ТЕХНИКА СРЕДСТВ СВЯЗИ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

№1 (141). 2018

СОДЕРЖАНИЕ

Ю.Л. Николашин
кандидат технических наук
В.И. Мирошников
доктор технических наук, профессор
И.А. Кулешов
кандидат военных наук, доцент
ОАО «Информационные телекоммуникационные технологии» г. Санкт-Петербург

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ СИСТЕМЫ СВЯЗИ НА СОВРЕМЕННОМ ЭТАПЕ

Аннотация. Рассматриваются проблемы реализации в перспективе единого инфокоммуникационного пространства (ЕИКП) Вооруженных Сил Российской Федерации (ВС РФ). Приводится перечень перспективных информационных и телекоммуникационных технологий, практическое применение которых должно обеспечить реализацию ЕИКП с требуемой функциональностью. Отражены основные результаты деятельности ОАО «Интелтех» в области разработки систем связи и управления двойного применения нового поколения.

Ключевые слова: оборонная инфраструктура, инфокоммуникационное пространство, системы управления, системы связи.

Проблемы реализации оборонной инфраструктуры и ЕИКП

Отличительной чертой современного этапа развития общества является возрастание вклада информационных и коммуникационных технологий в ускорение процесса развития науки, техники, экономики, социальной сферы и оборонной инфраструктуры. Перспективы и планы реализации оборонной инфраструктуры РФ, в свою очередь, во многом определяют направления развития военной техники, вооружения и технологий на современном этапе. В соответствии с определениями, приведенными в [1], *оборонная инфраструктура* объединяет объекты военной инфраструктуры и инфраструктуры двойного назначения.

Военная инфраструктура - это совокупность военных объектов и отдельных сооружений, предназначенных для обеспечения выполнения войсками оперативно-стратегических, оперативных и боевых задач вооруженной борьбы, а также для размещения и проведения повседневной подготовки войск и обслуживания военного производства в мирное время.

Инфраструктура двойного назначения - это система объектов федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, организаций и граждан, используемая (планируемая к использованию) как в целях социально-экономического развития страны, так и в целях обороны.

К приоритетным направлениям развития оборонной инфраструктуры [2] могут быть отнесены:

– разработка высокоэффективных систем разведки и управления, функционирующих в реальном масштабе времени;

– создание высокозащищенной системы управления войсками и оружием, способных противостоять информационному воздействию противника;

– обеспечение бесперебойного функционирования существующих объектов оборонной

инфраструктуры, при различного рода деструктивного воздействия;

– создание спутниковой группировки для решения задач разведки, навигации, связи, предупреждения о ракетном нападении и др.;

– создание быстродействующей распределенной телекоммуникационной инфраструктуры.

Системы управления являются неотъемлемой и важнейшей составной частью инфраструктуры органов государственной власти, ведомств, корпораций, предприятий. В настоящее время возможности построения систем управления в значительной степени ассоциируются со способностью их создателей вести разработку с использованием системного подхода к проектированию, новейших информационных и телекоммуникационных технологий, унифицированных аппаратно-программных платформ и т.д.

В последние годы в мировой практике в качестве наиболее общего принципа развития систем управления различного уровня (от систем управления общегосударственного масштаба для систем управления корпорациями и отдельными предприятиями) является ориентация на создание и использование ЕИКП [3].

Под *единым инфокоммуникационным пространством* понимается совокупность интегрированных информационных ресурсов всех уровней, с едиными правилами создания и потребления, едиными стандартами представления и возможностью непосредственного доступа к ним пользователей в соответствии с имеющимися полномочиями, а также телекоммуникационных сетей, обеспечивающих поддержку информационных взаимодействий за счет предоставления комплекса услуг по организации доступа к сети, коммутации, маршрутизации, доступа к службам.

Этот принцип закладывается в основу:

– программ по реализации оборонной инфраструктуры России, модернизации систем управления ВС РФ, отдельных видов и родов войск;

– реализации программ по созданию «Электронного правительства России»;

– информационных и управляющих систем органов государственного управления различных уровней;

– программ модернизации и развития инфраструктур крупнейших российских ведомств и корпораций (топливно-энергетического комплекса, МПС, МЧС, финансовых ведомств).

Программы реализации ЕИКП ВС РФ

Основные взгляды руководства Министерства обороны на особенности строительства Вооружённых Сил в обозримой перспективе изложены в [4].

Программы создания ЕИКП в военной области [5] ориентированы на реализацию концепции оборонной инфраструктуры, предусматривающей техническое переоснащение ВС и внедрение новых принципов управления. Предполагается, что создание ЕИКП ВС РФ будет достигаться на основе объединения и развития существующих информационно-аналитических ресурсов, предназначенных для обеспечения эффективной управленческой деятельности органов военного управления.

Информационное пространство ЕИКП образуют информационно-аналитические, управляющие системы (поддержки принятия решений, планирования операций и боевых действий, управления военными действиями, электронного документооборота и т.д.), реализуемые на различных уровнях системы управления ВС РФ, использующие общие информационные ресурсы и взаимодействующие с использованием ресурсов и услуг коммуникационного пространства, входящего в состав ЕИКП.

Телекоммуникационную основу ЕИКП ВС РФ должна составлять совокупность телекоммуникационных сетей (ТКС) ВС, других войск и воинских формирований, поэтапно реализуемая на базе существующих сетей и комплексов связи и ряда ведомственных сетей связи. ТКС включает стационарный компонент (с мобильной составляющей), а также резервный (полевой) компонент в особый период и в военное время. В [6] отмечается, что исходя из характера современных операций, на эффективность процесса управления во многом будет влиять способность должностных лиц, принимающих решения, и органов военного управления в целом перерабатывать значительные объемы информации, необходимые для управления силами (войсками) в сложной, быстро меняющейся обстановке. Основным направлением дальней-

шего совершенствования управления силами (войсками) должна стать автоматизация наиболее трудоемких информационных процессов.

В ходе автоматизации управления должны быть достигнуты две цели: основная цель - обеспечение максимальной реализации потенциальных возможностей сил (войск) в интересах достижения поставленных задач. Дополнительная цель - создание условий максимальной реализации интеллекта командующих (командиров) всех уровней управления.

В качестве основного принципа развития системы управления ВС РФ рассматривается *концентрация усилий на создание межвидовой многофункциональной (интегрированной) системы управления,* построенной на основе разработки и применения максимально унифицированных и совместимых программно-технических средств, минимальном составе пунктов и средств управления, необходимых для эффективного управления войсками (силами) и всеми видами обеспечения боевых действий при безусловном выполнении оперативно-стратегических требований к системе управления [7].

В качестве примера практической реализации рассмотренных выше концептуальных положений можно привести планы ВМФ, в котором уже начаты работы по созданию и развитию интегрированной системы управления [8]. При этом единое интегрированное информационное пространство ОВУ ВМФ отражает реализацию целевого предназначения ВМФ как боевой системы и позволяет, во-первых, установить информационные связи между всеми компонентами боевой системы; во-вторых, обеспечить единство рассмотрения всех информационных ресурсов и процессов, происходящих в боевой системе; в-третьих, более точно оценивать достаточность, противоречивость и избыточность информационных ресурсов для решения поставленных задач [9].

Перспективные технологии и направления их использования при создании средств связи и систем управления нового поколения

Компоненты ЕИКП могут быть реализованы на базе различных информационных, телекоммуникационных и компьютерных технологий (современных и перспективных), в том числе - технологий распределенных вычислений, искусственных интеллектуальных систем, нанотехнологий и т.д. (т.е. тех технологий, которые отнесены к критическим для РФ на текущий период).

Из всего множества перспективных информационных технологий могут быть выделены базовые технологии, в значительной степени определяющие облик систем управления нового поколения.

Перечень перспективных технологий может быть выявлен на основании анализа правительственных программных документов, результатов аналитических исследований ведущих экспертов в мировом и национальном масштабе, программ развития различных (в первую очередь силовых) ведомств зарубежных стран и России. Анализ перспективных телекоммуникационных технологий, в том числе - применительно к задачам реализации перспективных систем управления силами ВМФ, содержится в [10].

Обобщение и классификация аналитических материалов позволяет сформировать перечень перспективных технологий, являющихся актуальными для проводимых разработок на ближайшую (2011-2015 г.г.) и более отдаленную (2016-2020 г.г.) перспективу.

Информационные технологии:

– технологии распределенных вычислений;

– хранилища данных;

– системы управления знаниями, в том числе - оперативной аналитической обработки данных (OLAP), интеллектуального анализа данных (Data Mining), ведения отчетности (OLTP) и т.д.;

– экспертные системы;

– мультиагентные системы;

– расчетно-логические системы;

– системы поддержки принятия решений;

– архитектуры, ориентированные на сервисы;

– приложения, использующие данные о местоположении;

– семантический Web (в том числе - онтологические методы представления знаний);

– технологии автоматизации проектирования и программирования и т.д.

Коммуникационные технологии:

– широкополосная беспроводная связь (в том числе Wi-Fi, Mesh-сети, Wi-Max, HSxPA, EV-DO);

Таблица 1

Перечень представительных технологий и эволюция их развития

Технологии	XX век	2000-2015 г.г.	2016 г. и далее
Телекоммуникационные	ISDN. Internet	Intranet. Корпоративные сети. NGN, IMS. 4G (мобильные). Web **2.0**	Широкополосные конвергентные сети. Самоорганизующиеся сети
Информационные	Системы «клиент-сервер». Распределенные вычисления. Распределенные БД	Сервисно-ориентированные архитектуры. Системы поддержки принятия решений. Системы управления знаниями. Многоагентные локальные системы	Системы управления знаниями. Многоагентные глобальные системы. Интеллектуальные агенты реального времени
Поддержки эксплуатационных процессов	TMN. TMF	NGOSS. Системы поддержки принятия решений	Интеллектуальные системы поддержки эксплуатационных процессов
Формализации знаний о проблемной области	Спецификации. Языки визуального моделирования	Языки визуального модели-рования. Онтологии отдельных проблемных областей	Универсальные онтологии для Глобального инфокоммуникационного пространства

– подвижная спутниковая связь;

– оптическое волновое мультиплексирование;

– ячеистые фемсотовые, межтелесные, сенсорные сети;

– самоорганизующиеся сети;

– активная и пассивная ретрансляция;

– пакетная радиосвязь;

– помехоустойчивая передача информации;

– видеоконференц-связь и т.д.

В обобщенном виде эволюция технологий (для рассматриваемого нами класса систем) может иллюстрироваться данными, приведенными в таблице 1.

Основные направления деятельности ОАО «Интелтех» по созданию технических средств для МО РФ и двойного применения

ОАО «Информационные телекоммуникационные технологии» является одним из ведущих российских предприятий, специализирующихся на разработке и поставке телекоммуникационного оборудования и информационного обеспечения для систем связи и управления народно-хозяйственного и ведомственного назначения [11, 12].

ОАО «Интелтех» ориентируется на требования к современным системам управления и к средствам связи, которые определяют:

- резкое увеличение объема и скорости передаваемой и обрабатываемой информации;

- необходимость повышения устойчивости функционирования средств и комплексов связи в условиях различного рода деструктивных информационных воздействий;

- уменьшение массогабаритных показателей и величин потребляемой энергии, увеличение температурного диапазона разрабатываемых средств при увеличении надежности их функционирования;

- необходимость защиты каналов управления средствами и системами связи.

Многолетний опыт проведения фундаментальных научно-исследовательских работ и создание целого ряда телекоммуникационного оборудования, комплексов связи, систем коммутации и передачи данных позволили предприятию решить многие из этих проблем в разработанных современных комплексах связи. Соответствие разрабатываемой аппаратуры системным требованиям - обязательные составляющие всех проводимых разработок.

Оборудование интегрированных сетей ведомственной связи. ОАО «Интелтех» является одним из основных разработчиков средств автоматической коммутации для сетей телефонной связи Министерства обороны, Министерства внутренних дел и Федеральной службы охраны РФ. Созданные предприятием электронные автоматические телефонные станции установлены и

работают в штабах, управлениях и на командных пунктах систем связи этих ведомств [11]. Современный вариант интегрального оборудования предназначен для организации сетей связи, предоставляющих должностным лицам стационарных и мобильных пунктов управления услуги по оперативному высококачественному обмену документальной, аудио и видео информацией с управляемыми объектами по проводным и радио каналам. Комплексы средств связи для мобильных объектов могут размещаться в полевых аппаратных и на надводных кораблях.

В настоящее время при производстве коммутационного оборудования интегрированных сетей ведомственной связи используется аппаратная платформа Intel, сертифицированная операционная система жесткого реального времени КПДА.0002-01 (QNX) и отдельные комплектующие изделия зарубежной электронной техники.

Реализованы средства, обеспечивающие режим пакетной передачи речевой информации (IP-телефонии), производится разработка высоконадежного варианта коммутационного оборудования, аппаратные средства которого ориентированы на размещение в конструктиве Compact PCI.

Ближайшими планами предусматривается разработка дополнительных аппаратно-программных средств, обеспечивающих взаимодействие со средствами радиосвязи тактического звена управления 6-го поколения и подвижными средствами спутниковой связи, поддержка идеологии межвидовой интеграции и частичной самоорганизации элементов тактического звена в иерархии управления ВС РФ.

С учетом новых реалий и перспективных требований потребителей разрабатываются методы сетевого управления и технического обслуживания. В перспективе предусматривается внедрение в эти компоненты интеллектуальных элементов в виде систем поддержки принятия решений, систем математического моделирования вариантов развертывания подвижных средств, онтологии используемых понятий, технологий поддержки идеологии самоорганизующихся и самосохраняющихся сетей.

Средства и системы обмена данными для ВМФ РФ. ОАО «Интелтех» является одним из ведущих российских разработчиков и поставщиков сетей, систем, комплексов технических и программных средств для телекоммуникаций, включая комплексы обмена данными для подводных лодок и надводных кораблей [12]. Сегодня на их базе разработано новое поколение комплексов средств автоматизации связи двойного применения.

Представителем оборудования нового поколения, разработанного ОАО «Интелтех» для данной области, является аппаратура «Трасса-Э». Аппаратура автоматизированного приема и передачи быстродействующей (БД) и сверхбыстродействующей (СБД) связи «Трасса-Э» относится к оборудованию военно-морских систем радиосвязи и обмена управляющей информацией береговых командных пунктов (БКП) с подводными лодками (ПЛ) и надводными кораблями (НК), их соединениями, а также для связи между собой отдельных ПЛ и НК. В аппаратуре «Трасса-Э» в качестве программной платформы, обеспечивающей выполнение заданных функций в масштабе реального времени, применяется защищенная операционная система жесткого реального времени КПДА.0002-01 (QNX v. 4.2). При построении технических средств в аппаратуре используются аппаратные платформы Intel и MIPS. Создание прикладного алгоритмического и функционального программного обеспечения составляет 82% сложности и стоимости разработки и производства аппаратуры «Трасса-Э».

В перспективе предусматривается повышение уровня интеллекта системы с целью автоматизации действий операторов, основанное на применении комплекса математических моделей для расчета параметров сеансов связи, элементов систем поддержки принятия решений для оптимизации расписания и параметров сеансов связи с учетом многочисленных факторов внешней среды (в том числе - уровня радиопротиводействия) и взаимного пространственного расположения корреспондентов (на берегу, в море, в подводном положении).

Многофункциональные комплексы связи. В последние годы в соответствии с мировыми тенденциями развития телекоммуникационных технологий предприятие ориентируется на создание аппаратуры нового поколения, обеспечивающей решение задач сетевой и системной интеграции. Комплексное или фрагментарное использование мультисервисного оборудования ОАО «Интелтех» обеспечивает заказчикам возможность выбора и

реализации гибкой стратегии развития и модернизации своих сетей на основе принципов конвергенции и поэтапного внедрения новых сетевых и информационных услуг. «Интелтех» в этой области разрабатывает средства «двойного применения» - аппаратно-программные комплексы, ориентированные на текущие и перспективные потребности силовых ведомств, органов государственного управления, коммерческих структур.

Оборудование разрабатывается в соответствии с идеологией сетей нового поколения (NGN, IMS); при его реализации используются следующие технологии: формирования IP и SIP сетей формирования транспортной сети - SDH, IP/MPLS; формирования виртуальных частных сетей - IP/MPLS; базовые защищенные компьютерные технологии.

При разработке оборудования использована технология компонентного проектирования телекоммуникационных систем нового поколения. Для потребностей перспективных разработок ОАО «Интелтех» наиболее актуальной в данной области является технология MicroTCA (Micro Telecommunications Computing Architecture), которая в сфере телекоммуникаций предназначена для реализации корпоративных приложений. Стандарт MicroTCA определяет модульную архитектуру на основе объединительной панели, способную поддерживать резервированную встроенную систему на базе мезонинов AdvancedMC. Стандарт MicroTCA поддерживает «горячую» замену модулей, автономное управление системой и обеспечивает обмен данными между платами по быстрым коммутируемым соединениям.

В стиле компонентного проектирования производится разработка двух элементов для телекоммуникационных сетей нового поколения - интегрального коммутатора и комплекса организации видеоконференц-связи.

Интегральный коммутатор обладает следующими характеристиками:

– архитектура, поддерживающая основные положения концепций сетей нового поколения NGN и IMS;

– функции IP-УАТС;

– поддержка протокола SIP;

– реализация широкого набора дополнительных видов обслуживания;

– функции контроля доступа к услугам связи.

Аппаратно-программный комплекс организации ВКС предназначен для реализации серверных функций средств видеоконференцсвязи и обеспечения функций управления и защиты информации. Комплекс состоит из сервера сигнализации SIP и серверов многоточечных конференций, предназначенных для централизованного управления, и обладает следующими характеристиками:

– транспортный протокол - TCP/IP;

– протокол сигнализации - SIP;

– используемые видеокодеки: H.261, H.263, H.264, MPEG-4;

– используемые аудиокодеки: G.711, G.723, G.728.

Непрерывно совершенствуя свою продукцию, ОАО «Интелтех» готово поставлять оборудование для систем управления и сетей связи (стационарных, мобильных) как специального назначения, так и двойного применения.

СПИСОК ЛИТЕРАТУРЫ

1. Захаров В.П., Соколов А.В. Роль оперативного оборудования территории страны в повышении эффективности применений ракетного вооружения - Военная мысль, 2008, №2.

2. Долматович И.А. Проблемы обеспечения оборонной безопасности России. Журнал «Право и безопасность» Номер - 1 (34), Март 2010.

3. Волошенко М.В. Информационная безопасность, независимость инфокоммуникационного пространства России. www.sgk-urep.ru/documents/inf_security.doc.

4. Военная реформа: время сверять часы. Газета «Красная звезда» от 15 декабря 2010 года.

5. Государственная программа вооружения. Газета «Красная звезда» от 11 января 2011 года.

6. Изучая войны будущего. Газета «Красная звезда» от 15 января 2011 года.

7. Время «автоматизированных» войн. Единая система АСУ ВС – жизненная необходимость. Независимое военное обозрение. 2011 г. №1.

8. Создание и развитие комплексов связи атомных подводных лодок ВМФ МО РФ. Журнал «Электросвязь» № 11. 2010 г.

9. Директоров Н.Ф., Мирошников В.И. и др. Информационные технологии в системе управления силами ВМФ (теория и практика, состояние и перспективы развития). - СПб.: «Элмор», 2005.

10. За счет прорывных технологий. Газета «Красная звезда» от 22 декабря 2010 года.

11. Николашин Ю.Л. О вкладе ОАО «Интелтех» в развитие систем и средств связи Вооруженных сил России. - Связь в Вооруженных силах Российской Федерации - 2006. Тематический сборник. - Компания Информационный мост», 2006.

12. Николашин Ю.Л., Мирошников В.И. О вкладе ОАО «Интелтех» в развитие систем и средств связи ВМФ - Связь и АСУ Военно-Морского флота. Юбилейное издание, посвященное 95-летию Службы связи ВМФ. - Компания «Информационный мост», 2005.

И.В. Абашева
Военно-космическая академия имени А.Ф.Можайского

О ВНЕДРЕНИИ В УЧЕБНЫЙ ПРОЦЕСС ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ

В статье описан подход о внедрении параллельных вычислений в учебный процесс академии. Актуальность данной задачи обусловлена следующими основными причинами: массовое производство персональных компьютеров на базе многоядерных процессоров и на их основе широкое распространение кластерных вычислительных систем [1]. В то же время образовательные программы не обеспечивают в полной мере подготовку выпускников в области современных параллельных вычислительных технологий.

Введение

Поиски путей увеличения производительности ЭВМ привели к появлению в 50-е годы идеи параллельной обработки данных в многопроцессорных вычислительных системах (МВС). Первые конкретные шаги в исследовании параллельных вычислений были сделаны в первой половине 60-х годов. Это был период отбора и становления главных проблем и направлений развития параллельного программирования. К середине 60-х годов в рамках общей теории программирования начинает складываться теория параллельного программирования [5,7].

В настоящее время теория параллельного программирования имеет богатую библиографию, охватывающую широкий круг проблем. Параллельным вычислениям уделяется большое внимание. Это связано главным образом с двумя факторами. Первый фактор обусловлен научно-техническим прогрессом, в результате которого появились новые области знаний, требующие применения методов математического моделирования. Сами модели также существенно усложнились. В итоге происходит неуклонное возрастание потребности в ресурсоемких расчетах, которые в ряде случаев можно выполнить только на базе высокопроизводительной техники с помощью методов параллельных или распределенных вычислений.

Другой существенный фактор, в результате которого интерес к параллельным вычислениям существенно вырос, состоит в повсеместном распространении многоядерных компьютеров и кластерных систем.

В настоящее время актуальной является задача подготовки специалистов, владеющих современными параллельными вычислительными и суперкомпьютерными технологиями и способных эффективно применять их при проведении фундаментальных и прикладных исследований.

В данной статье описан подход к внедрению параллельного программирования в учебный процесс подготовки выпускников, который опробован в ходе работ и исследований военно-научного общества 63 кафедры 6 факультета академии.

Внедрение параллельных вычислений в учебный процесс подразумевает в первую очередь обучение знаниям и навыкам параллельного программирования сложных научных задач и обеспечение соответствующей материальной базой. Как отмечал один из основоположников параллельного программирования академик А.П.Ершов «Чтобы научиться программировать, надо программировать» [5]. Минимальная материальная база параллельного программирования включает в себя следующие компоненты:

1. Аппаратные средства параллельного программирования.

2. Программные средства параллельного программирования.

Аппаратные средства параллельного программирования

1. Многоядерные компьютеры:

Например, четырехядерные компьютеры с процессором Intel Core 2 Quad Q8300 2,5 GGz [4].

2. Отечественные кластерные системы ОАО «НИЦЭВТ»:

СВК ЕС1710, ЕС1720, ЕС1721 – мультипроцессорные системы для использования в задачах с большим объемов вычислений, а также как база для систем коллективного пользования и систем управления.

3. Локальные вычислительные системы на базе однородных типовых компьютеров.

Программные средства параллельного программирования

Программное обеспечение исследования процессов выполнения параллельно-последовательных программ (ПП - программ) в общем случае включает операционные системы (ОС), системы производства программ (СПП) и дополнительные программные системы для параллельного выполнения целевых программ пользователей.

Программное обеспечение включает:

Операционные системы (ОС), системы производства программ (СПП) и дополнительные программные системы для параллельного выполнения целевых программ.

Операционные системы:

Широко используются ОС Windows XP, WindowsVista, Windows 7 и Linux, но чаще других используются ОС Windows XP и Windows 7. Windows XP сочетает в себе преимущества Windows 2000 Professional с лучшими качествами Windows 98 и Windows ME.

Системы производства программ:

В широко используются системы производства программ на базе языков высокого уровня С, С++, Фортра́н , включенных в систему Visual Studio 2005 (2008) для создания параллельных приложений для ОС Windows 7 и XP.

Дополнительные программные средства

К ним относятся следующие средства:

- Vision Studio 2005 (программа создания приложений – проектов ОС);
- Vision Studio 2008 (программа создания приложений – проектов ОС);
- MPICH2 (MPI – 2.0) (интерфейс обмена данными в параллельном программировании);
- Open MP 3.0 (интерфейс прикладной параллельной программы);
- HPF (High Performance Fortran) – расширение языка Фортран-90;
- HPF-2 – расширение языка Фортран – 95 [2,3].

Меры по внедрению параллельного программирования в учебный процесс

На первом этапе проделана следующая работа:

1. В новый план по ФГОС – 3 на 63 кафедре включена дисциплина «Супер-ЭВМ». По этой дисциплине предусмотрены разделы « Основы параллельного программирования» и « Организация кластерных вычислений».

2. Разработано и подготовлено к изданию в 2013 г. « Руководство к лабораторным работам по дисциплине «Супер-ЭВМ» для отработки практических навыков по параллельному программированию и проведению исследований процессов выполнения параллельных программ.

3. На кафедре разработано и организовано автоматизированное рабочее место «АРМ-63» для проведения лабораторных работ по дисциплине «Супер-ЭВМ».

4. Выпускница 2013 г. Агафонова И.В. защитила выпускную квалификационную работу на тему: «Организация и исследование процессов параллельно – последовательного выполнения программ на многоядерных компьютерах». Она начинала свои исследования параллельных вычислений в военно-научном обществе кафедры на аппаратуре «АРМ-63».

На втором этапе ставится задача разработки и внедрения лабораторного практикума параллельных вычислений для проведения разного рода исследований, например:

- Исследование зависимости времени выполнения ПП - программы на языке С++ или Fortran в системе MPICH2 от числа процессоров в МВС.
- Исследование зависимости времени выполнения ПП - программы на языке С++ или

Fortran в системе Open MP от числа процессоров в МВС и др.

Предусмотрено также составление и отладка ПП – программ для типовых задач, например:

1. Перемножение матриц.

2. Решение системы линейных уравнений методом Гаусса.

3. Определение значения определенного интеграла методами прямоугольника, трапеций или Симпсона.

4. Решение дифференциальных уравнений 1-го порядка методами Эйлера и Рунге – Кутта и др.

Можно также подготовить варианты тем дипломов и диссертационных работ, например:

1. Исследование процессов выполнения ПП - программ военного назна-чения на многоядерных компьютерах [6].

2. Исследование процессов выполнения ПП – программ военного назна-чения на кластерных вычислительных системах [8].

3. Разработка методов распараллеливания последовательных алгоритмов для программирования целевых задач военного назначения.

4. Исследование организации вычислительного процесса реконфигурируемых мультиконвейерных вычислительных систем с перенастраиваемой структурой.

Заключение

Новые версии учебных программ предполагают преподавание основ параллельных вычислений, начиная с младших курсов. Это позволит на ранних этапах обучения вызвать у курсантов интерес к параллельным вычислениям и показать перспективу их использования.

Модернизация программ выполнена в рамках действующего ГОС. Дополнительные аудиторные часы для изучения параллельных вычислительных технологий получены за счет использования современных образовательных технологий: проведение лекций с использованием презентаций, использование лабораторных интернет - практикумов и компьютерное тестирование знаний курсантов.

В апреле 2013 г. вопрос внедрения параллельного программирования и кластерных вычислений в учебный процесс академии рассматривался на предметно-методической комиссии по информатике, где среди других были рассмотрены и учтены в решении следующие вопросы:

Придание параллельному программированию статуса учебной дисциплины (отдельный курс или раздел в дисциплину программирования, курсовые работы, дипломное проектирование).

Применение параллельного программирования в диссертационных работах.

Исследование и использование параллельного программирования в научно-исследовательской работе.

Развитие научных направлений работ в области параллельного про-грамммирования (операционные системы, языки параллельного про-граммирования, трансляторы, организация параллельного вычислительного процесса).

СПИСОК ЛИТЕРАТУРЫ

1. Воеводин В.В., ВоеводинВл.В. Параллельные вычисления. – СПб. Изд. «БХВ-Петербург», 2002.

2. Гергель В.П. Теория и практика параллельных вычислений. – М.: Интернет-Университет, БИНОМ. Лаборатория знаний, 2007.

3. Горелик А.М. Средства поддержки параллельности в языках программирования. Открытые системы 02/1995.

4. Гэри М., Джонсон Д. Высокопроизводительные машины и труднорешаемые задачи. – М. Мир, 1982.

5. Ершов А.П. Теория программирования и вычислительные системы, «Знание», М., 1972.

6. Захаров А.И. Исследование принципов параллельно – последовательного выполнения программ в многопроцессорных вычислительных системах. Кандидатская диссертация. СПб., ВКА им. А.Ф. Можайского, 1975.

7. Котов В.Е. Теория параллельного программирования. Прикладные аспекты. Кибернетика, 1974,№1.

8. Сбитнев Ю. Кластеры. Практическое руководство по параллельным вычислениям. Корпорация ЯВА, Екатеринбург, 2010.

Автамонов П.Н.
Охтилев М.Ю.
Соколов Б.В.
Юсупов Р.М.

НАУЧНО-ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ РАЗРАБОТКИ И ВНЕДРЕНИЯ УНИФИЦИРОВАННОЙ КОМПЛЕКСНОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ИНФОРМАЦИОННОМ И ИНФОРМАЦИОННО-ТЕЛЕМЕТРИЧЕСКОМ ОБЕСПЕЧЕНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ КОСМИЧЕСКИМИ КОМПЛЕКСАМИ

В статье представляются результаты междисциплинарных исследований, направленные на комплексное рассмотрение системо-технических факторов, связанных с автоматизированным управлением объектами военного назначения, в частности, космическими комплексами. При этом рассматриваются интегрированные интеллектуальные системы поддержки принятия решений как основной элемент в составе систем информационного и информационно-телеметрического обеспечения автоматизированных систем управления космическими комплексами. Предлагаемый в статье интегративный подход базируется на основе реализации концепций системного моделирования и интеграции знаний.

Ключевые слова: унифицированная комплексная система поддержки принятия решений, национальная интеллектуальная аналитическая платформа, информационное и информационно-телеметрическое обеспечение, автоматизированная система управления космическими комплексами.

В современных условиях успешное развитие любой сложной организационно-технической системы (СОТС), в том числе и орбитальных группировок космических аппаратов (ОГ КА) различного целевого назначения, во многом определяется эффективностью функционирования соответствующих автоматизированных систем управления (АСУ), обеспечивающих процессы обработки разнородных потоков информации и управления, как КА, так и наземными техническими средствами, входящими в состав наземного комплекса управления (НКУ). При этом важная роль при решении различных классов задач управления КА и НКУ отводится задачам организации и проведения моделирования указанных систем. Анализ результатов многочисленных исследований по вопросам моделирования показал, что для описания таких сложных объектов как АСУ указанными космическими комплексами (КК) должны использоваться полимодельные комплексы, создаваемые в рамках соответствующих интегрированных систем поддержки принятия решений (СППР) [6, 7, 10, 11, 12].

Характерной особенностью названных современных СОТС является наметившаяся устойчивая негативная тенденция, вызванная дальнейшим обострением одного из основных противоречий технико-экономической сферы в XXI веке, связанного с разрывом между уровнем и масштабами общественного производства и уровнем управления этим производством. Это объясняется, прежде всего, нарастающим усложнением объектов и процессов управления и,

соответственно, повышением меры ответственности за принимаемые решения (выбираемые управляющие воздействия), что настоятельно требует строгой регламентации и структуризации технологии управления или, другими словами, индустриализации управления на основе дальнейшей комплексной автоматизации всех видов деятельности, создания различных классов автоматизированных и информационных систем. При этом автоматизация предполагает применения комплекса технических, программных, организационных и прочих методов и средств с целью полного или частичного высвобождения человека от непосредственного участия в получении, передаче, хранении, обработке и использовании материалов, энергии и информации.

Временные задержки и ошибки в управлении, вызванные неверным решением задачи анализа состояний и выдачи управляющих воздействий СОТС, могут привести к необратимым негативным последствиям – срыву боевой задачи, отказам, различным по свои последствиям авариям и даже катастрофам (примеры – катастрофа на Чернобыльской АЭС, гибель АПЛ «Курск», многие авиакатастрофы). В наибольшей степени эта проблема обостряется при возникновении нештатных ситуаций – отклонении поведения СОТС от ожидаемого, вызванного различными внешними и внутренними факторами. В большинстве случаев процедуры анализа состояния и формирования управляющих воздействий СОТС в таких ситуациях не автоматизированы. Решение этой задачи возлагается на операторов. Практика управления различными СОТС показывает, что именно в этих ситуациях операторы не справляются с задачей оценки и контроля функциональных состояний СОТС, что и приводит к различным негативным последствиям.

Увеличение количества контролируемых параметров и требование обеспечить управление СОТС в реальном масштабе времени (РМВ), в том числе при возникновении нештатных ситуаций, обуславливают необходимость постоянного совершенствования процессов сбора, обработки, интерпретации и анализа (технологии мониторинга) измерительной информации, а также – создания специальных, принципиально новых по идеологии построения и функциональным возможностям комплексов автоматизированной интеллектуальной обработки и анализа информации, функционирующих в РМВ [1-5, 8, 9]. Создание и внедрение таких комплексов в наибольшей степени актуально там, где мониторинг состояний СОТС осуществляют операторы по показаниям десятков и более датчиков, донесений и пр. При этом в условиях ограниченных финансово-временных ресурсов особо актуальными становятся вопросы проектирования и внедрения унифицированных языковых средств и методов представления и обработки знаний о процессах функционирования СОТС в РМВ, использование которых позволит в масштабах, например, Вооруженных сил, создать единый многофункциональный комплекс автоматизации, заменяющий все существующие ныне узкоспециализированные программные системы анализа и контроля состояния СОТС. Все это обуславливает необходимость оперативного формирования таких процедур мониторинга состояния и управления (МСУ), при которых обнаружение, локализация и ликвидация сбоев, отказов нештатных аварийных ситуаций будет происходить значительно раньше, чем станут проявляться возможные их последствия.

На основе анализа современного состояния исследований и практической реализации в РФ вопросов проектирования и эксплуатации программных комплексов (ПК) как функционального ядра АСУ СОТС, предназначенных для автоматизации процессов МСУ СОТС, можно сделать вывод, что они, как правило, имеют узкую специализацию, жестко связаны с соответствующими СОТС. Указанные тенденции в настоящее время проявляются в том, что сейчас существует большое количество родственных по своим функциональным возможностям ПК, входящих в состав АСУ СОТС и отличающихся друг от друга лишь по способу организации вычислительного процесса и виду используемой операционной среды. При этом на их эксплуатацию, модернизацию и сопровождение ежегодно в масштабах, в частности, Вооруженных сил расходуются огромные финансовые средства. Из-за ведомственной разобщенности проектировщиков названных систем возникает параллелизм и дублирование в разработке единых по содержанию и назначению ПК МСУ объектов контроля. В случае создания унифицированных языковых

средств и методов представления и обработки знаний о процессах функционирования СОТС в РМВ появляется возможность существенной экономии затрачиваемых на разработку и постановку на информационное обслуживание новых и модификацию существующих объектов контроля.

Проведенный анализ существующих и проектируемых средств МСУ СОТС за рубежом, в частности, в США, показал, что, в первую очередь, в интересах министерства обороны и NASA в рассматриваемом направлении достаточно широко ведутся исследования, интенсивность которых, судя по количеству доступных публикаций, постоянно возрастает, что свидетельствует об актуальности и нетривиальности данной проблемы. Так, еще в начале 2010 года в МО США принята в эксплуатацию объединенная информационная система, что подтверждает намерения США достигнуть не только информационного превосходства, но и осуществить накопление знаний, то есть достигнуть превосходства в интеллектуальной сфере.

Это, по мнению руководства МО США, позволит опережать противника в информационной осведомленности, качестве (обоснованности) принятия решений и результативности (эффективности) применения сил (средств).

Путь, который прошли вооруженные силы США за последнее десятилетие, можно отразить следующим образом: от телекоммуникационной связности – к связности информации; от связности информации – к результатам ее обработки; от результатов обработки информации – к накоплению и использованию знаний.

Вызывает большие опасения, что в области создания автоматизированных систем проектирования и управления, в области создания и развития других информационных технологий (ИТ) для соответствующих автоматизированных систем мониторинга состояния и управления (АСМСУ) в промышленной сфере и военном деле российских фирм в числе мировых лидеров, как правило, нет. Подавляющее большинство российских фирм, как новых, так и вышедших из недр оборонных предприятий и работающих в области информационных и компьютерных технологий, являются распространителями продуктов западных фирм. Немногие компании предлагают конкурентно-способные отечественные разработки. Но, к сожалению, их продукты, с позиций научной и инженерной мысли, зачастую не являются новаторскими, а лишь используют ИТ, появившиеся за рубежом, и отличаются от последних, возможно, лишь большей степенью учета специфики конкретных условий применения.

