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 VI
No. 6-2013

Наукоёмкие технологии в космических исследованиях Земли

СОДЕРЖАНИЕ

CONTENTS

Vol. V
No. 6-2013

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

МТС и Билайн не готовы к предоставлению услуг по сохранению номера при переходе от одного оператора связи к другому

МТС и Билайн не готовы к предоставлению услуг по сохранению номера при переходе от одного оператора связи к другому

Два российских оператора сотовой связи из «большой тройки» не будут готовы принять к 1 декабря абонентов, которые захотят сменить оператора с сохранением номера. Об этом пишут «Известия» со ссылкой на протокол закрытого заседания представителей Минкомсвязи и ЦНИИСа (Центральный НИИ Связи, который правительство назначило оператором базы перенесенных номеров).

К назначенной дате отмены «мобильного рабства» (1 декабря) не успевают МТС и «ВымпелКом». Операторы объясняют это недостатком внутренних ресурсов и медлительностью подрядчиков.

«МегаФон» и «Tele2 Россия» успевают в срок. Сообщается, что они уже с 1 ноября начали межоператорские испытания MNP (Mobile Number Portability), 14 ноября к ним присоединится «Ростелеком». «ВымпелКом» будет готов к испытаниям не ранее начала следующего года, а МТС пока не может сообщить дату готовности к межоператорским тестам.

Как отметили представители двух неуспевающих операторов, главным препятствием для переносимости номеров является неготовность законодательства. Пресс-секретарь «ВымпелКома» Анна Айбашева отметила, что «ВымпелКом» как публичная компания всегда выполняет требования законодательства. И мы готовим свою сеть к выполнению требований закона о MNP». Оператор ожидает принятия всех нормативно-правовых актов, чтобы обеспечить качественную реализацию услуги по переносимости.

Глава пресс-службы МТС Дмитрий Солодовников отметил, что техническая готовность операторов вторична по отношению к готовности нормативно-правовой базы: «До сих пор нет приказа Минкомсвязи, основного документа, который определяет организационно-техническое взаимодействие всех участников процесса. Также не решены вопросы интеграции платежных систем, что может вызвать задержки при пополнении счетов перенесенных номеров. Не решен вопрос взаимодействия с операторами фиксированной связи. Для межоператорского тестирования регулятор должен разработать его расширенную методику».

В предыдущем номере журнал писал, что услуга по сохранению номера при переходе от одного оператора связи к другому может появиться у операторов лишь в середине марта 2014 года, хотя ранее озвучивался другой срок — 1 декабря 2013 года. Ранее против отмены «мобильного рабства» выступало Минэкономразвития, которое ссылалось на то, что в Европе соответствующий сервис не пользуется популярностью. Кроме этого, против сервиса по переносу номера выступали и сами операторы сотовой связи — его внедрение очень дорого и никогда не окупится.

Напомним, закон, который позволит сохранять за собой номер мобильного телефона при переходе к другому оператору, был подписан Владимиром Путиным в самом конце прошлого года. Согласно ему, стоимость сохранения номера для физических лиц не должна превышать 100 рублей, а перенос должен осуществляться в течение девяти дней.

Delphi за безопасность на дорогах

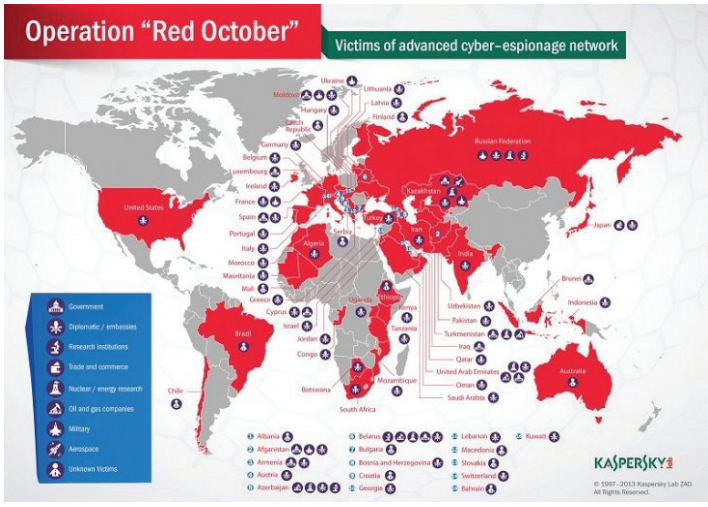
Продолжая свою работу в направлении обеспечения безопасности дорожного движения, компания Delphi на Международной выставке CES 2013 в Лас-Вегасе продемонстрировала технологию «MyFi® – безопасное подключение», которая позволяет водителю не отвлекаться от управления автомобилем для получения необходимой информации.

Компания Delphi разработала интерфейс человек-машина (human-machine interface – HMI), позволяющий выводить всю важную информацию на высокорасположенный прозрачный дисплей в поле зрения водителя и обеспечивающий управление всеми основными функциями с помощью кнопок на руле или системы распознавания голоса. Стоит сказать, что водитель сам выбирает необходимую для вывода на дисплей информацию.

«Мы считаем, что безопасность движения достигается в случае, когда взгляд водителя направлен на дорогу, руки он держит на руле и сосредоточен на управлении автомобилем», — утверждает Джеффри Джей Оуенс, исполнительный вице-президент и главный технический директор. — «Обеспечивая водителям возможность удерживать руль в руках в то время, когда они знакомятся с нужной информацией, мы гарантируем им безопасность».

Технология активно регулирует функциональность устройств, опираясь на реальные условия. Например, система MyFi® контролирует дорожное движение и текстовые сообщения, получаемые водителем, но при интенсивном движении водитель должен быть сосредоточен на управлении автомобилем и система активной безопасности не будет воспроизводить вслух полученные сообщения.

Кибероперация «красный октябрь»



«Лаборатория Касперского» опубликовала отчет об исследовании масштабной кампании, проводимой киберпреступниками с целью шпионажа за дипломатическими, правительственными и научными организациями в различных странах мира. Действия злоумышленников были направлены на получение конфиденциальной информации, данных, открывающих доступ к компьютерным системам, персональным мобильным устройствам и корпоративным сетям, а также сбор сведений геополитического характера. Основной акцент атакующие сделали на республиках бывшего СССР, странах Восточной Европы, а также ряде государств в Центральной Азии.

В октябре 2012 года эксперты «Лаборатории Касперского» начали расследование серии атак на компьютерные сети международных дипломатических представительств. В процессе изучения этих инцидентов специалисты обнаружили масштабную кибершпионскую сеть. По итогам ее анализа эксперты «Лаборатории Касперского» пришли к выводу, что операция под кодовым названием «Красный октябрь» началась еще в 2007 году и продолжается до сих пор.

Основной целью киберпреступников стали дипломатические и правительственные структуры по всему миру. Однако среди жертв также встречаются научно-исследовательские институты, компании, занимающиеся вопросами энергетики, в том числе ядерной, космические агентства, а также торговые предприятия. Создатели «Красного октября» разработали собственное вредоносное ПО, имеющее уникальную модульную архитектуру, состоящую из вредоносных расширений, модулей, предназначенных для кражи информации. В антивирусной базе «Лаборатории Касперского» данная вредоносная программа имеет название Backdoor.Win32.Sputnik.

Для контроля сети зараженных машин киберпреступники использовали более 60 доменных имен и серверы, расположенные в различных странах мира. При этом значительная их часть размещалась на территории Германии и России. Анализ инфраструктуры серверов управления, проведенный экспертами «Лаборатории Касперского», показал, что злоумышленники использовали целую цепочку прокси-серверов, чтобы скрыть местоположение главного сервера управления.

Преступники похищали из зараженных систем информацию, содержащуюся в файлах различных форматов. Среди прочих эксперты обнаружили файлы с расширением acid*, говорящим об их принадлежности к секретному программному обеспечению Acid Cryptofiler, которое использует ряд организаций, входящих в состав Европейского Союза и НАТО.

Для заражения систем преступники использовали фишинговые письма, адресованные конкретным получателям в той или иной организации. В состав письма входила специальная троянская программа, для установки которой письма содержали эксплойты, использовавшие уязвимости в Microsoft Office. Эти эксплойты были созданы сторонними злоумышленниками и ранее использовались в различных кибератаках, нацеленных как на тибетских активистов, так и на военный и энергетический секторы ряда государств азиатского региона.

Для определения жертв кибершпионажа эксперты «Лаборатории Касперского», анализировали данные, полученные из двух основных источников: облачного сервиса Kaspersky Security Network (KSN) и sinkhole-серверов, предназначенных для наблюдения за инфицированными машинами, выходящими на связь с командными серверами.

Значительная часть зараженных систем была обнаружена в странах Восточной Европы. В период со 2 ноября 2012 года по 10 января 2013 было зафиксировано более 55000 подключений с 250 зараженных IP-адресов, зарегистрированных в 39 странах. Большинство соединений, установленных с зараженных IP-адресов, были зафиксированы в Швейцарии, Казахстане и Греции.

Киберпреступники создали мультифункциональную платформу для совершения атак, содержавшую несколько десятков расширений и вредоносных файлов, способных быстро подстраиваться под разные системные конфигурации и собирать конфиденциальные данные с зараженных компьютеров.

К наиболее примечательным характеристикам модулей можно отнести:

- Модуль восстановления, позволяющий преступникам «воскрешать» зараженные машины. Модуль встраивается как плагин в Adobe Reader и Microsoft Office и обеспечивает атакующим повторный доступ к системе в случае, если основная вредоносная программа была детектирована и удалена или если произошло обновление системы.
- Возможность инфицирования мобильных устройств: помимо заражения традиционных рабочих станций это вредоносное ПО способно красть данные с мобильных устройств, в частности смартфонов. Также злоумышленники могли красть информацию о конфигурации с сетевого промышленного оборудования (маршрутизаторы, коммутационные устройства) и даже удаленные файлы с внешних USB-накопителей.

Регистрационные данные командных серверов и информация, содержащаяся в исполняемых файлах вредоносного ПО, дают все основания предполагать наличие у киберпреступников русскоязычных корней.

Популярные заблуждения о бюджетных смартфонах

Россияне с середины 2000-х готов насмотрелись на низкокачественные китайские подделки под мощные смартфоны. У значительной части населения России «бюджетный смартфон» по-прежнему ассоциируется с огромными бестолковыми аппаратами а-ля «двухсимочный айфон на Android со встроенным телевизором и выдвижной антенной». Однако сегодня можно с уверенностью сказать, что большинство стереотипов о недорогих мобильниках — только мифы. Не верите? Читайте дальше!

1. «Смартфоны нераскрученных марок по характеристикам уступают моделям от крупных производителей».

Утверждение, которое кажется очевидным, на самом деле миф. Действительно, суперчеткие дисплеи и невероятно мощные процессоры, а также невероятно важные инновации типа разблокировки постукиванием и прокручивания страниц глазами появляются в первую очередь в смартфонах крупнейших мировых производителей. Однако через какое-то время (скажем, 3—4 месяца спустя) практически все действительно «крутые», полезные и применимые на практике фишки из арсенала флагманов «крутых» марок появляются и в бюджетных аналогах.

Пример из жизни: в конце 2012 года появились первые смартфоны с суперчеткими Full HD дисплеями, средняя их цена была в районе 25 000 рублей. При этом задействованные в данных моделях процессоры плохо справлялись с поддержкой такого высокого разрешения дисплея, поэтому аппараты заметно «притормаживали» при работе с ресурсоемкими приложениями и играми.

В середине 2013 года в продаже появляется первый в России «бюджетный» аппарат с Full HD дисплеем — Highscreen Alpha R. Работа 5-дюймового суперчеткого экрана, обеспечивается более подходящим турбированным («разогнанным») 4-ядерным процессором MediaTek MT6589T. Highscreen Alpha R комплектуется двумя сменными аккумуляторами (2000 и 4000 мАч), которые, несмотря на «суперпрожорливый» в плане энергопотребления экран, обеспечивают смартфону целую неделю автономной работы. Цена — 12 990 рублей, аналогов от именитых брендов с таким же дисплеем, процессором и неделей работы без подзарядки в продаже попросту нет. Да, у крупнейших производителей достаточно Full HD моделей. Но, во-первых, там установлены существенно более слабые аккумуляторы, а во-вторых, стоят такие устройства минимум на 20—30% (то есть на 3—4 тысячи рублей) дороже, чем Highscreen Alpha R. В стоимость продукции именитых производителей все-таки закладывается значительная наценка «за бренд». Разумно ли переплачивать столько за «брендовость» устройства? Тут каждый решает для себя сам.

2. «У бюджетных смартфонов не бывает технических «фишек».

Выше мы рассказали о преемственности передовых технологий. Хорошо, малоизвестные бренды в состоянии сделать более дешевые технические аналоги крутых флагманов мировых брендов. Но как насчет собственных «фишек», есть ли в арсенале у недорогих моделей что-то такое, чего нет у самых дорогих и раскрученных смартфонов?

Кое-что точно есть. Первый пример приведен выше. Возможность работы с двумя сменными аккумуляторами различной емкости — такую функциональность пока не предлагает ни один «топовый» бренд смартфонов. Впервые она появилась именно в устройстве Highscreen Alpha R. Производитель процессора этого устройства — тайваньский MediaTek — даже проводил специальную программную доработку своей платформы, чтобы обеспечить возможность установки в смартфон попеременно двух батарей разной емкости без увеличения общего энергопотребления устройства.

Highscreen по-прежнему единственный в России производитель смартфонов с целой линейкой «долгоиграющих» моделей. Практически каждый современный «умный телефон» (даже самый дорогой) полностью разряжается за 1-2 дня использования, в то же время «живучие» аппараты Highscreen могут обходиться без подзарядки неделю и даже две!

Первый «долгоиграющий» смартфон в России — Highscreen Boost — вышел в начале 2013 года, но до сих пор остается одной из самых популярных моделей на нашем рынке. Секрет успеха прост: аккумулятор сверхбольшой емкости (4160 мАч) обеспечивает до недели работы на одном заряде батареи. Ну, и, конечно же, весьма аппетитная цена — 6990 рублей. Продолжением линейки летом 2013 года стал уже дважды упомянутый выше Higshcreen Alpha R.

Наконец, «венцом» развития темы долгоиграющих смартфонов Highscreen стал вышедший в октябре Highscreen Boost 2, первый во всем мире смартфон с двумя неделями работы без подзарядки. Аналогов этому аппарату нет нигде в мире, ни у одного «топового» производителя телефонов. Создатели даже подали заявку в Книгу Рекордов Гиннесса на официальное присвоение Highscreen Boost 2 статуса «смартфона с самым большим сроком автономной работы в мире».

3. «Все смартфоны российских брендов — на 100% китайские аппараты».

Частично правдивое утверждение. Для многих российских компаний принцип «купить в Китае, просто поставить свой логотип, продать

в России, но уже дороже» остается основной бизнес-моделью. Но есть и исключения.

Highscreen сотрудничает с китайскими производителями, но по несколько иному сценарию: азиатские партнеры предлагают «полуфабрикаты» — смартфоны с базовым набором характеристик. Инженеры Highscreen оценивают предложенные варианты и предлагают свои инструкции: частоту процессора — поднять, аккумулятор заменить, камеру поставить с более высоким разрешением, а вместо дешевого глянцевого пластика использовать более прочный и менее маркий матовый.

Например, у описанного выше «долгоиграющего» бюджетного смартфона с недельной «автономкой» Highscreen Boost 1,4-гигагерцевый процессор Qualcomm, 1 ГБ оперативной памяти, 1,3-мегапиксельная фронтальная камера и экран от японской Sharp. При этом в продаже есть аналогичный внешне и по многим характеристикам смартфон другого локального бренда. Однако в конкурирующей модели процессор на 1,2 ГГц, Android 4.0, и только 768 МБ «оперативки», камера на 0,3 Мп и недорогой дисплей от китайской фабрики.

Как так вышло? Дело в том, что Highscreen действительно участвует в разработке устройств и доведении до ума их спецификаций, тогда как многие компании просто используют то, что им предложили китайцы. Главная цель любой китайской фабрики — сделать максимально дешевый аппарат и продать с максимальной выгодой для себя. Объяснять пользователям, почему в новом смартфоне тормозит даже меню, а модуль камеры снимает только мутные фотографии, предстоит не им, а их русским партнерам.

4. «Я лучше закажу телефон из Китая напрямую и сэкономлю!»

Частично верно. Совершая покупку в китайском интернет-магазине, вы экономите деньги, но повышаете для себя риск «нарваться на проблемы». Какие?

Во-первых, сложности с гарантийным обслуживанием. Даже если продавец утверждает, что готов оперативно заменить бракованный или сломанный аппарат, отправка гаджета обратно в Китай на ремонт займет как минимум месяц, и столько же аппарат будет ехать обратно. Посылку могут не принять на почте или потерять, потому что отправка осуществляется обычной бандеролью. Посылку могут остановить на таможне.

Кроме того, китайцы могут запросто отказать вам в обмене. Наш «Закон о защите прав потребителей» на магазины, зарегистрированные в других государствах, не распространяется. Поэтому все, что вы можете сделать обманувшему вас китайцу — написать гневный отзыв в интернете. Не густо, правда?

Во-вторых, могут возникнуть проблемы соответствия аппарата российским сотовым сетям. Часто бывает такое, что приехавший из Китая аппарат поддерживает GSM, а вот с российским вариантом 3G-сетей — W-CDMA — не дружит. И даже китайские смартфоны, рассчитанные на сети W-CDMA, не всегда совместимы с нашими диапазонами или могут работать некорректно. Их ведь никто не тестировал в условиях сетей российских операторов сотовой связи!

И, наконец, в-третьих, аппараты для внутреннего рынка Китая часто не имеют установленного клиента приложений Google Play — его заменяют китайскими аналогами, которые в России, естественно, бесполезны. Также может отсутствовать поддержка русского языка в интерфейсе.

Это все, конечно, поправимо, если «руки растут оттуда, откуда надо» и есть возможность и желание просидеть парочку дней и ночей на специфических форумах, выискивая советы по «допиливанию китайца» до приемлемого уровня. Но большинство обычных людей найдет тысячу более интересных занятий, чем перепрошивка смартфонов. Именно на них, нормальных, живых, не повернутых на электронике пользователей и рассчитаны продукты таких брендов, как Highscreen, которые уже довели свои аппараты до кондиции и полного соответствия специфике нашего отечественного рынка и всем запросам российского потребителя.

5. «Я лучше куплю старую или б/у модель известной марки, чем новый "бюджетник"».

Предпочесть модель, заведомо уступающую по техническим характеристикам менее раскрученным «бюджетникам» с такой же ценой — весьма популярное решение. Каждый решает сам, готов ли он платить за реальную полезность и функциональность смартфона или за модный логотип на корпусе. Главный вопрос — удастся ли вам произвести на кого-то впечатление устаревшим аппаратом, пусть и популярной торговой марки? Скорее всего, нет. Иначе люди не сдавали бы в ломбарды в таком количестве iPhone предыдущего поколения при выходе новых моделей вожделенного бренда.

Бывшие в употреблении аппараты — всегда риск: велика вероятность, что продаваемый на барахолке аппарат не так уж хорош, как описывает его продавец. «Впарить» могут что угодно, начиная с «утопленных» или отремонтированных (причем многократно) аппаратов до моделей, привезенных из-за рубежа и вообще нормально не работающих в российских сотовых сетях. Уверены ли вы, что хотите в случае каких-то проблем караулить продавшего вам с рук негодный аппарат человека, обрывать ему телефон и изыскивать все возможные способы вернуть свои деньги? Скорее всего, нет. Как и большинство людей, которые все-таки предпочитают пресловутому «коту в мешке» пойти в магазин и купить новенький аппарат без каких-либо изъянов и с нор-

мальной гарантией. По крайне мере купленный в крупном магазине аппарат известного российского бренда всегда можно сдать или обменять — «Закон о защите прав потребителей» в нашей стране никто не отменял.

6. «Ни один бюджетный телефон не стоит своих денег!»

Не верно. Не так давно очень интересное исследование на эту тему опубликовали в одном из старейших и авторитетнейших российских компьютерных журналов. Собственная разработка редакции, аналитическая программа «Гид Покупателя» на основе системы искусственного интеллекта, оценивает соотношение функциональности и цены всей актуальной линейки гаджетов каждого конкретного бренда по 10-балльной шкале. И в итоге составляет рейтинг производителей. Важно отметить, что рейтинг отражает не уровень технической оснащенности гаджетов той или иной марки, не абсолютную «продвинутость» характеристик, не объемы продаж и долю рынка, а именно сбалансированность предлагаемых моделей — соответствие реальной полезности предлагаемых аппаратов запрошенным за них ценам. Иными словами, был дан ответ на вопрос «насколько гаджеты каждого бренда стоят своих денег?».

По итогам данного исследования бренд бюджетных смартфонов Highscreen получил 9 из 10 баллов и вошел в топ-5 с крупнейшими производителями смартфонов.

7. «У всех бюджетных смартфонов скучный дизайн».

Отчасти правда. Подавляющее большинство бюджетных смартфонов из ценовой категории до 10 тысяч рублей — скучные и однотипные плоские «лопаты» с черными, белыми и (в редких случаях) серебристыми корпусами. Однако и тут есть исключения.

В конце 2013 года в России начали продавать смартфон Highscreen Omega Prime Mini, в комплекте с которым поставляется аж пять разноцветных сменных задних панелей. Переставлять яркие «задники» красного, белого, черного, оранжевого и голубого цветов можно хоть каждый день, получая каждый раз аппарат нового цвета. Компактный (диагональ дисплея 11 сантиметров), тонкий (около 7,5 мм) и яркий Highscreen Omega Prime Mini стал особенно популярным у девушек.

Еще один стереотип, который сломал Omega Prime Mini — «мини-версия флагмана должна уступать по характеристикам старшей модели». Крупнейшие производители традиционно обеспечивают версиям с приставкой «mini» урезанную относительно старшей модели функциональность. Highscreen и тут пошел против течения и оснастил Omega Prime Mini таким же «железом», как и у старшей версии, Omega Prime с 4,7-дюймовым дисплеем. Всё то же самое, такая же мощная железка, как и в старшей модели, но в более компактном корпусе и с набором ярких крышечек.

8. «У всех доступных по цене смартфонов плохие условия гарантийного обслуживания».

Многие производители смартфонов второго эшелона действительно не имеют достаточно ресурсов на то, чтобы организовать на достойном уровне гарантийное и сервисное обслуживание на всей территории страны. В результате, даже если вам повезет, и в вашем Угличе есть авторизованный сервисный центр, придя туда со сломанным аппаратом, вы запросто можете услышать от мастера-приемщика что-то вроде: «Нет необходимых запчастей для починки данной модели, мы обязательно закажем из Москвы и все сделаем, но нужно будет подождать!» Как показывает практика, такой ремонт легко может затянуться на недели и даже месяцы.

