Министерство связи и массовых коммуникаций РФ

Федеральное агенство связи (РОССВЯЗЬ)
Московский технический университет связи и информатики (ФГОБУ ВПО МТУСИ)
Закрытое акционерное общество «Научно-производственный центр информационных региональных систем» (ЗАО «НПЦ ИРС»)

НПЦ ИРС

30.10.2014

ВСЕРОССИЙСКАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

по теоретическим и прикладным проблемам развития и совершенствования автоматизированных систем управления специального назначения

«НАУКА И АСУ – 2014»

МОСКВА

при информационной поддержке

МЕДИА ПАБЛИШЕР
T•Comm ТЕЛЕКОММУНИКАЦИИ И ТРАНСПОРТ
Hi-tech Earth Space RESEARCH
ИНТЕЛТЕХ

nauka-i-asu.ru
konferencia_asu_vka@mail.ru

H&ES RESEARCH

ТОМ V
No. 4-2013

Наукоёмкие технологии
в космических исследованиях Земли

СОДЕРЖАНИЕ

НОВОСТИ
Новости науки и техники, события, люди
4

ТЕХНОЛОГИИ
Ходжаев И.А., Соловьев А.М.
Математическая модель измерений и результаты моделирования параметров усилителя низкой частоты
10

ТЕЛЕКОММУНИКАЦИИ
Фрайди Б.
Что идет на смену эпохе мобильных телефонов?
16

Будко П.А., Чихачев А.В., Баринов М.А., Виноградено А.М.
Основные направления организации и планирования телекоммуникационной среды сил специального назначения
18

СИСТЕМЫ УПРАВЛЕНИЯ
Анисимов И.И., Толмачёв А.А., Чащин С.В.
Подход к оцениванию живучести сложных организационно – технических систем различного назначения
24

СТАНДАРТЫ БЕСПРОВОДНОГО ШИРОКОПОЛОСНОГО ДОСТУПА
Частотный спектр сетей четвертого поколения (4G): текущая ситуация, перспективы в России и мире MW RUS
30

УСЛУГИ ДОСТУПА В ИНФОКОММУНИКАЦИЯХ
Цветков К. Ю., Федосеев В.Е., Абазина Е.С.
Применение двумерных нелинейных сигналов Франка-Уолша, Франка-Крестенсона в методе формирования скрытого канала с кодовым уплотнением в структуре сжимаемых видеоданных
32

ИНФОРМАЦИОННАЯ И КИБЕРБЕЗОПАСНОСТЬ
Орлов А.А., Тельных А.А., Степанов Е.А., Сорокин А.Д., Аксенова Ю.Е.
Технические аспекты создания автоматизированных информационных систем многоцелевого применения
40

Компания «Инфосистемы Джет» раскрывает подробности защиты программы МАЛИНА от DDoS
45

КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ
Буренин А.Н., Легков К.Е.
Некоторые модели управления безопасностью инфокоммуникационных сетей специального назначения
46

«Борлас» добавит к технической безопасности информационную
51

CONTENTS

NEWS
News of science and technology, events, people
4

TECHNOLOGIES
Khodzhaev I., Soloviev A.
Mathematical model of measurement and simulation results parameters bass amplifier
10

TELECOMMUNICATIONS
Friday B.
What is going to replace the are of mobile phones?
16

Budko P., Chikhachev A., Barinov M.,Vinogradenko A.
Main directions of the organization and planning of the telecommunication environment of forces of a special purpose
18

CONTROL SYSTEMS
Anisimov I., Tolmachyov A., Chashchin S.
The approach to estimation of survivability of the difficult organizational - technical systems of different function
24

STANDARDS FOR BROADBAND WIRELESS ACCESS
The frequency spectrum for fourth generation networks (4G): curnent situotion and prospects in the world and in Russia
30

ACCESS SERVICES IN INFOCOMMUNICATIONS
Tsvetkov K., Fedoseev V., Abasina E.
Application of two-dimensional nonlinear signals of Frank-Uolsh, Frank-Krestenson into the method of formation of the hidden channel with code consolidation in structure of the compressed video data
32

INFORMATION AND CYBERSAFETY
Orlov A., Telnykh A., Stepanov E., Sorokin A., Aksenova U.
Technical aspects of automated information systems' multiple application development
40

The company «Infosystems Jet» reveals the details of the protection MALINA from DDoS
45

COMPLEX SAFETY
Burenin A., Legkov K.
Some models of security management infocommunication networks of the special purpose
46

The «Borlas» will add to the techical security information
51

Vol. V
No. 4-2013

H&ES RESEARCH
High technologies in Earth space research

Периодичность выхода — 6 номеров в год
Стоимость одного экземпляра 500 руб.

Тематические направления
• Вопросы развития АСУ • Физико-математическое обеспечение разработки новых технологий и средств инфокоммуникаций • Условия формирования основных стандартов подвижной связи • Проектирование, строительство и интерактивные услуги в СПС • Биллинговые и информационные технологии • Электромагнитная совместимость • Антеннофидерное оборудование • Источники электропитания • Волоконно-оптическое оборудование и технологии • Вопросы исследования космоса • Спутниковое телевидение, системы спутниковой навигации, GLONASS, построение навигационных систем GPS • Вопросы развития геодезии и картографии • Программное обеспечение и элементная база для сетей связи • Компьютерная и IP-телефония • информационная и кибербезопасность • Вопросы исследования Арктики • Метрологическое обеспечение • Правовое регулирование инфокоммуникаций, законодательство в области связи • Экономика связи

Hi-tech Earth Space RESEARCH

Редакция
Главный редактор: Константин Легков
HT-ESResearch@yandex.ru

Издатель: Светлана Дымкова
ds@media-publisher.ru

Предпечатная подготовка
ООО "ИД МЕДИА ПАБЛИШЕР"
www.media-publisher.ru

Адрес редакции
111024, Россия, Москва,
ул. Авиамоторная, д. 8, офис 512-514
Тел.: +7 (495) 957-77-43

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

Журнал "Наукоемкие технологии в космических исследованиях Земли" (H&ES) зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия.
Журнал входит в систему Российского индекса научного цитирования (РИНЦ)

Мнения авторов не всегда совпадают с точкой зрения редакции. За содержание рекламных материалов редакция ответственности не несет

ПРАВИТЕЛЬСТВО УДМУРТСКОЙ РЕСПУБЛИКИ

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ ПО УДМУРТСКОЙ РЕСПУБЛИКЕ

ГЛАВНОЕ УПРАВЛЕНИЕ МЧС РОССИИ ПО УДМУРТСКОЙ РЕСПУБЛИКЕ

АДМИНИСТРАЦИЯ ГОРОДА ИЖЕВСКА

УДМУРТСКАЯ ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА

ВЫСТАВОЧНЫЙ ЦЕНТР «УДМУРТИЯ»

ВЫСТАВКА ПРОХОДИТ ПОД ПАТРОНАЖЕМ ТОРГОВО-ПРОМЫШЛЕННОЙ ПАЛАТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Всероссийская специализированная выставка

5 ЛЕТ

Комплексная безопасность

18-20 сентября / 2013

ПРИГЛАШАЕМ ПРИНЯТЬ УЧАСТИЕ!

В ТЕЧЕНИЕ 5 ЛЕТ:

- **ВЕДУЩИЕ ПРЕДПРИЯТИЯ РОССИИ**
- **ДЕМОНСТРАЦИОННАЯ ПРОГРАММА С ИСПОЛЬЗОВАНИЕМ ПРОДУКЦИИ УЧАСТНИКОВ**
- **ДЕЛОВЫЕ МЕРОПРИЯТИЯ**
- **ПРОФЕССИОНАЛЬНАЯ АУДИТОРИЯ**

ПОЖАРНАЯ БЕЗОПАСНОСТЬ
ОБЩЕСТВЕННАЯ БЕЗОПАСНОСТЬ
МЕДИЦИНА КАТАСТРОФ
ЭКОЛОГИЧЕСКАЯ И ПРОМЫШЛЕННАЯ БЕЗОПАСНОСТЬ
БЕЗОПАСНОСТЬ В ЧС
БЕЗОПАСНОСТЬ ТРУДА
БЕЗОПАСНОСТЬ ДОРОЖНОГО ДВИЖЕНИЯ

ОДНОВРЕМЕННО СОСТОИТСЯ
II ВСЕРОССИЙСКАЯ СПЕЦИАЛИЗИРОВАННАЯ ВЫСТАВКА «МЕДИЦИНА И ЗДОРОВЬЕ»

Место проведения выставки:
г. Ижевск, ул. Кооперативная, 9

ЧЛЕН РОССИЙСКОГО СОЮЗА ВЫСТАВОК И ЯРМАРОК

Выставочный центр «УДМУРТИЯ»
тел./факс: (3412) 733-581, 733-585, 733-587, 733-664
safe@vcudm.ru | **www.safe.vcudm.ru** | vk.com/izh.safe

Ученые будущего встретились на озере Байкал

На озере Байкал завершилась вторая летняя школа-конференция в области естествознания и нанотехнологий для школьников (остров Ольхон).

Летняя школа прошла при поддержке Министерства образования Иркутской области, корпорации Intel, компании "НТ-МДТ", Иркутского научного центра СО РАН, Центра информационно-методического и психологического обеспечения деятельности муниципальных образовательных учреждений г. Иркутска.

Участие в проекте приняли 34 школьника 7-11 классов из 8 регионов России и Республики Казахстан, представившие свою научно-исследовательскую работу в областях физики, химии, биологии, математики или нанотехнологий и прошедшие отборочный тур.

В далеке от больших городов юные ученые и преподаватели школы на две недели погрузились в интересный мир науки и техники. Участников проекта ждали лекции по лазерным нанотехнологиям, структуре магнитных жидкостей и другим темам современного естествознания, мастер-классы по использованию сканирующего зондового микроскопа и проектированию электронных устройств, а также защита своих первых научно-инженерных проектов в кругу сверстников-единомышленников и перед квалифицированным жюри.

Участники конференции посетили самые удивительные места озера Байкал, отправившись в тридцатикилометровый пеший поход по острову Ольхон.

Одной из особенностей летней школы на Байкале стало то, что лекции и мастер-классы были проведены не только признанными преподавателями и учеными, но и студентами. Так, Юлия Соколова, студентка химического факультета СпбГУ и победитель международного конкурса научно-инженерных проектов старшеклассников Intel® ISEF 2012, совместно с Даниилом Козловым, студентом факультета наук о материалах МГУ имени М.В. Ломоносова провели мастер-класс "Химия цвета", полный занимательных и ярких химических экспериментов.

Самые активные юные ученые по результатам работы над научными проектами были награждены дипломами и специальными наградами. Имена победителей и интересные факты о школе можно найти в онлайн-дневнике проекта в блоге Народного учителя РФ и участника Летней школы Льва Васильевича Пигалицына на Образовательной Галактике Intel.

CSTB'2014 — конвергенция телевидения и мультимедийных технологий

28-30 января 2014 г.,
МВЦ "Крокус Экспо", пав. 1.

Выставочная компания МИДЭКСПО и Ассоциация кабельного телевидения России представляют 16-ю международную выставку и форум CSTB'2014

— консолидирующее медийное событие, которое охватывает все актуальные форматы и направления телевизионных и телекоммуникационных технологий: цифровое кабельное, спутниковое и эфирное ТВ; IPTV, OTT TV, HDTV, Ultra HDTV (4K, 8K); ТВ контент; мобильное мультимедийное ТВ; мультисервисные сети; спутниковая связь.

Более 500 ключевых зарубежных и российских компаний-экспонентов представят свои достижения в отрасли. CSTB проводится при поддержке и участии Федерального агентства по печати и массовым коммуникациям, Московской Торгово-Промышленной Палаты и Торгово-Промышленной Палаты РФ.

Выставка и форум CSTB заслуженно стали главным мероприятием орасли благодаря своей богатой на премьеры экспозиционной части и насыщенной деловой программе. Список участников выставки CSTB'2014 доступен на сайте мероприятия по ссылке http://cstb.ru/cstb/exhibitorsList/#.Ukra49K8CgY.

Новой экспозицией выставки станет CONNECTED TV & MOBILE MULTIMEDIA, где будут представлены актуальные телекоммуникационные технологии со всего мира. Телевизионные платформы становятся универсальными, едиными для любого типа доставки ТВ-сигнала. ТВ повсеместно превращается в IPTV, которое открывает безграничные возможности для передачи видео данных. Мобильное телевидение становится социальным. Социальные сети уходят в облачные технологии. В результате, контроль над контентом получает сам пользователь. Теперь абонент требует интерактивное и полностью персонализированное ТВ.

Экспозиция объединит такие направления, как доставка контента на несколько экранов / multiscreen, Smart TV, мобильное ТВ, Интернет ТВ, социальное ТВ, онлайн видео услуги, ТВ решения на базе облачных технологий, OTT, CDN, Ультра HDTV (4K, 8K).

Международный Форум CSTB'2014 предложит вниманию посетителей аналитические доклады и актуальные прогнозы ключевых персон отрасли — как представителей государственных структур, так и представителей бизнеса.

Предварительные секции Форума:

- IP&TV Форум;
- Мобильный мультимедийный Форум и технология мультискрин;
- Технологии будущего;
- Connected TV & Second Screen;
- Возможности интернет-вещания;
- Эволюция маркетинга операторов платного ТВ;
- Спутники как основное решение по доставке сигнала в России;
- Контент, как основная услуга оператора платного ТВ.

Национальная Премия "Большая Цифра" за четыре года существования стала знаковым событием для телевидения и телекоммуникационной отрасли в целом. В стремлении получить эту ценную награду номинанты постоянно совершенствуются, ведь обладание Премией является для победителя визитной карточкой не только в построении долгосрочных плодотворных отношений с бизнеспартнерами, но и для эффективного диалога с государственными ведомствами, регулирующими отрасль. Из нововведений необходимо отметить обновленный список номинаций в категориях "Компанияоператор", "Оборудование и технологии" и "Телеканалы". В категории "Компания-оператор" выделена специальная номинация "Поддержка и обслуживание абонентов" для компаний — операторов с абонентской базой от 10 000 до 100 000, у которых теперь есть ценная возможность приобрести общероссийскую известность как у партнеров и клиентов, так и у конечных потребителей. Прием заявок, начавшийся в июне, продлится до 1 ноября 2013 г. Торжественная церемония награждения победителей состоится 29 января 2014 г.

Среди посетителей CSTB: профильные министерства и ведомства, администрации регионов; телекоммуникационные компании, операторы связи, IT компании; операторы мультисервисных сетей, операторы платного ТВ; производители оборудования; дистрибьюторы, дилеры; системные интеграторы; вещатели и контент-провайдеры; телерадиокомпании; Интернетпровайдеры; финансовые и инвестиционные компании; корпоративные заказчики.

На выставке CSTB'2014 ожидается свыше 25 000 посетителей!

Подробная информация и регистрация для посещения выставки и форума CSTB'2014 на сайте www.cstb.ru.

Технопром-2013

Первый Международный форум технологического развития "Технопром-2013" пройдет в Новосибирске ноября 2013 г. Тема форума — "Шестой технологический уклад" — связана с переходом отечественной экономики к новому этапу развития, который характеризуется снижением энергоемкости и материалоемкости производства, переходом к конструированию материалов и организмов с заранее заданными свойствами. Оргкомитет Форума возглавил заместитель Председателя Правительства России Дмитрий Рогозин.

Начало шестого технологического уклада приходится на второе десятилетие XXI в. и характеризуется опережающим развитием робототехники, нано- и биотехнологий.

В Форуме "Технопром -2013" примут участие более тысячи представителей научного сообщества, бизнеса и власти, десятки экспертов из США, Японии, Китая, стран Европы и СНГ. Партнеры форума — Правительство России, Государственная Дума, Фонд перспективных исследований, Ассоциация инновационных регионов России, Ассоциация технических университетов, Российская академия наук, Сибирское отделение РАН; предприятия, определяющие технологический уровень российской промышленности: ОАО "РЖД", ОАО "РОСНАНО", ГК "РОСАТОМ", ГК "РОСТЕХ", МТС и др.

Участники Форума определят приоритетные направления развития критических технологий в России, ответят на вопросы о мерах стимулирования спроса на перспективные технологии, о создании новых рынков и высокотехнологических отраслей, обсудят лучшие мировые и региональные практики формирования инфраструктуры технологического развития. Отечественные и зарубежные производители представят свои разработки, обменяются идеями по их коммерциализации и заключат в рамках деловой программы мероприятия перспективные контракты. По итогам пленарного заседания и панельных дискуссий будут внесены дополнения в доклад для Президента России.

Выставочная программа Форума позволит гостям ознакомиться с прорывными научными достижениями и технологическими разработками предприятий Новосибирской области, России и зарубежных стран.

Технологии Delphi для новых автомобилей на мотор-шоу IAA во Франкфурте

В рамках проведения мотор-шоу IAA во Франкфурте автопроизводители представили свои новейшие модели, многие из которых оснащены устройствами компании Delphi, делающими автомобили безопаснее и экологичнее, при этом позволяя пассажирам всегда оставаться на связи с окружающим миром.

Удостоенный награды автомобильный звуковой генератор Delphi помогает пешеходам заметить почти бесшумные гибридные и электромобили и позволит производителям соответствовать грядущим нормам безопасности. Моноблочный автомобильный звуковой генератор, разработанный Delphi, примерно втрое легче стандартной многокомпонентной системы. Он потребляет на 90% меньше энергии, что обеспечивает его максимальную экологичность. Конструкция устройства позволяет сократить расходы на разработку, испытания и производство, а небольшие размеры и масса упрощают компоновку. Звуковой генератор устанавливается на новые BMW i3, Mercedes-Benz S-класса и Smart Fortwo.

Подушка безопасности надувается менее чем за 50 мс. Delphi предлагает решения для подсоединения к автомобильной проводке подушек безопасности, а также других пиротехнических устройств.

Технология Gasoline Direct Injection (GDi) позволяет создавать компактные турбированные двигатели с пониженным уровнем выброса CO2 и уменьшенным расходом топлива, что обеспечивает соответствие строжайшим экологическим нормам. Система GDi компании Delphi позволяет значительно сократить выбросы CO2 и уже применяется на автомобиле Peugeot 308.

Интегральные антенны Delphi обеспечивают автопроизводителям универсальность многофункциональных высокопроизводительных систем приема и используются на автомобилях BMW 4 серии купе, BMW i3, Citroen Grand C4 Picasso, Peugeot 308 и RCZ R. Интегральные антенны, при своей эффективности, не портят дизайн автомобиля.

Умный KAMAZ

На международном грузовом автосалоне COMTRANS 2013 ОАО "КАМАЗ" и корпорация Intel представили прототип бортовой информационно-развлекательной системы на базе процессора Intel® Atom™, разрабатываемой Intel для магистральных автомобилей KAMAZ-5490.

Представленный на выставке KAMAZ-5490 — новинка семейства магистральных автомобилей KAMAZ, созданная для перевозок в составе автопоезда полной массой до 44 тонн, — оснащен прототипом автомобильной информационно-развлекательной системы на базе процессора Intel® Atom™.

Программно-аппаратное решение локализовано для российского рынка и включает навигацию с актуальной информацией о загруженности транспортных сетей, радио, медиапроигрыватель, телефонное приложение, календарь, браузер, приложение для удобного общения в социальных сетях, а также голосовое управление и интеграцию с инфраструктурными сервисами.

По словам генерального директора ОАО "КАМАЗ" Сергея Когогина, оснащение нового модельного ряда бортовой информационной системой будет весьма своевременным. "Мы всегда стремимся к самому лучшему, и сотрудничество с Intel, безусловно, большой шаг в этом направлении. Ни один российский автопроизводитель не может похвастаться наличием в своих грузовиках аналогичной интеллектуальной автомобильной системы, которая в буквальном смысле сделает KAMAZ "умным" автомобилем. "КАМАЗ" традиционно рассматривается как компания - локомотив всей отрасли, и мы уверены, что с помощью Intel нам удастся поддержать эту высокую планку", — отметил руководитель крупнейшего российского автопроизводителя.

Прототип выполнен на базе новейшего двухъядерного процессора для встроенных систем Intel® Atom™ и операционной системы с открытым кодом, совместимой с ОС Tizen. Для спутникового позиционирования в прототипе использован гибридный чип GPS/GLONASS, а получение информации со всех датчиков машины в режиме реального времени происходит через CAN шину. Используя бортовую информационную систему, водитель KAMAZ будет имеет возможность всегда оставаться на связи с родными и близкими, а также с базой и грузополучателем при помощи аппаратно-программных средств передачи данных через Wi-Fi, LTE, 3G, GSM и Edge.

Система выполнена в формфакторе 1DIN и предназначена для расположения в верхней части кабины, 7дюймовый сенсорный экран предполагается вынести на переднюю панель. Система сможет управляться посредством голоса, касания, системными кнопками управления, а также с помощью "быстрых кнопок", вынесенных на руль.

Девять стартапов Фонда Сколково в "горячей двадцатке" Mashable

Практически половина лучших российских стартапов, вошедших в «горячую двадцатку» по версии Mashable, — родом из Фонда «Сколково» http://mashable.com/2013/11/14/russia-startups/# .

Mashable —англо-американский новостной сайт, специалит зирующийся на тематике социальных медиа и IT. Количество ежемесячных просмотров страниц сайта составляет порядка 50 млн., в Твиттере сайта — 3,2 млн. фолловеров.

Попадание в рейтинг Mashable «Топ-20 лучших стартапов» означает международное признание эффективности стратегии выбора и продвижения стартапов фонда «Сколково». Исполнительный директор IT-кластера «Сколково» Игорь Богачев комментирует: «Попадание в данный рейтинг наших стартапов наглядно иллюстрирует результаты наших усилий, которые напрямую вытекают из стратегии IT-кластера и деятельности «Сколково» в целом. Наша задача — выбрать те стартапы, которые обладают наилучшим потенциалом продаж своих продуктов на глобальном рынке, — и сделать эти стартапы максимально заметными на рынке. Не удивительно, что наши усилия в этом направлении оправдались: лучшие стартапы получили высокую оценку Mashable. Ведь мы умеем выбирать лучшие компании. Быть участником «Сколково» — это знак качества».

В России стремительно развиваются собственные модели и стандарты в области информационных технологий в отличие от предыдущих лет, когда страна была вынуждена копировать модели западных компаний. Сочетание традиционно сильной российской образовательной базы, новых стандартов и инициативы молодых амбициозных компаний в стране создает благоприятные условия для разработки уникальных проектов. Фонд «Сколково» собирает под своей крышей талантливых предпринимателей, чтобы помочь претворить в жизнь самые смелые и передовые идеи в России и во всем мире. География стартапов — вся страна: от Москвы и Санкт-Петербурга до Новосибирска.

Проекты, попавшие в топ-20 Mashable — Vizerra, Artolink, Penxy, Choister, Kuznech, Oktogo, Zingaya, Ostrovok и Ecwid. Они представляют яркий пример стартапов, которые уже определяют не только настоящее, но и будущее российской экономики в самых разнообразных отраслях: онлайн-сервисы для создания Интернет-бизнеса, «умные» поисковые системы, проектирование и визуализация.

Проект Vizerra — это уникальная 3D-технология, разработанная компанией 3 DreamTeam. Она предназначена для архитекторов, инженеров и дизайнеров и помогает им свободно передвигаться внутри пространства 3D-модели, летать или ходить, менять времена суток и года, осматривать объекты в различных режимах, взаимодействовать с различными объектами внутри модели, получать о них справочную информацию, и многое другое. Vizerra создает виртуальные модели техники для многих промышленных, сырьевых и инфраструктурных компаний, включая ОАО «Газпромавтоматика» и ОАО «КАМОВ». А для издательства National Geographic Vizerra обеспечивает визуализацию памятников истории и архитектуры, входящих в список Всемирного наследия ЮНЕСКО.

Другой интересный проект представлен рязанской компанией ЗАО «Мостком», которая разрабатывает и поставляет оборудование беспроводной оптической связи на основе Free Space Optics (FSO) технологии, а также тестеры каналов Ethernet под торговой маркой Artolink.

Сервис для проведения и записи живых презентаций Penxy при помощи мобильных приложений для смартфонов также получил высокую оценку Mashable и попал в топ-20 лучших стартапов. Среди других функций Penxy возможности презентации доклада, параллельной записи в облаке и онлайн транслирования.

Проект Choister представляет собой платформу для агрегации, структурирования и обогащения данных с обновлениями в режиме реального времени. Особенность «умного» поисковика Choister.ru заключается в том, что он выдает информацию не в виде стандартных ссылок на интернет-ресурсы, а в виде таблиц, карт, графиков и диаграмм. Данный проект имеет особую ценность для образовательной сферы и исследовательской и аналитической деятельности.

Технология визуального поиска в сети Интернет Kuznech представлена санкт-петербургским стартапом. Данный проект помогает обычным пользователям легко и быстро ориентироваться в огромном количестве изображений в Интернете, суммарный объем которых на сегодня составляет порядка 0,3% от их общего объема. Например, оборот компании в прошлом году составил 700 тыс. долл.

Также среди попавших в рейтинг — российские сервисы онлайн-бронирования отелей Oktogo (Санкт-Петербург) и Ostrovok (Москва); интернет-сервис Zingaya (Москва и Силиконовая долина), предлагающий компаниям новый способ общения с посетителями сайта — прямо с сайта компании; и виджет для создания интернет-магазинов в вебе и социальных сетях Ecwid (Ульяновск).

Компания ОАО "РНТ" приняла участие в автопробеге "Западная Европа — Западный Китай"

Компания ОАО "Русские Навигационные Технологии" (РНТ) стала техническим партнером автопробега "Западная Европа — Западный Китай", который стартует 27 августа 2013 года в городе Брест (Республика Беларусь). К старту автопробега будет приурочено проведение в Бресте международной конференции по проблемам экологической безопасности автомобильных дорог, конференция пройдет 26 августа, непосредственно перед стартом. Финиш состоится 7сентября 2013 г. в городе Хоргос.

В целях обеспечения возможности онлайн-мониторинга за участвующими в автопробеге автомобилями, а также повышения безопасности их перемещения на протяжении всего маршрута, организаторами данного мероприятия, — Межправительственным советом дорожников, — было принято решение обратиться за технической поддержкой в компанию ОАО "Русские Навигационные Технологии", которая с радостью примет участие в данном мероприятии в качестве технического партнера.

Компания ОАО "РНТ" оснастила два флагманских автомобиля автопробега системой ГЛОНАСС/GPS мониторинга и контроля транспорта "АвтоТрекер", а также "тревожными кнопками", позволяющими водителю подать сигнал в диспетчерский пункт в случае аварии, при возникновении нештатной ситуации или чрезвычайных обстоятельств на дороге. Это позволит непрерывно контролировать соблюдение графика движения, скоростной режим, возможные отклонения от маршрута, обеспечит безопасность участников пробега на протяжении всего пути. Любой желающий может наблюдать за ходом автопробега, в режиме реального времени видеть точное местонахождение участников, отслеживать пройденный путь, а также получать дополнительную информацию о ходе пробега на специально созданном web-сайте.

Умное управление умным городом на Форуме “Открытые инновации”

С 31 сентября по 2 ноября 2013 г. в МВЦ "Крокус Экспо" пройдет II Московский международный форум инновационного развития "Открытые инновации". В рамках программы Правительство Москвы представит трек "Умный город" с участием ведущих российских и иностранных экспертов.

