоже возит российский прибор. Таким образом, российские ученые показали, что научные приборы они могут делать более чем успешно. К большому сожалению, из отечественных летает сейчас всего один аппарат – «Радиоастрон», и до недавнего времени работал маленький спутник, сделанный в Академии наук, запущенный с помощью корпорации «Энергия» на грузовом корабле «Прогресс». Спутник очень хорошо проработал почти три года, но недавно просто сгорел из-за торможения в ионосфере.

Теперь рассмотрим перспективы развития российской космонавтики. Проект «Спектр», работающий в ультрафиолетовом диапазоне, разрабатывает Институт астрономии. «Спектр», работающий в рентгеновском диапазоне, который будет запущен через год или максимум через полтора, разрабатывал Институт космических исследований. Он почти готов, фактически это будет грандиозный российско-немецкий эксперимент.

Существует три объекта в Солнечной системе, на которые космическая отрасль нацелена в этот период. У американских коллег подобный список гораздо длиннее: они летают и к планетам-гигантам, и к планетам земной группы, планируют и экспедицию к астероидам. Первый объект – это Луна, но совершенно другая Луна, чем та, которая исследовалась в советское время. Теперь все исследования концентрируются на изу-

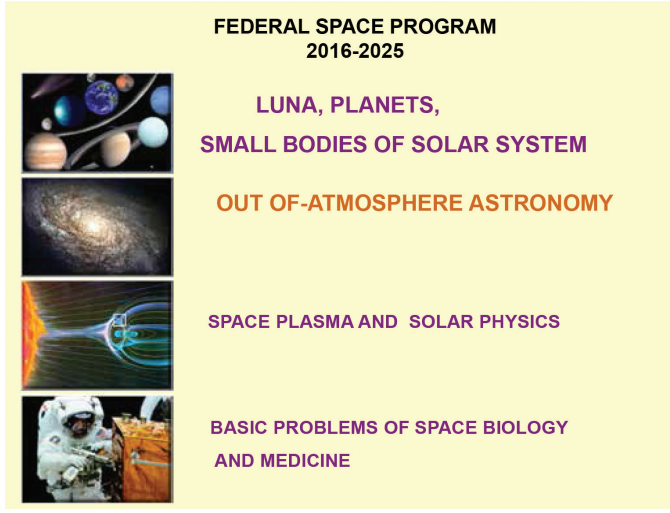


Рис. 6. Федеральная космическая программа 2016-2025

Рис. 7. Проекты и следования Российской академии наук и Роскосмоса

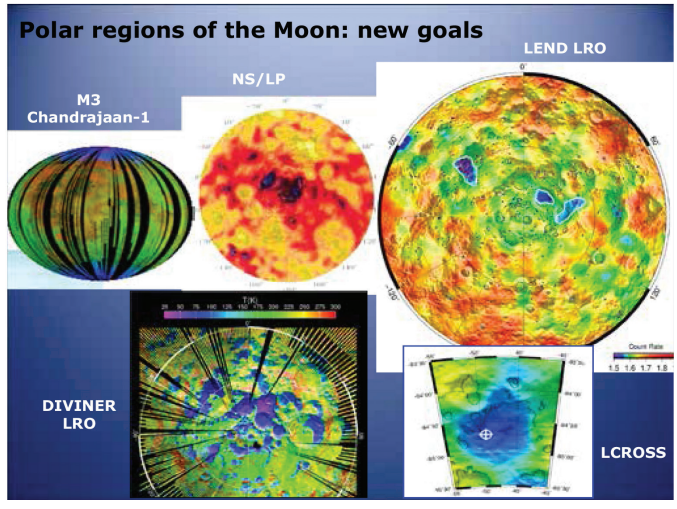


Рис. 8. Полярные области Луны

чение ее полярных областей, где под поверхностью находится ощутимое количество водяного льда (рис. 8).

Следующий проект – повторная экспедиция к Фобосу и доставка его грунта, что не удалось в 2011 году. И на основе этих двух проектов рассматриваются перспективные исследования Марса. Очевидно, что пилотируемый полет к Марсу в ближайшие десятилетия в нашей стране невозможен, до Марса живым человеку сейчас долететь очень трудно из-за космической радиации [2-3].