Очевидно, что для того, чтобы остаться независимым государством и иметь достаточный уровень обороноспособности, такое положение дел устраивать не может. Аргументом в пользу актуальности ИТ может служить факт о том, что холодную войну западные страны выиграли без применения «горячих» средств, а благодаря превосходству именно в ИТ. Более того, тотальная зависимость от кого-либо в информационных технологиях выливается в зависимость государства.

Комплексность и сложность моделей и методов в подобной интеллектуальной системе, ориентированной на цепочку «моделирование – прогнозирование – принятие решения», очевидна. Эта интеллектуальная система может стать регулирующим центром, распределяющим ограниченные ресурсы. И работать она будет в интересах тех, кто сумел создать реализованные в ней ИТ. Поэтому необходимо формулировать задачи соответствующей стратегической инициативы, предусматривающей ориентироваться на создание элементов будущей интеллектуальной системы для моделирования, прогнозирования и принятия решений по актуальным проблемам [1, 2, 5, 8, 9].

Работы по проектированию и использованию СППР с самого начала их возникновения велись и ведутся весьма интенсивно в государственных и коммерческих НИИ, а также в промышленных организациях и в нашей стране. Среди указанных организаций в РФ, которые ориентируют свои разработки в области СППР на задачи МО РФ, можно, в первую очередь, выделить следующие организации РАН: ВЦ РАН, ИСА РАН, ИПУ РАН, СПИИРАН; среди высших учебных заведений – МГУ, СПбГУ, ЛЭТИ, ГУАП, ВоенМех, МАИ, МВТУ, ТГТУ; среди промышленных организаций можно назвать – ЦНИИ ЭИСУ, Военно-промышленная корпорация «Научно-производственное объединение машиностроения» (г. Реутов Московской области); Государственный ракетный центр име-

ни академика В.П.Макеева (г. Миасс Челябинской области); «Информационные спутниковые системы» имени академика М.Ф.Решетнева (г. Железногорск, Красноярский край); Концерн «Гранит-Электрон» (г. Санкт-Петербург); Концерн «Моринформсистема-Агат» (г. Москва); Концерн ПВО «Алмаз-Антей» (г. Москва); Концерн радиостроения «Вега» (г. Москва); Концерн «Созвездие» (г. Воронеж); Объединенная авиастроительная корпорация (Москва); Ракетно-космическая корпорация «Энергия» имени С.П.Королева (г.Королев Московской области); Государственная акционерная компания «Оборонпромкомплекс» (г. Москва,); ОАО «Концерн «Системпром» (г. Москва); Концерн «Научно-производственное объединение «Аврора» (г. Санкт-Петербург); Объединенная судостроительная корпорация (г. Санкт-Петербург); Центр технологии судостроения и судоремонта (г. Санкт-Петербург) и ряд других [1 – 12].

Центральная роль в обеспечении необходимого качества управления СОТС принадлежит интегрированным системам поддержки принятия решений (СППР) и их ядру – специальному программно-математическому обеспечению (СПМО) поддержки принятия решений [8].

СППР предназначена для информационной, методической и инструментальной поддержки процессов подготовки и принятия решений лицом, принимающим решение (ЛПР) на всех этапах управления.

Целью внедрения СППР является повышение оперативности и эффективности деятельности органов управления за счет использования передовых ИТ, оперативного формирования на их основе комплексной аналитической информации, необходимой для выработки и принятия решений.

Для достижения этой цели в рамках внедряемой СППР должны быть решены следующие задачи:

– создание единого признакового пространства и показателей, характеризующих состояния объекта управления на базе централизованного информационного хранилища данных, обеспечивающего накопление, хранение и доступ к экспертным и историческим данным;

– интеграция существующих локальных баз данных в рамках централизованного информационного хранилища данных;

– сбор, накопление и применение знаний опытных экспертов в распределенных базах знаний для формирования выводов и рекомендаций;

– постоянный мониторинг (комплексный анализ) текущей ситуации;

– прогнозирование (сценарное и целевое) развития ситуации;

– повышение оперативности и качества управленческих решений на основе использования аналитических и прогнозных инструментальных средств;

– автоматизация процессов подготовки аналитической отчетности;

– визуализация данных с использованием средств когнитивной графики (в том числе с применением геоинформационных систем и пр.);

– инструментальная и информационная поддержка экспертно-аналитической деятельности ЛПР и экспертов.

В связи со сложностью и многовариантностью проблем управления СОТС и разработки соответствующей СППР необходимо, прежде всего, выработать и обосновать требования, предъявляемые как к СППР в целом, так и к ее основным элементам и подсистемам, исходя из специфики тех задач, которые будут решаться как в процессе управления СОТС, так и в процессе функционирования АСМСУ СОТС.

К числу таких требований, предъявляемых к СППР, можно отнести следующие.

1. Обоснованность принимаемых с использованием СППР решений на различных этапах жизненного цикла АСМСУ СОТС.

2. Обеспечение гармоничного взаимодействия ЛПР с вычислительной средой (создание интеллектуального интерфейса, когнитивной графики).

3. Обеспечение открытости СППР и ее способности к адаптации, самоорганизации и развитию.

4. Своевременность выработки управляющих воздействий.

5. Обеспечение требуемой степени адекватности моделирования АСМСУ СОТС.

Проведенный анализ перечисленных требований показывает, что создание СППР в рамках какого-либо одного класса моделей (математических, логико-лингвистических, логико-алге-

браических и т.п.) приводит к недостоверным, а в ряде случаев, и ошибочным результатам, вызванным низкой степенью адекватности и открытости, отсутствием необходимых программных и информационных средств, обеспечивающих адаптивность одномодельных систем принятия решений.

Выход из создавшейся ситуации состоит в реализации на практике концепции системного моделирования, которая, применительно к процессу управления жизненным циклом АСМСУ СОТС, предполагает полимодельное многоуровневое описание данной системы, а также разработку многоэтапных распределенных процедур принятия решений в условиях многокритериальности и неопределенности.

Анализ показывает, что применительно к задачам принятия решений в АСМСУ СОТС на различных этапах ее жизненного цикла в качестве потенциальных средств автоматизации принятия решений, которые в совокупности образуют распределенную СППР, могут использоваться:

– имитационные системы;

– интеллектуальные информационно-поисковые системы;

– экспертные системы поддержки принятия решений;

– расчетно-логические системы;

– инструментальные CASE–средства автоматизации проектирования.

Конкретный состав и структура взаимодействия данных систем на каждом иерархическом уровне АСМСУ СОТС и для каждого этапа применительно к каждой функции управления должны определяться с учетом специфики функционирования соответствующих элементов и подсистем рассматриваемой системы. Кроме того, при формировании конкретного состава и структуры СППР необходимо учитывать следующую зависимость свойств процедур принятия решений в зависимости от уровня иерархии АСМСУ СОТС (при движении от ее нижнего уровня к верхнему уровню): значимость и цена последствий (с точки зрения конечного предназначения АСМСУ СОТС) принимаемых решений возрастает; требуемые уровни точности и детализации представления информации снижаются; длительность реализации принимаемых решений возрастает.

Учитывая все вышесказанное, можно констатировать, что СППР является основным и, пожалуй, единственно возможным перспективным средством поддержки и принятия решений ЛПР для МСУ в АСУ СОТС военного и промышленного назначения в критических приложениях. Следуя тенденциям мирового развития ИТ, прикладная СППР (для конкретной предметной области) должна быть построена на основе некоторого упоминавшегося выше базового СПМО, которым может стать предлагаемая здесь национальная интеллектуальная аналитическая платформа (НИАП).

Необходимость использования и внедрения НИАП для решения задач проектирования и эксплуатации СППР продиктована неудовлетворительным состоянием в областях военного, государственного и промышленного управления по следующим основным причинам:

– отсутствие единой многоуровневой системы МСУ СОТС на территории РФ;

– отсутствие единой политики в области автоматизации задач МСУ;

– отсутствие единого информационного пространства, единых форматов и технологий обработки информации, единой сети передачи данных, единых корпоративных хранилищ данных;

– наличие разнородных, несовместимых информационных систем, функционирующих на различных программно-аппаратных платформах;

– отсутствие единых механизмов контроля за полнотой, достоверностью, целостностью используемой при МСУ СОТС разнородной информации;

– отсутствие регламентов информационного взаимодействия информационных систем и систем мониторинга;

– недостаточный уровень использования современных ИТ.

Ключевыми принципами построения НИАП должны быть следующие:

– объектно-ориентированный подход к описанию рассматриваемой предметной области;

– сервисно-ориентированные технологии построения систем сбора, обработки, анализа информации и дистрибуции знаний;

– организационное, информационное и функциональное единство в рамках единого ин-

формационного пространства и унифицированной программной платформы на базе единой модели представления данных;

– технологии распределенной разработки, непосредственное участие экспертов (аналитиков) и инженеров по знаниям в концептуальном и логическом проектировании онтолого-ориентированных баз знаний, построении сценариев интеллектуальной оперативно-аналитической обработки информации с опорой на принцип «Программирование без программирования»;

– имитационно-аналитический комплекс с широким набором описательных и предсказательных моделей;

– открытый исходный код и отсутствие лицензионных отчислений зарубежным производителям;

– кросс-платформенная поддержка.

Новизна предлагаемой технологии использования НИАП при построении прикладных СППР обеспечивается:

– внедрением интеллектуальных технологий аналитической обработки и анализа данных и знаний, интеллектуальных систем поддержки принятия решений;

– реализацией концепции единых информационных ресурсов, единого информационного пространства, обеспечивающих интеграцию разнородной полной, непротиворечивой, достоверной и актуальной информации;

– развертыванием систем сбора и хранения разнородной информации на основе оперативно-аналитической и интеллектуальной обработки данных с использованием технологий потоковой обработки;

– использованием единых стандартов сбора, передачи, хранения, обработки и анализа данных и знаний, ориентация на национальные и международные стандарты и протоколы.

Технология обработки и анализа данных при решении задач СППР МСУ СОТС на базе НИАП предполагает наличие следующих основных этапов:

1. Количественная и качественная параметризация разнородных данных, консолидация данных.

2. Предметная ориентация, формирование онтологии предметной области.

3. Поиск, извлечение, интерпретация знаний, формирование репозитария знаний.

4. Построение системы моделей объектов предметной области.

5. Разработка и проверка гипотез, имитационное моделирование.

6. Формирование модельных оценок.

Архитектура СППР АСМСУ СОТС на базе НИАП предполагает наличие следующих основных элементов, выполняющих соответствующие функции:

1. Подсистема сбора – загрузка и консолидация данных из разнородных ресурсов.

2. Подсистема хранения – оперативное и долговременное хранение.

3. Подсистема обработки и анализа – интеллектуальный анализ данных (ИАД).

4. Подсистема прогнозирования – предиктивная аналитика.

5. Подсистема генерации решений – генерация и выбор решений, генерация планов, объяснительная возможность.

6. Подсистема визуализации и отчетности – интерпретация знаний.

Тем самым, НИАП МСУ СОТС призвана сформировать единую информационно-технологическую инфраструктуру проектирования, разработки, развертывания и эксплуатации СППР АСМСУ СОТС на базе отечественных технологий и на основе внедрения технологической цепочки «данные – информация – знания – решения».

К настоящему времени имеется не только необходимость, но и возможность разработки и внедрения унифицированной комплексной интегрированной СППР для АСМСУ СОТС в критических приложениях. У организаций РАН и отечественных предприятий промышленности появился достаточный задел для разработки и внедрения рассматриваемой системы в общегосударственном масштабе.

С целью обеспечения функционирования СППР АСМСУ ВС понадобятся группы экспертов, которые смогут осуществить коррекцию циркулирующей в системе обработки данных информации.

1. Группа изменения исходных данных/знаний.

2. Группа анализа проведенных мероприятий и корректирования методологии функционирования СППР АСМСУ ВС.

С появлением новых средств вооруженной борьбы, изменением подходов к ведению войн

и военных конфликтов, возникнет необходимость изменения методологии принятия решения на применение сил и средств.

В целях подготовки необходимых данных/знаний для внесения изменений в действующую СППР АСМСУ ВС понадобятся экспертные группы, создаваемые при организациях, ответственных за сопровождение введенной в эксплуатацию СППР АСМСУ ВС и органах оперативного, оперативно-стратегического и стратегического уровней управления.

Контроль и оказание помощи в разработке новых походов к управлению и применению сил и средств должны осуществляться рабочими группами, создаваемыми при соответствующих органах военного управления и военно-научных организациях.

СПИСОК ЛИТЕРАТУРЫ

1. Вагин В.Н., Еремеев А.П. Некоторые базовые принципы построения интеллектуальных систем поддержки принятия решений реального времени. // Изд. РАН. Теория и системы управления, 2001, №6, с. 114 – 123.

2. Васильев С.Н. От классических задач регулирования к интеллектному управлению // Теория и системы управления, 2001. – № 1. – С.5-22; № 2. – С.5-21.

3. Гаврилов А.В. Гибридные интеллектуальные системы. Новосибирск.: Изд-во НГТУ, 2003. – 164 с.

4. Гаврилова Т.А. Использование онтологий в системах управления знаниями. Труды Международного конгресса «Искусственный интеллект в XXI веке». Россия, Дивноморское, 2001. с. 21 – 32.

5. Городецкий В.И. Многоагентные системы: современное состояние исследований и перспективы применения // Новости искусственного интеллекта, 1996, № 4, с. 44 – 59.

6. Калинин В.Н, Соколов Б.В. Многомодельный подход к описанию процессов управления космическими средствами //Теория и системы управления. – .1995. – №1. – с. 56 – 61.

7. Калинин В.Н., Резников Б.А. Теория систем и управления (структурно-математический подход). – Л.: ВИКИ, 1987.

8. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных объектов – М.: Наука, 2006.- 410 с.

9. Попов Э. В., Фоминых И. Б., Кисель Е. Б., Шапот М. Д. Статические и динамические экспертные системы. // М.: Финансы и статистика, 1996.

10. Ростовцев Ю.Г. Основы построения автоматизированных систем сбора и обработки информации. – СПб.: ВИКИ, 1992. – 717 с.

11. Ростовцев Ю.Г., Юсупов Р.М. Проблема обеспечения адекватности субъектно-объектного моделирования// Известия ВУЗов. Приборостроение. – № 7, 1991. – С.7-14.

12. Саати Т. Принятие решений. Метод анализа иерархий. М.: Радио и связь, 1993. 350 С.

С.В. Акимов
кандидат технических наук, доцент
Г.В. Верхова
доктор технических наук, профессор

МОДЕЛИРОВАНИЕ КОММУТАЦИОННОГО ПРОСТРАНСТВА СРЕДСТВ ТЕЛЕКОММУНИКАЦИИ

В работе приведены результаты исследования коммутационного пространства телекоммуникационных средств; предложена комплексная информационная модель коммутационного пространства; показано, как такая модель может использоваться при проектировании модульных систем; рассмотрены современные средства проектирования элементов коммутационного пространства.

Ключевые слова: коммутация, коммутационное пространство, интерфейс, магистраль, электрический соединитель, кабель, жгут, информационная модель, комплексная модель, средство телекоммуникации.

Введение

При создании телекоммуникационных комплексов и средств одной из важнейших задач является реализация коммутации между отдельными ячейками, блоками и стойками системы . При проектировании коммутационного пространства часто возникают проблемы, одна из которых учет совместимости интерфейсов, жгутов, кросс-плат, фидеров, оптоволоконных линий. Ситуацию усугубляет тот факт, что такие проблемы довольно часто возникают на поздних стадиях разработки, что ведет к значительным затратам на перепроектирование. Это во многом объясняется отсутствием специальной методологии проектирования коммутационных пространств, моделей и информационных систем, автоматизирующих процесс проектирования коммутационных пространств, обеспечивающих удобство и учет совместимости интерфейсов и средств коммутации на самых ранних этапах, снабжение проектировщика актуальной информацией о свойствах различных элементов коммутационного пространства, производимых разными фирмами.

Данная статья посвящена созданию комплексных моделей коммутационного пространства, учитывающих различные аспекты коммутационных пространств, и способных стать основой для объединения отдельных программных приложений, отражающих эти аспекты, в единую среду сквозного проектирования телекоммуникационных средств.

Логическое и физическое коммутационное пространство

Любая система может взаимодействовать с другими системами, агрегатами системы и с внешней средой. Такое взаимодействие осуществляется посредством интерфейсов и коммутационного пространства. Под интерфейсом будем понимать механизм сопряжения системы с внешним миром, через который осуществляется циркуляция вещественных, энергетических и информационных потоков. Примерами интерфейсов в таком понимании являются: клеммы резисторов, катушек индуктивности, транзисторов; соединительные муфты труб; кабельные муфты. Под коммутационным пространством

будем понимать совокупность связей между интерфейсами элементов.

Описать структуру системы на уровне интерфейсов составляющих ее элементов $I^{(E)}$, коммутационного пространства $R^{(I)}$ ожно в следующем виде:

$$S^{(I)} \underline{\underline{def}} < I^{(E)}, R^{(I)} > .$$

Целесообразно разделить интерфейсы и коммутационные пространства на два класса: логические и физические (рис. 1). Логические интерфейсы и коммутационные пространства описывают коммутационную структуру системы без учета привязки к конкретным типам «физических» интерфейсов (электрических соединителей, муфт и т.д.) и коммутационных средств (кросс-плат, кабелей и т.д.). Это обеспечивает в случае необходимости возможность при разработке принципиальных и потоковых схем отвлечься от привязки функциональных элементов к конкретным «физическим» модулям и способам их конструктивной связи. Отображение ло-

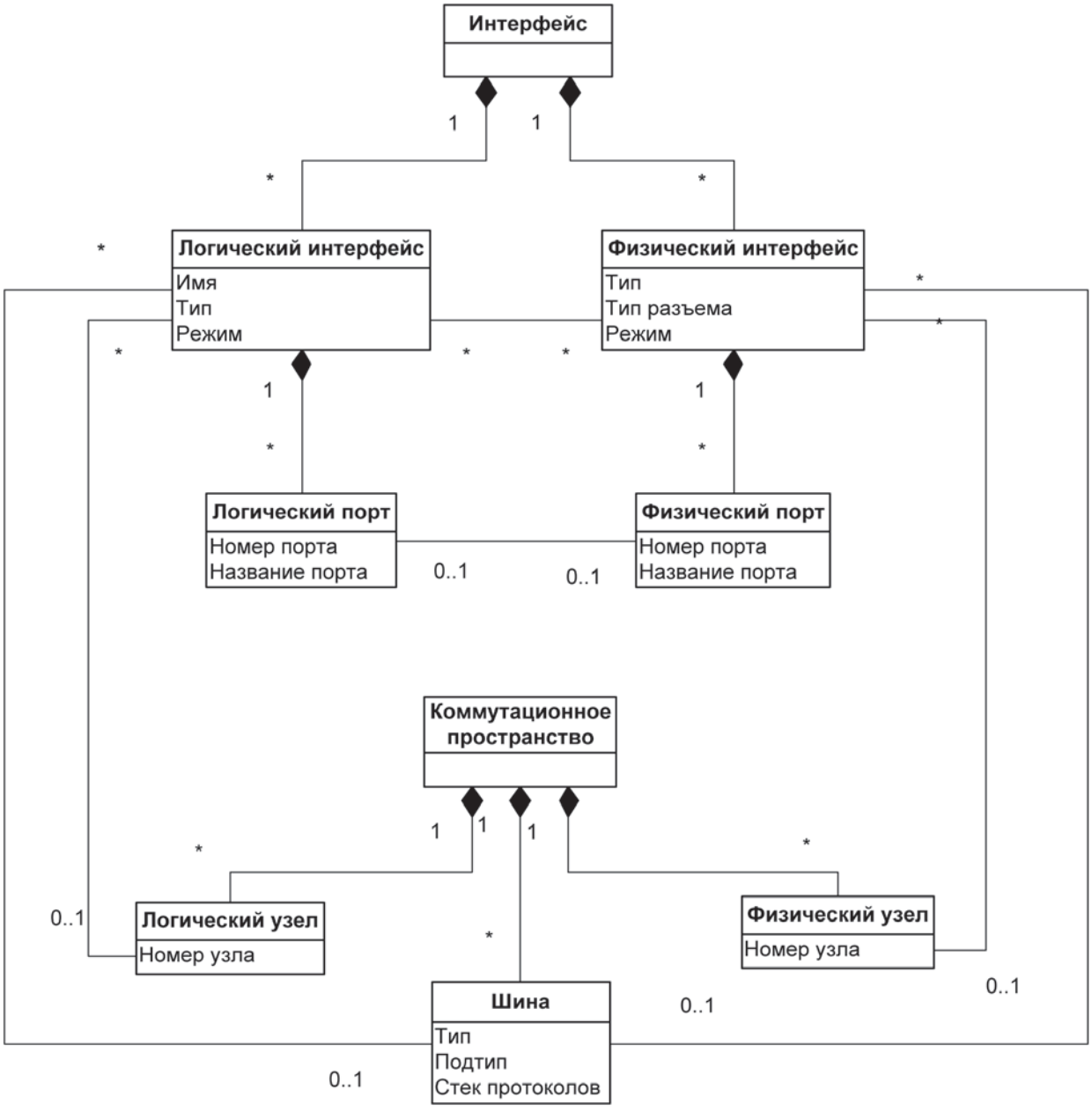


Рис. 1. Концептуальная модель логического и физического коммутационного пространства

гических интерфейсов и коммутационных пространств на физические может быть отложено на более поздние этапы.

При описание логического интерфейса необходимо указать его тип (USB, USB 2.0, PCI, RS-485 и т.д.) и режим коммутирования (шина / порты / шина + порты). В случае режима «шина», задается подключение к шине без конкретизации коммутационного пространства отдельных портов. В случае режима «порты» определяется коммутационное пространство для каждого задействованного порта. В случае режима «шина + порты» задается как шина, так и коммутационное пространство для всех задействованных портов.

При описании физического интерфейса необходимо указать его тип, тип разъема (USB Тип A, USB Тип B и т.д.), режим коммутирования (шина / порты / шина + порты). Более того, в случае создания комплексных моделей электронных модулей целесообразно иметь возможность указать и более подробную информацию о разъемах. То же самое справедливо и для комплексных моделей других классов объектов.

В случае электронных модулей под шиной будем понимать двунаправленный универсальный коммутатор, осуществляющий передачу информации между модулями. В общем случае шиной может быть любая магистраль, обеспечивающая двунаправленную передачу вещественных, энергетических или информационных потоков между двумя и более объектами.

Стратегия использования комплексных моделей коммутационного пространства в процессе проектирования телекоммуникационных средств

Логические модели позволяют задать интерфейсы и связи между ними без конкретизации как эти связи будут реализованы «в железе». Кроме того, при задании связей можно даже не учитывать, как будут реализованы эти связи (в виде кросс-плат, жгутов и т.д.); нет необходимости рассматривать, по каким шкафам будут распределены блоки, и по каким блокам будут разнесены модули. При работе с логически пространством разработчик целиком и полностью сосредотачивается на том, какие объекты (интерфейсы объектов) будут связаны между собой, не заостряя внимания на реализации такого соединения (рис. 2). Таким образом, логическое пространство, является частью логических (принципиальных и функциональных) схем.

В случае физического коммутационного пространства проектировщик реализует логическую модель «в железе» (выполняет отображения логической модели в физическую). Он определяет:

1) типы коннекторов плат и блоков (проектировщик модулей);

2) размещение модулей по блокам, блоков по шкафам, а шкафов на носителе;

3) реализация связей (жгутов, кросс-плат, оптических кабелей, wi-fi).

Пункты 1–2 и частично пункт 3 могут выполняться в рамках автоматизированной системы комплексирования телекоммуникационных средств с привлечением соответствующих баз данных [1]. Для реализации пункта 3 могут быть привлечены специальные САПР, причем должна быть реализована обратная связь между этими САПР и автоматизированной системы комплексирования телекоммуникационных средств. В данном случае такая автоматизированная система, в основу которой положены комплексные модели, будет выполнять еще и роль PDM системы [2], собирая воедино всю информацию о проекте, наглядно демонстрируя проектировщику, что уже реализовано, а что нет. Это второе важное назначение комплексной модели коммутационного пространства – собрать все воедино.

Комплексные модели могут лечь в основу САПР модульных систем, а точнее, той их части, которая отвечает за проектирование интерфейсов и связей (коммутационного пространства). Данные САПР могут действовать по следующей схеме. Сначала проектировщик создает логическое коммутационное пространство, используя исключительно информационные модели. Затем он выполняет отображение логического коммутационного пространства в физическое, но пока опять же оставаясь на уровне комплексных информационных моделей. Для наглядности элементы логического пространства, которые уже отображены на физическое, будут выделяться другим цветом. Далее, пользователь может в одной или нескольких программах начать проектирование (реализацию) физического коммутационного пространства, уже получая 3D модели. Информационные модели, уже реализованные

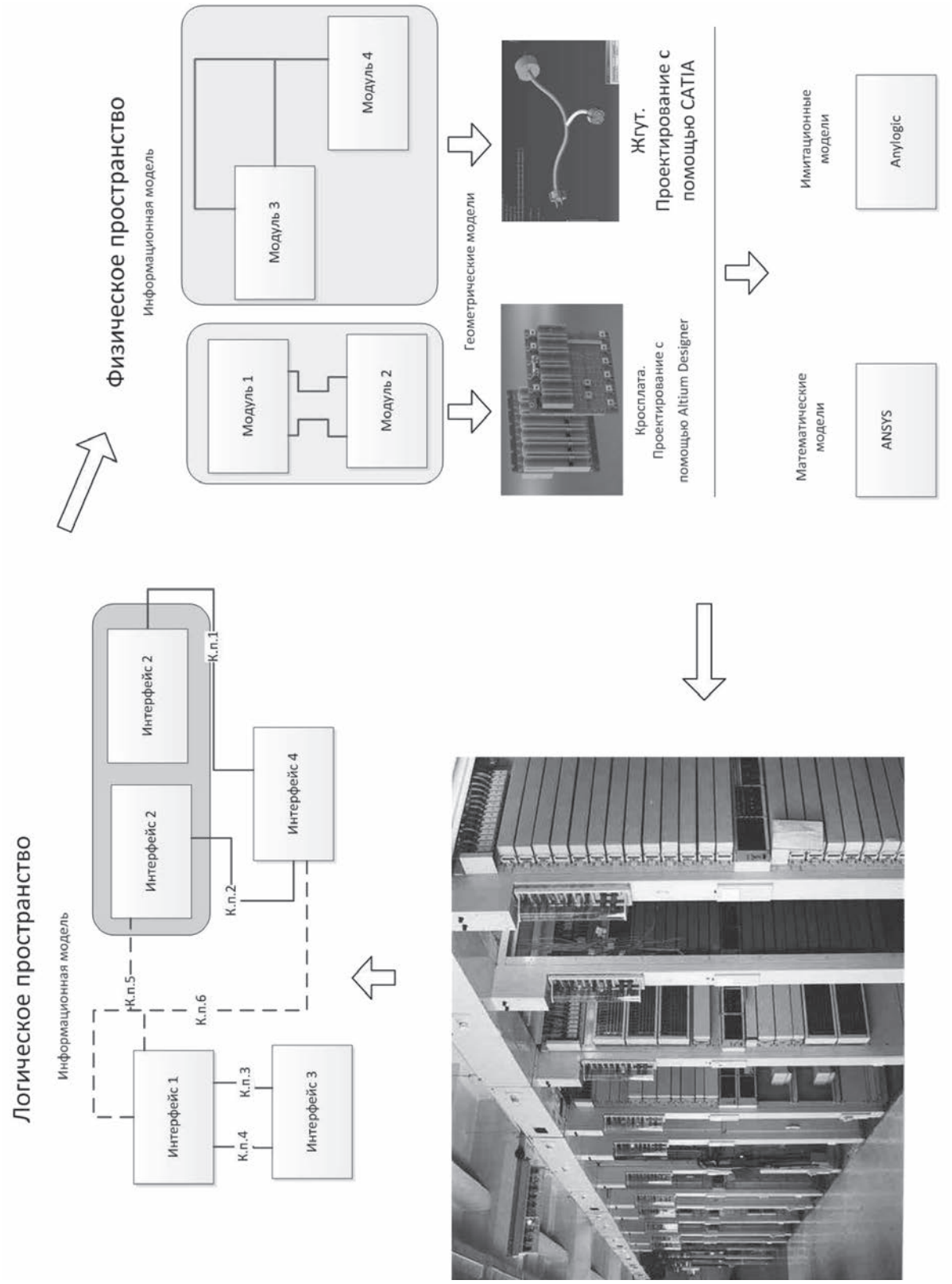


Рис. 2. Стратегия использования комплексных моделей коммутационного пространства в процессе проектирования телекоммуникационных средств

во внешних САПР, могут выделяться определенным образом (например, цветов), а через них будут выделяться и модели логического коммутационного пространства. Таким образом, образуется двунаправленная связь (отображение): логическое коммутационное пространство – информационная модель физического коммутационного пространства – конструктивная (3D) модель физического коммутационного пространства. Модель коммутационного пространства становится многоаспектной, связывающей воедино различные модели, отражающие отдельные аспекты коммутационного пространства. Причем для моделирования этих отдельных аспектов могут использоваться различные виды формализмов, реализованных в отдельных программных приложениях (ANSYS, CATIA и т.д.). Таким образом, данные модели обеспечивают как процесс сквозного проектирования, так и концентрацию разноаспектной информации (чисто коммутация, 3D, тепловые модели, механика разрушений и т.д.), с различной степенью детализации и точности.

Выводы

Предложенные в работе модели коммутационного пространства телекоммуникационных средств обеспечивают:

– разделение принципиально разных процессов в проектировании телекоммуникационных средств: разработку логических (функциональных, принципиальных схем) и их конструктивную реализацию;

– объединение многоаспектной информации о коммутационном пространстве, представляемой с помощью различных видов формализмов и пакетов прикладных программ;

– создание на их основе нового вида САПР, автоматизирующих процесс проектирования модульных телекоммуникационных систем, учитывающих специфику модульного принципа построения.

СПИСОК ЛИТЕРАТУРЫ

1. Акимов С.В., Меткин Н.П. Автоматизированная система комплексирования радиоэлектронных средств на основе комплексных моделей электронных модулей // Вопросы радиоэлектроники. Серия «Общетехническая», выпуск 1, 2012. С. 191-199.

2. Вичугова А.А., Дмитриева Е.А., Цапко Г.П. Разработка модели данных PDM-системы ENOVIA Smarteam для управления спецификациями при создании радиоэлектронной аппаратуры // Прикладная информатика. 2010. № 5. С. 23-29.

С. В. Акимов
кандидат технических наук, доцент (СПбГУТ),

Г. В. Верхова
доктор технических наук, профессор (СПбГУТ),

К. В. Белоус

ЕДИНОЕ ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО ПОЧТОВОЙ СВЯЗИ НА ОСНОВЕ МНОГОАСПЕКТНЫХ МОДЕЛЕЙ

Представлена концепция единого информационного пространства почтовой связи, в основу которого положены многоаспектные модели предметной области. Показано, что специфика почтовой связи накладывает особые требования на программно-информационное обеспечение, которые можно удовлетворить применением особого вида многоаспектных моделей.

Ключевые слова: единое информационное пространство, почтовая связь, многоаспектная модель, геоинформационная система, почтовое отправление, объект почтовой связи.

Введение

Управление сложными организационными системами, к которым относится «Почта России», обеспечение их эффективного функционирования, их проектирование и оптимизация требуют соответствующего информационно-программного обеспечения. На кафедре «Автоматизации предприятий связи» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича проводятся исследования, целью которых является разработка единого информационного пространства ФГУП «Почта Россия», которое должно послужить информационному обеспечению управления, проектирования и оптимизации структур и производственных процессов ФГУП «Почта России», повышению качества предоставляемых населению услуг, расширения их номенклатуры. Отдельно следует отметить необходимость актуальной исчерпывающей и хорошо структурированной информации для решения задач автоматизированного проектирования и оптимизации в почтовой связи, к которым относятся оптимизация почтовых маршрутов, размещение отделений почтовой связи и автоматизированных сортировочных центров. Решение этих задач не возможно без использования единой информационной системы, основанной на модели предметной области, так как только такая система способна обеспе-

чить целостность и актуальность данных, и только такая система способна обеспечить единое информационное пространство почтовой связи. Данная статья посвящена концепции единого информационного пространства ФГУП «Почта России», в основу которого положен особый вид многоаспектных моделей предметной области.

Многоаспектное моделирование

Особенностью комплексной информатизации процессов проектирования, управления и реорганизации в современных корпорациях является необходимость поддержки различных видов деятельности [1-2]: стратегическое и оперативное управление, оптимизация бизнес-процессов, поддержка обслуживания клиентов, ведомственная связь (рис. 1). В их основе используются различные виды моделей, методов и пакетов компьютерных программ (таблица 1), поэтому для создания единого информационного пространства необходим особый вид моделей, в которых будут гармонично сочетаться вышеперечисленные аспекты, традиционно представ-

Рис. 1. Единое многоаспектное пространство проектирования и управления

Таблица 1

Отношение видов деятельности, моделей, методов и программного обеспечения

Деятельность	Модели и методы	Программное обеспечение
Оперативное управление	Методы общего менеджмента, системный анализ, теория принятия решений в условиях неопределенности, методы контроля качества, множества Парето, реляционная модель данных	ERP, СУБД, Decision Support Systems, GIS, экспертные системы, заказное программное обеспечение
Обработка почтовых отправлений	Теория автоматического управления, методы распознавания образов, теория маршрутизации	АСУ ТП
Проектирование и реорганизация	Общая теория проектирования, теория принятия проектных решений, имитационное моделирование, теория логистики, математическое программирование, комбинаторные методы, методы поиска на графах, многокритериальная оптимизация	CAD/CAM/CAE, GIS, системы имитационного моделирования, программные пакеты статистических расчетов, системы визуализации графов, заказное программное обеспечение
Интеграция почтовых и банковских услуг	Криптография, статистические методы, реляционные модели данных	Автоматизированные банковские системы, системы электронных платежей, СУБД, заказное программное обеспечение
Организация подписки на периодические издания и торговля по каталогу	Реляционные модели данных, методы математической статистики, криптография	СУБД, системы электронных платежей, заказное программное обеспечение

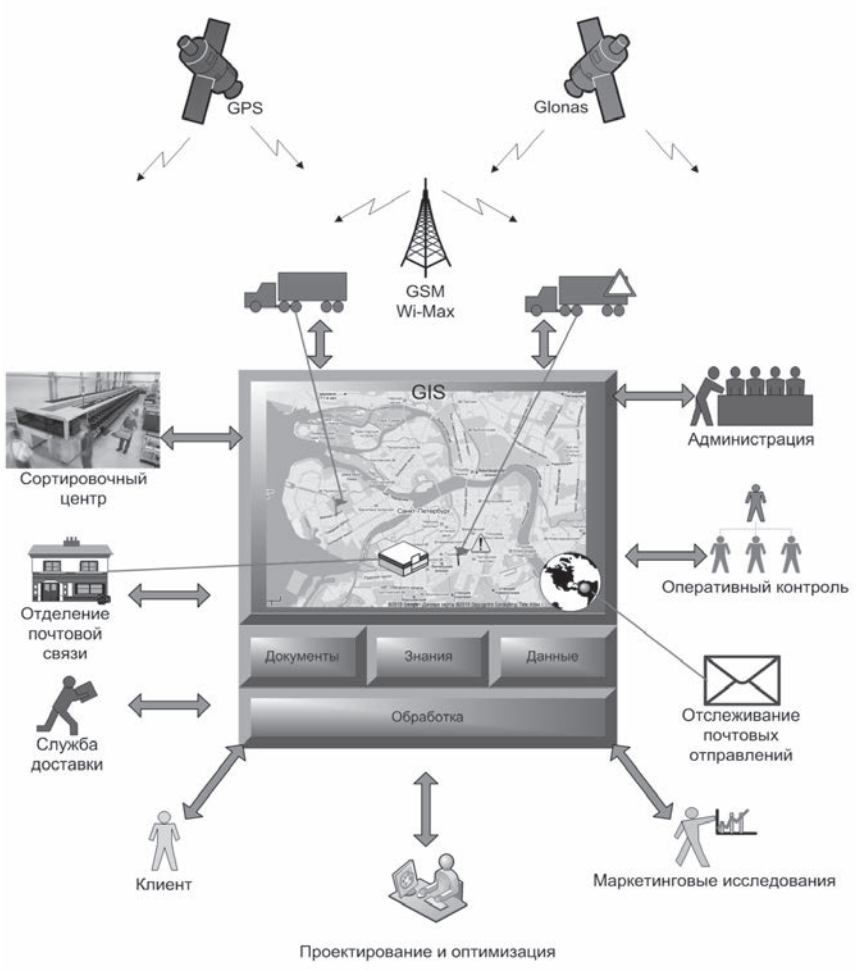


Рис. 2. Единое информационное пространство ФГУП «Почта России»

ляемые формализмами, относящимися к различным классам (рис. 2).