Панельные дискуссии состоятся с участием Правительства Москвы, руководителя Департамента науки, промышленной политики и предпринимательства Москвы Алексея Комиссарова, Заместителя Мэра Москвы в Правительстве Москвы, руководителя Департамента транспорта и развития дорожно-транспортной инфраструктуры Москвы Максима Ликсутова, Министра Правительства Москвы, руководителя Департамента информационных технологий Артема Ермолаева.

"Smart city management — умное управление городскими инновациями", "Мобильный город или как "откупорить" пробку?", "Цифровые технологии создания "умного города" — панельные дискуссии, которые пройдут в рамках трека "Умный город".

Центр инновационного развития при поддержке Департамента науки, промышленной политики и предпринимательства Москвы запустит базу данных инновационной продукции и услуг для Москвы, своего рода виртуальный "банк" решений, куда инноваторы могут присылать свои предложения по различным отраслевым направлениям. Город испытывает серьезную потребность в комплексных решениях, которые в идеале можно интегрировать в уже сложившуюся городскую среду с целью ее улучшения. Многие наши ноу-хау ничуть не хуже американских или японских, надо просто готовить к ним отечественный спрос. Ведущие международные эксперты и представители администраций различных городов обсудили новые подходы в управлении городами, инструменты отбора городских инноваций, а также изменения, которые необходимо вносить в систему закупок инновационной продукции для стимулирования развития мегаполисов.

В последние годы сетевые технологии стали драйвером развития и трансформации городской инфраструктуры. Изменение городской среды и исполь-зование в управлении городом цифровых технологий обсудили участники панельной дискуссии "Цифровые технологии создания "умного города".

Отдельная экспозиция на Выставке Open Innovations Expo будет носить название "Комплексный проект Smart City". В 5-ти тематических зонах города будет представлено более 30 решений для городской среды: технологии портфельных компаний и стартапов четырех институтов развития: РОСНАНО, Сколково, РВК и Фонда содействия.

Свои разработки представят Департамент образования Москвы, компании РТИ (Россия), SAP (Германия), Huawei (Китай), а также девять финских компаний.

Norton Report 2013

Корпорация Symantec представила результаты отчета Norton Report 2013, которые указывают на то, что хотя число жертв кибератак среди взрослого населения в мире снизилось, средний ущерб из расчета на одного потерпевшего увеличился на 50%. Потери на каждого потерпевшего в соответствии с Norton Cybercrime Report за 2012 г. составляли в среднем 197 долл., в то время, как потери на каждого потерпевшего в соответствии с Norton Report за 2013 г. составили в среднем 287 долл.

Сегодня киберпреступники используют все более изощренные методы атаки, такие как ransomware (программавымогатель) и spear-phishing (направленный фишинг), и средний ущерб от отдельно взятой атаки как никогда высок. Результаты исследования Norton Report указывают на то, что 49% пользователей используют свои персональные мобильные устройства одновременно и для игры, и для работы, что приводит к появлению совершенно новых угроз безопасности для компаний, поскольку теперь киберпреступники могут получать доступ к еще более ценной информации.

Несмотря на то, что для почти половины всех пользователей смартфонов их устройства настолько важны, что они с ними спят, пользователи не обеспечивают этим устройствам надлежащего уровня защиты. 48% пользователей смартфонов и планшетов даже не предпринимают таких базовых мер предосторожности, таких как установка пароля, установка антивирусного ПО и создание резервных копий хранящихся на мобильном устройстве файлов. Такая беспечность ставит и их самих, и их личные данные под угрозу.

"Если бы это было испытанием, пользователи мобильных устройств его бы провалили. И хотя пользователи предпринимают меры по защите своих персональных компьютеров, у них отсутствует понимание необходимости защищать свои смартфоны и планшеты. Это как иметь дома надежную систему сигнализации и при этом оставлять свою машину незапертой и с открытыми окнами", — отметила Мариан Мерритт , адвокат отдела интернет-безопасности Symantec.

Другие интересные находки по России:

• 85% россиян сталкивались с киберпреступлениями;

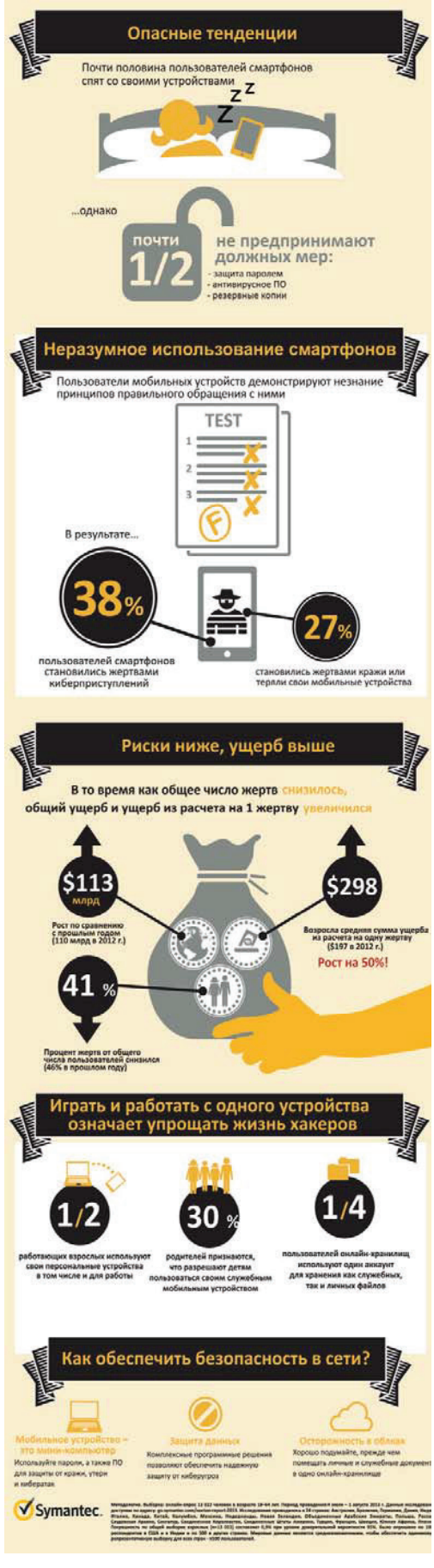
• 59% пользователей смартфонов сталкивались с мобильными киберпреступлениями в последний год;

• 56% пользователей мобильных устройств в России не знают о существовании решений для безопасности для них;

• 56% работающих пользователей старше 18 лет используют свое личное мобильное устройство и для развлечения, и для работы;

• 60% пользователей старше 18 лет используют публичные или незащищенные сети Wi-Fi.

Отчет Norton Report (ранее известный как Norton Cybercrime Report) — это одно из крупнейших в мире исследований киберпреступности в потребительском сегменте. В период между 4 июля и 8 августа 2013 г. компания Edelman Berland провела онлайн-опрос 13022 человек в возрасте от 18 до 64 лет из 24 стран (Австралия, Бразилия, Германия, Дания, Индия, Италия, Канада, Китай, Колумбия, Мексика, Нидерланды, Новая Зеландия, Объединенные Арабские Эмираты, Польша, Россия, Саудовская Аравия, Сингапур, Соединенное Коро-левство, Соединенные Штаты Америки, Турция, Франция, Швеция, Южная Африка, Япония). Погрешность по общей выборке взрослых составляет 0,9% при уровне доверительной вероятности 95%. Было опрошено по 1000 респондентов в США и в Индии и по 500 в других странах.



Cisco и МГУУ Правительства Москвы подписали соглашение о сотрудничестве в области развития и внедрения ИКТ

В сентябре 2013 г. ректор Московского городского университета управления Правительства Москвы (МГУУ Правительства Москвы) Андрей Марголин (и вице-президент компании Cisco по связям с государственными учреждениями Майкл Тиммени подпишут соглашение о сотрудничестве. Документ призван укрепить и расширить стратегическое партнерство между МГУУ Правительства Москвы и компанией Cisco в области развития и внедрения информационных и коммуникационных технологий. Правительство Москвы как учредителя университета на церемонии подписания соглашения представит и.о. начальника Управления государственной службы и кадров Правительства Москвы В. Фивейский.

Двустороннее партнерство предполагает поддержку ИТ-отрасли и ИТ-образования в Москве. С целью изучения опыта и проектов Cisco, направленных на развитие информационного общества, создание эффективной экономики, системы государственного управления и бизнеса, будет организована рабочая группа. Она займется разработкой рекомендаций, соответствующих планам Правительства Москвы по развитию информатизации и подготовке кадров для государственной гражданской и муниципальной служб, а также для подведомственных организаций в таких областях, как электронное правительство, образование и здравоохранение.

С целью поддержки ИТ-образования в Москве будут рассмотрены вопросы модернизации информационной и телекоммуникационной инфраструктуры МГУУ Правительства Москвы и разработаны совместные проекты, направленные на развитие и широкое применение современных информационных технологий и участие зарубежных и отечественных образовательных учреждений-партнеров МГУУ Правительства Москвы в совместных образовательных программах.

Подписание соглашения между Cisco и МГУУ Правительства Москвы станет очередным шагом в плодотворном сотрудничестве двух организаций.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИЗМЕРЕНИЙ И РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ ПАРАМЕТРОВ УСИЛИТЕЛЯ НИЗКОЙ ЧАСТОТЫ

Ходжаев И.А., *к.т.н, доцент,*
Академия ФСО России,
timofej@orel.ru

Соловьев А.М.,
Академия ФСО России,
solowjevam@mail.ru

Ключевые слова:
математическая модель, моделирование, контроль, усилитель, коэффициент усиления.

АННОТАЦИЯ

Предмет исследования: метод оценки качества функционирования усилителей низкой частоты. Объект исследования: усилитель низкой частоты в аппаратуре каналообразования. Целью исследования является повышение качества функционирования усилителей низкой частоты путем постоянного контроля его параметров подключенным измерительным прибором. При непрерывном контроле измерительный прибор в известной степени становится «элементом» усилителя, обладает шунтирующим воздействием, поэтому важно выработать рекомендации на параметры входных цепей, чтобы исключить такое влияние. В качестве математической модели использовано выражение для коэффициента усиления по напряжению усилителя низкой частоты, которое выступает в качестве обобщенного параметра при контроле параметров аналоговых электронных устройств, основанного на сравнении текущих измеренных показателей с эталонными значениями.

Разработка математической модели усилителя низкой частоты с учетом подключенного измерительного прибора проведена в три этапа. На первом этапе по принципиальной схеме усилителя низкой частоты составлена эквивалентная схема усилительного каскада, содержащая сопротивление базы, дифференциальные сопротивления коллектора, эмиттера и источник тока коллектора. На втором этапе выполнен расчет выходного сопротивления усилителя низкой частоты как параллельное подключение сопротивления нагрузки и сопротивления измерительного прибора. На третьем этапе определены коэффициенты усиления отдельных каскадов и усилителя в целом с учетом того, что входное сопротивление последующего (n+1) каскада является сопротивлением нагрузки предыдущего n-го каскада, а выходное сопротивление n-го каскада является сопротивлением источника сигнала для последующего (n+1) каскада.

На основе разработанной математической модели получены результаты моделирования процесса оценки качества функционирования усилителя низкой частоты с учетом влияния параметров применяемой измерительной аппаратуры. На практике полученные результаты позволяют задать требования на параметры прибора с целью минимизировать инструментальную погрешность, а, значит, повысить точность измерения основных показателей качества функционирования усилителя, а также других критически важных исследуемых объектов.

Практическая значимость статьи заключается в оценке влияния на коэффициент усиления многокаскадного усилителя полного сопротивления измерительного прибора.

В настоящее время усилители являются одним из основных узлов различной аппаратуры в устройствах автоматики, вычислительной и телекоммуникационной техники [1, 5]. Рассмотрим процесс моделирования работы усилителя низкой частоты (УНЧ), который находит широкое применение в каналообразующей аппаратуре.

Под математической моделью УНЧ понимают функцию, отражающую аналитически зависимость основного показателя качества функционирования (например, коэффициента усиления) от конечного числа влияющих факторов (от схемы включения усилительного эле-мента, от параметров входных и выходных цепей УНЧ и др.). Оценивание качества функционирования производится с использованием средств измерений, при этом появляется допол-нительный фактор, обусловленный шунтирующем воздействием измерительных приборов, и поэтому влияющий на качество функционирования исследуемого усилителя. При непрерывном контроле измерительный прибор в известной степени становится «элементом» усилителя.

В [3] представлена условная классификация существующих математических моделей усилителей, среди которых математическое выражение для коэффициента усиления по напряжению:

$$K_U = \frac{U_{\text{н}}}{U_{\text{вх}}}, \qquad (1)$$

где $U_{\text{н}}$ – напряжение на нагрузке УНЧ; $U_{\text{вх}}$ – напряжение на входе УНЧ играет важную роль для, так называемого, структурного контроля [4].

Рассмотренные в [3] математические модели, учитывающие разные режимы работы усилителей, не являются полностью адекватными, так как отражают процесс проверки в идеальных условиях, без учета влияния параметров подключенного измерительного прибора. Кроме того, отсутствие в известных математических моделях учета подключенного измерительного прибора на результаты измерений характеристик на входе и выходе объекта контроля снижает достоверность контроля параметров усилителя.

Это делает актуальным создание комплексной математической модели, учитывающей наличие измерительного прибора в структуре усилителя (рис.1), позволяющей минимизиро-вать его влияние на результаты измерений и повысить достоверность контроля качества усилителей.

При расчетах многокаскадных усилителей (рис. 2, а). каждый транзистор заменяют эквивалентной схемой, содержащей сопротивление базы дифференциальные сопротивления коллектора $r_{\text{б}}$ и эмиттера $r_{\text{э}}$ и источник тока коллектора $I_{\text{к}} = h_{21}\, I_{\text{б}}$ (рис. 2, б).

Для упрощения формул принимают типовые допущения: пренебрегают объемным сопротивлением базы ($r_{\text{б}} \to 0$) и сопротивлением коллектора ($r_{\text{к}} \to \infty$), принимают коэффициент усиления тока базы $h_{21} >> 1$ и вычисляют сопротивление эмиттера $r_{\text{э}} \approx \varphi_{\text{т}} / I_{\text{э}}$ по температурному потенциалу $\varphi_{\text{т}} \approx 25$ мВ и току эмиттера $I_{\text{э}}$.

Также при расчетах многокаскадных усилителей проще использовать структурное представление усилителя в виде последовательно соединенных «черных ящиков» (рис. 3), что позволяет избежать ошибок и в целом наглядно представить весь процесс расчета.

В такой структуре входное сопротивление $R_{\text{вх}}$ последующего $(n+1)$ каскада является сопротивлением нагрузки $R_{\text{н}}$ предыдущего n-го каскада, а выходное сопротивление n-го каскада является сопротивлением источника сигнала $R_{\text{г}}$ для последующего $(n+1)$ каскада:

$$R_{\text{вх}(n+1)} = R_{\text{н}(n)};\ R_{\text{вых}(n)} = R_{\text{н}(n+1)}. \qquad (2)$$

Применительно к условиям эксплуатации необходимо знать значения входного сопротивления первого каскада усилителя и выходного сопротивления его последнего каскада.

Для расчета входного сопротивления первого каскада на транзисторе с общим эмиттером (рис. 2) следует учесть и сопротивление делителя $R_{Д} = R_1 \cdot R_2 /(R_1 + R_2)$:

$$R_{\text{вх.1}} = \frac{R_1 R_2 \cdot (1 + h_{21}) \cdot (R_3 + r_{\text{э1}})}{(1 + h_{21}) \cdot (R_3 + r_{\text{э1}}) + R_1 + R_2} \quad . \qquad (3)$$

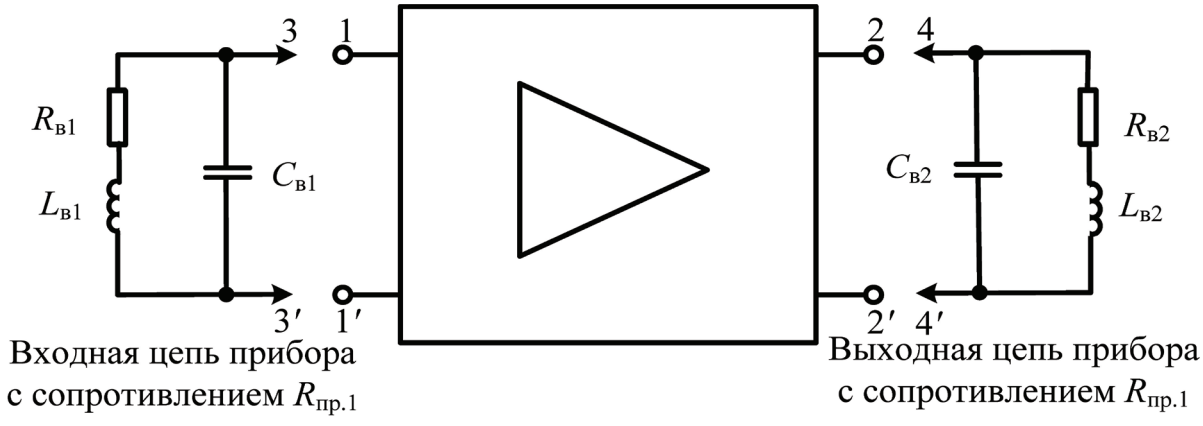


Рисунок 1 – Подключение измерительного прибора к усилителю
прибора оценки качества

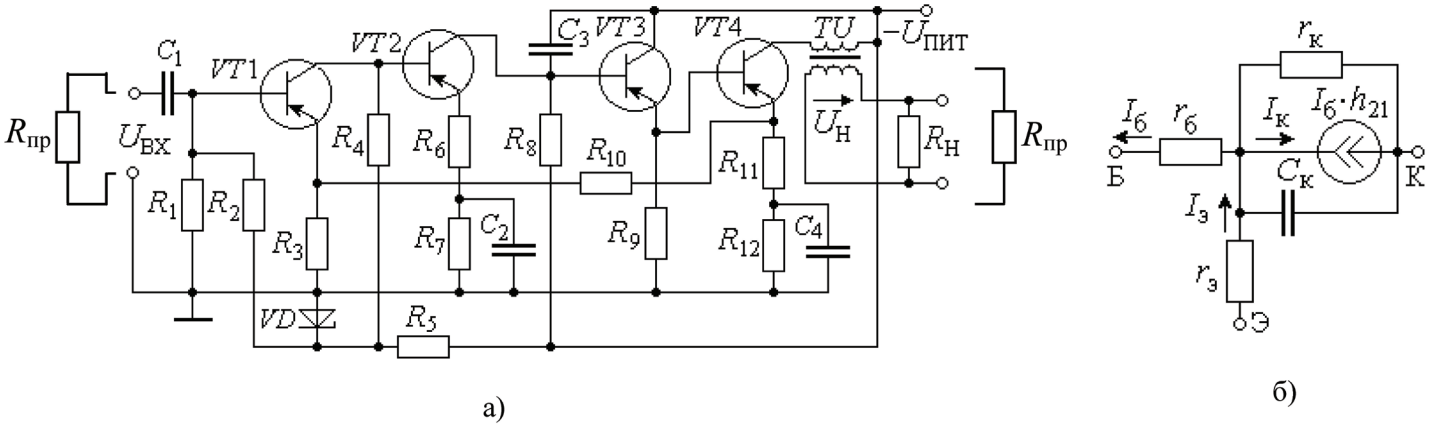


Рисунок 2 – Схема исследуемого усилителя низкой частоты:
а – принципиальная схема усилителя; б – эквивалентная схема транзистора

Выходное сопротивление последнего каскада усилителя $R_{вых}$ устанавливают с учетом коэффициента трансформации $n_T < 1$ выходного трансформатора, служащего для согласования с сопротивлением нагрузки усилителя, составляющим в данном случае $R_н$ = 600 Ом:

$$R_{вых.4} = R_н / n_T^2 . \quad (4)$$

Коэффициент усиления многокаскадного усилителя определяется произведением коэффициентов усиления последовательно включенных каскадов по выражению:

$$K_U = K_{U1} \cdot K_{U2} \cdot K_{U3} \cdot K_{U4} / (1 + \gamma K), \quad (5)$$

где $(1 + \gamma K)$ – глубина общей отрицательной обратной связи усилителя.

Коэффициент усиления усилителя с учетом обратной связи определяется выражением:

$$K_U = \frac{K_{U1} K_{U2} K_{U3} K_{U4}}{1 + r_{э1} R_3 / \left(r_{э1} R_3 + r_{э1} R_{10} + R_3 R_{10}\right)}, \quad (6)$$

где коэффициенты усиления отдельных каскадов можно определить, начиная от последнего каскада к первому, по формулам:

$$K_{U4} = R_н / n_T^2 \left(R_{11} + r_{э4}\right); \quad (7)$$

$$K_{U3} = \frac{R_9 \cdot h_{21} \left(R_{11} + r_{э4}\right)}{r_{э4} \cdot \left[R_9 + h_{21} \left(R_{11} + r_{э4}\right)\right] + R_9 \cdot h_{21} \left(R_{11} + r_{э4}\right)} = \frac{R_9 \cdot R_{вх.4}}{r_{э4} \cdot \left(R_9 + R_{вх.4}\right) + R_9 \cdot R_{вх.4}} \approx 1 ; \quad (8)$$

$$K_{U2} = -\frac{R_8 \cdot R_{вх.3}}{\left(R_8 + R_{вх.3}\right) \cdot \left(r_{э2} + R_6\right)} = -\frac{R_8 \cdot h_{21} \cdot \left[r_{э3} \cdot \left(R_9 + R_{вх.4}\right) + R_9 \cdot R_{вх.4}\right]}{\left(R_9 + R_{вх.4}\right) \cdot \left(r_{э2} + R_6\right)}; \quad (9)$$

$$K_{U1} = -\frac{R_4 \cdot R_{вх.2}}{\left(R_4 + R_{вх.2}\right) \cdot \left(r_{э1} + R_3\right)} = -\frac{R_4 \cdot h_{21} \left(r_{э2} + R_6\right)}{\left[R_4 + h_{21} \left(r_{э2} + R_6\right)\right] \cdot \left(r_{э1} + R_3\right)} . \quad (10)$$

Согласно выражениям (6) – (10), коэффициент усиления зависит от дифференциального сопротивления эмиттера $r_{э1}$ транзистора $VT1$, которое зависит от температурного потенциала $\varphi_т$ и изменяется примерно на 3 % при изменении температуры эксплуатации на $\Delta T = 10^oC$.

Для повышения стабильности коэффициента усиления в диапазоне рабочей температуры нужно изменить структуру усилителя, т. е. разделить на две части сопротивление R_3 в первом каскаде и уменьшить вдвое сопротивление R_{10} в цепи обратной связи (рис. 4).

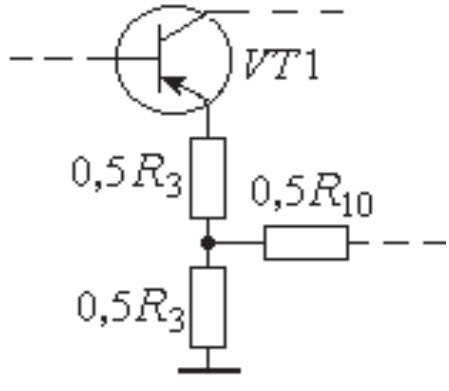


Рисунок 4 – Изменение схемы первого каскада

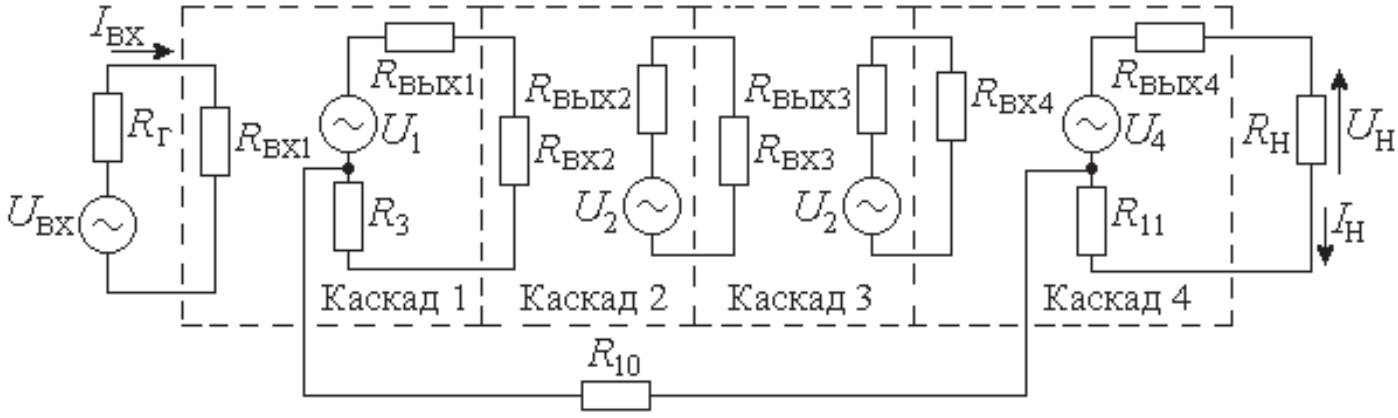


Рисунок 3 – Структурная схема усилителя переменного тока

При такой сравнительно небольшой модернизации схемы коэффициент усиления определяется выражением

$$K_U = \frac{K_{U1}K_{U2}K_{U3}K_{U4}}{1+R_3(r_{э1}+0{,}5R_3)/(r_{э1}R_3+r_{э1}R_{10}+R_3R_{10}+0{,}5R_3\cdot R_3)}. \quad (11)$$

Согласно формуле (11), температурная стабильность коэффициента усиления повышается в $(1+0{,}5\ R_3/r_{э1})$ раз по сравнению с исходной схемой усилителя (рис. 2). Таким образом, применение математической модели позволяет обеспечить улучшение основных параметров усилителя посредством изменения его структуры.

Математическая модель усилителя при подключении измерительного прибора позволяет оценить влияние параметров прибора контроля на его коэффициент усиления. Для оценки влияния измерительного прибора на коэффициент усиления вследствие достаточно большого емкостного сопротивления по сравнению с активным сопротивлением $(1/(w\cdot C_{В2}) >> R_{В2})$ и возможностью пренебречь индуктивностью проводов, представим цепи прибора контроля, подключаемые на выход усилителя в виде активного сопротивления $R_{В2}$.