Альтернатива авторизации сервисных центров по всей стране есть — это так называемая «европейская» система сервисного обслуживания. По ней в России работают только производители первого эшелона, а из брендов бюджетных смартфонов — один лишь Highscreen. Суть данного метода проста: каждый пользователь смартфонов Highscreen может бесплатно выслать устройство с гарантийной поломкой на обслуживание в главный сервис-центр из абсолютно любого отделения «Почты России». Их по всей стране порядка 42 000, так что можно сказать, что во всех, даже в самых небольших населенных пунктах есть свой полноценный пункт сервисного приема. Пересылка устройств осуществляется не обычной бандеролью, а курьерской службой «Почты России» — это что-то вроде нашей российской версии зарубежного DHL. Каждая отправка будет застрахована от потери и повреждения, а время пересылки в Москву и обратно не превышает 3-4 суток (5-6, в случае самых отдаленных регионов).

Какой можно сделать вывод после такого развернутого сеанса «разрушения мифов»? Для тех, кто привык считать свои деньги и не хочет переплачивать за раскрученный бренд при покупке смартфона, сегодня есть довольно широкий выбор моделей с достойным функционалом за адекватные деньги. При выборе смартфона следует полагаться на надежные источники информации и не торопиться с выводами, а самое важное — отбросить все стереотипы и не забивать голову разными мифами. Раскрученный бренд — это еще далеко не повод тут же доставать кошелек и немедленно расставаться со своими кровными.

P. S. Тех, кто верит в «мифы о бюджетниках», все меньше. В ноябре «Ведомости» опубликовали выдержки из отчета института маркетинговых исследований GfK за первые три квартала 2013-го года. Исследования показали, что продажи смартфонов ряда российских локальных брендов (B-брендов) в натуральном выражении выросли на сотни процентов по сравнению с аналогичным периодом 2012 года. Между тем суммарная доля лидирующей тройки (Samsung, Apple, Nokia) сократилась более чем на 15 процентов: с 66 до 50,9 процентов.

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

ОЦЕНКА ИНФОРМАЦИОННО-БОЕВОГО ПОТЕНЦИАЛА СТОРОН В ТЕХНОСФЕРНЫХ КОНФЛИКТАХ

Семенов С.С., *д.т.н., доцент,*
Военная академия связи
имени С.М. Буденного,
SemSem@Yandex.ru
Гусев А.П., *к.т.н.,*
Военная академия связи
имени С.М. Буденного,
AlexeyGusew@mail.ru
Барботько Н.В.,
Военная академия связи
имени С.М. Буденного,
Barbotko-nikolay@mail.ru

Ключевые слова:
техносферная война, боевой потенциал, информационное противоборство, асимметричность оценки, взаимное влияние сторон.

АННОТАЦИЯ

В статье проведен анализ существующих подходов к оценке боевых потенциалов сторон в современных конфликтах. Внесены предложения по учету при оценке боевого потенциала информационной составляющей и взаимного влияния сторон, что позволяет получать ассиметричные оценки, в зависимости от стороны производящей оценку.

Анализ современных методов оценки боевых потенциалов показал не соответствие имеющихся взглядов новым видам противоборства конфликтующих сторон. Имеющиеся методики позволяют оценивать только боевой потенциал, определяемый наличием вооруженных сил и их вооружением, при этом возможности информационного потенциала не рассматриваются. Основным недостатком данных подходов оценки является линейная аддитивность учитываемых параметров и определение абсолютного потенциала, то есть оцениваемая сторона рассматривалась изолированно от предполагаемой конфликтующей стороны. Для устранения этого недочета предлагается рассматривать информационно-боевой потенциал стороны в отношении к конфликтующей стороне, или относительный боевой потенциал с учетом параметров отражающих способы ведения техносферной войны. Основной сутью предлагаемой методики является переход от изолированной (одноидексной) оценке к интегративной (двухиндексной) при учете информационных факторов.

Предложенный подход позволяет оценить информационно-боевой потенциал страны с учетом не только ее «внутренних» показателей, но и с учетом взаимосвязи с другими государствами и в частности с государством, относительно которого производится оценка, а так же учесть современные тенденции ведения техносферных боевых действий. Новизна предложенного подхода заключается в ассиметричности получаемых значений информациоо-боевого потенциала страны, в зависимости от страны производящей оценку, что по мнению авторов статьи является более обоснованным в современных условиях глоболизации и интеграции.

Проведена декомпозиция основных показателей на ряд частных, сформулированы обобщенные методы их расчета. Намечены возможные пути их развития.

Авторы отдают себе отчет, что предложенный подход требует существеного развития и детализации с привлечением значительного числа заинтересованных ученых.

Анализ конфликтов в современном мире указывает на необходимость введения нового понятия войны – войны в искусственной сфере (защищаемый ресурс, среда существования этого ресурса, средства разведки и воздействия, а так же среда в которой эти воздействия осуществляются, являются искусственными) – техносферная война. Это явление подробно описано в ряде публикаций [1, 2, 5].

Техносферная война (ТСфВ) – (от греческого технито – искусственный и сфера – среда, то есть война в искусственной среде) форма конфликта, в котором объекты нападения (защиты) и средства нападения (защиты) являются информацией, существующей в рамках инфотелекоммуникационного пространства (общемирового единого телекоммуникационного пространства (ОМЕТП)). Под информацией понимается не только данные передаваемые (хранимые) через ОМЕТП, а так же информация о состоянии ОМЕТП (или его части) и состояниях АСУ атакуемой системы и алгоритмах их функционирования. Воздействия (разведка) осуществляются за счет использования искусственно созданных цифровых кодов, переданных по средствам искусственной среды (ОМЕТП) и воздействующих на коды (программы, аппаратуру) атакуемой (разведываемой) АСУ.

Таким образом, можно сформулировать определение ТСфВ – это система согласованных по цели, месту и времени ин-формационных действий, направленных на захват управле-ния (частичный, полный) выбранных систем автоматизированного (автоматического) управления, либо перевод их в деструктивный режим функционирования.

Суть – воздействие на выбранную автоматизированную информационную систему для захвата ресурса (экономического, политического, информационного и т.д.). Средством достижения цели является целенаправленное изменение режима, а в приделе перевод атакуемой системы в критические режимы функционирования.

В отличии от классического представления противоборства сторон, в котором конфликтующие стороны имели доступ к информации о состоянии СУВ, СВС, АСУ противника опосредованно и только через естественную среду, в складывающейся конфликтной ситуации АСУ противоборствующих сторон используют один и тот же инфотелекоммуникационный ресурс ОМЕТП и тем самым имеют возможность непосредственного доступа к элементам АСУ.

Анализ современных методов оценки боевых потенциалов [4] покозал не соответствие имеющихся взглядов новым видам противоборства конфликтующих сторон. Имеющиеся методики позволяют оценивать только боевой потенциал, определяемый наличием вооруженных сил и их вооружением, при этом возможности информационного потенциала не рассматриваются. Основным недостатком данных подходов оценки является линейная аддитивность учитываемых параметров и определение абсолютного потенциала, то есть оцениваемая сторона (W_i) рассматривалась изолированно от предполагаемой (W_j) конфликтующей стороны. Для устранения этого недочета предлагается рассматривать информационно-боевой потенциал стороны в отношении к конфликтующей стороне, т.е. относительный боевой потенциал с учетом параметров отражающих способы ведения техносферной войны (W_{ij}). Основной сутью предлагаемой методики является переход от изолированной (одноидексной) оценке к интегративной (двухиндексной) при учете информационных факторов.

Таблица 1 Показатели оценки информационно-боевого потенциала страны

№ п/п	Информационно-технический показатель (T)	Организационный показатель (O)	Научный показатель (S)	Геополитический показатель (G)
1.	Уровень используемых информационно-технических средств (технической базы)	Уровень техносферных подразделений	Уровень научных школ в области информационных технологий и информационной безопасности	Уровень террористической угрозы в информационном пространстве страны
2.	Плотность покрытия территории государства ИТКС	Уровень информатизированности органов государственного управления	Уровень ВУЗов области информационных технологий	Уровень социально-политической стабильности в обществе
3.	Трафик ИТКС	Количество абонентов ИТКС	Уровень инновационных технологий в области информационных технологий	Уровень участия в союзах с другими государствами
4.	Средняя скорость доступа к ИТКС страны	Уровень законодательной базы в области информационных технологий	Уровень научно-исследовательских центров области информационных технологий	Географическое положение страны в мире и площадь территории
5.	Структура ИТКС страны	Уровень влияния на общемировое адресное пространство	Уровень образованности населения в области информационных технологий	Уровень имеющихся ресурсов
6.	Уровень используемого программного обеспечения			

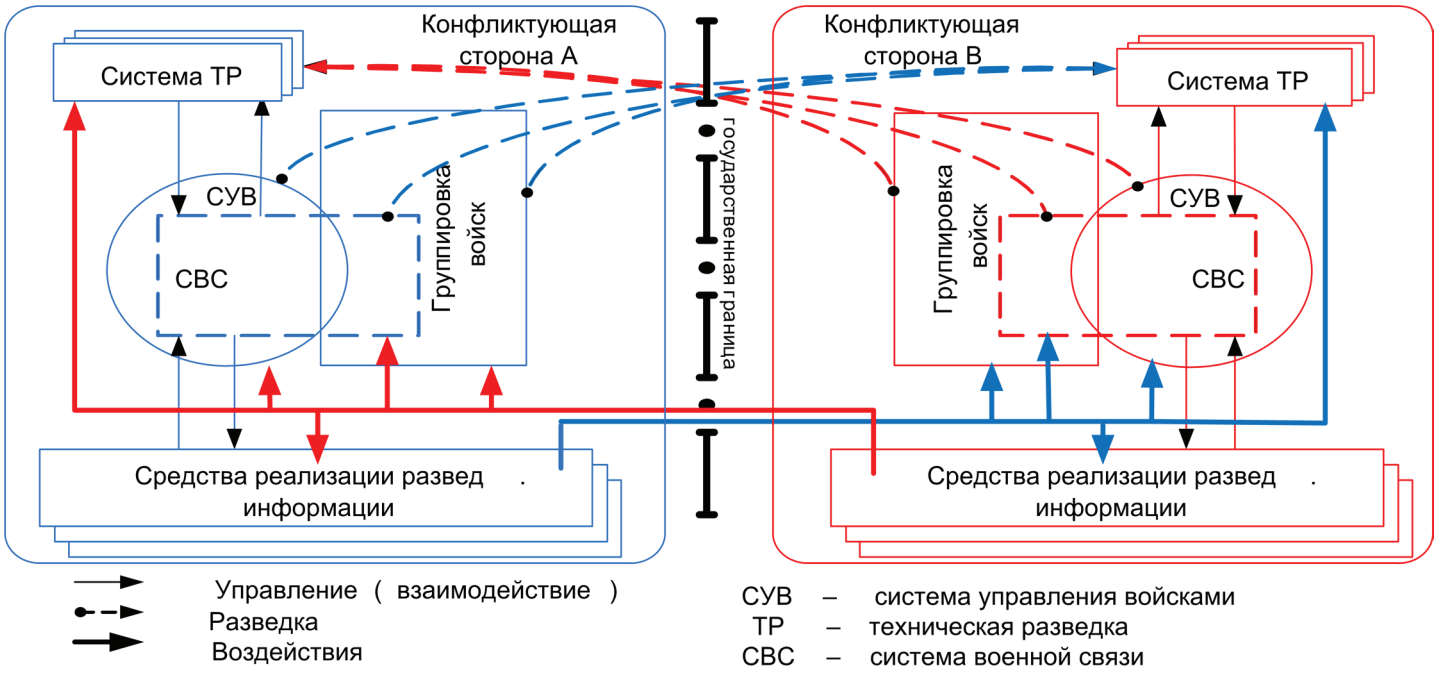


Рис. 1 Классическое представление противоборства сторон

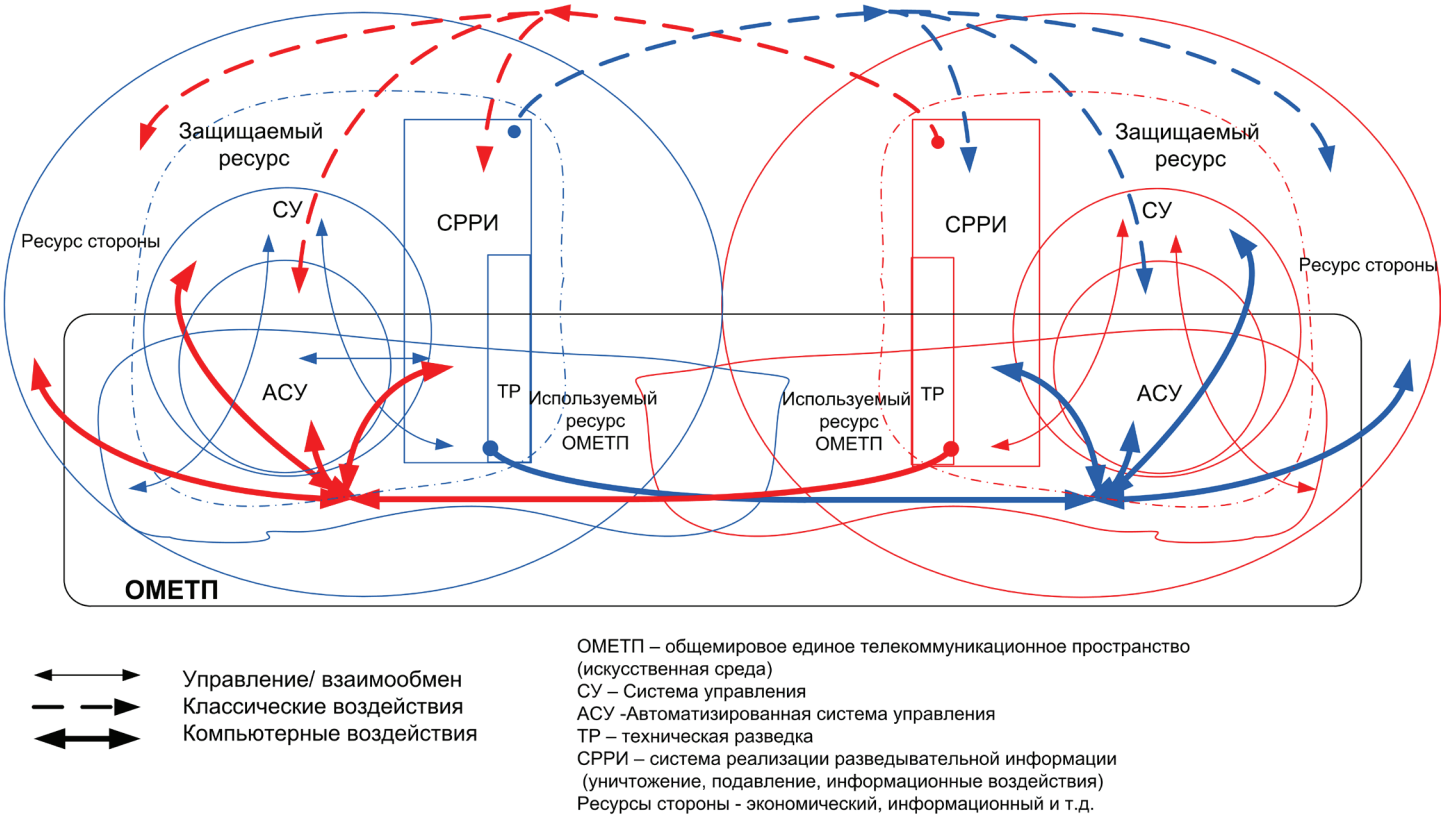


Рис. 2 Графическая модель конфликтной ситуации применительно к условиям техносферной войны

Общий показатель потенциала страны предлагается представить в виде четырех составляющих, каждая из которых представлена рядом частных показателей. Предлагаемые показатели представлены в таблице 1. При проведении оценки информационно-боевого потенциала необходимо учитывать неравнозначность предложенных показателей. Так показатели «технический» и «организационны» будут иметь больший весовой коэффициент в реальном масштабе времени, а показатели «научный» и «геополитический» должны учитываться в прогнозе перспектив развития.

В отличии от классического представления противоборства сторон, представленного на рис. 1, в котором конфликтующие стороны имели доступ к информации о состоянии СУВ, СВС, АСУ противника опосредованно и только через естественную среду, в складывающейся конфликтной ситуации АСУ противоборствующих сторон используют один и тот же инфотелекоммуникационный ресурс общемирового единого телекоммуникационного пространства (ОМЕТП) и тем самым имеют возможность непосредственного доступа к элементам АСУ. Графическая модель складывающейся конфликтной ситуации представлена на Рис. 2.

Информационно-технический показатель (Т)

Уровень используемых информационно-технических средств (технической базы). Для подсчета параметра предлагается использовать матрицу размерностью $[m \times k]$, где m-количество элементов структуры ИТКС (узлов связи), а k-количество типов используемых информационно-технических средств [3]. Ячейка матрицы содержит значение количества используемой на i-м элементе j-го информационно-технического средства.

Таким образом, появляется возможность определить степень использования информационно-технических средств в ИТКС.

Используемость j-го типа средств определяется по формуле (1):

$$W = K_{\text{мн}} \sum_{i=1}^{m} (A_i V_i), \quad (1)$$

где $K_{\text{мн}}$ – коэффициент монопольности (принимает значение 1 – если данный тип средств не может быть заменен аналогом, и принимает значение равное количеству возможных аналогов – если данный тип средств, возможно, заменить аналогом); A_i – значение ячейки матрицы для j-го типа средств; V_i – коэффициент важности i-го элемента структуры ИТКС (коэффициент важности – параметр, указывающий степень ухудшение качества функционирования при удалении элемента из структуры). Степень используемости информационно-технических средств представляется следующим образом (формулы 2-5):

$$S = \frac{S_B - S_A}{S_o}; \quad (2)$$

$$S_A = \sum_{i=1}^{k} (W_i K_{Ai}); \quad (3)$$

$$S_B = \sum_{i=1}^{k} (W_i K_{Bi}); \quad (4)$$

$$S_o = \sum_{i=1}^{k} W_i; \quad (5)$$

где K_{Ai} – коэффициент производства в стране "A" (принимает значение 1 – если i-й тип информационно-технических средств производиться в стране "A" и 0 – если нет). K_{Bi} – коэффициент производства в стране "B" (принимает значение 1 – если i-й тип информационно-технических средств производиться в стране "B" и 0 – если нет). S_o – общая сумма используемости; S – обобщенный показатель, позволяющий оценить вклад используемых информационно-технических средств в боевой (информационный) потенциал страны.

Плотность покрытия территории государства ИТКС

Данный показатель выводиться из простого отношения количества точек доступа к ресурсам ИТКС к площади анализируемой страны – формула (6).

$$П = \frac{N_{ТД}}{S} \quad (6)$$

где $N_{mò}$ - количество точек доступа, S – площадь страны (км^2).

Трафик ИТКС. Для оценки трафика, необходимо оценивать внутренний, внешний и транзитный трафик ИТКС (Рис.3).

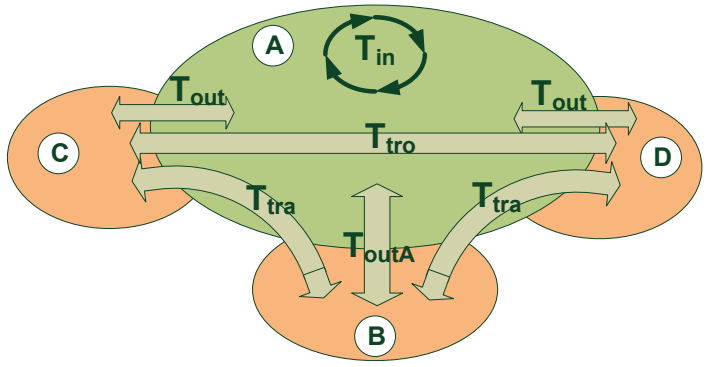


Рис. 1 Графическое представление потоков (трафика), циркулирующих в ИТКС

Внешний трафик (T_{out})- сумма трафика стороны «A» с другими странами, исключая трафик со стороной «B». Внешний трафик стороны «A» (T_{outA}) – трафик между стороной «A» и «B». Транзитный трафик общий (T_{trO})– это трафик третьих стран, проходящих через ИТКС стороны «A». Транзитный трафик стороны «A» (T_{trA})- это трафик между стороной «B» и третьими странами, проходящий через ИТКС стороны «A».

Оценка трафика будет определяться соотношением объемов циркулирующего трафика в ИТКС по его принадлежности (формула 7):

$$Q = \frac{T_{in}}{(T_{outA} K_{out} + T_{out})(T_{trA} K_{tr} + T_{tro})}, \quad (7)$$

где T_{in} – внутренний трафик, T_{out} – внешний трафик, T_{tr} – транзитный трафик, T_{outA} – внешний трафик со страной "A", T_{out} – внешний трафик с остальными странами, K_{out} – коэффициент важности для внешнего трафика со страной «A», T_{trA} – транзитный трафик страны "A", T_{trO} – транзитный трафик остальных стран, K_{tr} – коэффициент важности для транзитного трафика со страной "A".

Наличие транзитного трафика, позволяет оцениваемой стране воздействовать на потоки других стран и тем самым ее информационно-боевой потенциал возрастает.

Средняя скорость доступа к ИТКС страны. Данный показатель определяется отношением суммы скоростей доступа к количеству линий доступа.

$$V_{ср} = \frac{\sum_{i=1}^{n} V_i}{N} \quad (8)$$

где N - количество линий доступа, V_i – скорость i-й линии.

Структура ИТКС страны. Для первичной оценки структуры транспортной сети на определенной площади можно использовать параметр, характеризующий среднюю связанность в сочетании с пропускной способностью ребер транспортной сети (9).

$$G = K_{\text{ср}} W_{\text{ср}}, \quad (9)$$

Связанность элементов структуры – матрица связанности элементов структуры ИТКС между собой, где каждая ячейка матрицы несет значение суммарной (если между двумя точками несколько соединений) пропускной способности между двумя элементами ИТКС.

Ранг каждого элемента – вычисляется, как количество соединений с другими элементами ИТКС – формулы (10, 11).

$$K_{\text{св}} = \frac{\sum_{i=1}^{n} R_i}{N}, \quad (10)$$

$$W_{\text{св}} = \frac{\sum_{i=1}^{m} W_i}{M}, \quad (11)$$

где R_i – ранг i-го элемента транспортной сети; N – количество элементов транспортной сети; W_i – пропускная способность ребра транспортной сети в выделенном районе; M – количество ребер транспортной сети.

Уровень используемого программного обеспечения. Для расчета параметра предлагается осуществлять по выражению (12):

$$W_{ПО} = \frac{R_o}{R_B + K_{др} R_{др} + R_A N_A}, \quad (12)$$

где R_o – общий показатель используемого ПО, R_B – частный показатель используемого ПО, разработанного в стране «B»; $R_{др}$ – частный показатель использования ПО, разработанного третьими странами; R_A – частный показатель использования ПО, разработанного в стране «A»; $K_{др}$ – коэффициент снижения безопасности при использовании стороннего ПО; K_A – коэффициент снижения безопасности при использовании ПО из страны «A».