Из таблицы можно видеть, что с одной стороны, для обеспечения различных видов деятельности используется отдельное множество моделей, методов и пакетов программного обеспечения, но с другой – эти множества частично пересекаются. Это является основанием для создания особой единой среды многоаспектного моделирования, которая должна обеспечить системное объединение таких моделей, методов и программного обеспечения, а также минимизировать их избыточность и дублирование. В рамках проводимых исследований единое информационное пространство строится на базе многоаспектных моделей объектов, теория и методология которых разрабатывается сотрудниками кафедры. Многоаспектную модель можно представить в виде системы [3]:

$$\begin{cases} \mathrm{E} \underline{\underline{\mathrm{def}}} \bigcup\limits_{iasp=0}^{nasp} Asp_{iasp}, \ iasp \in \overline{1, nasp} \\ M \underline{\underline{\mathrm{def}}} \bigcup\limits_{im=0}^{nm} M_{im}, \quad im \in \overline{1, nm} \\ \mathrm{E}M \underline{\underline{\mathrm{def}}} \bigcup\limits_{i\alpha=0}^{n\alpha} AM_{i\alpha}, \ i\alpha \in \overline{1, n\alpha} \\ AM_{i\alpha} \underline{\underline{\mathrm{def}}} \langle A_{i\alpha}, M_{i\alpha} \rangle, \\ A_{i\alpha} \in \mathrm{E} \\ M_{i\alpha} \in M \\ \left\| \mathrm{E}M \right\| \geq \left\| \mathrm{E} \right\| \end{cases}$$

где Å – множество аспектов моделируемого объекта; M – множество моделей, представляющих Å; ÅM – множество связей аспект-модель.

В роли объектов могут выступать структурные подразделения, материальные и человеческие

ресурсы, документы, оказываемые услуги и т.д. Многоаспектная модель объекта может содержать различную информацию: геоинформационную, статистическую, мультимедийную. Также могут учитываться семантические связи между объектами (класс/подкласс, вышестоящий/нижестоящий, часть/целое и т.д.) и потоки (материальные, информационные, энергетические). Для представления и обработки этой информации могут использоваться программные пакеты сторонних производителей, оптимизированных для решения определенных задач, так как большая часть современного программного обеспечения создается по технологии открытых систем. Кроме того в рамках интегративных моделей возможно моделирование не только отдельных объектов, но и целых классов объектов и даже методов их синтеза (оптимизации). В таких моделях множество отдельных объектов задается интенсионально (аксиоматически) при помощи методов морфологического анализа и инженерии знаний, а модель конкретного объекта получается путем наложения соответствующих ограничений.

Особенность представления информации об объектах почтовой связи

Основными типами объектов системы почтовой связи являются предприятия почтовой связи и почтовые отправления. Предприятия почтовой связи обеспечивают доставку почтовых отправлений, посредством создания географически распределённых вещественных потоков. В организации потоков задействованы различные виды доставки: автомобильный, железнодорожный, морской и воздушный транспорт. Единая информационная система почтовой связи должна обеспечивать:

- оперативный контроль функционирования многочисленных предприятий почтовой связи;
- согласованное функционирование различных служб;
- отслеживание в реальном времени прохождения регистрируемых почтовых отправлений, как сотрудниками почтовой связи, так и клиентами;
- оперативное взаимодействие с клиентами;
- динамическую диспетчеризацию почтовых транспортных средств;
- проектирование и оптимизацию предприятий почтовой связи.

Это накладывает особые требования на модели информационной системы, обеспечивающей единое информационное пространство почтовой связи (рис. 2), сводя воедино датологические, геоинформационные и финансовые модели; информационные модели предприятий почтовой связи и регистрируемых почтовых отправлений, а также транспортных средств.

Объекты и связи между объектами (дорожно-транспортные сети), имеющие географическую привязку, могут отображаться при помощи геоинформационных систем. Важность геоинформации для единого информационного пространства «Почты России» определяется основным назначением почтовой службы: организацией материальных потоков, обеспечивающих доставку почтовых отравлений адресатам. Такая информация необходима для обеспечения:

- оперативного управления деятельностью многочисленных отделений почтовой связи;
- мониторинга транспортных средств, задействованных в обеспечении материальных потоков почтовых отправлений;
- оптимизации почтовых маршрутов, размещения отделений почтовой связи и сортировочных центров;
- эффективного взаимодействия с клиентами.

Единое информационное пространство почтовой связи представляет собой многоаспектную среду, включающую в себя различные виды программного обеспечения, построенных на соответствующих формализмах. Назначением многоаспектных моделей является объединение данных гетерогенных систем в единое целое, дополнение функциональности, отсутствующей в других моделях и пакетах программного обеспечения.

Отображения геоинформации в едином информационного пространстве ФГУП «Почта России» реализуется с помощью геоинформационных служб Google (Google Maps, Google Earth) и Яндекс Карты, благодаря следующим свойствам:

- открытый и хорошо документированный интерфейс прикладного программирования (API);
- возможность представления информации в Интернете;
- гибкость в способах отображения информации на электронной карте;

• полная поддержка технологии XML.

В контуре разработки и оптимизации транспортных маршрутов используется система Open Street Map, благодаря ее открытости и возможности автоматического извлечения информации об организации движения. Контур оптимизации разрабатывается сотрудниками кафедры «Автоматизации предприятий связи». Особенность контура состоит в возможности гибкой настройки на решаемую задачу: поиск кратчайшего маршрута, определение маршрутов выемки почтовой корреспонденции, диспетчеризация транспортных средств; наличие расширяемого модуля квалиметрии [4]. Результаты расчетов могут быть экспортированы как в систему Open Street Map, так и в другие геоинформационные системы с открытым интерфейсом (Google Map, Яндекс Карты). Таким образом, сам модуль строится по технологии многоаспектных моделей и может быть включен в многоаспектную информационную систему более высокого уровня, в нашем случае – в единое информационное пространство почтовой связи.

Для представления и обработки данных и документальной информации служат системы, построенные с использованием технологии объектно-ориентированного программирования и реляционных баз данных. Именно эти модели отражают специфику объектов почтовой связи, и служат ядром многоаспектного информационного пространства (многоаспектные модели на рис. 1). Данные модели отражают различные аспекты предметной области, обеспечивая информационное описание объектов почтовой связи, сводя в единое целое все многообразие прикладного программного обеспечения, выполняющего конкретные задачи, обеспечивая скоординированную работу почтовой связи (рис. 2).

Заключение

Важность единого информационного пространства для таких организаций как «Почта России» трудно переоценить. Имея разветвленную сеть материальных потоков, обеспечивающую доставку материальных объектов в любую точку России, необходимы прогрессивные средства управления этими потоками, своевременное информирование населения и обеспечение удобного дистанционного взаимодействия с клиентами, что возможно эффективно осуществить лишь на базе единого информационного пространства. Учитывая принципиальную многоаспектность данного информационного пространства, необходим особый вид моделей, на основе которых такое информационное пространство будет построено – многоаспектные модели, обеспечивающие гармоничное представление различных видов знаний, на основе которых строится единое информационное пространство ФГУП «Почта России», концепция которого предложена в данной статье.

СПИСОК ЛИТЕРАТУРЫ

1. Мельник В.И., Феликсон А.Е. Ориентировочная оценка эффективности мероприятий по совершенствованию АСУ / Вопросы радиоэлектроники. 2006. № 1. С. 24-32.

2. Буряков В.А. Технология повышения достоверности принятия решений в автоматизированных системах управления / Вопросы радиоэлектроники. 2007. № 2. С. 30-40.

3. Акимов С.В., Меткин Н.П. Многоаспектная модель структурно-параметрического синтеза системных объектов // Вопросы радиоэлектроники. 2012. Т. 1. № 1. С. 178-190.

4. Крылов А.Д. Использование открытых картографических данных в объектной модели дорожно-транспортной сети для задач транспортной оптимизации / SWorld. Материалы международной научно-практической конференции «Современные проблемы и пути их решения в науке, транспорте, производстве и образовании» 2011. Выпуск 4. Том 1. С. 74-78.

С.В. Акимов.
В.А. Бабошин
П.А. Ботин
Г.В. Верхова

МЕТОДИКА АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ТЕЛЕМАТИЧЕСКИХ УЗЛОВ СВЯЗИ НА ОСНОВЕ КОМПЛЕКСНЫХ МОДЕЛЕЙ

Телематические узлы связи являются основными составными единицами глобальных вычислительных сетей общего и специального назначения, на основе которых строятся распределенные системы, качество функционирования и эффективность которых, во многом определяется тактико-техническими (ТТХ) и технико-экономическими характеристиками (ТЭХ) телематических узлов. Это определяет важность наличия эффективных методик автоматизированного проектирования телематических узлов связи с заданными ТТХ и ТЭХ. Телематический узел представляет собой сложный программно-аппаратный комплекс, строящийся с использованием магистрально-модульного принципа построения [1].

Несмотря на большое разнообразие систем автоматизированного проектирования (САПР), применяемых при создании радиоэлектронных средств (РЭС), к которым можно отнести и телематические узлы связи, в свободном доступе отсутствуют САПР, ориентированные на проектирование модульных систем. Автоматизированные системы проектирования телематических узлов должны базироваться на особых методиках и моделях, учитывающих особенности построения (комплексирования) систем и комплексов из готовых модулей различного уровня разукрупнения. В основу таких САПР должны быть положены комплексные модели радиоэлектронных средств, учитывающие на системном уровне многоаспектную информацию о модулях [2]. САПР, ориентированные на комплексирование телематических узлов связи в первую очередь должны обеспечить информационную поддержку о доступных модулях (включая информацию о разрешении использования тех или иных модулей в системах специального и двойного назначения), учету совместимости этих модулей и вычислению ТТХ и ТЭХ телематических узлов.

Комплексную модель электронного модуля можно представить в следующем виде [3]:

$$CXM = <P^{(1)}, P^{(2)}, I, E, I^{E}, R, Eval>,$$

где $P^{(1)}$ – первичные параметры объекта; $P^{(2)}$ – вторичные параметры объекта; I – информация об интерфейсах моделируемого объекта; E - информация о компонентах (подсистемах), составляющих объект; I^{E} – информация об интерфейсах компонентов (подсистем); R – коммутационное пространство; $Eval$ – правила вычисления вторичных параметров объекта.

Комплексные модели электронных модулей обеспечивают представление о ТЭХ (посредством $P^{(1)}$ и $P^{(2)}$), подсистемах, интерфейсах и правилах вычисления вторичных параметров с учетом ТЭХ подсистем и способов их коммута-

ции. На системном уровне большая часть расчетов может выполняться по формулам, непосредственно заложенным в комплексные модели отдельных модулей, но могут привлекаться и внешние САПР и системы компьютерного моделирования. Информация, содержащаяся в комплексной модели электронного модуля, приведена в таблице 1. Следует заметить, что структура представления информации пунктов 1 – 9 является инвариантной типу электронного модуля; специфической для конкретных типов модулей (сервер, модуль памяти, коммутатор и т.д.) будет лишь информация, приведенная в пунктах 10 – 11. Данный факт способствует сокращению расходов на создание комплексных моделей модулей, из которых будут создаваться телематические узлы связи.

Среда комплексного моделирования может быть представлена следующим выражением:

$$UCXM = <\boldsymbol{CXM}, Select, Modif>,$$

где ***CXM*** – множество всей совокупности комплексных моделей; *Select* – оператор выбора объектов, удовлетворяющих определенным признакам; *Modif* – оператор модификации *CXM* и ***CXM***.

Одной из особенностей методики автоматизированного проектирования телематических

Таблица 1

Виды информации, представляемой комплексными моделями

№	Вид информации	Примечание
1	Общая информация	Тип модуля, производитель, общий вид модуля и т.д.
2	Конструкторско-технологическая информация	Массогабаритные характеристики, файлы с документацией ЕСКД и ЕСТД
3	Интерфейсы	Информация об интерфейсах модуля, включая типы и марки электрических соединителей; возможны различные уровни конкретизации, вплоть до назначения каждого PIN
4	Компоненты	Информация о модулях, являющихся подсистемами данного модуля. Представляются комплексными моделями, имеющими аналогичную структуру.
5	Коммутационное пространство	Информация о связях интерфейсов компонентов между собой и с интерфейсами модуля. Коммутационное пространство может быть логическим (указываются связи, без конкретизации реализации) и физическим, когда конкретизируется реализация (жгуты, кросс-платы)
6	Требование по питанию	Информация о требуемых характеристиках: номиналы напряжения и тока, коэффициент пульсаций, качество стабилизации и т.д. Вид электрических соединителей, обеспечивающих пинатие, может быть задан через интерфейсы
7	Электронная документация	Мультимедийные файлы с электронной документацией
8	Условия эксплуатации, технические условия, расписание регламентных работ, статистика, паспорт объекта и т.д.	Мультимедийные файлы, содержащие указанную информацию
9	Тепловой режим	Информация о тепловыделении модуля. Может быть использована при выборе систем охлаждения и оптимизации размещения блоков в стойке
10	Функциональные характеристики	В структурированном виде содержит данные о функциональных характеристиках модуля
11	Конфигурация объекта	Информация о текущей конфигурации расположение перемычек, положение регуляторов и т.д.

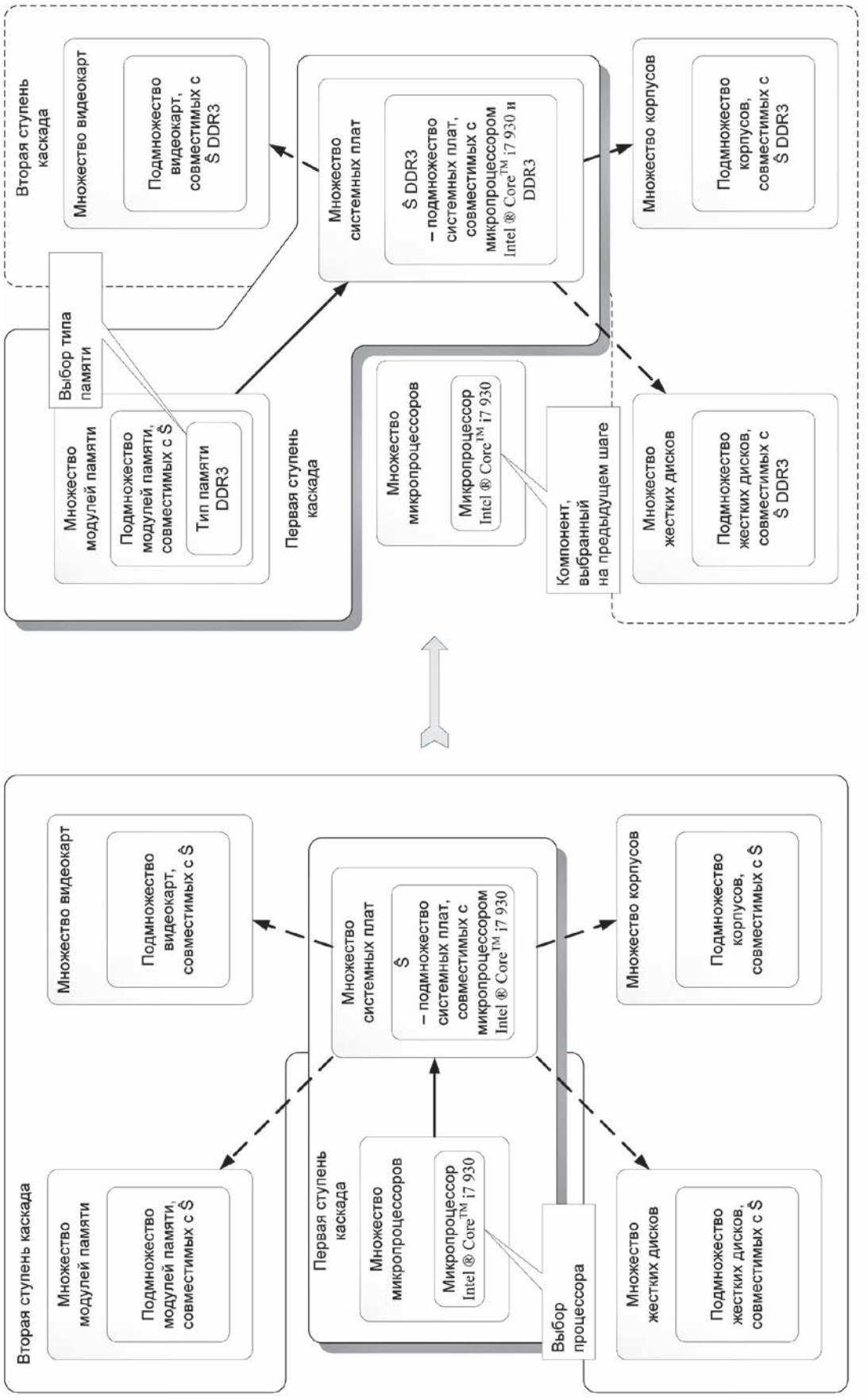


Рис. 1. Пример использования механизма каскадной фильтрации при комплексировании системного блока

узлов, является механизм каскадной фильтрации, обеспечивающий разработчику возможность выбора лишь тез модулей, которые совместимы с текущим решением, которое получено на предыдущих шагах процесса комплексирования. Рассмотрим пример комплексирования с использованием механизма каскадной фильтрации на примере выбора компонентов системного блока (рис. 1). Выбор на первом шаге процессора конкретного типа автоматически влечет отсев системных плат, несовместимых с данным процессором (первая ступень каскада). Полученное множество системных плат, позволяет отфильтровать другие компоненты (модули памяти, видеокарты, корпуса и т.д.), которые несовместимы ни с одной из системных плат, совместимых с выбранным процессором (рис. 1, а). Выбор конкретного типа модуля памяти, осуществляемый на втором шаге, влечет фильтрацию множества печатных плат, совместимых как с данным модулем памяти, так и с процессором, выбранным на первом шаге. На втором каскаде фильтрации происходит отсев компонентов, несовместимых с новым множеством системных плат (рис. 1, б).

Применение комплексных моделей в автоматизации проектирования телематических узлов связи специального и двойного назначения обеспечит:

- унифицированное предсатвления системной информации об электронных модулях и переферийных устройствах;
- базу данных электронных модулей и переферийных устройств, сертифицированных для создания телематических узлов специального назначения;
- композицию комплексных моделей сложных объектов (блоков, пультов, стоек, телематических узлов) из комплексных моделей объектов-агрегатов (подсистем);
- представление множества комплексных моделей отдельных объектов и определения на нем операторов манипуляции отдельными моделями (модификация, фильтрация, каскадная фильтрация).

СПИСОК ЛИТЕРАТУРЫ

1. Акимов С.В., Меткин Н.П. Автоматизированная система комплексирования радиоэлектронных средств на основе комплексных моделей электронных модулей // Вопросы радиоэлектроники. Серия «Общетехническая», выпуск 1, 2012. С. 191-199.

2. Акимов С.В., Меткин Н.П. Автоматизированная система комплексирования радиоэлектронных средств на основе комплексных моделей электронных модулей // Вопросы радиоэлектроники. Серия «Общетехническая», выпуск 1, 2012. С. 191-199.

3. Акимов С.В., Демидов А.А, Никифоров О.Г. Методология комплексных моделей системных объектов // Вопросы радиоэлектроники. Серия «Системы отображения информации и управления спецтехникой (СОИУ)», выпуск 2, 2012. С. 138-149.

А.Ф. Акмолов
кандидат технических наук;

С.Н. Ефимов
кандидат технических наук, доцент;

Е.А. Викторов
кандидат технических наук;

А.С. Веремчук
Военно-космическая академия имени А.Ф.Можайского

ДЕЦЕНТРАЛИЗОВАННЫЙ АЛГОРИТМ РАСШИРЯЮЩЕГОСЯ ПОИСКА АБОНЕНТОВ МНОГОСПУТНИКОВОЙ СИСТЕМЫ СВЯЗИ

Рассматриваются вопросы организации децентрализованного алгоритма расширяющегося поиска мобильных абонентов разновысотной многоспутниковой системы связи, обеспечивающей глобальное и непрерывное покрытие земной поверхности. Представлены три возможных варианта передачи пакетов запроса поиска абонента в зонах покрытия кластеров космических аппаратов первого и второго уровней.

Одним из перспективных направлений построения орбитальной группировки (ОГ) многоспутниковых систем связи с мобильными абонентами является использование разновысотных спутников-ретрансляторов (СР). Специфика таких разновысотных многоспутниковых систем связи (РМСС) объясняется наличием большого количества космических аппаратов (КА), требующих управления, а также малой продолжительностью сеанса связи через один КА, что влечет за собой неоднократный переход наземных абонентов с одного КА на другой следующий за ним. При этом основным предназначением РМСС является обеспечение непрерывного и глобального обмена всеми видами информации между мобильными абонентами РМСС – как между собой, так и с абонентами других существующих сетей: стационарных и мобильных сетей связи, использующих различные телекоммуникационные технологии.

Создание РМСС с комбинированной структурой построения ОГ КА связи позволяет сочетать преимущества различных типовых вариантов построения ССС и за счёт этого компенсировать их отдельные слабые стороны [1]. При этом одними из основных базовых принципов построения РМСС, схема организации связи в которой представлена на рисунке 1, являются:

баллистическое построение на основе разновысотных спутниковых кластеров первого и второго уровня (в состав космического сегмента РМСС входят 24 КА на низких и восемь КА на средних околополярных круговых орбитах, причем в зоне покрытия КА второго уровня (КА-2) постоянно находятся три КА первого уровня (КА-1));

использование широковещательного режима передачи пакетов в канале управления зоны покрытия каждого СР РМСС, который может быть реализован на основе алгоритма поиска мобильного абонента.

Предлагаемый алгоритм использует широковещательные возможности кластеров КА-1 и КА-2 в пределах своих зон покрытия и учитывает наличие межспутниковых радиолиний между КА-2, обеспечивающих возможность

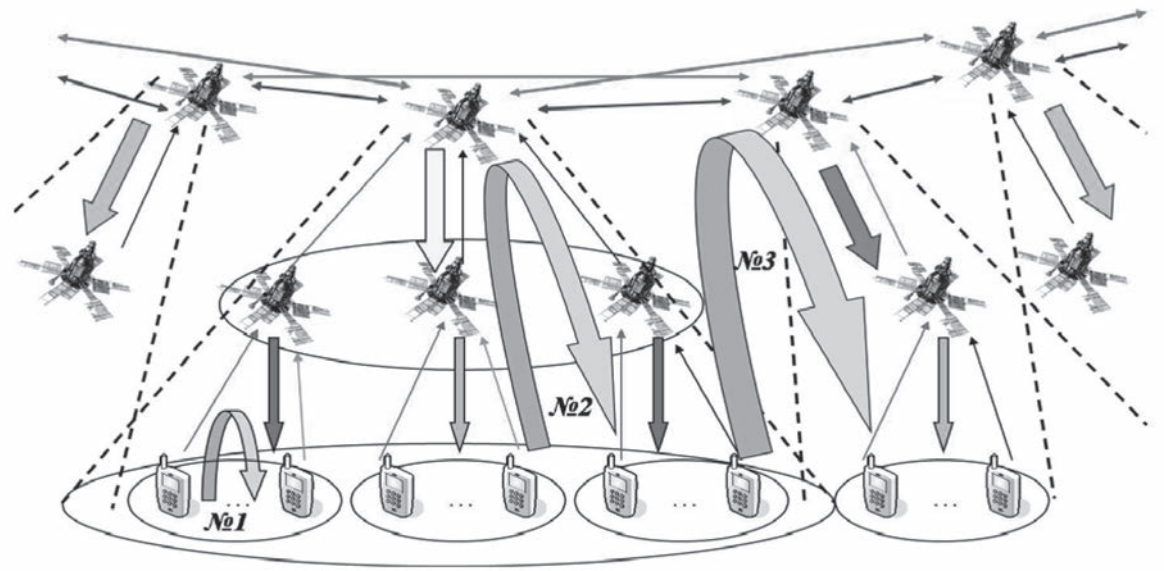


Рис. 1. Схема организации связи в РМСС

трансляции пакетов запроса в остальных кластерах РМСС.

Реализация алгоритма поиска абонента в РМСС в глобальном пространстве осуществляется с использованием канала управления, организуемого на выделенных частотах для передачи пакетов запроса поиска абонента в зонах покрытия кластеров КА-1 и КА-2. Данный канал может быть организован на основе протокола случайного множественного доступа типа P-ALOHA применительно к случаю коммутируемого спутникового моноканала [2], который в отличие от традиционной однолучевой схемы обеспечивает такую же степень использования пропускной способности каналов связи, что и протокол S-ALOHA, но в отличие от последней не требует синхронизации при передаче пакетов во временных окнах.

Последовательность поиска вызываемого абонента в РМСС предполагает реализацию следующего алгоритма:

1. Передача пакета запроса в канале управления на организацию сеанса обмена в пределах зоны покрытия кластера КА-1 с получением автоматической квитанции по обратному каналу связи в пределах пятна покрытия. В случае неудачной попытки, обусловленной искажением пакета, конфликтом пакетов или блокировкой пакета в коммутируемом моноканале кластера КА-1, данный пакет через случайный временной интервал передается повторно. Эта процедура осуществляется до успешной передачи пакета запроса в пятне покрытия кластера КА-1.

2. Если вызываемый абонент находится в зоне покрытия кластера КА-1, то его терминал, осуществляет прием пакета запроса с использованием процедуры селекции по своему адресу. При этом осуществляется автоматическая передача пакета ответа. Передача пакета ответа осуществляется аналогичным образом в канале управления кластера КА-1 в соответствии с протоколом P-ALOHA.

3. При приеме пакета ответа до истечения времени таймера ожидания вызывающий терминал определяет наличие требуемого абонента в зоне кластера КА-1 и формирует запрос на установление сеанса связи требуемого вида (рисунок 1, вариант № 1). Соответствующий вариант связи представлен на рисунке 2.

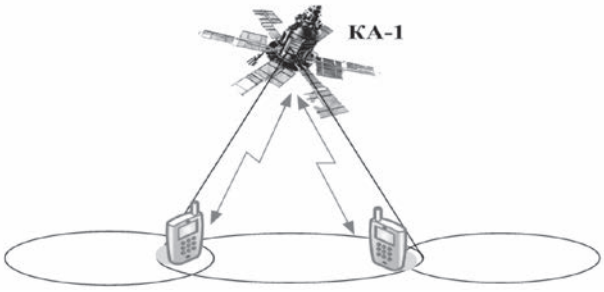


Рис. 2. Вариант связи в режиме прямой ретрансляции сигналов в кластере КА-1 РМСС

4. При отсутствии вызываемого абонента в зоне кластера КА-1 таймер ожидания терминала вызывающего абонента превысит установленный порог. При этом будет сформирован пакет запроса с признаком поиска абонента в кластере КА-2. Данный пакет демодулируется на борту КА-1, фиксируется в списке и поступает в очередь для передачи в канале управления кластера КА-2. Далее реализуется описанный выше алгоритм передачи пакета запроса КА-1 в кластере КА-2.

5. Пакет запроса ретранслируется КА-2 в зоне покрытия. Этот пакет принимают соответствующие КА-1 и ретранслируют его каждый в своей зоне покрытия. При наличии вызываемого абонента в зоне одного из кластеров КА-1 его терминал селектирует пакет запроса по адресу вызываемого абонента и автоматически формирует ответный пакет, который передаются в канале управления кластером КА-1. Данный пакет ответа ретранслируется в канале управления кластером КА-2, который фиксирует факт наличия вызываемого абонента в своей зоне обслуживания (рисунок 1, вариант № 2). Вариант связи в пределах одного кластера КА-2 представлен на рисунке 3.

6. При отсутствии вызываемого абонента в зоне кластера КА-2 его таймер ожидания ответа превысит установленный порог. КА-2, используя межспутниковые радиолинии, транслирует пакет по кольцу из кластеров КА-2 с использованием сети коммутации пакетов управления связью.

7. Пакет запроса ретранслируется в каждом кластере КА-2 в зоне покрытия. Механизм передачи пакета запроса в пределах каждого кластера, реализуется аналогичным образом, как описано выше в пунктах 5 и 6.

С учетом суммарной глобальной зоны покрытия поверхности земли всеми кластерами КА-2 вызываемый абонент будет найден самой

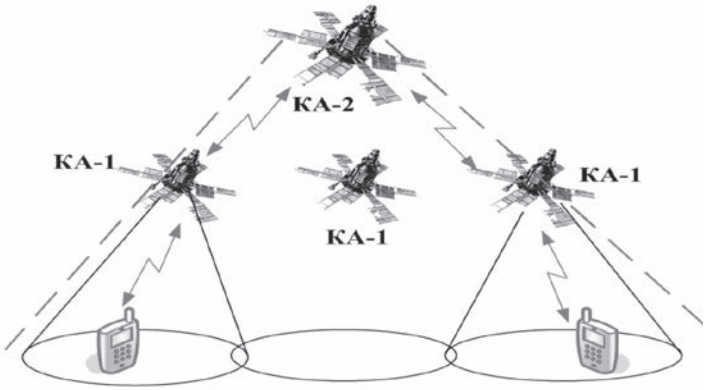


Рис. 3. Вариант связи в пределах одного кластера КА-2 РМСС

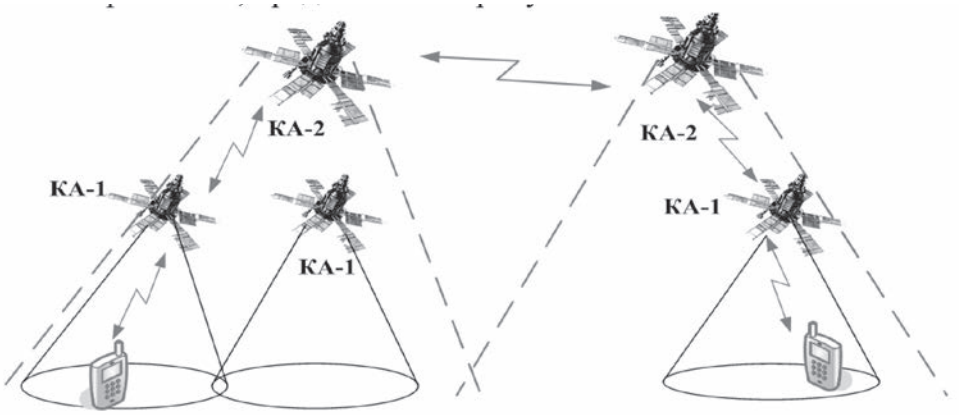


Рис. 4 – Вариант связи в пределах разных кластеров КА-2 РМСС

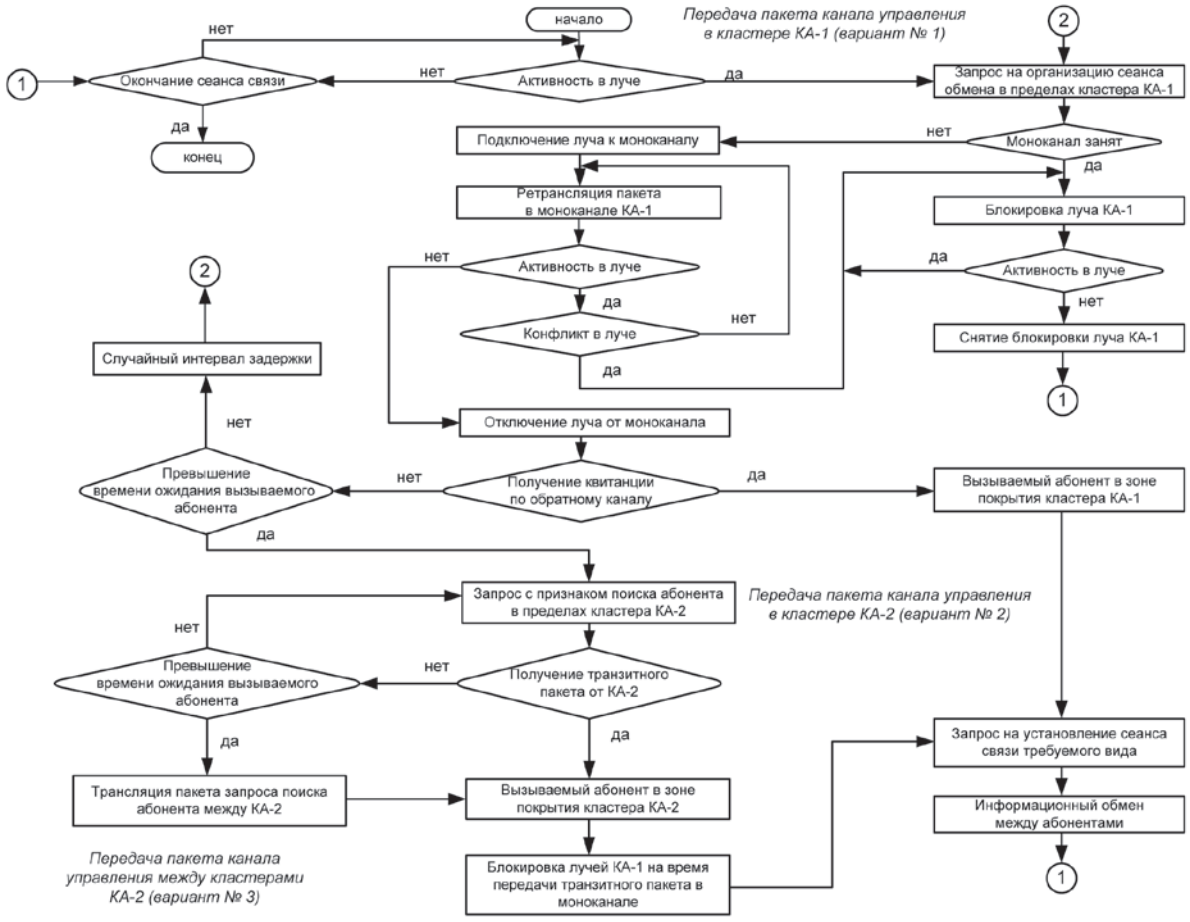


Рис. 5. Алгоритм расширяющегося поиска абонентов

сетью в одном из этих кластеров в зоне покрытия кластера КА-1 (рисунок 1, вариант № 3). Вариант связи для удаленных абонентов, находящихся в зонах покрытия разных кластеров КА-2, представлен на рисунке 4.

Общая реализация децентрализованного алгоритма расширяющегося поиска абонентов РМСС показана на рисунке 5, где представлены все три варианта передачи пакетов запроса поиска абонента в зонах покрытия кластеров КА-1 и КА-2.

Достоинством предлагаемого подхода является его децентрализованность, что с учетом возможного применения РМСС как системы двойного назначения является важным фактором, обеспечивающим успешное функционирование системы связи в особые периоды военно-политической обстановки.

СПИСОК ЛИТЕРАТУРЫ

1. Мальцев Г.Н., Цветков К.Ю., Родионов А.В., Акмолов А.Ф., Ефимов С.Н., Косаревич Д.В., Викторов Е.А. Концепция построения разновысотной многоспутниковой системы связи с мобильными абонентами. // Труды Военно-космической академии имени А.Ф. Можайского. Выпуск № 630. / под ред. М.М. Пенькова. – СПб.: ВКА им. А.Ф. Можайского, 2011. – С. 5-10.

2. Цветков К.Ю., Акмолов А.Ф., Викторов Е.А. Модель канала управления передачей смешанного трафика речи и данных в разновысотной системе спутниковой связи. // Информационно-управляющие системы, 2012. №3. – С. 63-70.