Входные сопротивления измерительного прибора приводят к изменению коэффициента усиления напряжения из-за изменения сопротивления нагрузки усилителя до сопротивления Z_2, определяемого параллельным подключением сопротивления $R_Н$ и сопротивления измерительного прибора $R_{В2}$:

$$Z_2 = \frac{R_Н \cdot R_{В2}}{R_Н + R_{В2}}. \quad (12)$$

После подстановки (12) вместо $R_Н$ в выражении (7), получим:

$$K_{U4} = R_Н \Big/ n_т^2(R_{11}+r_{э4}) = \frac{R_Н \cdot R_{В2}}{R_Н + R_{В2}} \Big/ n_т^2(R_{11}+r_{э4}). \quad (13)$$

Тогда с учетом (7), (8), (9), (10) (11) и (13) получим математическую модель коэффи-циента усиления, который рассчитываться в приборе контроля:

$$K_U = -\frac{\frac{R_4\cdot h_{21}(r_{э2}+R_6)}{\left[R_4+h_{21}(r_{э2}+R_6)\right]\cdot(r_{э1}+R_3)}\cdot\frac{R_8\cdot h_{21}\cdot\left[r_{э3}\cdot(R_9+R_{вх.4})+R_9\cdot R_{вх.4}\right]}{(R_9+R_{вх.4})\cdot(r_{э2}+R_6)}\cdot\frac{R_9\cdot R_{вх.4}}{r_{э4}\cdot(R_9+R_{вх.4})+R_9\cdot R_{вх.4}}}{1+R_3(r_{э1}+0{,}5R_3)/(r_{э1}R_3+r_{э1}R_{10}+R_3R_{10}+0{,}5R_3\cdot R_3)}\cdot$$
$$\frac{R_н\cdot R_{в2}}{R_н+R_{в2}} / n_т^2(R_{11}+r_{э4}) \quad (14)$$

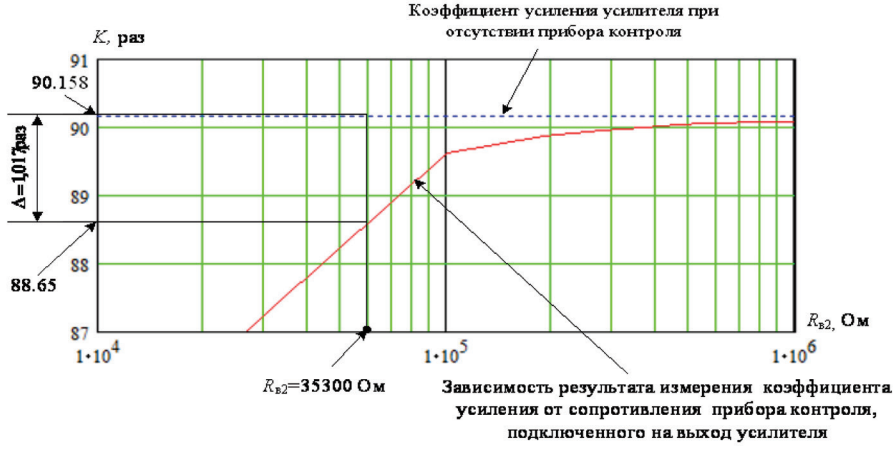


Рисунок 3 – График зависимости коэффициента усиления по напря-жению от сопротивления входных цепей рибора контроля, подклю-ченного на выход усилителя

Анализ выражения (14) показывает, что на результаты измерений коэффициента усиления по напряжению усилителя могут оказывать влияние значения параметров, характеризующие построение схемы измерительного прибора. Учет входного сопротивления измерительного прибора ($R_{в2}$) позволяет повысить точность контроля коэффициента усиления по напряжению и практически исключить влияние измерительного прибора на погрешность оценки качества исследуемого усилителя.

Результаты моделирования в среде *Matchad* по выражению (14) представлены в виде графической зависимости коэффициента усиления от входного сопротивления прибора контроля (рис. 5).

Анализ графика показывает, что выполняя условия на значения сопротивления цепей измерительного прибора можно минимизировать и даже исключить их влияние на результаты измерений контролируемого параметра усилителя.

Так, сравнивая разность коэффициента усиления усилителя при отсутствии измерительного прибора и коэффициента усиления с подключенным измерительным прибором с допустимой величиной погрешности измерения электрических величин – $\Delta = 0{,}15$ дБ (или 1.017 раз) [1] видно, что допустимые значения сопротивлений входных цепей измерительного прибора $R_{в2}$ при подключении на выход усилителя должны быть более 35300 Ом.

Таким образом, предлагаемая математическая модель измерений коэффициента усиления (14), учитывающая влияние измерительного прибора может быть выбрана в качестве базовой модели усилителя при проведении измерительного контроля. Заданием требований на параметры прибора контроля можно минимизировать инструментальную погрешность, а, значит, повысить точность измерения основных показателей качества функционирования усилителя, а также других критически важных исследуемых объектов.

Литература

1. ГОСТ 23849-87 (действующий). Изм. №2 от 21.10.1993. Аппаратура Радиоэлектронная бытовая. Методы измерения электрических параметров усилителей сигналов звуко-вой частоты.
2. Миловзоров О.В. Электроника: Учебник для вузов. - М.: Высш. школа, 2008. – 288 с.: ил.
3. Петров М.Н. Моделирование компонентов и элементов интегральных схем. - СПб.: Издательство «Лань», 2011. – 464 с.: ил.
4. Соловьев А. М. О математической модели структурного контроля аппаратуры каналообразования // Информационные системы и технологии управления, 2012. – № 5 (73). – С. 35-42.
5. Травин Г.А. Основы схемотехники устройств радиосвязи, радиовещания и телевидения: Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2009. – 592 с.

MATHEMATICAL MODEL OF MEASUREMENT AND SIMULATION RESULTS PARAMETERS BASS AMPLIFIER

Khodzhaev I., Ph.D, assistant professor Academy FSO Russia, timofej@orel.ru

Soloviev A.,
Academy FSO Russia, solowjevam@mail.ru

Abstract
Subject of research: method of assessing the quality of functioning amp low- quency. Object of study: low-frequency amplifier in equipment kanaloobra - education. The purpose of research is to improve the functioning of low-frequency amplifiers by continuously monitoring its parameters connected meter ethyl device. When continuous monitoring meter to a certain extent becomes a "member" of the amplifier, the shunt has influence, but so important to make recommendations on the parameters of the input circuits to eliminate the influence of such. As a mathematical model used for the expression of the gain voltage low frequency amplifier, which acts as a parameter of a generalized under the control parameters of analog electronic devices based on a comparison of the first indicators of the current measured with the reference values.
Development of mathematical model low-frequency amplifier based on the connected measuring device held in three stages. In the first stage -tion of fundamental low-frequency amplifi-er circuit composed of the equivalent circuit of the amplifier cascade containing the base resistance, the differential resistance of the collector, the emitter and collector current source. In the second phase have been calculated output impedance low-frequency amplifier as a parallel connection of the load resistance and resistance measuring device. In the third step the coefficients of the individ-ual stages and the gain of the amplifier as a whole, considering that the input impedance of the sub-sequent (n+1) stage is the load impedance of the previous n-th stage and the output impedance of the n-th stage is the source impedance for the subsequent (n+1) stage. On the basis of the developed mathematical model obtained simulation results validate qual-ity of functioning low-frequency amplifier with the influence of the parameters used instrumenta-tion. In practice, the results obtained allow to specify requirements on the parameters of the device to minimize the instrumental error, and thus improve the accuracy of measurements of key quality indicators of functioning of the amplifier, as well as other critical of the investigated objects.
The practical significance of the article is to assess the impact of the gain multistage amplifier impedance measuring device.

Keywords: mathematical model , modeling, control, power, gain coefficient.

References

1. GOST 23849 1993, 'Radioelectronic equipment, household. Methods for measuring electri-cal parameters of signal amplifiers the sonic frequency'.
2. Milovzorov, OV 2008, 'Electronics: Textbook for Universities', Vysshaya School, Moscow, p. 288.
3. Petrov, MN 2011,'Gudkov Simulation of components and integrated circuits', Publish-er 'Lan', St. Petersburg, pp. 464.
4.Soloviev, MA 2012 'Mathematical model of structural control equipment kanaloobra-zovaniya' Information Systems and Technology Management, vol. 112, no. 5 (73), pp. 35-42.
5. Travin, GA 2009, 'Basics circuitry wireless devices, radio broadcasting and television', Hotline Telecom, Moscow, p. 592.

ВУС

Военно-учетный стол

Программный комплекс

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

Воинский учет в организациях:

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

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

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

• Генерация документов по бронированию.

Первичный воинский учет в органах местного самоуправления:

• Ведение Картотеки организаций зарегистрированных на территории ОМСУ;

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

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

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

Учет и Бронирование в Межведомственных комиссиях:

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

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

• Анализ обеспеченности трудовыми ресурсами;

• Ведение перечня должностей и профессий по бронированию граждан;

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

• Заполнение, передача, сбор и обобщение форм ГД.

НПЦ ИРС

Научно-производственный центр
Информационных региональных систем

npcirs.ru

ЧТО ИДЕТ НА СМЕНУ ЭПОХЕ МОБИЛЬНЫХ ТЕЛЕФОНОВ?

Фрайди Б.,
компания Cisco Systems

Ключевые слова:
всеобъемлющий Интернет, Internet of Everything (IoE), мобильная связь, беспроводные технологии.

Сорок лет назад, в апреле 1973 года, был сделан первый звонок на переносной мобильный телефон. Мартин Купер (Martin Cooper) из коммуникационного подразделения компании Motorola позвонил своему конкуренту из Bell Labs, открыв тем самым новую эпоху. Для этого он воспользовался прототипом мобильного телефона размером с кирпич, весившим около килограмма и стоившим почти 4 тысячи долларов.

Размышления о первом мобильном телефоне помогают понять, на какой уровень могут подняться мобильные коммуникации в будущем. Всего за четыре десятилетия сотовые телефоны перестали быть неуклюжими аппаратами для толстосумов, превратившись в неотъемлемый атрибут повседневной жизни.

Сегодня люди всех возрастов пользуются мобильными телефонами и другими мобильными устройствами для личных и деловых коммуникаций, прослушивания музыки и просмотра видеоматериалов, для работы в социальных сетях, приобретения товаров и услуг, оплаты счетов, банковских операций, поиска оптимальных маршрутов и многого другого. Но и это еще не все. По мере развития мобильных устройств люди ожидают от них все более высокого уровня персонализации услуг. Они хотят, чтобы услуги работали на их условиях и поддерживали высокий уровень информационной безопасности.

Сами по себе устройства не могут удовлетворить растущие ожидания абонентов. Чтобы выйти на новый уровень мобильности, необходимо обеспечить тесное взаимодействие между мобильными устройствами и сетями, развернутыми в помещениях. Такое взаимодействие должно постоянно совершенствоваться и становиться все более интеллектуальным, чтобы поспевать за миниатюризацией и интеллектуализацией подключенных устройств.

Между тем на наших глазах рождается Всеобъемлющий Интернет, который подключит друг к другу людей, процессы, данные и неодушевленные предметы и обеспечит взаимодействие между ними. В результате Интернет станет такой же жизненной необходимостью, как электричество и вода. Интеллектуальная же сеть сделает соединения более ценными, персонализированными и актуальными.

Интеллектуальные сетевые функции не только покажут организациям список подключенных объектов, но и укажут тип и причину каждого подключения, а также дадут информацию о том, какие совместные действия были предприняты с помощью этих подключений. Интеллектуальные функции обеспечат безопасную доставку нужной информации нужному адресату или устройству в нужный момент. В условиях экспоненциального роста объема данных сетевая информация должна помогать мобильным пользователям получать нужные и полезные данные нажатием одной-двух кнопок на мобильном устройстве. В результате возможности пользователей должны намного превзойти то, что нам доступно сегодня.

К примеру, получив данные о местоположении пользователя и его деятельности в сети в реальном времени, розничный торговец может изучить ситуацию в торговом зале с точностью до минуты и использовать этот контекст (знание местоположения мобильных пользователей) для активации локальных сервисов и предоставления покупателям полезной, нужной им информации (если, конечно, они выразили готовность получать ее в безопасном режиме). Таким образом, покупатели получат своевременные персонализированные услуги, а продавцы освоят новые способы изучения покупателей, взаимодействия с ними и повышения прибыли.

Нет ни малейшего сомнения в том, что завтра сетевые устройства станут еще более компактными, дешевыми, гибкими и специализированными. Но главным условием реализации потенциала мобильных технологий была и остается сеть.

Дополнительную информацию журналистам рад предоставить Александр Палладин, глава пресс-службы ООО "Сиско Системс"
тел. (985) 226-3950

НЕВАЛАБ

ПРОЕКТИРОВАНИЕ СТРОИТЕЛЬСТВО ОСНАЩЕНИЕ

лабораторий
для научно-исследовательских
и промышленных предприятий

ОСНАЩЕНИЕ ЛАБОРАТОРИЙ «ПОД КЛЮЧ»

- Комплектация лабораторий оборудованием и расходными материалами для комплексного решения аналитических задач

ПРОЕКТИРОВАНИЕ ЛАБОРАТОРИЙ

- С соблюдением СНиП, СН, СанПиН, ГОСТ
- В соответствии с нормативными требованиями на методы испытаний продукции

СТРОИТЕЛЬСТВО МОДУЛЬНЫХ ЛАБОРАТОРНЫХ КОМПЛЕКСОВ

- Строительство
- Шеф-монтаж и авторский надзор

ПУСКО-НАЛАДОЧНЫЕ РАБОТЫ И ОБУЧЕНИЕ

- Установка и запуск оборудования
- Обучение методикам работы

ПОДГОТОВКА ЛАБОРАТОРИЙ К АККРЕДИТАЦИИ

- Подготовка комплекта документов
- Сопровождение, методическая и информационная поддержка

ПОСТАВКА ОБОРУДОВАНИЯ, МЕБЕЛИ И РАСХОДНЫХ МАТЕРИАЛОВ

- Аналитическое, лабораторное и метрологическое оборудование
- Лабораторная и специализированная мебель
- Расходные материалы и стандартные образцы

СЕРВИСНОЕ И РЕМОНТНО-ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

- Техническая поддержка
- Ремонт и обслуживание оборудования

КРУПНЫЕ ПРОЕКТЫ

НЕФТЯНАЯ КОМПАНИЯ РОСНЕФТЬ · TRANSNEFT ТРАНСНЕФТЬ · ГАЗПРОМ · РОСАТОМ · ИНТЕР РАО ЕЭС · НОВАТЭК

nevalab.ru

БОЛЕЕ 10 ЛЕТ НА РЫНКЕ!

г. СПб, Московское шоссе, дом 46, литер «Б»
тел: +7(812)336-3200; +7(812) 327-0152
факс: +7(812)336-3223, info@nevalab.ru

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОРГАНИЗАЦИИ И ПЛАНИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СРЕДЫ СИЛ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Будко П.А., *д.т.н., профессор,*
Военная академия связи
имени С.М. Буденного,
budko62@mail.ru
Чихачев А.В., *к.т.н., доцент,*
Военная академия связи
имени С.М. Буденного,
anton_best@mail333.com
Баринов М.А., *к.т.н.,*
Военная академия связи
имени С.М. Буденного,
barinovy.spb@yandex.ru
Виноградeнко А.М., *к.т.н.,*
Военная академия связи
имени С.М. Буденного,
vinogradenkoao@rambler.ru

Ключевые слова:
телекоммуникационная сеть, сеть передачи данных, связность, пропускная способность, каналы связи.

АННОТАЦИЯ

В статье рассматриваются общие принципы формирования телекоммуникационной компоненты единого информационно-управляющего пространства сил специального назначения с целью преодоления проблем создания сильносвязной свободно масштабируемой структуры единого алгоритмического пространства распределенных вычислений. При этом широкополосная связность пространства должна доходить до мобильного высокоскоростного объекта в условиях воздействия агрессивной внешней среды в различных физических средах. Авторами к принципам внутрисетевой организации и распределенного управления телекоммуникационной сети отнесены следующие: телекоммуникационная сеть должна иметь максимальную при заданных ограничениях информационную емкость; максимальную при вводимых ограничениях связность; быть изотропной; обеспечивать минимальные потери целевой информации, которая должна обладать минимальной избыточностью; использовать минимальный объем буферной памяти, достаточный для оптимального согласования параметров трафика с параметрами каналов связи; быть гибкой и реагировать достаточно быстро на изменение состояния её элементов и внешней среды. Соблюдение данных принципов позволяет рассматривать результаты решения сетевых оптимизационных задач в виде закономерностей для сетей заданных структур. Причем сети связи и обмена данными в системном аспекте рассматриваются с общих позиций, независимо от применяемых технологий.

Введение

В современных условиях, характеризующихся многовариантностью угроз и задач, решаемых силами специального назначения, а также высокой динамичностью изменения обстановки, для принятия и реализации своевременных эффективных решений и обеспечения согласованности действий требуется пересмотр принципов и подходов построения и применения телекоммуникационной компоненты системы управления. Комплексность современных угроз затрудняет решение проблем старыми методами. В этой связи все более актуальным и приоритетным направлением реформирования сил специального назначения становится всесторонняя интеграция боевых формирований и повышение уровня их взаимодействия на основе создаваемого единого информационно-управляющего пространства звеньев управления [1] за счет реализации сетеориентированного подхода и интеграции систем управления и связи, средств поражения, разведки и обеспечения.

В настоящее время все больше ученых и специалистов склоняются к тому, что преимущества принципов сетецентрического управления (СЦУ) проявляются как в наступательном, так и в оборонительном отношении за счет существенного повышения эффективности применения каждой системы на основе объединения и использования всех сил и средств, участвующих в противоборстве. Здесь и проявляется эффект синергизма, когда целое представляет нечто большее, чем сумма его частей, когда (в случае сетецентрической организации противника) мы боремся не с отдельным подразделением (единицей техники, средством поражения), а с системой, которая в силу своей глобальности приобретает новый уровень живучести.

Последние вооруженные конфликты XXI века показали техническую реализуемость этих подходов по сравнению с устоявшимися стратегиями [2]. А поиск методов противодействия им сводится к тезису, что сетевое противоборство можно выиграть только сетевыми средствами, адаптировав к собственным условиям и целям эффективные и стремительно развивающиеся технологии. При этом повышение возможностей сторон осуществляется не только за счет улучшения маневренных и других характеристик вооружения, а в первую очередь за счет информационной связности всех компонент системы. Именно без наличия глобальных коммуникационных связей между географически распределенными мобильными, но объединенными в единую сеть силами нельзя реализовать максимальный потенциал средств поражения за счет новых возможностей систем разведки, управления и обеспечения.

Цель статьи – сформулировать основные принципы организации сильносвязной телекоммуникационной среды сил специального назначения.

Проблемы создания сильносвязного пространства

Важно отметить, что убедительное понимание нового подхода к ведению противоборства в едином информационном пространстве только формируется. Отдельные фрагменты представляют разрозненность видения проблем, как в направлении электроники, так и в других направлениях, в том числе в управлении, топологиях и телекоммуникациях. А поскольку ключевым системообразующим элементом СЦУ являются средства связи и компьютерные сети, обеспечивающие поддержание функционально интегрированного поля посредством построения надежной работы мобильных беспроводных сетей, то необходим прорыв и в этом направлении.

Однако на сегодня имеется ряд проблемных вопросов в направлении телекоммуникаций, которые «лежат на поверхности» при реализации принципов СЦУ. Это, прежде всего, реализация сильносвязного пространства с многочисленными взаимоувязанными средствами сете- и каналообразования, то есть необходима широкополосная высокоскоростная транспортная основа (транспортная сеть) автоматизированных систем связи сил специального назначения, не только выстроенная по принципам их вертикальных иерархий, но и с сильно развитыми горизонтальными связями (прежде всего межвидовыми), что позволит осуществить как вертикальную так и горизонтальную интеграцию всех компонентов объединенных сил группировки. При этом широкополосная связность пространства должна доходить до мобильного высокоскоростного объекта в условиях воздействия агрессивной внешней среды в различных физических средах: атмосфера, космос, вода. Основными требованиями при формировании такой «горизонтальной» интеграции являются: обеспечение необходимой пропускной способности каналов передачи данных; организация взаимодействия на любом уровне управления и др. А главным принципом такой структуры становится обеспечение постоянной связи между любыми двумя потребителями в любое время и в любом месте.

Мировые тренды развития телекоммуникаций таковы, что уже к 2016 г. до 70% общемирового мобильного трафика составит видеотрафик, средняя скорость мобильных соединений с 2013 по 2017 гг. вырастет примерно в 7 раз, фактически, скорость и пропускная способность с точки зрения связи должна быть обеспечена по схеме «каждый с каждым» [3]. А для реализации принципов СЦУ необходимо стремиться к техническому обеспечению этих цифр уже сейчас. И ясно, что без наличия в связях взаимодействия достаточного количества каналов с широкополосным доступом, доходящих до подразделений, обеспечение сильносвязного пространства СЦУ затруднительно. Так в таблице 1 представлен вклад родов связи в управление войсками в ходе реализации современных войсковых операций ВС США.

Получение сегодня таких высоких показателей по надежным и широкополосным связям вплоть до подразделений для сил специального назначения весьма затруднительно, поскольку их техническое переоснащение пока еще не завершено. Даже эти, пока еще не достижимые для нас цифры не решают проблему острой нехватки пропускной способности каналов передачи данных. И её вряд ли удастся решить в ближайшее время [4].

Таблица 1

Вклад родов связи в управление
(по объему передаваемой информации)

Рода связи	Процентное соотношение предоставляемых каналов
Спутниковая связь	Более 50-60%
Радиорелейная связь	До 18-22%
Тропосферная связь	До 12%
КВ-, УКВ-радиосвязь	До 5-6%

По оценкам бюджетного управления конгресса и американского высшего командования, потребности ВС в пропускной способности каналов связи в 20 раз превышают существующие возможности. Так, управление информационных систем МО США констатирует, что во время операции в Ираке собственными средствами МО осуществляло передачу только 20 % информации, а остальные 80 % передавались через коммерческие системы спутниковой связи [4]. Без решения данной проблемы трудно говорить об осуществлении так называемой горизонтальной интеграции. Более того, потребности в пропускной способности в дальнейшем будут только возрастать.

Кроме того, наращивание горизонтальной связности требует пересмотра общих принципов организации связи в сторону существенного повышения роли связи взаимодействия, связи обеспечения боевых действий и связи оповещения (прежде всего межвидовых), наряду со связями боевого управления. Обмен разведывательной и оперативно-командной информацией в сетях управления должны обеспечить системы связи и обмена данными, строящиеся на сетевых принципах, но не как видовые, а как межвидовые открытые системы, позволяющие наращивать количество потребителей, независимо от их ведомственной принадлежности, места дислокации и выполняемых задач, в пределах своей максимальной производительности.

Скорости и нагрузки это далеко не все самые «узкие» места в современных сетях связи. Проблемы возникают в управлении этими распределенными многоуровневыми технически сложными системами. При этом современные инфокоммуникационные технологии работают на фундаменте, заложенном полвека назад. И уже более 10 лет в основе инфокоммуникационной отрасли (NGN) лежат компьютерные сети. Сегодня пропускная способность каналов связи приближается к насыщению не только в силу отставания в создании новых каналов, сколько из-за существующих методов и средств управления трафиком на сети, из-за «конечности» скорости света (как мы не считали её «бесконечной», но пределы в электронике достигнуты), а также из-за того, что архитектура современных сетей не соответствует постоянно растущим требованиям. И потому основным направлением совершенствования системы управления силами специального назначения ведущих стран мира является создание интегрированных систем управления сетевой архитектуры, обеспечивающих реализацию единой информационно-управляющей структуры и единого информационного пространства всех участников боевых действий. Конфигурировать современные сети вручную практически невозможно, и, значит, пришло время для изменений в управлении архитектурой сетей и вычислений в ней.

Сетевая структура системы связи и системы обмена данными должна представлять собой необходимое количество узлов связи с автоматизированными коммутационными центрами и блоками управления на ЭВМ, объединенных релейными, кабельными, космическими и другими линиями связи. Соответственно, и результатом конструирования является система, а не совершенствование отдельных средств с улучшенными по отношению к антисредству характеристиками. А, следовательно, и подходить к созданию СЦУ надо как к качественно совершенно новой системе, предназначенной не столько для борьбы с отдельными средствами или их группой, а как к системе, предназначенной для разрушения всей системы нападения. Только объединив в единую систему все разнородные и разновидовые объекты сил (средства разведки, средства поражения, системы управления и связи), на основе комплексирования их возможностей можно достичь главной цели – системоразрушения противоположной стороны.

Это далеко не полный перечень проблем и особенностей, которые необходимо учесть специалистам и промышленности для формирования принципов создании и обеспечения нормального функционирования телекоммуникационной среды сил специального назначения. В общем виде сетецентрическая модель представляет систему, состоящую из трех подсистем, имеющих структуру решетки: информационной, сенсорной и боевой [1]. При этом основой системы считается первая подсистема (сети связи и обмена данными), на которую накладываются вторая и третья. И действительно, как было показано выше, практическая реализация принципов СЦУ невозможна без эффективного решения вопросов создания такой ключевой компоненты как сверхнадежного сильносвязного коммуникационного пространства, обеспечивающего эффективное функционирование на его основе компьютерных сетей сил специального назначения. Опуская в статье вопросы формирования второй и третьей подсистем сетецентрической модели, остановимся подробнее на основных принципах организации и планирования телекоммуникационной компоненты.

Принципы формирования сильносвязной телекоммуникационной среды

Анализ показывает, что проблемы интеграции и конвергенции различных видов связи, включая информационный, системный и сетевой аспекты, в течение последних лет остаются самыми актуальными в области телекоммуникаций. Трудность решения указанных проблем связана с двумя особенностями телекоммуникационных систем как информационно технических систем с коллективно используемыми ресурсами: географической рассредоточенностью сетевых ресурсов, источников и получателей информации, а также пульсирующим характером трафика.

Первая особенность определяет высокую стоимость сетевых ресурсов и выдвигает требование их эффективного использования. Кроме того, в распределенной системе конкурирующие за ресурсы требования не могут самоорганизовываться в согласованную очередь без дополнительных затрат на координацию и управление. Потому система управления должна обеспечивать коллективный доступ к ресурсам сети в режиме разделения времени, при котором ресурсы предоставляются большому числу пользователей, каждый из которых предъявляет относительно небольшие требования, но которые определяют общий профиль нагрузки (трафика), обеспечивая равномерное и эффективное их использование в силу «сглаживающего эффекта» больших популяций (закона больших чисел). Таким образом, вторая особенность привела к необходимости применения метода коммутации с промежуточным накоплением (пакетная коммутация).

Отсюда вытекает общая задача проектирования телекоммуникационной среды – достижение эффективного коллективного использования ресурсов множества несовместимых устройств географически распределенной системы, в которой запросы на доступ к ресурсам возникают от асинхронных процессов в существенно неравные промежутки времени [5]. Из общей задачи вытекает третья особенность телекоммуникаци-

онных систем – разнородность оборудования и применяемых сетевых технологий. Однако проблема совместимости различных устройств, преодолевается в рамках семиуровневой эталонной модели взаимодействия открытых систем и регламентируется протоколами на всех уровнях её организации. Исходя из вышеизложенного и на основе исследований [5], сформулируем основные принципы организации и планирования телекоммуникационной сети в системном аспекте.

1. Телекоммуникационная сеть должна иметь максимальную при заданных ограничениях информационную емкость.

Модель сети может быть представлена взвешенным графом G, который состоит из упорядоченного множества узлов z и соединяющих их линий (дуг) hij, причем оба конца линии соединены с двумя узлами i и j, где $i,j=\overline{1,k}$, k – общее число узлов графа G. Каждому узлу и линии ставятся в соответствие некоторые числа (веса), например, mi – число элементов буферной памяти, V_{ij}, и F_{ij} – пропускная способность линии связи и соответствующий поток в данной линии. Каждая линия может иметь некоторое число каналов n_{ij} в каждом направлении. Тогда в соответствии с формулой Литтла, справедливость которой в широком спектре применений доказана многочисленными экспериментами [6], можно записать:

$$\gamma T_{\text{зад}} = \sum_{ij}^{l} N_{ij}\ , \qquad (1)$$

где γ – общий трафик в сети; $T_{\text{зад}}$ – среднее время задержки пакетов в сети; l – общее число линий графа G; N_{ij} – число сообщений на входе в каждый канал (линию связи). Уравнение (1) справедливо при условии, что

$$W = \gamma T_{\text{зад}} = \text{const}, \qquad (2)$$

т. е. определяет стационарный (установившийся) режим работы сети, когда число сообщений (пакетов), поступающих в сеть равно числу сообщений, покидающих её. При этом входной трафик равен выходному и справедливо

$$\gamma_{\text{вх}} T_{\text{зад}} = \gamma_{\text{вых}} T_{\text{зад}}. \qquad (3)$$

Если условие (3) не выполняется, например, $\gamma_{\text{вх}} T_{\text{зад}} > \gamma_{\text{вых}} T_{\text{зад}}$, информация накапливается в сети, приводя её в состояние блокировки. Если $\gamma_{\text{вх}} T_{\text{зад}} < \gamma_{\text{вых}} T_{\text{зад}}$, то каналы связи используются неэффективно.