Частные показатели рассчитываются по выражениям (13-16):

$$R_o = \sum_{i=1}^{n} (N_{исп\,i} \times K_{в\,i}); \quad (13)$$

$$R_B = \sum_{i=1}^{m} (N_{исп\,i} \times K_{в\,i}); \quad (14)$$

$$R_{др} = \sum_{i=1}^{l} (N_{исп\,i} \times K_{в\,i}); \quad (15)$$

$$R_A = \sum_{i=1}^{k} (N_{исп\,i} \times K_{в\,i}), \quad (16)$$

где $N_{исп\,i}$ – количество используемых копий i-го программного продукта (ПП), $K_{вi}$ – коэффициент важности i-го ПП, n – количество всех используемых ПП, m – количество ПП, разработанных в стране «B», l – количество ПП, разработанных третьими странами, k – количество ПП, разработанных страной «A».

Организационный показатель (О)

При оценке боевого потенциала страны организационный показатель определяет подготовленность к возможному ведению техносферных операций и их масштаб.

Уровень техносферных подразделений – $K_{2.1}$. Данный показатель отражает понимание страной возможных последствий при ведении техносферной войны и необходимость создания и развития соответствующих подразделений – формула (17).

$$K_{2.1} = \left(\frac{N_{2.1.1} + N_{2.1.2}}{N}\right)\left(\frac{V_{2.1.1} + V_{2.1.2}}{V}\right)\left(F_{2.1.1} + F_{2.1.2}\right), \quad (17)$$

где $N_{2.1.1}$ – количество государственных техносферных подразделений; $N_{2.1.2}$ – количество негосударственных техносферных организаций действующие по заданию и при финансовой поддержке государства; N – количество государственных структур (учреждений); V – количество населения государства; $V_{2.1.1}$ – количество сотрудников государственных подразделений; $V_{2.1.2}$ – количество сотрудников негосударственных организаций; $F_{2.1.1}$ – эффективность техносферных воздействий подразделений – рассчитывается по формуле (18); $F_{2.1.2}$ – эффективность противодействий техносферных подразделений - рассчитывается по формуле (19).

$$F_{2.2.1} = X_{\text{общ}} / X_{\text{пр}}, \quad (18)$$

где $X_{\text{общ}}$ – количество атак совершенных государством; $X_{\text{пр}}$ – количество реализованных атак.

$$F_{2.2.2} = Z_{\text{общ}} / Z_{\text{пр}}, \quad (19)$$

где $Z_{\text{общ}}$ – количество атак совершенных на государство; $Z_{\text{пр}}$ – количество атак преодолевших защиту.

Уровень информатизированности органов государственного управления – $K_{2.2}$. Данный показатель позволяет оценить возможность ведения техносферных операций и масштаб их воздействий. При этом чем выше уровень информатизированности органов государственного управления тем выше потенциальный ущерб, который возможно нанести стране в техносферной войне (20).

$$K_{2.2} = \left(\frac{N_{2.2.1} + N_{2.2.2}}{N}\right) \bullet \left(\frac{C_a}{C}\right), \quad (20)$$

где $N_{2.2.1}$ – количество государственных структур (учреждений) имеющих автоматизированные системы (использующие информационные технологии); $N_{2.2.1}$ – количество государственных структур (учреждений) объединенных выделенными ИТКС и имеющие соединения с сетями общего пользования; N – количество государственных структур (учреждений); C_a – количество автоматизированных функциональных процессов в государственных структурах (учреждениях); C – количество функциональных процессов в государственных структурах (учреждениях);

Количество абонентов ИТКС – ***$K_{2.3}$***. Количество абонентов ИТКС позволяет оценить масштаб возможных техносферных операций (21).

$$K_{2.3} = \left(\frac{V_{2.3.1}}{V}\right) \bullet \left(\frac{V_{2.3.2}}{V}\right) \bullet \left(\frac{V_{2.3.3}}{V}\right), \quad (21)$$

где V – количество населения государства; $V_{2.3.1}$ – количество абонентов фиксированной связи; $V_{2.3.2}$ – количество абонентов подвижной связи; $V_{2.3.3}$ – количество пользователей Интернет.

Уровень правовой базы в области информационных технологий - $K_{3.4}$. Уровень правовой базы определяет степень проработанности вопросов информационной безопасности при ведении техносферной войны и осознанию опасности возможных угроз – формула (22).

$$K_{2.4} = \left(\frac{M_{2.4.1}}{M}\right) \bullet \left(\frac{M_{2.4.2}}{M}\right) \bullet D_{2.4}, \quad (22)$$

где $M_{2.4.1}$ – количество законодательных актов по безопасности информации; $M_{2.4.2}$ – количество законодательных актов уголовного преследования за нарушения в области безопасности информации; M – общее количество законодательных актов в государстве; $D_{2.4}$ – актуальность (своевременность) законодательных актов по безопасности информации – формула (23);

$$D_{2.4} = 1/T_{2.4}, \quad (23)$$

$T_{2.4}$ – время существования закона (от принятия до замены или отмены).

Уровень влияния (управления) на общемировое адресное пространство – ***$K_{2.5}$***. Данный показатель определяет возможности страны при проведении техносферных операций влиять на управление ИТКС атакуемой стороны за счет изменения адресации – формула (24).

$$K_{2.5} = P/N_{2.5}, \quad (24)$$

где P – доля государства в участи распределения адресации в IP-сетях (в настоящее время единовластные решения со стороны США); $N_{2.5}$ – количество государств участвующих в общемировом информационном обмене.

Научный показатель (S)

Уровень научных школ в области информационных технологий и информационной безопасност рассчитывается по формуле (25).

$$Q_s = \sum_{i=1}^{8} Q_{3.1.i} K_i, \quad (25)$$

где K_i – весовой коэффициент каждого показателя; $Q_{3.1.1}$ – интенсивность проводимых конференций – формула (26)

$$Q_{3.1.1} = \frac{N_{3.1.1}}{N_{общ1}}; \quad (26)$$

$N_{3.1.1}$ – количество проводимых конференций по тематике информационной безопасности (ИБ); $N_{общ1}$ – общее количество проводимых в стране научных конференций; $Q_{3.1.2}$ – интенсивность выпуска трудов – формула (27)

$$Q_{3.1.2} = \frac{N_{3.1.2}}{N_{общ2}}; \quad (27)$$

$N_{3.2}$ – количество выпускаемых трудов (научные, методические, авторефераты, монографии) по тематике ИБ; $N_{общ2}$ – общее количество выпускаемых научных трудов в стране; $Q_{3.1.3}$ – интенсивность издания книг и учебников (28)

$$Q_{3.1.3} = \frac{N_{3.1.3}}{N_{общ3}}; \quad (28)$$

$N_{3.1.3}$ – количество изданных книг и учебников по тематике ИБ; $N_{общ3}$ – общее количество издаваемых книг и учебников; $Q_{3.1.4}$ – индекс реферативности (ссылаемости) – формула (29)

$$Q_{3.1.4} = \frac{N_{3.1.4}}{N_{общ4}}; \quad (29)$$

$N_{3.1.4}$ – количество ссылок на работы по тематике ИБ; $N_{общ4}$ – общее число ссылок на научные работы страны; $Q_{3.1.5}$ – интенсивность подготовки специалистов с высшим образованием – формула (30)

$$Q_{3.1.5} = \frac{N_{3.1.5}}{N_{общ5}}; \quad (30)$$

$N_{3.1.5}$ – количество подготовки специалистов с высшим образованием по тематике ИБ; $N_{общ5}$ – общее количество подготавливаемых специалистов; $Q_{3.1.6}$ – интенсивность подготовки специалистов с учеными степенями (31)

$$Q_{3.1.6} = \frac{N_{3.1.6}}{N_{общ6}}; \quad (31)$$

$N_{3.1.6}$ – количество подготавливаемых специалистов с учеными степенями по тематике ИБ; $N_{общ6}$ – общее количество подготавливаемых специалистов с учеными степенями. Причем $N_{3.1.6}$ и $N_{общ6}$ рассчитываются по формуле:

$N = N_{кн} + N_{дн} \times K_{кд}$, где $N_{кн}$ - количество кандидатов наук, $N_{дн}$ - количество докторов наук, $K_{кд}$ - весовой коэффициент доктора перед кандидатом.

$Q_{3.7}$ – интенсивность получения государственных наград и премий работниками и коллективами – формула (32)

$$Q_{3.1.7} = \frac{N_{3.1.7}}{N_{общ7}}; \quad (32)$$

где $N_{3.1.7}$ – количество наград и премий, получаемых работниками и коллективами по тематике ИБ; $N_{общ7}$ – общее количество наград и премий, получаемых научными сотрудниками страны; $Q_{3.1.8}$ – индекс признания в мире (включение имен работников в международные рейтинговые оценки, получение международных наград и премий) – формула (33)

$$Q_{3.1.8} = \frac{N_{3.1.8}}{N_{общ8}}; \quad (33)$$

$N_{3.1.8}$ – количество признанных в мире ученых по тематике ИБ.

Причем $N_{3.1.8} = N_B K_з + N_{др}$, где N_B – количество признанных ученых в стране «B»; $K_з$ – коэффициент значимости; $N_{др}$ – количество признанных ученых в других странах; $N_{общ8}$ – общее количество признанных в мире ученых.

Для достижения адекватности показателей, подсчет необходимо производить за период времени не менее пяти лет.

Уровень ВУЗов области информационных технологий.

Общая последовательность расчета - формула (34).

$$Q_{3.2} = Q_{3.2.1}K_{3.2.1} \times Q_{3.2.2}K_{3.2.2} \times Q_{3.2.3}K_{3.2.3} \quad (34)$$

I. Оценка профессорско-преподавательского состава (ППС) (35-37).

$$Q_{3.2.1} = Q_{3.2.1.1}P + N_{3.2.1.2}K_{3.2.1}, \quad (35)$$

$$Q_{3.2.1.1} = \frac{(N_{3.2.1.3} - N_{3.2.1.4}) + K_{кд}(N_{3.2.1.5} - N_{3.2.1.6})}{N_{3.2.1.1}}, \quad (36)$$

$$P_{3.2.1} = \frac{\sum_{i=1}^{N_{3.2.1.1}} P_i}{N_{3.2.1.1}}, \quad (37)$$

где $N_{3.2.1.1}$ – общее количество преподавателей; $N_{3.2.1.2}$ – количество преподавателей, получивших престижные международные награды; $N_{3.2.1.3}$ – количество преподавателей, имеющих степень КН; $N_{3.2.1.4}$ – количество преподавателей, получивших степень КН в стране «А»; $N_{3.2.1.5}$ – количество преподавателей, имеющих степень ДН; $N_{3.2.1.6}$ – количество преподавателей, получивших степень ДН в стране «А»; $Q_{3.2.1.1}$ – доля остепененных преподавателей (коэффициент остепененности); $K_{кд}$ – весовой коэффициент доктора перед кандидатом; $P_{3.2.1}$ – опыт преподавателей; P_i – преподавательский стаж i-го преподавателя.

II. Оценка студентов – формула (38).

$$Q_{3.2.2} = \prod_{i=1}^{5} Q_{3.2.2.i} + N_{3.2.2.2}K_{3.2.2.1} + N_{3.2.2.3}K_{3.2.2.2} \quad (38)$$

Расчет составляющих производится по формулам (39-40).

$$Q_{3.2.2.3} = \frac{N_{3.2.2.5}}{N_{3.2.2.1}}, \quad (39)$$

$$Q_{3.2.2.4} = \frac{N_{3.2.2.6}}{N_{3.2.2.1}}, \quad (40)$$

$$Q_{3.2.2.5} = \frac{N_{3.2.2.1}}{N_{3.2.1.2}}, \quad (41)$$

где $N_{3.2.2.1}$ – число выпускников окончивших заведение за всю его историю; $N_{3.2.2.2}$ – число студентов, обучаемых в данный период времени; $N_{3.2.2.3}$ – число выпускников, получивших престижные международные награды; $N_{3.2.2.4}$ – количество студентов отмеченных в национальных (международных) научных конкурсах; $Q_{3.2.2.1}$ – соотношение числа поступающих к окончившим обучение; $Q_{3.2.2.2}$ – средний выпускной балл; $N_{3.2.2.5}$ – число выпускников, устроившихся работать по специальности; $N_{3.2.2.6}$ – число выпускников, поступивших в аспирантуру; $Q_{3.2.2.3}$ – доля выпускников, устроившихся работать по специальности; $Q_{3.2.2.4}$ – доля выпускников, поступивших в аспирантуру; $Q_{3.2.2.5}$ – число студентов на одного преподавателя.

III. Другие аспекты – формулы (42-44).

$$Q_{3.2.3} = Q_{3.2.3.1} \times Q_{3.2.3.2} \times N_{3.2.3.1}, \quad (42)$$

где $N_{3.2.3.1}$ – число статей сотрудников ВУЗа, включенных в международные индексы цитируемости; $R_{3.2.3.1}$ – расходы ВУЗа на преподавание; $R_{3.2.3.2}$ – расходы ВУЗа на исследования; R – общие расходы ВУЗа.

$$Q_{3.2.3.1} = \frac{R_{3.2.3.1} + R_{3.2.3.2}}{R}, \quad (43)$$

где $Q_{3.2.3.1}$ – доля расходов на научно-преподавательскую деятельность; $N_{3.2.3.2}$ – число аспирантов, защитивших диссертацию.

$$Q_{3.2.3.2} = \frac{N_{3.2.3.2}}{N_{3.2.2.4}}, \quad (44)$$

где $Q_{3.2.3.2}$ – Доля аспирантов, защитивших диссертацию.

Уровень инновационных технологий в области информационных технологий

Методические положения оценки инновационного потенциала

Общая методологическая схема многоуровневой оценки уровня инновационного потенциала имеет такую последовательность:

1. Устанавливается перечень кластер-факторов, связанных с соответствующими свойствами инновационного потенциала и строится «дерево кластер-факторов», ствол которого – уровень развития и качество инновационного потенциала в целом, а ветви, расположенные на соответствующих уровнях, более детальные его свойства.
2. В соответствии с установленным перечнем кластер-факторов и структуризацией их за разработанным «деревом кластер-факторов» устанавливаются показатели оценки потенциала.
3. Согласно проведенной структуризации и иерархизации показателей оценки рассчитывается коэффициент весомости каждого показателя.
4. Избирается база сравнения уровня инновационного потенциала, за которую может быть взятый инновационный потенциал исследующегося предприятия за предыдущий период или инновационный потенциал ближайшего в стратегической группе конкурента.

5. Проводя сравнительный анализ посредством метода средневзвешенной рассчитываем показатель роста инновационного потенциала (или показатель уровня инновационного потенциала) исследуемой страны. Оцениваем интенсивность инновационного развития.
6. На основании полученных данных делается вывод относительно уровня инновационного потенциала.

Расчет уровня инновационного потенциала

Определяется величина показателя роста инновационного потенциала исследующегося объекта по формуле (45):

$$\Delta ИП_t = \sum_{i=1}^{n} (\frac{Q_i^o}{Q_i^б} \times B_i) \quad (45)$$

где $ИП_t$ – показатель роста инновационного потенциала, исследуемой страны за период времени t; O^o_i – оценка i-го показателя инновационного потенциала, исследуемой страны (в балах); $O^б_i$ – оценка i-го показателя инновационного потенциала базы сравнения (в балах); B_i - коэффициент весомости i-го показателя (в % или относительных величинах) ($B_i = 100\%$ или $B_i = 1$).

Отметим, что посредством приведенных формул можно получить, как показатель роста инновационного потенциала страны, относительно изменения этого потенциала за предыдущий период времени (год, 5 лет), так и показатель уровня инновационного потенциала страны относительно потенциала страны «А» (проводящей оценку).

Используя показатель прироста инновационного потенциала, можно оценить интенсивность инновационного развития страны по формуле (46):

$$I_{ip} = \frac{\Delta ИП}{\Delta T} \quad (46)$$

где I_{ip} – показатель интенсивности инновационного развития страны; Δ T – период расчета интенсивности инновационного развития, годы.

Показатель интенсивности инновационного развития страны показывает величину прироста его инновационного потенциала за один год (или другую единицу времени).

Аналогичный подход можно использовать и для прогнозной оценки инновационного развития, приравнивая во времени, имеющийся потенциал и рассчитывая через одинаковый период времени, будущий потенциал.

Другим, не менее важным критерием оценки инновационного развития нужно считать стоимостную оценку, которая может быть проведенная посредством показателя удельных расходов на инновационное развитие. Этот показатель может быть рассчитанный как отношение расходов на инновационное развитие к величине прироста инновационного потенциала с учетом фактору времени – формула (47).

$$ПВ_{ip} = \frac{B_{ip}}{\Delta ИП} \quad (47)$$

где $ПВ_{ip}$ – удельные расходы на инновационное развитие; $\Delta ИП$ – рост инновационного потенциала за период времени I; Bip – расходы на инновационное развитие за период времени I.

Экономическое содержание показателя заключается в следующем: он показывает, сколько средств (денежных единиц) расходует страна для достижения единичного роста своего инновационного потенциала. К расходам на инновационное развитие следует выносить расходы на НИОКР, приобретение патента или лицензии, расходы на освоение и внедрение в производство продуктовых и технологических организационно-управленческих инноваций.

Уровень научно-исследовательских центров в области информационных технологий

Оценка технического потенциала НИЦ.

Главной чертой НИЦ, отличающей его от лаборатории, является наличие приборов, обеспечивающих проведение многопрофильных, многометодовых и междисциплинарных исследований. Многопрофильность и возможность проводить многометодовые исследования, испытания и измерения определяют научно-исследовательский потенциал НИЦ, повышают уровень востребованности его услуг. Многопрофильность НИЦ определяется наличием различных видов объектов приборной базы. Соответственно, чем больше видов измерительного оборудования представлено в НИЦ, тем выше уровень его многопрофильности. НИЦ не считается многопрофильным при наличии одного или нескольких приборов только одного вида.

Возможность проведения в НИЦ многометодовых измерений определяется количеством объектов приборной базы одного вида. Это требование обусловлено тем, что для получения достоверных научных результатов одно и то же измерение необходимо проводить на различных измерительных приборах. Считается, что НИЦ имеет возможность проводить многометодовые измерения при наличии не менее 5 единиц измерительного оборудования одного вида; для каждого вида измерительного оборудования может быть установлено определенное количество приборов, минимально необходимое для проведения многометодовых измерений; также могут быть установлены минимальные требования к стоимости научного оборудования.

Технический потенциал НИЦ, определяемый по факторам «многопрофильность» и «многометодовые измерения», может быть оценен с помощью системы баллов, приведенных в таблице 2.

Таблица 1 Количество баллов, набираемых НИЦ по схеме «многопрофильность – многометодовые измерения»

Наличие приборов	Количество измерительных приборов					
	Менее 5 единиц	От 5 единиц				
		1 вида	2-х видов	3-х видов	4-х видов	5-ти видов
1 вида	1	2				
2 видов	2	3	4			
3 видов	3	4	5	6		
4 видов	4	5	6	7	8	
5 видов	5	6	7	8	9	10

Согласно разработанному алгоритму количество баллов, которые НИЦ получает по фактору «многопрофильность», эквивалентно числу видов имеющегося измерительного оборудования. По фактору «многометодовые измерения» НИЦ получает количество баллов, эквивалентное числу видов.

Распределение НИЦ по группам в зависимости от количества набранных баллов по схеме «многопрофильность–многометодовые измерения» выглядит следующим образом: группа A – 9-10 баллов (максимальный технический потенциал); группа B – 7-8 баллов; группа C – 4-6 баллов; группа D – 1-3 балла (минимальный технический потенциал). Выделенные группы можно рассматривать как уровни технического потенциала НИЦ.

Научно-технический потенциал НИЦ может быть охарактеризован следующими абсолютными и относительными показателями:

1. *Численность сотрудников НИЦ* – среднегодовая численность сотрудников НИЦ, в том числе докторов и кандидатов наук.

2. *Уровень квалификации сотрудников НИЦ* - отношение числа сотрудников НИЦ, имеющих ученую степень, к общей численности сотрудников НИЦ. Данный показатель указывает на профессиональный уровень сотрудников НИЦ.

3. *Стоимость оборудования НИЦ* (условных денежных единицах (УДЕ)) - среднегодовая балансовая стоимость объектов приборной базы, закрепленных за НИЦ.

4. *Техновооруженность в НИЦ* (УДЕ) - отношение стоимости оборудования к численности сотрудников НИЦ.

Результативность использования ресурсного потенциала НИЦ носит мультикритериальный характер. Условно показатели результативности можно разделить на две большие группы: стоимостные и нестоимостные.

Несколько комментариев о нестоимостных параметрах. К ним, в частности, можно отнести число выполненных исследований, измерений, испытаний; количество публикаций, содержащих научные результаты, полученные на приборной базе НИЦ; число организаций-пользователей; патентная активность, количество докладов сотрудников НИЦ, сделанных на российских и зарубежных конференциях; количество подготовленных в рамках НИЦ дипломных работ, кандидатских и докторских диссертаций; число аттестованных методик, разработанных сотрудниками НИЦ; документы о международном признании НИЦ, уровень загрузки научного оборудования и др. Безусловно, каждый их указанных показателей важен, однако при проведении сравнительного анализа НИЦ по нестоимостным параметрам возникает множество сложностей при их сопоставлении. Например, если рассматривать число публикаций, оценка их качества является самостоятельной задачей, отнимающей много ресурсов на экспертизу. Что касается параметров загрузки научного оборудования, популярного среди НИЦ показателя, то здесь возможны различные ситуации, когда меньшая загрузка дает на выходе больше научных результатов. Аналогичные соображения применимы к патентам, докладам, диссертациям, аттестованным методикам.

В то же время, нестоимостные показатели наилучшим образом свидетельствуют о результативности НИЦ. Однако эти показатели оказываются довольно проблематичными с точки зрения использования в сравнительном анализе и оценке содержания и качества деятельности НИЦ. Тем не менее, несмотря на методические сложности вряд ли стоит игнорировать нестоимостные показатели. Вместе с тем, параметры результативности, имеющие денежное выражение, более удобны в управленческих целях. Они универсальны, проверяемы, контролируемы, наконец, имеют ту же единицу измерения, что и государственные инвестиции в НИЦ. Исходя из этого, в рамках данной методики будут использованы преимущественно стоимостные показатели результативности.

Итак, для оценки экономической результативности НИЦ были выбраны следующие показатели:

1. *Стоимость выполненных НИР и услуг НИЦ* - суммарная стоимость НИР и услуг, оказанных НИЦ на возмездной основе.

2. *Использование приборной базы НИЦ* - отношение стоимостного объема выполненных НИР и оказанных услуг к стоимости оборудования НИЦ.

3. *Производительность НИЦ* - отношение стоимостного объема выполненных НИР и оказанных услуг к численности сотрудников НИЦ.

4. *Степень ориентированности НИЦ на внешних пользователей* определяется как отношение себестоимости услуг, оказанных НИЦ внешним пользователям, к себестоимости всех услуг, оказанных НИЦ.

Себестоимость услуги НИЦ предлагается рассчитывать по следующей формуле: $S = tG$, где S – себестоимость услуги в условных денежных единицах (УДЕ); t – продолжительность оказания услуги; G – себестоимость одного часа работы на оборудовании НИЦ УДЕ/час, требуемом для оказания услуги.