В этом году создается интегрированная программа исследования Луны, где пилотируемая программа будет тесно связана с робототехникой [3-5]. До этого, к сожалению, автоматические и пилотируемые исследования развивались почти параллельно и мало пересекались. Изучение полярных областей Луны – наиболее перспективные исследования. Голубые пятна на фотографиях сделанных индийским аппаратом Чандраян, американским исследовательским аппаратом LunarReconnaissanceOrbiter (рис. 8) – это области, где по данным российского прибора LEND происходит особое поглощение нейтронов. Голубой цвет на поверхности означает маленький поток нейтронов, нейтроны хорошо замедляются в воде, потому, что масса нейтрона и масса протонов, которые входят в атомы водорода – соизмеримы. Рассеяние всегда происходит хорошо, когда сталкиваются шарики одинаковой массы, и эти голубые области (те области, где сильно поглощаются нейтроны) – есть указание на то, что под этими областями находятся запасы различных летучих веществ, в том числе и столь желанного водяного льда. Данный факт был подтвержден и прямыми измерениями. Американцы сбросили на одну из таких областей одну из ступеней своего космического аппарата. Он ударился, произошёл выброс вещества, а орбитальный аппарат, пролетая в это время, увидел линии поглощения воды. Таким образом, присутствие на Луне воды можно считать доказанным фактом [2].

Рассмотрим фотографию Луны на основании проведенных исследований в 60-е и 70-е годы: синими звёздочками обозначены места посадки «Аполлонов», откуда было доставлено несколько сотен килограммов лунного грунта, а красные звёздочки – это места советских доставок (рис. 9). Все эти области находятся в средних широтах, соответственно полярные области Луны тогда не исследовались [2-3].

В 60-е и 70-е годы было время большой лунной гонки. Благодаря президенту Кеннеди и объявленной американцами программе, они считают, что ее выиграли. Однако, то, что было сделано тогда в Советском Союзе, тоже достойно очень высокой оценки. Луна-16, -20, -24 (рис. 10) – это три успешных доставки лунного вещества из разных районов (рис.9), сейчас находятся в музее и в лабораториях Института геохимии имени Вернадского. Вещества, конечно, доставлено на порядки меньше, чем астронавтами «Аполлона», но в данном случае результат измеряется не килограммами, пото-

Рис. 9. Районы доставки грунта

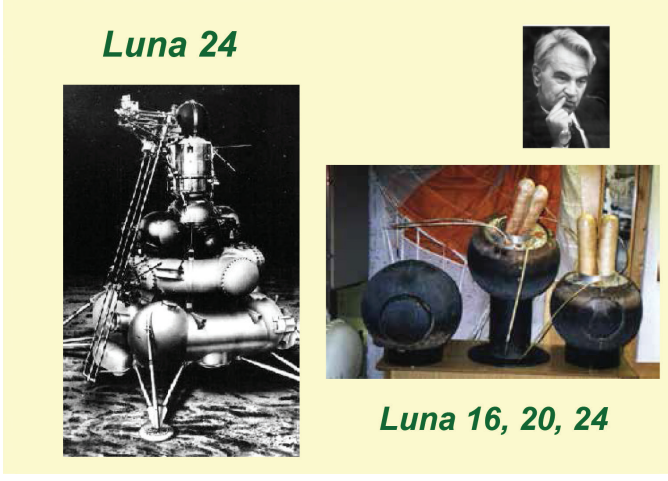


Рис. 10. Луна 16, 20, 24.

Рис. 11. Молекулы в межзвездной среде и в кометах

му что для подробного геохимического анализа много вещества не нужно [1-3].

С помощью бурильной установки грунт извлекался довольно глубоко, на глубине примерно два метра. При этом испарялись все летучие включения, которых в этих областях и так почти нет. В настоящее время перед исследователями будет стоять гораздо более сложная задача – понять, как вообще вода попала на Луну, как она сохраняется, и как извлечь этот лёд не нагревая его. Это, прежде всего, связано с созданием лунных баз в будущем, которые лучше размещать не на сухом, мёртвом месте, а там, где есть хоть какой-то запас воды. Кроме того в кометах обнаружен длинный список молекул, среди которых много и органических молекул (рис. 11).