Правая часть уравнения (1) фактически и определяет информационную емкость W сети

$$W = \sum_{ij}^{l} N_{ij}, \qquad (4)$$

поскольку равна сумме всех сообщений, пребывающих в очереди и передаваемых в канал в любой момент времени. В выражении (4) вид функции

$$N_{ij} = f(\lambda_{ij}, \mu_{ij}, m_{ij}, n_{ij}) \qquad (5)$$

определяется из анализа системы массового обслуживания, с помощью которой моделируются входы в каждый канал в узлах коммутации [6]. Здесь λ_{ij} – интенсивность потока заявок; μ_{ij} – интенсивность их обслуживания.

Тогда отношение

$$\chi = \frac{\lambda_{ij}}{n_{ij}\mu_{ij}} = \frac{L\lambda_{ij}}{L\mu_{ij}n_{ij}} = \frac{F_{ij}}{V_{ij}n_{ij}}, \quad i,j = \overline{1,k}$$

называемое коэффициентом загрузки канала, справедливо при фиксированной длине пакета L, так что в дальнейшем выражение (5) запишем в виде

$$N = f(\chi_{ij}, n_{ij}, m_{ij})\ . \qquad (6)$$

Формула (1) является по существу единственным средством, позволяющим на сетевом уровне эталонной модели взаимодействия открытых систем решать такие сетевые задачи, как оптимизация пропускных способностей и распределение потоков в сети. Как следует из (2), рост входного трафика приводит к необходимости пропорционального снижения среднего времени задержки. Это может быть достигнуто за счет снижения загрузки каналов, что эквивалентно увеличению пропускных способностей этих каналов. При пульсирующем трафике сеть, рассчитанная на средние значения, таким образом, должна иметь максимальную информационную емкость, чтобы удовлетворять типовым значениям трафика. В качестве ограничения в этом случае выступает стоимость сети, которая определяется стоимостью каналов связи и задается одной из наиболее распространенных форм функций стоимости:

$$C = k\sum_{ij}^{l} V_{ij}\ . \qquad (7)$$

2. Телекоммуникационная сеть должна иметь максимальную при введенных ограничениях связность.

Поскольку связность графа определяется числом цепей, соединяющих два узла и не имеющих других общих узлов, то в сильносвязном пространстве всегда существует соединяющая цепь для любой пары узлов (схема «каждый с каждым»). Сильная связность повышает устойчивость системы, которая определяется надежностью и живучестью телекоммуникационной сети.

Задача топологического проектирования сети сводится к нахождению рациональной топологической структуры (оптимальности не добиться), удовлетворяющей различным ограничениям при наименьших затратах. Эта задача относится к теории потоков, примечательной особенностью которой является принципиальная невозможность решения большинства её постановок, поскольку при этом не применимы методы комбинаторики и перебора вариантов из-за их многочисленности и колоссального числа вариантов топологических структур K_0 при заданном числе узлов коммутации k:

$$K_0 = \sum_{l=0}^{l_n} C_{l_n}^{l} = \sum_{l=0}^{l_n} \frac{l_n!}{l!(l_n - l)!}\ ,$$

где $l_n = \dfrac{k(k-1)}{2}$ – число ветвей полносвязной сети.

Полносвязная структура, описанная выше, является единственной, которую можно построить при заданном числе узлов коммутации в телекоммуникационной сети и которую можно анализировать аналитическими методами, например, методами

линейного программирования при выборе алгоритмов маршрутизации и решении задач распределения потоков в сети. Существующее в литературе мнение, что полносвязная сеть имеет высокую стоимость, опровергается выражением (7). Заданную стоимость можно поддерживать на постоянном уровне за счет снижения пропускной способности каналов при одновременном увеличении числа линий связи до полносвязности. Это оправдано тем, что полносвязная структура исключает возможность переполнения буферов узлов коммутации транзитными потоками трафика.

Высокая связность усиливает действие гипотезы Клейнрока о независимости, оправдывая применение моделей телекоммуникационной сети в виде системы массового обслуживания $M/M/n$ (с пуассоновским характером трафика и экспоненциальным распределением времени обслуживания), когда в каждом узле сходятся потоки с 3–5 независимых направлений [7].

Однако применение полносвязных структур вряд ли может быть оправдано при использовании широкополосных линий связи (например, волоконно-оптических или космических). В этом случае наиболее приемлем подход с поиском процедур, обладающих вычислительной эффективностью [7], которому удовлетворяют графы, имеющие определенную регулярность, т. е. графы, узлы которых равноправны в смысле топологии. Задача синтеза таких графов может быть решена аналитически для любого числа узлов графа при связности, не ниже заданной. Регулярные графы одинаковой связности имеют ограниченный набор структур, отличающихся порядком следования путевых потоков относительно выделенных корреспондирующих узлов.

3. Телекоммуникационная сеть должна быть изотропной.

Этот принцип предполагает, что загрузка каналов должна быть по возможности равномерной и не зависеть от направления передачи информации:

$$\chi = \frac{\lambda_{ij}}{n_{ij}\mu_{ij}} = \frac{F_{ij}}{V_{ij}n_{ij}} = \text{const}$$

Что не только упрощает решение оптимизационных задач, но и согласуется с интуитивными представлениями о причинах возникновения перегрузок. В данном случае входные потоки F_{ij} определяются априорно заданной матрицей тяготения $|\lambda_{ij}|$ между узлами коммутации.

Пропускные способности V_{ij} каналов при этом должны иметь определенное превышение над потоком для исключения блокировок ($\chi \leq 1$) и согласовываться с условием (7).

4. Телекоммуникационная сеть должна обеспечивать минимальные потери целевой информации, которая должна обладать минимальной избыточностью.

Этот принцип основывается на том, что телекоммуникационная сеть представляет собой распределенную динамическую систему с ограниченными ресурсами. А при использовании пульсирующего трафика высокое качество обслуживания пользователей обеспечить крайне сложно.

Данный принцип ориентирован на технологии, использующие в качестве транспортной магистрали среды, имеющие малый уровень помех (например, волокно, космические каналы связи), при которых оказывается возможным избежать необходимости регенерации и повторных передач, т. е. не хранить копии и не посылать подтверждений (например, ATM). В целях обеспечения временной прозрачности сети функции и объем заголовков ячейки ATM значительно ограничены. Основной функцией заголовка является идентификация виртуального соединения и обеспечение гарантии правильной маршрутизации при мультиплексировании разных виртуальных соединений в одном цифровом тракте. Это дает возможность совершенствования алгоритмов кодирования и сжатия информации с целью уменьшения требуемой полосы пропускания.

5. Телекоммуникационная сеть должна использовать минимальный объем буферной памяти, достаточный для оптимального согласования параметров трафика с параметрами каналов связи.

Неконтролируемое использование накопителей для сглаживания трафика приводит к неограниченному росту очередей. Возникает ситуация, когда время задержки резко возрастает и величина этой задержки становится зависимой от загрузки сети. Это приводит к нарушению масштаба времени, что делает невозможным передачу трафика реального времени (аудио, видео). Аналогичная ситуация возникает при недостатке буферов, когда при неконтролируемой нагрузке коммутатор попросту отбрасывает пакеты, которые не в состоянии обработать, что делает невозможным передачу трафика данных, чувствительного к потере пакетов. Попытки компенсировать потери за счет повторных передач приводят к увеличению общего трафика и росту задержек, что делает также невозможным передачу аудио- и видеоинформации. Минимизация потерь полосы пропускания при передаче полезной информации, связанной с адресацией, приводит к дополнительным задержкам.

Предложена методика оценки объемов буферной памяти, ориентированная на технологии, использующие в качестве среды передачи широкополосные системы. Эти объемы необходимы только для сглаживания трафика с целью оптимального согласования с параметрами сети и осуществления, в случае необходимости, обменных процессов. В этом случае предполагается точная дозировка объема буферов вблизи области оптимального решения [8].

6. Телекоммуникационная сеть должна быть гибкой и быстро реагировать на изменение состояния её элементов и внешней среды.

Гибкость сети обеспечивается за счет того, что любой источник может генерировать информацию с той скоростью, которая ему необходима. Это дает возможность быстро реагировать на появление новых служб с еще неизвестными характеристиками. Все виды информации должны транспонироваться единым способом, что дает возможность их оптимального распределения путем статистического мультиплексирования и, следовательно, обеспечивать высокую эффективность использования сетевых ресурсов.

Так как все виды информации транспортируются одним методом, то это дает возможность организации, планирования, проектирования и ввода в эксплуатацию, а в дальнейшем – контроля, управления и технического обслуживания одной сети, что сокращает общие затраты на ее содержание. Такой сетью может быть широкополосная цифровая сеть с развитой системой управления, реагирующей как на изменения текущего состояния сети, так и на динамические изменения потоков за пределами номинальных значений.

Заключение

Сформулированные общие принципы организации и планирования сильносвязной телекоммуникационной среды сил специального назначения в системном аспекте рассматривают сети связи и обмена данными с общих позиций, независимо от применяемых технологий. Их соблюдение позволяет рассматривать результаты решения сетевых оптимизационных задач в виде закономерностей для сетей заданных структур. Использование регулярных структур в сочетании с принципом изотропности позволяет получить аналитическое решение большинства задач оптимизации сетевых ресурсов, что облегчает интерпретацию результатов решения. Точное дозирование объема буферной памяти узлов коммутации вблизи области оптимального решения позволяет осуществить сглаживание трафика с целью согласования его статистических характеристик с параметрами сети и при необходимости, реализацию обменных процессов с соблюдением требований поддержания постоянства основных качественных показателей. Использование данных принципов требует глубокого анализа свойств потока данных, т. к. при разделении общей среды передачи возникают коллизии, оказывающие воздействие на временные интервалы между пакетами, увеличивающиеся с ростом загрузки каналов, особенно при использовании технологий с встроенными функциями контроля качества виртуального соединения с помощью стратегий буферизации, резервирования и приоритезации. При этом применение шестого принципа позволяет предотвратить возможные блокировки и деградацию сети.

Литература

1. Чирков В.В. Единое информационно-управляющее пространство ВМФ – современная технология превосходства над противником в вооруженной борьбе на море. // Морская радиоэлектроника. №4(42), 2012. – С. 2-9.
2. Паршин С., Кожанов Ю. Концепции сетецентрического боевого управления ВС США, Великобритании и ОВС НАТО. Общее и различия. // Зарубежное военное обозрение. №4, 2010. – С. 7-10.
3. Голышко А.В. Информационное общество: Тренды и последствия. // Электросвязь. №4, 2013. – С. 4-9.
4. Баулин В., Кондратьев А. Реализация концепции «Сетецентрическая война» в ВМС США // Зарубежное военное обозрение. №6, 2009. – С. 61-67.
5. Будко П.А. Управление ресурсами информационно-телекоммуникационных систем. Методы оптимизации. – СПб.: ВАС, 2012, – 512 с.
6. Бертсекас Д., Галлагер Р. Сети передачи данных. – М.: Мир, 1989. – 544 с.
7. Клейнрок Л. Вычислительные сети с очередями.–М.: Мир, 1979. –600с.
8. Будко П.А. Динамическое управление ресурсами широкополосных цифровых сетей с использованием обменных процессов элементов сети // Электронное моделирование. №4, Т. 25, 2003. – С.113-118.

MAIN DIRECTIONS OF THE ORGANIZATION AND PLANNING OF THE TELECOMMUNICATION ENVIRONMENT OF FORCES OF A SPECIAL PURPOSE

Budko P., Doc.Tech.Sci., professor,
Military Academy of communication, budko62@mail.ru

Chikhachev A., Ph.D, docent,
Military Academy of communication, anton_best@mail333.com

Barinov M., Ph.D,
Military Academy of communication, barinovy.spb@yandex.ru

Vinogradenko A., Ph.D,
Military Academy of communication, vinogradenkoao@rambler.ru

Abstract
In article the general principles of formation telecommunication components of uniform management information space of forces of a special purpose for the purpose of overcoming of problems of creation of strongly connected freely scalable structure of uniform algorithmic space of the distributed calculations are considered. Thus broadband connectivity of space has to reach mobile high-speed object in the conditions of influence of aggressive environment in various physical environments. Authors to the principles of the intra network organization and the distributed management of a telecommunication network referred the following: the telecommunication network has to have maximum at the set restrictions information capacity; the maximum connectivity at entered restrictions; to be isotropic; to provide the minimum losses of target information which has to possess the minimum redundancy; to use the minimum volume of buffer memory, sufficient for optimum coordination of parameters of a traffic with parameters of communication channels; to be flexible and to react quickly enough to change of a condition of its elements and environment. Observance of these principles allows to consider results of the solution of network optimizing tasks in the form of regularities for networks of the set structures. And a communication network and data exchange in system aspect are considered from the general positions, irrespective of applied technologies.

Keywords: telecommunication network, data transmission network, connectivity, capacity, communication channels

References

1. Chirkov V.V. Single information and control space Navy – modem technology superiority over the enemy in the armed struggle of the sea // Marine electronics, 2012, № 4(42), pp. 2-9/
2. Parshin S., Kozhanov Yu. Concepts network-centic command and control VS U.S., UK and NATO. General and differences // Foreign Military Review, 2010, № 4, pp. 7-10.
3. Golyshko A.V. The information Society: Trends and implications // Electrosyaz, 2013, № 4, pp. 4-9.
4. Baulin V. Kondratiev A. Implementation of the concept of " network-ceniric warfare" in the U.S. Navy // Foreign Military Review, 2009, № 6, pp. 61-67.
5. Budko P.A. Resource management information technology systems. Optimization techniques. St.Petersburg: EAC, 2012, 512 p.
6. Bertsekas D., Gallager R. Data Networks. Moscow, 1989. 544 p.
7. Kleinrock L. Computer networks with queues. Moscow, 1979, 600 p.
8. Budko P.A. Dynamic resource management of broadband digital networks using the metabolic network elements // Electronic modeling, 2003, № 4. T.25, pp. 113-118.

ПОДХОД К ОЦЕНИВАНИЮ ЖИВУЧЕСТИ СЛОЖНЫХ ОРГАНИЗАЦИОННО – ТЕХНИЧЕСКИХ СИСТЕМ РАЗЛИЧНОГО НАЗНАЧЕНИЯ

Анисимов И.И.,
Военно-космическая академия имени А.Ф. Можайского, the_lexys@bk.ru.
Толмачёв А.А.,
Военно-космическая академия имени А.Ф. Можайского, the_lexys@bk.ru.
Чащин С.В.,
Военно-космическая академия имени А.Ф. Можайского, the_lexys@bk.ru.

Ключевые слова:
сложная организационно–техническая система, живучесть систем, метод, модель, методика.

АННОТАЦИЯ

В данной статье рассматриваются различные точки зрения на основные методических вопросов теории оценки живучести сложных организационно–технических систем различного назначения, изложена авторская точка зрения в вопросе общетехнического понимания живучести.

На основе проведенного анализа работ в области исследований живучести сложных организационно–технических систем различного назначения, в качестве примера рассмотрена методика использования логико-вероятностного подхода к оцениванию живучести элементов сложных систем.

Оценка живучести сложной организационно-технической системы с помощью построения логико-вероятностных моделей живучести рассматривает модели живучести сложной организационно-технической системы, как, состоящую из совокупности согласованных частных моделей различного назначения, использующих для описания протекающих в ней процессов как детерминированные, так и вероятностные методы. Живучие системы должны быть способны поддерживать непрерывное выполнение своих основных функций, временно или постоянно отказываясь от выполнения менее важных функций, изменять свою структуру и поведение, находить и выполнять новые функции, необходимые для успешного противостояния неблагоприятным воздействиям, приспосабливаясь к условиям своего функционирования. Механизмы обеспечения живучести, входящие в такие системы, являются их неотъемлемой частью.

Сложные организационно–технические системы независимо от их назначения, должны обладать способностью эффективно функционировать при получении повреждений (разрушений) или восстанавливать ее в течение заданного времени, то есть обладать свойством – живучести.

Для построения таких систем необходимо совершенствование методов и алгоритмов оценивания и обес-печения живучести. Учитывать и анализ различных типов воздействия. Применять новые архитектуры по-строения распределенных элементов сложных систем, устойчивых к внешним воздействиям.

В рамках проведенного анализа в области оценки и определения живучести сложных организационно–технических систем различного назначения, представленного в данной статье примера оценивания живучести с использованием логико–вероятностного подхода позволяют сделать вывод о, том, что существенную роль необходимо уделить созданию реализации разработанных в различных методиках–моделей живучести.

Введение

В последние годы наблюдается значительное повышение интереса к свойству живучести сложных систем, как в теоретическом, так и в практическом отношении. Обусловлено это в первую очередь возросшим масштабом и уровнем сложности систем, что приводит к увеличению возможности «отказов» системы. В случае отказа работы системы, процесс её восстановления представляет собой трудоемкий процесс, поэтому уменьшение возможности отказов системы является одной из основных задач, которые ставятся при проектировании сложных систем. Остается так же актуальной и проблема рационального и оптимального задействования сохранившихся в системе ресурсов направленных на выполнение жизненно важных функций системы после интенсивного воздействия на нее. Решение этой проблемы требует от системы новых качеств, которыми она может и не располагать, если спроектирована для работы только в нормальных условиях эксплуатации.

Учитывая вышеизложенные проблемы, к свойству живучести и его особенностям широко применяемым в создании сложных систем различного назначения, предъявляются ряд особенных требований, которые касаются как структурной, так и функциональной части сложных систем. Требования к структурной составляющей, сводятся к выявлению уязвимых мест в топологии системы и определению степени их влияния на целостность системы, требования к функциональной составляющей сводится к определению способности системы решать стоящие перед ней задачи при изменяющихся возможностях ее элементов.

На сегодняшний день точные определения и понятия в теории живучести не сформированы должным образом, об этом можно судить исходя из большого разнообразия предлага-емых показателей живучести, отсутствия моделей живучести которые применялись в практике длительное время, в то же время имеются различные методики, по вопросам оценки живучести для различных систем, оперирующие разной терминологией.

Понятие живучести в различных сферах деятельности

Для формулировки общетехнического понятия «живучесть», необходимо собрать воедино наиболее устоявшиеся определения данного свойства в различных областях техники.

В области самолетостроения [12] живучесть представляет собой способность летательного аппарата выполнять поставленную задачу в различных экстремальных условиях. Совершенствование расчетных методов оценки надежности, безопасности и живучести разрабатываемых самолетов приобретает важное значение, позволяет сократить сроки кон-структивно-технологической доводки нового самолета и значительно уменьшить объем дорогостоящих испытаний. Использование ЭВМ для хранения и выдачи информации по статистике летных происшествий, отказов и неисправностей позволяет наиболее полно учесть опыт промышленности. Имитационное моделирование с использованием как достаточно сложных, но зато и точных математических моделей, так и натурных функционирующих стендов, открывает новые перспективы для выявления недостатков конструкции нового самолета и более раннего их устранения.

В судостроении [7] живучесть судна определена, как способность противостоять воздействию стихийных сил ветра и волн, пожаров, оружия противника, а при повреждениях сохранять и восстанавливать полностью или частично мореходность и боевые качества. Важнейшие элементы живучести судна - непотопляемость и остойчивость. Живучесть судна обеспечивается рациональностью конструкции и оборудования судна, в том числе расположением непроницаемых переборок, люков, горловин, дверей, иллюминаторов, системами сигнализации, автоматическими защитными устройствами. Отметим, что в данном определении указаны условия, когда проявляется живучесть (стихийные силы ветра и волн, пожары, оружие), стадии развития процесса и степень тяжести неблагоприятных воздействий (противостоять возникновению повреждений, при повреждениях, сохранять мореходность и боевые качества, а при их потере восстанавливать их полностью или частично), способы обеспечения живучести (ограничение неблагоприятных последствий непроницаемые переборки и пр.), стойкость, (рациональная конструкция), оповещение и управление (системы сигнализации, защитные устройства).

Живучесть системы городского электротранспорта [11] определяется способностью не прерывать работу всей системы или значительного ее участка из-за планового ремонта, аварии, повреждения контактной сети и (или) рельсового пути. При возникающих затруднениях маршруты пускаются по обходным путям, укорачиваются за счет промежуточных разворотных колец или перенаправляются на запасную конечную станцию. Для троллейбусов также возможно применение систем автономного хода. В случаях, когда работа маршрута на участке невозможна в течение длительного времени (ремонт) – вводят временные маршруты электротранспорта и компенсирующие автобусные маршруты. В некоторых случаях, когда разветвленный участок соединен с основной линией (по мосту, например) – на этом участке стараются запроектировать собственное депо. При его отсутствии организуют временные площадки для ночной стоянки. В случаях с трамваями, когда на заблокированном на длительный период участке нет разворотного кольца, применяют челноки – вагоны, сцепленные хвостами.

В электроэнергетике [4] под живучестью понимается свойство объекта противостоять возмущениям, исключая возможность последовательного развития отказа с массовым нарушением питания. Основным требованием к системе в данном случае к системе является способность противостоять переводу ее элементов в нерабочее состояние из-за отказов, вызванных нарушением внешних условий функционирования.

В вычислительных системах [8] с живучестью связывается отсутствие потерь любой задачи (функции) из-за отказов элементов. Это свойство обеспечивается развитыми средствами технического диагностирования восстановления и реконфигурации.

Общетехнические определения живучести приведены в [1, 2, 3, 9, 13]. В [2] под живучестью понимается способность систем к сохранению своих основных функций (хотя бы с допустимой потерей качества их выполнения) при воздействии факторов внешней среды катастрофического характера - неблагоприятных условий эксплуатации. Это определение близ-

ко по содержанию к определению [9]. В [1] живучесть определена как свойство объекта, заключающееся в его способности выполнять заданное назначение в процессе неблагоприятных воздействий на весь объект или отдельные его компоненты, поддерживая в допустимых пределах свои эксплуатационные показатели. В этих определениях следует обратить внимание на следующее: Во-первых, живучесть следует рассматривать как внутреннее свойство системы, которым она обладает незави¬симо от возникающих в данный момент времени условий функционирования. Она обладает им всегда и в определенной мере может проявляться при нормальных условиях функционирования, когда возникают отказы элементов, вызванные производственными дефектами, старением, уходом параметров и пр. Но в полной мере живучесть проявляется при крупных внешних воздействиях, не предусмотренных условиями нормальной эксплуатации и поэтому трудно прогнозируемых, так как они создают в системе экстремальные условия функционирования. Во-вторых, живучесть проявляется в том, что система сохраняет не все функции, которые она должна выполнять при нормальной работе, а лишь основные функции, да и то с возможным понижением качества их выполнения. Это означает, что возможно изменение стратегии функционирования системы по мере увеличения тяжести неблагоприятных воздействий. В-третьих, система должна обладать свойством постепенной деградации по мере увеличения тяжести неблагоприятных последствий и для каждого уровня таких последствий уметь оперативно и максимально эффективно использовать сохранившиеся ресурсы для выполнения основных функций с учетом изменения стратегии функционирования (целевой функции), а в дальнейшем реализовать оптимальную стратегию восстановления с учетом возникающих ограничений.

В рамках данной трактовки следует понимать:

1) Живучесть - внутреннее свойство системы, которым она обладает при крупных внешних воздействиях, не предусмотренных условиями нормальной эксплуатации (в нерасчетных условиях).

2) Живучесть проявляется в том, что система сохраняет не все функции, которые она должна выполнять при нормальной работе, а лишь основные, с возможным понижением качества их выполнения. Это означает, что возможно изменение стратегии функционирования системы по мере ее деградации.

3) Система должна обладать свойством постепенной деградации по мере увеличения тяжести неблагоприятных воздействий и для каждого уровня последствий уметь оперативно и максимально эффективно использовать сохранившиеся ресурсы для выполнения основных функций с учетом изменения стратегии функционирования (целевой функции), а в дальнейшем реализовать оптимальную стратегию восстановления с учетом возникающих ограничений.

С учетом вышеизложенного можно дать общетехническое определение живучести, как свойство системы сохранять и восстанавливать способность к выполнению основных функций в заданном объеме и в течение заданного времени при изменении структуры системы и (или) алгоритмов и условий ее функционирования вследствие непредусмотренных регламентом нормальной работы воздействий.

Данное определение допускает учет последствий воздействий, влияющих на выполнение задания, а именно потери работоспособности элементов и (или) связей между ними вследствие их физического разрушения, изменения (ухудшения) технических характеристик (скорости, производительности, пропускной способности и пр.), нарушения алгоритмов функционирования, изменения внешних условий функционирования (резкое уменьшение или увеличение нагрузки).

Понятие живучесть с течением времени эволюционирует и приобретает новое содержание, что влечет за собой, не всегда своевременное закрепление данного понятия в нормативных документах.

Пути и методы оценивания живучести сложных организационно – технических систем различного назначения

Исследования, проведенные в работах [5, 6, 11], подробно рассматривают подходы к оценке и управлению свойством живучести сложных организационно – технических систем (СОТС), основанные на построении логико-вероятностных моделей живучести с использованием вероятностных и детерминированных показателей.

На пример, оценка живучести СОТС с помощью построения логико-вероятностных моделей живучести предполагает рассмотрение модели живучести СОТС, как, состоящую из совокупности согласованных частных моделей различного назначения, использующих для описания протекающих в ней процессов как детерминированные, так и вероятностные методы [14]. На основании предложенных в работе [14] подходов к оцениванию живучести СОТС, в качестве основного показателя живучести СОТС $P_{ж}$ может быть использован показатель оценивания живучести по результатам выполнения целевых задач, $P_{ж} = P(\{Z_i\}, Q, B)$ - вероятность выполнения текущего набора целевых (функциональных) задач $\{Z_i^*\}$ в условиях действия неблагоприятного внешнего воздействия (НВВ) – Q и окружающей среды – B.

Полагая, что в зависимости от интенсивности процессов выполнения задач, внешних условий функционирования и эффективности работы системы, обеспечения живучести системы в конечном счете перейдет в одно из возможных устойчивых состояний (или останется в прежнем): 1 - работоспособное, выполнение задач без ограничений (система обладает свойством живучести); 2 -работоспособное, выполнение задач с ограничениями (система обладает ограниченной живучестью); 3 - неработоспособное, возможно восстановление работоспособности (система временно не обладает живучестью); 4 - неработоспособное, восстановление сети нецелесообразно (система не обладает свойством живучести), можно, при определенных допущениях, считать:

$$P(\{Z_i\}, Q, B) = P\left(\bigcap_{j=1}^{m} E_j\right) = \prod_{j=1}^{m} P(E_j)$$

где E_j - событие, состоящее в связности j-й двухполюсной сети графа $G(A, B)$, отражающей j-ю функциональную подсистему (например, маршрут передачи информации в ТКС.) системе, m – количество анализируемых подсистем согласно технологии передачи информации в рамках выполнения целевых задач системы. Следовательно,

$$P_{ж} = \prod_{i} \prod_{j} P\left(E_j\right)$$

, при выполнении указанных ограничений.

Для вычисления $P(E_j)$ необходимо, прежде всего, формализовать архитектуру системы, для построения графа , и определить математические методы расчета элементов этой системы.