И.Е.Афонин
Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)

В.Е.Федосеев
Военно-космическая академия имени А.Ф.Можайского

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ СИГНАЛА, ОТРАЖЕННОГО ОТ ЦЕЛИ СЛОЖНОЙ ФОРМЫ

Рассматривается задача разработки математической модели радиолокационного сигнала, отраженного от воздушной цели, представляющей собой объект сложной формы. Так модель летательного аппарата представляет собой совокупность «блестящих точек». Произведен анализ результатов моделирования в среде Mathcad отраженного от такой цели сигнала.

Введение

Существует ряд теоретических подходов к анализу отражающей поверхности тел различной формы [1, 2]. Принимая во внимание геометрическую сложность реальных радиолокационных объектов, а также значительное превышение размеров протяженных целей длины волны, наиболее приемлемыми оказываются геометрическая теория дифракции [1] и физическая теория дифракции, а именно метод геометрической теории дифракции Келлера [3] и метод краевых волн Уфимцева [4]. Эти методы сочетают в себе простоту, присущую чисто геометрической оптике, с необходимым условием учета и рассмотрения фаз и длин волн при отражении сигнала от цели.

Здесь наиболее важным является полная взаимная компенсация составляющих поля рассеяния с противоположными фазами, которая приводит к подавлению результирующего излучения от всех частей протяженной цели за исключением участков вблизи геометрических разрывов. Это и позволило ввести понятие центров рассеяния (ЦР), локализованных вблизи точек разрыва непрерывной поверхности тела. В геометрической теории дифракции в связи с этим вводится понятие дифрагированных лучей при касании и встрече падающих лучей с центрами рассеяния, а именно, с кромками, углами или вершинами граничных поверхностей. При зеркальном отражении этими лучами обычно пренебрегают, однако в отсутствие его, последние становятся преобладающими.

Амплитуда и фаза каждого луча меняется от точки к точке и зависит от формы, размеров разрывов, определяющих ход луча. Таким образом, центры рассеяния реальной цели своим возникновением в большей степени обязаны суперпозиции дифрагированных лучей в местах разрывов, чем плоским поверхностям с зеркальным отражением. Иными словами центр рассеяния – это не какая-либо геометрическая точка протяженной цели, а некоторая совокупность отражающих элементов. Сигнал, отраженный от такого центра рассеяния характеризуется амплитудой, пропорциональной эффективной поверхности рассеяния (ЭПР) этого центра и начальной фазой. Однако на практике начальная фаза считается равной нулю, а ее влияние учитывается при локализации центров рассеяния на поверхности протяженной цели, то есть включается фазовый множитель, пропорциональный расстоянию,

выраженному в длинах волн от центра рассеяния до радиолокационной станции (РЛС).

В общем случае центры рассеяния перемещаются относительно геометрического центра протяженной цели, когда меняется угол обзора, однако, в пределах небольших секторов наблюдения можно считать их в среднем практически неподвижными и характеризовать координатами в связанной системе координат протяженной цели.

Поле рассеяния всей протяженной цели представляется, таким образом, векторной суммой полей отдельных центров рассеяния. При этом сигналы от большинства центров рассеяния в характерных условиях радиолокационного наблюдения можно считать статистически независимыми.

Исторически, экспериментальные исследования с целью отыскания центров рассеяния начали проводиться с позиций оптики. Поэтому центры рассеяния были названы «блестящими» точками (БТ). Оптические методы определения местоположения центров рассеяния с успехом применяются и в настоящее время [1, 2]. Ряд методов визуализации центров рассеяния связан с применением когерентных источников света, а также с использованием широкополосных сигналов, обеспечивающих высокую разрешающую способность, как по дальности, так и по угловым координатам. Оригинальный метод визуализации центров рассеяния, использующий спектральный анализ предложен в [5].

Модель отраженного сигнала

Модель полезного радиолокационного сигнала получается путем вычисления сигналов, отраженных только от наиболее «ярких» точек ЭПР цели, которые могут быть представлены в виде разбросанных точечных рассеивателей. Местоположение и отражательные способности рассеивателей зависят от формы, размеров и физических свойств цели. Местоположение рассеивателей выражается в фиксированных координатах точек в системе координат корпуса цели. Кроме того, радиолокационный сигнал рассеивателей является чувствительным к ракурсу цели, так как некоторые из поверхностей могут затенять отраженный сигнал от других поверхностей.

На рис. 1 представлена модель, состоящая из 13 «блестящих» точек и разработанная применительно к самолету-истребителю, полученная на основе сочетания теоретического анализа с проведением аналоговых измерений высокого разрешения на масштабных моделях целей. Области ракурсов, при которых каждый из рассеивателей добавляет свою долю энергии в сигнал, помечены круговыми сегментами и дугами (полный круг означает всенаправленное рассеяние). Из рис. 1 видно, что типовые цели обладают конечным числом достаточно четко локализованных на поверхности цели центров рассеяния. Это позволяет выделить данную математическую модель из числа чисто статистических моделей, в которых делается предположение о большом количестве произвольно расположенных многократно переизлучающих центров рассеяния.

Таким образом, для описания сигнала, отраженного от цели сложной формы, необходимо выполнить следующую последовательность действий. Во-первых, необходимо

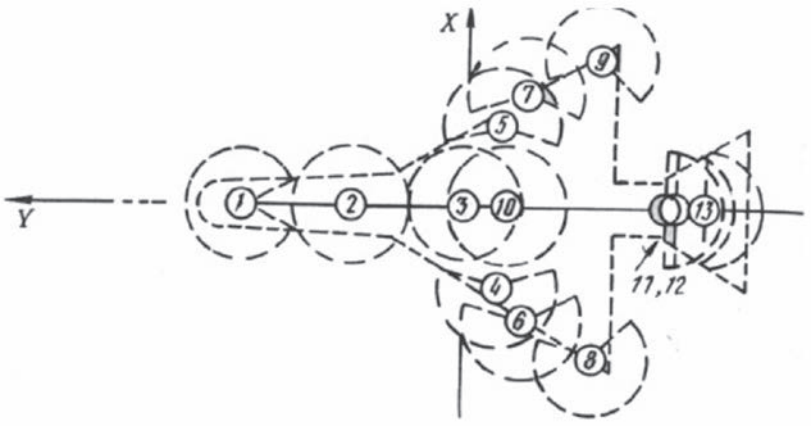


Рис. 1. Модель самолета-истребителя

задать вектор координат «блестящих» точек r_i в связанной с целью системе координат (СК), вектор нормали ЭПР каждой БТ n_i и углы, ограничивающие наблюдение БТ A_i:

$$\begin{aligned} r_i &= (x_i, y_i, z_i) \\ n_i &= (x_{ni}, y_{ni}, z_{ni}), \\ \mathrm{A}_i &= (\alpha_1 \ldots \alpha_N) \end{aligned} \qquad (1)$$

где i – номер «блестящей» точки; N – количество «блестящих» точек.

Кроме того, необходимо задать радиус-вектор направления на воздушную цель (ВЦ) *r0* и углы ее пространственного положения относительно точки наблюдения (бортовой РЛС (БРЛС) своего истребителя) – углы крена, рысканья и тангажа. И затем следует перейти от связанной с целью СК к связанной с БРЛС своего самолета СК, используя матрицу преобразования координат F [6]:

$$F(a,b,c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(a) & \sin(a) \\ 0 & -\sin(a) & \cos(a) \end{pmatrix} \times \begin{pmatrix} -\sin(c) & \cos(c) & 0 \\ \cos(c) & \sin(c) & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \cos(b) & 0 & -\sin(b) \\ 0 & 1 & 0 \\ \sin(b) & 0 & \cos(b) \end{pmatrix}, \qquad (2)$$

где a, b, с – углы крена, рысканья и тангажа ВЦ соответственно.

Для описания результирующего сигнала необходимо рассчитать параметры наблюдения БТ. Дальность до каждой из БТ рассчитывается по следующей формуле:

$$D_i = \sqrt{X_i \cdot X_i^T}, \qquad (3)$$

где $X_i = r0 + r_i \cdot F$ – вектор наблюдения i – ой «блестящей» точки; X_i^T – транспонированный вектор наблюдения i – ой БТ.

В зависимости от ракурса наблюдения ВЦ не все «блестящие» точки будут отражать зондирующий сигнал. Для того чтобы это учесть, необходимо рассчитать угол между радиус-вектором БТ и вектором нормали ЭПР этой точки:

$$\beta_i = \arccos\left(\frac{-X_i \cdot Y_i^T}{\sqrt{X_i \cdot X_i^T} \cdot \sqrt{Y_i \cdot Y_i^T}} \right), \qquad (4)$$

где $Y_i = n_i \cdot F$ – вектор нормали ЭПР i – ой «блестящей» точки; Y_i^T – транспонированный вектор нормали ЭПР i – ой БТ.

А также рассчитать вектор ЭПР каждой «блестящей» точки с учетом угла наблюдения ВЦ:

$$E_i = \sqrt{Y_i \cdot Y_i^T}. \qquad (5)$$

С учетом того, что не все «блестящие» точки отражают зондирующий сигнал, вектор ЭПР воздушной цели примет следующий вид:

$$E_i' = E_i^* \cdot E_i, \qquad (6)$$

где $E_i^* = \begin{cases} 1, \beta_i < a_i \\ 0, \beta_i > a_i \end{cases}$ – вектор «видимости» БТ.

Таким образом, результирующий сигнал, отраженный от ВЦ, представляет собой результат интерференции сигналов, отраженных от всех БТ, составляющих объект сложной формы, коим и является любая ВЦ:

$$S_\Sigma = \sum_{i=1}^{N} E_i' \cdot K_П \cdot S_{изл}(t - t_{зад\ i}), \qquad (7)$$

где $K_П$ – коэффициент потерь в среде распространения; $S_{изл}(t)$ – зондирующий радиолокационный сигнал; $t_{зад\ i} = 2D_i / C$ – время задержки сигнала от i – ой БТ; N – количество «блестящих» точек.

На рис. 2 представлены результаты моделирования процесса отражения радиолокационного импульсного сигнала от одиночной цели представленной совокупностью блестящих точек, причем показаны только сигналы, отраженные от доминирующей блестящей точки, двух второстепенных и результирующий сигнал.

Анализ полученных графиков дает возможность сделать следующие выводы:

1) на характер отражения от сложной цели в большей степени оказывают влияние доминирующие блестящие точки, т.е. имеющие большую ЭПР (например, фазированная антенная решетка БРЛС самолета противника);

2) суммарный сигнал имеет большее амплитудное значение, чем сигнал, отраженный от любой из блестящих точек;

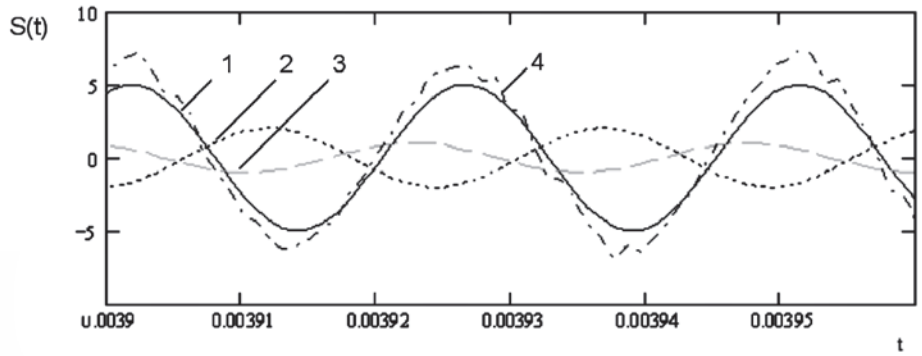


Рис. 2. Сигнал, отраженный от доминирующей БТ *(1); сигналы, отраженные от двух второстепенных* БТ *(2, 3); результирующий сигнал, о*траженный от ВЦ, представленной совокупностью БТ *(4)*.

3) смещение блестящей точки относительно мгновенного центра отражения имеет вид аддитивного шума на суммарном сигнале, причем уровень шума составляет не более 10 процентов от амплитуды результирующего сигнала.

Заключение

Таким образом, допустимо представление одиночной сложной цели ее мгновенным центром отражения, при этом отраженный от цели сигнал необходимо представить аддитивной смесью полезной составляющей и шума.

Использование данных результатов возможно только при создании математической модели неподвижных целей. Для реальных воздушных целей необходимо также учитывать траекторные нестабильности самолета при полете в турбулентной атмосфере, а также упругие деформации всего корпуса летательного аппарата, которые будут приводить к смещениям блестящих точек относительно друг друга.

Учет этих процессов принято осуществлять в виде нормального шума координат (угловых или линейных, в зависимости от алгоритма обработки).

Среднеквадратическое отклонение разности расстояний отдельных блестящих точек от мгновенного центра отражения определяется суммой:

$$\sigma_{\Delta}^2 = \sigma_{K}^2 + \sigma_{Tp}^2 + \sigma_{Ш}^2, \qquad (8)$$

где $\sigma^2_{К}$ – СКО разности расстояний, обусловленное упругими деформациями корпуса летательного аппарата; $\sigma^2_{Тр}$ – СКО разности расстояний, обусловленное траекторными нестабильностями самолета при полете в турбулентной атмосфере; $\sigma^2_{Ш}$ – СКО разности расстояний, обусловленное шумовой составляющей.

По результатам моделирования и анализа известных источников определено, что величина σ^2_{Δ} не превышает 10 процентов от длины волны зондирующего сигнала и, следовательно, не оказывает влияния на полученные выводы.

СПИСОК ЛИТЕРАТУРЫ

1. Справочник по радиолокации в 4-х томах: Пер. с англ. / Под ред. М. Сколника. – М.: Сов. Радио, 1976-1979.

2. Авиационные радиолокационные комплексы и системы: учебник для слушателей и курсантов ВУЗов ВВС / П.И. Дудник, Г.С. Кондратенко, Б.Г. Татарский, А.Р. Ильчук, А.А. Герасимов. Под ред. П.И. Дудника. – М.: Изд. ВВИА им. проф. Н.Е. Жуковского, 2006 – 1112 с.

3. Keller J.B. Geometrical theory of diffraction. – J. Opt. Soc. Am., 1962, v.52, № 2. – pp. 116-130.

4. Уфимцев П.Я. Метод краевых волн в физической теории дифракции. – М.: Сов. радио, 1962. – 244 с.

5. Граф Г. Система для одновременного отображения рассеивающих центров вращающихся радиолокационных целей. – М, ВЦП, перевод № Д-28569, 1982.

6. ГОСТ 20058-80. Динамика летательных аппаратов в атмосфере. Термины, определения и обозначения. – Взамен ГОСТ 20058-74; введ. 1981.07.01. – М.: Государственный комитет СССР по стандартам, 1981. – 54 с.

В.И. Мирошников
доктор технических наук; профессор

П.А. Будко
доктор технических наук; профессор

Н.П. Будко
А.М. Жебрун
С.Л. Чибышев
ОАО «Информационные телекоммуникационные технологии» г. Санкт-Петербург

РЕАЛИЗАЦИЯ СПОСОБА ГИБРИДНОЙ КОММУТАЦИИ ЦИФРОВЫХ КАНАЛОВ СВЯЗИ НА РАСПРЕДЕЛЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

Предложен способ гибридной коммутации (ГК) цифровых каналов связи (ЦКС), позволяющий снизить временные задержки в передаче сообщений при допустимом уровне отказов в обслуживании за счет выбора режима коммутации, учитывающем уровень загрузки буферов памяти и реализации режима обучения и настройки устройства с широким классом видов трафика, используемых в современных технологиях. Устройство, реализующее предложенный способ, работает в трех режимах: в режиме обучения, в режиме коммутации пакетов (КП) и в режиме коммутации каналов (КК).

Ключевые слова: коммутация пакетов, коммутация каналов, гибридная коммутация, цифровые каналы связи, распределенная телекоммуникационная система, модуль идентификации, генератор сетевого трафика.

Введение

Известен способ адаптивной коммутации [1], обеспечивающий организацию на сети соединений в режиме КК с одновременной передачей сообщений в режиме КП. При этом осуществляется динамическое перераспределение пропускной способности трактов сети между потоками сообщений, передаваемых в режимах КК и КП. Недостаток данного способа коммутации состоит в высокой вероятности отказа в обслуживании сообщений, поскольку выбор того или иного способа коммутации осуществляется в режиме с отказами при отсутствии свободных ячеек памяти. При этом сообщения разбиваются на блоки и записываются в общее поле памяти независимо от способа коммутации, а различные блоки одного и того же сообщения могут передаваться с использованием различных методов коммутации, что приводит к нарушению масштаба времени всего сообщения.

Наиболее близким по технической сущности к заявленному способу, является способ ГК [2], основанный на интеграции коммутационного оборудования, необходимого для реализации каждого метода коммутации: КК и КП. Он заключается в том, что предварительно устанавливают пороговое значение длины $L_{пор}$ сообщения, сравнивают длину L принимаемого сообщения с $L_{пор}$ и по результатам сравнения принимают решение о выборе режима коммутации. При этом если $L>L_{пор}$, то выбирают режим КК. В противном случае, при $L<L_{пор}$ выбирают режим КП.

Недостатками данного способа коммутации являются относительно большие временные

задержки передачи сообщений, вызывающие частые блокировки и отказы в обслуживании при передаче длинных сообщений в режиме КП, а также нарушение реального масштаба времени передачи сообщений. Кроме того, данный способ также не предусматривает предварительного обучения системы при выборе режимов коммутации для разнородного трафика, что опять же приводит к росту среднего времени задержки сообщений из-за времени, отводимого на анализ.

Известно устройство гибридного коммутатора сообщений, состоящее из блока ввода-вывода, блока управления, запоминающего блока и коммутатора [3]. Недостатком данного устройства является относительно большое время задержки в передаче сообщений, вызванное отсутствием возможности автоматического управления режимами коммутации в зависимости от величины трафика и использованием отдельных трактов оборудования для осуществления режимов КК и КП. Также в нем отсутствует режим обучения системы на различные типы нагрузки (трафика), что приводит к увеличению времени задержки при прохождении сообщений через устройство.

Наиболее близким к заявленному устройству ГК ЦКС является устройство, описанное в работе [4]. Структурная схема данного центра коммутации содержит модули доступа, промежуточной памяти, идентификации, сопряжения с каналами связи и управления. Его недостатками являются относительно большие временные задержки в обслуживании неравномерного трафика, на нагрузках, близких к критическим, а также неконтролируемый рост величины вероятности отказа в обслуживании сообщения при изменяющихся видах трафика и интенсивности его поступления.

Также известно устройство принятия решения [5], реализующим условие нахождения оптимального значения порогов, обеспечивающих минимальную ошибку идентификации состояния системы. Недостатком устройства является относительно высокая вероятность отказа в обслуживании, вызванная тем, что назначение порогов осуществляется без учета общего состояния телекоммуникационной системы и величины загрузки буферных устройств узлов коммутации (УК) каналов связи, вызывающее блокировку устройства на загруженной сети, при передаче коротких сообщений методом КП.

Наиболее близким по технической сущности к заявленному устройству является идентификатор блока принятия решения [6]. Его недостатком является его относительно низкая производительность, вызванная ростом времени задержки сообщений из-за необходимости производить измерение, преобразование и обработку большого числа параметров, что нередко связано с отключением системы и ее простаиванием.

Техническим результатом, достигаемым с помощью предложенного способа и устройства ГК ЦКС, является снижение временных задержек в передаче сообщений при допустимом уровне отказов в обслуживании за счет выбора режима коммутации, учитывающем уровень загрузки буферов памяти и реализации режима обучения и настройки устройства с широким классом видов трафика, используемого в современных технологиях, а также повышения производительности модуля идентификации параметров сообщений.

1. Сущность способа гибридной коммутации ЦКС

В заявленном способе ГК ЦКС технический результат достигается тем, что предварительно устанавливают пороговое значение длины $L_{\text{пор}}$ сообщения, сравнивают длину L принимаемого сообщения с $L_{\text{пор}}$ и по результатам сравнения принимают решение о выборе режима коммутации. При этом для предварительной установки значения $L_{\text{пор}}$ генерируют сетевые трафики с отличающимися длинами сообщений L и интенсивностью λ их поступления для N типов сетей связи и M видов трафика, по данным L и λ и заданной интенсивности обслуживания сообщений μ вычисляют коэффициент загрузки ρ_m^n для каждого m-го вида трафика и n-го типа сети связи, где $m = 1, 2, ..., M$; $n = 1, 2, ..., N$, удовлетворяющий требованию выполнения заданной вероятности отказа $P_{\text{отк}}^{\text{доп}}$ в обслуживании, и по полученным результатам вычислений ρ_m^n рассчитывают соответствующие ему критические длины $L_{\text{кр}}^{mn}$ сообщения и формируют критические значения уровней порога $U_{\text{пор}}^{mn}$ переключения режима коммутации, причем массив сформированных значений $U_{\text{пор}}^{mn}$ запоминают, принимают от абонентов сообщения на

обслуживание, измеряют их длины L^{mn}, идентифицируют для каждого сообщения его вид трафика m и тип сети n, запоминают принятое сообщение, преобразуют измеренную длину сообщения L^{mn} в значение уровня напряжения U^{mn}, и сравнивают его с соответствующим ему предварительно вычисленным пороговым значением $U^{mn}_{\text{пор}}$, при $U^{mn} > U^{mn}_{\text{пор}}$ выбирают режим «КК» и устанавливают физическое соединение для передачи сообщения получателю, в противном случае сообщение L^{mn} разбивают на пакеты, каждый из которых снабжают адресной частью в их заголовках и выбирают режим «КП» для дальнейшей передачи получателю по виртуальному соединению в режиме дейтограмм.

Благодаря перечисленной новой совокупности существенных признаков способа ГК ЦКС и введенной последовательности действий обеспечивается предварительное обучение системы и более корректная оценка параметров поступающих на обслуживание сообщений, на основе чего обосновывается выбор режима коммутации и достигается поставленная цель по своевременной доставке сообщений с допустимым значением вероятности отказа. При этом величина $L^{mn}_{\text{кр}}$, а следовательно и $L_{\text{пор}}$ может быть установлена как путём анализа трафика, поступающего в устройство ГК ЦКС, так и за счет обучения системы заблаговременно, путем моделирования различных видов сетевого трафика при проектировании устройства и сети.

2. Состав устройства гибридной коммутации ЦКС

Структурная схема предложенного устройства ГК ЦКС приведена на рис. 1. В нем технический результат достигается тем, что в известное из [4] устройство ГК ЦКС, дополнительно введен генератор сетевого трафика, информационный выход которого подключен к первому информационному входу модуля промежуточной памяти, к второму информационному входу которого подключен информационный выход модуля доступа, управляющие выходы «генератор сетевого трафика», «величина задержки» и «включение» модуля управления подключены к соответствующим управляющим входам генератора сетевого трафика, а управляющие выходы «величина порога» и «установка 0» к соответствующим управляющим входам модуля идентификации, управляющий вход «длина сообщения» и информационный вход которого соединен соответственно с управляющим выходом «длина сообщения» и информационным выходом модуля промежуточной памяти, а информационные выходы «КК» и «КП» подключены к информационным входам

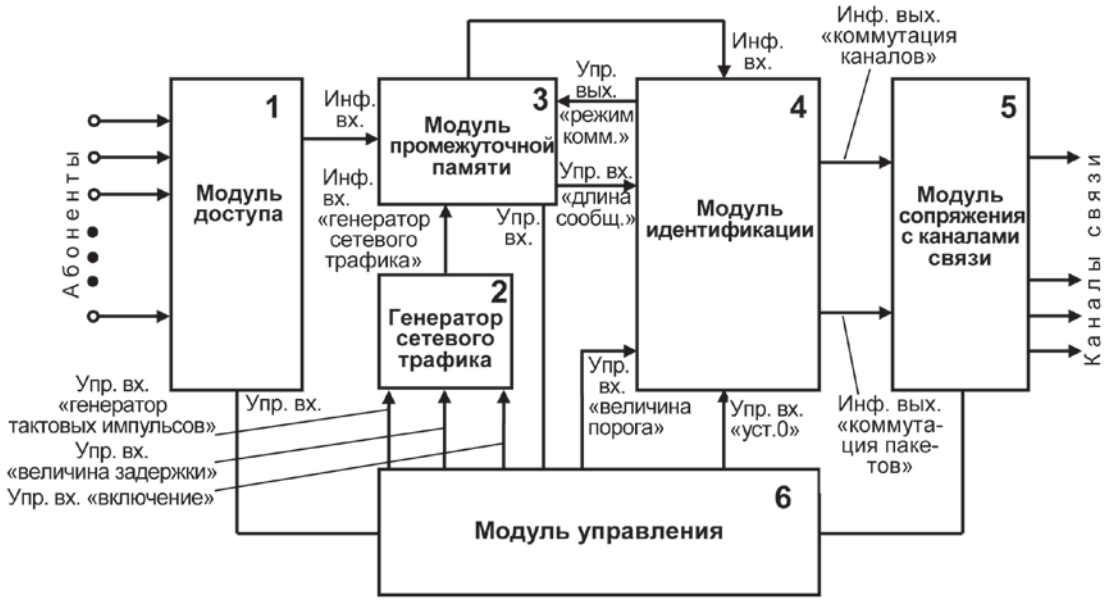


Рис. 1

соответственно «КК» и «КП» модуля сопряжения с каналами связи.

При этом модуль доступа 1 (см рис. 1) осуществляет сопряжение входящих линий абонентов с устройством; ГСТ 2 формирует в режиме обучения для основных типов сетей различные виды современного сетевого трафика (данные, звук, видео и др.); модуль промежуточной памяти 3 выделяет объемы буферного пространства памяти для хранения сообщений и пакетов, а также производит их обработку; модуль идентификации 4 формирует решение на осуществление режима КК или режима КП с учетом длины передаваемого сообщения, объема загрузки буферов памяти и текущего состояния каналов; модуль сопряжения с каналами связи 5 осуществляет сопряжение устройства с каналами связи для организации виртуального канала или дейтограммной рассылки пакетов информации в сеть связи; модуль управления 6 служит для управления и контроля соединения исходящих и входящих линий, выполняет функции управления устройством, а также функции по вычислениям, логике и другие, связанные с учетом и контролем текущего его состояния. Такая структура устройства ГК ЦКС позволяет осуществлять управление его работой обычным процессором.

Благодаря перечисленной новой совокупности существенных признаков устройства ГК ЦКС обеспечивается снижение вероятности отказа и среднего времени задержки сообщений при обслуживании устройством неравномерного трафика за счет предварительного обучения системы и учета её состояния при выборе режима коммутации, чем и достигается поставленная цель. Причем уведомление устройства ГК ЦКС о длине подлежащего передаче сообщения в фазе установления соединения позволяет предотвратить коллизии в сети, связанные с переполнением памяти узлов УК, повысить эффективность использования каналов связи за счет передачи очень длинных сообщений в реальном масштабе времени по физическому соединению и уменьшить общее число сообщений, получающих отказ в обслуживании по причине отсутствия свободных буферов памяти. При этом хранение длинных сообщений возложено на вызывающего абонента, а время хранения не должно превышать некоторой величины τ в соответствии с рекомендацией Q.543 сектора JTU – T (CCITT).

Функциональная схема предложенного генератора сетевого трафика (ГСТ) представлена на рис. 2. Геометрическая интерпретация процесса формирования сетевого трафика показана на рис. 3. Предложенная схемная

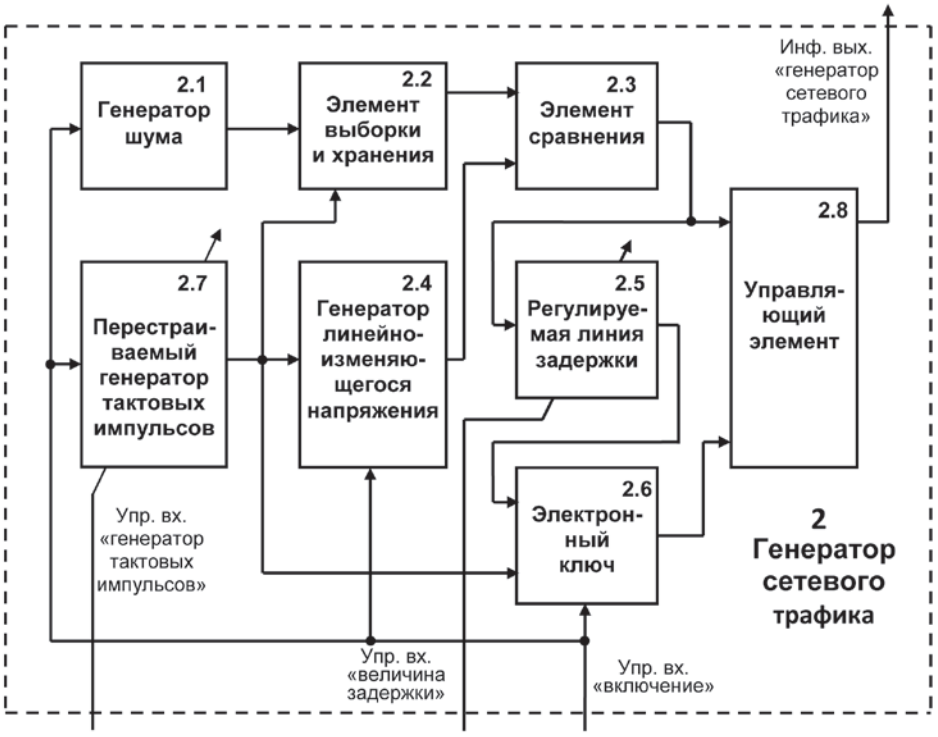


Рис. 2

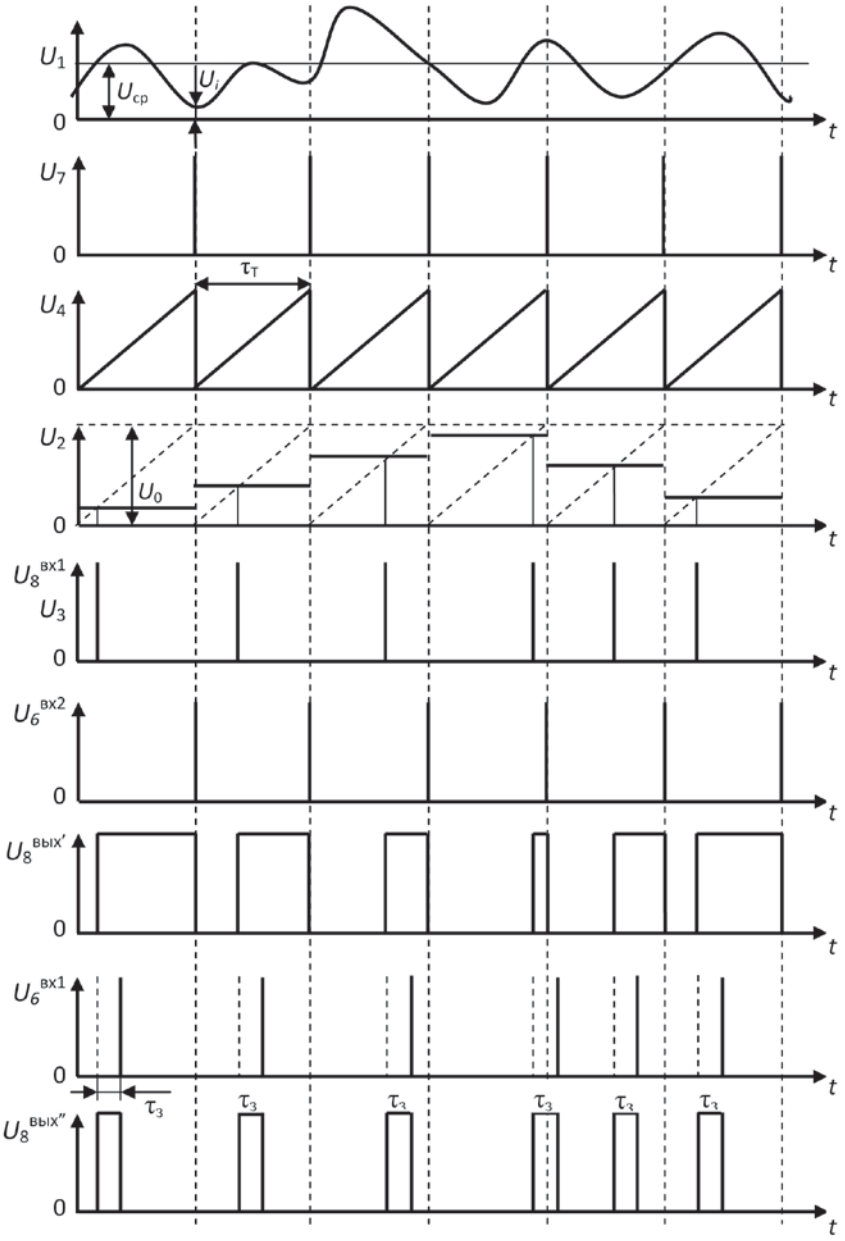


Рис. 3

реализация ГСТ обеспечивается более широкий класс генерируемых случайных импульсных последовательностей, позволяющий моделировать основные виды трафика современных телекоммуникационных систем (ТКС) за счет использования в своем составе перестраиваемого генератора тактовых импульсов, регулируемой линии задержки и настраиваемого на случайные последовательности с основными законами распределения генератора шума. Причем, обеспечивая режим обучения, ГСТ позволяет прогнозировать нагрузку ТКС без привлечения пользователей (абонентов).

Функциональная схема предложенного модуля идентификации представлена на рис. 4. Решение о выборе режима коммутации осуществляется непосредственно в модуле на основе сравнения измеренной длины поступившего на коммутацию сообщения с расчетной величиной порога для изменения режимов коммутации, а само пороговое значение длины сообщения устанавливается с учетом коэффициента загрузки устройства или по результатам его обучения (с использованием ГСТ), что обеспечивает снижение среднего времени задержки сообщений за счет сокра-

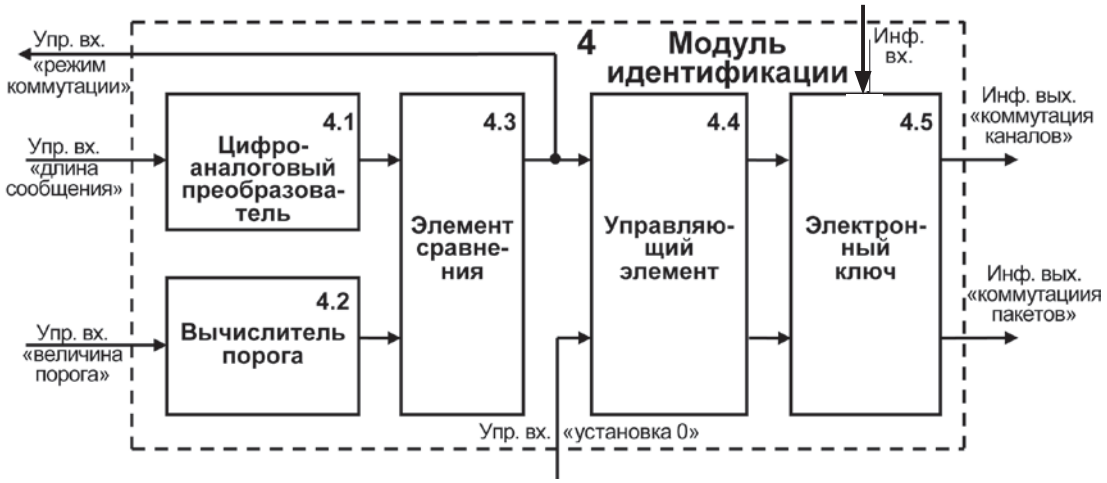


Рис. 4

щения времени анализа при выборе режима коммутации, чем и достигается поставленная цель.

3. Реализация этапов способа ГК ЦКС

Первым этапом способа является обучение системы, при котором устанавливают пороговые значения $U_{\text{пор}}^{mn}$, соответствующие пороговым длинам сообщений $L_{\text{пор}}$ для различных видов трафика m и типов сетей n. Для этого генерируют импульсные последовательности с различными длинами сообщений L и интенсивностью λ их поступления, моделируя основные виды трафика m при различных дисциплинах обслуживания (протоколах) сетевых технологий n. По данным L и λ и заданной интенсивности обслуживания сообщений μ вычисляют коэффициент загрузки ρ_m^n для каждого m-го вида трафика и n-го типа сети связи, удовлетворяющий требованию выполнения заданной вероятности отказа $P_{\text{отк}}^{\text{доп}}$ в обслуживании, и по полученным результатам вычислений ρ_m^n рассчитывают соответствующие ему критические длины $L_{\text{кр}}^{mn}$ сообщения и формируют критические значения уровней порога $U_{\text{пор}}^{mn}$ переключения режима коммутации. Рассчитанные значения $U_{\text{пор}}^{mn}$ для различных m и n запоминают в виде массива данных.