Себестоимость одного часа работы на оборудовании НИЦ определяется по 6 основным элементам затрат – формула (48):

$$G = A + B + C + D + E + F \qquad (48)$$

где A – амортизационные отчисления по основному оборудованию, участвующему в проведении испытания, измерения, исследования, УДЕ/час; B – амортизационные отчисления по вспомогательному оборудованию, участвующему в проведении испытания, измерения, исследования, УДЕ/час; C – затраты на содержание и обслуживание основного и вспомогательного оборудования, участвующего в проведении испытания, измерения, исследования, УДЕ/час; D – затраты на оплату электроэнергии, УДЕ/час; E – затраты на расходные материалы, УДЕ/час; F – заработная плата оператора оборудования за один час работы, УДЕ /час.

Опираясь на расчетные значения себестоимости услуги НИЦ, его эффективность может быть оценена с использованием показателя рентабельности по формуле (49):

$$R = \frac{(Z - S)}{S} \times 100\% , \qquad (49)$$

где R – рентабельность деятельности НИЦ (%); Z – размер выручки (в стоимостном выражении объем услуг, оказанных НИЦ); S – себестоимость услуг.

Сопоставление параметров ресурсного потенциала, которые носят статический характер (при отсутствии форс-мажорных событий) и параметров экономической результативности использования ресурсного потенциала, иллюстрирующих достижения, которые весьма изменчивы во времени, позволяет перейти к системе координат «ресурсный потенциал (статика) – результативность использования ресурсного потенциала (динамика)».

Уровень образованности населения в области информационных технологий

Введем новый показатель - **индекс образованности населения (ИОН) и методике его формирования.**

Этот индекс учитывает разную степень образованности населения – от неграмотности до высшего образования. Учет численности граждан с поствысшим образованием (получивших два высших образования, ученые степени и т. д.) не учитывается: эти лица проходят вместе с получившими высшее образование. В признанном ООН индексе потенциала человеческого развития (ИПЧР) в качестве одного из трех составляющих его показателей принят уровень образованности населения в возрасте полных 19 – полных 49 лет, иначе говоря, от 20 до 50. Указанный показатель плюс еще два, а именно: средняя продолжительность жизни и уровень дохода на душу населения – обобщаются в ИРЧП вполне определенным образом, что дает численное представление о степени *развития человеческого потенциала*. При выработке нового показателя образованности населения предлагается сохранить, притом в качестве *основного* первый из обозначенных выше показателей ИРЧП. Но не ограничиться им, а добавить к нему еще два, с тем, чтобы объединить их определенным образом в ***новом показателе – индексе образованности населения (ИОН)*** страны, государства, региона, этноса и т.д. В каждой стране он может применяться с известными модификациями, учитывающими ее специфику. Предлагаемый способ исчисления ИОН обладает обобщенным характером.

Для полноты ИОН вводятся дополнительно два новых показателя образованности населения, в результате чего ИОН складывается из трех частей:

a) A - показатель среднего уровня образованности населения в активном, рабочем возрасте (20–50 лет);

b) S - численность студентов на 10000 чел. населения;

c) R - расходы на содержание системы образования и обучения учащихся, поступающие (по возможности или, по крайней мере, на основе приблизительной оценки) из всех источников, в % к ВВП страны в соответствующий период.

Поскольку значение ИОН определяется на основе измерения этих показателей, основным методологическим вопросом становится способ их сведения воедино. Предлагается суммировать их по простейшей схеме, весьма условно полагая параметры равнозначными. Иначе говоря, если обозначить эти параметры как a, b, c, то **значение ИОН выводится следующим образом** – формула (50):

$$ИОН = \frac{A + S + R}{3} \qquad (50)$$

Таким образом, чтобы учесть действие всех трех показателей, предполагается измерять ИОН как третью часть их суммы. Трудность состоит прежде всего в том, что получаемые величины *разнокачественные*, так как характеризуют разные явления и измеряются каждый своим способом. Чтобы преодолеть эту трудность, преобразуем абсолютные цифры частных показателей в *дробные* числа. *Числителем* выступает значение каждого их трех параметров в данной стране за данный период, а *знаменателем* – наивысшее (или вплотную приближающееся к нему) значение этого показателя в наиболее передовых странах. Сумма этих трех дробей, поделенная на три, дает значение ИОН, которое, таким образом, всегда меньше единицы – формула (51).

$$ИОН = \frac{A/A_{\max} + S/S_{\max} + R/R_{\max}}{3} \qquad (51)$$

Геополитический показатель (G)

Уровень террористической угрозы в информационном пространстве – $K_{4.1}$. Уровень террористической угрозы позволяет оценить возможные угрозы информационной безопасности со стороны террористических организаций и возможности страны в этих условиях противостоять техносферным операциям атакующей стороне – формулы (52, 53).

$$K_{4.1} = \left(\frac{L_{4.1.1} + k_{4.1} \cdot L_{4.1.2}}{L_{4.1}}\right)\left(\frac{D_{4.1.1}}{D_{4.1}}\right) \cdot F_{4.1}, \qquad (52)$$

где $L_{4.1.1}$ – количество террористических организаций (групп) действующих на территории государства; $L_{4.1.2}$ – количество террористических организаций (групп) действующих в регионе; $k_{4.1}$ – коэффициент учитывающий влияние на государство террористических организаций действующих в регионе; $L_{4.1}$ – количество террористических организаций (групп) действующих в мире; $D_{4.1.1}$ – количество террористических актов осуществленных в информационном пространстве государства; $D_{4.1.2}$ – количество террористических актов предотвращенных в информационном пространстве государства; $D_{4.1}$ – количество террористических актов в мировом информационном пространстве

$$F_{4.1} = D_{4.1.2} / D_{4.1.1}, \qquad (53)$$

$F_{4.1}$ – эффективность системы государства противодействия террористическим информационным атакам.

Уровень социально-политической стабильности в обществе – $K_{4.2}$. Данный показатель позволяет оценить возможности страны обеспечить необходимый уровень социально-политической стабильности в обществе, который влияет на появление возможных внутренних угроз, рассчитывается по формуле (54).

$$K_{4.2} = \left(\frac{L_{4.2.1}}{L_{4.2}}\right)\left(\frac{P_{4.2.1}}{P_{4.2}}\right), \qquad (54)$$

где $L_{4.2.1}$ – количество демонстраций экстремисткой направленности (стихийные восстания, бунты, погромы) проведенных в государстве; $L_{4.2}$ – количество демонстраций экстремисткой направленности в мире; $P_{4.2.1}$ – уровень качества жизни в государстве (доход на человека или средний прожиточный минимум); $P_{4.2}$ – максимальный уровень качества жизни в мире.

Уровень участия в союзах с другими государствами в информационной сфере – $K_{4.3}$. При оценке уровня участия в союзах с другими государствами учитывается количество как военно-политических блоков, в которых участвует государство, так и количество экономические союзов, которые так же могут иметь большое влияние при решении проведения техносферной операции – формула (55).

$$K_{4.3} = \left(\frac{J_{4.3.1} + k_{4.3.1} \cdot J_{4.3.2}}{J_{4.3}}\right)\left(\frac{B_{4.3.1} + k_{4.3.2} \cdot B_{4.3.2}}{B_{3.4}}\right), \qquad (55)$$

где $J_{4.3.1}$ – количество военно-политических блоков (договоров) в которых участвует государство в информационной сфере; $J_{4.3.2}$ – количество военно-политических блоков в которых участвуют союзники данного государства в информационной сфере; $k_{4.3.1}$ – коэффициент учитывающий влияние на государство действия союзных государств; $J_{4.3}$ – количество военно-политических блоков в мире поддерживающих информационный обмен; $B_{4.3.1}$ – количество экономические блоков в которых участвует государство в информационной сфере; $B_{4.3.2}$ – количество экономические блоков в которых участвуют союзники данного государства в информационной сфере; $k_{4.3.2}$ – коэффициент учитывающий влияние на государство действия союзных государств; $B_{4.3}$ – количество экономические блоков в мире поддерживающих информационный обмен.

Географическое положение страны в мире и размер территории – $K_{4.4}$ рассчитывается по формуле (56).

$$K_{4.4} = \left(\frac{H_{4.4.1}}{H_{4.4}}\right)\bullet\left(\frac{S_{4.4.1}}{S_{4.4}}\right), \qquad (56)$$

где $H_{4.4.1}$ – количество государств, с которыми граничит данное государство; $H_{4.4}$ – количество государств в мире; $S_{4.4.1}$ – размер территории государства; $S_{4.4}$ – размер территории земного шара (всех государств).

Уровень имеющихся ресурсов – $K_{4.5}$. Данный показатель определяет с одной стороны возможность страны существовать без взаимодействия с другими государствами, а с другой степень возможных притязаний агрессивных стран – формула (57).

$$K_{4.5} = \left(\frac{Q_{4.5.1}}{Q_{4.5}}\right)\bullet\left(\frac{W_{4.5.1}}{W_{4.5}}\right)\bullet\left(\frac{R_{4.5.1}}{R_{4.5}}\right)\bullet\left(\frac{I_{4.5.1}}{I_{4.5}}\right), \qquad (57)$$

где $Q_{4.5.1}$ – количество запасов государства по ресурсу – источников энергии (горючие ископаемые, гидро- и ветровая энергия, атомное топливо, биотопливо и т.д.); $Q_{4.5}$ – количество запасов в мире по ресурсу – источников энергии; $W_{4.5.1}$ – количество запасов государства по ресурсу – сырья и материалов (полезные ископаемые, леса, биоресурсы, запасы технической воды и др.); $W_{4.5}$ – количество запасов в мире по ресурсу – сырья и материалов; $R_{4.5.1}$ – количество запасов государства по ресурсу – продуктов питания (питьевая вода, растения – сельскохозяйственные культуры, продукты охоты и рыболовства); $R_{4.5}$ – количество запасов в мире по ресурсу – продуктов питания; $I_{4.5.1}$ – количество информационных ресурсов государства; $I_{4.5}$ – количество информационных ресурсов в мире.

Таким образом, общий информационный потенциал страны может оценен по формуле (58)

$$W_{ij} = f\left(Tk_t \bullet Ok_o \bullet Sk_s \bullet Gk_g\right), \qquad (58)$$

где k_t – весовой коэффициент информационно-технического показателя, k_o – весовой коэффициент организационного показателя, k_s – весовой коэффициент научного показателя, k_g – весовой коэффициент геополитического показателя.

Введение весовых коэффициентов, обусловлено не равноценным влиянием всех показателей на общий информационно-боевой потенциал, при чем $k_t > k_o >> k_s > k_g$.

При этом функционал явно будет иметь нелинейный вид (Рис. 4). Кривизна функции (коэффициенты) будут определены после набора статистических данных при оценке реальных объектов (стран).

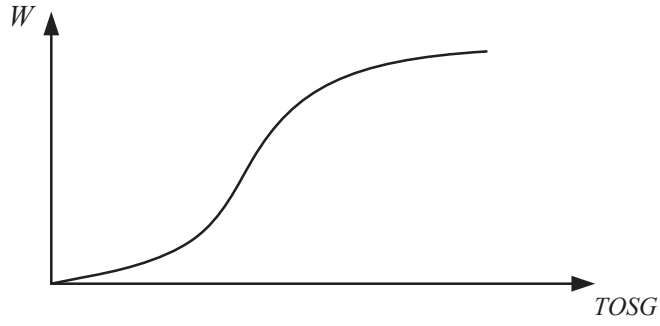


Рис. 2 Предполагаемая зависимость информационного потенциала от обобщенного показателя (TOSG)

Предложенный подход позволяет оценить информационно-боевой потенциал страны с учетом не только ее «внутренних» показателей, но и с учетом взаимосвязи с другими государствами и в частности с государством, относительно которого производится оценка, а так же учесть современные тенденции ведения техносферных боевых действий. Новизна предложенного подхода заключается в ассиметричности получаемых значений информационо-боевого потенциала страны, в зависимости от страны производящей оценку, что по мнению авторов статьи является более обоснованным в современных условиях глоболизации и интеграции.

Авторы отдают себе отчет, что предложенный подход требует существеного развития и детализации с привлечением значительного числа заинтересованных ученых.

Литература

1. Стародубцев Ю. И., Семенов С. С., Бухарин В. В., "Техносферная война" научно-технический журнал "Известия Орел ГТУ".-Орел: Орел ГТУ, №1 2011.
2. Стародубцев Ю. И., Семенов С. С., Бухарин В. В., "Техносферная война", научно-технический журнал "Вестник военного университета": М.: Наука-XXI, №4 2010.
3. Нечипоренко В. И., Структурный анализ и методы построения надежных систем. – М.: Советское радио, 1968, 256 с.
4. Балахонцев Н., Кондратьев А. Зарубежные методы оценки потенциала стран. // Зарубежное военное обозрение. – М.: Красная звезда – 2010. – № 11. – С. 101-104.
5. Стародубцев Ю. И., Семенов С. С., Бухарин В. В. Техносферная война // Военная мысль, №7, 2012.

6. 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.
7. 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.
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.

ASSESSMENT INFORMATION THE COMBAT POTENTIAL OF THE PARTIES IN TECHNOSPHERE CONFLICTS

Semenov S., Doc.Tech.Sci., docent, Military Academy of communications, SemSem@Yandex.ru
Gusev A., PhD, Military Academy of communications, AlexeyGusew@mail.ru
Barbotko N., Military Academy of communications, Barbotko-nikolay@mail.ru

Abstract
Annotation. In article the analysis of existing approaches to an assessment of fighting capacities of the parties in the modern conflicts is carried out. Offers on the account are made at an assessment of fighting potential of information component and mutual influence of the parties that allows to receive asymmetric estimates, depending on the party making an assessment. The analysis of modern methods of an assessment of fighting potentials showed not compliance of available views to new types of an antagonism of conflicting parties. Available techniques allow to estimate only the fighting potential determined by existence of armed forces and their arms, thus possibilities of information potential aren't considered. The main lack of these approaches of an assessment is linear additivity of considered parameters and determination of absolute potential, that is the estimated party was considered separately from an estimated conflicting party. For elimination of this defect it is offered to consider the information and fighting capacity of the party in the relation to a conflicting party, or relative fighting potential taking into account parameters reflecting ways of conducting tekhnosferny war. The main essence of an offered technique is transition from isolated (odnoideksny) assessment to integrative (two-index) at the accounting of information factors. The offered approach allows to estimate the information and fighting capacity of the country taking into account not only its "internal" indicators, but also taking into account interrelation with other states and in particular with the state concerning which the assessment is made and as to consider current trends of maintaining the tekhnosfernykh of operations. Novelty of the offered approach is in asymmetry of received values of informatsiono-fighting capacity of the country, depending on the country making an assessment that according to authors of article is more reasonable in modern conditions of globalization and integration. Decomposition of the main indicators on a row private is carried out, the generalized methods of their calculation are formulated. Possible ways of their development are planned. Authors realize that the offered approach demands essential development and specification with attraction of considerable number of the interested scientists

Keywords: Technosphere war, combat potential, informational confrontation, the asymmetry assessment, mutual influence of the parties.

References
1. Starodubcev U I, Semenov S S, Buharin V V, "Technosphere war" scientific-technical magazine "Izvestiya Orel STU".-Orel:, №1 2011.
2. Starodubcev U I, Semenov S S, Buharin V V, " Technosphere war" scientific-technical magazine " Bulletin of the military University ": science -XXI, №4 2010.
3. Nechiporenko V I, Structural analysis and methods for building reliable systems. – M.: Soviet radio, 1968, 256c.
4. Balahoncev N, Kondratyev A "Foreign methods of assessment of country capacity". // Foreign military review. – M.: Red star – 2010. – № 11. – C. 101-104.
5. Starodubcev U I, Semenov S S, Buharin V V, "Technosphere war" Military thought: №7 2012.
6Legkov, 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.
6. 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.
7. Legkov, K.E.Model of monitoring processes when ensuring operative control of operation of infokommunikatsionny networks of special purpose / A.N. Burenin, K.E.Legkov//H&ES: High technologies in space researches of Earth. - 2011.-№ 2. - Page 19-23.

К ВОПРОСУ ПОСТРОЕНИЯ СИСТЕМ УПРАВЛЕНИЯ СОВРЕМЕННЫМИ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Буренин А.Н., *к.т.н., доцент,*
Военно-космическая академия имени А.Ф. Можайского,
konferencia_asu_vka@mail.ru
Легков К.Е., *к.т.н.,*
Военно-космическая академия имени А.Ф. Можайского,
constl@mail.ru
Нестеренко О.Е.,
Военно-космическая академия имени А.Ф. Можайского,
benaffee@gmail.com

Ключевые слова:
инфокоммуникационная система, качество обслуживания, службы, управление, услуги, эффективность.

АННОТАЦИЯ

Рассматриваются вопросы организации процессов управления инфокоммуникационной сетью специального назначения (ИКС СН) входящих в состав сложных инфокоммуникационных систем, обеспечивающих поддержание на требуемом уровне показателей качества обслуживания спецпользователей и направленных на непосредственное изменение параметров, определяющих качественные показатели функционирования ИКС СН – процессов управления эффективностью.
В статье показано, что для выполнения задач, возлагаемых на ИКС СН, особенно в условиях силового и информационного противоборства, требуется чтобы она предоставляла обоснованный ранжированный перечень гарантированных услуг связи соответствующих служб: телефония, передача данных (ПД), электронная почта (ЭП), файловый обмен (ФО), видеоконференцсвязь (ВКС) и т.д. требуемого качества, для чего необходимо решить многокритериальную оптимизационную задачу. Сделан вывод о том, что многоуровневое управление ИКС СН в сложных условиях невозможно без гибкого оперативного распределения предоставляемых спецпользователям услуг в реальном масштабе времени. При этом обеспечение гибкости, масштабируемости и возможности наращивания номенклатуры требуемых услуг при управлении ИКС СН невозможно без рациональной организации процедур управления комплексом предлагаемых услуг.

Перспективы создания и развития современных систем инфокоммуникаций для нужд обороны, безопасности страны и обеспечения правопорядка [1] связаны с концепциями глобальной информационной инфраструктуры (Global Information Infrastructure, GII) и сетей следующего поколения (NGN-сетей) [2–5].

Концептуально ИКС СН включает в себя четыре основных элемента:

– спецпользователи (СП), которые являются источниками и получателями сообщений;

– информационные устройства (information appliances), которые применяются для хранения, обработки данных, и обеспечивают доступ к информации;

– коммуникационная инфраструктура, которая осуществляет передачу информации между географически удаленными информационными устройствами (она может быть представлена в виде транспортной сети и сетей доступа);

– собственно информация, которая включает в себя, прежде всего, видеоинформацию, речь, данные, а также прикладное программное обеспечение (ПО) (пользовательские приложения), конвертирующее сообщения из оригинальной формы (речь, изображение, компьютерная графика, видео) в электронную форму, доступную другим пользователям ИКС СН.

Взаимодействие перечисленных элементов показано на рис. 1.

В качестве платформы поддержки приложений применяются вычислительные средства в совокупности с операционными системами (ОС), микропрограммное обеспечение информационных устройств, прикладное ПО, специализированные процессоры и кодеки.

Платформы поддержки коммуникаций – это оконечное оборудование данных, модемы, устройства доступа различного назначения. Примеры средств доступа – абонентская линия связи до автоматической телефонной связи (АТС), линия DSL-доступа, сеть кабельного телевидения, оптическая линия доступа, канал радиосвязи, спутниковый канал, линия радиодоступа. Примеры ТКС – телефонная (Тф) сеть связи общего пользования, первичная сеть связи (на основе технологий PDH, SDH.WDM, DWDM и др.), сети передачи данных (СПД) различных стандартов (X.25, IP, Frame Relay, ATM, MPLS), ограниченно сеть Интернет. Все перечисленные программные и аппаратные компоненты ИКС СН, а также услуги, оказываемые на их основе, являются объектами управления.

Структура ИКС СН связывает между собой в единое целое сетевые ресурсы ведомственных сетей, устройства хранения и обработки данных пунктов управления (ПУ), а также ресурсы промежуточного ПО (middleware) для того, чтобы предложить стандартные услуги и поддержать приложения каждого пользователя. К средствам middleware в рамках ИКС СН можно отнести средства обеспечения информационной безопасности (ИБ), биллинг, а также средства сетевого управления и администрирования. Средства middleware могут быть одновременно доступны не только индивидуальным пользователям, но и достаточно большим группам сторонних абонентов (например, населению при обращении в различные силовые ведомства). Не участвуя непосредственно в преобразовании информации из одной формы в другую, средства middleware позволяют регулировать этот процесс, обеспечивая оптимальное распределение, защищенность и управляемость сетевых ресурсов. Услуги телекоммуникаций и приложения СП строятся из отдельных компонентов, которые обычно называют «блоками построения» (building blocks). Наличие тех или иных компонент определяет свойства и возможности ресурсов.

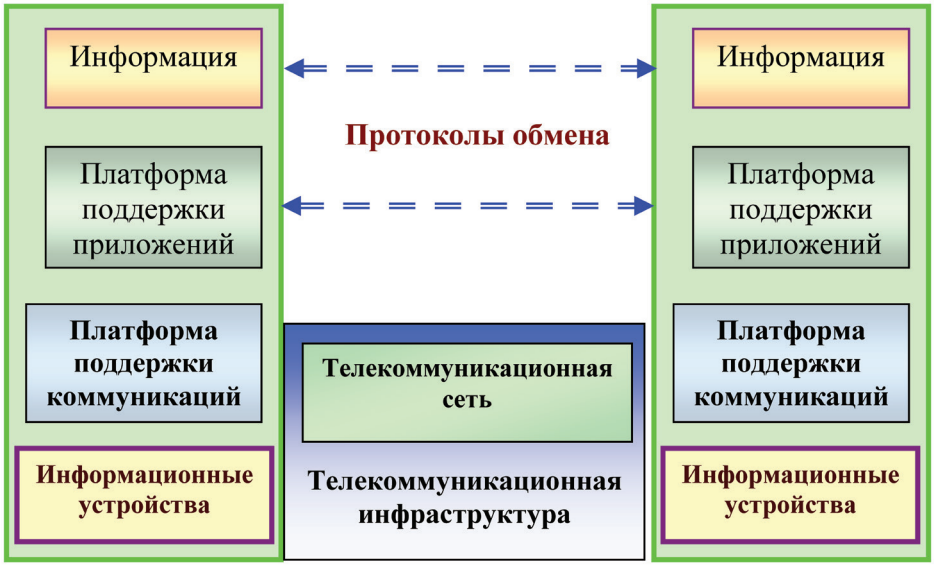


Рис. 1 - Взаимодействие основных элементов ИКС СН

В рамках ИКС СН услуги телекоммуникаций характеризуются транзакциями, которые осуществляет СП при запросе/активизации услуги. Приложения СП обладают полными правами по использованию данной услуги. Например, установка программы почтового клиента на его персональный компьютер или сервер приложений позволяет СП воспользоваться услугами сетевой электронной почты (разумеется, если СП имеет авторизацию и доступ к почтовой службе сети, что обеспечивается middleware). Данная программа имеет пользовательский интерфейс для практического использования услуги. Этот интерфейс можно рассматривать в самом широком смысле. Например, радиотелефон в системе подвижной связи ведомства также можно рассматривать как интерфейс пользователя, который, являясь информационным устройством, поддерживает пользовательские приложения (электронная телефонная книга) и средства коммуникаций (цифровое кодирование и передача речи).