На рассматриваемом промежутке времени на элемент системы могут действовать как отдельные НВВ, так и их совокупность. В последнем случае первоначально оценивается вероятность сохранения работоспособности по каждому анализируемому фактору P_i, затем для суммы совместных событий находится интегральная вероятность сохранения элементом работоспособности:

$$P\left(E_j\right) = \sum_{\forall i \in I} P_i - \sum_{\forall i,j \in I \; i \neq j} \Pi \; P_i P_j + \ldots + \left(-1\right)^{I-1} \prod_{i=1}^{I} P_i$$

,

где I – количество действующих на элемент поражающих факторов. Вероятности P_i вычисляются относительно факторов обстановки и природы НВВ.

Подобная логика поведения элементов сложных систем позволяет использовать для описания и оценки живучести логико-вероятностные методы.

Так, для каждого элемента, способного находится в одном из четырех указанных состо-яний можно ввести следующие логические переменные: χ_i - индикатор работоспособности i-го элемента ($\chi_i = 1$ - элемент работоспособен (состояния 1 и 2); $\chi_i = 0$ - в противо-положном случае (состояния 3 и 4)) и y_i - индикатор состояния работоспособного состояния ($y_i = 1$ - элемент работает; $y_i = 0$ - работает с функциональными ограничениями эле-мент (восстанавливается); Z_{ij}=1 - индикатор j-го воздействия на i-й элемент (Z_{ij}=1 - воздействие j-го типа действует на i-й элемент; 0 - в противном случае), тогда Z_i=$V_j Z_{ij}$ - индикатор общего НВВ на i-й элемент. Таким образом, можно вывести индикаторы со-стояний элементов: $u_{i1} = 1[A_1] = x_i y_i \overline{Z}_i$; $u_{i2} = 1[A_2] = x_i \overline{y}_i \overline{Z}_i$; $u_{i3} = 1[A_3] = x_i Vy_i Z_i$, а также относительно состояния элементов составить логические уравнения вида: y_i=$f_y(x_k, y_e, Z_k; k=\overline{1,N}, l \in M_i), i = i = \overline{1,N}$, где N – число элементов в системе; M_i - множество элементов смежных с i-м элементом.

Совокупность данных уравнений образует замкнутую систему логических уравнений, решаемую известными методами (методом определителей, методом подстановки, матричным методом и т.д). При этом, решение системы логических уравнений надо проводить многократно: один раз для базовой структуры ТКС, когда все Z_{ij}=0 и еще столько же раз, сколько различных типов воздействий. В конечном счете, перебирая все типы воздействий, необходимо получить полный набор работоспособных структур ТКС, что в итоге позволит составить и преобразовать логическую функцию работоспособности $F = f(X, Y, Z)$ к ортогональной дизъюнктивной нормальной форме.

Помимо описано выше метода логико – вероятностного подхода к оценке живучести СОТС, в большинстве работ особое значение уделяется оценке живучести систем лишь с точки зрения структуры ее построения и позволяет достаточно достоверно определять ее показатели.

Разработано несколько методик [11], применимых для ассоциативных, ассоциативно-структурных и структурных систем, в которых учитывается их связность. Однако весомости действующих в системе функциональных взаимосвязей должного значения не придается.

В работе [6] этот недостаток устранен, но в ней не предусматривается оценка степени способности системы в целом функционировать после повреждающих воздействий на ее элементы.

Методика, предложенная в [5], направлена на оценку живучести систем с точки зрения ее функциональности с учетом иерархических взаимосвязей. Но в этой работе структурный аспект живучести представлен только одним видом взаимосвязей и к тому же без учета их значимости.

В работе [10], разработана методика оценки живучести сложных систем военного назначения, позволяющая получать комплексную оценку живучести системы с точки зрения ее структурной уязвимости и функциональности. Однако применяемый математический аппарат для моделирования распространения внешних воздействий по структуре системы, не полностью учитывает все возможные последствия нежелательных воздействий.

Таким образом, можно считать, что на настоящий момент в теории живучести СОТС не обозначен устоявшийся методологический подход, позволяющий решать задачу комплексной оценки живучести сложной системы с точки зрения ее структурной уязвимости и функциональности с учетом значимости существующих в системе взаимосвязей.

Наиболее полным, является рассмотренный пример с использование логико – вероятностного метода при оценке живучести СОТС.

Заключение

Живучие системы должны быть способны поддерживать непрерывное выполнение своих основных функций, временно или постоянно отказываясь от выполнения менее важных функций, изменять свою структуру и поведение, находить и выполнять новые функции, необходимые для успешного противостояния неблагоприятным воздействиям, приспосабливаясь к условиям своего функционирования. Механизмы обеспечения живучести, входящие в такие системы, являются их неотъемлемой частью.

СОТС независимо от их назначения, должны обладать способностью эффективно функционировать при получении повреждений (разрушений) или восстанавливать ее в течение заданного времени, то есть обладать свойством – живучести.

Для построения таких систем необходимо совершенствование методов и алгоритмов оценивания и обеспечения живучести. Учет и анализ различных типов воздействия. При-менение новых архитектур построения распределенных элементов сложных систем, устойчивых к внешним воздействиям.

В рамках проведенного анализа в области оценки и определения живучести СОТС различного назначения, представленного в данной статье примера оценивания живучести с использованием логико – вероятностного подхода позво-

ляют сделать вывод о, том, что существенную роль необходимо уделить созданию реализации разработанных в различных методиках – моделей живучести.

Литература

1. Волик Б.Г., Рябинин И.А., 1984, Эффективность, надежность и живучесть управляющих систем, 'Автоматика и телемеханика № 12', С.23-25.
2. Глушков В.М., 1979, Словарь по кибернетике, р.87.
3. Горшков В.В., 1982, Логико-вероятностный метод расчета живучести сложных систем, 'Кибернетика АН УОТ -№ 1', С.104-107.
4. Каган Б.М., Долкарт В.М., Каневский М.М., 1978, Управляющий вычислительный ком-плекс с автоматической реконфигурацией для ответственных АСУ ТП, 'Кибернетические проблемы АСУ ТП', Знание, 'МДНТП', С.3-11.
5. Казаков В.И., 1977, Основы теории топогеодезического обеспечения боевых действий войск, 'Раздел 1 ВИА', С.32-36.
6. Кочкаров А.А., Малинецкий Г.Г., 2005, Обеспечение стойкости сложных систем. Структурные аспекты, ИПМ имени М.В.Келдыша РАН, С.45-48.
7. Прохоров А.М., 1972, Большая советская энциклопедия, 'Том № 9', 569 с.
8. Руденко Б.Н., Ушаков ИН, 1986, Надежность систем энергетики, Наука, 252 с.
9. Рябинин И.А., 1964, Теоретические основы проектирования ЭЭС кораблей, ВМА, 240 с.
10. Сафонов Р.А., 2003, Методика оценки живучести сложных систем военного назначе-ния, 'УДК 519.876', С.1-3.
11. Стекольников Ю.И., 2002, Живучесть систем, 'Политехника', 69 с.
12. Томилов Ю.М., Меднов О.Н., Свищев Г.П., 1993, 'Боевая живучесть', Большая Рос-сийская энциклопедия, С.7-10.
13. Ушаков И.Н., 1985, Надежность, в технических системах. Справочник, 'Радио и связь', 606 с.
14. Черкесов Г.Н., Черкесов Г.Н., Можаев А.С., 1991, Логико-вероятностные методы расче-та надежности структурно-сложных систем , 'Качество и надежность изделий, № 3 (15), Знание, С.3-64.

THE APPROACH TO ESTIMATION OF SURVIVABILITY OF THE DIFFICULT ORGANIZA-TIONAL - TECHNICAL SYSTEMS OF DIFFERENT FUNCTION

Anisimov I.,
Military Space Academy, the_lexys@bk.ru.
Tolmachyov A.,
Military Space Academy, the_lexys@bk.ru.
Chashchin S.,
Military Space Academy, the_lexys@bk.ru.

Abstract
In given article the various points of view on the cores of methodical questions of the theory of an estimation of survivability of difficult organizational-technical systems of different function are considered, the point of view in a question the general technical understanding of survivability is stated avtor. On the basis of the spent analysis of works in the field of researches of survivability of difficult organizational - technical sys-tems of different function, as an example the technique of use of the logiko-likelihood approach to estimation of survivability of elements of difficult systems is considered. The estimation of survivability of difficult organizational-technical system by means of construction of logiko-likelihood models of survivability considers models of survivability of difficult organizational-technical system, as, consisting of set of the co-ordinated private models of different function using for the description of processes proceeding in it both determined, and like-lihood methods. Hardy systems should be capable to support continuous performance of the basic functions, temporarily or constantly refusing performance of less important functions, to change the structure and behaviour, to find and carry out the new functions necessary for successful opposition for adverse effects, adapting to conditions of the functioning. Mechanisms of maintenance of the surviv-ability, entering into such systems, are their integral part. Difficult organizational-technical systems irrespective of their appointment, should possess ability effectively to function at re-ception of damages (destructions) or to restore it during set time, that is to possess property - survivability. For construction of such systems perfection of methods and algorithms of estimation and survivability maintenance is neces-sary. To consider and the analysis of various types of influence. To apply new architecture of construction of the distributed ele-ments of the difficult systems steady against external influences. Within the limits of the spent analysis in the field of an estimation and definition of survivability of the difficult organizational-technical systems of different function, the example of estimation of survivability presented in given article with use of the logiko-likelihood approach allow to draw a conclusion about, volume that it is necessary to give an essential role to creation of realisation developed in various techniques-models of survivability.
Keywords: difficult organizational-technical system, survivability of systems, a method, model, a technique.

References

1. Volik BG, Ryabinin of news agency, 1984, Efficiency, reliability and survivability of operating systems, ' Automatics and telemechanics № 12 ', pp.23-25.
2. Glushkov BM, 1979, the Dictionary on cybernetics, p.87.
3. Pots BB, 1982, the Logiko-likelihood method of calculation of survivability of difficult systems, ' Cy-bernetics of AN UOT - № 1 ', pp.104-107.
4. Kagan VM, Dolkart BM, Kanevsky MM, 1978, the Operating computer complex with automatic for re-sponsible MANAGEMENT information systems TP, ' Cybernetic problems of MANAGEMENT information system TP ', Knowledge, ' MDNTP ', pp.3-11.
5. Cossacks VI, 1977, the ory Bases maintenance of operations of armies,' Section 1VIA ', pp.32-36.
6. Kochkarov AA, Malinetsky GG, 2005, Maintenance of firmness of difficult systems. Structural aspects, IPM of M.V.Keldysh of the Russian Academy of Sciences, pp.45-48.
7. Prokhorov AM, 1972, the Big Soviet encyclopaedia, ' Volume №9 ', p.569.
8. Rudenko BN, Ushakov IN, 1986, Reliability of systems of power, the Science, p.252.
9. Ryabinin of news agency, 1964, Theoretical bases of designing EES of the ships, MMA, p.240.
10. Safonov RA, 2003, the Technique of an estimation of survivability of difficult military-oriented sys-tems, ' UDC 519.876 ', pp.1-3.
11. Stekolnikov UI, 2002, Survivability of systems, ' Politehnika ', p, 69.
12. Tomilov UM, Mednov IT, Svishchev GP, 1993, ' Fighting survivability ', the Big Russian encyclopae-dia, pp.7-10.
13. Ushakov IN, 1985, Reliability, in technical systems. A directory, ' Radio and communication ', p.606.
14. Circassians GN, Circassians GN, Mozhaev the EXPERT, 1991, Logiko-likelihood methods of calcula-tion of reliability of structurally-difficult systems, ' Quality and reliability of products, № 3 (15), Knowledge, pp.3-64.

НАЦИОНАЛЬНАЯ ПРЕМИЯ

Большая Цифра

КАТЕГОРИИ:

«КОМПАНИЯ-ОПЕРАТОР»

«ОБОРУДОВАНИЕ И ТЕХНОЛОГИИ»

«ТЕЛЕКАНАЛЫ»

www.bigdigit.ru

Национальная премия в области многоканального цифрового телевидения «БОЛЬШАЯ ЦИФРА» проводится в рамках 16[й] выставки и форума CSTB'2014

Зрительское голосование в номинации «Телеканалы» пройдет **с 1 по 15 декабря** на сайте **www.bigdigit.ru**

18+

Организаторы: MIDexpo, АКТР

Генеральный партнер: eutelsat COMMUNICATIONS

Стратегический партнер: ТРИКОЛОР ТВ FULL HD

Платиновый спонсор: Билайн

Официальный партнер: СИГНАЛ МЕДИА

Партнеры: СТРИМ, РСКС Космическая связь

Генеральный информационный партнер: ТЕЛЕСПУТНИК

Генеральный интернет-партнер: COMNEWS

ЧАСТОТНЫЙ СПЕКТР СЕТЕЙ ЧЕТВЕРТОГО ПОКОЛЕНИЯ (4G): ТЕКУЩАЯ СИТУАЦИЯ, ПЕРСПЕКТИВЫ В РОССИИ И МИРЕ MW RUS

Наличие достаточного объема частотного спектра является необходимым условием для развития полноценных сетей LTE, а в России «частотная» проблема стоит наиболее остро. Компания J'son & Partners Consulting представляет основные результаты исследования ***«Частотный спектр для сетей четвертого поколения (4G): текущая ситуация и перспективы в мире и в России»***.

Диапазоны частот для LTE и практика их использования в мире

По данным GSA, на 17 октября 2013 года в 83 странах мира было запущено 222 коммерческие сети LTE, причем почти половина из этого количества сетей – в последние 12 месяцев. Как ожидается, к концу 2013 года количество стран с коммерческими сетями LTE возрастет до 93, а число самих сетей – до 260. Наиболее масштабные сети (по количеству абонентов) развернуты в США, Японии, Южной Корее и Австралии.

Большая часть сетей LTE работает в парном спектре в режиме FDD , но интерес к сетям LTE TDD продолжает расти – в 18 странах мира уже развернуто 23 LTE-сети, которые поддерживают режим TDD (из них 11 сетей поддерживают оба режима - FDD и TDD).

Всего под технологию LTE выделено более 40 диапазонов частот (bands), при этом использование спектра для LTE имеет региональные особенности. Например, в США наиболее популярными являются диапазоны 700 МГц (в основном, band 13 и band 17) и AWS (1,7/2,1 ГГц), в Европе – диапазоны 1800 МГц (band 3) и 2600 МГц (band 7), в перспективе – 800 МГц (band 20). В Японии первые запуски LTE состоялись в диапазоне 800/850 МГц; 1,5 ГГц; 1,7 ГГц и 2,1 ГГц (в зависимости от оператора); также был выделен диапазон 700 МГц (APT700) для запуска будущих сетей LTE.

Большой интерес в мире связан с рефармингом частот GSM для их использования в сетях LTE. В особенности это касается диапазона 1800 МГц, а в некоторых случаях – 900 МГц. При этом большинство регуляторов одобряет технологически нейтральный подход, при котором операторы могут использовать имеющиеся у них частоты вне зависимости от конкретной технологии.

В целом, наиболее распространенным в мире диапазоном остается 1800 МГц (band 3) – его используют 43% коммерческих сетей LTE FDD. Следующие по популярности диапазоны – это 2,6 ГГц (band 7) и 800 МГц (band 20), в них работают 30% и 12% LTE-сетей, соответственно.

В условиях дефицита частот для LTE в отрасли поднимается вопрос об использовании дополнительных диапазонов частот. В июле 2013 года Консорциум 3GPP завершил стандартизацию технологии LTE для диапазона 450 МГц, что дает возможность операторам (в том числе в России), имеющим такие частоты, разворачивать сети LTE в этом диапазоне. Использование низких частот при строительстве сетей мобильной связи позволяет существенно экономить на строительстве сетей, поскольку для обеспечения покрытия одной и той же площади требуется значительно меньшее количество базовых станций, чем в случае использования высоких частот (например, 2,6 ГГц). Использование низкочастотных диапазонов (450, 700 и 800 МГц) актуально для покрытия территорий с низкой плотностью населения, где не требуется высокая емкость сетей, достигаемая при использовании высоких частот.

Частоты для сетей LTE в России

В России по состоянию на октябрь 2013 года в коммерческую эксплуатацию запущены сети LTE в 37 регионах. В подавляющем большинстве регионов сети запущены в парном спектре (LTE TDD) в диапазоне 2600 МГц (band 7), за исключением сетей LTE TDD - МТС в Москве (2600 МГц, band 38) и «Вайнах Телеком» в Чеченской Республике (2,3 ГГц, band 40).

Кроме того, компания «Основа Телеком» разворачивает сети LTE TDD в диапазоне 2,3 ГГц (band 40), в котором компания обладает большим частотным ресурсом - от 70 до 100 МГц, в зависимости от региона. К концу января 2014 года, согласно лицензионным требованиям, оператор должен постро

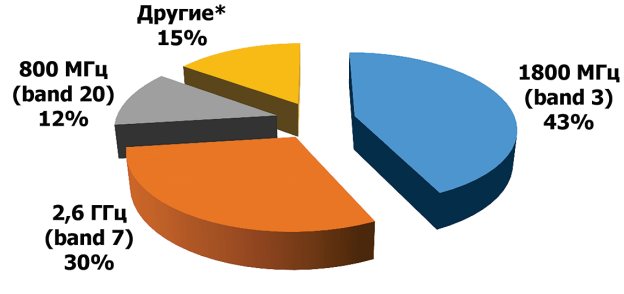


Рис.1. Наиболее используемые в коммерческих сетях LTE FDD диапазоны частот в мире

* К другим диапазонам частот для LTE относятся (в порядке убывания популярности использования в коммерческих сетях LTE в мире): 700 МГц (band 12, 13, 14, 17); AWS (band 4); 2100 МГц (band 1); 1900 МГц (band25); 850 МГц (band 5); 900 МГц (band 8); 1900 МГц (band 2).

Источники: GSA, J'son & Partners Consulting, 17 октября 2013 г.

Основные диапазоны частот для построения сетей LTE в России, июнь 2013 г.

Оператор	Режим	Диапазон (band)	Частоты, МГц
Скартел	FDD	7	2500—2530 / 2620—2650
МегаФон	FDD	20	847—854,5 / 806—813,5
	FDD	7	2530—2540 / 2650—2660
	TDD	38	2570—2595
ВымпелКом	FDD	20	854,5-862 / 813,5-821
	FDD	7	2550—2560 / 2670—2680
МТС	FDD	20	839,5-847 / 798,5—806
	FDD	7	2540—2550 / 2660—2670
	TDD	38	2595—2620
Ростелеком	FDD	20	832—839,5 / 791—798,5
	FDD	7	2560—2570 / 2680—2690
Основа Телеком	TDD	40	2300—2400

ить и запустить сети в 40 регионах. На 3 октября 2013 года «Основа Телеком» подготовила к тестовому запуску сети в 12 регионах.

Напомним, что по итогам конкурса состоявшемся в 2012 года, «Ростелеком», МТС, «МегаФон» и «ВымпелКом» получили LTE-лицензии в нижнем (720-790 МГц, 791-862 МГц) и верхнем (2500-2690 МГц) диапазонах. Каждый из победителей получил по 2 полосы в верхнем диапазоне шириной в 10 МГц и 7,5 МГц – в нижнем. Верхний спектр частот является относительно свободным и пригодным для развития LTE-сетей, а нижний – преимущественно занят силовыми структурами и системами радионавигации и радиолокации и требует проведения конверсии.

По оценке Ассоциации региональных операторов связи (АРОС), по состоянию на май 2013 года «МегаФон» и «Скартел» в совокупности контролировали около 36% спектра, доступного для построения сетей мобильного ШПД (3G, 4G) в России. Примерно одинаковым частотным ресурсом обладали «Ростелеком» (с учетом дочерней компании «Скай Линк») и МТС (24% и 23%, соответственно). На долю «ВымпелКома» пришлось оставшиеся 17% спектра. При этом, по оценке АРОС, в России по тем или иным причинам не используется около до 135 МГц спектра, пригодного для LTE.

Важным событием может стать получение разрешения от регулятора использовать для развертывания сетей LTE GSM-диапазон 1800 МГц. Однако решение этого вопроса по-прежнему откладывается, главным образом из-за разногласий чиновников по поводу обязательств, накладываемых на операторов, которые планируют строить LTE в этом диапазоне. Между тем задержка внедрения принципа технологической нейтральности остается существенным сдерживающим фактором развития LTE в России.

Особенности использования верхних и нижних частот для LTE

1.Развитие LTE на частоте 1800 МГц в среднем на 60% экономичнее, чем строительство сетей в высокочастотных диапазонах. Использование этого диапазона позволяет сократить время выхода технологии LTE на рынок и ускорить его развитие. В более выгодном положении окажутся те компании, которые смогут провести рефарминг для нижних частот 800-900 МГц, где развертывание сетей LTE в несколько раз дешевле, чем в диапазонах выше 2 ГГц.

2.Развертывание сетей в низкочастотной области спектра более привлекательно с точки зрения затрат и оптимально подходит для покрытия районов с низкой плотностью населения (пригороды и сельские районы). Низкие частоты, по сравнению с высокими, обеспечивают существенно лучшее проникновение внутри зданий и большую площадь покрытия, что, с одной стороны, позволяет обеспечить связью большие территории, а с другой – серьезно ограничивает плотность базовых станций и обостряет проблему внутрисистемной интерференции.

3. Высокие частоты отлично подходят для построения систем LTE в регионах с высокой плотностью населения, где требуются высокие скорости передачи данных. Однако если работать только в высокочастотном диапазоне, то неизбежно возникают проблемы с радиопокрытием. Фемтосоты, установленные в местах с высокой концентрацией абонентов (трафика) и в помещениях, помогают уменьшить «теневые» зоны в покрытии. Фемтосоты необходимы для улучшения покрытия сети на первых этажах зданий, в подвальных помещениях и на складах, а также для решения абонентских проблем, связанных с перегрузкой сети в часы пик.

Возможность использовать комбинацию из двух диапазонов (высокого и низкого) - залог объемного покрытия и обеспечения необходимой емкости в местах, где трафик особенно востребован. Для улучшения покрытия внутри зданий рекомендуется использовать фемтосоты.

Перспективы частотного регулирования России

Регуляторные изменения в области назначения и использования частотного ресурса будет определять вектор развития широкополосных мобильных коммуникаций на среднесрочную и долгосрочную перспективу. Основные направления регулирования касаются нескольких ключевых вопросов:

– переход от распределения частот по частным и общим решениям и конкурсам к частотным аукционам;

– принятие принципа технологической нейтральности;

– возможность совместного использования частот несколькими операторами;

– правила оплаты радиочастотного спектра.

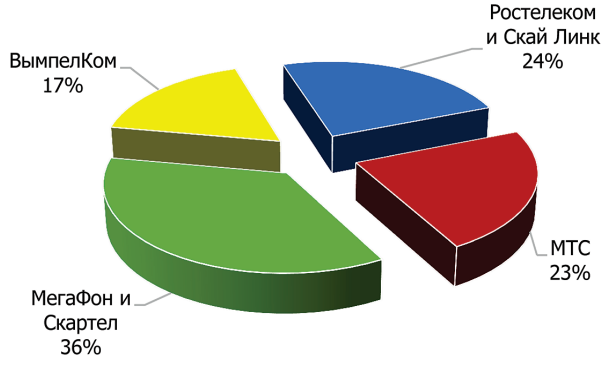


Рис.2. Распределение спектра 3G и 4G у основных операторов мобильной связи России

ПРИМЕНЕНИЕ ДВУМЕРНЫХ НЕЛИНЕЙНЫХ СИГНАЛОВ ФРАНКА-УОЛША, ФРАНКА-КРЕСТЕНСОНА В МЕТОДЕ ФОРМИРОВАНИЯ СКРЫТОГО КАНАЛА С КОДОВЫМ УПЛОТНЕНИЕМ В СТРУКТУРЕ СЖИМАЕМЫХ ВИДЕОДАННЫХ

Цветков К. Ю., *д.т.н., профессор,*
Военно-космическая академия имени А.Ф. Можайского,
wavelet3@mail.com.
Федосеев В.Е., *к.т.н., доцент,*
Военно-космическая академия имени А.Ф.Можайского,
veterfve@yandex.ru.
Абазина Е.С.,
Военно-космическая академия имени А.Ф.Можайского,
e.s.abazina@yandex.ru.

Ключевые слова:
встраивание данных в видеоданные, скрытые каналы, стеганография, сигнальные последовательности Франка–Уолша, Франка-Крестенсона, стандарты MPEG, JPEG.

АННОТАЦИЯ

В статье предлагается новый метод формирования скрытого канала с кодовым уплотнением на уровне спектральной плоскости видеоданных с устранением избыточности в соответствии со стандартами JPEG, MPEG-2. Вопросы, исследуемые в работе, относятся к области цифровой (компьютерной) стеганографии. Принципиальным отличием предлагаемого метода от известных является организация множественного доступа к среде обмена информацией, требующей скрытой передачи. Такая возможность достигается благодаря применению ансамблей ортогональных сигналов, посредствам которых реализовано кодовое уплотнение скрытого канала передачи информации. Заявляемый метод относится к классу методов с расширением спектра. Особенность построения скрытых каналов состоит в том, что дополнительно внедряемая информация кодируется с помощью ансамблей ортогональных дискретных двумерных широкополосных сигналов Франка-Уолша, Франка-Крестенсона, имеющих псевдошумовую природу. Сравнительный анализ ансамблей нескольких ортогональных сигналов, подтвержденный результатами проведенных компьютерных экспериментов, представленных в статье, позволил рассматривать дискретные двумерные широкополосные сигналы Франка-Уолша, Франка-Крестенсона как наиболее оптимальные для решения задачи формирования скрытого канала с кодовым уплотнением. При выборе ансамблей сигналов оценивание проводилось по рассчитанным значениям коэффициента дельтакорреляции сигналов и коэффициента ошибок извлеченных данных. В статье также уделено внимание степени соответствия структуры ансамблей сигналов принципам сжатия видеоданных JPEG, MPEG-2. Кроме того представлена зависимость достоверной передачи скрываемых данных от номера модифицируемого бита видеоданных и сделаны выводы относительно выбора бита, наилучшего для встраивания. Для оценки качества встраивания информации в соответствии с описываемым методом был выбран показатель средне квадратичного отклонения, для которого была рассчитана зависимость от различных значений качества изображения. Сравнение полученных результатов для заявляемого метода с аналогичными значениями других методов встраивания, позволило сделать вывод о том, что дискретные двумерные широкополосные сигналы Фрака-Уолша, Франка-Крестенсона являются наилучшими при решении задачи множественного доступа к скрытому каналу.

Вопросы формирования скрытых каналов передачи информации относятся к области стеганографии. Задача компьютерной (цифровой) стеганографии, наиболее популярной сегодня, состоит во внедрении информации в мультимедийные данные, что возможно благодаря следующим особенностям [1-3]:

- мультимедийные данные могут быть видоизменены без потери своей функциональности, в отличие от других типов данных, обладающих значимо меньшей избыточностью;

- органы чувств человека не способны замечать минимальные изменения в цвете изображения, в качестве звука или видео.

Анализ существующих стегопрограмм, запатентованных и получивших распространение, а также стегоалгоритмов, описанных в известной литературе, показал, что наиболее популярным типом мультимедийных файлов, используемых в качестве стегоконтейнеров, являются файлы изображений и видео форматов jpg, gif, bmp и avi, vob, mpg соответственно. Выбор стандартов jpg и mpg обусловлен следующими причинами:

- группа стандартов JPEG, MPEG постоянно развиваются, по оценкам экспертов именно эти стандарты продолжают выполнять основную роль в сжатии видеоданных (неподвижных и подвижных) при информационном обмене в современных мультисервисных сетях [4-6];

- в сети Интернет доля трафика видеоданных растет и на настоящее время составляет более 70% от общего информационного обмена;

- наиболее стойкие к атакам стеганографические методы разработаны для видео и изображений, так как они обладают неоднородной файловой структурой, анализ которой представляет сложную вычислительную задачу большой размерности [3].