Вторым этапом способа является выбор режима коммутации сообщений. При этом в фазе установления соединения с вызывающим абонентом принимают сообщение на обслуживание, измеряют его длину L, идентифицируют вид трафика m и тип сети n по адресу назначения и запоминают длину L^{mn} сообщения, соответствующего виду трафика и типу сети. Далее преобразуют измеренную длину сообщения L^{mn} в значение уровня напряжения U^{mn}, и сравнивают его с соответствующим ему предварительно вычисленным на этапе обучения пороговым значением $U_{\text{пор}}^{mn}$. при $U^{mn} > U_{\text{пор}}^{mn}$ выбирают режим «КК» и устанавливают физическое соединение для передачи сообщения получателю, в противном случае, при $U^{mn} < U_{\text{пор}}^{mn}$, сообщение L^{mn} разбивают на пакеты, каждый из которых снабжают адресной частью в их заголовках и выбирают режим «КП» для дальнейшей передачи получателю по виртуальному соединению в режиме дейтограмм.

Процедура формирования информационных пакетов из сообщения подробно описана, например, в [7]

4. Расчет критической длины сообщения для формирования критические значения уровней порога переключения режима коммутации

Выбор режима коммутации происходит путем сравнения величины длины сообщения L^{mn} с пороговым значением $L_{\text{пор}}$, которое может быть рассчитано по формуле $L_{\text{пор}} = L_{\text{кр}}[1 - \nu_з(t) / \nu] + \beta[\partial \nu_з(t) / \partial t]$, где ν – общий объем памяти, занятый сообщением; $\nu_з(t)$ – текущее значение занятого объема памяти; $\partial \nu_з(t) / \partial t$ – производная по времени от занятого объема памяти; β – коэффициент пропорциональности. Данное значение $L_{\text{пор}}$ преобразуют в значение уровня напряжения

$U_{\text{пор}}^{mn}$ и сравнивают его с соответствующим ему предварительно вычисленным пороговым значением $U_{\text{пор}}^{mn}$. При этом общее число пакетов фиксированной длины ($L_{\text{пак}}$), которые могут быть сформированы из сообщения длиной L, определяется как

$$B=\frac{L}{L_{\text{пак}}}\le \nu, \qquad (1)$$

т. е. не должно превышать объем буферной памяти, так как, в противном случае, сообщение получает отказ, или должно разбиваться на блоки.

Таким образом, критическую длину сообщения можно определить из соотношения (1) как $L_{\text{кр}}= \nu L_{\text{пак}}$. Для одноканального устройства, как системы массового обслуживания с ожиданием, вероятность получения сообщением отказа в обслуживании в соответствие с [8] равна

$$P_{\text{отк}}=\frac{\rho^{\nu+1}(1-\rho)}{1-\rho^{\nu+2}}\le P_{\text{отк}}^{\text{доп}}, \qquad (2)$$

где $\rho=\lambda/\mu$ – коэффициент загрузки устройства; λ – интенсивность поступления сообщений; μ – интенсивность обслуживания; $P_{\text{отк}}^{\text{доп}}$ – допустимое значение вероятности отказа в обслуживании. Решая уравнение (2) относительно ν для предельного значения $P_{\text{отк}}^{\text{доп}}$, получим $\nu=\frac{1}{\ln\rho}\cdot\ln\frac{P_{\text{отк}}^{\text{доп}}}{\left[1-\rho(1-P_{\text{отк}}^{\text{доп}})\right]}$. Критическая длина сообщения с учетом загрузки устройства и допустимого значения вероятности отказа равна:

$$L_{\text{кр}}=\frac{L_{\text{пак}}}{\ln\rho}\cdot\ln\frac{P_{\text{отк}}^{\text{доп}}}{\left[1-\rho(1-P_{\text{отк}}^{\text{доп}})\right]}. \qquad (3)$$

Условие выбора критической длины сообщения (3) не учитывает структуру сети, к которому принадлежит устройство ГК и такие ее показатели, как время задержки сообщения в сети, общий трафик сети, стоимость сети и другие показатели, являющиеся исходными данными при проектировании сети.

5. Этапы работы устройства гибридной коммутации ЦКС

Предложенное устройство ГК ЦКС работает в трех режимах: в режиме КП; в режиме КК; в режиме обучения.

При реализации *режима КП*, в фазе установления соединения абонентов с устройством между ними происходит диалог, в ходе которого выясняют длину сообщения L и адрес вызываемого абонента. В конце этой фазы выбирается метод коммутации посредством анализа длины сообщения и занятости буферной памяти модуля промежуточной памяти 3. Если длина сообщения не превышает критическую величину, т.е. $L<L_{\text{кр}}$, а все буферы канала, установленного для передачи сообщения адресату, свободны, то по команде с выхода элемента сравнения 4.3 модуля идентификации 4 (см. рис. 4) через управляющий выход «режим коммутации» сообщение разбивают на пакеты в модуле промежуточной памяти 3 и передают на информационный вход модуля идентификации и на информационный вход первого элемента И1 (см. рис. 6) электронного ключа 4.5, управляющий вход которого в исходном состоянии находится под высоким потенциалом, снимаемым с инверсного выхода управляющего элемента (триггера) 4.4 модуля идентификации, и далее транслируют через модуль сопряжения с каналами связи 5 в дейтограммном режиме абоненту-получателю. Модуль управления 6 обеспечивает модуль промежуточной памяти 3 информацией, необходимой для формирования заголовков пакетов, размещает пакеты в выделенной части буфера памяти, пересылает адрес буфера в адресный регистр модуля 5, обрабатывающего выходящие линии. В аналогичных устройствах ГК транзитных УК и узла назначения также выделяется необходимый объем буферной памяти для каждого виртуального соединения под пересылку или сборку сообщения соответственно.

Реализация *режима КК* заключается в следующем. Если длина сообщения превышает пороговую величину, т.е. $L>L_{\text{кр}}$, то независимо от состояния буферной памяти и величины трафика принимается решение об установлении физического соединения и передаче сообщения в режиме КК (см. рис. 7). В этом случае сообщение может быть передано непосредственно в модуль сопряжения с каналами связи 5 путем подачи соответствующего уровня потенциала на второй вход элемента сравнения 4.3 модуля идентификации (см. рис. 4). Функции модуля управления 6 в этом случае сводятся к анализу адресной части сообщения и установлению физического соединения. Если часть буферной

памяти занята и(или) недостаточна для размещения всего сообщения, то принятие решения об использовании метода КК принимается в блоке идентификации 4 в соответствии с выражением $L>k\cdot L_{кр}+b$ путем подачи соответствующих потенциалов на первый и второй входы схемы сравнения 4.3 модуля идентификации.

Режим обучения может включаться заблаговременно на этапе проведения пусконаладочных работ, или в ходе эксплуатации при отсутствии реального трафика (также при проведении специальных тренировок). Модуль управления 6 устройства ГК ЦКС постоянно контролирует по линиям управления загрузку буферов модуля промежуточной памяти 3 и состояния каналов связи в модуле 5. При построении устройства ГК ЦКС, а также в отсутствии реального трафика для передачи сообщений модуль управления через управляющий выход «включение» включает режим обучения, при котором ГСТ 2 моделируются различные режимы нагрузки системы, необходимые в процессе обучения и настройки устройства. При этом для основных типов сетей (ATM, SDH и др.) формируют последовательности сообщений, характерные различным видам сетевого трафика (данные, звук, видео и др.). В результате проведения методом статистических испытаний набирают статистику для различных видов трафика m и типов сетей n в определении критической длины сообщения $U_{пор}^{mn}$, влияющую на величины соответствующих ей порогов напряжения $U_{пор}^{mn}$ для переключения режимов коммутации. Физический смысл критической длины сообщения заключается в выборе такой длины сообщения, которая при заданном виде трафика не вызывает роста таких показателей как загрузки объема буферов памяти, среднего времени задержки сообщений и вероятности отказа в обслуживании сообщения. При увеличении данных показателей (система близка к блокировке) устройство должно изменить режим КП на режим КК. И, наоборот, при снижении данных показателей (сеть недогружена), режим КК изменяется на режим КП. Массив статистических данных, полученных при моделировании различных типов сетей n и видов сетевого трафика m, сохраняют в модуле промежуточной памяти для последующего использования при включении основных режимов работы устройства.

ГСТ 2 предназначен для формирования в режиме обучения для основных типов сетей различных видов современного сетевого трафика. Его схема может быть реализована различным образом, например, как показано на рис. 2. При этом она включает в свой состав: генератор шума (ГШ) 2.1, предназначенный для формирования (генерации) случайных сигналов с основными законами распределения; элемент выборки и хранения (ЭВХ) 2.2, предназначенный для получения мгновенных значений напряжения из случайных сигналов (формируемых ГШ) в заданные моменты времени, и состоит из смесителя и экстраполятора нулевого порядка; элемент сравнения (ЭС) 2.3, предназначенный для сравнения значений напряжений сигналов, подаваемых на его входы и представляющий собой компаратор; генератор линейно-изменяющегося напряжения (ГЛИН) 2.4, предназначенный для формирования пилообразного напряжения; регулируемая линия задержки (РЛЗ) 2.5, предназначена для формирования заднего фронта импульса, задержанного по времени на необходимую величину; электронный ключ (ЭК) 2.6, предназначенный для переключения видов формируемых импульсных последовательностей, и содержащий два информационных входа, управляющий вход и информационный выход; перестраиваемый генератор тактовых импульсов (ГТИ) 2.7, предназначенный для генерирования тактовых импульсов с различным периодом следования; управляющий элемент (УЭ) 2.8, предназначенный для формирования выходного искусственного трафика для обучения системы и представляющий собой RS-триггер.

В режиме обучения предлагаемый ГСТ работает следующим образом. При подаче из модуля управления устройства ГК ЦКС на ГСТ 2 (см. рис. 2) через управляющий вход «включение» управляющего сигнала в двоичном коде «11» происходит включение генератора и, соответственно по управляющему сигналу «00», его отключение. При этом команды включения и выключения параллельно поступают на ГШ 2.1, перестраиваемый ГТИ 2.7 и ГЛИН 2.4. При подаче управляющего сигнала «01» происходит включение режима генерации последовательности импульсов, длительность которых изменяется по случайному закону. На выходе ГСТ 2 формируются импульсы

с фиксированным по положению тактового импульса задним фронтом. Этот случай соответствует сетям SDH (синхронной цифровой иерархии). Временные диаграммы работы устройства представлены на рис. 3. Здесь обозначено: U_1 – напряжения на выходе ГШ; U_7 – напряжение на выходе перестраиваемого ГТИ; U_4 – напряжение на выходе ГЛИН; U_2– напряжение на выходе ЭВХ; U_3 – напряжение на выходе ЭС; $U_8^{\text{вх.1}}$ – напряжение на первом входе УЭ; $U_6^{\text{вх.1}}$ – напряжение на первом входе ЭК; $U_6^{\text{вх.2}}$ – напряжение на втором входе ЭК; $U_8^{\text{вых}'}$ – напряжение на выходе УЭ с фиксированным по положению тактового импульса задним фронтом; $U_8^{\text{вых}''}$ – напряжение на выходе УЭ с фиксированной на величину задержки задним фронтом импульса; U_0 – уровень компарации ЭС, совпадающий с амплитудой линейно изменяющегося напряжения; $U_{\text{ср}}$ – среднее значение случайного процесса; U_i – мгновенное значение случайного процесса; $\tau_{\text{Т}}$ – период следования тактовых импульсов; $\tau_{\text{з}}$ – величина задержки, создаваемая РЛЗ.

Случайный сигнал, с заданным законом распределения (см. U_1 на рис. 3) с выхода ГШ 2.1 (см. рис. 2) поступает на вход ЭВХ 2.2, который содержит смеситель и экстраполятор нулевого порядка. Тактовые импульсы (см. U_7 на рис. 3), получаемые в перестраиваемом ГТИ 2.7, поступают на управляющий вход ЭВХ 2.2, где «вырезаются» мгновенные значения U_{i} из случайного сигнала (см. U_1 на рис. 3), которые затем экстраполируются (см. U_2 на рис. 3) и поступают на первый вход ЭС (компаратор) 2.3, на второй вход которого подаются пилообразные импульсы с выхода ГЛИН 2.4 (см. U_4 на рис. 3). Как только линейно изменяющееся напряжение превысит уровень компарации (экстраполированное напряжение), на выходе ЭС выделяется импульс (см. U_3 на рис. 3), который передним фронтом переведет управляющий элемент (RS-триггер) 2.8 во второе устойчивое состояние, при этом на его выходе появится высокий потенциал (см. $U_8^{\text{вх.1}}$ на рис. 3). Этим самым будет зафиксирован передний фронт импульса, момент появления которого случаен и определяется законом распределения исходного процесса U_{i}, которые легко пересчитываются во временные интервалы, отсчитываемые от начала координат. Положение импульсов на временной оси можно определить по следующей формуле: $\tau_i = \frac{\tau_{\text{Т}}}{U_0}\left(\sum_{i=1}^{n} U_i - iU_{cp}\right)$.

Следующий тактовый импульс, поступающий с выхода перестраиваемого ГТИ 2.7 через ЭК 2.6, открытый по управляющему сигналу «01» для его второго входа (см. $U_6^{\text{вх.2}}$ на рис. 3), поступает на вход установки в нуль УЭ (RS-триггера) 2.8, который возвращает его в первое (нулевое) устойчивое состояние, при этом на его выходе появится низкий потенциал (см. $U_8^{\text{вых}'}$ на рис. 3). Этим самым будет зафиксирован задний фронт импульса, момент появления которого фиксирован по положению тактового импульса.

Если на управляющий вход «включение» ГСТ поступает управляющий сигнал в двоичном коде «10», то задний фронт выходного импульса оказывается задержанным на величину $\tau_{\text{з}}$ (см. $U_6^{\text{вх.2}}$ на рис. 3), а формированные импульсы будут иметь постоянную длительность. Так при $\tau_{\text{з}}$ =53 байта/V(бит/с), где 53 байта – длина ячейки АТМ, а V – скорость передачи ячейки, можно имитировать технологию асинхронного режима передачи – сеть АТМ (см. диаграмму $U_6^{\text{вх.1}}$ на рис. 3).

При этом по управляющему сигналу в двоичном коде «10», поступающему на управляющий вход ЭК 2.6 будет закрыт его второй вход и открыт первый, подключая вход установки нуля УЭ (RS-триггера) к выходу РЛЗ 2.5, на вход которой поступает с выхода ЭС сигнал, идентифицирующий передний фронт импульса (см. U_3 на рис. 3). И управляющий элемент будет переходить в первое (нулевое) устойчивое состояние с задержкой $\tau_{\text{з}}$, а на его выходе появится низкий потенциал, чем будет зафиксирован задний фронт импульса (см. $U_8^{\text{вых}''}$ на рис. 3), момент появления которого фиксируется РЛЗ 2.5. Тем самым на выходе ГСТ 2 будет формироваться последовательность одинаковых по длительности импульсов, но моменты появления которых, случайны и определяются законом распределения исходного процесса, который формируется ГШ 2.1.

Поскольку перестраиваемый ГТИ 2.7 и РЛЗ 2.5 имеют возможность настройки, а ГШ можно задавать случайные сигналы, с основными законами распределения, то можно добиться

любой длительности генерируемых сообщений, передаваемых с различной частотой следования, подчиняющихся необходимому закону распределения.

Таким образом, система может быть настроена на моделирование основных типов трафика и видов сетей, что и достигает поставленную цель и может использоваться при проектировании, испытании ТКС, а также в ходе обучения (настройки) УК и модулей системы и для прогнозирования нагрузки на них без привлечения пользователей (абонентов).

Модуль идентификации 4 предназначен для формирования решения на осуществление режима КК или режима КП с учетом длины передаваемого сообщения, объема загрузки буферов памяти и текущего состояния каналов. Его схема может быть реализована различным образом, например, как показано на рис. 4. При этом она включает в свой состав: цифро-аналоговый преобразователь (ЦАП) 4.1, предназначенный для преобразования двоичного кода в напряжение; вычислитель порога (ВП) 4.2, предназначенный для вычисления значения уровня порогового напряжения для переключения режимов коммутации с учетом занятого сообщением объема памяти в модуле промежуточной памяти; (ЭС) 4.3, предназначенный для сравнения значений напряжений сигналов, подаваемых на его входы и представляющий собой компаратор; управляющий элемент (УЭ) 4.4, предназначенный для формирования управляющего сигнала на включение режима КК или режима КП и представляющий собой RS-триггер; электронный ключ (ЭК) 4.5, предназначенный для переключения режимов коммутации.

При этом выход ЦАП 4.1 подключен к первому входу ЭС 4.3, второй вход которого соединен с выходом ВП 4.2, а выход является управляющим выходом «режим коммутации» модуля 4 и подключен к первому входу УЭ 4.4, второй вход которого является управляющим входом «установка 0» модуля 4, а первый и второй выходы являются первым и вторым входами ЭК 4.5, информационный вход которого соединен с информационным входом модуля 4. Управляющие входы ЦАП 4.1 и ВП 4.2 являются управляющими входами соответственно «длина сообщения» и «величина порога» модуля 4, а информационные выходы ЭК 4.5 являются информационными выходами «КК» и «КП» модуля 4.

В качестве ВП 4.2 (см. рис. 5) может быть использованы ЦАП 4.2.1, соединенный своим входом с входом ВП 4.2, первым своим выходом подключен к первому входу напрямую, а вторым входом – через дифференцирующий элемент 4.2.2 к второму входу суммирующего усилителя 4.2.3, выход которого является выходом ВП 4.2.

В качестве ЭК 4.5 (см. рис. 6) могут быть использованы два логических элемента И (И1 и И2) информационные входы которых подключены к информационному входу ЭК модуля идентификации 4, информационные выходы «КК» и «КП» – к одноименным информационным выходам ЭК и модуля идентификации, а управляющие первый и второй входы ЭК, поступающие соответственно на второй и первый логические элементы И соединены с прямым и инверсным выходами RS-триггера УЭ 4.4 модуля идентификации.

Предлагаемый модуль идентификации работает следующим образом. Если информация о длине сообщения (L) и пороговое значение ($L_{пор}$) задаются в двоичном коде, то в примере реализации блока идентификации 4 на рис. 4 ЦАП 4.1 и 4.2.1 соответственно модуля идентификации и его ВП 4.2 (см. рис. 5) непосредственно преобразуют код в напряжения, которые

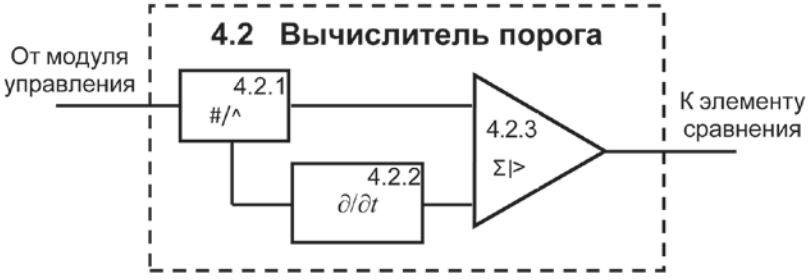


Рис. 5

сравниваются в ЭС 4.3 модуля идентификации. Если же значения L и $L_{пор}$ задаются каким-либо иным кодом, то перед ЦАП 4.1 и 4.2.1 необходимо поставить дешифраторы, преобразующие этот код в двоичный.

Код, соответствующий длине передаваемого сообщения, поступает на вход ЦАП 4.1 по окончании диалога, в то время как на вход ЦАП 4.2.1 ВП 4.2 поступают текущие значения $L_{пор}$, вычисляемое модулем управления 6 (см. рис. 1) в течение всего времени функционирования устройства с учетом состояния буферов памяти в модуле промежуточной памяти 3.

Если истинная длина сообщения, преобразованная в напряжение ЦАП 4.1 модуля идентификации 4, превысит порог $U_{пор} = \alpha L_{пор}$, где α – коэффициент передачи ЦАП, то на выходе ЭС 4.3 появится высокий потенциал, при котором УЭ 4.4 (триггер) перейдет во второе устойчивое состояние и на его прямом выходе появится высокий потенциал. Первый элемент И1 ЭК 4.5 (см. рис. 6) закроется, а второй элемент И2 ЭК 4.5 откроется. Модуль идентификации 4 готов к передаче сообщения из модуля промежуточной памяти 3 в модуль сопряжения с каналами связи 5. После установления сквозного канала до адресата устройство ГК ЦКС инициирует передачу сообщения. В противном случае, если соединение не установлено, абонент получает отказ.

Учет динамики изменения трафика поступающих на обслуживание сообщений в схеме на рис. 4 реализован в ВП 4.2 на суммирующем усилителе (см. рис. 5), на один вход которого подается $U_{пор}$, а на второй вход – его производная $\partial U_{пор}/\partial t$, знак которой повышает или снижает порог $U_{пор}$ в зависимости от того, увеличивается или уменьшается число занятых буферов в данный момент в модуле промежуточной памяти, изменяя тем самым соотношение между обоими режимами коммутации (см. рис. 7).

После передачи сообщения УЭ 4.4 возвращается в исходное состояние, например, путем подачи сигнала «установка 0» на его R-вход из модуля управления 6 через управляющий вход «установка 0».

Таким образом, согласно рис. 7, при длинных сообщениях и увеличивающемся трафике будет преобладать метод КК и, наоборот, если в устройство будут поступать короткие сообщения при сильно пульсирующем трафике, передачу сообщений целесообразно осуществлять с использованием метода КП. Использование того или иного режима определяется выбором величины $L_{кр}$. Если число занятых буферов ($\nu_з$) и величина b могут контролироваться в пределах данного устройства ГК ЦКС или во всей сети в зависимости от принятого метода маршрутизации, то критическая длина сообщения ($L_{кр}$) является проектным параметром и устанавливается на стадии проектирования конкретной устройства сети, или методом статистических испытаний в режиме обучения с использованием предложенного ГСТ.

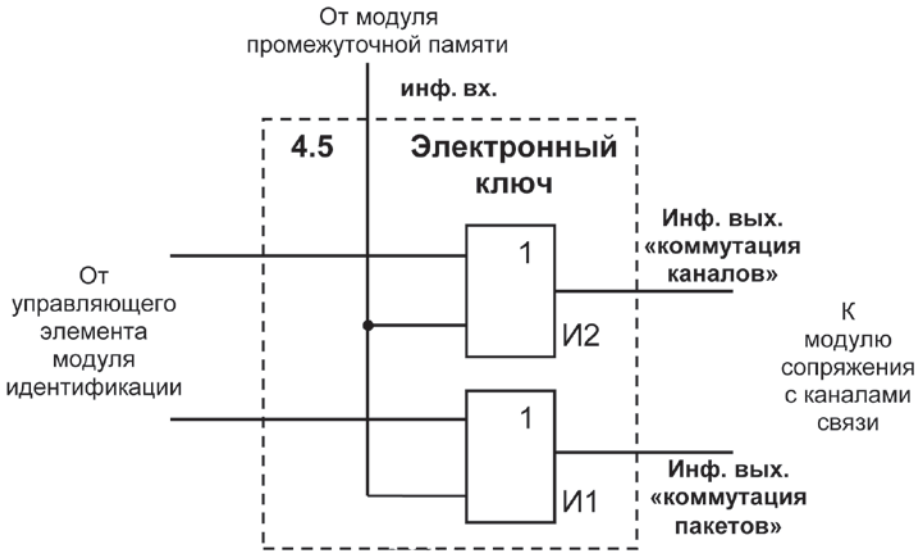


Рис. 6

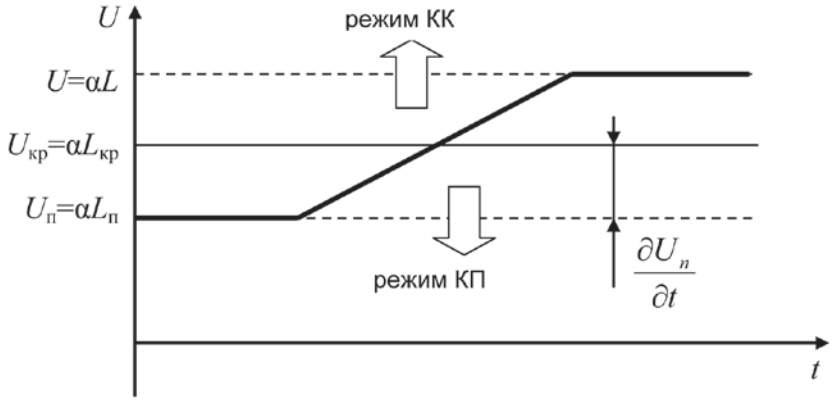


Рис. 7

6. Оценка эффективности заявленного способа

Исследования, проведенные в [9], позволяют осуществить более обоснованный выбор $L_{кр}$ и расчет основных вероятностно-временных характеристик и показателей сети. Минимальное среднее время задержки сообщения может быть вычислено из соотношения

$$T_{ср}^{min} = \frac{1}{\gamma}\frac{C_{зад}}{k}\left(\frac{S'_\nu}{S_\nu}\right)_{opt}, \qquad (4)$$

где γ – общий трафик; $C_{зад}$ – заданная стоимость передачи единицы количества информации; k – коэффициент пропорциональности; для полностью загруженной системы, когда $\rho=1$ соотношение в скобках равно

$$\left(S'_\nu/S_\nu\right)\Big|_{\rho=1} = \frac{1+2+\ldots+(\nu+1)}{\underbrace{1+1+\ldots+1}_{\nu+2}} = \frac{(\nu+1)(\nu+2)}{2(\nu+2)} = \frac{\nu+1}{2}, \qquad (5)$$

при этом учтено, что числитель $1+2+\ldots+(\nu+1) = \frac{(\nu+1)(\nu+2)}{2}$ – есть сумма арифметической прогрессии.

Тогда оптимальное значение равно

$$\left(\frac{S'_\nu}{S_\nu}\right)_{opt} = -\frac{\sum_{k=0}^{\nu}(k+1)\rho_{опт}^k}{\sum_{k=0}^{\nu+1}\rho_{опт}^k}.$$

Данное условие определяет оптимальное значение коэффициента загрузки устройства гибридной коммутации $\rho_{опт} = C_{зад}/kr$, обеспечивающее минимальное значение среднего времени задержки сообщений в виде выражения (4). Здесь r – общее число узлов сети, влияющее на количество выходных линий. При этом $0 < \rho_{опт} < 1$. А условие (5) соответствует максимальному значению задержки сообщения при $r = 1$, и не зависит от стоимости устройства и сети $T_{зад}^{max} = \frac{r}{\gamma}\cdot\frac{(\nu+1)}{2}$.

Кривые зависимостей $T_{ср}^{min} = f(\rho_{опт})$ и $P_{отк} = \varphi(\rho_{опт})$, построенные в соответствии с выражениями (4) и (2), приведены на совмещенном графике рис. 8 и подтверждают предположение о том, что использование в системе бесконечного числа буферов позволяет получить верхнюю границу для задержки, которую можно достичь при конечном числе элементов буферной памяти, при этом задержка в системе без буферов дает нижнюю границу для задержки большого разнообразия систем множественного доступа с буферизацией и управляемым потоком.

Анализ полученных результатов показывает, что минимальная средняя задержка ($T_{ср}^{min} = 1{,}8$ с), соответствующая $\rho'_{opt} = 0{,}6$ и $\nu = \infty$, (точка А) может быть достигнута при более высоком трафике поступающих на обслуживание заявок ($\rho''_{opt} = 0{,}78$ и $\nu = 3$) при ограниченном числе буферов в модуле промежуточной памяти устройства ГК ЦКС (точка В). При этом вероят-

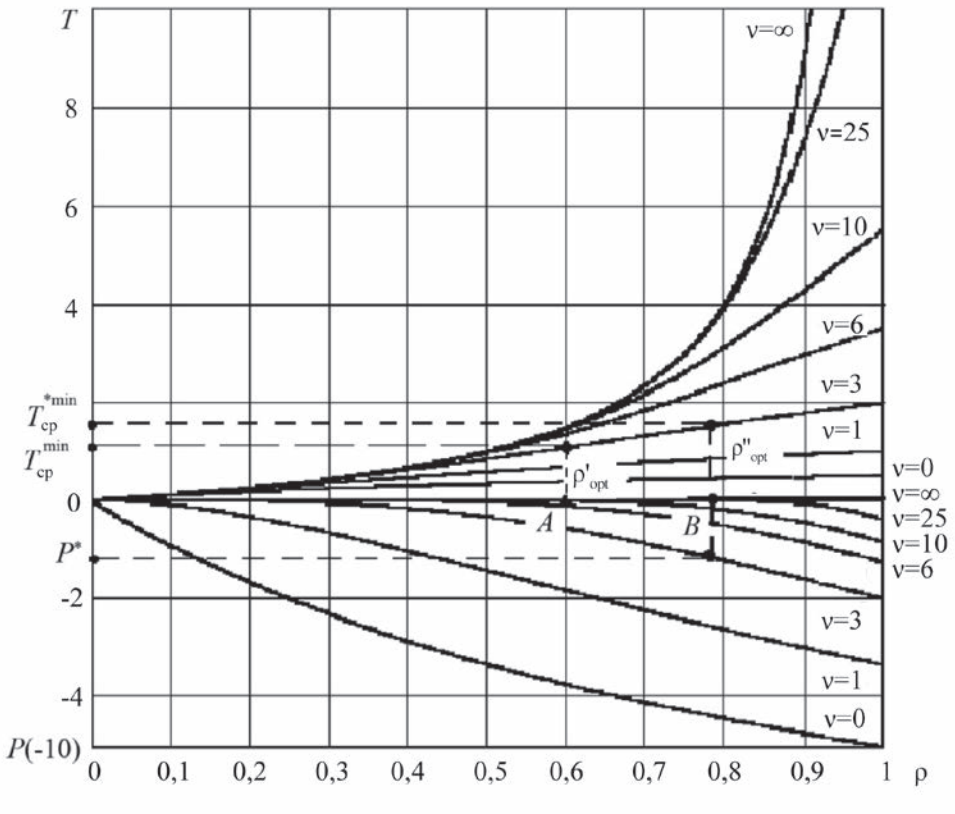


Рис. 8

ность отказа $P^* = 0,12$, что приблизительно соответствует значению ~10 % и является вполне приемлемым [3].

Аналитические расчеты подтверждают, что при ужесточении требования к вероятности отказа значение $P_{отк}^{доп} = 0,01$ может быть достигнуто при количестве буферов ν=20 и коэффициенте загрузки $\rho_{opt} = 0,9$. При этом для сложной сети, например, содержащей $l = 40$ УК, и напряженном трафике $\gamma = 36$ пакетов/с, среднее время задержки сообщений будет равно $T_{ср}^{min} = 7$ с. В соответствии с (3) критическая длина сообщения для заявленного устройства ГК ЦКС будет равна $L_{кр} = 20480$ бит при длине пакета $L_{пак} = 1024$ бит.

Вывод

Исходя из примера расчета критической длины сообщения и оценки эффективности предложенного способа, реализованного на устройстве гибридной коммутации цифровых каналов связи, генераторе сетевого трафика и модуле идентификации позволяет при заданной стоимости передачи единицы информации осуществить выбор числа элементов буферной памяти и оптимального значения сетевого трафика, обеспечивающего минимальную среднюю задержку передачи сообщений и допустимую вероятность отказа в обслуживании поступающих от абонентов заявок, а также подтверждает целесообразность передачи длинных сообщений методом коммутации каналов, а коротких – методом коммутации пакетов, поскольку обеспечивает сохранение масштаба времени и служит достижению указанных целей способа.

СПИСОК ЛИТЕРАТУРЫ

1. Самойленко С. И. Метод адаптивной коммутации // Электросвязь, 1981. – №6.

2. Jenny Christian J., Kummerle Karl, Burge Helmut. Network node with integrated circuit /Packet switching capabilities. – "Communes. Networks Eur. Comput. Conf. , London, 1975". Oxbridge, 1975, 207-228.

3. Баркун М. А., Ходасевич О. Р. Цифровые системы синхронной коммутации. – Москва: Эко-Трендз, 2001.

4. Будко П. А., Федоренко В. В. Управление в сетях связи. Математические модели и методы оптимизации. – М.: Физматлит, 2003. – 226 с.

5. Фомин Л. А., Будко П. А. Эффективность и качество инфокоммуникационных систем. Методы оптимизации. – Москва: Физматлит, 2008. – 296 с.

6. Патент РФ №2450335 Кл. G06F 15/00, G05B 23/00. Опубликован 10.05.2012 Бюл. №13.

7. Мизин И. А., Богатырёв В. А., Кулешов А. П. Сети коммутации пакетов / Под ред. В. С. Семенихина. – М.: Радио и связь, 1986. – 408 с.

8. Вентцель Е. С. Исследование операций. – М.: Наука, 1989. – 552 с.

9. Будко П. А. Управление ресурсами информационно-телекоммуника-ционных систем. Методы оптимизации. – Спб.: ВАС, 2012. – 512 с.

Г.А. Бузов
Москва (учебный центр ИНФОРМЗАЩИТА)
В.Д. Алексеев
С.Т. *Аманжолова*
Казахстан, Алматы (КазНТУ имени К.И.Сатпаева)

ОСОБЕННОСТИ РАБОТЫ С ИНДИКАТОРАМИ ПОЛЯ ДЛЯ ПОИСКА АКУСТИЧЕСКИХ КЕЙЛОГЕРОВ.

Исследователи из Университета Беркли показали, что аудиозапись нажатий на кнопки клавиатуры позволяет с высокой точностью восстановить набранный текст. Группе ученых удалось на 96 процентов распознать информацию, содержащуюся в десятиминутной записи. Таким образом, размещенный радиомикрофон вблизи от клавиатуры, создает канал утечки информации, нарушающий такой механизм идентификации, как пароли. Для выявления подобных каналов утечки конфиденциальной информации наиболее простыми и распространенными поисковыми приборами являются индикаторы поля. Однако применение этих приборов для выявления радиомикрофонов в современных условиях имеет свои особенности, которые необходимо рассмотреть.

Использование индикаторов поля позволяет по демаскирующим признакам определить и локализовать источники электромагнитных излучений. Оптимальный комплект оборудования по выявлению закладочных устройств (ЗУ) состоит из: аппаратно-программного комплекса радиомониторинга, сканирующего приёмника, индикаторов поля, оптических обнаружителей видеокамер. В качестве дополнительного оборудования можно рекомендовать нелинейный локатор и комплект инструментов.

Наличие аппаратно-программного комплекса снимает необходимость приобретения оборудования для проверки линий различного назначения.

Однако не всегда финансовые возможности, позволяют приобрести весь рекомендованный комплект поискового оборудования, и в этом случае приходится довольствоваться минимальным набором поисковых приборов.

В общем случае это не гарантирует выявления всех видов современных ЗУ, но в любом случае, даже при использовании минимального комплекта оборудования, для достижения цели проверки необходимо придерживаться определённой последовательности при проведении поисковых мероприятий.

В рамках одной статьи сложно дать рекомендации по выявлению всех видов ЗУ поэтому ограничимся рассмотрением вопросов проведения мероприятий по выявлению радиомикрофонов с использованием индикаторов поля.

Любое поисковое мероприятие по выявлению ЗУ начинается с визуального осмотра проверяемого помещения. Методика проведения визуального осмотра достаточно полно изложена во многих печатных изданиях посвященных методике проведения поиска.

Основной целью данной статьи является анализ возможностей по выявлению работающих радиомикрофонов с помощью различных типов индикаторов поля и определению наиболее

оптимальных способов применения их при проведении поиска.

Поиск, с применением любого индикатора поля, начинается с подготовки его к поиску. Для этого необходимо, в соответствии с руководством по применению используемого прибора выставить необходимый уровень порога обнаружения. Данный уровень рекомендуется устанавливать с превышением уровня фонового электромагнитного поля в проверяемом помещении на 5-10 Дб.

Методику проведения поиска рассмотрим для поиска ЗУ с применением как светодиодных, так и цифровых индикаторов поля.