Луна испещрена кратерами, на Луне нет атмосферы. И всё, что на Земле стирается от эрозии – ветровой, дождевой, на Луне лежит, как в вечном музее. Кометы, упавшие на Луну за четыре миллиарда лет её существования, оставили следы, принесли туда те органические вещества, которые по многим теориям считаются источниками жизни. Это ключ к каким-то важным вопросам о происхождении, возникновении жизни. Есть такая известная теория панспермии – о том, что споры жизни разносятся кометами. На Луне, где эти вещества хранятся вблизи полюсов, как в вечном холодильнике, можно это увидеть [1-3].

Существует еще другой подход. Наши европейские коллеги сейчас осуществили очень смелый полёт к комете Чурюмова-Герасименко, сели на неё и подробно исследовали её вещество. В свою очередь российские ученые решили действовать по-другому: ловить то, что уже принесли кометы за миллиарды лет и хранится в полярных областях Луны. В перспективе рассматривается создание на Луне посещаемой базы – базы, которую в вахтовом режиме будут посещать космонавты. Много конструкций такой базы было проработано раньше (рис. 12). В России был знаменитый учёный и инженер Владимир Бармин, разработчик и ракетных стартов на Байконуре и лунных жилых модулей, поэтому такие поселения даже получили названия «Барминграды».

Отдельный вопрос – какие научные задачи могут быть решены на Луне. Сейчас выбираются районы для будущих посадок на Луне (рис. 13), области вблизи полюса, которые обладают ещё одним важным свойством: здесь есть постоянная радиовидимость Земли. На обратной стороне Луны тоже очень много интересного, но тогда посадочный аппарат утратит связь с Землей, и это может создать много технических сложностей [1-3].

Рассмотрим перспективы разработки посадочных аппаратов, над которыми работает Научно-производственное объединение имени С. А. Лавочкина, монополист и единственная фирма, которая занимается такими межпланетными роботами ещё со времён Королева. Первый перспективный аппарат называется ЛУНА-25. Поскольку последний советский посадочный аппарат назывался ЛУНА-24, было решено показать, что разработки ведутся давно и отсчёт ведется именно

Рис. 12. Стратегическая цель освоения Луны № 1

Рис. 13. Стратегическая цель освоения Луны № 2

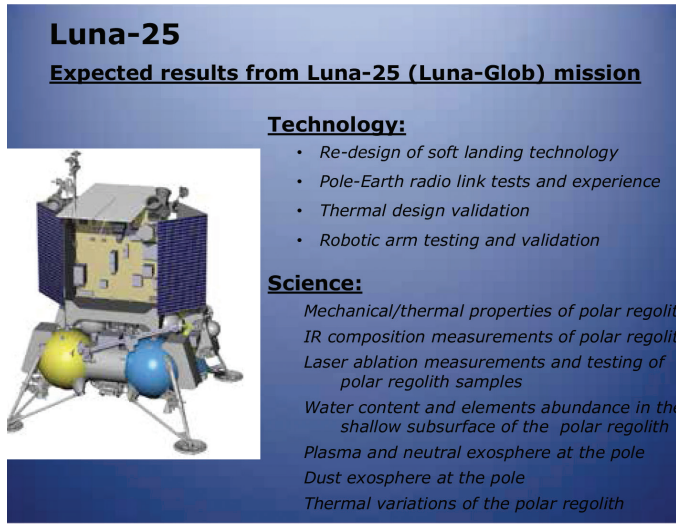


Рис. 14. Луна-25

от этой цифры. ЛУНА-25 – это аппарат, который планируется к посадке в 2018 – начале 2019 года (рис. 14). Он будет простой, на этом этапе проводится восстановление технологии посадки. Большой орбитальный аппарат, который будет исследовать окружение Луны, оказавшееся гораздо сложнее и интереснее, чем представлялось ранее. В частности, есть очень важная проблема для будущих посещений – это лунная пыль.

Главный проект – ЛУНА-27. Этот аппарат будет оснащён бурильной установкой, которую предоставят европейские коллеги. Планируется бурение на глубину примерно на 1,5–2 метра под поверхностью Луны, где предположительно и хранятся запасы летучих веществ, присыпанные слоем лунного грунта, который называется «реголит» (рис. 15). Несмотря на все санкции, продолжается сотрудничество с Европейским космическим агентством (ЕКА), особенно по освоению и исследованию Луны. Наиболее важный вклад ЕКА – бурильная установка (рис. 16). Также совместно с Европейским космическим агентством продолжается большая программа по исследованию Марса. Если в лунной программе европейские коллеги присоединяются к нашей программе — при исследовании Марса наоборот: программа сформирована в Европе, и Россия присоединилась к ней позже, но с несколькими жизненно важными составляющими – носителями, посадочной платформой на Марс и комплектами научных приборов [1-3].