Несмотря на то, что стандарты JPEG и MPEG-2 не являются самыми эффективными в отношении степени сжатия видеоданных, однако именно они продолжают оставаться наиболее популярными, в первую очередь в мультисервисных сетях специального назначения.

Проведенный анализ в области программных продуктов и запатентованных решений в области компьютерной (цифровой) стеганографии показал, что наиболее распространенными являются стегокомплексы, допускающие использование графических контейнеров, наиболее эффективные из них представлены ниже [1-3].

OutGuess – программный комплекс, написанный для UNIX-подобных операционных систем, осуществляющий сокрытие в младших битах элементов блоков спектра после квантования с использованием встроенного комплекса оценки статистики амплитуд частот, благодаря чему обеспечивает высокую стойкость к факту обнаружения встраивания.

Steganos – программа, разработанная для операционной системы MS-DOS и Windows 95/98/NT, оперирует с графическими файлами формата BMP и позволяет шифровать и сжимать сообщение перед сокрытием, встраивание происходит так же в младшие биты, обеспечивая большую скрытую пропускную способность, однако обладает более низкой стеганографической стойкостью.

EZStego – программа последовательно встраивает в видеопоток цифровой водяной знак (ЦВЗ) с целью исключения несанкционированного копирования и распространения видео. Реализованный в EZStego метод встраивания не позволяет избежать локализации энергии ЦВЗ в определенной части видеопотока, что делает его легко обнаруживаемым.

MSU StegoVide осуществляет встраивание ЦВЗ в видеопоток с применением помехоустойчивого кодирования, благодаря которому достигается стойкость к сжатию с потерями.

Однако среди представленных программных реализаций стеганографических методов нет тех, которые бы позволяли вести скрытый обмен между несколькими абонентами одновременно. Таким образом, заявляемый оригинальный метод формирования скрытого канала с кодовым уплотнением в структуре сжимаемых видеоданных является новым. Метод предполагает изменение среднечастотных коэффициентов подходящих кадров изображения, полученных после проведения процедур дискретно-косинусного преобразования (ДКП), квантования и представления в двоичном виде. Замене подвергаются биты с 3-5, не считая наименее значащего. Основу скрытого обмена составляет использование широкополосных двумерных нелинейных сигналов Франка – Уолша (Ф-У) или Франка-Крестонсона (Ф-К), модулированных сообщениями пар абонентов, участвующих в скрытом обмене. На приемной стороне восстановление скрыто передаваемых данных выполняется корреляционными методами. Подробное описание предлагаемого метода представлено в работах [7,8].

В работах [1,2] определено, что для незаметного встраивания данных стегокодер должен решить три задачи: выделить подмножество бит, модификация которых мало влияет на качество (незначимые биты), выбрать из этого подмножества нужное количество бит в соответствии с размером скрываемого сообщения и выполнить их изменение. Если статистические свойства контейнера не изменились, то внедрение информации можно считать успешным. Так как распределение незначащих бит зачастую близко к белому шуму, встраиваемые данные должны иметь тот же характер. В известных методах [1-3] это, как правило, достигается за счет предварительного шифрования внедряемого сообщения либо за счет его сжатия. В предлагаемом методе такой эффект достигается использованием двумерных нелинейных сигнальных конструкций Ф-У, Ф-К, структура которых близка к структуре белого шума, постоянно присутствующего в канале.

Для оценки влияния встраивания информации в контейнер применяется один из показателей, относящийся либо к группе разностных либо к группе корреляционных характеристик [1, 2].

Оценивание качества встраивания заявляемым способом осуществляется по выбранному показателю средне квадратичного отклонения (СКО) [1, 2]:

$$CKO = \frac{1}{XY}\sum_{x,y}(E_{x,y} - M_{x,y})^2,$$

где $E_{x,y}$ – пиксель пустого контейнера изображения с координатами (x,y), $M_{x,y}$ – пиксель заполненного (модифицированного) контейнера изображения с координатами (x,y), X*Y – размер изображения с X строками и Y столбцами.

В работах [9-12] было доказано, что на периодах $N = n^s$, $n \geq 2$, $s \geq 1$ существует дискретный базис Виленкина-Крестенсона (В-К), который является обобщением базиса Фурье (случай $s = 1$) и базиса Уолша (случай $n = 2$), естественным оператором сдвига для базиса В-К является n-ичный сдвиг. Обобщение понятий и определений теории сложных дискретных сигналов, устоявшиеся в базисе Фурье, для базиса В-К позволило построить ансамбли дельта-n-коррелированных сигналов с основанием $n = 2$ (двумерные сигналы Франка-Уолша) и $n > 2$ (двумерные сигналы Франка-Крестенсона). Исследование структуры и свойств сигналов Ф-У и Ф-К, представленные в работах [9-12] свидетельствуют, что для этих сигналов характерны следующие особенности:

- ансамбли двумерных сигналов Ф-У (Ф-К) ортогональны, что позволяет использовать их для передачи информации с кодовым множественным доступом;
- блочная структура двумерных сигналов Ф-У (Ф-К) согласована с алгоритмами сжатия видео и изображений MPEG, JPEG соответственно;
- в спектре отсутствуют нулевые составляющие, максимально приближая структуру сигналов Ф-У (Ф-К) к структуре белого шума.

Двумерный сигнал Франка – Крестенсона φ_2 имеет вид:

$$\varphi_2(j_1, j_2) = \varphi(j_1) \otimes \varphi(j_2),$$

где $\oplus$ - знак кронекерова произведения, φ определено формулой:

$$\varphi(kn^s + j) = a_k v_{\pi(k)}(j +_n \tau(k)), k, j \in T_s,$$

где $v_{\pi(k)}$ функции В-К при n>2.

Пример двумерного четырёхзначного сигнала Франка – Крестенсона $\varphi_2(j)$ размерностью 16x16, сформированного путём кронекерова произведения двух матриц вида $\varphi(j)$ (1), представлен матрицей (2).

$$\varphi(j) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \quad (1)$$

$$\varphi_2(j) = \left(\begin{array}{cccc|cccc|cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i & 1 & -i & -1 & i \\ \hline 1 & 1 & 1 & 1 & i & i & i & i & -1 & -1 & -1 & -1 & -i & -i & -i & -i \\ 1 & i & -1 & -i & i & -1 & -i & 1 & -1 & -i & 1 & i & -i & 1 & i & -1 \\ 1 & -1 & 1 & -1 & i & -i & i & -i & -1 & 1 & -1 & 1 & -i & i & -i & i \\ 1 & -i & -1 & i & i & 1 & -i & -1 & -1 & i & 1 & -i & -i & -1 & i & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & i & -1 & -i & -1 & -i & 1 & i & 1 & i & -1 & -i & -1 & -i & 1 & i \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -i & -1 & i & -1 & i & 1 & -i & 1 & -i & -1 & i & -1 & i & 1 & -i \\ \hline 1 & 1 & 1 & 1 & -i & -i & -i & -i & -1 & -1 & -1 & -1 & i & i & i & i \\ 1 & i & -1 & -i & -i & 1 & i & -1 & -1 & -i & 1 & i & i & -1 & -i & 1 \\ 1 & -1 & 1 & -1 & -i & i & -i & i & -1 & 1 & -1 & 1 & i & -i & i & -i \\ 1 & -i & -1 & i & -i & -1 & i & 1 & -1 & i & 1 & -i & i & 1 & -i & -1 \end{array}\right) \quad (2)$$

В случае, когда $n = 2$, при $\Omega_2 = \{1, -1\}$ и Ts = {0, 1, …, 2–1} функции Виленкина – Крестенсона принимают вид:

$$v_k(j) = \prod_{\nu=0}^{s-1} (-1)^{k_\nu j_\nu}, k, j \in T_s,$$

т.е. становятся функциями Уолша.

Двумерный сигнал Франка–Уолша $\psi 2$ имеет вид:

$$\psi_2(j_1, j_2) = \psi(j_1) \otimes \psi(j_2),$$

где $\oplus$ - знак кронекерова произведения, ψ определено формулой:

$$\psi(k2^s + j) = a(k) v_{\pi(k)}(j +_2 \tau(k)), k, j \in T_s,$$

где $v_{\pi(k)}$ функции В-К при n=2.

Пример двумерного четырёхзначного сигнала Франка – Уолша $\psi_2(j)$ размерностью 16x16, сформированного путём кронекерова произведения двух матриц вида $\psi(j)$ (3), представлен матрицей (4).

$$\psi(j) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad (3)$$

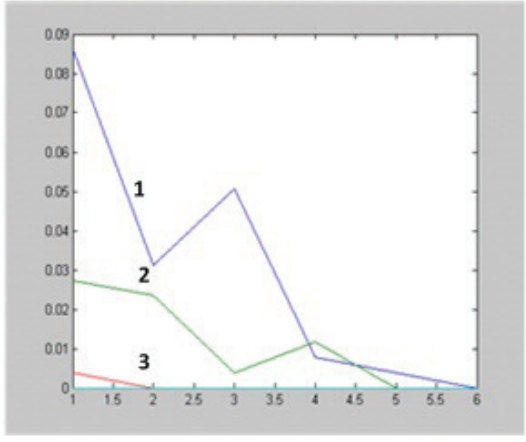
Близость структуры сигнала к шумоподобному оценивается коэффициентом дельтакорреляции γ, значения которого для различных ШПС представлены в таблице 1 Наименьшее значение, которое может принимать γ, равно 1 и соответствует максимально похожему на белый шум сигналу. Математическое моделирование показало, что сигналы необходимо согласовывать с видом проводимого над ними преобразования в выбранном базисе, что так же, как и тип используемых сигналов, является ключевой информацией

но, что встраивание в 2 бит устойчиво к сжатию в 5 раз, в 3 бит – к сжатию в 8 раз, 4 бит – примерно в 12 раз. Визуальнозаметные искажения наступают при внедрении в 5 бит.

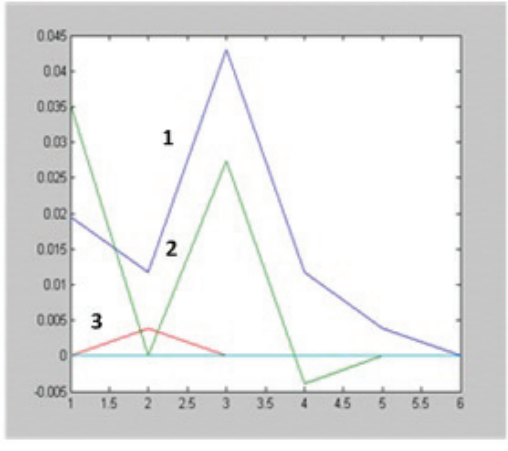
Лучшие результаты могут быть получены при модификации малых по величине, высокочастотных коэффициентов ДКП изображения, в этом случае вносимое искажение имеет характер высокочастотного шума, равномерно распределённого по изображению, и, следовательно, сложно определяемое и визуально и методами статистического стегоанализа. Оценка изменения статистики видеоизображения после модификации скрыто передаваемой информацией осуществляется по СКО.

Полученные значения СКО от качества изображения для описываемого метода встраивания с применением двумерных нелинейных сигналов Ф-У в паре с диадным сдвигом в базисе В-К (кривая 1), для описываемого метода встраивания с применением сигналов Уолша в паре с циклическим сдвигом в базисе Уолша (кривая 3), для метода встраивания по алгоритму OutGuess (кривая 2), представленные на рисунке 9, позволяют считать метод формирования скрытого канала с кодовым уплотнением в структуре сжимаемых видеоданных на основе сигналов Ф-У (Ф-К) стеганографически стойким, а двумерные нелинейные сигналы Ф-У (Ф-К) - наилучшими для задачи стегообмена.

Таким образом, наиболее оптимальными сигнальными конструкциями при формировании скрытого канала с кодовым уплотнением в структуре сжимаемых видеоданных являются двумерные нелинейные сигналы Ф-У (Ф-К) в паре с диадным и n-сдвигом в базисе Уолша и В-К соответственно. Их основными особенностями являются: ортогональность формируемого ансамбля сигналов; блочность структуры сигналов; отсутствие в спектре нулевых составляющих. Благодаря этим свойствам обеспечивается множественный доступ к среде скрытого обмена; устойчивость скрытно встраиваемых данных к сжатию по стандартам MPEG, JPEG; стойкость к статическим методам стегоанализа.



а) сигнал Ф-У в паре с цикличиским сдвигом в базисе Уолша



б) сигнал Ф-У в паре с диадным сдвигом в базисе Уолша

Рисунок 7 (а, б) - Зависимость коэффициента ошибок извлеченных данных скрытого канала с кодовым уплотнением от степени сжатия изображения

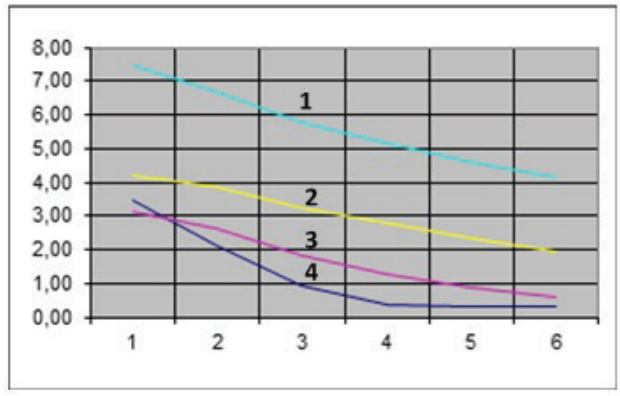


Рисунок 8- Зависимость отношения центрального пика функции корреляции к боковому от степени сжатия для внедрения в пикселы от 2 до 5

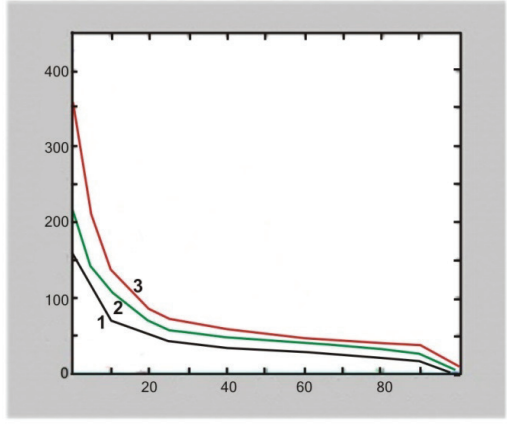


Рисунок 9 – Зависимость СКО от качества изображения

Литература

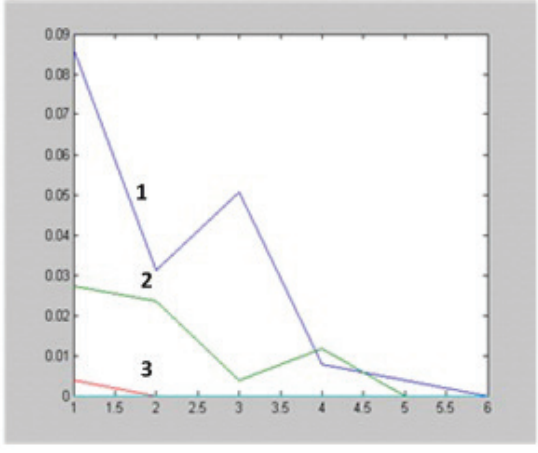
1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.

но, что встраивание в 2 бит устойчиво к сжатию в 5 раз, в 3 бит – к сжатию в 8 раз, 4 бит – примерно в 12 раз. Визуальнозаметные искажения наступают при внедрении в 5 бит.

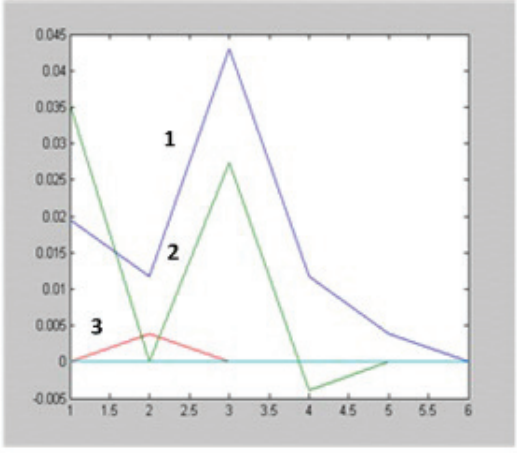
Лучшие результаты могут быть получены при модификации малых по величине, высокочастотных коэффициентов ДКП изображения, в этом случае вносимое искажение имеет характер высокочастотного шума, равномерно распределённого по изображению, и, следовательно, сложно определяемое и визуально и методами статистического стегоанализа. Оценка изменения статистики видеоизображения после модификации скрыто передаваемой информацией осуществляется по СКО.

Полученные значения СКО от качества изображения для описываемого метода встраивания с применением двумерных нелинейных сигналов Ф-У в паре с диадным сдвигом в базисе В-К (кривая 1), для описываемого метода встраивания с применением сигналов Уолша в паре с циклическим сдвигом в базисе Уолша (кривая 3), для метода встраивания по алгоритму OutGuess (кривая 2), представленные на рисунке 9, позволяют считать метод формирования скрытого канала с кодовым уплотнением в структуре сжимаемых видеоданных на основе сигналов Ф-У (Ф-К) стеганографически стойким, а двумерные нелинейные сигналы Ф-У (Ф-К) - наилучшими для задачи стегообмена.

Таким образом, наиболее оптимальными сигнальными конструкциями при формировании скрытого канала с кодовым уплотнением в структуре сжимаемых видеоданных являются двумерные нелинейные сигналы Ф-У (Ф-К) в паре с диадным и n-сдвигом в базисе Уолша и В-К соответственно. Их основными особенностями являются: ортогональность формируемого ансамбля сигналов; блочность структуры сигналов; отсутствие в спектре нулевых составляющих. Благодаря этим свойствам обеспечивается множественный доступ к среде скрытого обмена; устойчивость скрытно встраиваемых данных к сжатию по стандартам MPEG, JPEG; стойкость к статическим методам стегоанализа.



а) сигнал Ф-У в паре с цикличиским сдвигом в базисе Уолша



б) сигнал Ф-У в паре с диадным сдвигом в базисе Уолша

Рисунок 7 (а, б) - Зависимость коэффициента ошибок извлеченных данных скрытого канала с кодовым уплотнением от степени сжатия изображения

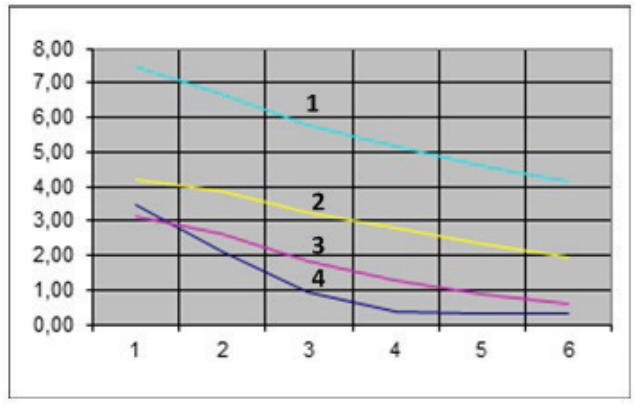


Рисунок 8- Зависимость отношения центрального пика функции корреляции к боковому от степени сжатия для внедрения в пикселы от 2 до 5

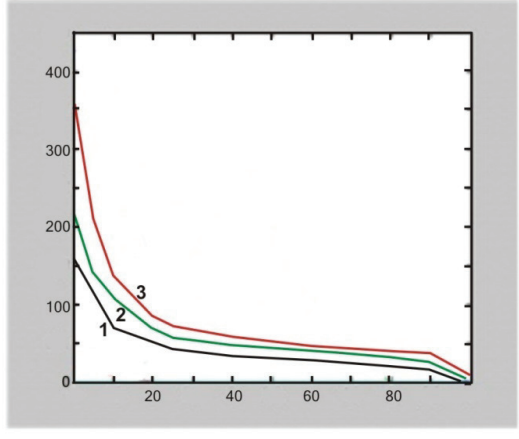


Рисунок 9 – Зависимость СКО от качества изображения

Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.

2. Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В. Bases компьютерной стеганографии. – Ростов-на-Дону: 2003. – 110 с.
3. Радаев С.В., Кирюхин Д.А., Иванов И.В. Разработка алгоритма встраивания цифрового водяного знака в файлы формата MPEG-4 // Информационные системы и технологии, 2010, № 1/57 (584). С. 13 – 17.
4. Локшин Б.А., Цифровое вещание: от студии к телезрителю – М.: Компания Сайрус Системс, 2001. – 446
5. Умбиталиев А.А. Перспективы развития цифрового телерадиовещания: комплексное решение внедрения цифрового телевидения в регионах // Вопросы радиоэлектроники. Сер. Техника телевидения. 2008. Вып. 2. С. 3 – 8.
6. Сухов Т.М. ОБ иерархическом кодировании в цифровой си-стеме видеонаблюдения // информационные управляющие системы. – 2014. – № 2(69). – С. 50 – 62.
7. Абазина Е. С. Алгоритмы внедрения двумерных нелинейных кодовых последовательностей в структуру сжатых видеоданных // Вопросы радиоэлектроники. Сер. Техника телевидения. 2013. №1. с. 85-94.
8. Абазина Е. С. Алгоритмы обработки широкополосных цифровых водяных знаков при организации стеганографического канала в структуре видео данных // Труды Военной академии связи, Выпуск 79– СПб: ВАС: 2013. – С.9 – 14.
9. Цветков К.Ю. Синтез ортогональных систем сложных дискретных сигналов для широкополосных сетей связи с кодовым множественным доступом // Проблемы внедрения новых сетевых технологий в системы связи ВС РФ. Сб. научных трудов. Вып. 2 / Под ред. Н.И. Буренина. – СПб.: Международная Академия Информатизации, ВУС, 2002. – С. 52 – 63.
10. Цветков К.Ю., Малозёмов В.Н. Об оптимальной паре сигнал–фильтр // Проблемы передачи информации. – 2003. – Т.1. – Вып.2. – С. 50 – 62.
11. Дискретный гармонический анализ и его приложения к задачам синтеза оптимальных сигналов: монография / К.Ю.Цветков, В.М. Коровин – СПб.: ВКА им. А.Ф. Можайского, 2008. – 108 с
12. Коровин В.М., Цветков К.Ю. Синтез оптимальных двумерных сигналов и фильтров подавления боковых лепестков корреляционных функций сложных дискретных сигналов в базисе Виленкина – Крестенсона // Авиакосмическое приборостроение. – 2008. – № 12. – С. 19 – 23.
13. Буренин А.Н., Легков К.Е. Эффективные методы управления потоками в защищенных инфокоммуникационных сетях // H&ES: Наукоемкие технологии в космических исследованиях Земли. – 2010. –№ 2. – С. 29-34.
14. Буренин А.Н., Легков К.Е. Модели процессов мониторинга при обеспечении оперативного контроля эксплуатации инфокоммуникационных сетей специального назначения // H&ES: Наукоемкие технологии в космических исследованиях Земли. – 2011. –№ 2. – С. 19-23.

APPLICATION OF TWO-DIMENSIONAL NONLINEAR SIGNALS OF FRANK-UOLSH, FRANK-KRESTENSON INTO THE METHOD OF FORMATION OF THE HIDDEN CHANNEL WITH CODE CONSOLIDATION IN STRUCTURE OF THE COMPRESSED VIDEO DATA

Tsvetkov K., Dr.Sc.,Professor,
Military Space Academy, wavelet3@mail.com.
Fedoseev V., PhD, Associate Professor,
Military Space Academy, veterfve@yandex.ru.
Abasina E., Military Space Academy,
e.s.abazina@yandex.ru.

Abstract
In article the new method of formation of the hidden channel with code consolidation at level of a spectral plane of the video data with redundancy elimination according to standards JPEG, MPEG-2 is offered. The questions investigated in work, concern area digital (computer) stegonography. Basic difference of the offered method from known is the organisation of plural access to the shared medium where information interchange demanding hidden transfer. Such possibility is reached by application of ensembles of the orthogonal signals to which means code consolidation of the hidden channel of information transfer is realised. The declared method belongs to the class of methods with spectrum expansion. Feature of construction of the hidden channels consists of addition introduced information is coded by means of the ensembles of orthogonal discrete two-dimensional broadband signals of Frank-Uolsh, Frank-Krestenson having the pseudo-noise nature. The comparative analysis of ensembles of the several orthogonal signals, confirmed with results of the spent computer experiments presented in article, has allowed to consider discrete two-dimensional broadband signals Frank-Uolsh, Frank-Krestenson the best for the decision of the formation's problems of the hidden channel with code consolidation. At a choice of ensembles of signals estimation was spent on the calculated values of deltacorreletion's factor of signals and factor of errors of the transferred data. In article the attention of degree of conformity of structure of ensembles of signals also is paid to principles of compression of video data JPEG, MPEG-2. Dependence of authentic transfer of the hidden data on number of the modified bit of the video data is presented and conclusions concerning the bit choice, the best for embedding are drawn. For an estimation of quality of embedding of the information according to a described method has been chosen the indicator mean square error which dependence on various values of quality of the image has been calculated. Comparison of the received results for a declared method with similar values of other methods of embedding, has allowed to get a conclusion that discrete two-dimensional broadband signals of the Dress coat-Uolsh, Frank-Krestenson are the best at the decision of a problem of plural access to the hidden channel.

Keywords: data embedding into the video, the hidden channels, steganography, signal sequences of Frank-Uolsh, Frank-Krestenson, standards MPEG, JPEG.

References
1. Gribunin V. G, Okov I.N., Turintsev I.V. Digital steganografy. Moscow, Solon-press Publ., 2002. 272 p. (In Russian)
2. Agranovskij A.V., Devjanin P. N, Hadi R. A, Cheremushkin A.V. Bases of computer steganografy. Rostov-on-Don Publ., 2003. 110 p. (In Russian).
3. Radaev S.V., Kirjuhin D.A., Ivanov I.V. Working of algorithm of embedding of a digital watermark in files of format MPEG-4. Information systems and technologies, 2010, no. 1/57 (584). pp. 13 – 17 (In Russian).
4. Lokshin B. A, The digital announcement: from studio to the television. Moscow, Company Sajrus Sistems Publ., 2001. 446 p. (In Russian).
5. Umbitaliev A. A. Prospect of development of digital tele-radio broadcasting: the complex decision of introduction of digital television in regions. Radio electronics Questions. Series is the technics of television. 2008. vol. 2. pp. 3 – 8 (In Russian).
6. Suhov T.M. About hierarchical coding in digital system of video observation. Information operating systems. 2014. no. 2 (69). pp. 50 – 62 (In Russian).
7. Abasina E.S. Algorithms of introduction of two-dimensional nonlinear code sequences in structure of the compressed video data. Radio electronics Questions. Series is the technics of television. 2013. vol. 1. pp. 85-94 (In Russian).
8. Abasina E.S. Algorithms of processing of broadband digital watermarks at the organisation of the steganografic channel in structure of video. Works of Military academy of communication. no. 79. 2013. pp. 9 – 14 (In Russian).
9. Tsvetcov K.U. Synthesis of orthogonal systems of difficult discrete signals for broadband communication networks with code plural access. Problems of introduction of new network technologies in communication systems AF of the Russian Federation. vol.2. 2002. pp. 52 – 63 (In Russian).
10. Tsvetkov K.U., Malozermov V. N. About optimum pair the signal-filter. Information transfer Problems. 2003. vol.1. no.2. pp.50 – 62 (In Russian).
11. Tsvetkov K.U., Korovin V.M. The discrete harmonious analysis and its appendices to problems of synthesis of optimum signals. Mozhajskii Military Space Academy Publ., 2008. 108 p. (In Russian).
12. Korovin V. M, Tsvetkov K.U. Synthesis of optimum two-dimensional signals and filters of suppression of lateral petals of correlation functions of difficult discrete signals in basis of Vilenkin – Krestenson. Aerospace instrument making. 2008. no. 12. pp. 19 – 23 (In Russian).
13. Legkov, K.E.Effective methods of control over streams in protected infokommunikatsionny networks / A.N. Burenin, K.E.Legkov//H&ES: High technologies in space researches of Earth. - 2010.-№ 2. - Page 29-34.
14. Legkov, K.E. To a question of modeling of the organization of the information managing director of a network for a control system of modern infokommunikatsionny networks /A.N. Burenin, K.E.Legkov//H&ES: High technologies in space researches of Earth. - 2011.-№ 1. - Page 22-25.