В процессе визуального осмотра помещения поисковики, как правило, определяют несколько потенциальных мест возможного размещения ЗУ, вызывающих у них подозрение по тем или иным косвенным признакам. Зачастую не всегда можно обнаружить камуфлированные ЗУ визуальным осмотром. Поэтому поиск, с применением поисковых приборов, целесообразно начинать с обследования мест вызвавших у вас подозрение. Для этого с включённым индикатором поля (ИП) обследуют подозрительные места путем плавного перемещения ИП над подозрительным местом на высоте 5-10 см от контролируемой поверхности.

Светодиодный индикатор, при перемещении его в районе возможного отклика излучающего сигнала выдает информацию в виде засветившихся светодиодов. Затем путем поворота индикатора поля в разные стороны необходимо добиться максимального излучения. В зависимости от расположения источника излучения на устройстве индикации будет загораться большее или меньшее число светодиодов. При загорании максимального числа светодиодов необходимо путём загрубления чувствительности прибора уменьшить число светящихся светодиодов до двух или трех и опять повторить операцию до максимального числа загоревшихся светодиодов. При приближении к источнику излучения возможно проявление акустозавязки, проявляющееся в виде характерного свиста в динамике ИП. Режим акустозавязки характеризуется возникновением положительной обратной связи между источником излучения и динамиком ИП. По максимуму излучения и возникновению акустозавязки оператор делает вывод о наличии в районе поиска источника излучения и визуально, методом осмотра подозрительных мест, выявляет его.

Однако при кажущейся простоте использования светодиодных индикаторов поля для поиска и локализации ЗУ, применение для этих целей данных индикаторов, имеет ряд существенных недостатков:

- по индикации невозможно определить характеристики источника излучения, а это особенно важно при сложной электромагнитной обстановке в районе поиска;
- при наличии рядом с проверяемым помещением мощного внешнего источника излучения, каким может быть излучение базовой станции сотовой связи, индикатор поля зацикливается на мощный источник излучения и на другие не реагирует.

Таким образом, для успешного проведения поиска наиболее целесообразно использование цифровых, селективных ИП. По принципу действия селективный индикатор поля представляет собой скоростной супергетеродинный приемник с низкой ПЧ и синтезатором частоты. Индикатор поля осуществляет широкополосное сканирование частотного диапазона работы индикатора.

При этом на цифровой дисплей ИП выводится информация об обнаруженных сигналах, превышающих пороговое значение: частота источника излучения, мощность излучаемого сигнала в децибелах. По этим параметрам, зная характеристики легальных источников излучения, оператор может сосредоточиться на анализе подозрительных излучений.

Более подробно рассмотрим методику поиска ЗУ на примере использования селективного индикатора поля «RAKSA-120».

Селективный индикатор поля «RAKSA-120» предназначен для обнаружения в ближней зоне и определения местоположения радиопередающих устройств, использующихся для негласного съема информации, включая сотовые телефоны стандартов GSM900/1800, UMTS(3G), CDMA450, беспроводные телефоны стандарта DECT, устройства Bluetooth и Wi-Fi. По принципу действия селективный индикатор поля «RAKSA-120» представляет собой супергетеродинный приемник с низкой ПЧ и синтезатором частоты. При работе осуществляется непрерывное сканирование частотного диапазона и анализ пиков спектрограммы. Идентификация стандар-

тных цифровых сигналов осуществляется по их амплитудно-временной характеристике.

Время цикла сканирования и анализа всех цифровых и аналоговых сигналов составляет около 1,0-1,5 секунд. Для фильтрации кратковременных помех необходимо наличие сигнала как минимум в двух циклах сканирования. Этим и определяется время обнаружения сигнала равное 2-3 секундам.

Любой непрерывный радиосигнал, с коэффициентом амплитудной модуляции <0,5 и без скачков частоты, классифицируется как аналоговый. Сюда относятся собственно аналоговые сигналы с различными видами модуляции (АМ, ЧМ, ФМ) и цифровые сигналы с модуляцией FSK, PSK и др.

Индикатор поля «RAKSA-120» может работать в режимах охраны, обзора, поиска, поиска с вычитанием спектра и мониторинга цифровых сигналов.

Любое поисковое мероприятие начинается с подготовки поискового оборудования. Включение прибора осуществляется нажатием кнопки **[C/PWR]** с удержанием более одной секунды (до короткого звукового сигнала). После включения индикатора на дисплее отображается главное меню.

Нажатием ▼ выбрать режим «Настройки» и нажать кнопку **[OK]**. На дисплее высветится

Analog – аналоговый сигнал
GSM – сигнал GSM900/1800
UMTS – сигнал UMTS (3G)
CDMA – сигнал CDMA450
DECT – сигнал DECT
Bluetooth – сигнал Bluetooth
Wi-Fi – сигнал Wi-Fi
2.4 GHz – прочие импульсные сигналы диапазона 2,4 ГГц.

Выбрать тип сигналов, для поиска **«Меню [OK] Настройки [OK] Сигналы»**. Выбранные типы сигналов отмечаются значком «V» путем нажатия ▼.

Установить пороговые уровни сигналов, для их обнаружения при поиске. **Для** этого из режима **«Меню [OK] Настройки [OK] Пороги» переключиться в режим Пороги.**

Во время поиска в помещении не должно быть работающих источников радиосигнала - сотовых и беспроводных телефонов, устройств Bluetooth, Wi-Fi, бытовых микроволновых печей. Для активации радиопередатчиков, использующих акустопуск, необходимо обеспечить наличие в помещении тестового акустического сигнала, например от работающего радиоприемника.

Выбор порогового значения осуществляется за пределами проверяемого помещения и зависит от оперативной обстановки. В сложной оперативной обстановке выбирается уровень порога равный 5-10 дБ. Нажатием кнопки [OK] перейти в меню и выбрать режим «обзор».

Поиск радиомикрофонов, при использовании данного режима, целесообразно проводить в сложной оперативной обстановке, так как в этом режиме на дисплее отображается список текущих обнаруженных сигналов, отсортированный по частоте или типу сигнала.

В верхней строке отображается номер выбранного сигнала и общее число сигналов в списке. Список начинается с аналоговых сигналов, для которых определено значение частоты. Затем из всех аналоговых сигналов, для которых невозможно достоверно определить значение частоты, отображается один, имеющий максимальный уровень. В конце списка находятся цифровые сигналы. В случае пропадания, сигнал удаляется из списка не сразу, а с задержкой примерно 10 секунд, в это время на дисплее отображается последнее ненулевое значение уровня сигнала.

Перемещением индикатора поля в районе обнаруженного излучения добиться максимума излучения и визуально обнаружить источник излучения. Для более надежного обнаружения источника излучения аналогового сигнала, можно осуществить его аудиоконтроль нажав на кнопку **[OK]**. В данном режиме при работе ЗУ с открытым каналом передачи данных возможна акустозавязка, проявляющаяся в виде характерного свиста и, при наличии тестового акустического сигнала в контролируемом помещении, его прослушивание в динамике индикатора поля.

После обнаружения источника излучения вернуться в режим обзора, для анализа списка обнаруженных сигналов. Для возврата к списку нажмите на кнопку **[OK]** или **[C].** Затем аналогично провести анализ и локализацию другого подозрительного сигнала.

В более простых случаях при незагруженной электромагнитной обстановке можно применять

режимы «поиска» и «поиска с вычитанием спектра». В данных режимах ИП выявляет только аналоговые сигналы, превышающие фоновые значения в проверяемом помещении. Поиск сигналов в режиме «поиск» существенно не отличается от поиска в режиме обзора. В данном режиме ИП фиксирует максимальное излучение, превышающее фоновое в проверяемом помещении, а в дальнейшем динамика работы аналогична.

Более интересен метод поиска с вычитанием спектра. В режиме поиска с вычитанием спектра определяется не абсолютный уровень аналоговых сигналов, а относительный, то есть его разница с базовым спектром, который был измерен в начале работы в этом режиме. Известно, что при приближении или удалении от радиопередатчика, который находится внутри помещения, уровень сигнала изменяется сильнее, по сравнению с радиопередатчиком, расположенным вне помещения. Так как в режиме поиска с вычитанием спектра индикатор поля селективно реагирует на изменения уровня, то локальные радиопередатчики будут обнаружены с большей вероятностью.

Поиск с вычитанием спектра начинается с накоплением в течение 5 секунд базового спектра аналоговых сигналов. В это время на дисплей выводится соответствующее сообщение и прогресс накопления. Накопление спектра проводится в помещении находящемся рядом с проверяемым, в котором гарантированно отсутствуют ЗУ. С включенным индикатором поля, после накопления фона, оператор заходит в проверяемое помещение.

После завершения накопления на дисплее отображается, аналоговый сигнал, имеющий максимальный относительный уровень. В режиме поиска с вычитанием спектра реализована световая и звуковая индикация относительного уровня сигнала – по частоте повторения вспышек светодиода можно судить о приближении или удалении от радиопередатчика. В данном режиме возможен «Аудиоконтроль» обнаруженного сигнала. Для аудиоконтроля текущего сигнала необходимо нажать кнопку **[ОК]**.

В данной статье рассмотрена общая методика поиска радиомикрофонов с применением светодиодных ИП и цифровых ИП на примере использования «Раксы 120». Хотя поиск, с применением индикаторов поля и не дает полной гарантии, но в некоторых случаях, при защите конфиденциальной информации, применение ИП бывает достаточно.

П.В. Вахромеев
г. Москва, ОАО «Концерн «Системпром»

МЕТОДИКА ОПРЕДЕЛЕНИЯ МИНИМАЛЬНОГО КОЛИЧЕСТВА ЗОН ДЕЖУРСТВА ИСТРЕБИТЕЛЬНОЙ АВИАЦИИ, НЕОБХОДИМЫХ ДЛЯ ПЕРЕХВАТА ЦЕЛЕЙ НА ЗАДАННОМ РУБЕЖЕ

В настоящей работе предложен способ определения минимального количества зон дежурства истребительной авиации, необходимого для выполнения боевой задачи по перехвату целей на заданном рубеже. Данная задача встречается в тех случаях, когда выполнение боевой задачи по перехвату целей на заданном рубеже невозможно из единственной зоны дежурства.

В настоящее время ведущие военные державы мира имеют на вооружении образцы авиационной и ракетной техники, такие как крылатые ракеты, штурмовая и бомбардировочная авиация, с дальностью действия свыше 1000 км. В этой ситуации для перехвата воздушных целей на дальних расстояниях следует считать наиболее универсальным средством истребительную авиацию (ИА). Современные истребители способны поражать цели на расстоянии до 1500 км. К тому же истребительная авиация обладает высокой мобильностью: время поднятия в воздух для истребителя из первой степени боевой готовности не превышает 5–10 минут.

Если рубежи обнаружения воздушного противника силами радиотехнических войск расположены недалеко от аэродромов взлета истребителей, или самолеты противника летят на больших скоростях, то с учетом времени подлета целей к заданным рубежам перехвата истребители не успевают взлететь или набрать необходимые им для атаки высоту и скорость [1]. В этом случае приходится предварительно выводить истребители в зону дежурства.

В работе [1] приведено решение задачи расчета положения зоны дежурства для одного типа истребителя, базирующегося на одном аэродроме. Решение задачи для группировки средств ИА сводится к разбиению выбранного участка заданного рубежа уничтожения на несколько непересекающихся частей с последующим решением задачи для одного типа истребителя в соответствии с приведенной выше методикой.

Таким образом, становится актуальной задача расчета минимального количества зон дежурства истребительной авиации, необходимых для выполнения истребителями боевой задачи по уничтожению воздушного противника на заданном рубеже.

Задача расчета положения зоны дежурства при перехвате целей на заданном рубеже строится исходя из возможного варианта действия противника. Вариантом действия противника является такой налет воздушных объектов противника (целей), действующих по различным направлениям, который призван причинить наибольший ущерб группировке наших войск с учетом их противодействия.

Вариант действия противника характеризуется скоростью, высотой полета целей и списком направлений действия противника. Каждое направление действия характеризуется координатами точки взлета, объекта поражения, точки обнаружения средствами радиотехнических войск (РТВ) и курсом.

Задача расчета положения зоны дежурства решается для выбранной группировки средств истребительной авиации (ИА). Таким образом, известны аэродромы взлета и посадки истребителей, типы истребителей, типы заправки и запасы топлива.

В данной работе рассматривается выполнение боевой задачи по уничтожению средств воздушного нападения (СВН) противника на заданном рубеже уничтожения (ЗРУ). Заданный рубеж уничтожения вводится оператором на картографическом фоне. Удаление ЗРУ от потребного рубежа [2] обычно выбирают таким, чтобы обеспечить уничтожение СВН противника до достижения ими потребного рубежа. Таким образом, нижней границей для ЗРУ служит потребный рубеж уничтожения, а верхней границей – располагаемый рубеж ИА. В настоящее время ЗРУ вводится оператором на карте без каких-либо ограничений.

Поскольку конфигурация заданного рубежа ИА заранее не определена и может быть достаточно сложной, то задача расчета положения зоны дежурства в общем случае является сложной и громоздкой. Поэтому перед решением такой задачи необходимо определить количество зон дежурства, минимально необходимых для выполнения боевой задачи истребителями. Ниже приведен алгоритм решения задачи расчета минимального количества зон дежурства для группировки ИА.

Алгоритм решения задачи расчета минимального количества зон дежурства

1. Рассчитать и сформировать заданный рубеж ИА[1] для уничтожения воздушного противника.

2. Перед расчетом количества зон дежурства (ЗД) решается задача[3,4] по перехвату СВН противника из готовности №1[5] с аэродрома методом «маневр»[6] для каждого аэродрома группировки ИА. Если по направлению действия воздушного противника (ВП) уничтожение с аэродрома (любого из аэродромов) возможно, данное направление исключается из расчета количества зон дежурства. Для всех направлений действия ВП, уничтожение которых с аэродрома невозможно, выполняется расчет количества зон дежурства.

3. Для выбранных варианта и направлений действия противника определяются точки пересечения траекторий полета целей с ЗРУ. Так определяется участок ЗРУ, на котором необходимо перехватывать цели. Выбранный участок ЗРУ представляет собой ломаную линию (без разрывов).

4. Положить количество зон дежурства k, равным 1.

5. Решить задачу расчета положения зоны дежурства[1] ИА для данного участка ЗРУ последовательно для каждого истребителя группировки ИА. Если задача решена успешно для какого-либо истребителя, минимальное количество зон дежурства k найдено и алгоритм завершен. Иначе, переходим к п.6.

6. Двигаясь от произвольного (но фиксированного) края участка ЗРУ, методом половинного деления (по точкам излома) находим такую точку излома, после которой зоны дежурства для данного участка ЗРУ не существует. На каждой итерации выполняется расчет положения зоны дежурства[1] последовательно для каждого истребителя группировки ИА.

7. Осуществляем уточнение участка ЗРУ, дополнив его новой точкой излома. Эта точка находится между двумя соседними уже имеющимися точками излома: найденной в п.6 и следующей за ней. Новая точка излома является последней точкой между двумя соседними точками излома, для которой зона дежурства существует. На каждой итерации выполняется расчет положения зоны дежурства[1].

8. Увеличиваем число зон дежурства k на единицу.

9. Для оставшегося участка ЗРУ выполняем п.5.

Разбиение зон дежурства по участкам ЗРУ, полученное в результате выполнения алгоритма, очевидно, не является оптимальным. Алгоритм предоставляет только минимальное количество зон дежурства, необходимых для выполнения истребителем боевой задачи. Задачи распределения зон дежурства по участкам ЗРУ и распределения истребителей группировки ИА по зонам дежурства должны быть решены отдельно.

СПИСОК ЛИТЕРАТУРЫ

1. Бородакий Ю.В., Вахромеев П.В., Шумилов Ю.Ю. Методика расчета положения зоны дежурства истребительной авиации при перехвате целей на заданном рубеже // Научно-технический сборник ФГУП «Концерн «Системпром». №1 (1), 2011.

2. Теория и методика управления авиационными подразделениями и частью. Под ред. В.Н. Каменского. М.: Военное издательство, 1993. – 248 с.

3. Вахромеев П. В. Алгоритм перехвата цели на заданном рубеже методом «маневр» // Научно-методический сборник 2 ЦНИИ МО РФ, 2010.

4. Вахромеев П.В. Алгоритм выбора варианта полета истребителя для перехвата воздушной цели на заданном рубеже методом «маневр» // Научно-технический сборник ФГУП «Концерн «Системпром». №1 (1), 2011.

5. Горощенко Б.Т., Горощенко Л.Б. Расчет дальности полета и рубежей перехвата. М.: ВВИА им. проф. Н.Е. Жуковского, 1968. – 151 с.

6. Дуров В. Р. Боевое применение и боевая эффективность истребителей-перехватчиков. М., Воениздат, 1972. – 280 с.

П.В. Вахромеев, А.А. Дубровина
г. Москва, ОАО «Концерн «Системпром»

МЕТОДИКИ ПОСТРОЕНИЯ ЗОНЫ ОБОРОНЫ ЗЕНИТНО-РАКЕТНОГО КОМПЛЕКСА

В данной статье рассмотрены две методики построения зоны обороны зенитного ракетного комплекса (ЗРК). Первая методика описывает построение зоны обороны с учетом моделирования удара оперативно-тактических и тактических баллистических ракет (далее – ОТР) противника по объектам обороны с различных точек старта. Также учитывается смещение позиции ЗРК относительно объекта обороны. Вторая методика описывает построение зоны обороны ЗРК на основе минимально и максимально допустимых высот входа и выхода траекторий ОТР из зоны поражения, при которой обеспечивается ее поражение.

Опыты вооруженных конфликтов последних десятилетий позволяют сделать вывод о том, что в полосе, удаленной от переднего края района обороны на 100-180 км, а в перспективе до 200-300 км и более, задачи по уничтожению военных и государственных объектов будут решаться при широком применении противником ОТР различных типов. Оперативно-тактические ракеты являются специфическими целями для зенитно-ракетных войск. Их специфика определяется следующими основными факторами: параметрами траекторий полета, высокой скоростью падения, малым подлетным временем до поражаемого объекта, значительным радиусом поражения головной части при снаряжении их ядерным зарядом.

При проведении тактических расчетов по прикрытию объекта от удара ОТР пользуются, как правило, параметрами зоны обороны ЗРК. В общем случае под зоной обороны понимается участок местности, прикрываемый ЗРК от ударов баллистических целей, наносимых в пределах ракетоопасного сектора при реализуемых в данных условиях углах их падения [1]. Величина угла ракетоопасного сектора вычисляется, исходя из рассмотрения сферического треугольника, образованного точками старта и точкой прицеливания. Для определения ракетоопасного сектора необходимо из множества точек старта ОТР, с которых возможен удар по объекту, выбрать две крайние относительно некоторого направления точки старта.

По объекту прикрытия с заданными координатами наносится удар ОТР. Удар наносится из известных точек старта, тип ОТР и все необходимые характеристики для расчета ее траектории известны. Существуют два возможных типа траектории полёта ОТР к прикрываемому ЗРК объекту – настильная и навесная. Настильная траектория характеризуется углом падения до 20°, навесная – углом падения свыше 20°[2]. ЗРК находится в точке с известными координатами и характеризуется заданными зоной поражения, зоной обнаружения, параметрами ведения стрельбы. Зона поражения ЗРК – область пространства, в каждой точке которой обеспечивается поражение одной ракетой одиночной цели определенного типа при фиксиро-

ванных условиях стрельбы [3]. Необходимо определить возможности ЗРК по прикрытию объекта от ОТР, летящих по обеим возможным траекториям, т.е. рассчитать зону обороны ЗРК – участок на земной поверхности, прикрываемую группировкой от ударов ОТР.

В качестве положения ЗРК в расчетах рассматриваются усредненные координаты всех составных частей. Данное допущение не вносит существенной погрешности в результаты расчетов, т.к. расстояния от позиции ЗРК до составных его частей существенно меньше расстояния между точкой старта ОТР и объектом обороны.

Рассмотрим методики построения зоны обороны ЗРК.

Первая методика

Для решения задачи построения зоны обороны ЗРК последовательно рассматриваются различные пары возможных точек старта ОТР и точек, находящихся вблизи ЗРК. Рассмотрим с дискретностью в несколько градусов все направления вокруг выбранного комплекса.

На выбранном направлении сначала определяется удаление от ЗРК границы зоны обороны для первой рассматриваемой точки старта. Для этого, начиная с некоторого начального приближения – например, $d_0 =$ 10 км, определяется, прикрыта ли точка на рассматриваемом расстоянии d_0 от ЗРК от удара ОТР, летящих из заданной точки старта. Если времени от момента входа ОТР в зону обнаружения до ее выхода из зоны поражения достаточно для ЗРК, чтобы провести мероприятия по ее уничтожению, точка прицеливания ОТР считается прикрытой. Точка должна быть прикрыта от ОТР, летящих по двум возможным типам траектории – настильной и навесной, в противном случае она считается незащищённой.

Увеличивая или уменьшая значение d_0, определяется отрезок, для которого точка, находящаяся на одном его конце прикрыта от удара, а на другом не прикрыта. Далее используется метод бинарного поиска: рассматривается точка на середине отрезка, и определяется, лежит ли она в зоне обороны. После выполнения необходимого числа шагов, метод сойдется к значению, которое и принимается за оценку величины удаления границы зоны обороны на рассматриваемом направлении для данной точки старта.

Затем рассматривается следующая точка старта, если она есть. Определяется удаление от ЗРК границы зоны обороны, как если бы единственной точкой старта была бы эта точка. В качестве границы зоны обороны на данном направлении, соответствующей двум рассмотренным точкам старта, принимается минимальное из двух найденных значений удаления границы зоны обороны на данном направлении. Минимальное значение берется потому, что в зоне обороны должны находиться точки, которые прикрыты от удара как с первой, так и со второй точки старта.

Затем, при последовательном рассмотрении остальных точек старта, определяется удаление от ЗРК границы зоны обороны на данном направлении. После рассмотрения одного направления и получения для него удаления зоны обороны от ЗРК, выполняется переход к рассмотрению следующего направления.

Таким образом, после рассмотрения всех направлений и нахождения для них удаления зоны обороны от ЗРК, формируется граница зоны обороны ЗРК с учетом месторасположения прикрываемого объекта.

Вторая методика

На основе минимального значения высоты зоны поражения ЗРК при стрельбе по баллистической цели (БЦ), минимальному реализуемому в данных условиях значению угла падения БЦ и длине участка траектории БЦ, соответствующей данному углу и лежащей внутри зоны поражения, рассчитывается удаление передней $L_{\Pi i}$ границы зоны обороны.

На основе максимального значения высоты зоны поражения ЗРК при стрельбе по БЦ, максимальному реализуемому в данных условиях значению угла падения БЦ и длине участка траектории БЦ, соответствующей данному углу и лежащей внутри зоны поражения, рассчитывается удаление тыльной L_{Ti} границы зоны обороны.

Затем задается ряд значений предельного параметра P_i, дискретность определяется необходимой точностью определения границ зоны обороны. Для каждого значения параметра рассчитывается удаление передней $L_{\Pi i}$ и тыльной L_{Ti} границ зоны обороны $L_{\Pi i}$ соответствует настильной траектории, L_{Ti}– навесной.

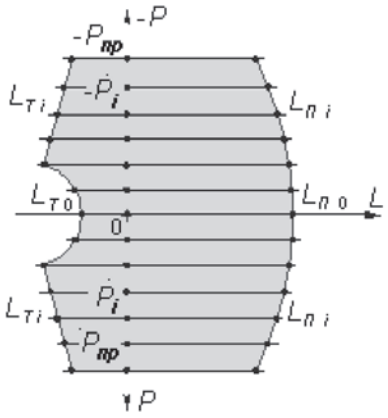


Рис.2. Построение зоны обороны ЗРК с учетом ракетоопасного сектора

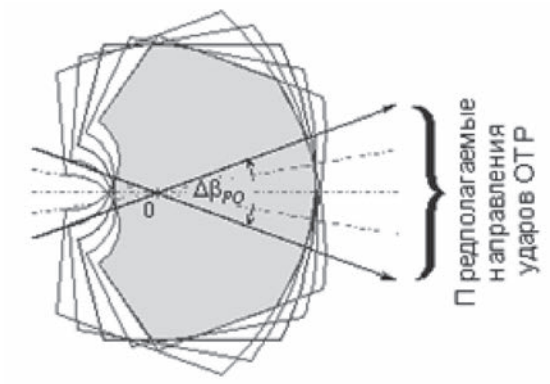


Рис. 1. Построение зоны обороны

Значения предельного параметра и рассчитанные для каждого из них удаления передней $L_{\Pi i}$ и тыльной L_{Ti} границ зоны обороны используются для графического построения зоны обороны (рис. 1).

Затем в пределах ракетоопасного сектора с некоторой дискретностью рассматриваются все направления возможного удара, и относительно каждого направления строится зона обороны (рис. 2).

Для построения области пересечения построенных зон обороны используется графический метод. Область пересечения и является зоной обороны ЗРК с учетом величины ракетоопасного сектора.

В данной статье рассмотрены методики построения зоны обороны ЗРК при ударе ОТР. Зона обороны является важной характеристикой комплекса при планировании и проведении военных действий; она позволяет оценить, прикрыт ли защищаемый объект от удара или нет.

В первой методике сразу учитывается величина ракетоопасного сектора. Для нескольких точек старта ОТР определяется, прикрыта ли ЗРК точка прицеливания; рассматриваются различные точки прицеливания. Необходимые для расчетов точки определяются исходя из известного вида зон обнаружения и поражения ЗРК, а также известной траектории ОТР. К достоинствам данной методики относится учет смещения объекта обороны относительно позиций ЗРК, к недостаткам – отсутствие указаний для построения тыльной границы зоны обороны.

Во второй методике границы зоны обороны определяются возможностями ЗРК по уничтожению ОТР с минимально допустимой высотой входа настильной и максимально допустимой высотой выхода навесной траектории БЦ в зону поражения, при которой обеспечивается ее обстрел. Таким образом определяется удаление границ зоны обороны для одного направления полета ОТР. При рассмотрении всех направлений в пределах ракетоопасного сектора и наложении рассчитанных зон обороны получается зона обороны ЗРК с учетом величины ракетоопасного сектора. К достоинствам методики относится простота построения передней и тыльной границ зоны обороны, к недостаткам – отсутствие учета положения объекта обороны относительно позиций ЗРК, а также графический подход к построению области пересечения зон обороны, найденных без учета возможного направления удара.

СПИСОК ЛИТЕРАТУРЫ

1. Н. Бокий. Особенности организации ПРО. // Информационно-аналитический журнал «Воздушно-космическая оборона», №5 (24) 2005 год, издательский дом «Алмаз-Медиа».

2. А.А. Дмитриевский, Л.Н. Лысенко, С.С. Богодистов. Внешняя баллистика – 3-е изд. перераб. и доп. – М. Машиностроение, 1991. – 640 с.

3. Ф.К. Неупокоев. Противовоздушный бой. М.: Военное издательство, 1989г. –262 с.

4. А.В. Скворцов. Обзор алгоритмов построения триангуляции Делоне // Вычислительные методы и программирование. 2002. Т. 3. С. 14–39. URL: http://num-meth.srcc.msu.su.

П.В. Вахромеев
О.А. Пантелеева
г. Москва, ОАО «Концерн «Системпром»

МЕТОДЫ РАЗМЕЩЕНИЯ ФОРМУЛЯРОВ ВОЗДУШНЫХ ОБЪЕКТОВ НА ЦИФРОВОЙ КАРТЕ МЕСТНОСТИ

В данной работе рассматриваются наиболее часто используемые методы размещения меток объектов применительно к задаче размещения формуляров воздушных объектов на цифровой карте местности, анализируются их достоинства и недостатки, оценивается возможность использования для решения поставленной задачи.

Цифровая карта – двухмерная визуальная модель карты или поверхности Земли, отображаемая с помощью средств компьютерной графики в заданной картографической проекции и обладающая возможностью изменения масштаба отображения и изменением визуально отображаемых деталей [1].

В век интенсивного развития компьютерной техники и программного обеспечения цифровые карты широко используются в различных предметных областях: топография, геология, метеорология, и многих других.

Особое место среди цифровых карт занимают карты военного назначения. Цифровая карта военного назначения – основа всей информации, используемой в геоинформационных системах военного назначения (ГИС ВН), предназначенных для применения в автоматизированных системах управления войсками и оружием, поддержки принятия решения командованием, планирования боевых действий войск и видов боевого обеспечения [2].

Одной из задач, решаемых с помощью ГИС ВН, является задача контроля воздушной обстановки (одновременного взаимного расположения по вертикали и горизонтали воздушных судов и других материальных объектов в определённом районе воздушного пространства [3]) на цифровой карте местности. Одно из обязательных условий при решении данной задачи – создание и размещение формуляров (меток) для воздушных объектов (ВО) на цифровой карте местности в режиме реального времени.

Причинами для автоматизации задачи размещения формуляров являются следующие:

1. Размещение формуляров является одной из основных задач при создании цифровых карт для предоставления необходимой информации;

2. Ручное размещение формуляров – долгий и трудоемкий процесс;

3. Эффективный способ размещения формуляров позволяет своевременно получать важную и актуальную информацию.

В общем случае формуляр представляет собой графический элемент карты, как правило, в виде прямоугольника, содержащего необходимую информацию. Прямоугольник может связываться с объектом с помощью прямой линии.

Целью данной работы является поиск решения, обеспечивающего автоматическое размещение формуляров воздушных объектов, удовлетворяющее приведенным ниже требованиям:

1. Необходимо избегать перекрытий нескольких формуляров для разных воздушных объектов, перекрытий формулярами воздушных объектов и выноса формуляров за границы области цифровой карты. При этом нужно рассматривать каждый тип перекрытия отдельно, учитывая степень его критичности;

2. Так как воздушные объекты динамически изменяют свое положение на цифровой карте, механизм размещения формуляров должен обеспечивать предоставление актуальной информации по воздушным объектам в режиме реального времени;

3. Необходимо учитывать важность других объектов, находящихся на цифровой карте местности. Такие объекты нельзя перекрывать формулярами, так как они являются особо важными и всегда должны находиться в зоне видимости;

4. Необходимо учитывать ограничения на значения допустимых углов и расстояний между воздушным объектом и формуляром (например, для каждого ВО недопустимым будет являться угол, при котором формуляр будет находиться по курсу воздушного объекта).

Существуют различные методы размещения меток объектов: метод полного перебора, метод запретов, генетический алгоритм размещения меток, быстрый алгоритм размещения меток и другие. Последние два метода, наиболее часто используемые на практике, будут рассмотрены ниже.

Сначала рассмотрим генетический алгоритм (Genetic Algorithm for Feature Labelling, GA) размещения меток для отдельных объектов, расположенных в некоторых ограниченных областях, например, на цифровых картах [4].

В общем случае генетический алгоритм – это эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путём случайного подбора, комбинирования и вариации искомых параметров с использованием механизмов, напоминающих биологическую эволюцию. Генетические алгоритмы служат, главным образом, для поиска решений в многомерных пространствах поиска.

Задача, которую необходимо решить, формализуется таким образом, чтобы её решение могло быть закодировано в виде вектора («генотипа») генов, где каждый ген может быть битом, числом или неким другим объектом [5].

Каждая метка, размещаемая с помощью генетического алгоритма, представляют собой прямоугольник, один из краев которого соединен с центром объекта прямой линией. Текущее положение метки определяется углом поворота вокруг центра окружности. Центр окружности совпадает с центром объекта, а радиус равен длине соединительной линии, связывающей центр объекта с краем формуляра.

Основной задачей данного алгоритма является размещение меток с минимальным количеством перекрытий.

Существуют три возможных способа перекрытия:

1. Метка выходит за рамки допустимой области ее размещения (под допустимой областью размещения понимается прямоугольная область цифровой карты);

2. Метка перекрывает другую метку;

3. Метка перекрывает другой объект.

На цифровой карте все объекты, в том числе метки, состоят из пикселей. Генетический алгоритм размещения меток решает проблему перекрывающихся меток в терминах перекрывающихся пикселей.

Условиями останова алгоритма являются отсутствие перекрывающихся пикселей (на практике это условие сводится к минимизации количества перекрывающихся пикселей), и истечение заданного периода времени [4].

Подробнее данный метод описан в работе [4].

Достоинством данного метода является возможность достаточно быстрого поиска приемлемого решения благодаря механизмам случайного подбора, комбинирования и вариации значения угла поворота метки вокруг центра окружности.

Теперь рассмотрим алгоритм, предназначенный для размещения меток для точечных объектов на цифровой карте местности в режиме реального времени – быстрый алгоритм для размещения меток (Fast Algorithm for Label-Placement, FALP) [6].

Основные правила данного алгоритма:

1. Метка создается для каждого точечного объекта. Метка может быть расположена в одной из четырех возможных позиций относительно объекта, представленных на рисунке 1. Таким образом, положение каждой метки определяется парой значений: точка размещения и позиция относительно этой точки;

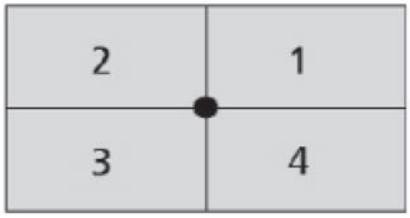


Рис. 1. Варианты расположения метки для точечного объекта

2. Каждая из возможных позиций метки имеет определенный весовой коэффициент, определяющий ее предпочтительность. На рисунке 1 цифра, расположенная внутри каждого прямоугольника, является весовым коэффициентом позиции метки. Чем меньше значение, тем выше предпочтительность позиции;

3. Рамки меток могут иметь разный размер;

4. Перед непосредственным выполнением алгоритма необходимо определить количество и позиции точечных объектов, для которых необходимо создать и разместить метки. На основании этих данных необходимо построить граф конфликтов, для которого затем будет построена матрица смежности;

5. Для оценки оптимальности расположения меток используется целевая функция. Оптимальность расположения зависит от количества перекрывающихся меток и предпочтительности позиций меток относительно точек размещения [6].

Более подробно данный метод описан в работе [6].

Достоинствами данного метода являются скорость размещения меток с минимальным количеством перекрытий.

Рассмотренные выше методы не полностью удовлетворяют требованиям, предъявляемым к размещению формуляров воздушных объектов.

Генетический и быстрый алгоритмы не удовлетворяет следующим требованиям, предъявляемым к размещению формуляров ВО:

1. Учет степени критичности каждого типа перекрытия (перекрытие нескольких формуляров для разных воздушных объектов, перекрытие формулярами воздушных объектов и вынос формуляров за границы области цифровой карты) при решении задачи минимизации разных типов перекрытий. Данные алгоритмы не разделяют вышеперечисленные типы перекрытий при решении задачи минимизации перекрытий;

2. Учет важности объектов, находящихся на цифровой карте местности. Данные алгоритмы работают со всей доступной для размещения меток областью (прямоугольной областью цифровой карты) и не учитывают отдельных районов внутри данной области, которые нельзя перекрывать метками;

3. Учет ограничений на значения допустимых углов и расстояний между воздушным объектом и формуляром. Генетический алгоритм работает с метками, имеющими фиксированное расстояние до объекта, единожды заданное для всех меток, что может привести к большому числу перекрытий. Расстояние в быстром алгоритме вообще не учитывается, положение метки определяется только точкой расположения и позицией относительно данной точки.

Для решения поставленной задачи можно взять за основу генетический алгоритм размещения меток, устраняя его недостатки и дополняя достоинствами других методов.

Для учета критичности каждого типа перекрытия можно ввести некий критерий важности (весовой коэффициент) перекрытия для каждого конкретного случая. Этот критерий будет использоваться в случае, если при размещении формуляра для отдельного ВО будут иметь место все вышеперечисленные случаи перекрытий, и не будет других альтернативных вариантов размещения. Вариант размещения будет выбран с учетом значения весового коэффициента, даже если данный вариант не будет лучшим среди возможных.

Для учета важности объектов, находящихся на цифровой карте местности, можно запретить перекрывать формулярами области карты, содержащие данные объекты. Таким образом, в список типов перекрытий добавится еще один тип со своим весовым коэффициентом.

При выборе положений меток нужно учитывать заранее заданные допустимые расстояния между ВО и формулярами. Возможность варьирования расстояния может существенно уменьшить количество перекрытий.