Спецпользователи могут воспользоваться услугами ИКС СН напрямую или с помощью пользовательских приложений. Компоненты пользовательских приложений должны поддерживаться в ИКС СН. Компоненты приложений и услуг ИКС СН могут объединяться в пакеты, чтобы создать для СП требуемую услугу или предоставить доступ к приложению. Общая структура услуг информационной подсистемы в рамках ИКС СН представлена на рис. 2, при этом традиционные услуги Тф связи, как правило, предлагают пользо-

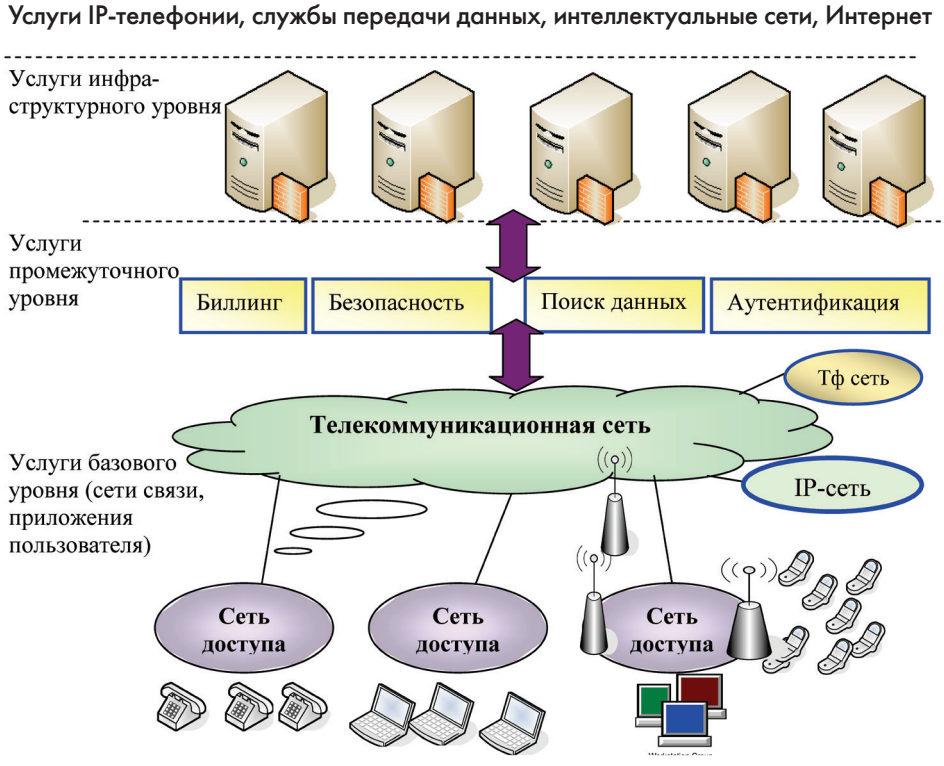


Рис. 2 - Уровни услуг ИКС СН

вателям технологии для доступа к новым услугам (за исключением базовых услуг связи), в то время как информационная технология – пользовательские приложения для доступа/организации услуг.

В перспективе целесообразна конвергенция этих элементов, так как уже сегодня получить доступ к большинству новых услуг связи невозможно без пользовательских приложений (Интернет-браузеров, почтовых программ, приложений для кодирования и передачи речи по IP-сетям).

Спектр услуг, которые предлагаются в рамках ИКС СН, достаточно широк и может динамически меняться вместе с изменением доступных ресурсов. Поэтому зачастую целесообразно классифицировать компоненты услуг, нежели сами услуги. Каждый компонент услуги зависит от ресурса, необходимого для ее поддержки. Различают несколько компонентов услуги.

Инфраструктурные компоненты услуги (infrastructural service components) предоставляют доступ к конечным информационным услугам (службам, телесервисам) для передачи речи через Тф сеть, пересылки файлов данных через Интернет и т. п. Инфраструктурные компоненты также могут включать услуги компонент промежуточного и базового уровня (base ware).

Компоненты услуг промежуточного (middleware) уровня используются, прежде всего, для обеспечения межсетевого взаимодействия и совместного функционирования нескольких приложений. Они позволяют объединять компоненты услуг базового уровня и поддерживать инфраструктуру, которая необходима для предоставления всего набора услуг. Как правило, компоненты услуг, которые могут быть предоставлены конечному пользователю, включают в себя описание способов предоставления этих услуг, способов учета их использования, средства мониторинга и описание уровней качества услуги.

В целом ИКС СН составляет совокупность баз данных(БД), средств обработки информации, взаимодействующих сетей связи и терминалов пользователя. Доступ к информационным ресурсам в ИКС СН реализуется посредством услуг связи нового типа, получивших название инфокоммуникационных услуг (ИУ). Предполагается, что они будут преобладать на сетях связи перспективных систем связи министерств, ведомств и корпораций уже в ближайшем будущем.

На сегодняшний день основное развитие ИУ происходит рамках сети Интернет, доступ к услугам которой осуществляется через традиционные сети связи. В то же время в ряде случаев услуги Интернет, ввиду открытости сети, отсутствия требуемого уровня безопасности, ограниченных возможностей ее транспортной инфраструктуры не отвечают требованиям специальных систем. По - этому развитие ИУ в рамках систем связи министерств, ведомств и корпораций требует решения задач эффективного управления информационными ресурсами с одновременным расширением функциональности сетей связи собственных систем связи.

К основным технологическим особенностям, отличающим ИУ от услуг традиционных сетей связи, можно отнести следующие:

– инфокоммуникационные услуги оказываются на верхних уровнях модели взаимодействия открытых систем (ВОС) (в то время как услуги связи предоставляются на сетевом уровне);

– большинство ИУ предполагает наличие клиентской части и серверной. Клиентская часть реализуется в оборудовании пользователя, а серверная – на специальном выделенном узле сети, называемом узлом служб;

– инфокоммуникационные услуги, как правило, предполагают передачу информации мультимедиа, которая характеризуется высокими скоростями передачи и несимметричностью входящего и исходящего информационных потоков;

– для предоставления ИУ зачастую необходимы сложные многоточечные конфигурации соединений;

– для ИУ характерно разнообразие прикладных протоколов и возможностей по управлению услугами со стороны пользователя;

– для идентификации абонентов ИУ может использоваться дополнительная адресация в рамках данной ИУ.

Большинство ИУ являются «приложениями», т. е. их функциональность распределена между оборудованием поставщика услуги и оконечным оборудованием пользователя. Как следствие, функции оконечного оборудования также должны быть отнесены к составу ИУ, что необходимо учитывать при их регламентации.

Модель, определяющая участников процесса предоставления ИУ и их

взаимоотношения, также отличается от модели традиционных услуг электросвязи, в которой было представлено всего лишь три основных участника: оператор, абонент и пользователь. Новая модель предполагает наличие поставщика услуг, который предоставляет ИУ абонентам и пользователям сетей. Сам поставщик является потребителем услуг переноса, предоставляемых ТС.

Обычно к ИУ предъявляются такие требования как:

– мобильность услуг;

– возможность гибкого и быстрого создания новых услуг;

– гарантированное качество услуг.

Большое влияние на требования к ИУ оказывает процесс конвергенции, приводящий к тому, что они становятся доступными пользователям вне зависимости от способов доступа.

При формировании требований к перспективным сетям связи ИКС СН необходимо учитывать особенности деятельности поставщиков услуг. В частности, современные подходы к регламентации услуг присоединения предусматривают доступ поставщиков услуг, в том числе и не обладающих собственной инфраструктурой, к ресурсам сети общего пользования на не дискриминационной основе. К основным требованиям, предъявляемым поставщиками услуг к сетевому окружению, относятся:

обеспечение возможности работы оборудования в «мультиоператорской» среде, т. е. увеличение числа интерфейсов для подключения к сетям нескольких операторов связи, в том числе на уровне доступа;

– обеспечение взаимодействия узлов поставщиков услуг для их совместного предоставления;

– возможность применения «масштабируемых» технических решений при минимальной стартовой стоимости оборудования.

Еще существующие в настоящее время традиционные сети связи с коммутацией каналов (Тф сети общего пользования) и коммутацией пакетов (СПД) в настоящее время не отвечают перечисленным выше требованиям. Ограниченные возможности традиционных сетей являются сдерживающим фактором на пути внедрения новых ИУ.

С другой стороны, наращивание объемов предоставляемых ИУ может негативно сказаться на показателях качества обслуживания вызовов базовых услуг существующих сетей связи. Все это вынуждает учитывать наличие ИУ при планировании способов развития традиционных сетей связи, в направлении создания сетей NGN или МСС, базовым принципом концепции которых является отделение друг от друга функций переноса и коммутации, функций управления вызовом и функций управления услугами.

Функциональная модель ИКС СН, в общем случае, может быть представлена тремя уровнями: транспортный; управления коммутацией и передачей информации; предоставления услуг и управления услугами.

Задачей транспортного уровня является коммутация и прозрачная передача информации пользователя.

Задачей уровня управления коммутацией и передачей является обработка информации сигнализации, маршрутизация вызовов и управление потоками.

Уровень предоставления и управления услугами содержит функции управления логикой услуг и приложений и представляет собой распределенную вычислительную среду, обеспечивающую:

– предоставление ИУ;

– управление услугами;

– создание и внедрение новых услуг;

– взаимодействие различных услуг.

Данный уровень реализует специфику услуг, и позволяет применять одну и ту же программу логики услуги вне зависимости от типа ТС (IP, ATM, FR, MPLS и т. п.) и способа доступа. Наличие этого уровня позволяет также вводить на сети любые новые услуги без вмешательства в функционирование других уровней.

Уровень управления услугами включает множество независимых подсистем («сетей услуг»), базирующихся на различных технологиях, имеющих своих абонентов и использующих свои, внутренние системы адресации, что весьма удобно при построении перспективной ИКС СН.

Назначением транспортной сети (ТС) ИКС СН, как уже отмечалось, является предоставление услуг переноса, а реализация ИУ осуществляется на базе узлов служб (SN) с привлечением узлов управления услугами (SCP).

Узлы служб рассматриваются в качестве серверов приложений для ИУ, клиентская часть которых реализуется оконечным оборудованием пользователя, в то время как SCP является элементом распределенной платформы, выполняющей функции управления логикой и атрибутами услуг.

Совокупность нескольких узлов служб или узлов управления услугами, задействованных для предоставления одной и той же услуги, образуют сетевую платформу управления услугами определенного типа. В состав каждой платформы входят узлы административного управления услугами и серверы различных приложений.

Оконечные/оконечно-транзитные узлы ТС, в принципе, могут выполнять функции узлов служб, т. е. состав функций граничных узлов может быть расширен за счет добавления функций предоставления услуг и для построения таких узлов может использоваться технология гибкой коммутации (Soft Switch), которая также позволяет согласовывать различные системы сигнализации.

Инфокоммуникационные услуги предполагают реализацию на основе функциональной модели распределенных (региональных) БД, например, в соответствии с Рекомендацией МСЭ-Т X.500. Доступ к БД организуется с использованием протокола LDAP.

Вышеуказанные БД позволяют решить следующие задачи:

– создание абонентских справочников;

– автоматизация взаиморасчетов используемых ресурсов между потребителями и поставщиками услуг;

– обеспечение взаимодействия между потребителями и поставщиками в процессе предоставления услуг;

– обеспечение взаимодействия терминалов с различной функциональной организацией информационно-справочных услуг.

Концепция создания и развертывания для многих ИКС СН во многом опирается на технические решения, уже разработанные международными организациями стандартизации. Так, взаимодействие серверов в процессе предоставления услуг предполагается осуществлять на базе протоколов, специфицированных IETF (MEGACO), ETSI (TIPHON), Форумом 3GPP2 и т. д. Управления услугами в МСС СН осуществляются протоколами H.323 (H.325), SIP.

В качестве технологической основы построения транспортного уровня в на-

стоящее время рассматриваются технологии IP-MPLS, ATM, FR, MPLS over ATM и редко IP поверх SDH (WDM и т. д.) для выделенных направлений.

Для доступа СП к услугам используются:

– интегрированные сети доступа, подключенные к оконечным узлам ИКС СН и обеспечивающие подключение СП как к самой сети, так и к традиционным сетям (например, Тф связи);

– традиционные сети (Тф, СПД), абоненты которых получают доступ к услугам ИКС СН через узлы, подключенные к шлюзам (Media Gateway).

На Тф сети для доступа часто пропускную способность абонентского участка увеличивают за счет применения технологии xDSL, а на сетях подвижной связи – 2G, 3G и 4G.

Особенностями ИКС СН с точки зрения управления является то, что она состоит из большего числа разнотипных компонентов, а не из сравнительно небольшого количества менее разнообразных крупных коммутационных устройств. Кроме того, в ИКС СН будет поддерживаться большее число интерфейсов, чем в существующих сетях, разные системы сигнализации и более высокая пропускная способность. Все это ведет к необходимости пересмотра принципов и подходов к управлению для ИКС СН по всему спектру задач управления.

Система управления ИКС СН должна представлять собой набор решений, обеспечивающих управление сетями, реализованными на базе различных технологий (фиксированные и мобильные Тф сети, СПД, сети сигнализации и т. д.), предоставляющих различные услуги и построенных на оборудовании различных производителей. Система управления будет строиться с использованием объектно-ориентированной распределенной структуры.

Одной из главных особенностей СУ ИКС СН является открытая модульная архитектура, позволяющая разрабатывать и внедрять новые модули, работать с существующими приложениями и модернизировать установленные модули. Для реализации интегрированного управления системами и сетями независимо от их производителей и технологий применяются разнообразные стандарты и протоколы, такие как SNMP, SMIP, CORBA. Стандартом же управления в сетях в настоящее время дефакто является протокол SNMP. В модели TMN предполагалось использование протоколов ВОС. Однако практическая реализация СУ на базе TMN оказалась сложной, медленной и дорогостоящей, в ней недостаточно проработаны вопросы управления услугами. В последнее время активно развиваются и реализуются решения по организации управления на базе архитектуры CORBA, которая является весьма перспективной, особенно на верхних уровнях управления.

Существенное влияние на создание автоматизированной СУ (АСУ) оказывает мировая тенденция эволюции СУ, заключающаяся в переходе к системам с функциональностью класса Operation Support System (OSS) и далее – Business Support System (BSS), однако это затрагивает в основном функциональные особенности подсистем АСУ.

В ИКС СН СУ будет в первую очередь нацелена на решение конкретных задач, а уровневая архитектура TMN, хотя и сохранится, уже не будет иметь первостепенное значение для всей ИКС СН, и отойдет на второй план, так как TMN ориентирована на управление одной ТКС, а их в составе ИКС СН несколько и разного рода с отличными целевыми задачами. Большую значимость приобретают вопросы управления сетями и управления услугами.

Интерфейсы СУ должны быть открытыми. Отличительными чертами подобных интерфейсов являются: стандартизированные протоколы (например, CMIP, SNMP, FTP, FTAM и др.), использование формальных языков для описания стандартизированных интерфейсов (например, CORBA, IDL, JAVA, GDMO, ASN1 и др.), стабильность, которая позволяет вносить только те изменения, которые будут обратно совместимы.

Для посылки аварийных сообщений могут быть реализованы протоколы CMIP, SNMP или CORBA с объектной моделью, определенной в X.733, а для организации услуг – интерфейсы CORBA, для пересылки данных о рабочих характеристиках в части телекоммуникационной поддержки может применяться протокол FTP, а для обмена информацией между ДЛ ОУ – протоколы электронной почты (ЭП) SMTP, IMAP4, POP3.

Основными требованиями, предъявляемые к СУ ИКС СН, являются:

– обеспечение гибкости реализации СУ и ее совместимости с другими решениями в ИКС СН, высокая надежность и, как результат – высокое качество обслуживания;

– реализация возможностей ДЛ по модификации ПО СУ с целью выполнения специфических функций и введения новых услуг через изменение конфигурации сетей ИКС СН, учитывающие требования по информационной безопасности процессов управления;

– реализация компонентных решений, которые упрощают возможности оператора по введению новых СП и функций;

– обеспечение практической реализации подготовленных решений по организации управления и быстрого наращивания перечня услуг в сжатые сроки в условиях возможного существенного изменения обстановки и возрастания угроз кибератак.

Таким образом, гибкость и масштабируемость решений, закладываемых в процедуры управления ИКС СН, позволят легко адаптироваться к быстро появляющимся новым технологиям и продуктам, к изменяющимся потребностям пользователей, а также к возможным атакам и воздействиям противника.

Подсистема управления услугами (ПУУ) (сервисами) ИКС СН решает задачи управления, которые затрагивают не - посредственные интересы СП этих услуг.

Управление услугами осуществляется на основе информации, которая предоставляется подсистемами управления сетями (ПУС) ИКС СН. Подсистема управления услугами «не видит» детальную внутреннюю структуру каждой сети, т. е. структура каждой сети, входящей в состав ИКС СН, скрыта от ПУУ, а маршрутизаторы, коммутаторы, АТС, сервера и шлюзы IP-телефонии, СПД не могут непосредственно управляться из ПУУ.

Основными функциями управления, выполняемыми ПУУ являются:

– контроль качества услуг связи (задержки пакетов, времена доставки сообщений, уровень потерь, оценка вероятности своевременной доставки и т. д.);

– распределение услуг по СП (кому, какие услуги, какого качества, параметры услуг);

– учет объема использования услуг связи отдельными СП;

добавление и удаление СП в списки

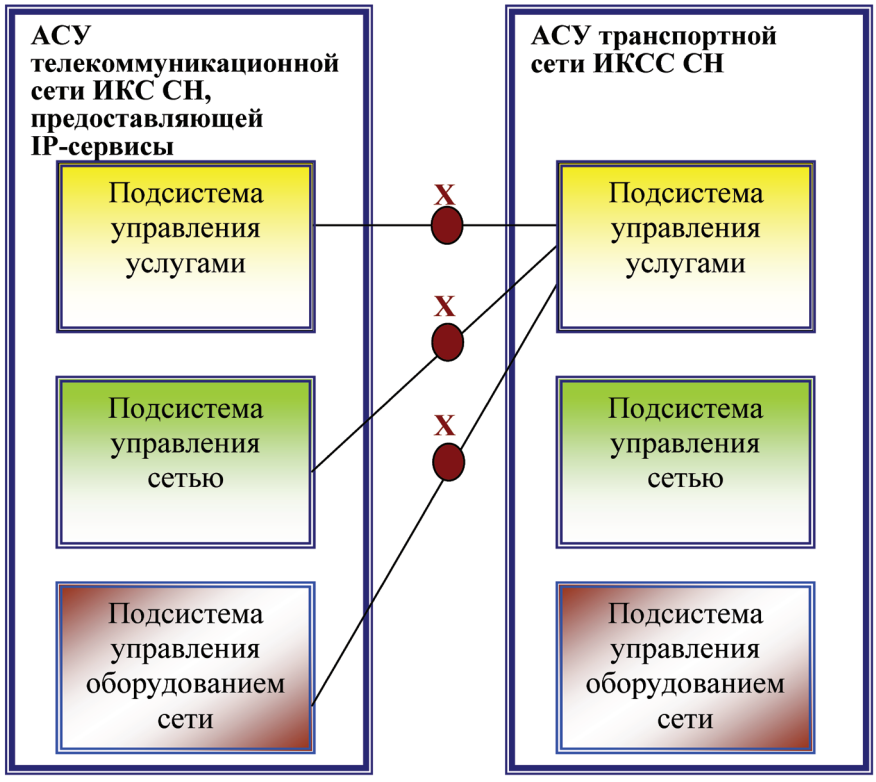


Рис. 3 - Точки взаимодействия автоматизированной системы управления сетей ИКС СН с автоматизированной системой управления транспортной сети, предостав-ляющей им услуги переноса

предоставляемых услуг;

– назначение сетевых адресов (если услуга предоставляется сетью) или адресов внутри службы, номеров Тф аппаратов;

– сопровождение группы адресов или номеров.

Управление услугами используется и при взаимодействии СУ разных сетей ИКС СН, например две СУ разными сетями обмениваются информацией по управлению для того, чтобы управлять своими взаимосвязанными сетями (межсетевое управление). Из соображений безопасности и в условиях возможных кибератак нарушителей каждая из этих систем будет скрывать внутреннюю структуру своей сети связи от другой СУ. Обмен будет осуществляться только в той части информации управления, которая необходима для обеспечения качества предоставления услуг связи – данные о приоритетах или профиль услуг.

Другой вариант использования ПУУ связи при межсетевом взаимодействии состоит в том, что СУ ТКС (например, сети доступа) или службы связи, предоставляющей определенные виды услуг, сами используют услуги ТС с ее СУ переносом информации, для того, чтобы соединить коммутационные элементы ТКС или службы. Этот вариант типичен для сетей ИКС СН, предоставляющих услуги IP-телефонии, IP-телевидения или других IP-сервисов, которые используют услуги переноса ТС на FR-, ATM-, SDH, MPLS- или NG SDH-технологиях, чтобы осуществить соединение маршрутизаторов, причем для этого варианта характерна организация трех точек взаимодействия СУ с тремя необходимыми интерфейсами на пути от одной СУ к другой (рис. 3).

На стороне СУ ТС все точки взаимодействия соединяются с ПУУ АСУ ТС. Таким образом, ПУУ ТС также не позволяет подсистеме управления другой ТКС ИКС СН контролировать и изменять внутреннюю организацию ТС. Для поставщика IP-услуг ТС ИКС СН является неким отдельным элементом, что обеспечивается наличием точки взаимодействия и стыком с подсистемой управления коммутационными элементами ТКС, предоставляющей услуги связи (IP-услуги). В случае если подсистеме управления ТКС предоставлена возможность выбора качества обслуживания с заданием, например пропускной способности при передаче по ТС, то создается точка взаимодействия ПУУ ТС с подсистемой управления ТКС. Вместе с тем, учитывая, что пропускная способность транспортного «соединения» по ТС ИКС СН непосредственно сказывается на качестве обслуживания (QoS) СП, то точку взаимодействия целесообразно организовать и с ПУУ ТКС. Аналогично, вариант, предусматривающий обмен информацией взаимодействия между АСУ ТКС, предоставляющей IP-услуги СП, и СУ присоединенной сети доступа, также обеспечивает доступ СУ сети доступа только к общей информации о качестве предоставленных услуг.

Несмотря на то, что практически единственным протоколом управления, применяемым на уровне управления сетевыми элементами, является протокол SNMP из стэка протоколов TCP/IP, на других уровнях управления (сетями и услугами) его применение потребует интерпретации параметров MIB верхних уровней управления. Кроме того, эффективность применения SNMP на уровнях управления сетью и услугами недостаточно высока, а функциональные возможности – ограничены. Все это приводит к актуальности использования на верхних уровнях управления ИКС СН протоколов управления, определенных моделью управления ВОС.

Данные протоколы управления (CMIP), осуществляя передачу информации управления, могут создавать экземпляры объектов управления одного и того же уровня, т. е. нет «главного» менеджера, однако из «интеллектуальности» агентов CMIP (при сравнении с SNMP-агентами) следует ответственность агентов за сбор информации на основании запросов. Каждая программа-менеджер или программа-агент является достаточно «интеллектуальной». Протоколы CMIP обеспечивают намного более мощные средства управления, чем SNMP. Стандарты CMIS/CMIP позволяют в рамках многоуровневой модели предлагать жизнеспособные стандарты для прикладных программ управления сетями ИКС СН.