Мария Гринчук
фотограф
mariagrinchuk.com
+7 905 263 64 58

ТЕХНИЧЕСКИЕ АСПЕКТЫ СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ МНОГОЦЕЛЕВОГО ПРИМЕНЕНИЯ

Орлов А.А.,
Научно-исследовательский испытательный центр «Авиационно-космической медицины и военного эргономики» 4 ЦНИИ МО РФ, For_orlov@mail.ru
Тельных А.А., *к.ф-м.н., «Институт прикладной физики» РАН, telnykha@yahoo.com*
Степанов Е.А.,
ЗАО «РНТ», blikolab@mail.ru
Сорокин А.Д.,
ЗАО «РНТ», dalwe@yandex.ru
Аксенова Ю.Е.,
Московский Государственный Университет, aksionova@yahoo.com

Ключевые слова:
Автоматизированная система управления, информационное обеспечение, безопасность передачи информации, распределенное хранение, распределенная обработка, интерактивная визуализация, транспортная безопасность, антикриминальная безопасность, техногенная безопасность.

АННОТАЦИЯ

В современных условиях высокой вероятности возникновения чрезвычайных ситуаций в различных сферах деятельности не вызывает сомнения актуальность разработки технологии, позволяющей принимать превентивные меры при возможности возникновения угроз различного характера. Предложенные в статье подходы к созданию подобных информационных систем позволяют решать конкретные задачи обеспечения транспортной, антикриминальной, техногенной безопасности. Создание макетного образца совместно с несколькими организациями совершенно разных по виду деятельности обеспечили адекватные и универсальные решения для безопасности передачи информации, распределенного хранения, обработки и интерактивной визуализации разного типа информации. Разработанная технология представляет собой модульное программное обеспечение, спроектированное по принципу «сверху-вниз», с возможностью расширения функционала за счет динамически подключаемых модулей и удаленного взаимодействия компонентов системы между собой. Основными компонентами, АИС являются интеграционная подсистема (ИП) и система отображения информации (СОИ). Приведенный материал, представлен на примере взаимодействия интеграционной платформы с системами видеонаблюдения (IP видеокамерами), как наиболее технически сложных и требовательных к ресурсам каналов передачи данных и обработки из имеющихся современных технических систем. Представленный материал может быть адаптирован к любой другой технической системе или компьютерной программе содержит анализ существующих подходов, рекомендации по способам развертывания ИП, аспекты информационной безопасности, предложения по структуре программного обеспечения, состав и функции подсистем, решения по анализу технической информации и ее интерактивное отображение. Разработанная технология позволяет: создавать автоматизированные информационные системы многоцелевого применения; обеспечивать работу высоконагруженных распределенных информационных систем в АИС; интегрировать различное техническое оборудование и обеспечивать прием обработку и передачу технической информации; интерактивно отображать в трехмерном представлении, на цифровой карте мира различного рада информацию в виде пиктограмм, графиков, анимированных объектов во взаимосвязи с глобальными координатами; изменять и расширять функционал без перепроектирования АИС в целом; разворачивать интеграционную подсистему на различных операционных системах Linux/Windows.

Законодателями и разработчиками автоматизированных информационных систем выступают в основном зарубежные компании (Microsoft, IBM, Oracle, Forrester): многие компоненты (протоколы обмена, системы управления базами данных, сжатие и шифрование информации) разрабатываются и производятся исключительно по патентам западных стран без предоставления исходных кодов программного обеспечения, что ставит российских разработчиков в информационную и финансовую зависимость, а также не позволяет использовать иностранные наработки в системах военного назначения. От момента создания технического задания до первого макетного образца проходит от 3-5 лет и более, за это время меняются стандарты технологий программного обеспечения: появляются новые платформы (frameworks), новые версии операционных систем, протоколы обмена данных, методы обеспечения безопасности, что ведет к тому, что результат 3-5 летней работы становится не актуальным.

В статье представлены подходы к созданию информационных систем, позволяющих принимать превентивные меры при возможности возникновения угроз различного характера, разработанные на стендовом образце программно-аппаратного комплекса (ПАК) «ISPLab». ПАК является технологией моделирования и проектирования комплексных систем автоматизации и управления, представляющих собой распределенные геоинформационные системы с централизованными пунктами управления информационными потоками от различных технических систем. Данный комплекс объединяет технические системы, с наличием внешних интерфейсов взаимодействия, привязывает их к глобальным географическим координатам и трехмерным моделям местности и дает возможность интегрировать новые системы в процессе эксплуатации.

Технические решения программного обеспечения «ISPLab» могут быть использованы в различных сферах: при создании систем антикриминальной, антитеррористической безопасности, защищенных систем передачи данных видео/аудио/текстовой информации через локальные компьютерные сети или через сеть «Интернет», специальных компьютерных тренажеров, АИС безопасности полетов.

Актуальность проведения таких работ можно проиллюстрировать на примере существующей системы обеспечения безопасности полетов, созданной в 60 х годах прошлого столетия в РФ: С 1995 по 2009 год общие потери государственной авиации составили 395 воздушных судов, при этом погибли 906 человек. Относительный показатель (число авиационных происшествий на 100 тыс. часов налета), характеризующий уровень аварийности, в течение 30 лет находится на уровне 4-5 авиационных происшествий на 100 тыс. часов налета, в то время как в ведущих авиационных державах этот показатель в 2 и более раза ниже.

Технология «ISPLab» представляет собой модульное программное обеспечение, спроектированное по принципу «сверху-вниз», с возможностью расширения функционала за счет динамически подключаемых модулей и удаленного взаимодействия компонентов системы между собой. Основными компонентами, АИС являются интеграционная подсистема (ИП) и система отображения информации (СОИ).

Приведенный далее материал, представлен на примере взаимодействия интеграционной платформы с системами видеонаблюдения (IP видеокамерами), как наиболее технически сложных и требовательных к ресурсам каналов передачи данных и обработки из имеющихся современных технических систем [1]. Представленный материал может быть адаптирован к любой другой технической системе или компьютерной программе.

Интеграционная подсистема (платформа)

Назначение

Объединить общий функционал различных подсистем АИС в условиях, когда этот функционал распределён между несколькими самостоятельными исполняемыми модулями программного обеспечения, а также предоставить единый программный (для разработчика) и графический (для пользователя) интерфейс.

Анализ существующих подходов

Можно выделить два основных подхода к разработке интеграционной подсистемы:

1. Каждый исполняемый модуль со своим специфическим функционалом импортирует общую интеграционную подсистему, при этом обязуется предоставить клиентскому ПО универсальный коммуникационный интерфейс.

2. Интеграционная подсистема включает первичные запускаемые программные модули, при этом она самостоятельно включает тот функционал, который экспортируется из специализированных функциональных модулей. В этом случае за коммуникацию с клиентским ПО отвечает интеграционная подсистема, а взаимодействие со специализированными функциональными модулями осуществляется исключительно через программный интерфейс.

Достоинством первого подхода является простота реализации, как общего функционала, так и модулей со своим специфическим функционалом. Данный подход более гибок с точки зрения расширения функционала.

Недостатком данного подхода является сложность реализации коммуникационной подсистемы в целом и развёртывания распределённого приложения, в частности, сложность адаптации клиентского ПО к различным коммуникационным особенностям модулей. Дублирование участков кода в различных модулях может приводить к нежелательным ошибкам в кодировании алгоритмов.

Второй подход напротив, сложнее в реализации интеграционной подсистемы, и немного сложнее в реализации модулей, при этом сильно упрощается реализация взаимодействия клиентского ПО с конечными функциональными модулями.

Архитектура подсистемы:

Проведённые исследования на макетах программного обеспечения показали преимущество второго подхода, так как он даёт больше гарантий (меньше возможностей допустить ошибки) при реализации конечного продукта.

В подсистему входят:

– подсистема запуска приложения;

– подсистема поиска и загрузки специализированных функциональных модулей;

– подсистема хранения настроек спе-

циализированных функциональных модулей;
– подсистема разграничения прав доступа пользователей к функциям модулей и интеграционной подсистемы в рамках приложения;
– подсистема идентификации и аутентификации пользователей;
– подсистема межпроцессной коммуникации;
– клиентская подсистема одновременного доступа к независимым приложениям (различным процессам) с подключенными специализированными функциональными модулями;
– подсистема тестирования;
– подсистема логирования;
– подсистема конфигурирования (и серверной и клиентской части).

Аспекты информационной безопасности на уровне интеграционной подсистемы

Оценка рисков информационной безопасности выходит за рамки описания данной подсистемы, однако, учитывая то, что элементы информационной безопасности должны быть учтены на всех уровнях АИС, далее будут приведены основные тезисы [2].

Информационная безопасность состоит в противодействии реализации следующих угроз:

1. Угроза нарушения конфиденциальности информации (НСД)
2. Угроза нарушения доступности информации (отказ в обслуживании)
3. Угроза нарушения целостности информации (изменение информации)

Стоит отметить, что реализация противодействия всем угрозам одновременно не возможна – необходимо ранжировать угрозы и на этой основе сбалансировать меры информационной безопасности.

Выявить риски и ранжировать эти угрозы по значимости – не простая задача. Ведь, например, злоумышленник может получить доступ на просмотр видеоизображения некоторой камеры. Это однозначно нехорошая ситуация. Однако если злоумышленник не может получить права на просмотр камеры, то он может попытаться загрузить её большим числом подключений, и в результате она выключится. Пока дежурный будет предпринимать меры по устранению неисправности, изображение с камеры будет отсутствовать. И последний пример нарушения целостности информации – если злоумышленник не может воздействовать на оборудование, но имеет возможность физически (или логически через маршрутизатор) встать в разрыв соединения, то он сможет транслировать записанный ранее видеопоток.

Таким образом, при разработке интеграционной подсистемы, необходимо учесть все угрозы информационной безопасности.

Общий подход к обеспечению информационной безопасности заключается в том, что если злоумышленник реализовал угрозу для одного из элементов системы, то это не должно сказаться на других элементах. Например, если злоумышленник смог проникнуть в систему с установленным сервисом АИС, то он не должен получить доступ на все сервисы системы.

Предлагается:

• Хранить пароли для сервисов по отдельности либо сервисы должны иметь только право проверки хешей паролей из центрального хранилища [3];
• Реализовать шифрование и цифровую подпись сообщений в коммуникационной подсистеме;
• Все программные средства системы (сервисы, подключаемые модули и клиенты) должны иметь цифровую подпись (или подписанный сертификат). Сервисы и клиенты не должны загружать неверифицированные модули. Клиенты не должны подключаться к неверифицированным серверам [4];
• Для защиты от атак отказа в обслуживании настроить сетевое оборудование, использовать средства сетевого мониторинга, для объёмного трафика использовать специализированные протоколы;
• Использовать антивирусные средства, IDS;

Подсистема отображения информации

Описание подсистемы отображения информации

Подсистема отображения представляет собой клиентское приложение для конфигурирования и контроля работы интеграционной платформы в конкретных условиях эксплуатации.

Подсистема отображения информации представляет собой графическую прикладную программу, предназначенную для визуализации потока технической информации, поступающего из системы распределенных сервисов интеграционной платформы. Данная система декодирует поток событий технических систем (видео аналитики и др.) в поток элементов изображения на экран в виде динамического цифрового макета объекта управления.

Система включает средства фильтрования потока элементов изображения с помощью системы глобального позиционирования (Global Positioning System) на экране пользователя и систему вычисления трехмерного изображения. В результате совместной работы двух систем каждый декодированный элемент потока технической информации визуализируется как элементарное трехмерное изображение с точным позиционированием и масштабированием относительно контролируемого участка местности (GPS- rectangle).

Техническим результатом является минимизация объема передаваемого трафика, например, от систем видеонаблюдения за счет представления видеоинформации как событий обычной технической системы на цифровом макете объекта.

Предложения по структуре подсистемы

• клиентская подсистема
• система анализа информационных моделей
• средства фильтрования потока элементов
• система вычисления трехмерного изображения
• система отображения

Общий алгоритм работы подсистемы

Клиентская подсистема запрашивает у сервиса аутентификации список разрешенных текущему пользователю подключений к удалённым сервисам интеграционной платформы.

Клиентская подсистема осуществляет подключение к разрешенным удалённым процессам, и при необходимости, запрашивает аутентификацию.

Клиентская подсистема предоставляет Системе анализа информацион-

ных моделей список удалённых процессов, список специализированных функциональных модулей в каждом удалённом процессе, список доступных функций в каждом модуле.

Далее клиентская подсистема осуществляет взаимодействие со специализированными функциональными модулями по установленному протоколу обмена.

Система отображения с помощью конвекторов переводит техническую информацию в трехмерное графическое изображение на цифровой карте мира.

Состав и функции компонентов подсистемы

Клиентская подсистема

Клиентская подсистема – представляет собой сервис, который реализует CallBack интерфейс интеграционной платформы. Клиентская подсистема предназначена для функций конфигурирования, настройки устройств, работы с уровнями доступа и передачи пользовательской и сервисной информации.

Работа клиентов через данный интерфейс выполняется в следующей последовательности:

- Подключение пользователя с указанием имени пользователя;
- Выбор типа устройства;
- Выбор устройства;
- Подписка на события

Клиентская часть подключения к СПМ Сервису строиться на базе автоматически формируемого файла описания интерфейса (XML). Данный класс имеет набор методов, реализующих интерфейс и обратное событие. Таким образом, события, происходящие в интеграционной платформе, будут доставляться клиенту.

Класс имеет специальный поток контроля соединения с интеграционной платформой. При разрыве или ошибке связи происходит автоматическая попытка переподключения клиента к интеграционной платформе.

Система анализа информац онных моделей

Данный модуль оперирует информационными моделями изображений видеокамер «цифрой моделью устройства» (далее - устройство).

Описание устройства определяет характеристики устройства, значение состояния (параметры, характеризующие работу устройства – например, текущее состояние устройства или найденные объекты на видеоизображении), родительское устройство (например, группу), набор подчиненных устройств.

При загрузке сервиса все устройства производят подключение к интеграционной платформе, на которой они зарегистрированы. С помощью TCP\IP канала происходит всё взаимодействие системы визуализации и Сервиса Информационной модели для конкретного устройства – обновление статуса устройства, получение событий, вызов команд и т.п. Происходит загрузка системных событий и команд, которые зарегистрированы в Сервисе, и объединение с системными событиями и командами, прочитанными при загрузке из файла конфигурации устройства.

Все поступающие системные события от Сервиса анализируются и кладутся в очередь событий для последующей передачи клиенту. Анализ события производится в зависимости от типа события и в очередь событий устройства добавляется соответствующая запись. Впоследствии, в специальном потоке происходит проверка всех устройств на наличие событий в очереди, анализ события и соответствующая обработка.

Аналогично происходит формирование системных событий: событие кладется в очередь событий клиентов, в потоке контроля соединения клиента очередь проверяется, и событие отправляется Системе визуализации.

Устройства могут быть объединены в группы. Группа определяет устройства, которые включены в данную группу. Они могут быть двух типов – отдельно сконфигурированное устройство, или уже созданная группа устройств. На стороне клиента для построения дерева требуется загрузить все устройства и группы, пройтись по всем группам, рекурсивно построить дерево объектов исходя из массива объектов, которые находятся в конкретной группе.

Права доступа к группам устройств делегируются по правилам интеграционной платформы.

Для устройства настраиваются элементы отображения в зависимости от вариантов состояния устройства. Для каждого состояния имеется возможность задать графический ресурс (пиктограмму) и звуковой файл. Звуковой файл проигрывается при переходе из одного состояния в другое.

Система вычисления трехмерного изображения

Система вычисления трехмерного изображения обеспечивает надежное и адаптивное отображение объектов любого вида из потока информационных моделей. Главной задачей системы является кодирование системы выведения на экран цифрового макета объекта в виде синтезированного 3D-изображения, в котором поток динамической информации сужается при помощи специфического кодирования, что позволяет также существенно улучшить непрерывность выведения на экран 3D-изображения.

Система вычисления трехмерного изображения предназначена для получения обработки потока элементов изображения, который включает адресуемые элементы изображения, каждый из которых образован геометрической формой, согласно действующим правилам системы видео аналитики.

В зависимости от информации, заложенной в информационной модели, система вычисления трехмерного изображения создает графический трехмерный объект. Например, если с модуля видеоаналитики пришло событие о появлении нового человека, данная система создаст 3d модель человека с его отличительными признаками.

Система отображения

Главной целью Подсистемы отображения является скорость визуализации. Чтобы обеспечить своевременное отображение сложных текстур, специальных эффектов вроде частичной прозрачности и трехмерной графики. Прорисовка сложной трехмерной графики (DirectX's forte) проходит через конвейер DirectX, который включает поддержку всех современных видеокарт. DirectX передает как можно больше работы узлу обработки гра-

фики (graphics processing unit — GPU), который представляет собой отдельный процессор на видеокарте. Кроме того, система отображения базирует свое масштабирование на системной установке DPI, а не на DPI физического дисплейного устройства. Это значит, что любое отображение (включая фигуры, элементы управления, текст и любые другие ингредиенты, которые помещаются в окно приложения) на 100-дюймовом проекторе или видеостене, будет выглядеть также как на 17 дюймовом мониторе [5].

Система отображения предназначена для окончательного синтеза всей графической информации, имеющейся в памяти программы, для вывода ее на экран пользователя. Данный процесс осуществляется следующим образом: информационные модели в виде синтезированного трехмерного изображения макета объекта, выдаваемым прикладным модулем видеоаналитики, поступают в Систему отображения, из потока выделяются элементарные изображения, образующие часть выводимого на экран синтезированного трехмерного изображения.

Выводы

Разработана технология «ISPLab», позволяющая:

- создавать автоматизированные информационные системы многоцелевого применения;
- обеспечивать работу высоконагруженных распределенных информационных систем в АИС;
- интегрировать различное техническое оборудование и обеспечивать прием обработку и передачу технической информации;
- интерактивно отображать в трехмерном представлении, на цифровой карте мира различного рада информацию в виде пиктограмм, графиков, анимированных объектов во взаимосвязи с глобальными координатами;
- изменять и расширять функционал без перепроектирования АИС в целом;
- разворачивать интеграционную подсистему на различных операционных системах Linux/Windows.

Литература

1. Davis, K., 2012. Ethics of Big Data 2012. б.м.:O'Reilly Media. -79с.
2. Konheim, A.G., 2007. Computer security and cryptography. б.м.:John Wiley & Sons, Inc. 542с.
3. В. С. Горбатов, О. Ю. П., 2011. Основы технологии PKI. б.м.:Горячая Линия - Телеком. 248с.
4. Леве, Д., 2008 . Programming WCF Services. б.м.: Питер. 910 с.
5. Мак-Дональд, М., 2008. WPF. Windows Presentation Foundation в NET 3.5 с примерами на C# 2008 для профессионалов (2-е издание). б.м.:Диалектика, Вильямс. 922 с.
8. Буренин А.Н., Легков К.Е. К вопросу моделирования организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями // H&ES: Наукоемкие технологии в космических исследованиях Земли. – 2011. – № 1. – С.22-25.

TECHNICAL ASPECTS OF AUTOMATED INFORMATION SYSTEMS' MULTIPLE APPLICATION DEVELOPMENT

Orlov A., Scientific Research Center "Aerospace Medicine and military ergonomics", For_orlov@mail.ru
Telnykh A., Institute of Applied Physics, Studies telnykha@yahoo.com
Stepanov E., JSC "RNT", blikolab@mail.ru
Sorokin A., JSC "RNT", dalwe@yandex.ru
Aksenova U., Moscow State University, aksionova@yahoo.com

Abstract

In modern conditions, the high likelihood of emergency situations in the various spheres of activity is no doubt the urgency of developing technology that allows to take preventive measures when possible threats of a different nature . In the article are approaches to the creation of such systems allow information to solve specific problems of maintenance of transport , anti-crime , technological safety . Create a mock-up together with several organizations of vastly different kind of activity to ensure adequate and universal solutions for transmission of information security , distributed storage , processing, and interactive visualization of different types of information. The developed technology is a modular software designed on the principle of "top-down ", with the ability to extend the functionality through plug-ins dynamically and remoting system components together. The main components are the AIS subsystem integration (PI), and display system information (SDI) . Above material is presented as an example of interaction platform integration with video surveillance (IP cameras) as the most technically complex and demanding data channels and processing of available modern technology systems . The material presented can be adapted to any other technical system or computer program provides an analysis of existing approaches , recommendations on ways to deploy IP aspects of information security , proposals for software structure , composition and functions of the subsystems solutions for analysis of technical information and an interactive map. The developed technology allows you to: create automated information systems of multiple use ; provide work heavily distributed information systems in AIS ; integrate different technical equipment capable of receiving and processing and transfer of technical information ; interactively display three-dimensional representation on a digital map of the world is pleased to different information in the form of icons , graphics, animated objects in conjunction with the global coordinates ; modify and extend functionality without redesigning the AIS as a whole; deploy subsystem integration on different operating systems Linux / Windows.

Keywords: automated information system, security of information transmission, allocated storage
distributed processing, interactive visualization, transport security, anticriminal security, technological security

References

1. Davis, K., 2012. Ethics of Big Data in 2012. Infinitesimal: O'Reilly Media. Vol.79.
2. Konheim, AG, 2007. Computer security and cryptography. BM: John Wiley & Sons, Inc. Vol. 542.
3. VS Gorbatov, O. P., 2011. Basics of PKI. BM: Hot Line - Telecom. Vol. 248.
4. Lowe, D., 2008. Programming WCF Services. BM: Peter. Vol.910.
5. McDonald, M., 2008. WPF. Windows Presentation Foundation in. NET 3.5 with examples in C # 2008 for Professionals (2nd edition). BM: Dialectics Williams. Vol. 922.
6. Burenin, A & Legkov, K 2011,' To a question of modeling of the organization of the information managing director of a network for a control system of modern infokommunikatsionny networks', H&ES: High technologies in space researches of Earth, vol. 3, no. 1, pp.22-25.

КОМПАНИЯ «ИНФОСИСТЕМЫ ДЖЕТ» РАСКРЫВАЕТ ПОДРОБНОСТИ ЗАЩИТЫ ПРОГРАММЫ МАЛИНА ОТ DDoS

9 июля 2013 г., г. Москва – Программа МАЛИНА (управляющая компания «Лоялти Партнерс Восток») и компания «Инфосистемы Джет» рассказали о подробностях успешного отражения одной из самых мощных в России DDoS-атак, целью которой стали ресурсы Программы. Атака состояла из нескольких этапов, была ориентирована на web-серверы и ряд инфраструктурных сервисов Программы. Ее продолжительность составила более двух суток, а объем нелегитимного трафика, направленного злоумышленниками на ресурсы Программы, превысил 40 Гбит в секунду.

Для эффективного отражения атаки и восстановления работы всех сервисов Программы в сжатые сроки была сформирована экспертная группа, в которую вошли специалисты Сервисного центра и Центра информационной безопасности компании «Инфосистемы Джет», обладающие необходимыми компетенциями. Был проанализирован характер трафика, сформированы и направлены провайдеру для последующей блокировки «черные списки» IP-адресов, с которых велась атака. Это позволило «сбить» первую волну DDoS. В дата-центре компании «Лоялти Партнерс Восток» был установлен межсетевой экран (Cisco ASA) и развернут программный комплекс мониторинга, проведена повторная диагностика сетевого трафика и установлено, что злоумышленники начали использовать подложные IP-адреса. Это потребовало оперативного подключения внешнего сервиса защиты от DDoS-атак – Kaspersky DDoS Prevention (KDP), который обеспечил максимальную фильтрацию поступающих запросов.

Принятые меры в совокупности позволили оперативно отразить DDoS-атаку и полностью восстановить работоспособность всех сервисов и сайтов компании.

«Данный случай можно считать своего рода показательным, наглядно продемонстрировавшим прямую зависимость между продуктивным решением бизнес-задач и эффективной организацией ИБ, – комментирует Евгений Акимов, заместитель директора Центра информационной безопасности компании «Инфосистемы Джет». – По итогам выполненных работ мы предложили компании «Лоялти Партнерс Восток» скорректировать комплексный план дальнейшего развития информационной безопасности с учетом таких задач, как защита публичных и внутренних сервисов, организация эффективного мониторинга и управления информационной безопасностью в режиме 24/7 на базе Jet Security Operation Center».

«Компания «Инфосистемы Джет» осуществляет комплексный аутсорсинг ИТ-инфраструктуры Программы МАЛИНА с 2006 года. В момент совершения атаки средства мониторинга работоспособности оборудования начали сигнализировать о чрезмерной нагрузке, эксперты Сервисного центра компании приняли оперативные меры и привлекли к дальнейшей работе специалистов Центра информационной безопасности. Вектор и способы атаки постоянно менялись, что требовало оперативных мер защиты, при этом особенно хочется отметить высокий уровень профессионализма наших партнеров в отражении DDoS-атаки, оперативность, нацеленность на результат и по-настоящему командную работу – это позволило совместными усилиями успешно отразить атаку», резюмирует Операционный директор компании «Лоялти Партнерс Восток» Денис Кручинин.

Компания «Инфосистемы Джет»
www.jet.msk.su

НЕКОТОРЫЕ МОДЕЛИ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Буренин А.Н., *к.т.н., доцент,*
Военно-космическая академия имени А.Ф. Можайского,
constz@mail.ru
Легков К.Е., *к.т.н.,*
Военно-космическая академия имени А.Ф. Можайского,
constl@mail.ru

Ключевые слова:
встраивание данных в видеоданные, скрытые каналы, стеганография, сигнальные последовательности Франка–Уолша, Франка-Крестенсона.

АННОТАЦИЯ

В статье показано, что функционирование современных инфокоммуникационных сетей специального назначения с высокими качественными показателями, может быть обеспечено только при решении комплекса задач управления их безопасностью.
Чрезвычайно сложная организация сетей, входящих в состав выделенной инфокоммуникационной сети (абонентские сети, сети доступа, транспортная сеть, сети услуг прикладного уровня), и механизмов их защиты приводят к тому, что возрастает число уязвимостей и потенциальных ошибок в использовании различных средств телекоммуникаций, а это обуславливают необходимость разработки достаточно мощных автоматизированных подсистем управления безопасностью.
В статье для описания атак приводятся различные модели, описывающие возможные варианты реализации атакующих действий противника с учетом его первоначального положения, уровня знаний и навыка, конфигурации самой инфокоммуникационной сети, а также реализуемой в ней политики безопасности.
На основе моделей в статье произведен анализ защищенности инфокоммуникационной сети, определены «узкие» места сети, выработаны рекомендации по устранению обнаруженных «дыр» безопасности, предлагаются модели программных комплексов, встроенных в архитектуру системы управления, позволяющих выявлять характер и интенсивность информационных воздействий на критически важные элементы сетей.