Рассмотрим некоторые актуальные аспекты, вызывающие особое внимание в последнее время. Одним из основных – является пилотируемая программа. Существует решение, что МКС будет использоваться до 2024 года совместно с международными партнерами. После 2024 года возможно построение собственной перспективной орбитальной станции на базе российских новых модулей. Рубеж 2030 года – освоение Луны. Напомним, что никакая пилотируемая космическая программа освоения космоса не обеспечивает экономические или научные результаты, которые сами по себе превосходят те же результаты от космических автоматов. Уход от пилотируемого космоса – огромный риск развала вообще всей системы мотиваций заниматься российской космической программой. С этой точки зрения пилотируемый космос играет помимо безусловных научно-исследовательских аспектов еще и роль скрепляющего элемента национальной космической программы как таковой [2-3].

Средства выведения: актуально то, что российская промышленность не выпускает сверхтяжелую ракету, а выпускает «Ангару-5В», которая сравнительно взвешенная по параметрам. Кроме того, этой весной прозвучали призывы к тому, чтобы усилия в рамках Федеральной космической программы соизмерялись с возможностями по финансированию и видением на десятилетнюю перспективу развития космической отрасли [3].

Результатами планируемой космической программы являются: запуск более 180 космических аппаратов, пилотируемый облёт Луны, начало работ по сверхтяжелому классу ракет и ряд других интересных, а самое главное полезных аспектов.

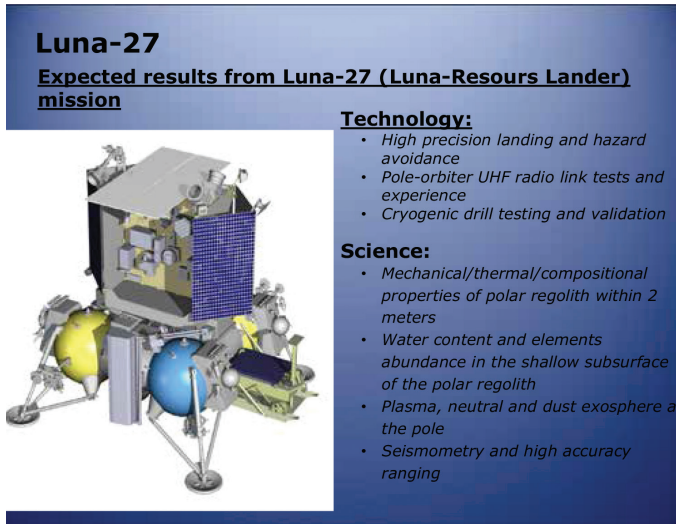


Рис.15. Луна-27

Рис. 16. Сферы потенциального сотрудничества с ЕКА

Подводя итоги можно с уверенностью сказать, что Россия – мировая космическая держава. Космонавтика стала одним из системообразующих элементов нашего представления о себе как о великой державе, как о государстве с большим позитивным наследием. Вся российская космонавтика как феномен, как элемент социокультурного ландшафта, уникальна в том плане, что вносит свой вклад в самоосознание наших людей, которые все-таки причастны к чему-то хорошему. Существует надежда, что примерно до конца этого года будет принята Федеральная космическая программа России на 2016–2025 годы. И все аспекты, которые были рассмотрены выше, прежде всего в части исследований Луны, найдут там своё достойное место, и в

скором времени можно будет увидеть и новые российские космические аппараты, и новые научные результаты, полученные с использованием этих аппаратов.

Литература

1. http://www.federalspace.ru/21430/(дата обращения 01.08.2015).

2. Цикл публичных дискуссий «Кто, что и как делает в космосе. Проекты и субъекты в космонавтике». № 75. М. 2015. 80 с.

3. http://nikitskyclub.ru/?p=1205 (дата обращения 01.08.2015).

4.http://protown.ru/information/doc/4317.html (дата обращения 01.08.2015).