При выборе допустимого угла поворота метки относительно воздушного объекта нужно учитывать допустимые значения угла поворота, проводить соответствующие проверки. Таким образом будет исключена ситуация размещения формуляров по курсу ВО.

Соблюдение данных условий будет способствовать своевременному получению и удобному отображению важной и актуальной информации о воздушной обстановке, обеспечивая ее контроль.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровые карты и цифровые модели [Электронный ресурс] - Электрон. текст. дан. - Режим доступа: http://gis-tech.ru/digitalmap.html, свободный. – Загл. с экрана. - Яз. рус.;

2. Присяжнюк С.П., Филатов В.Н., Федоненков С.П. Геоинформационные системы военного назначения [Электронный ресурс] / С.П. Присяжнюк, В.Н. Филатов, С.П. Федоненков. - Электрон. текст. дан. - С.Пб.: БГТУ, 2009. - Режим доступа: http://gistechnik.ru/primgis/sila.html?showall=1, свободный. - Загл. с экрана. - Яз. рус.;

3. Воздушная обстановка [Электронный ресурс] – Электрон. текст. дан. - Режим доступа: http://ru.wikipedia.org/wiki/Воздушная_обстановка, свободный. - Загл. с экрана. - Яз. рус.;

4. A Genetic Algorithm for Feature Labelling in Interactive Applications [Электронный ресурс] - Электрон. текст. дан. - Режим доступа: http://usabilityetc.com/articles/feature-labelling-genetic-algorithm/, свободный. - Загл. с экрана. - Яз. англ.;

5. Генетический алгоритм [Электронный ресурс] – Электрон. текст. дан. - Режим доступа: http://ru.wikipedia.org/wiki/Генетический_алгоритм, свободный. - Загл. с экрана. - Яз. рус.;

6. Yamamoto M., Camara G., Lorena L. Fast Point-Feature Label Placement Algorithm for Real Time Screen Maps [Электронный ресурс] / M. Yamamoto, G. Camara, L. Lorena. - Электрон. текст. дан. – [VI Brazilian Symposium in Geoinformatics, 2005] - Режим доступа: http://mtc-m18.sid.inpe.br/col/dpi.inpe.br/geoinfo%4080/2006/07.11.13.14/doc/P59.pdf, свободный. - Загл. с экрана. - Яз. англ.

В.М. Ветошкин
доктор технических наук, профессор, ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина»;

О.В. Саяпин
кандидат технических наук, доцент, 27 Центральный научно-исследовательский институт Минобороны России;

С.В. Чискидов
кандидат технических наук, доцент, Академия гражданской защиты МЧС России;

МЕТОДИКА РАЗРАБОТКИ КОНЦЕПТУАЛЬНОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ СИСТЕМЫ БАЗ ДАННЫХ

Представленная методика направлена на ликвидацию технологической неопределенности процесса накопления и систематизации информации о проектируемой автоматизированной системе для формирования обоснованных требований к её подсистемам и видам обеспечения, а также на сокращение сроков разработки и внедрения. Реализация предложенного подхода позволит методологически обеспечить, технологически определить и инструментально оснастить процессы анализа информационного содержания функционирования сложных организационно-технических систем.

Разработка автоматизированной системы (АС) является многоплановой, чрезвычайно сложной и трудоёмкой задачей, предполагающей разработку всех видов ее обеспечения, а также осуществления совокупности организационных мероприятий, обеспечивающих функционирование создаваемой системы. Проектирование автоматизированных систем проходит в крайне противоречивых и сложных условиях. С одной стороны, стоимость создаваемых технических и программных систем достаточно высока, при этом информационные потребности пользователей нечетко определены, плохо сформулированы и меняются в процессе проектирования, увеличивая его сроки. С другой стороны, процесс совершенствования видов обеспечения АС настолько стремителен, что при длительных сроках проектирования систем они к моменту ввода в эксплуатацию оказываются устаревшими.

Указанные обстоятельства усиливают необходимость определения научно-методических основ и технологических стандартов для формирования концептуального облика системы в виде согласованной совокупности требований к ней, её составным частям и видам обеспечения. Такая система требований должна быть инвариантной по отношению к быстрой эволюции технических средств автоматизации, их программного обеспечения и всей информационной технологии. Здесь необходимо отметить, что активные зарубежные исследования последних лет в данном направлении уже воплощены в ряде технологических решений [1].

Основой автоматизации процессов функционирования организационно-технических систем являются современные информационные технологии (ИТ), базирующиеся на максимально широком использовании вычислительной техники, объединении ее в различные классы сетей, создании локальных и территориально-распределенных банков данных, реализующих режимы видеообработки, развитии систем искусственно-

го интеллекта, обеспечивающих решение трудноформализуемых задач принятия решений и дружественный интерфейс пользователям информационно-расчетных систем. Фундаментом современных ИТ является концепция интегрированных систем баз данных (СБД), состоящая в централизации функций накопления и распределения информации, позволяющая не только устранить многие трудности развития автоматизированных систем, но и определяющая основные технологические аспекты проектирования перспективных систем обработки данных для разных сфер применения. Теоретической базой таких технологий являются различные методологии проектирования систем баз данных [2-8].

Проектирование баз данных представляет собой длительный и трудоемкий процесс, требующий привлечения специалистов высокой квалификации. Будучи семиотической моделью определенной части, непрерывно изменяющегося реального мира, базы данных должны постоянно обновляться, чтобы адекватно отображать реальную действительность. Поэтому для сопровождения и эксплуатации информационных систем требуется постоянное использование процедур проектирования (трансформации и ведения) баз данных, образующих в рамках АС единую систему автоматизированного проектирования (сопровождения).

Использование процедур автоматизированного проектирования СБД направлено на уменьшение стоимости и времени разработки систем обработки данных, сокращение доли рутинных, нетворческих работ (связанных со сбором и редактированием исходных данных) и затрат на разработку прикладных систем и может служить основой для формирования требований ко всем видам обеспечения автоматизированной системы. Однако проектирование баз данных до сих пор остается скорее искусством, чем наукой. Основными ресурсами проектировщика баз данных служат собственные интуиция и опыт, причем качество получаемого при этом результата чрезвычайно сложно оценить. Во многих завершённых автоматизированных системах слабым местом оказывается структура базы данных. Основная проблема проектирования заключается в определении назначения элементов данных, их наилучшей взаимной связи и системы условий, которым должны удовлетворять значения элементов, вводимые в базу данных.

Создание систем автоматизированного проектирования баз данных требует разработки специальной теории, постановки, формализации и решения ряда сложных научно-технических задач, создания соответствующих технических и программных комплексов. Затраты на эти виды работ будут полностью компенсированы за счет значительного сокращения сроков проектирования, повышения качества проектных решений, а также многократного использования таких систем в процессе сопровождения и развития систем баз данных.

В широком смысле проектирование СБД автоматизированных систем представляет собой процесс выработки и документирования решений по составу информационных элементов (имен атрибутов и соответствующих им множеств допустимых значений); по организации элементов в структуры, соответствующие принятым в системе уровням представления данных, и определению связей структур различных уровней (отображений друг в друга); по определению ограничений целостности СБД и соответствующих процедур их контроля; по разграничению доступа к СБД и описанию процессов первоначальной загрузки и ведения баз данных; по разработке или выбору требуемого программного обеспечения, а также формированию организационно-методических и инструктивных материалов.

Содержательная формулировка проблемы эффективного проектирования СБД заключается в создании за минимальное время детально продуманной системы баз данных, обладающей свойствами расширяемости (учет новых требований) и целостности. Эту проблему удобно рассматривать в сопоставлении с этапами жизненного цикла системы, которые можно считать общепринятыми [3, 9-10]. Жизненный цикл системы БД делится на две фазы: фазу системного анализа и проектирования и фазу эксплуатации. В течение первой фазы проектировщик осуществляет сбор и анализ требований всех категорий пользователей и выполняет проектирование БД. В течение второй фазы осуществляется машинная реализация системы, сбор статистики и анализ функционирования.

Детализацию содержания фаз будем представлять следующими этапами.

Фаза моделирования, системного анализа и проектирования:

– функциональное моделирование;
– информационно-логическое проектирование;
– концептуальное проектирование;
– логическое проектирование;
– физическое проектирование.

Фаза реализации, функционирования и модификации:
– реализация БД;
– анализ функционирования;
– модернизация и адаптация.

Здесь не нашли отражения два важнейших этапа создания автоматизированной системы: выбор (или разработка) системных технических средств (комплекса средств автоматизации, вычислительных комплексов и т.д.) и системного программного обеспечения (операционных систем и систем управления базами данных). Основой для решения этих вопросов являются этапы инфологического и концептуального проектирования, которые позволяют обоснованно сформировать систему требований, определяющих желаемый облик создаваемой АС и ее технического и программного обеспечений. Только после того, как будут приняты основные проектные решения по составу и типам вычислительного комплекса, операционным системам и системам управления базами данных, специалисты по этим компонентам на основе концептуального проекта смогут приступить к логическому и физическому проектированию БД, а также к завершению разработки специального математического и программного обеспечений.

Схема, представленная на рисунке 1, иллюстрирует содержание и взаимосвязь этапов фазы моделирования, системного анализа и проектирования информационной базы. Реализация этой фазы основывается на разработке модели функционирования организационно-технической системы (ОТС), состоящей в структурном описании ее процессов и функций, и структурировании информационного содержания процессов, функций и задач (инфологическое и концептуальное проектирование СБД).

Модель функционирования ОТС в общем случае представляет собой максимально полное описание функциональных областей, процессов, функций, задач, документов и отрабатывающих их типов должностных лиц в процессе деятельности анализируемой ОТС. Модель функционирования служит основой для планирования процессов создания автоматизирован-

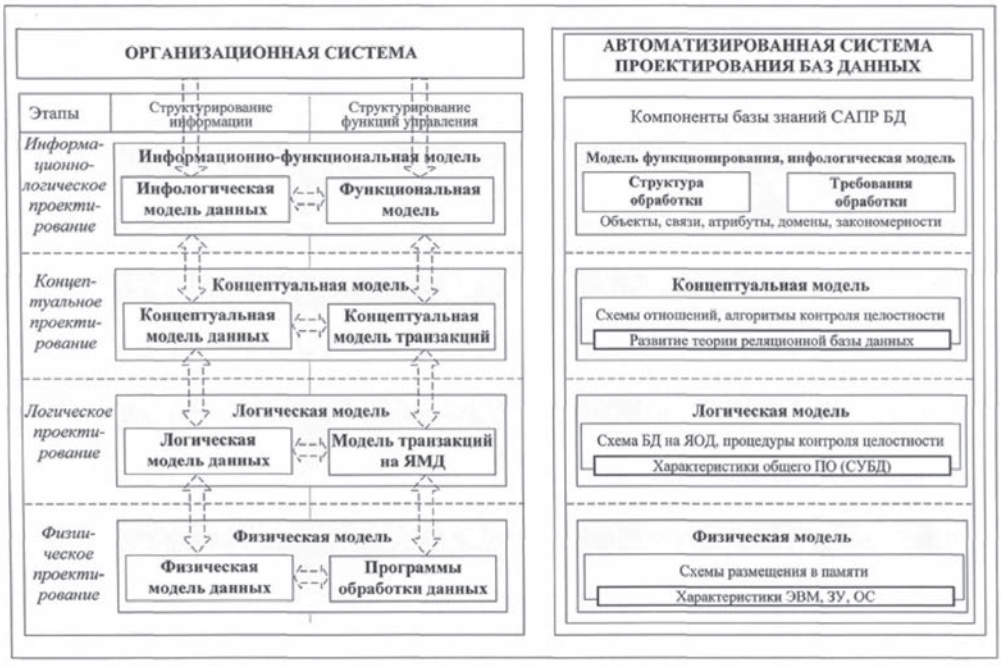


Рис. 1. Содержание и взаимосвязь этапов фазы системного анализа и проектирования информационной базы

ных систем, а также разработки их основных видов обеспечения.

Одним из результатов информационно-функционального анализа является инфологическая модель данных системы, соответствующая анализируемой части предметной области. Инфологическая модель данных формализуется семантической сетью в виде инфологического графа (ИЛГ) и описывается тройкой:

$$Мил=<Sил,Рил,Qил>,$$

где Sил – ИЛГ, включающий множество типов информационных объектов (сущностей) и их информационных связей, задаваемых именами своих типов и составом типов своих свойств (характеристик, атрибутов), а также множествами их значений; Рил – правила интерпретации инфологического графа данных; Qил – закономерности предметной области, существенные для контроля целостности и согласованности информационной модели.

Инфологическая модель (ИЛМ) данных обеспечивает первоначальную (предварительную) формализацию описания информационного содержания автоматизируемых процессов, согласовывая и объединяя в себе представления всех категорий пользователей. Основными критериями оценки качества ИЛМ являются её полнота и простота понимания, детальность, ясность и согласованность описания элементов.

Концептуальное проектирование имеет целью формирование обобщенной точки зрения на создаваемую информационную систему для всех категорий пользователей создаваемой автоматизированной системы, независимой от технических и системных программных средств, а также создание модели обработки данных (транзакций) в виде последовательности взаимосвязанных действий с базой данных в процессе её ведения.

Концептуальная модель (КМ) информационной системы понимается как математически точное формализованное описание элементов данных, их семантических связей и организационной структуры с указанием ограничений целостности и согласованности данных, а также соответствующих алгоритмов их контроля. Кроме того, КМ должна быть ясной и однозначно понимаемой, легко трансформируемой при изменении требований или появлении новых приложений. Перечисленным требованиям к описанию КМ наилучшим образом удовлетворяет расширенные и уточненные формальные средства описания реляционной модели данных [8]. В этом случае

$$Мк=<Sк,Рк,Qк>,$$

где Sк – схема модели реляционного типа; Рк – система операций реляционной алгебры; Qк – система алгоритмов, описывающих процедуры контроля целостности и согласованности модели.

Логическое проектирование состоит из двух взаимосвязанных процессов: проектирование логической модели БД (формулирование КМ на языке описания данных конкретной СУБД) и проектирование программ обработки данных (модели транзакций на языке манипулирования данными конкретной СУБД). В результате этого этапа разрабатывается логическая схема данных и структурированное описание обрабатывающих программ в терминах языковых средств конкретной системы управления данными.

Физическое проектирование состоит в определении способов размещения базы данных на носителях информации и в окончательной отладке программ обработки данных, специфицированных на предыдущих этапах. Результатом этого этапа является полностью готовая к внедрению система баз данных.

Итак, процесс проектирования СБД определяется как процесс преемственной последовательной трансформации и наследования свойств моделей различных уровней:

$$М_{ИЛ} \rightarrow М_К \rightarrow М_Л \rightarrow М_Ф,$$

где $М_Л$, $М_Ф$ – модели данных логического и физического уровней, имеющие соответствующие концептуальной модели компоненты.

Данный процесс целесообразно реализовывать в рамках единой интегрированной системы автоматизированного проектирования (САПР), позволяющей проектировщику СБД накапливать информацию, необходимую для проведения проектных расчетов, анализировать решения и запоминать их варианты, разрабатывать проектную документацию, возвращаться с любого последующего этапа на любой предыдущий в случае получения неудовлетворительных результатов, получать по запросам необходимую справочную информацию о состоянии проекта и т.п. Поэтому в ба-

зах данных САПР накапливаются метаданные (данные о данных, которые будут содержаться в разрабатываемых БД) создаваемой АС. Они играют роль *базы знаний*, которая может передаваться, использоваться и пополняться на стадиях опытной и практической эксплуатации АС. Созданная АС должна содержать в своих базах данных информацию о самой себе, которая необходима и может быть быстро доступна персоналу для решения возникающих проблем.

Заключение

Разработка концептуальных проектов систем БД основывается на анализе функционирования и структурном представлении информационных процессов функционирования конкретных организационно-технических систем. В результате такой деятельности выявляются, формализуются и систематизируются знания о деятельности автоматизируемых ОТС. При этом объем баз знаний определяется масштабами и задачами автоматизации.

СПИСОК ЛИТЕРАТУРЫ

1. Данилин А.В., Слюсаренко А.И. Архитектура предприятия. – М.: Интуит, 2007.

2. Марка Д, МакГоуэн К. Методология структурного анализа и проектирования. – М.: Метатехнология, 1993.

3. Мартин Дж. Организация баз данных в вычислительных системах. – М.: Мир, 1980.

4. Мартин Дж. Планирование развития автоматизированных систем. – М.: Финансы и статистика, 1984.

5. Тиори Т., Фрай Дж. Проектирование структур баз данных. – М.: Мир, 1985.

6. Гейн К., Сарсон Т. Структурный системный анализ: средства и методы. – М.: Эйтекс, 1993.

7. Ветошкин В.М. Основы теории концептуального проектирования баз данных для автоматизированных систем. – М: ВВИА им. проф. Н.Е. Жуковского, 1992.

8. Дейт, К. Дж. Введение в системы баз данных, 7-е издание.: Пер. с англ. – М: Издательский дом «Вильямс», 2001. – 1072 с.

9. Ветошкин В.М. Теоретические основы систем баз данных. – М: ВВИА им. проф. Н.Е. Жуковского, 2003.

10. Вендров А.М. Проектирование программного обеспечения экономических информационных систем. – М.: Финансы и статистика, 2000.

А.М. Виноградeнко
кандидат технических наук**, старший преподаватель кафедры технического обеспечения связи и автоматизации, ВАС**,

СПОСОБ РАСЧЕТА НЕОБХОДИМОГО ЧИСЛА КАНАЛОВ В МНОГОКАНАЛЬНОЙ ЛИНИИ СВЯЗИ

При решении задач промышленной экологии важное место отводится вопросам мониторинга безопасности промышленных объектов с помощью многоканальных измерительных систем, содержащих подсистемы сбора и обработки измерительной информации, линии связи и пункты диспетчерского управления. *Для экономии канального ресурса и достоверности переданной информации по многоканальным линиям связи представлен способ расчета необходимого числа каналов, основанный на применении методов теории передачи сигналов и методов теории массового обслуживания.* Оперативный контроль за технологическими объектами может быть выполнен в виде систем обслуживания заявок, представляющих собой многофазные системы массового обслуживания, *осуществляющих обнаружение и замеры отклонивши*хся параметров, их регистрации и приоритетный опрос датчиков, «снимающих» замеры с аппаратуры, что позволяет сократить потери информации.

Ключевые слова: устройства мультиплексирования, датчики, информационно-телеметрические системы, телеметрия, теория массового обслуживания.

Одной из проблем многоканальных измерительных систем является повышение эффективности использования дорогостоящих трактов передачи (линий связи). С этой целью в системах телеметрии, в которых предусматривается одновременная передача информации от большого числа датчиков, размещенных на одном и том же объекте, целесообразно использовать не только общую линию связи, но и групповые передатчики и приемники, осуществляющие соответственно преобразование сообщений в электрические сигналы (передаваемые по линии связи) и обратное преобразование последних в сообщения. При этом основной проблемой является оптимальное закрепление каналов за линиями связи (ЛС), осуществляемой с помощью устройств мультиплексирования (УМП). Одним из направлений решения указанной проблемы является моделирование процесса мультиплексирования разноприоритетных сообщений, то есть распределение каналов связи за потоками измерительной информацией с различной степенью важности [1,2].

Для современных информационно-телеметрических систем (ИТС) характерна работа в режиме решения потока случайных по своим характеристикам задач, поступающих в общем случае в случайные моменты времени. Случайность характерна и для отдельных подсистем, таких, как подсистема «датчик-контроллер-мультиплексор». Анализ и, самое главное, синтез подобных систем с учетом вероятностного характера протекающих в них процессов возможен методами теории массового обслуживания.

Передаваемый по тракту передачи групповой сигнал формируется из канальных сигналов, удовлетворяющих, как правило, условию линейной независимости или ортогональности. Объединение канальных последовательностей дискретных сигналов на принципах частотного разделения каналов, предполагает, что в результате образуется одна общая групповая последо-

вательность, в которой каждому каналу соответствует определенный частотный интервал.

Процесс поступления информации можно представить как случайный поток заявок (требований) на размещение очередного объема информации в одном из частотных диапазонов, а многоканальную линию связи как многоканальную (n-канальную) систему массового обслуживания (СМО) с неограниченной очередью. В этом случае, некоторые частотные интервалы многоканальной линии остаются незанятыми и простаивают некоторое время. Случайный характер потока заявок и времени обслуживания приводит к тому, что линия связи оказывается загруженной неравномерно: в какие-то периоды времени скапливается очень большое количество заявок, которые становятся в очередь на обслуживание (размещение в свободном частотном интервале). При полностью загруженных каналах заявки могут ждать обслуживания в общей очереди с числом мест m. В другие же периоды СМО работает с недогрузкой или простаивает. Поток заявок, поступающих в СМО, имеет интенсивность λ, а поток обслуживаний – интенсивность μ. Тогда $\mu = \frac{1}{t_{\text{обс}}}$, где $t_{\text{обс}}$ – время обслуживания одной заявки.

Одной из главных характеристик технических систем с передачей и переработкой информации является их помехоустойчивость, то есть способность системы противостоять воздействию посторонних возмущений (помех). Помехи в каналах связи представляют собой посторонние случайные электрические процессы, которые аддитивно суммируются с сигналом. Следовательно, учитывая воздействие помех, в случае ЧРК, на каждом частотном интервале будет своя помеховая обстановка.

Учитывая, что: $\overline{T}_{\text{об}} = N \cdot T_c$, где N – количество информационных символов в пакете; T_c – длительность информационного символа. При этом минимальное значение T_c определяется при решении обратной задачи расчета помехоустойчивости, то есть по допустимой вероятности ошибки приема сообщений $p_{ош.доп}$, заданным значениям мощности сигнала с элементом сообщения P_c, спектральной плотности шума $E_ш$ и т.д.

Для передачи дискретных сообщений используется определенный набор (ансамбль) k сигналов [3]. Под ошибкой будем понимать регистрацию вместо переданного сигнала $A_i(t)$ какого-либо другого сигнала $A_j(t)$, $i \neq j$. Явление ошибочной регистрации сигнала будем называть также искажением переданного сигнала. Обозначим вероятность искажения переданного сигнала $A_i(t)$: $P\left[A_j(t) \text{ вместо } A_i(t), j \neq i\right] = P_A \quad A_j \quad p_i = P_{A_i}\left(A_j\right) = p_i$. Помехоустойчивость дискретных каналов связи может быть оценена средней вероятностью ошибки $P_{\text{ош}}$ в канале связи, которая определяется формулами:

$$P_{\text{ош}} = \sum_{i=1}^{k} p(A_i) P_{A_i}\left(A_j\right), \qquad (1)$$

где $p(A_i)$ – априорная вероятность передачи сигнала $A_i(t)$,

$$p_{\text{ош}} = \frac{1}{2}\exp\left(-\frac{h^2}{2}\right);$$

$$h^2_{\text{доп}} = f\left(p_{\text{ош доп}}\right) = \frac{E_{\text{с}}}{E_{\text{ш}}} = \frac{P_{\text{с}} T_{\text{с}}}{E_{\text{ш}}}, \qquad (2)$$

где $h^2 = \frac{E}{N_0}$ – отношение энергии сигнала к спектральной плотности флуктуационной помехи.

При поступлении заявок в канал связи, с учетом помеховой обстановки (для ЧМ):

$$h^2_{\text{доп}} = \frac{P_{\text{с}} \cdot T_{\text{с}}}{E_{\text{ш}}} = -2\ln(2P_{\text{ош доп}}). \qquad (3)$$

Тогда, например, в случае некогерентного приема элемента сообщения:

$$T_c = -2\left(E_ш / P_c\right) \cdot \ln\left(2p_{ош.доп}\right). \qquad (4)$$

В уплотняемых каналах (особенно, если они используют различную среду распространения сигналов – воздушные либо кабельные линии, радиочастотные линии и т.д.) характеристики сигнала, шума и помех значительно различаются, следовательно, длительность информационного символа и соответственно время обслуживания заявки будут также иметь различные значения: T_{cj}, $\overline{T}_{\text{об } j}$ $\left(j = \overline{1,n}\right)$, где n – число каналов в системе связи. При этом предполагаем, что интенсивности обслуживания $\mu_j = 1/\overline{T}_{\text{об } j}$ распределены

по показательному закону. Таким образом, под каждый поток заявок с i-м уровнем приоритета формируется линия связи в составе n_i каналов, причем $\sum_{i=1}^{M} n_i = n$.

С учетом $\overline{T}_{\text{об}} = N \cdot T_c$, интенсивность обслуживания заявки:

$$\mu = \frac{1}{\overline{T}_{\text{об}}} = \frac{1}{N\,T_c} = \frac{P_{\text{с}}}{N\,h^2_{\text{доп}} E_{\text{ш}}}. \qquad (5)$$

Следовательно, время обслуживания заявки:

$$\overline{T}_{\text{об}} \geq N\,T_c = \frac{E_{\text{ш}} N}{P_c} h^2_{\text{доп}} \left(P_{\text{ош доп}}\right), \qquad (6)$$

где $\frac{E_{\text{ш}} N}{P_c} h^2_{\text{доп}} \left(P_{\text{ош доп}}\right)$ – нижняя граница для $\overline{T}_{\text{об}}$, следовательно

$$\overline{T}_{\text{об}} = -2N \frac{E_{\text{ш}}}{P_{\text{с}}} \ln\left(2P_{\text{ош доп}}\right). \qquad (7)$$

С учетом (5), (6) и (7) среднее время обслуживания одной заявки, относящееся ко всем заявкам, как обслуженным, так и ушедшим из очереди[4]:

$$\overline{T}^{\forall}_{\text{об}} = -2N\,p_{\text{об}} \frac{E_{\text{ш}}}{P_{\text{с}}} \ln\left(2P_{\text{ош доп}}\right). \qquad (8)$$

Так как, вероятность $p_{\text{об}}$ представляет собой относительную пропускную способность Q, то:

$$Q = -\frac{\overline{T}^{\forall}_{\text{об}} P_{\text{с}}}{2N\,E_{\text{ш}} \ln\left(2P_{\text{ош доп}}\right)}. \qquad (9)$$

Среднее время пребывания заявки в системе можно вычислить по формуле

$$\overline{T}_{\text{сист}} = \overline{T}_{\text{оч}} + \overline{T}^{\forall}_{\text{об}}, \qquad (10)$$

где $\overline{T}^{\forall}_{об}$ – среднее время обслуживания одной заявки, относящееся ко всем заявкам, как обслуженным, так и ушедшим из очереди, которое можно подсчитать по формуле:

$$\overline{T}^{\forall}_{\text{об}} = p_{\text{об}} + \overline{T}_{\text{об}} = Q / \frac{P_{\text{с}}}{Nh^2\varepsilon_0^2}. \quad (11)$$

Если использовать (11), то из (9) получим:

$$\overline{T}^{\forall}_{\text{об}} = -2N \times \left[\begin{cases} p_0 \sum_{k=0}^{n-1} \frac{\rho^k}{k!}, \text{если } 0 < \overline{T}_{\text{ож}} < \frac{1}{n\mu}, \\ p_0 \sum_{k=0}^{n} \frac{\rho^k}{k!}, \text{если } \frac{1}{n\mu} \leq \overline{T}_{\text{ож}} < \frac{2}{n\mu}, \\ p_0 \sum_{k=0}^{n} \frac{\rho^k}{k!} + \\ + \frac{1}{n!} \sum_{k=n+1}^{n+i-2} \frac{\rho^k}{(n+\beta)(n+2\beta)\ldots\left[n+(k-n)\beta\right]}, \\ \text{если } (i-1)/(n\mu) \leq \overline{T_{\text{ож}}} < i/(n\mu), i \geq 3. \end{cases}\right] \times \qquad (12)$$

$$\times \frac{E_{\text{ш}}}{P_{\text{с}}} \ln\left(2P_{\text{ош доп}}\right).$$

Среднее число занятых каналов (среднее число заявок, находящихся под обслуживанием), можно получить по определению относительной пропускной способности и, так как $Q = \frac{A}{\lambda}$:

$$\overline{K} = \overline{N}_{\text{об}} = \frac{A}{\mu} = \frac{Q\lambda}{\mu} = Q\rho, \qquad (13)$$

то, с учетом (9) и при наличии помеховой обстановки, расчет числа каналов, необходимых для обеспечения требуемой пропускной способности, производится по выражению:

$$\overline{K} = \overline{N}_{\text{об}} = -\frac{\overline{T}^{\forall}_{\text{об}} P_{\text{с}}}{2NE_{\text{ш}} \ln\left(2P_{\text{ош доп}}\right)} \rho. \qquad (14)$$

С учетом (1) и (8) для различных состояний СМО на момент прихода заявки данное выражение можно привести к виду:

$$\overline{K} = \overline{N}_{\text{об}} = \left(\left[\begin{cases} p_0 \sum_{k=0}^{n-1} \frac{\rho^k}{k!}, \text{если } 0 < \overline{T}_{\text{ож}} < \frac{1}{n\mu}, \\ p_0 \sum_{k=0}^{n} \frac{\rho^k}{k!}, \text{если } \frac{1}{n\mu} \leq \overline{T}_{\text{ож}} < \frac{2}{n\mu}, \\ p_0 \sum_{k=0}^{n} \frac{\rho^k}{k!} + \frac{1}{n!} \sum_{k=n+1}^{n+i-2} \times \\ \times \frac{\rho^k}{(n+\beta)(n+2\beta)\ldots\left[n+(k-n)\beta\right]}, \\ \text{если } (i-1)/(n\mu) \leq \overline{T_{\text{ож}}} < i/(n\mu), i \geq 3. \end{cases}\right] + NT_{\text{с}}\right) P_{\text{с}} = \qquad (15)$$

$$= -\frac{}{2NE_{\text{ш}} \ln\left(2P_{\text{ош доп}}\right)} \rho.$$

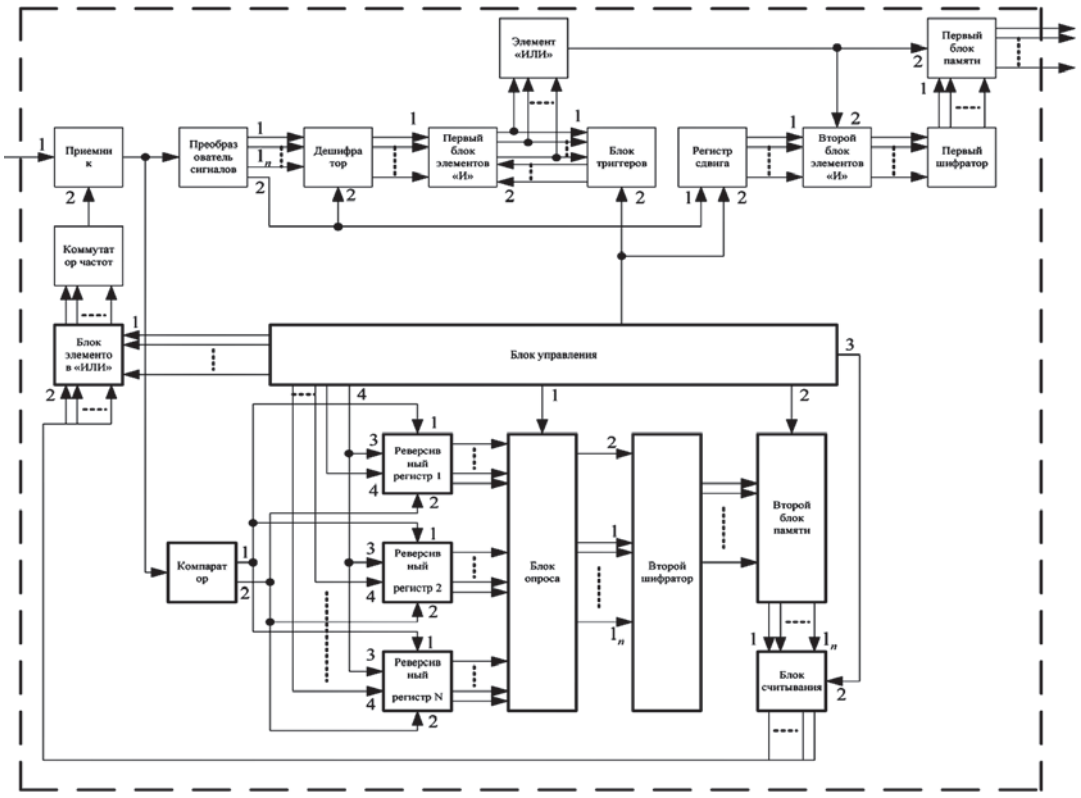


Рис. 1 Устройство автоматического поиска каналов радиосвязи

Таким образом, формула (15) позволяет производить расчет необходимого числа каналов связи в телеметрических системах с учетом помеховой обстановки, необходимых для обеспечения требуемой пропускной способности и достоверности переданной информации по линии связи.

Выбор оптимального КС осуществляет устройство автоматического поиска каналов радиосвязи (УАПКС) (рисунок 1), обеспечивающее увеличение достоверности выбора оптимального канала, за счет двухэтапного анализа [5].

СПИСОК ЛИТЕРАТУРЫ

1. Виноградено А.М. Разработка способа прогнозирования предаварийного состояния технологических объектов. СПбНТОРЭС, 66-я НТК, 2011 г., с.161-162.

2. Назаров А.В., Козырев Г.И., Шитов И.В. и др. Современная телеметрия в теории и на практике. Учебный курс. СПб.: Наука и Техника, 2007. 672 с.

3. Зюко А.Г., Кловский Д.Д., Коржик В.И., Назаров М.В. Теория электрической связи. Под ред. Кловского Д.Д. М.: Радио и связь, 1999. 432 с.

4. Крайников А.В., Кудриков Б.А. и др. Вероятностные методы в вычислительной технике. / Под ред. А.Н. Лебедева, Е.А. Чернявского М.: Высш. шк., 1986. 312 с.

5. Будко Н.П., Виноградено А.М., Федоренко И.В. Устройство автоматического поиска каналов радиосвязи. Патент №2450447, 2012 г.

П.А. Глыбовский
кандидат технических наук, доцент, ВКА им. А.Ф.Можайского

А.М. Зыков
кандидат технических наук, ВКА им. А.Ф.Можайского

П.В. Мажников
кандидат технических наук, доцент, ВКА им. А.Ф.Можайского

МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ИСПОЛЬЗОВАНИЕМ МЕЖДУНАРОДНОЙ АССОЦИАЦИИ СЕТЕЙ ИНТЕРНЕТ

В данной статье рассмотрены меры обеспечения информационной безопасности электронного документооборота с использованием средств электронной подписи. Изложенные ниже рекомендации будут полезны как для организаций, имеющих единственную локальную вычислительную сеть, так и для организаций, использующих глобальные вычислительные сети общего пользования.

Интенсивное развитие информационных технологий и проникновение их практически во все сферы общественной жизни, ежедневно возрастающий объем информации, которую надо обработать в минимально возможный срок, а также еще очень и очень много различных факторов обусловили необходимость в настоящее время практически каждому иметь доступ к глобальным информационным ресурсам.

В рамках федеральной целевой программы «Электронная Россия» планируется использовать информационно-коммуникационные технологии в деятельности органов государственной власти, осуществляется развитие системы электронного документооборота (ЭДО), локальных информационных сетей, использование стандартов делопроизводства и документооборота.

Электронный документооборот должен сопровождаться различными организационно-техническими мерами, позволяющими защитить передаваемые по сетям электронные документы, как от несанкционированного доступа, так и от случайной или преднамеренной модификации [1,2]. Наиболее остро вопрос защиты ЭДО стоит для организаций, имеющих территориально-распределенную структуру. Такие организации могут иметь несколько локальных вычислительных сетей (ЛВС), расположенных в разных местах, в том числе в различных регионах России, и вынуждены использовать для передачи информации различные неконтролируемые глобальные вычислительные сети (ГВС) общего пользования, например, международную ассоциацию сетей Интернет.

В общем случае выделяют следующие меры обеспечения информационной безопасности ЭДО с использованием средств электронной подписи [3]:

- обеспечение безопасности ключа электронной подписи (ЭП) и ключевых носителей ЭП;
- соблюдение регламента ограниченного доступа к компьютеру, подключенного к ЭДО;

• использование лицензионного программного обеспечения (ПО);

• использование и оперативное обновление системного и прикладного ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ и недекларируемых возможностей;

• использование и оперативное обновление специализированного ПО обеспечения информационной безопасности;

• соблюдение правил безопасной работы в ГВС.