В настоящее время в составе выделенных систем связи специального назначения создается ряд телекоммуникационных сетей, образующих в своей совокупности инфокоммуникационную сеть, являющуюся фактически информационным и телекоммуникационным ядром соответствующей системы связи и предоставляющей различным пользователям требуемые услуги связи.. [1, 2].

Функционирование таких выделенных инфокоммуникационных сетей с высокими качественными показателями в условиях достаточно жестких требований, предъявляемых к ним со стороны пользователей информационных систем и автоматизированных систем управления, возможно только при решении целого комплекса задач обеспечения информационной безопасности. При этом решающая роль в этом вопросе отводится автоматизированной системе управления инфокоммуникационной сетью [4].

Возросшая сложность телекоммуникационных сетей, входящих в состав выделенной инфокоммуникационной сети (абонентские сети, сети доступа, транспортная сеть, сети услуг каждого уровня сети), и требуемых механизмов их защиты, увеличение количества уязвимостей, потенциальных ошибок в использовании различных средств телекоммуникаций, предоставления услуг и управления, а также возможностей потенциального нарушителя по реализации различного рода атак, обуславливают необходимость разработки достаточно мощных автоматизированных подсистем анализа атак и управления безопасностью выделенной инфокоммуникационной сетью, которые, в свою очередь, существенно повышают защищенность элементов сети и призваны выполнять задачи как по обнаружению состоявшихся фактов информационных воздействий, существующих ошибок в конфигурировании каждой сети, выявлению возможных атакующих действий различных категорий нарушителей, определению критичных сетевых ресурсов, так и подготовить данные по выбору адекватной программы управления безопасностью.

При решении различных задач обеспечения управления информационной безопасностью выделенной инфокоммуникационной сети используются понятия моделей атак, нарушителя, объекта атак (инфокоммуникационная сеть, элементы сети) и т.д. [5 – 16].

Модель атак используется для описания возможных действий противника и формирования сценариев реализации этих действий. Как правило [5, 6, 8, 11], модель имеет вид иерархической структуры, состоящей из нескольких уровней.

Верхними уровнями являются комплексный и сценарный уровни. Комплексный уровень определяет множество высокоуровневых целей процесса анализа защищенности (анализ на нарушение основных аспектов информационной безопасности: целостности, конфиденциальности, доступности) и множество анализируемых (атакуемых) объектов. На комплексном уровне может быть обеспечено согласование нескольких сценариев, которые реализуются группой нарушителей противника.

Сценарный уровень учитывает модель нарушителя (противника), определяет конкретный атакуемый объект выделенной инфокоммуникационной сети (АРМ ДЛ ПУ, сервер и т.д.) и цель атаки (например, «определение типа операционной системы АРМ», «реализация атаки отказа в обслуживании» и т.п.). Он содержит определенные этапы сценария, множество которых состоит из групп элементов: разведка, внедрение (первоначальный доступ к объекту атаки), повышение привилегий, реализация угрозы, сокрытие следов, создание потайных ходов.

Элементы сценарного уровня, расположенные ниже, служат для детализации целей, достигаемых реализацией данного сценария. Нижний уровень в иерархии концептуальной модели компьютерных атак описывает низкоуровневые атакующие действия нарушителя.

Модель нарушителя (противника) тесно связана с моделью атак. Их взаимосвязь состоит в том, что в модели атак содержится максимально полное описание возможных способов компрометации объектов выделенной инфокоммуникационной сети, а модель противника конкретизирует кто, какими средствами и с использованием каких знаний может реализовать данные угрозы и нанести ущерб тому или иному объекту сети. При этом сама модель должна учитывать основные параметры противника:

– первоначальное положение (внутренние и внешние нарушители);

– уровень знаний и умений, определяющий возможности противника, по реализации атакующих действий (задается перечнем известных противнику уязвимостей выделенной инфокоммуникационной сети, средств реализации атаки и т.п.);

– первичные знания об атакуемой выделенной инфокоммуникационной сети (например, в виде перечня АРМ ДЛ ПУ, коммутаторов, маршрутизаторов, серверов, пользователей и т.п.);

– используемый метод генерации сценария (используется ли оптимизация сценария для достижения заданной цели).

Для более подробного описания сценариев различных атак часто применяется модель формирования общего графа атак, которая служит для построения графовой модели, описывающей всевозможные варианты реализации атакующих действий противника с учетом его первоначального положения, уровня знаний и навыка, конфигурации выделенной инфокоммуникационной сети, реализуемой в ней политики безопасности.

На основе графа атак производится анализ защищенности выделенной инфокоммуникационной сети, определены «узкие» места сети, на основе чего могут быть выработаны рекомендации по устранению обнаруженных уязвимостей с учетом их уровня критичности и по управлению безопасностью.

В общем случае, при успешной реализации противником разведывательных действий, не происходит нарушения конфиденциальности, целостности и доступности информационных ресурсов выделенной инфокоммуникационной сети. Однако, возможно нарушение конфиденциальности, например, в том случае, если политикой безопасности в сети установлено, что информация о топологии той или иной внутренней сети выделенной инфокоммуникационной сети является закрытой. При успешном получении противником прав локального пользователя, возможности выполнения действий,

направленных на нарушение конфиденциальности, целостности и доступности, или на получение прав администратора увеличиваются, так как, например, он может нарушить конфиденциальность, целостность и доступность некоторой совокупности объектов сети, имея только права пользователя.

При успешном получении прав администратора на определенном АРМе или сервере противник может полностью нарушить конфиденциальность, целостность, доступность всех объектов данного узла выделенной инфокоммуникационной сети или даже ее фрагмента.

В направлении роста степени сложности все объекты выделенной инфокоммуникационной сети обычно упорядочиваются следующим образом: элементы сети → атакующие действия → трассы атак → угрозы → общий граф атак.

После реализации каждого из сценариев, принадлежащих множеству сценариев разведки, производится проверка условий выполнения атакующих действий, использующих уязвимости программного и аппаратного обеспечения элементов выделенной инфокоммуникационной сети. При успешной реализации атакующих действий заданной группы, приводящих к получению противником прав локального пользователя или администратора на атакованном АРМе или сервере, осуществляется проверка необходимости перехода противника (нарушителя) на данный элемент сети. В случае реализации перехода, эта же последовательность действий повторяется для нового положения противника.

Модель выделенной инфокоммуникационной сети служит для представления используемого в данной сети программного и аппаратного обеспечения, распознавания действий нарушителя и определения реакции сети на реализуемые противником атакующие действия. Для спецификации аппаратного и программного обеспечения обычно используется некоторый специализированный язык, использующий основные объектно-ориентированные технологии структурирования и концептуализации. При этом производится описание выделенной инфокоммуникационной сети на уровне ее топологии и сетевых сервисов. Сетевая топология описывается классами физических элементов сети, связанных физическими линиями (цифровыми каналами, трактами), а сетевые сервисы – классами электронная почта, файловый обмен, диалоговый режим и т.д.

В модель выделенной инфокоммуникационной сети обычно встраивается общая модель распознавания действий противника, которая позволяет осуществлять преобразование низкоуровневого представления атакующих действий (последовательности «ложных» сетевых пакетов или «ложных» команд для операционной системы) в высокоуровневые идентификаторы атак. Как правило, в основу этой модели закладывается механизм, реализующий сигнатурный метод – поступающая на вход модели выделенной инфокоммуникационной сети последовательность (поток) атакующих действий сравнивается с заранее определенными сигнатурами и, в случае обнаружения сходства, определяется высокоуровневый идентификатор атаки.

Другой моделью, используемой при решении задач обеспечения информационной безопасности выделенной инфокоммуникационной сети, является модель оценки уровня защищенности, которая охватывает определенную систему различных метрик безопасности и правил, используемых для их расчета и оценки. При этом множество всех метрик безопасности строится на основе уже рассмотренного сформированного общего графа атак. Метрики безопасности обычно характеризуют защищенность как базовых, так и составных объектов графа атак и классифицируются по разделению объектов общего графа атак на базовые и составные, в соответствии с порядком вычислений, в соответствии с тем, используются ли метрики для определения общего уровня защищенности выделенной инфокоммуникационной сети. Примерами метрик безопасности являются: критичность конкретного АРМа, сервера, коммутатора, маршрутизатора, размер ущерба при реализации угрозы, количество трасс атак на графе и т.д.

Во многих случаях для оценки уровня защищенности выделенной инфокоммуникационной сети может быть применен упрощенных экспресс метод так называемой интеллектуальной системы анализа [6], который состоит из следующих этапов: определение уровня критичности элементов выделенной инфокоммуникационной сети по упрощенной трехуровневой шкале (высокий, средний, низкий), определение критичности атакующих действий, определение размера ущерба, вызванного успешной реализацией атакующего действия, зависящего от уровней критичности действия и атакуемого элемента сети, определение размера ущерба для всех угроз, определение метрик сложности в доступе для всех атакующих действий во всех трассах с учетом значений данного показателя для каждого из действий, составляющих трассу, и всех угроз с учетом значений данного показателя для всех трасс, составляющих угрозу, определение степени возможности реализации угрозы на основе показателя сложности в доступе, определение общего уровня защищенности выделенной инфокоммуникационной сети на базе полученных оценок степени реализации угрозы и размера ущерба, вызванного ее успешной реализацией.

Традиционные методы защиты телекоммуникационных сетей в большей мере ориентированы на защиту от конкретных (известных или прогнозируемых) видов угроз и атак и реализуются в виде набора программных и аппаратных компонентов, функционирующих относительно независимо друг от друга. При этом существующие системы защиты обычно имеют централизованную структуру, характеризуются неразвитыми адаптационными возможностями, пассивными механизмами обнаружения атак, большим процентом ложных срабатываний при обнаружении вторжений, значительной деградацией трафика целевых информационных потоков из-за большого объема ресурсов, выделяемых на защиту и т. п.

Поэтому в последнее время появился другой перспективный подход к построению комплексных систем защиты информации в выделенных инфокоммуникационных сетях, позволяющий преодолеть некоторые из перечисленных недостатков. В основу его положена технология интеллектуальных мультиагентных систем, которая позволяет существенно по сравнению с традиционными методами повысить эффективность защиты информации, в том числе ее адекватность, отказоустойчивость, устойчивость к деструктивным действиям, универсальность, гибкость и т. д.

В соответствии с данным подходом предполагается, что компоненты систем защиты информации в выделенной инфокоммуникационной сети, специализированные по типам решаемых задач, тесно взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений, адаптируются к изменению трафика, реконфигурации аппаратного и программного обеспечения, а также новым видам атак.

В рамках предлагаемого подхода компоненты мультиагентной системы защиты информации представляют собой интеллектуальные автономные программы (агенты защиты), реализующие определенные функции защиты с целью обеспечения требуемого класса защищенности. Они позволяют реализовать комплексную надстройку над механизмами безопасности используемых сетевых программных средств, операционных систем и приложений, повышая защищенность сети до требуемого уровня.

Согласно этой технологии процесс создания мультиагентных систем для любой предметной области, в том числе защиты информации в выделенной инфокоммуникационной сети, предполагает решение двух высокоуровневых задач:
– создание «системного ядра» мультиагентной системы;
– клонирование программных агентов и отделение сгенерированной мультиагентной системы от «системного ядра».

В формальной модели и прототипе агентно-ориентированной системы моделирования атак, распределенные скоординированные атаки на выделенную инфокоммуникационную сеть должны рассматриваться в виде последовательности совместных действий агентов-противников, которые выполняются с различных элементов сети, в которые они заранее внедрены. Агенты противника координируют свои действия согласно некоторому общему сценарию. На каждом шаге сценария атаки они пытаются реализовать некоторую частную подцель.

Важным для решения задач обеспечения информационной безопасности выделенной инфокоммуникационной сети при воздействиях противника является математическое описание потоков информационных воздействий. Так как информационные воздействия противника на элементы выделенной инфокоммуникационной сети могут происходить в произвольные случайные моменты времени, интервалы между воздействиями также в общем случае являются случайными величинами, то последовательность информационных воздействий может быть математически описана моделью стохастического потока атак. Наиболее общим видом потока является рекуррентный поток, характерный тем, что интервалы времени между двумя информационными воздействиями независимы и имеют одинаковые произвольные функции распределения $F(t)$. Так простейший поток является частным случаем рекуррентного потока, у которого $F(t) = 1\text{-}e^{-x}$.

Вероятность того, что в интервале времени длительностью Δt поступит ровно k воздействий, равна

$$P_k(\Delta t) = \int_0^{\Delta t} P_{k\text{-}1}(\Delta t - x)\, dF(x) \qquad (1)$$

Ясно, что $P_0(0) = 1\text{-}F(\Delta t)$.

Математическое ожидание числа требований рекуррентного потока информационных воздействий на выделенную инфокоммуникационную сеть, приходящихся на интервал длиной Δt, определяется формулой:

$$m(\Delta t) = \int_0^{\Delta t} \left[1 + m(\Delta t - x)\right] dF(x) = F(\Delta t) + \int_0^{\Delta t} m(\Delta t - x) dF(x) \qquad (2)$$

Если вероятность нулевой длительности промежутка между информационными воздействиями противника недостаточно мала, то замена такого интервально-рекуррентного потока простейшим приведет к заметным ошибкам. Интервально-рекуррентный поток с такими функциями распределения промежутков времени между двумя требованиями «хуже» пуассоновского, поэтому получаемую интенсивность эквивалентного потока при управлении безопасностью выделенной инфокоммуникационной сети можно увеличить на величину, полученную на основе моделирования.

Математическое описание потоков информационных воздействий позволяет обоснованно осуществлять в контуре системы управления выделенной инфокоммуникационной сетью моделирование программно-аппаратных атак в соответствии с предполагаемыми угрозами, которые в настоящее время существуют в арсенале потенциального противника и известны создателю и обслуживающему персоналу сети. При этом удобно осуществлять моделирование атак в рамках агентов системы управления, реализованных во всех без исключения элементах выделенной инфокоммуникационной сети (АРМ, серверах, коммутаторах, маршрутизаторах и др.), путем придания им дополнительных функций по генерированию образов программных агентов, реализующих различные компоненты программно-аппаратных атак. Менеджеры же системы управления будут выступать в качестве агентов, имитирующих организацию комплексов атак. Эти же компоненты системы управления будут выполнять функции компонент мультиагентной системы обеспечения информационной безопасности сети, каждый из которых реализует вполне конкретные функции защиты. При этом периодически осуществляется сравнение множества многомерных векторов состояния контролируемых параметров после имитационного (тестового) воздействия с реально фиксируемым вектором состояния во время функционирования выделенной инфокоммуникационной сети.

Литература

1. Легков, К.Е. О некоторых подходах к повышению эффективности системы управления в рамках изменения подхода к автоматизации и информации / К.Е. Легков // Мобильные телекоммуникации (Mobile Communications). – 2013. – № 7. – С. 48.
2. Легков, К.Е. Основные теоретические и прикладные проблемы технической основы системы управления специального назначения и основные направления создания инфокоммуникационной системы специального назначения/ К.Е. Легков // T-Comm: Телекоммуникации и транспорт. – 2013. – Т. 7, № 6. – С. 42–46.

3. Легков, К.Е. Процедуры и временные характеристики оперативного управления трафиком в транспортной сети специального назначения пакетной коммутации/ К.Е. Легков // T-Comm: Телекоммуникации и транспорт. – 2012. – Т. 6, №6. – С. 22–26.
4. Легков, К.Е. Вероятность потери пакета в беспроводных сетях со случайным множественным доступом к среде передачи/ К.Е. Легков, А.А. Донченко // T-Comm: Телекоммуникации и транспорт. – 2011. – Т. 5, № 5. – С. 32–33.
5. Легков, К.Е. Современные технологии беспроводного широкополосного доступа 802.16E и LTE: перспективы внедрения на транспорте/ К.Е. Легков, А.А. Донченко, В.В. Садовов // T-Comm: Телекоммуникации и транспорт. – 2010. – Т. 4, № 2. – С. 30–32.
6. Легков, К.Е. Беспроводные MESH сети специального назначения / К.Е. Легков, А.А. Донченко // T-Comm: Телекоммуникации и транспорт. – 2009. – Т. 3, № 3. – С. 36–37.
7. Легков, К.Е. Анализ систем передачи в сетях беспроводного доступа / К.Е. Легков, А.А. Донченко // T-Comm: Телекоммуникации и транспорт. – 2009. – Т. 3, № 2. – С. 40–41.
8. Легков, К.Е. Эффективные методы управления потоками в защищенных инфокоммуникационных сетях / А.Н. Буренин, К.Е. Легков // H&ES: Наукоемкие технологии в космических исследованиях Земли. – 2010. –№ 2. – С. 29-34.
9. Легков, К.Е. Модели процессов мониторинга при обеспечении оперативного контроля эксплуатации инфокоммуникационных сетей специального назначения / А.Н. Буренин, К.Е. Легков // H&ES: Наукоемкие технологии в космических исследованиях Земли. – 2011. –№ 2. – С. 19-23.
10. Легков, К.Е. К вопросу моделирования организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями / А.Н. Буренин, К.Е. Легков // H&ES: Наукоемкие технологии в космических исследованиях Земли. – 2011. – № 1. – С. 22-25.

SOME MODELS OF SECURITY MANAGEMENT INFOCOMMUNICATION NETWORKS OF THE SPECIAL PURPOSE

Burenin A., Ph.D, Military Space Academy, constz@mail.ru
Legkov K., Ph.D, Military Space Academy, constl@mail.ru

Abstract
In article it is shown that functioning of the modern infocommunication networks of a special purpose with high quality indicators, can be provided only in case of the solution of a complex of tasks of control with their safety.
Extremely difficult organization of the networks which are a part of the selected infocommunication network (subscriber premises networks, access networks, a transport network, networks of services of the application layer), and mechanisms of their protection lead to that the number of vulnerabilities and potential errors increases in use of different means of telecommunications, and it powerful automated subsystems of security management cause need of development enough.
The different models describing possible options of implementation of attacking actions of the opponent taking into account his original situation, level of knowledge and skill, configuration of the most infocommunication network, and also trust relationships policy implemented in it are given in article for the description of attacks.
On the basis of models in article the analysis of security of an infocommunication network is made, "narrow" places of a network are defined, recommendations about elimination of found "holes" of safety are worked out, models of the program complexes which have been built in a system architecture of control, allowing to reveal character and intensity of information impacts on crucial elements of networks are offered.
Keywords: embedding of data to video these, hidden canals, a steganografiya, Frank-Walsh, Frankayokrestenson's alarm sequences.

References
1. Legkov, K 2013, 'About some approaches to increase of system effectiveness of control within change of approach to automation and information', Mobile telecommunications (Mobile Communications), no. 7, p. 48.
2. Legkov, K 2013, 'Main theoretical and application-oriented problems of a technical basis of management system of a special purpose and main directions of creation of infocommunication system of special assignment', T-Comm: Telecommunications and transport, vol. 7, no. 6, pp. 42-46.
3. Legkov, K 2012, 'Procedures and time response characteristics of operational management of traffic on the transport network of a special purpose of package switching', T-Comm: Telecommunications and transport, vol. 6, no. 6, pp. 22-26.
4. Legkov, K & Donchenko, A 2011, 'Veroyatnost of loss of a packet on the wireless networks with accidental multiple access to the environment transmission', T-Comm: Telecommunications and transport, vol. 5, no. 5, pp. 32-33.
5. Legkov, K & Donchenko, A & Sadovov, V 2010, 'The modern technologies of broadband wireless access 802.16E and LTE: implementation perspectives on transport', T-Comm: Telecommunications and transport, vol. 4, no. 2, pp. 30-32.
6. Legkov, K & Donchenko, A 2009, 'Wireless MESH networks of a special purpose', T-Comm: Telecommunications and transport, vol.3, no. 3, pp. 36-37.
7. Legkov, K & Donchenko, A 2009, 'The analysis of transmission systems on networks of wireless access', T-Comm: Telecommunications and transport, vol. 3, no. 2, pp. 40-41.
8. Burenin, A & Legkov, K 2010, 'Effective methods of control over streams in protected infokommunikatsionny networks', H&ES: High technologies in space researches of Earth, vol.2, no.2, pp. 29-34.
9. Burenin, A & Legkov, K 2011, 'Model of monitoring processes when ensuring operative control of operation of infokommunikatsionny networks of special purpose', H&ES: High technologies in space researches of Earth, vol. 3, no. 2, pp. 19-23.
10. Burenin, A & Legkov, K 2011,' To a question of modeling of the organization of the information managing director of a network for a control system of modern infokommunikatsionny networks', H&ES: High technologies in space researches of Earth, vol. 3, no. 1, pp. 22-25.

«БОРЛАС» ДОБАВИТ К ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННУЮ

Москва, 16 июля 2013 года. – Один из крупнейших системных интеграторов дополнит продуктовое предложение решениями от лидера рынка защиты от внутренних угроз.

Консалтинговая группа «Борлас» и группа компаний InfoWatch сообщают о заключении стратегического партнерского соглашения, согласно которому продуктовый портфель «Борласа» будет расширен за счет услуг поставки и внедрения решений InfoWatch в области защиты от внутренних угроз. Они дополнят экспертизу компании в области технической безопасности, благодаря чему «Борлас» сможет создавать комплексные системы безопасности, обеспечивающие защиту от всех видов угроз.

Группа «Борлас» обладает многолетней экспертизой в области построения систем управления финансами, производством и персоналом, благодаря чему специалисты компании досконально изучили принципы организации, хранения и движения информации в них. Совмещая экспертные знания в данной сфере с возможностями передовых решений InfoWatch, «Борлас» сможет обеспечивать высокий уровень безопасности корпоративной информации российских заказчиков, в том числе в рамках комплексных проектов.

Создание эффективных систем безопасности возможно только при системном подходе к их организации, это означает, помимо прочего, создание механизмов защиты от различных угроз: и физических, и информационных. В течение последних лет группа «Борлас» в лице дочерней компании «Борлас Секьюрити Системз» является заметным игроком рынка средств технической безопасности, поставляя специализированное оборудование и услуги. Расширение портфеля ИБ-решениями от InfoWatch позволит создавать системы безопасности, обеспечивающие защиту информационных активов от внутренних угроз.

Согласно подписанному соглашению «Борлас» сможет продавать и обеспечивать услуги по внедрению на территории России следующих продуктов InfoWatch:

- InfoWatch Traffic Monitor – DLP-система, предназначенная для контроля информационных потоков, защиты конфиденциальной информации от утечки и несанкционированного распространения;
- InfoWatch KRIBRUM – облачный сервис мониторинга социальных медиа и управления репутацией в Интернете в режиме реального времени;
- InfoWatch APPERCUT – продукт для автоматического аудита исходного кода заказных бизнес-приложений на предмет наличия уязвимостей и закладок.

«Мы отмечаем интерес ряда клиентов к получению максимально широкого спектра решений и услуг в области обеспечения безопасности. Именно поэтому в дополнение к нашей традиционно сильной области – специальным технологиям безопасности, мы развиваем направление информационной безопасности. Партнерство с InfoWatch расширит наши возможности создания «под ключ» комплексных систем, включающих технические системы безопасности и решения для противодействия утечкам информации и киберпреступности. Такой подход и наличие необходимой экспертизы, безусловно, будет выделять нашу компанию на рынке», – говорит директор департамента систем безопасности консалтинговой группы «Борлас» Андрей Прозоров.

«Комплекс решений InfoWatch, по которым «Борлас» будет развивать экспертизу, сформирован таким образом, чтобы максимально точно детектировать и предотвращать все угрозы, идущие изнутри организации, – комментирует Константин Левин, директор по продажам компании InfoWatch. – Мы считаем, что у нашего сотрудничества с группой «Борлас» очень хорошие перспективы, и планируем совместно расширить применение продуктов InfoWatch не только в государственном, финансовом и нефтегазовом секторе, где они уже хорошо представлены, но и тех отраслях, где мы видим большой потенциал для развития, например в ОПК».

ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ МАТЕРИАЛОВ

Предоставляемая для публикации статья должна быть актуальной, обладать новизной, отражать постановку задачи, содержать описание основных результатов исследования, выводы, а также соответствовать указанным ниже правилам оформления. Текст должен быть тщательно вычитан автором, который несет ответственность за научно- теоретический уровень публикуемого материала.

1. Статья подготавливается в редакторе MS Word.
2. Формульные выражения выполняются во встроенном формульном редакторе MS Word 2003 или в редакторе Math Type. Также в отдельной папке должны содержаться экспортированные изображения формул в формате TIFF (качество изображений не менее 600 dpi). Названия файлов должны соответствовать номерам формул в статье (например: Формула 2-1.tiff).
3. Объём статьи с аннотацией – от 10 до 20 тыс. знаков. Рисунки и таблицы в объеме статьи не учитываются.
4. Объем аннотации 250-300 слов. Аннотация должна быть информативной (не содержать общих слов), структурированной, отражать основное содержание статьи: предмет, цель, методологию проведения исследований, результаты исследований, область их применения, выводы. Приводятся основные теоретические и экспериментальные результаты, фактические данные, обнаруженные взаимосвязи и закономерности. Выводы могут сопровождаться рекомендациями, оценками, предложениями, гипотезами, описанными в статье.
5. Ключевые слова (не менее пяти).
6. фамилия, имя, отчество всех авторов полностью, полное название организации – места работы каждого автора, почтовый адрес, должность, звание, ученая степень каждого автора, адрес электронной почты для каждого автора.
7. Список литературы не менее пяти наименований, для статей – с указанием страниц, для книг – с указанием общего числа страниц в книге, для интернет-сайта – с указанием даты обращения.
8. Формулы нумеруются в круглых скобках, источники – в прямых. Нумерация формул и приведение в списке источников, на которые нет ссылок по тексту, не допускается.
9. На английском языке предоставляется: название статьи, для каждого автора имя и фамилия, место работы, должность, электронный адрес, аннотация, ключевые слова и списки литературы (по стандарту Harvard).
10. Статья предоставляется в электронном виде, единым файлом, имеющим следующую структуру: заглавие статьи, сведения об авторах, ключевые слова, аннотация, текст статьи (включая иллюстрации, таблицы и формулы), пристатейный список литературы, англоязычный блок. Также представляется отдельная папка с экспортированными изображениями формул в формате TIFF, по требованиям указанным в п.2.
11. К статье прилагается экспертное заключение о возможности опубликования статьи в открытой печати и две рецензии кандидатов или докторов наук по профилю планируемой публикации материалов.

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

MANUSCRIPT REQUIREMENTS

Format

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

Author Details (in English and native language)

Details should be supplied on the Article Title Page including:

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

It is appropriate to describe the research methods/methodology if they are original or of interest for this particular research. For papers concerned with experimental work describe your data sources and data procession technique.

Describe your results as precisely and informatively as possible. Include your key theoretical and experimental results, factual information, revealed interconnections and patterns. Give special priority in your abstract to new results and long-term impact data, important discoveries and verified findings that contradict previous theories as well as data that you think have practical value.

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

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

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

Keywords (in English and native language)

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

Figures

All figures should be of high quality, legible and numbered consecutively with arabic numerals. All figures (charts, diagrams, line drawings, web pages/screenshots, and photographic images) should be submitted in electronic form preferably in color as separate files, that match the following parameters:

References

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