Стандарты CMIS/CMIP существенно превосходят протокол SNMP по уровню решений проблем ИБ [3, 5], имеют много функций контроля, управления и поддержки сложных инфраструктур современных сетей связи. Ориентация на

объекты управления и объектно-ориентированный подход позволяет стандартам CMIS/CMIP оставаться базовыми в концепции TMN и применять их в практике управления сетями и услугами в ИКС СН.

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.

TO A QUESTION OF CREATION OF CONTROL SYSTEMS OF THE MODERN INFOCOMMUNICATION NETWORKS OF A SPECIAL PURPOSE

Burenin A., Ph.D, docent, Military Space Academy, konferencia_asu_vka@mail.ru

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

Nesterenko O., Military Space Academy, benaffee@gmail.com

Abstract

Questions of the organization of management processes by an infocommunication network of a special pur-pose (ICN SP) the difficult infocommunication systems which were a part providing maintenance at demanded level of indicators of quality of service of specialusers and directed on direct change of parameters, defining quality indicators of functioning ICN SP management of efficiency are considered.

In article it is shown that for performance of the tasks assigned to ICN SP, especially in the conditions of a power and information antagonism, it is required that it provided the reasonable ranged list of the guaranteed communication services of the relevant services: telephony, the data transmission (DT), the e-mail (EM), the file ex-change (FE), video conferencing (VC) of, etc. demanded quality for what it is necessary to solve a multicriteria op-timizing problem.

The entered concept a condition of management ICN SP which has allowed rather strictly to consider options of achievement of the objectives, put before ICN SP and to connect them with management procedures, and also to formulate a number of optimizing tasks for creation of procedures of optimum control by efficiency of its functioning.

Keywords: information communication system, quality of service, service, manage-ment, services, efficiency.

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 pur-pose', 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.

Уфа
18-20 марта

Форум "БЕЗОПАСНОСТЬ"

Выставка "Безопасность-2014"

XXI специализированная выставка

XIX специализированная выставка

Выставка "Связь. Инфоком-2014"

450080, Уфа, а/я 144, тел./факс: (347) 256-51-80, 256-51-86, 256-58-21
E-mail: secur@bashexpo.ru, infocom@bashexpo.ru
www.bashexpo.ru

ИНТЕЛЛЕКТ ВО ВСЕМ

Благодаря постоянному развитию компьютерной техники мы способны сделать разумным все, что нас окружает. Возможности в этом начинании безграничны: процессоры и датчики можно разместить даже под кожей человека или в его обуви.

Вообразите, что вы живете в доме, где всё подключено к интернету. Всё, что вам нужно в течение дня, работает «вживую», начиная с момента вашего пробуждения. Кровать знает, когда нужно проснуться. Она дает команду радиоприемнику, чтобы он включился и вы могли послушать информацию о дорожных пробках, прогноз погоды и любимую музыку. Она приказывает кухне приготовить кофе. Во время утренних процедур зубная щетка сообщает вам, что пора посетить стоматолога и записывает на прием в удобное время. Душ регулирует температуру воды с учетом ваших предпочтений, а зеркало в ванной напоминает о необходимости принять витамины. Когда вы одеваетесь, зеркало помогает выбрать одежду с учетом погоды и ваших планов. А при выходе из дома дисплей на двери сообщает, что вы забыли взять кошелек.

Мы подошли к тому рубежу, когда огромные массивы информации и данных превращаются в знания, способные изменить нашу жизнь к лучшему. С помощью «доверенных сред», в которые мы (и вещи) помещаем нужную информацию, мы можем улучшить жизнь самым невероятным образом.

Корпорация Intel как лидер в области компьютерных инноваций разрабатывает и создает основополагающие технологии для широкого спектра вычислительных устройств и приложений. Intel предлагает инструментальные средства, которые позволяют использовать комплексные данные и интеллектуальные возможности подключенных к сети устройств просто, легко и почти незаметно для нас, даже если при этом меняется весь стиль жизни.

Интеллектуальные вещи

Дома, в автомобиле, в офисе нас окружают интеллектуальные устройства, которые собирают данные о том, как мы живем и что делаем. Интеллект во всем — это возможность обмена данными в самых неожиданных местах, с участием предметов, которые обычно не считают приборами. Например, кроссовки, нарукавная повязка или солнцезащитные очки могут сообщить, где лучше заняться оздоровительным бегом. Датчики в телефоне, автомобиле, на уличных вывесках информируют об уровне загрязнения воздуха. Мы вступаем в эру, когда самые обычные предметы смогут общаться с нами и друг с другом, выполняя задания по команде и предоставляя такие данные, которых у нас прежде никогда не было.

Итак, мы имеем миллиарды устройств с триллионами соединений, генерирующие огромные объемы данных. Однако без «цифрового разума», который объединял бы эти устройства и понимал эти данные, непомерный объем информации будет почти бесполезным для человека. К примеру, вы собираетесь совершить утреннюю пробежку в соседнем парке. Лето, на улице смог. Датчики в парке ведут активный мониторинг качества воздуха, но какой смысл в датчиках, если они «не понимают», что загрязненный воздух негативно скажется на вашем здоровье. И что хорошего в этих датчиках, если они не знают маршрута вашей пробежки? И наконец, в чем польза, если они не предупредят, что лучше выбрать другой маршрут? «Интеллект во всем» означает не просто оснастить различные предметы функцией сбора данных. Это повсеместные изменения, поскольку умные микросхемы позволят окружающей среде воспринимать и понимать информацию, чтобы в конечном итоге служить нам. Это дополнение к интеллектуальности и коммуникациям, которое «оживит» устройства и наше окружение.

Инновации для интеллектуальной жизни

«Интеллект во всем» — это неотвратимая реальность, которая свяжет человека и принадлежащие ему устройства и вещи таким образом, чтобы сэкономить ему время, силы и сделать возможным то, что раньше было недостижимо.

У большинства из нас сегодня есть смартфоны, у некоторых — умные телевизоры; мы все чаще встречаем умные

автомобили на дороге. Вскоре в нашу жизнь войдут умные часы, подсчитывающие калории, столовые приборы, ведущие мониторинг пищи, абажуры, меняющие характеристики в зависимости от времени суток. Датчики можно запрограммировать на выполнение операций самого разного рода: измерение параметров окружающей среды, отправка данных, сообщение о температуре, весе, скорости и т.д. Одним из примеров может служить интеллектуальная система уличного освещения в Хельсинки (Финляндия), где светильники оснащены датчиками, анализирующими окружающую среду и изменяющими яркость освещения в зависимости от силы солнечного света, погодных условий и других факторов.

Все больше устройств будут становиться интеллектуальными. По оценкам, к 2020 г. свыше 50 млрд устройств на земном шаре (около 6 на каждого человека), будет подключено к интернету.

Реализации концепции «интеллект во всем»

Об умном городе будущего мы говорим уже давно, но тогда почему он до сих пор не стал реальностью? Есть три основных момента в практическом осуществлении этой концепции. Во-первых, необходимо снизить стоимость решений, во-вторых, повысить эффективность использования энергии в датчиках и микросхемах и наконец, обеспечить обмен данными между устройствами, чтобы они могли поставлять информацию и использовать ее непрерывно.

В 2020 г. к интернету будет подключено 50 млрд устройств, а число людей, имеющих доступ к Всемирной сети, утроится. Возникет проблема эффективности энергопотребления. Ведь нужно снабжать энергией все эти гаджеты, управляемые компьютерами. Концепция предполагает незаметное для нас использование подключенных устройств, помогающих улучшить жизнь, но это осуществимо только в том случае, если нам не придется беспокоиться о замене батарей. Одним из решений проблемы является использование энергии окружающей среды. Энергия при каждой возможности собирается малыми порциями от таких источников, как Солнце, телевизионные антенны, солнечные панели, и даже от обуви во время прогулки.

Что касается стоимости, то сегодня потребители платят высокую цену за дополнительные микросхемы и датчики, необходимые для сетевого обмена данными с дверным замком, термостатом или лампочкой. Однако закон Мура гарантирует, что микросхемы и датчики, встраиваемые в эти устройства, со временем станут еще более высокоскоростными, миниатюрными и дешевыми. Стоимость передачи данных снижается. При этом инженеры, проявляющие интерес к инновациям, и новые фирмы изобретают недорогие умные системы датчиков.

В будущем умные устройства смогут не просто направлять вам оповещения, но и беспрепятственно подключаться к сети и получать обновленные данные с других устройств, они будут работать по принципу «настроил и забыл». Мы уже имеем нечто подобное в умных домах, которые автоматически выключают свет и отопление, когда никого нет в помещении, а также в умных светофорах, которые помогают улучшить движение транспорта, реагируя на пробки и автомобильные аварии.

Устройства и сенсорные технологии становятся дешевле, миниатюрнее и эффективнее, и мы видим, что рассматриваемая концепция в конечном итоге воплощается в реальность, позволяя нам подключать к сети больше устройств и получать больше информации. По мере увеличения числа таких устройств их мощность и возможности будут расти. Такие перемены позволят подключать к сети все новые предметы по всему миру и обеспечат всем нам реальные преимущества.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ВСЕОБЪЕМЛЮЩИЙ ИНТЕРНЕТ

Хейден Л.,
компания Cisco Systems

Ключевые слова:
информационная безопасность, Всеобъемлющий Интернет, человеческий брандмауэр, культура информационной безопасности.

Сетевое общество распространилось по всей планете, вызвав фундаментальные изменения и создав новые возможности для целых стран, компаний и для каждого из нас. Люди, связанные между собой Всемирной паутиной, повсюду находят новые способы для успешного развития экономики, социального взаимодействия и личного процветания. Сегодня мы носим с собой множество сложнейших устройств: смартфонов, планшетов и других портативных компьютеров, подключенных друг к другу. Социальные сети сделали виртуальное общение столь же важным, как личное деловое взаимодействие. Новые технологии все шире проникают в повседневную жизнь, и если раньше человек просто использовал сети, то теперь он стал неотъемлемой частью сетевой среды. Во Всеобъемлющем же Интернете люди и технологии будут обмениваться информацией, вести совместную работу и взаимодействовать без каких-либо ограничений.

Учитывая вышеизложенное, реализация Всеобъемлющего Интернета становится важнейшей задачей на будущее, и ключевую роль в этом сыграют те люди, кто воспользуется им и его потенциалом . Вместе с тем история хакерских атак и компьютерных преступлений показывает теневую сторону сетевой отрасли, где возникают новые возможности для преступлений, мошенничества и информационных диверсий. Поэтому организациям следует учиться находить золотую середину между преимуществами беспрепятственного распространения информации и необходимостью защиты информационных и деловых активов.

В современных организациях, связанных глобальной сетью, управление рисками и защита информационных активов стали критически важными компонентами любой успешной ИТ-стратегии. Откуда бы угроза ни исходила: от консумеризации технологии и политики BYOD или от так называемых «комплексных постоянных угроз», подразумевающих долгосрочное несанкционированное использование чужих информационных ресурсов с целью воровства или шпионажа, – сетевая безопасность становится критически важным фактором, повышающим эффективность бизнеса и социальную ценность сетевых информационных систем.

Как защитить Всеобъемлющий Интернет? Как помочь организациям оградить от этих угроз своих сотрудников и ценную корпоративную информацию? Успешные организации разрабатывают комбинированные стратегии управления рисками, включающие определение сложности проблем, формирование устойчивой культуры безопасности и внедрение передового опыта, обеспечивающего защиту информации на основе объективных данных.

Наиболее успешные программы информационной безопасности не замалчивают риски и не пытаются упрощать проблемы. Исследования показывают, что с рисками лучше справляются те организации, которые учитывают возможность неудач и постоянно стремятся обнаружить признаки проблем, чреватых большим кризисом. Уделяя должное внимание поиску и своевременному устранению проблем на их ранней стадии, эти организации не дают малым угрозам перерасти в катастрофу. А вот в тех организациях, где руководство неспособно различать крупные и мелкие проблемы и считает недопустимым малейший сбой, сотруд-

ники опасаются докладывать о неприятностях и умалчивают о них до тех пор, пока игнорировать их не становится невозможно.

Еще одна важная область управления рисками в сфере информационной безопасности в рамках Всеобъемлющего Интернета связана с человеческими культурой и поведением. Организации начинают сознавать, что устранение проблем, связанных с информационной безопасностью, невозможно без высоконадежной культуры безопасности, которая, в сущности, представляет собой «человеческий брандмауэр» из общих приоритетов и знаний. Человеческие эмоции и доверие будут влиять на Всеобъемлющий Интернет совсем не так, как при взаимодействии с обезличенными технологиями и устройствами. Вспомним эволюцию фишинга и прочих «социальных атак», цель которых не машина, а человек. В прошлом такой «социальный инжиниринг» считался особым видом мошенничества, не связанным с традиционным хакерством. А сегодня он стал обыденным делом. Согласно отчету компании Verizon по информационной безопасности за 2013 год (2013 Verizon Data Breach Investigations Report), социальный инжиниринг стал причиной каждого третьего информационного взлома, изученного авторами этого документа.

Высоконадежная культура информационной безопасности предполагает хорошее знание ее сути и ее врагов, внедрение решений по защите данных на всех уровнях, обучение персонала, а также принятие мер, побуждающих сотрудников распознавать проблемы в этой области и своевременно на них реагировать. Там, где создана высоконадежная культура информационной безопасности, людей объединяют общие убеждения по поводу необходимости защищать информационные активы и понимание возможных последствий взлома системы безопасности.

Чтобы сформировать высоконадежную культуру информационной безопасности, руководство должно подавать личный пример поведения в этой области, совершенствовать систему обучения и информирования кадров, неустанно работать над тем, чтобы лучше понимать и преобразовывать корпоративную культуру. В разных компаниях корпоративная культура может быть более жесткой или более гибкой, более бюрократичной или демократичной, и точно так же разные компании могут иметь разный уровень информационной безопасности. Но при этом те организации, где необходимость соответствующего поведения на всех без исключения иерархических уровнях недооценивается, более уязвимы для всякого рода неприятностей.

Еще одно условие успешной стратегии в области информационной безопасности состоит во внедрении правил, основанных на объективных данных. Иными словами, решения в области информационной безопасности должны приниматься на основе реальных измерений и фактических данных и не зависеть от каких-либо спекуляций и домыслов. Измерение уровня информационной безопасности – относительно молодая, но развивающаяся дисциплина. Главным локомотивом ее развития служит необходимость перевода информации о стоимости и пользе мер по защите данных на язык, понятный другим участникам бизнеса, многие из которых не понимают «айтишный» жаргон. Несогласованность приоритетов и результатов деятельности специалистов по информационной безопасности и бизнесменов может сформировать у бизнеса ложное представление, будто в ИТ-отделах работают одни ретрограды, стоящие на пути экономического роста и инноваций.

Метрики информационной безопасности и прозрачность операций помогают организациям наращивать свои возможности и лучше бороться с угрозами. Многие современные программы в области защиты данных управляют рисками на основе допущений и спекулятивных предположений и зачастую исходят не из эмпирических данных, а из взломов систем безопасности, получивших широкую огласку. В этом случае оценка рисков может оказаться неполной или неточной, одни угрозы будут недооцениваться, а другие, наоборот, переоцениваться. Повышение качества сбора и оценки данных может принести в этом смысле определенную пользу, но в условиях нехватки финансовых средств и ресурсов достичь этого непросто.

Организации, стремящиеся повысить качество метрик безопасности, убеждаются в том, что в результате информационная безопасность становится таким же бизнес-процессом, как работа с финансами, логистикой или кадрами. Наглядность таких операций позволяет коррелировать решения в сфере информационной безопасности с другими деловыми приоритетами, убедительнее обосновывать просьбы расширить поддержку и повысить финансирование решений по защите данных. Управление информационной безопасностью на основе объективных данных (равно как использование объективных данных во всех других сферах деятельности) улучшает эффективность работы, способствуя росту и развитию бизнеса.

В предстоящее десятилетие технологические вопросы будут по-прежнему играть ключевую – но не доминирующую, как прежде – роль при обсуждении проблем информационной и сетевой безопасности. Во Всеобъемлющем Интернете, который нам предстоит создать, поведение и культура людей и целых организаций станут определяющим фактором в том, что касается применения технологий и защиты информационных активов. Впрочем, это естественный процесс, через который прошли предыдущие технологические революции от изобретения печатного станка до появления телефона. Объемы и сложность угроз будут нарастать, и системы информационной безопасности должны адекватно реагировать на эти угрозы. Это означает необходимость смириться с тем, что развитие Всеобъемлющего Интернета чревато определенными рисками, и требует разработки мощной и надежной культуры информационной безопасности, способной адаптироваться к переменам. Одновременно надо работать над тем, чтобы лучше понимать и измерять цели и результаты стратегий, направленных на защиту информации.

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

КОНЦЕПТУАЛЬНЫЕ ВОПРОСЫ МНОГОУРОВНЕВОЙ ЗАЩИТЫ ОБЪЕКТОВ И ИНФОРМАЦИИ

Никифоров О.Г., *к.т.н., доцент,*
ОАО «Научно-исследовательский институт «Рубин»,
nikiforov-55@mail.ru

Ключевые слова:
информационная безопасность, многоуровневая защита, опасные события, агрегатная модель, вектор показателей эффективности.

АННОТАЦИЯ

Рассматриваются концептуальные вопросы построения многоуровневых систем защиты, предназначенных для решения задач обеспечения безопасности объектов и информации различного назначения. Показано, что предложенных подход к построению таких систем защиты позволяет преодолеть существующую грань, проводимую между двумя важнейшими классами систем защиты – системами защиты информации и системами защиты информационной инфраструктуры, предоставляя для их структурной организации единый теоретический базис.

Представлен анализ основных функций систем многоуровневой защиты и приведены основные принципы, на которых она основывается. Определено, что процесс защиты должен содержать подпроцессы, которые по своему содержанию условно могут быть разделены на пять уровней. Приведено основное содержание указанных подпроцессов. При этом проведена композиция подпроцессов каждого из уровней на составные процедуры. Особое внимание уделено процедурам, которые реализуются на уровне сбора и обработки информации, так как именно от их качества в первую очередь зависит эффективность защиты.

Рассмотренный процесс многоуровневой защиты описан в виде агрегативной схемы. Представлено обобщенное выражение для определение вектора показателей эффективности систем многоуровневой защиты. Раскрыты основные компоненты указанного вектора, определяющие состав и содержание процедур защиты и входящие в состав обобщенного выражения.

Введение

Основная цель многоуровневой многопозиционной защиты (ММЗ) состоит в обеспечении требуемого уровня защищенности от воздействия дестабилизирующих факторов на информационную инфраструктуру объектов управления и связи и информацию, хранимую, обрабатываемую и передаваемую на этих объектах в рамках существующих технологий, с использованием аппаратно-программных средств и способов защиты объектов и информации. На современном этапе это направление совершенствования информационной безопасности объектов управления и связи представляется наиболее перспективным и экономически оправданным. Очевидно, что достижение указанной цели возможно при условии развития теоретического базиса ММЗ [1, 2].

Основным направлением использования ММЗ является реализация систем обеспечения информационной безопасности объектов управления и связи, поддерживающих традиционный подход к обеспечению физических и логических контролируемых зон. В рамках общей теории информационной безопасности подход к созданию систем ММЗ позволяет, как представляется, преодолеть существующую грань, проводимую между двумя важнейшими классами систем защиты – системами защиты информации и системами защиты информационной инфраструктуры, предоставляя для их структурной организации единый теоретический базис.

Концептуальные основымногоуровневой защиты

Независимо от физической природы всей возможной совокупности потенциальных угроз, система обеспечения информационной безопасности объектов управления и связи должна выполнять следующие основные функции:

осуществлять предотвращение или существенное усложнение действий дестабилизирующих факторов, приводящих к реализации одной из возможных угроз, то есть обеспечивать непосредственную защиту подвергаемых угрозам ресурсов объекта защиты;

обеспечивать своевременное и достоверное обнаружение опасных событий, заключающихся в том, что их наступление открывает реальную возможность реализации какой-либо угрозы объекту защиты;

своевременно пресекать действия дестабилизирующих факторов, представляющие собой угрозу информационной безопасности объекта управления и связи.

Очевидно, что техническую основу для выполнения данных функций может составлять многоуровневая многопозиционная система защиты, создание которой базируется на следующих основных принципах [2].

1. Независимо от физической природы потенциально возможной угрозы система защиты должна противодействовать ее реализации с определенной (требуемой) степенью надежности.

2. В системе должен осуществляться мониторинг состояния защищенности объекта защиты, основной функцией которого является своевременное и достоверное обнаружение опасных событий.

3. В системе должна осуществляться идентификация обнаруженного опасного события и принятие наиболее рационального применительно к возникающей конкретной ситуации решения о принятии мер по пресечению действий факторов, угрожающих информационной безопасности объекта защиты.

4. Система должна быть построена таким образом, чтобы независимо от вида реализуемой угрозы всегда существовали условия, необходимые для ее пресечения.

5. Система должна обеспечивать пресечение действий дестабилизирующих факторов, представляющих собой угрозу информационной безопасности объекта защиты, с требуемой степенью надежности.

В соответствии с рассмотренными функциями и принципами система обеспечения информационной безопасности объекта управления и связи может содержать ряд следующих уровней:

уровень непосредственной защиты, обеспечивающий предотвращение или существенное затруднение воздействия физических или логических атак на защищаемый ресурс объекта;

уровень обнаружения, обеспечивающий своевременное и достоверное обнаружение наступления опасного события и передачу информации об этом событии органу, принимающему решение на обеспечение пресечения возможной угрозы;

уровень сбора и обработки информации;

уровень оперативного реагирования системы защиты, обеспечивающий своевременное создание условий для нейтрализации опасного события и воздействующей в результате его наступления угрозы;

уровень нейтрализации опасного события и воздействующей в результате его наступления угрозы.

Каждый из указанных уровней системы защиты может быть реализован с использованием различных технических и программных средств с их многопозиционным использованием, обеспечивающим высокую логическую, техническую и оперативную устойчивость работы системы защиты.

На содержательном уровне последовательность реализации многоуровневой защиты представляется следующим образом.

На первом уровне реализуются административно-организационные, инженерно-технические и программно-логические меры защиты от воздействия всего спектра дестабилизирующих факторов.

На втором уровне рассматриваемого процесса защиты осуществляется мониторинг – сбор, хранение и, возможно, отображение состояния системы защиты и обнаружения признаков или факта возникновения опасных событий.

На третьем уровне производится верификация и идентификация обнаруженного опасного события и осуществляется принятие решения по способу его нейтрализации. Уместно предположить, что в процессе функционирования объекта и системы его защиты некоторые опасные события могут повторяться: спецотказы средств защиты [3], удачные попытки их преодоления нарушителем и т. д. В таком случае после установления факта наличия данного вида опасного события возможно использование ранее принимавшихся вариантов его нейтрализации.