5. http://ras.ru/scientificactivity/planto20.aspx (дата обращения 01.08.2015).

Для цитирования:
Мясникова А.И. Основные направления развития космических исследований в России // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 60–67.

THE MAIN DIRECTIONS OF SPACE RESEARCH DEVELOPMENT IN RUSSIA

Myasnikova Anna Ivanovna,
Rostov-on-Don, Russian, *man@yandex.ru*

Abstract
There was a time when that space was an area of absolute pride of our country: the first satellite, the flight of Yuri Gagarin, the first spacewalk by Alexei Arkhipovich Leonov. It seemed that then won the space race is not only reasonable reason to be proud of their country and the achievements of their country, but also achieved something forever. After we have changed the circumstances of life, it became clear that not forever. And how space exploration was in the late 50s, the 60s-70s rather a cause for pride, for people are not very dedicated to it rather upset: malfunctions, accidents, delays in the development of space industry.
There is an opinion that is no more or less a single point of view within the country that in our space is happening: we need to get together, up, focus, and fly to Mars; mission to Mars we don't have enough resources. There is an opinion that we win the struggle for the market of commercial launches, however, the commercial launch market is the most uninteresting thing in the space at all.
The project of development of the spaceport «Vostochny» at the present time does not justify the hopes assigned to it. It was thought that this would be not just a spaceport, and it will be a center of attraction for economic, intellectual and other forces, which will move forward the development of the Far East, almost the whole of Siberia. Recently, this spaceport is associated more with economic crimes, than with the economic and intellectual development. According to the plans of the «Angara - 5» should fly in 2018, «Angara - 7» in 2020, and according to the information from the media data is being put into question. Thus, there is no clear understanding about what is happening in the modern space industry.

Keywords: space research, launches, space exploration, space industry development programme.

References

1. http://www.federalspace.ru/21430/ (date of assess 01.08.2015).
2. A series of public discussions «Who, what and how makes in space. Projects and subjects in space». Vol. 75. M., 2015. 80 p. (In Russian).
3.http://nikitskyclub.ru/?p=1205 (date of assess 01.08.2015).
4. http://protown.ru/information/doc/4317.html (date of assess 01.08.2015).
5. http://ras.ru/scientificactivity/planto20.aspx (date of assess 01.08.2015).

Information about authors:
Myasnikova A.I., post-graduate student of North-Caucasus branch of the Moscow technical University of communications and Informatics.

For citation:
Myasnikova A.I. The main directions of space research development in Russia. H&ES Research. 2015. Vol. 7. No. 4. Pp. 60–67. (in Russian).

24-Я НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ «МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ»

С 29 июня по 2 июля в пригороде Санкт-Петербурга п.Репино (Загородный клуб «forRestMix») прошла 24-я научно-техническая конференция «Методы и технические средства обеспечения безопасности информации», посвященная 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 было 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.

В работе конференции приняли участие около 200 человек, из них научных работников высшей квалификации: докторов наук около 30 человек, кандидатов наук около 40 человек.

В составе участников конференции: ведущие ученые и специалисты в области информационной безопасности, представители органов государственной власти субъектов Российской Федерации, руководители и представители вузов, академических учреждений, научно-исследовательских организаций и предприятий из различных регионов России.

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

МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ «СИНХРОИНФО-2015»

В Санкт-Петербургском государственном университете телекоммуникаций имени профессора М.А.Бонч-Бруевича 29–30 июня 2015 состоялась Международная научно-техническая конференция «Системы синхронизации, формирования и обработки сигналов в инфокоммуникациях» (СИНХРОИНФО 2015).

Научные проблемы конференции были вынесены на пленарное заседание и заседания трех секций:

1. Системы и устройства синхронизации.
2. Устройства генерирования и формирования сигналов.
3. Системы и устройства приема и обработки сигналов.

Кроме того на конференции проводилось обсуждение актуальных вопросов теории и практики создания перспективных инфокоммуникационных систем и устройств. В работе конференции приняли участие более 100 представителей российских и зарубежных предприятий и организаций научной отрасли.

Лучшие доклады конференции были рекомендованы к публикации в виде статей в журналах: «T-Comm – Телекоммуникации и транспорт», «Наукоемкие технологии в космических исследованиях Земли» и «Электросвязь».