Возможны следующие подходы к решению задачи идентификации [3]. Первый основан на использовании дополнительных специальных средств, таких как средства видеоконтроля

для систем физической защиты, измерительные приборы и аппаратура дл средств защиты информации от утечки и специальные программные продукты для верификации и идентификации компьютерных атак. Второй подход базируется на использование шаблонов ситуаций. Эти шаблоны должны включать в себя параметры, описывающие состояние системы защиты и объекта защиты, поведение нарушителей, внешние факторы и т. п. Совпадение ситуации с заданной в одном из шаблонов должно указывать на наличие опасного события. Преимущества подхода связаны с относительной простотой и оперативностью идентификации. Реализационный аспект данного подхода может сдерживаться трудоемкостью построения множества шаблонов, описывающих все допустимые состояния ММЗ и действия нарушителей. Кроме того, нетривиальной задачей является отбор параметров, включаемых в шаблоны: их малое число не в состоянии адекватно описать ситуацию, большое число приведет к усложнению системы мониторинга.

Компромиссное решение видится в разумном сочетании указанных подходов. Типовые предопределенные ситуации описываются с помощью шаблонов. Дополнительно осуществляется верификация и идентификация опасных событий с использованием специальных средств. Комплексное использование подходов позволит сбалансированно выявлять как типовые, так и неординарные опасные события, приводящие к необходимости их нейтрализации.

Затем осуществляется выработка варианта реагирования на опасное событие. Его реализация состоит в синтезе возможных вариантов, удовлетворяющих критерию выполнения требований к эффективности нейтрализации опасного события и процессам, ее реализующим. Задача синтеза может формулироваться как оптимизационная. В этом случае отыскивается единственное наилучшее решение (вариант реагирования). При невозможности ее решения в такой постановке по определенным формальным и/или эвристическим правилам генерируются допустимые альтернативные варианты реагирования с последующей их оценкой и выбором наиболее предпочтительного.

На четвертом уровне осуществляется оперативное реагирование на опасное событие с целью его нейтрализации. Реализация процедур данного уровня зависит от организации управления защитой и от пространственно-технологических возможностей системы защиты по пресечению опасных событий. Меры, реализуемые на данном уровне, являются обязательными только для систем защиты, в которых нейтрализация угроз связана с необходимостью организации специальных действий, например пресечение нарушений безопасности информации, передаваемой по линиям связи.

Последний пятый уровень предусматривает осуществление непосредственной нейтрализации опасных событий. Особую сложность мероприятия этого уровня представляют для систем защиты, для которых нейтрализация характерных для них опасных событий осуществляется путем разрешения конфликтной ситуации и требует использования специальных ресурсов. Завершают рассматриваемую последовательность мер данного уровня контроль результатов нейтрализации опасного события и их оценивание по установленным критериям.

Представление процесса ММЗ в виде функционирования агрегативной схемы [4, 5] позволяет описать его следующим образом

$$\vec{U}(t) = F\{\vec{X}(t), \vec{Y}(t), \vec{S}, \vec{P}, \vec{R}, \vec{Z}\}, \quad (1)$$

где $\vec{X}(t)$ – вектор характеристик опасных событий, характерных для рассматриваемого объекта защиты; $\vec{Y}(t)$ – вектор характеристик среды функционирования системы ММЗ; $\vec{S}$ – вектор описания структуры системы ММЗ, $\vec{P}$ – вектор требований к результатам ММЗ; $\vec{R}$ – вектор требований к процессам, реализуемым в ходе обеспечения многоуровневой защиты, $\vec{Z}$ – вектор параметров процедур многоуровневой защиты; $\vec{U}(t)$ – вектор показателей эффективности ММЗ; F – функционал, определяющий порядок перехода от указанных векторов к вектору $\vec{U}(t)$.

В свою очередь, компоненты выражения (1) имеют вид:

вектор характеристик опасных событий:

$$\vec{X}(t) = \left\{\vec{b}(t), \vec{h}(t), \vec{g}(t)\right\},$$

где $\vec{b}(t)$ – вектор значимости (степени опасности) опасных событий; $\vec{h}(t)$ – вектор вероятностно-временных характеристик опасных событий, $\vec{g}(t)$ – вектор пространственного положения опасных событий;

вектор характеристик среды:

$$\vec{Y}(t) = \left\{\vec{q}(t), \vec{d}(t), \vec{k}(t)\right\},$$

где $\vec{q}(t)$ – вектор природно-климатических условий функционирования системы ММЗ; $\vec{d}(t)$ – вектор социально-политических условий функционирования системы ММЗ; $\vec{k}(t)$ – вектор технологических ограничений на построение и функционирование системы ММЗ;

вектор описания структуры системы ММЗ:

$$\vec{S} = \left\{\left(\vec{M}\right), \left(\vec{N}_m\right)\right\},$$

где $\left(\vec{M}\right)$ – множество позиций, на которых обеспечивается многоуровневая защита, $\left(N_m\right)$ – множество рубежей защиты на каждой *m*-й позиции;

вектор требований к эффективности ММЗ:

$$\vec{P} = \left\{\left(\vec{p}^{\,\text{рб}}\right), \left(\vec{p}^{\,\text{инт}}\right)\right\},$$

где $\left(\vec{p}^{\,\text{рб}}\right)$ – множество рубежных значений показателей эффективности ММЗ, $\left(\vec{p}^{\,\text{инт}}\right)$ – множество интервальных значений показателей эффективности ММЗ.

вектор требований к процессам, составляющим ММЗ:

$$\vec{R} = \{(\vec{r}^{\,\text{нз}}), (\vec{r}^{\,\text{м}}), (\vec{r}^{\,\text{и}}), (\vec{r}^{\,\text{ор}}), (\vec{r}^{\,\text{н}})\},$$

где $\vec{r}^{\,\text{нз}}$ – вектор требований к характеристикам средств непосредственной защиты; $\vec{r}^{\,\text{м}}$ – вектор требований к характеристикам средств мониторинга опасных собы-

тий; $\vec{r}^{\,\text{и}}$ – вектор требований к характеристикам средств идентификации опасных событий и принятия решений по их нейтрализации; $\vec{r}^{\,\text{ор}}$ – вектор требований к возможным действиям по созданию условий для успешной нейтрализации опасных событий; $\vec{r}^{\,\text{н}}$ – вектор требований к средствам и способам нейтрализации опасных событий.

вектор параметров процедур ММЗ:

$$\vec{Z} = \{(\vec{z}^{\,\text{нз}}), (\vec{z}^{\,\text{м}}), (\vec{z}^{\,\text{и}}), (\vec{z}^{\,\text{ор}}), (\vec{z}^{\,\text{н}})\},$$

где $\vec{z}^{\,\text{нз}}$ – вектор характеристик средств непосредственной защиты; $\vec{z}^{\,\text{м}}$ – вектор характеристик средств мониторинга опасных событий; $\vec{z}^{\,\text{и}}$ – вектор характеристик средств идентификации опасных событий и принятия решений по их нейтрализации; $\vec{z}^{\,\text{ор}}$ – вектор возможных действий по созданию условий для успешной нейтрализации опасных событий; $\vec{z}^{\,\text{н}}$ – вектор средств и способов нейтрализации опасных событий.

Заключение

Подобное представление процесса многоуровневой многопозиционной защиты позволяет сделать следующие выводы.

Многоуровневая защита может быть использована для решения задач обеспечения информационной безопасности объектов различного назначения как в части защиты самого объекта, так и в части защиты информации, на нем циркулирующей.

По своей сущности системы многоуровневой защиты в совокупности с системой управления относятся к классу организационно-технических систем с рефлексивным управлением и обладают следующими принципиальными особенностями:

наличием цели функционирования, в качестве которой выступает обеспечение требуемого состояния защищенности объекта защиты от возможных угроз и соответствующих им опасных событий; близость к данному состоянию формализуется в виде некоторого функционала качества, экстремум которого соответствует оптимальному состоянию системы с учетом ограничений;

наличием неопределенности относительно опасных событий, приводящих к появлению потенциальной возможности для противодействующей стороны для реализации угроз объекту защиты;

случайными значениями параметров, характеризующих процедуры каждого из уровней защиты вследствие начальной неопределенности и меняющихся условий функционирования, в результате чего событие, заключающееся в достижении цели, поставленной перед системой защиты, тоже будет случайным.

Анализ процесса и условий функционирования ММЗ позволяет сформулировать следующие гипотезы:

а) о существовании возможности создания системы ММЗ и поддержания показателей ее качества в требуемых пределах и возможности ее оптимального синтеза по критерию качество/стоимость;

б) о существовании компромисса между ресурсными и временными издержками на создание системы ММЗ и эффективностью ее применения.

Литература

1. Никифоров, О. Г. О научно-методическом подходе к оцениванию эффективности функционирования многоуровневых систем защиты. [Текст] // Вопросы радиоэлектроники. –Сер. СОИУ. – 2012. – Вып. 2. – С. 120–123.

2. Никифоров, О. Г. О некоторых концептуальных вопросах построения многоуровневых многопозиционных систем защиты объектов и информации [Текст] // Труды XI Российской научно-технической конференции «Новые информационные технологии в системах связи и управления», 6 июня 2012. Секция 2. Теория и технологии создания аппаратуры систем связи и управления. – Калуга: Изд-во ООО «Ноосфера», 2012. – С. 583–585.

3. Масановец, В. В., Фисун, А. П., Никифоров, О. Г. Методы комплексного контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления: Монография. Под общей ред В. В. Масановца. – М.: Управление делами Президента Российской Федерации, 2009. – 368 с.

4. Советов, Б. Я., Яковлев, С. А. Моделирование систем: Учебник.– М.: Высшая школа, 1998. – 319 с.

5. Бусленко, Н. П. Моделирование сложных систем.– М.: Наука, 1978.– 399 с.

CONCEPTUAL IDEAS ABOUT MULTILEVEL PROTECTION OF FACILITIES AND INFORMATION

Nikiforof O., Ph.D, associate professor, nikiforov-55@mail.ru

Abstract

Here we have common ideas of multilevel protection systems design for facilities and information. This approach allows building both information and facility protection systems based on common theoretical foundation. There are functions and basic principles of the multilevel protection systems. Protection flow has five levels. Procedures of each level are examined. Information picking and processing procedures have the biggest attention. Multilevel protection flow described as an aggregative scheme. There is a formula for efficiency indicators of multilevel protection systems.

Keywords: information security, multilevel protection, dangerous events, aggregative model, efficiency indicators.

References

1. Nikiforov, O. G. About a scientific and methodical approach to estimation of efficiency of functioning of multilevel systems of protection. // Questions radio electronics. - Ser.SOIU. - 2012. - Vol. 2. - Page 120-123.

2. Nikiforov, O. G. About some conceptual questions of creation of multilevel multiitem systems of protection of objects and information //Works XI of the Russian scientific and technical conference «New information technologies in communication systems and managements», on June 6 2012. Section 2. Theory and technologies of creation of equipment of communication systems and management. - Kaluga: JSC Noosfera publishing house, 2012. - Page 583-585.

3. Masanovets, V.V., Fisun, A.P., Nikiforov, O.G. Metody of complex control of safety of information on objects of telecommunication systems of state bodies: Monograph. Under the general edition V. V. Masanovtsa. - M: Administration of the President of the Russian Federation, 2009. - 368 pages.

4. Sovetov, B. I., Yakovlev, S.A. Modelirovaniye of systems: Textbook. - M: The higher school, 1998. - 319 pages.

5. Buslenko, N.P. Modelirovaniye of difficult systems. - M: Science, 1978. - 399 pages.

6. Glushkov, V.M., Ivanov, V.V., Yatsenko, V.M. Modelirovaniye of developing systems. - M: Science, 1983.-350 pages.

К ВОПРОСУ ПОСТРОЕНИЯ ИНТЕГРИРОВАННОГО НАЗЕМНОГО КОМПЛЕКСА В СТРУКТУРЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ КОСМИЧЕСКИМИ АППАРАТАМИ

Рыбочкин Ю.Н., *к.т.н.,*
Военно-космическая академия имени А.Ф.Можайского,
ryun-73@mail.ru
Травкин В.В., *к.т.н.,*
Военно-космическая академия имени А.Ф.Можайского,
tr-75@yandeks.ru

Ключевые слова:
радиоэлектронные систем, главный испытательный космический центр, отдельный командно-измерительный комплекс, отдельный измерительный пункт, автоматизированные системы управления.

АННОТАЦИЯ

Применение РЭС НАКУ при выполнении стоящих перед ними задач осуществляется в составе космических систем (комплексов) во взаимодействии с другими средствами, обеспечивающими запуск и управление КА. Космическая система включает в себя один или несколько космических комплексов и специальный комплекс. Космический комплекс представляет собой совокупность взаимосвязанных орбитальных и наземных технических средств, предназначенных для самостоятельного решения задач в космосе и из космоса. В состав космического комплекса в общем случае входят: орбитальная группировка КА, ракетно-космический комплекс, наземный комплекс управления и комплекс средств посадки и послеполетного обслуживания. Специальный комплекс представляет собой совокупность взаимосвязанных орбитальных и наземных технических средств, предназначенных для приёма, обработки, хранения специальной (космической) информации, поступающей с КА, и выдачи её потребителям.
Наземные средства, принятые на вооружение ГИКЦ, располагаются на отдельных командно-измерительных комплексах (ОКИК), отдельных измерительных пунктах (ОИП) и Испытательных центрах (ИЦ) и составляют наземную группировку ГИКЦ. Территориальное расположение ОКИК и ОИП сложилось с учетом обеспечения требований по оперативности, глобальности и надежности управления КА при их прохождении в зонах радиовидимости наземных РЭС, а также требуемой точности определения параметров их орбит. Средства, расположенные на ОКИК (ОИП), связаны со средствами ИЦ с помощью системы связи и передачи данных (ССПД) НАКУ.

Возможны различные варианты организации управления КА и приема с КА целевой информации. В частности, могут быть использованы специализированный НКУ и интегрированный с ним НСпК, как это имеет место в зарубежных космических системах [4]. Поскольку применение космических средств в соответствии с их целевым назначением обеспечивается соответствующей организацией управления полетом и информационным обменом с КА на орбите, при разработке новых космических систем специального назначения выбор принципов построения НКУ и НСпК относится к числу наиболее важных системных решений. Практически принципы построения определяются выбранным вариантом: для НКУ – многоцелевым или специализированным, для НСпК – структурно независимым или интегрированным с НКУ.

Проведенный технико-экономический анализ показывает, что при разработке перспективных космических систем специального назначения наряду с вариантом передачи КА на управление НАКУ целесообразно рассматривать вариант использования совмещенного наземного комплекса (СНК), объединяющего специализированные НКУ и НСпК в единый интегрированный комплекс. При определенных условиях и научно обоснованных системных решениях интеграции НКУ и НСпК достигается синергетический эффект повышения эффективности выполнения целевых задач космической системы за счет взаимного усиления функциональных возможностей каждого из взаимодействующих комплексов.

Создание для разрабатываемой космической системы специального назначения интегрированного космического комплекса для решения задач управления, приема и обработки целевой информации с КА специального назначения, таким образом, предполагает два взаимосвязанных системных решения:

– во-первых, использование для управления орбитальной группировкой КА разрабатываемой космической системы специализированного НКУ;

– во-вторых, интеграцию НКУ и НСпК в единый СНК.

НКУ принадлежит ключевая роль в обеспечении применения космических систем по целевому назначению, поскольку выполнение КА целевых задач осуществляется по программам, передаваемым с Земли средствами НКУ. Сравнительный анализ вариантов построения НКУ управления отечественных космических систем показывает, что в современных условиях использование многоцелевого НКУ означает передачу орбитальной группировкой КА разрабатываемой космической системы на управление НАКУ. Такой вариант управления КА является основным для отечественных космических систем военного и двойного назначения, однако он сложился в процессе их эволюционного развития с учетом преемственности в организации целевого применения и технологии управления КА.

В случае передачи орбитальной группировки КА той или иной космической системы на управление НАКУ организация, в интересах которой функционирует космическая система, выступает в качестве заказчика, который формирует заявки на управление КА, обеспечивающие его целевое применение, а НАКУ, по сути, оказывает заказчику операторские услуги по управлению КА. При таком варианте организации управления КА НАКУ выполняет следующие задачи [4]:

– планирование применения средств НКУ;

– непосредственное выполнение сеансов управления КА;

– оперативное управление работой средств НКУ при подготовке и в ходе выполнения сеансов управления КА;

– обеспечение приема, передачи и обработки всех видов информации, циркулирующей в НКУ при решении задач командно-программного обеспечения, навигационно-баллистическое обеспечение и информационно-телеметрическое обеспечение;

– осуществление частотно-временного обеспечения средств НКУ;

– обеспечение НКУ каналами связи для передачи всех видов информации, циркулирующих в НКУ;

– техническую эксплуатацию средств НКУ, а также зданий и сооружений, в которых они расположены.

При передаче орбитальной группировки КА перспективной космической системы на управление НАКУ в его Главном центре (ГЦ) будет развернут центр управления полетом (ЦУП) КА, для непосредственного проведения сеансов управления КА будет использоваться одна из штатных командно-измерительных систем (КИС) НАКУ, при этом на КА должна быть установлена соответствующая бортовая аппаратура КИС. Заказчик взаимодействует с ЦУП, выдавая туда заявки на управление КА, а все планирование применения средств НКУ и непосредственное взаимодействие с КИС осуществляет ЦУП по принятой в НАКУ технологии информационного взаимодействия с использованием системы связи и передачи данных НАКУ. В этих условиях проявляются достоинства, связанные с использованием для проведения сеансов управления КА всех территориально распределенных на территории страны средств НАКУ, а также с сокращением сроков разработки и создания АСУ КА за счет формирования НКУ на основе существующих средств управления и обработки информации НАКУ и использования готовых технических решений реализации БКУ.

Однако вариант реализации НКУ космической системы на основе средств НАКУ имеет и ряд недостатков, которые оказываются особенно заметны при разработке и развертывании новых, не имеющих близких аналогов, космических систем специального назначения, а именно:

– универсальность средств управления и измерений НАКУ приводит к невозможности учета специфики и особенностей технологического и целевого управления КА специального назначения, а также выполнения повышенных требований по предотвращению несанкционированного доступа (НСД) к информации, циркулирующей в НКУ и в радиоканалах управления и информационного обмена с КА;

– большинство из средств управления КА, входящих в состав НАКУ, были разработаны в 80–90-е годы прошлого века, многократно выработали гарантийный ресурс и не могут обеспечить требуемого для космических систем специального назначения уровня надежности проведения операций управления и информационного обмена с КА;

– заложенные в КИС НАКУ технические решения и характеристики радиоканалов даже с учетом их модерни-

зации не соответствуют современным требованиям к характеристикам помехозащищенности, скорости передачи информации, точности измерений для радиоканалов управления, измерений и информационного обмена с КА;

– разработанные для работы во взаимодействии со штатными средствами НАКУ бортовые радиотехнические комплексы КА имеют массогабаритные характеристики и энергопотребление, не соответствующие современным требованиям к бортовой аппаратуре, особенно для КА, создаваемых на основе малогабаритных космических платформ;

в функции НКУ, сформированного на основе средств НАКУ, не входит прием с КА целевой (специальной) информации, а в составе НАКУ отсутствуют соответствующие РЭС, поэтому при передаче КА на управление НАКУ необходима разработка полнофункционального НСпК с пунктами приема и центрами обработки информации, функционирующего параллельно с НКУ.

Следует также отметить следующее обстоятельство. КИС, привлекаемые для проведения сеансов управления КА, могут одновременно применяться и в составе других НКУ, и возможны конфликты при выполнении заявок на проведение операций управления КА, полученные от различных заказчиков. Поэтому в масштабе НАКУ кроме планирования применения средств каждого НКУ осуществляется координационное планирование применения всех средств. Для этого в состав ГЦ входит Система оперативного координационного планирования применения (СОКПП) средств НАКУ. Алгоритмы координационного планирования, реализуемые СОКПП, позволяют частично устранить возникающие конфликты на основе приоритетов, однако определение приоритетов осуществляется непосредственно в СОКПП, и в случае неустранимых конфликтов неизбежно невыполнение одной или нескольких конфликтующих заявок.

Использование для управления КА перспективной космической системы специального назначения специализированного НКУ предусматривает его разработку и последующее использование в составе космической системы без передачи орбитальной группировки КА на управление НАКУ. Данный вариант требует решения задач обоснования состава, структуры, принципов действия НКУ и средств, входящих в него, их реализацию и дальнейшую эксплуатацию, однако позволяет в полной мере учесть специфику целевых задач космической системы и оптимизировать расходы на ее эксплуатацию. При этом возможна организация взаимодействия с НАКУ по отдельным вопросам в рамках согласованных протоколов взаимодействия.

Преимуществами использования специализированного НКУ, функционирующего в составе космической системы, являются:

– учет специфики и особенностей построения и функционирования космических систем специального назначения, в том числе в вопросах технологического и целевого управления КА и предотвращения НСД к радиоканалам управления, измерений и информационного обмена с КА;

– отсутствие необходимости координации применения средств НКУ с планами применения других космических систем и связанных с этим ограничений при реализации ТЦУ КА, в полной мере согласованных с задачами целевого применения КА;

– отсутствие технологической привязки к существующим штатным средствам НАКУ, возможность реализации современных принципов построения и унификации оборудования наземных и бортовых средств управления, измерений и информационного обмена с КА, в том числе с учетом стандартов ITU, ISO, CCSDS;

– возможность выбора рациональной структуры и состава средств НКУ, реализации в нем технологических циклов управления (ТЦУ) КА, в наибольшей степени учитывающих принципы применения КА при решении целевых задач и выполнении на орбите различных операций программы полета;

– возможность поэтапного развертывания специализированного НКУ с учетом частичного или полного развертывания орбитальной группировки КА и результатов функционирования космической системы на предыдущих этапах.

Для перспективных космических систем специального назначения эти преимущества имеют важное значение вследствие особенностей командно-программного и навигационно-баллистического обеспечения управления КА, связанных с характером их целевого применения (вследствие наличия нескольких режимов орбитального полета и целевого применения, особо ответственных операций, выполняемых на орбите, маневрирования и других особенностей). При этом затраты на разработку и эксплуатацию специализированного НКУ частично или полностью компенсируются исключением расходов по оплате представляемых НАКУ услуг по управлению КА.

Состав элементов специализированного НКУ должен определяться с учетом ряда факторов. Укажем их.

1. Обоснование структуры, принципов функционирования, эксплуатации и технического обслуживания специализированного НКУ проводится на этапе проектирования космической системы в рамках проводимых научно-исследовательских и опытно-конструкторских работ.

2. Все разрабатываемые элементы НКУ должны соответствовать требованиям современных стандартов и рекомендаций, регламентирующих задачи, алгоритмы и методы управления и информационного обмена с КА.

3. Элементы НКУ должны быть унифицированными, что позволит на всех этапах функционирования космической системы проводить эффективное поэтапное развертывание средств управления и информационного обмена с КА без дополнительных затрат на их проектирование.

4. Средства НКУ должны быть максимально гибкими и модернизируемыми. Для этого большая часть элементов НКУ должна реализовываться на основе ЭВМ, на программируемых логических интегральных схемах, цифровых сигнальных процессорах, а в основе общего и специального программного обеспечения должны лежать объектно-ориентированные технологии программирования, в том числе с использованием универсальных языков моделирования (UML).

5. Вопросы предотвращения НСД к радиоканалам управления и информационного обмена с КА должны решаться на всех уровнях управления КА, приема и обработки информации, включая

аутентификацию абонентов на всех средствах НКУ и в БКУ.

6. Построение наземной информационной сети НКУ должно осуществляться по сетевой иерархической структуре с возможностью защищенного удаленного доступа и контроля всех средств на основе современных стандартизованных технологий и протоколов защищенного информационного обмена.

Учет перечисленных факторов при реализации НКУ в составе многоцелевого комплекса существующих средств НАКУ затруднителен и зачастую нецелесообразен. Кроме того, в специализированном НКУ в полной мере могут быть учтены требования, предъявляемые к созданию и эксплуатации средств управления КА разрабатываемой космической системы, по ряду позиций существенно отличающиеся от требований к средствам управления КА в других космических системах. В то же время с НАКУ может быть организовано технологическое взаимодействие по отдельным вопросам управления КА, а также по вопросам технического обеспечения эксплуатации средств НКУ, расположенных в районах расположения пунктов командно-измерительных пунктов (ОКИК, ОИП) НАКУ.

Основными функциями НСпК является прием с КА и обработка целевой (специальной) информации. Для этого в состав НСпК входят средства приема информации с КА, ее обработки, хранения, распределения и доведения до потребителей, расположенные в пунктах приема информации (ППИ) и центрах обработки (ЦО) информации. В подавляющем большинстве космических систем НСпК являются специализированными, что связано как с их различной ведомственной принадлежностью, так и со спецификой приема с КА и обработки различных видов целевой информации. НСпК также часто объединяются с центром управления космической системой.

Так, НСпК космических систем наблюдения решает следующие основные задачи [6]:

– прием информации (данных наблюдения) с КА;

– обработку информации, принятой с КА, и представление ее потребителям;

– формирование и передачу в ЦУП заявок на управление КА и планирование программы его полета;

– анализ по результатам обработки принятой информации качества функционирования аппаратуры БСпК и разработку рекомендаций по дальнейшей программе полета;

– регистрацию (запись) принятой информации для хранения и последующей обработки.

В случае выбора при разработке перспективной космической системы варианта использования специализированного НКУ целесообразно его объединение с НСпК в составе интегрированного СНК. Преимуществами объединения специализированного НКУ с НСпК в составе СНК космической системы специального назначения являются:

– учет специфики и особенностей построения и функционирования космических систем специального назначения, в том числе в вопросах приема целевой информации с КА и предотвращения НСД к радиоканалам информационного обмена с КА;

– реализация централизованного управления космической системой при сосредоточении функций управления полетом КА, планирования целевого применения КА и обработки целевой информации, принимаемой с КА, в рамках единого центра управления системой;

– совмещение функций управления КА и приема с КА целевой информации в многофункциональных наземных радиоэлектронных средствах – объединенных земных станциях (ОЗС), интегрирущих функции КИС и ППИ, с возможностью их одновременного функционирования в интересах НКУ и НСпК;

– отсутствие необходимости координации решения задач средствами СНК с планами применения других космических систем и связанных с этим ограничений при реализации ТЦУ и программ работы бортовой аппаратуры КА, в полной мере согласованных с задачами целевого применения КА;

– возможность реализации современных технологий проектирования, отработки в процессе реализации проекта перспективных технических решений, унификации наземного и бортового оборудования, в том числе с учетом международных стандартов и рекомендаций;

– интеграция функций управления, контроля состояния бортовой аппаратуры и передачи целевой информации в рамках единого бортового радиотехнического комплекса.

Основными элементами СНК являются:

1.Единый командно-информационный центр (КИЦ), выполняющий функции Центра управления системой, ЦУП и ЦОИ.

2. Система ОЗС, с помощью которых осуществляются все операции информационного взаимодействия с КА – проводятся сеансы управления и приема целевой информации с КА.

3. Система связи и передачи данных СНК.

Основными объединяемыми функциями в СНК являются:

– управление орбитальной группировкой КА, прием с КА целевой информации и ее обработка;

– управление космической системой и поддержание единой базы данных;

– обмен информацией между средствами комплекса с использованием единой системы связи и передачи данных;

– баллистическое обеспечение управления и целевого применения КА.

Функции управления орбитальной группировкой КА, приема с КА целевой информации и ее обработки разделяются в КИЦ на уровне ЦУП и ЦОИ, а в системе ОЗС – на уровне функциональных каналов управления КА и приема целевой информации с КА в ОЗС. Эффективное решение задач управления КА и обработки целевой информации КА требует разработки для КИЦ надежного и высокоинтеллектуального программного обеспечения, обеспечивающего высокую степень автоматизации всех видов обеспечения управления КА (командно-программного, информационно-телеметрического и навигационно-баллистического обеспечения), процессов планирования управления КА и применения средств СНК, тематической обработки целевой информации. принимаемой с КА, и ее выдачи потребителям.

При обосновании принципов построения и взаимодействия элементов МНК между собой и с внешними организациями следует учитывать следую-

щие факторы:

1. Совмещение НКУ и НСпК на двух уровнях (КИЦ и СОЗС) позволяет в наибольшей степени сохранить степень режимности наземных объектов космической системы.

2. При решении целевых задач разрабатываемой космической системой особое значение имеет возможность совмещения сеансов управления КА и приема целевой информации с КА.

3. При реализации технологий управления и информационного обмена с КА в современных условиях необходимо ориентироваться прежде всего на унифицированные технические решения, стандарты и рекомендации.

4. При обосновании системных решений разрабатываемых космических систем существенную роль играет степень их преемственности с существующими космическим системами по решаемым целевым задачам и организации управления и целевого применения КА.

5. Современные тенденции развития космических систем и комплексов направлены на реализацию специализированных малопунктных (а в перспективе – и однопунктных) НКУ и их интеграцию с НСпК.

Технико-экономический эффект использования СНК достигается по ряду основных направлений, которыми являются:

– возможность оперативного решения задач управления и целевого применения КА;

– реализация на основе современных технических решений гибкой архитектуры комплекса;

–использование современных тех-нологий технической эксплуатации средств комплекса;

– сокращение численности обслуживающего персонала.

Литература

1. Макаренко Д.М., Потюпкин А.Ю. Современное состояние и перспективы развития космических систем. – М.: ВА РВСН, 2005. – 179 с.
2. Кравец В.Г. Автоматизированные системы управления космическими аппаратами.– М.: Машиностроение, 1995. – 194 с.
3. Соловьев В.А., Лысенко Л.Н., Любинский В.Е. Управление космическими полетами. – М.: МГТУ имени Н.Э. Баумана. – Ч.1.– 2009. – 476 с.; ч.2.– 2010. – 426 с.
4. Богинский Л.П., Половников В.И. Командно-измерительные системы иностранных государств. – СПб., ВКА имени А.Ф. Можайского, 2010. – 63 с.
5. Молотов Е.П. Наземные радиотехнические системы управления космическими аппаратами. — М.: Физмалит, 2004. – 256 с.
6. Лебедев А.А., Нестеренко О.П. Космические системы наблюдения. Синтез и моделирование. – М.: Машиностроение, 1991. – 224 с.
7. 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.
8. 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.
9. 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.

TO A QUESTION OF CREATION OF THE INTEGRATED TERRESTRIAL COMPLEX IN STRUCTURE OF AN AUTOMATED CONTROL SYSTEM FOR SPACECRAFTS

Rybochkin Yu., Ph.D, Military Space Academy,
ryun-73@mail.ru
Travkin V., Ph.D, Military Space Academy,
tr-75@yandeks.ru

Abstract
Application RES when performing their tasks carried out in cosmic systems in conjunction with other means of initiating and managing SC. Space system includes one or more space complexes and special complex. Space complex is a set of interrelated orbital and ground hardware designed for independent problem solving in and from space. The structure of space complex in the general case are: the orbital constellation of spacecraft, rocket and space complex, ground control and a set of tools and postplanting maintenance. Special package provides a set of interrelated orbital and ground-based facilities for receiving, processing, storing special (space) information from the spacecraft, and the issuance of its consumers. Ground facilities, placed on separate commandmeasuring complexes, the individual measuring points and testing center and prepare the ground grouping. Geographical location developed with a view to ensuring the requirements for efficiency, globality and reliability of spacecraft control during their passage in the areas of land LOS RES, as well as the required accuracy of determining the parameters of their orbits.
Keywords: electronic systems, major test Space Center, a separate command and test system, separate measuring station, automated control systems.

References

1.Makarenko D.M., Potyupkin A.Y. Current state and prospects of development of space systems. Moscow, 2005. 179 p.
2. Kravets V.G.Automated control of space apparatami. Moscow, 1995. 194 p.
3. Soloviev V.A., Lysenko L.N., Lubinsky V.E. Mission Control. Moscow, P1. 2009. 476 p., P.2. 2010. 426 p.
4. Boginsky L.P., Polovnikov V.I.Commandmeasuring systems of foreign countries. St. Petersburg., 2010. 63 p.
5. Molotov E.P. Terrestrial radio systems spacecraft control. Moscow, 2004. 256 p.
6. Lebedev A.A., Nesterenko O.P.Space surveillance system. Synthesis and simulation. Moscow, 1991. 224 p.
7. Burenin K.E., Legkov K.E. Effective methods of control over streams in protected infokommunikatsionny networks //H&ES: High technologies in space researches of Earth. - 2010.-№ 2. - pp. 29-34.
8. Burenin K.E., 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 //H&ES: High technologies in space researches of Earth. - 2011.-№ 1. - pp. 22-25.
9. Burenin K.E., Legkov K.E. 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. - 2011.-№ 2. - pp. 19-23.

2014

ЯНВАРЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

ФЕВРАЛЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

МАРТ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

АПРЕЛЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

МАЙ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

ИЮНЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

ИЮЛЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

АВГУСТ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

СЕНТЯБРЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

ОКТЯБРЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

НОЯБРЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

ДЕКАБРЬ

Пн	Вт	Ср	Чт	Пт	Сб	Вс
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

В ПОДГОТОВЛЕННОМ КОМПАНИЕЙ MCAFEE ОТЧЕТЕ РАССМАТРИВАЮТСЯ ТРУДНОСТИ, С КОТОРЫМИ СТАЛКИВАЮТСЯ ПРЕДПРИЯТИЯ РОЗНИЧНОЙ ТОРГОВЛИ ПРИ ЗАЩИТЕ СИСТЕМЫ ПЛАТЕЖЕЙ В МАГАЗИНЕ

Исследование, проведенное McAfee и консалтинговой фирмой IHL Group, показывает, что соблюдение требований PCI и уязвимости в защите остаются главными проблемами эксплаутации кассовых систем.

Москва, 1 октября, - компания McAfee сегодня объявила о том, что выступила спонсором совместного исследования с IHL Group, международной исследовательской и консалтинговой компанией, специализирующейся в области технологий для розничной торговли и гостиничного бизнеса. Целью исследования стала оценка безопасности розничной торговли и подходов, используемых для защиты систем обработки транзакций в розничной торговле. Согласно отчету, отсутствие адекватных средств, необходимых для управления системами магазинов, а также увеличение числа и разнообразия устройств будет и далее способствовать быстрому росту затрат на обеспечение безопасности в розничной торговле. В начале этого года компании McAfee и IHL Group провели анонимный опрос среди руководителей высшего звена в сфере розничной торговли и гостиничного бизнеса, чтобы рассмотреть применяемые ими стратегии соблюдения требований PCI и защиты систем розничной торговли.

Вот лишь некоторые ключевые выводы:

Учитывая, что информационные технологии развиваются постоянно, столь же постоянно должны развиваться и технологии защиты, причем в несколько раз быстрее, чем устройства, защиту которых они призваны обеспечивать. Возможность эффективно управлять предприятием — серьзный фактор, способствующий надежному управлению безопасностью и снижению затрат.

Уверенность в защите тесно связана с разнообразием устройств в магазине, при этом с увеличением числа устройств растет и сложность задач обеспечения безопасности в среде магазина.

В категории предприятий розничной торговли с выручкой свыше 1 млрд долларов наблюдается разделение на два приблизивно равных лагеря: одни предпочитают решения на основе белых списков, другие выбирают антивирусные решения.

«За последние десять лет ситуация в розничной торговле менялась неоднократно, но лишь одно остается неизменным: клиенты предпочитают комфорт и положительные впечатления от посещения магазина», — говорит Грег Бузек (Greg Buzek), президент компании IHL Group, — Потребители хотят иметь возможность совершать покупки, пользоваться товарами в полном объеме и возвращать товары в любом месте. Успешное внедрение мобильных устройств в инфраструктуру магазина создаст новые возможности для взаимодействия с клиентами, однако, будет сопровождаться и новыми рисками».

Результатом изменений в розничной торговле стали два значимых события: рост совместного использования информации различными типами устройств (с подключением по локальным и беспроводным сетям) и потребность в обмене информацией по беспроводным сетям в пределах магазина. Необходимо также отметить, что одновременно с ужесточением требований стандарта PCI наблюдается увеличение сложности действий киберпреступников, которые нацеливаются на системы розничной торговли.

Исследование показало, что предприятия розничной торговли вполне осознают необходимость соблюдения требований стандарта PCI. Вместе с тем, они испытывают трудности, вызванные ростом числа и разнообразия информационных систем для магазинов, затрудняющих надлежащее управление защитой и нормативно-правовым соответствием. В среднем, лишь 22 процента респондентов полагают, что производители защитных решений в состоянии обеспечить их безопасность.

«С целью повышения уровня комфорта и скорости обслуживания потребителей в сфере розничной торговли были проведены значительные преобразования, — отмечает Павел Эйгес, региональный директор McAfee в России и СНГ, — Утечка данных давно не новость для этой отрасли, однако, включение в систему дополнительного оборудования, такого как терминалы самообслуживания и цифровые мониторы для показа рекламы, существенно осложняет инфраструктуру в целом. Исследование подтвердило, что проблема безопасности реальна, и розничная торговля действительно нуждается в защищенных системах для взаимодействия с покупателями. В связи с этим у производителей торговых терминалов возникает возможность не только освободить предприятия розничной торговли от забот по обеспечению безопасности, но и предложить им более ценные продукты с уже встроенными системами защиты, тем самым, получив конкурентное преимущество на рынке».

Согласно данным отчета, уровень осведомленности о существовании решений для обеспечения безопасности на основе белых списков растет и уже составил 31 процент опрошенных. Причем многие из них уже сегодня используют белые списки для защиты своих систем торговых терминалов. Решения McAfee на основе белых списков приложений позволяют предотвратить проникновение вредоносных программ в системы торговых терминалов и другие устройства, поскольку позволяют запускать только утвержденные приложения. Любое несанкционированное приложение, попавшее в систему, блокируется.
http://www.mcafee.com/us/resources/reports/rp-preparing-paradigm-shift.pdf

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

nevalab.ru

БОЛЕЕ 10 ЛЕТ НА РЫНКЕ!

КРУПНЫЕ ПРОЕКТЫ

НЕФТЯНАЯ КОМПАНИЯ РОСНЕФТЬ · TRANSNEFT ТРАНСНЕФТЬ · ГАЗПРОМ · РОСАТОМ · ИНТЕР РАОЕЭС · НОВАТЭК

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

НА МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ «ИНФОФОРУМ ЕВРАЗИЯ/СИТИ» РКСС ОБСУДИЛА ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ РОССИЙСКОЙ ПРОМЫШЛЕННОСТИ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ВАЖНЫХ ОБЪЕКТОВ

«Российская корпорация средств связи» (РКСС) выступила золотым партнером Евразийского форума информационной безопасности и информационного взаимодействия «Инфофорум Евразия/Сити». Мероприятие прошло в здании Правительства Москвы при поддержке комитета Государственной думы РФ по безопасности и противодействию коррупции, аппарата Совета безопасности РФ и других министерств и ведомств России. В ходе форума РКСС приняла активное участие в обсуждении проблемы обеспечения национальной безопасности.

Заместитель генерального директора госкорпорации «Ростехнологии» (Ростех) Николай Волобуев выступил на пленарном заседании форума с докладом об использовании возможностей российской промышленности в целях повышения безопасности объектов критической инфраструктуры. В частности, он рассказал о комплексной автоматизированной системе управления безопасностью (КАСУБ), разработанной дочерним предприятием Ростеха «Российской корпорацией средств связи».

«Основная задача этой системы - информационная поддержка всего цикла управления безопасностью от сбора и мониторинга информации до принятия решений и накопления опыта, - отметил в своем выступлении Н.Волобуев. - Система носит многоуровневый характер, начиная от объекта, территории и заканчивая информационной поддержкой федеральных структур. В основе КАСУБ лежат отечественные разработки и доверенное оборудование РКСС».

Подчеркивая актуальность обсуждаемой темы, Н.Волобуев отметил: «Руководство страны целенаправленно ведет работу по повышению устойчивости функционирования критически важных объектов инфраструктуры России в связи с тем, что наблюдается рост угроз в отношении этих объектов. Это происходит во всем мире: как в Российской Федерации, так и за рубежом. Нам всем хорошо известен ряд примеров негативного воздействия на эти объекты, в том числе через компьютерные сети. Очевидно, что подход к вопросам защиты объектов критической инфраструктуры должен предусматривать превентивное реагирование и максимальное снижение последствий негативного воздействия. Отдельным вопросом, требующим нашего внимания, является проблема совершенствования нормативной базы и разработки пакета соответствующих документов, направленных на повышение безопасности объектов критически важной инфраструктуры».

В своем выступлении Н.Волобуев рассказал о существующей нормативной базе в сфере обеспечения безопасности критически важных объектов (КВО) и сравнил ее с мировым опытом: «К настоящему моменту разработано значительное количество нормативных документов. К сожалению, появление многих из них связано не с планомерной системной работой, а с уже случившимися негативными событиями, требующими незамедлительной реакции. В этих условиях сложно говорить о взаимоувязке и гармонизации этих документов. Поэтому очень важно подкрепление ключевых законов в сфере безопасности промышленных объектов соответствующими нормативными документами».

Обсуждая важность использования сертифицированного оборудования, Н.Волобуев подчеркнул: «Очевидно, что нельзя строить системы безопасности, даже если в них нет обработки государственной тайны, на недоверенном оборудовании и программном обеспечении. Это ключевым образом влияет на непрерывность функционирования критически важной инфраструктуры».

Н.Волобуев отметил необходимость обеспечения взаимодействия систем

безопасности критически важных объектов и программ класса «Безопасный-Умный город». Это позволяет создать единое информационное пространство для координации и согласованного межведомственного и межуровневого взаимодействия. Яркий пример такого согласования – проект «Безопасный город» в Красноярске, реализованный РКСС по заказу краевой администрации. «Безопасный город - современная интеллектуальная система безопасности, которая позволяет максимально быстро зафиксировать правонарушение и отправить на место наряд полиции, - подчеркнул Н. Волобуев. - Это первая масштабная информационная система, реализованная полностью на базе отечественного программно-аппаратного комплекса. Она позволяет мгновенно передать сигнал зарегистрированного правонарушения на пульт дежурного полиции. Операторы службы 02 и операторы управления патрульными нарядами города ведут единый мониторинг ситуации, находясь в одном месте, что позволяет быстро и своевременно реагировать на поступивший сигнал».

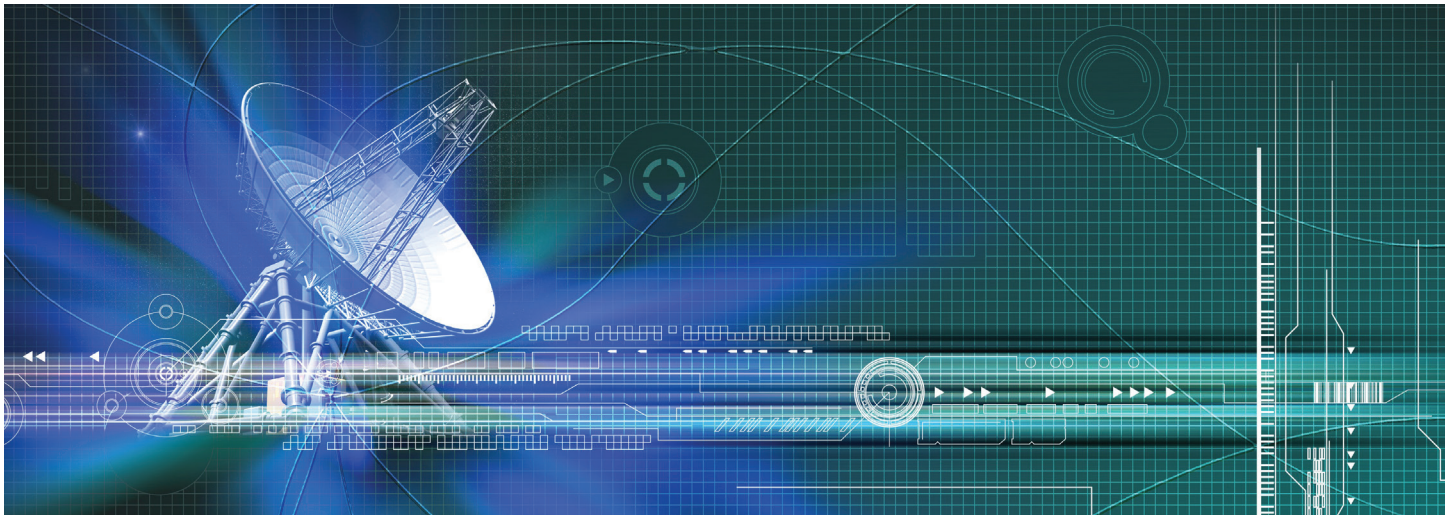
Подводя итоги своего выступления, Н. Волобуев сформулировал ряд предложений для более эффективного решения проблемы обеспечения безопасности КВО:

- Разработка гармонизированных нормативных документов
- Создание государственных целевых программ
- Государственная техническая политика в части доверенного оборудования
- Использование опыта ГК «Ростехнологии» и РКСС и рассмотрение возможности его применения в различных областях критически важной инфраструктуры.

Более подробно о проекте «Безопасный город» и комплексной системе безопасности рассказали сотрудники РКСС в ходе секций и заседаний «Инфофорума». По итогам работы РКСС получила почетный диплом за активное участие в конференции. Выставочный стенд РКСС посетили представители различных министерств и ведомств России, а также представители региональных органов власти и бизнеса.

ЗАО «Российская корпорация средств связи» (РКСС) - первая в России компания, которая специализируется на производстве и разработке доверенного телекоммуникационного оборудования и создании комплексных систем безопасности. Компания обеспечивает адаптацию технологий мировых лидеров ИТ-индустрии с учетом требования российского рынка. РКСС была создана в декабре 2007 года и входит в состав госкорпорации Ростех. Компания производит доверенное оборудование, прошедшее сертификацию в соответствии с требованиями российского законодательства на отсутствие недекларированных возможностей. РКСС осуществляет проверку комплектующих и сборку на отечественных предприятиях, принадлежащих Ростеху.

Контакты для прессы:
Ольга Калинина
«Российская корпорация средств связи»
+ 7(985)255- 34-11, okalinina@pkcc.ru



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.