К мерам обеспечения информационной безопасности ЭДО с использованием ГВС относятся:

1. Обеспечение безопасности ключа ЭП и ключевых носителей ЭП.

Для хранения ключа ЭП небходимо использовать только внешние носители (дискеты или “eToken”), а не жёсткие/сетевые диски компьютера. Владелец ключа ЭП должен хранить его в условиях, исключающих доступ к нему третьих лиц (использовать для хранения сейф). Нельзя размещать пароли в видимой зоне вблизи компьютера (например, записывать пароли на листах бумаги, приклеенных к дисплею рабочего компьютера). В случае потери ключа ЭП или утраты пароля, необходимо немедленно сообщить об этом в удостоверяющий центр, выдавший ключевые документы.

Нельзя использовать носители с ключами ЭП для каких-либо других целей (в частности, не хранить на них любую другую информацию). Необходимо извлекать носители с ключами ЭП из компьютера каждый раз после завершения их использования (т.е. носители с ключами ЭП должны находиться в компьютере только в период подписания электронных документов в ЭДО).

2. Соблюдение регламента ограниченного доступа к компьютеру, подключенному к ЭДО.

Следует строго соблюдать регламент ограниченного доступа к компьютеру, используемому для работы с ЭДО.

Любой физический доступ к компьютеру – это потенциальная возможность подключения отчуждаемого носителя (дискеты, компакт-диска, USB-накопителя) и, как следствие, возможность привнесения на компьютер вредоносной программы (вируса, трояна и т.п.).

Любой физический доступ к компьютеру – это потенциально неконтролируемая работа в ГВС, и, как следствие, возможность случайной или намеренной загрузки вредоносной программы. Поэтому необходимо придерживаться следующих правил, позволяющих обеспечить контролируемый физический доступ к компьютеру, с которого осуществляется работа в ЭДО:

• право доступа к рабочим местам, с которых осуществляется работа с ПО ЭДО должно предоставляться лицам, непосредственно осуществляющим работу с ЭДО;

• доступ посторонних лиц в помещения с рабочими местами ЭДО должен осуществляться под контролем сотрудника службы безопасности организации;

• не следует оставлять без контроля рабочие места ЭДО. При кратковременном отсутствии необходимо: сохранить все открытые на редактирование документы; средствами операционной системы или средствами защиты информации от НСД заблокировать рабочее место;

• для исключения возможности несанкционированного изменения аппаратной части системный блок и разъемы рабочих мест ЭДО должны опечатываться сотрудником службы безопасности организации и, при каждом включении должна проверяться их целостность;

• на рабочих местах ЭДО следует использовать только лицензионное программное обеспечение;

• на рабочих местах ЭДО должны быть отключены: загрузка с внешнего носителя, загрузка по сети, если внутренним регламентом организации не предусмотрено иное;

• вход в BIOS рабочих мест ЭДО должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору безопасности информации или другому лицу в соответствии с внутренним регламентом организации;

• для всех учетных записей в операционной системе должны использоваться пароли, удовлетворяющие следующим требованиям: длина пароля не менее 8 символов; в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы; периодичность смены пароля определяется политикой безопасности организации, но не должна превышать одного года;

• количество неудачных попыток входов в систему должно быть ограничено в соответствии с политикой безопасности, принятой в организации. Рекомендуется блокировать систему после трех неудачных попыток;

• должна быть отключена учетная запись для гостевого входа (Guest);

• должно быть исключено использование режима автоматического входа пользователя в операционную систему при ее загрузке;

• должны быть отключены режимы отображения окна всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей;

• в случае обнаружения на рабочих местах ЭДО незарегистрированных программ, нарушения целостности операционной системы, либо выявления факта повреждения печатей на системных блоках, работа должна быть прекращена;

• для защиты от несанкционированного доступа к рабочим местам ЭДО из внешней сети рекомендуется использовать антивирусное ПО, персональный межсетевой экран и средства защиты информации от НСД.

3. Использование лицензионного ПО.

Установка и обновление системного и прикладного ПО (операционная система, браузеры, почтовые клиенты, офисные программы, бухгалтерские программы и пр.) из ненадежных источников приводит к проникновению на компьютер вредоносных программ, в том числе троянов. Следует использовать программное обеспечение только из надежных доверенных источников.

Если это коммерческие программы – Microsoft Windows, Microsoft Office, 1С:Бухгалтерия и пр. – они должны быть легально приобретены клиентом и установлены с легального дистрибутива, гарантирующего отсутствие вредоносных программ. Если это свободно распространяемые программы – Linux, Firefox, Thunderbird, Java и пр. – они должны быть получены на компакт-диске из доверенного источника или загружены через ГВС с публичных сайтов разработчиков с использованием механизмов обеспечения целостности загружаемого ПО.

4. Использование и оперативное обновление системного и прикладного ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ и недекларируемых возможностей.

Оперативное обновление системного и прикладного ПО на компьютере– это необходимое условие для снижения рисков заражения компьютера вредоносными программами, в том числе троянами, через новые выявленные уязвимости и ошибки в используемых клиентом программах.

5. Использование и оперативное обновление специализированного ПО обеспечения информационной безопасности.

Для защиты от вредоносных программ в первую очередь необходимо использовать и оперативно обновлять на своем компьютере специализированные программы для обеспечения информационной безопасности - сертифицированное антивирусное ПО, применять персональные межсетевые экраны и средства защиты информации от НСД.

Минимально необходимый набор на компьютере– это антивирусное ПО + персональный межсетевой экран (firewall) + СЗИ от НСД.

6. Соблюдение правил безопасной работы в сети ГВС.

Наиболее надежным способом обеспечения безопасности данных при работе в ЭДО является использование компьютера только для работы с указанной системой и исключение случаев использования применяемого компьютера для каких-либо других задач.

Вне зависимости от того, используется ли компьютер, применяемый для работы в ЭДО для каких-либо иных целей, необходимо соблюдение следующих правил безопасности:

• обращать особое внимание на отправителя почтовой корреспонденции при работе с электронной почтой, вне зависимости от того, выполняется работа с почтой через Web-интерфейс одной из известных почтовых систем mail.ru, yandex.ru и т.п., или в локально установленных программах типа Outlook, Outlook Express, The Bat! Не открывать вложение письма, что бы ни содержало данное сообщение, если отправитель почтового сообщения вам неизвестен;

• при использовании служб мгновенного обмена сообщениями – ICQ, Instant Messaging, Mail.ru-агент и т.д. необходимо соблюдать рекомендации аналогично работе с почтовыми кли-

ентами – не принимать файлы из неизвестных источников, к файлам из известных источников относиться с осторожностью. Проверять все полученные файлы антивирусными программами;

• не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях;

• не допускать использования компьютера для посещения сайтов сомнительного содержания. Зачастую такие сайты содержат вредоносные программы, загружаемые и запускаемые при входе на сайт;

• немедленно вызывать администратора безопасности информации при любом подозрении, заражения компьютера (неадекватная реакция на действия пользователя, самостоятельная активность, появляющиеся непонятные окна и т.п.).

СПИСОК ЛИТЕРАТУРЫ

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства/ – М.: ДМК Пресс, 2010. – 544 с.: ил.

2. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи».

К. А. Деньжонков
кандидат технических наук

А. В. Кий
кандидат технических наук
Россия, г. Санкт-Петербург, Военная академия связи

АНАЛИЗ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПУНКТА УПРАВЛЕНИЯ ОБЪЕДИНЕНИЯ

Рассматриваются состав и возможности вычислительной сети пункта управления объединения, а также системы резервного копирования и восстановления информации. Указаны особенности данных сетей, обуславливающие повышенные требования к ним. Представлено описание процесса резервирования данных. Отмечены недостатки присущие существующей системе резервного копирования.

Одним из основных направлений развития системы управления Вооруженных Сил Российской Федерации является автоматизация деятельности органов военного управления. Исследования показывают, что при равенстве сил и средств сторон, достижение превосходства над противником за счет совершенствования системы управления (прежде всего за счет автоматизации процессов управления) может достичь 25% и более [1].

Для эффективного управления войсками и силами необходимо решение возникающих задач в реальном масштабе времени, широкое использование средств автоматизации, баз данных, комплексов прикладных программ, документооборот в электронном виде, применение цифровых карт и геоинформационных систем, а также обеспечение видеоконференцсвязи.

Должностные лица (ДЛ) органов военного управления все активнее используют информационные средства поддержки принятия решения и различные модели для оценки обстановки, а также проверки и выбора рационального варианта решения при планировании боевых действий [2].

В таких условиях значительную помощь по предоставлению и обработке информации могут оказать вычислительные сети, которые являются одним из основных компонентов автоматизированных систем управления (АСУ).

Вычислительные сети военного назначения (ВС ВН) имеют ряд особенностей, отличающих их от других вычислительных сетей:

1. Информация, обрабатываемая в ВС ВН, может носить характер военной или государственной тайны и может иметь различный гриф секретности. В связи с этим организация информационного процесса в ВС ВН регламентируется приказами, руководствами, наставлениями и другими руководящими документами МО РФ.

2. Сосредоточение в отдельных элементах ВС ВН значительных объемов информации различного назначения, принадлежности и грифа секретности.

3. ВС ВН подвержены риску деструктивного воздействия со стороны противника.

4. Информационный процесс, протекающий в ВС ВН, претерпевает значительные изменения в зависимости от степени боевой готовности соответствующих органов военного управления и условий их функционирования. В связи с этим интенсивность потоков информации в ВС ВН может изменяться, что должно учитываться при резервировании.

5. Личный состав, допущенный к работе в ВС ВН, имеет различные степени допуска к обрабатываемой информации и выполняет различные функции. В связи с этим возникает необходимость в разграничении доступа в соответствии с функциональными обязанностями ДЛ и обеспечении защиты информации от несанкционированного доступа со стороны внутренних пользователей.

6. В случае возникновения вооруженного конфликта, необходимо обеспечить устойчивое и непрерывное управление, то есть возможность передачи управления с одного пункта управления (ПУ) на другой, а также резервирование данных.

Поэтому к АСУ, построенным на основе ВС ВН, по сравнению с автоматизированными системами общего назначения предъявляется более жесткие требования по обеспечению надежного функционирования, целостности и сохранности информации.

Однако средства резервного копирования информации и ее восстановления (РКВИ), входящие в состав ВС ПУ различных звеньев, имеют ряд недостатков, которые не позволяют обеспечить оперативное резервирование и восстановление информации.

Рассмотрим состав ВС повседневного ПУ объединения и порядок создания резервной копии данных, расположенных на автоматизированных рабочих местах (АРМ) ДЛ.

АСУ объединения представляет собой совокупность комплексов средств автоматизации (КСА), построенных на основе ВС ВН и предназначенных для оснащения штабов и стационарных пунктов управления, и функционально-технологических систем, объединенных в единую информационно-техническую структуру на основе существующей системы связи объединения.

КСА ПУ объединения включает [3]:

1. АРМ ДЛ оперативного состава, которые позволяют в автоматизированном режиме выполнять функциональные обязанности по управлению войсками.

2. АРМ удаленного объекта управления для удаленного автоматизированного по управления войсками.

3. Сервер единого времени обеспечивает автоматизированную привязку формируемой шкалы к Российской системе единого времени или международной системе единого времени, а так же передачу информационных пакетов с указанием и без указания оперативного времени.

4. Сервер регламентной обработки данных предназначен для хранения управляющей информации, документов и их атрибутов, базы данных пользователей, перенаправления документов в соответствии с управляющей информацией;

5. Сервер функциональных групп предназначен для хранения информации, используемой внутри группы, зависящей от организационной структуры объекта установки КСА, выполнения серверных приложений, необходимых для данной функциональной группы.

6. Сервер вычислительного комплекса обеспечивает связи между АРМ КСА и АСУ военного округа по специальному протоколу, функционирование комплексов программных средств.

7. Многопротокольный коммутатор пакетов обеспечивает прием данных из локальной вычислительной сети КСА ПУ объединения (АРМ-У и выносного АРМ) и передачу их по каналам связи.

8. Комплекс программно-технических средств защиты информации обеспечивает контроль и управление функционированием средств защиты информации на всех АРМ и серверах КСА.

9. Система управления функционированием обеспечивает контроль и устойчивое функционирование КСА, контроль трактов обмена информации, сбор, накопление и выдачу информации о состоянии технических средств КСА.

10. Система резервного копирования и восстановления и информации обеспечивает создание резервных копий данных АРМ ДЛ и серверов и их восстановление в случае отказа или потери данных. В состав системы РКВИ входит специальное рабочее место (технологическое), не подключенное к ВС, но имеющее дополни-

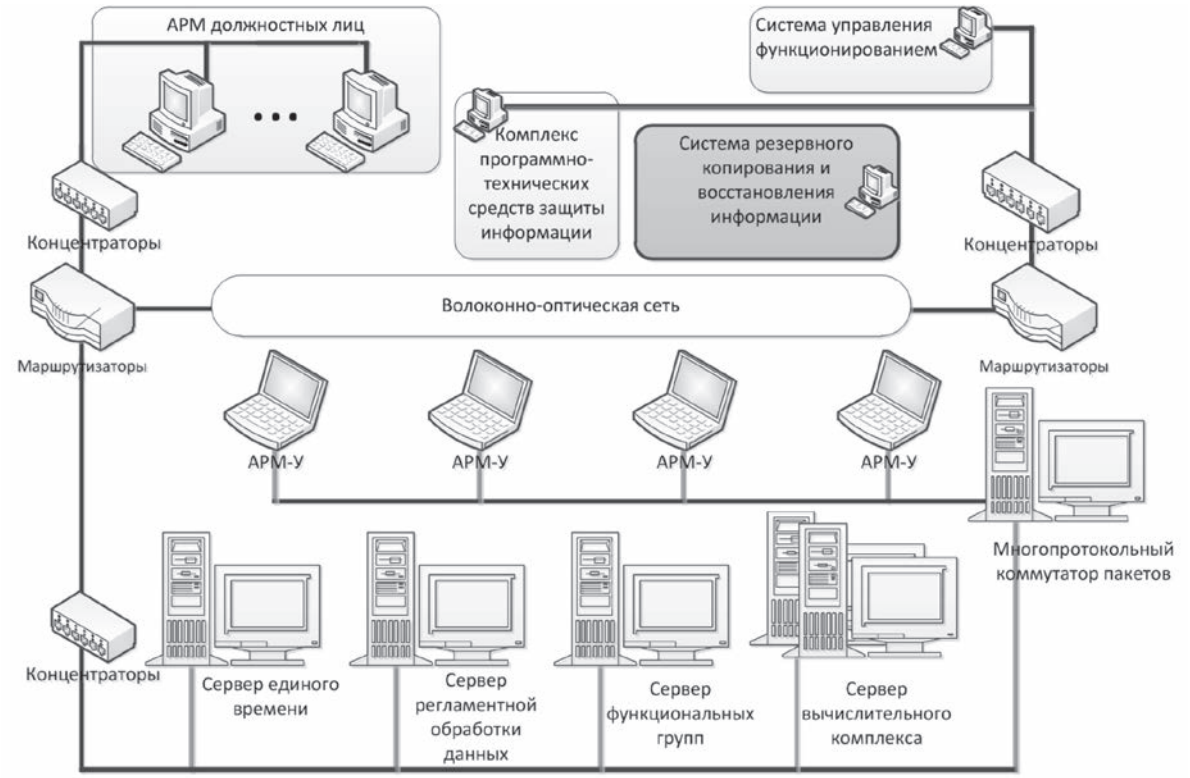


Рис. 1. Схема взаимодействия элементов КСА ПУ объединения и место системы РКВИ (вариант)

тельные технологические разъемы для подключения жестких дисков АРМ ДЛ. Администратор ВС на данном рабочем месте осуществляет снятие резервных копий, восстановление данных, а также подсчет контрольных сумм.

Схема взаимодействия компонентов КСА ПУ объединения и место системы РКВИ представлены на рис. 1.

В настоящее время для резервного копирования и восстановления необходимых данных (планового или вынужденного) администратору ВС, приходится выполнять следующую последовательность действий [3].

1. Прибытие администратора сети в помещение, где расположено АРМ ДЛ. Так как ВС ПУ объединения может занимать значительное место в пространстве, то АРМ и сервера могут находиться достаточно далеко друг от друга. Это потребует временных затрат на перемещение администратора сети. При этом администратор будет вынужден покинуть штатное рабочее место.

2. Отключение питания АРМ ДЛ. ДЛ не участвует в процессе автоматизированного управления войсками на время резервного копирования.

3. Извлечение из АРМ ДЛ жесткого диска для резервирования данных.

4. Прибытие администратора с жестким диском АРМ ДЛ в помещение, где установлено технологическое рабочее место системы РКВИ.

5. Отключение питания технологического рабочего места.

6. Установка жесткого диска АРМ ДЛ в системный блок технологического рабочего места.

7. Включение питания технологического рабочего места. Загрузка операционной системы.

8. Запуск программы резервного копирования.

9. Создание образа данных, расположенных на АРМ ДЛ, и сохранение их на жестком диске технологического рабочего места;

10. Подсчет контрольной суммы, созданного образа данных. Сравнение полученной контрольной суммы с первоначальной (если копирование этого набора данных уже имело место).

11. Отключение питания технологического рабочего места.

12. Извлечение жесткого диска АРМ ДЛ из системного блока технологического рабочего места.

13. Прибытие администратора сети с жестким диском в помещение, где расположено АРМ ДЛ.

14. Установка жесткого диска в системный блок АРМ ДЛ.

15. Включение питания АРМ. Загрузка операционной системы.

Как видно из описанной последовательности действий процесс резервного копирования информации АРМ и серверов ВС, развернутых в настоящее время на стационарных ПУ объединений, мало автоматизирован и не может быть выполнен удаленно – по сети. К недостаткам существующей системы РКВИ также можно отнести значительные временные затраты на создание копий данных и их восстановление, перерывы в работе ДЛ, на АРМ которых выполняется копирование/восстановление данных, невозможность одновременного создания нескольких копий с различных АРМ, отвлечение администратора от управления комплексом и его убытие со штатного места. Необходимо также учесть, что количество рабочих мест объектов автоматизации может быть значительным (до 200), которые могут быть размещены на нескольких этажах, в разных зданиях, на различных территориях. В случае проведения оперативных мероприятий, когда расписание создания копий данных может потребовать ежедневного резервирования, реализовать надежное копирование данных станет практически невозможным.

В связи с этим актуальными представляются вопросы совершенствования существующих средств РКВИ.

СПИСОК ЛИТЕРАТУРЫ

1. Курс лекций «Теоретические основы автоматизации управления войсками и связью». СПб.: ВАС.

2. Малюков В.А. Современным войскам – современную связь. Связь в Вооруженных Силах Российской Федерации – 2013. Тематический сборник. М.: «Информационный мост», 2013.

3. Эксплуатационная документация КСА.

К. А. Деньжонков
кандидат технических наук
К. А. Чирушкин
кандидат технических наук
Россия, г. Санкт-Петербург, Военная академия связи

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА КОМПЛЕКСНОГО ОСНАЩЕНИЯ УЗЛА СВЯЗИ

Рассматриваются объекты комплексного оснащения Объединённой автоматизированной цифровой системы связи и их система защиты информации. Отмечены возможные проблемы безопасности информации на указанных объектах. Представлены предложения по развитию системы защиты информации.

В настоящее время завершается этап оснащения узлов связи Министерства Обороны Российской Федерации объектами комплексного оснащения, которые представляют собой комплекс программно-технических средств для обеспечения функционирования Объединённой автоматизированной цифровой системы связи (ОАЦСС) ВС РФ [1].

Система связи, построенная на основе модернизированных узлов связи, позволит обеспечить создание линейных трактов между узлами связи пунктов управления и на линиях привязки к узлам доступа единой сети электросвязи (ЕСЭ) РФ, сопряжение с оборудованием цифровых систем передачи ЕСЭ РФ, коммутацию и маршрутизацию цифровых потоков, а также предоставление набора телематических служб.

Сеть обеспечивает безопасность информации, включая шифрование информации, передаваемой по каналам связи, защиту информации от НСД и технических средств разведки.

Таким образом, развернутая сеть отвечает требованиям, предъявляемым к системам управления войсками, использует современные протоколы обмена информацией и обеспечивает современные услуги должностным лицам пунктов управления ВС РФ [1].

Оборудование объекта комплексного оснащения разделяется на открытый и закрытый сегменты сети [2].

В состав оборудования открытого сегмента входят:

пограничный маршрутизатор узла;

шлюз VOIP телефонии;

цифровая автоматическая телефонная станция (АТС) открытого сегмента (с рабочим местом оператора);

сервер общего назначения (электронной почты, точного времени, доменных имен, гипертекстовой обработки данных);

сервер технологического управления (может устанавливаться совместно с сервером общего назначения);

рабочее место администратора открытого сегмента сети;

локальная вычислительная сеть открытого сегмента.

В состав оборудования закрытого сегмента входят:

криптомаршрутизатор;

межсетевой экран;

шлюз VOIP телефонии закрытого сегмента;

цифровая АТС закрытого сегмента (с рабочим местом оператора);

основной сервер общего назначения;

резервный сервер общего назначения;

автоматизированные рабочие места администратора технологического управления и администратора обеспечения безопасности информации;

локальная вычислительная сеть закрытого сегмента.

Программное обеспечение объектов комплексного оснащения строится на базе применения отечественных защищенных программно-аппаратных средств, которые служат базой для построения интегрируемых защищенных автоматизированных телекоммуникационных систем МО РФ.

Структура программного обеспечения объектов комплексного оснащения включает следующие составляющие [3]:

защищенную операционную систему;

защищенную систему управления базами данных;

программные средства общего применения (обеспечения повседневной деятельности, распределенной гипертекстовой обработки данных, средств разработки приложений, средств обмена информацией, средств технологического управления и т.д.);

средства защиты информации.

Для обеспечения защиты информации на узлах связи объектов комплексного оснащения предусмотрена система защиты, состоящая из совокупности аппаратного и программного обеспечения, позволяющая обеспечить возможность обмена и обработки информации, содержащей сведения государственной тайны. Система защиты включает [2, 3]:

шифрование потоков данных IP-пакетов и скрытие состава оборудования закрытого сегмента;

установка на автоматизированные рабочие места (АРМ) должностных лиц (ДЛ) аппаратно-программного модуля доверительной загрузки;

система защиты информации защищенной операционной системы;

комплекс программных средств антивирусной защиты;

комплекс средств защиты от несанкционированного доступа;

комплекс средств защиты информации от случайных воздействий и аварийных ситуаций;

программное средство системы обнаружения вторжений.

Так как со временем количество различных типов и способов организации несанкционированных проникновений в автоматизированные системы будет только увеличиваться, то остается актуальным вопрос развития и совершенствования средств защиты информации, в том числе и развернутых на объектах комплексного оснащения несмотря на то, что на данный момент они соответствуют предъявляемым требованиям. Одним из основных направлений развития защиты информации на объекте комплексного можно считать развитие систем обнаружения вторжений.

Это также подтверждается разглашением сведений о программе PRISM в июне 2013 года. Директор Национальной разведки США Джеймс Клеппер подтвердил существование PRISM, принятой Агентством национальной безопасности США, и заявил, что программа работает в соответствии с законом об иностранной разведке, недавно пересмотренным Конгрессом США. PRISM описывается как комплекс административных мер, предоставляющих возможность углубленного наблюдения за интернет-трафиком пользователей некоторых ресурсов. PRISM дает право Агентству получать самую разнообразную информацию: просматривать электронную почту, прослушивать голосовые и видеочаты, просматривать фотографии, видео, отслеживать пересылаемые файлы, узнавать другие подробности из социальных сетей [4].

Можно сделать вывод, что подобные средства функционируют и с целью наблюдения и раскрытия информации, обрабатываемой ДЛ пункта управления с использованием программно-технических средств объекта комплекса оснащения. В настоящее время разработано большое количество средств выявления несанкционированных проникновений в сети и аномалий в трафике, различающихся по эффективности и области применения. Однако практически все эти средства разработаны зарубежными производителями и не могут быть напрямую использованы на объектах комплексного оснащения. Установленная система обнаружения вторжений изготовлена отечественным научно-исследовательским институтом, однако она имеет ряд недостатков, что обуславливает актуальность разработки предложений по ее совершенствованию.

Основные предложения в развитии систем обнаружения вторжений на наш взгляд сводятся к следующим.

Так как в процессе анализа трафика и состояния сети агенты собирают и обрабатывают большое количество информации, появляется

необходимость определения информации, которая должна храниться в журналах регистрации, и способа её сбора для более эффективного управления любой системой обнаружения вторжений.

Определение наилучшей структуры и формата хранения регистрационных данных, чтобы они могли быть быстро обработаны, не требуя больших объемов памяти для хранения и обработки. Формат в защищенной операционной системе не позволяет напрямую работать с другими программными средствами, в связи с чем, система обнаружения вторжений вынуждена создавать документы в определенном формате.

Перемещение обработанных данных центральной консоли ближе к фактическому источнику данных. Для улучшения защиты информации, устанавливается больше количество сенсоров и датчиков, что приводит к снижению производительности и увеличение времени обработки данных.

Так как обмен между агентами и сервером системы обнаружения вторжений осуществляется по защищенным каналам связи, то необходимо распределять ключи между АРМ объекта. Необходима разработка руководящего документа по порядку передачи от сервера к АРМ закрытого ключа и сертификата сервера системы обнаружения вторжений.

Создание дополнительных способов извещения администратора системы обнаружения вторжений об атаках и аномалиях в сетевом трафике. В связи с необходимостью администратора периодически покидать место несения дежурства предлагается организовать оповещение не только по средствам отправки информации на управляющую консоль, но и с помощью электронной почты, телефонной связи, рассылкой оповещений на мобильный телефон администратора.

Для улучшения качества отслеживания и обнаружения возможных/производимых атак необходимо произвести расширение перечня контролируемых событий (расширение набора сенсоров), а также расширение перечня подтипов и параметров для известных событий.

Сервер системы обнаружения вторжений находится в закрытом сегменте, в то время как открытый сегмент остается незащищенным. Важным шагом по повышению защищенности информации является установка системы и в открытом сегменте.

СПИСОК ЛИТЕРАТУРЫ

1. Курс лекций «Эксплуатация узлов связи соединений МО РФ нового облика». СПб.: ВАС.

2. Назначение, состав и основные возможности узла связи объекта комплексного оснащения. Учебное пособие для оператора телекоммуникационной сети МО РФ. Москва, 2011.

3. Эксплуатационная документация ОКО.

4. Robert O'Harrow Jr., Ellen Nakashima, Barton Gellman U.S., company officials: Internet surveillance does not indiscriminately mine data. The Washington Post (8 June 2013).

Дудаков Н.С.,
инженер-программист, ОАО «Концерн «Системпром»

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ХРАНЕНИЕМ ДАННЫХ АСУ ВКО

В работе рассматриваются вопросы проектирования системы хранения данных для АСУ ВКО. Предложена методика оценки и повышения эффективности систем хранения данных. Разработан прототип системы, предназначенной для обработки разнородных данных.

В настоящее время невозможно переоценить важность автоматизированных систем управления (АСУ) во всех аспектах информационной деятельности. Одной из важнейших сфер применения АСУ является процесс управления вооруженными силами (ВС), обеспечивающими безопасность государства. В свою очередь, анализ современных вооруженных конфликтов показывает особую значимость авиации и противовоздушной (противоракетной) обороны.

Создание современной эффективной системы воздушно-космической обороны невозможно без автоматизации процессов управления войсками, силами и средствами ВКО во всех звеньях системы управления. Превосходство в получении развединформации, в скорости и эффективности управления способно обеспечить победу даже уступающей противнику по численности и огневым средствам армии. Таким образом, особое значение в настоящее время приобретают вопросы надежного и эффективного управления войсками.

В настоящее время, АСУ войсками, силами и средствами ВКО находятся на этапе развития, проходящем в условиях ужесточения требований к оперативности, непрерывности, устойчивости и скрытности управления войсками ВКО, ограниченного финансирования разработок средств автоматизации, появления и разработки новых огневых и информационных средств авиации, ЗРВ, РТВ, обладающих более широкими возможностями, чем существующие средства. Его отличительными чертами являются активное развитие и внедрение в АСУ новых информационных и телекоммуникационных технологий, высокие темпы совершенствования элементной базы средств автоматизации и связи [1].

При проектировании АСУ ВКО одним из наиболее важных моментов является управление доступом, хранением и использованием информации. Функциональная и эффективная работа современных АСУ невозможна без специализированных средств хранения и обработки информации. С увеличением объемов информации и сложности производимых вычислений возрастают требования к базам данных (системам управления хранением данных, СУХД), которые являются ядром современных АСУ.

При работе АСУ доступ к хранимой информации, так или иначе, получают все приложения и модули системы: источники информации, расчетные модули, средства визуализации, и т.д. Интенсивность и характер взаимодействия приложений с СУХД АСУ различны и определяются функциональностью приложений и спецификой хранимых данных.

СУХД (далее, в т.ч., хранилище данных) является централизующим звеном в работе АСУ, от характеристик его работы, от удобства доступа к данным зависит работа всего комплекса, т.е., при большом количестве обращений к хранилищу именно оно может быть узким местом

комплекса с точки зрения производительности. Эффективность работы хранилища данных зависит от используемых программных средств, осуществляющих доступ к данным, модели данных и производительности используемого оборудования.

На настоящий момент существует большое количество систем управления хранением данных, удовлетворяющих различным запросам. При этом закрытые код и архитектура коммерческих СУБД не позволяют рассматривать их в качестве хранилища данных АСУВ. Тем не менее, несмотря на развитие и распространенность систем хранения данных, они не лишены недостатков. Так, информационные системы с клиент-серверной архитектурой чрезвычайно зависимы от мощности сервера (серверного кластера) и пропускной способности каналов передачи информации. Клиент-серверная архитектура более удобна для хранения больших объемов редко запрашиваемой информации, так как частая передача больших объемов данных по сети может быть затруднена. Локально-ориентированные системы частично решают данные проблемы, но появляется необходимость решения ряда задач по синхронизации в клиентских и серверных копиях баз данных, кроме того, при большом количестве хранящихся данных может быть затруднен запрос полной копии базы данных при инициализации клиентских рабочих мест.

Ряд программных решений сочетают в себе возможности приведенных архитектур, осуществляя частичное разделение хранимых данных и располагая часть из них, в том числе, в локальных базах данных [2]. В таких случаях фактором, определяющим производительность системы при фиксированных программных решениях, является алгоритм разделения данных (выделения локальной части). В большинстве подобных систем разделение данных осуществляется по принципу кэширования, т.е., динамического размещения часто запрашиваемых данных в локальных хранилищах. Механизм кэширования позволяет оперировать только частотой запросов и не учитывает характеристики локальных хранилищ данных. В ряде других решений, разделение осуществляется исходя из предметной области и «примерных» свойств частей. Также, достаточно распространенным подходом является проектирование распределенных баз данных, при котором данные разделяются между серверами кластера таким образом, что каждый из серверов хранит часть данных и таблицу размещения всех данных хранилища, осуществляя передачу запросов частей данных соответствующим серверам и последующую компиляцию результатов. Однако, при проектировании АСУ ВКО, данный подход не является целесообразным, в виду небольшого количества серверов, требований по резервированию и отсутствия данных объема, существенного для масштабирования.

Основная сложность при разработке систем управления хранением данных состоит в разнородности хранимой информации и, как следствие, сложности построения достаточно универсального внутреннего механизма хранения данных (движка СУХД). Разнородность данных проявляется, например, в значительном различии темпов доступа к информации. В АСУ хранимые данные варьируются от сравнительно редко меняющихся объектов большого объема до меньших, запрашиваемых и изменяемых несколько раз в секунду.

В целом, для каждого готового программного решения, в соответствии с его внутренней архитектурой, существуют данные с «наиболее подходящим» набором свойств, обрабатываемые с наибольшей для данного решения эффективностью и данные с «менее подходящим» набором свойств, обработка которых данным программным решением затруднена. В то же время, учитывая значительную разнородность хранимых данных, жесткие требования и высокая нагрузка современных АСУ не позволяют пренебречь характеристиками обрабатываемых данных за счет производительности того или иного программного решения.

Таким образом, отсутствие универсальной СУБД с открытым кодом, ограничение на мощность и стоимость серверного оборудования приводит к тому, что при проектировании крупной АСУ, предназначенной для обработки разнородных данных, зачастую невозможно обеспечить все требования к системе одним готовым программным решением.

В данной работе предлагается повысить эффективность управления хранением данных при проектировании АСУ за счет разделения

хранимых данных и использования нескольких взаимодействующих в той или иной степени доработанных программных решений [3].

Соответственно, рассматривая хранимую информацию, как набор классов данных (таблиц в реляционной модели данных), предлагается улучшить эффективность управления хранением данных за счет подбора распределения классов по базам данных. Выбор, в общем случае, нескольких программных решений позволяет совместить преимущества каждой из систем, избегая, по возможности, недостатков за счет наилучшего сопоставления части обрабатываемых данных и хранилища, отвечающего за часть. При этом разбиение предлагается считать неизменным на протяжении работы комплекса.

При проектировании СУХД АСУ, используя данный подход, возникают две задачи – выбор программных решений (хранилищ) и получение оптимального распределения классов данных по хранилищам.

Для решения первой задачи предлагается использовать два хранилища с клиент-серверной и распределенной архитектурой соответственно. С точки зрения предметной области, актуальным является разделение данных по темпам обновления, на более медленную «статическую» (справочные данные, классификационная информация) и более быструю «динамическую» (информация о воздушных объектах) части. Соответственно, на основании обзора современных систем хранения данных, предлагается использовать СУБД PostgreSql – мощную реляционную базу данных – для статических данных и систему хранения динамической информации (динамическое хранилище данных – ДХД), основанную на SQLite – производительной реляционной библиотеке, в качестве основы базы данных для динамической информации. ДХД представляет собой распределенное хранилище данных, эффективное для часто меняющихся данных с приоритетом чтения.

Решение задачи разбиения хранимых данных требует создания методики, включающей в себя математическую модель процесса обработки запросов хранилищем данных (системой из нескольких хранилищ), критерии эффективности отдельного хранилища и совокупной СУХД, а также методы получения оптимального разбиения классов данных по хранилищам.

Одним из возможных подходов к построению мат. модели может быть использование математического аппарата теории массового обслуживания (ТМО) для описания процесса обработки запросов к СУХД. Так, согласно теоретическим и экспериментальным, полученным в работе, данным, поток запросов к хранилищу данных можно описывать, как пуассоновский поток событий [4]. Соответственно, в качестве критерия эффективности предлагается использовать производные от среднего времени ожидания величины:

Критерий эффективности хранилища данных $m_i, i = \overline{1, M}$:

$$w_i = \frac{\lambda_i \sigma_B^2}{2\left(1 - \lambda_i b_i\right)}$$

где λ_i суммарная интенсивность потока заявок для i-того хранилища, b_i мат. ожидание времени обслуживания заявок, σ_B^2 дисперсия времени обслуживания заявок.

Критерий эффективности системы из M хранилищ данных:

$$J = \sum_i^M \sum_j^N (b_{ij} + w_i) x_{ij}$$

где b_{ij} время обслуживания заявки класса $n_j, j = \overline{1, N}$ риментельно к хранилищу m_i т.е., $n_j \in m_i$ x_{ij} элемент принадлежности: $x_{ij} = \begin{cases} 1, n_j \in m_i \\ 0, n_j \notin m_i \end{cases}$. Данные критерии позволяют охарактеризовать как конкретное хранилище, так и систему из нескольких хранилищ данных, каждое из которых обрабатывает свою часть классов данных.

Также, для выделения более существенных свойств данных в работе предлагается провести рекластеризацию первоначального набора классов, так, чтобы в новом наборе классов каждому классу соответствовал единственный поток запросов с более или менее постоянными характеристиками. Рекластеризация не вносит принципиальных изменений в сущность методики получения оптимального разбиения данных, но положительно сказывается на её точности.

Далее, определение оптимального разбиения хранимых данных является задачей оптимизации критерия J тносительно переменных x_{ij} относящейся к классу нелинейных псевдо-булевых задач. Вариантом решения задачи оптимизации является алгоритм частичной линеаризации, позволяющий перейти к дробно-линейной задаче оптимизации, а также – алгоритм сведения дробно-линейной задачи к задаче булевой выполнимости (*SAT*-задача). *SAT*-задача является широко известной *NP*-полной задачей в теории алгоритмов [5].

Несмотря на высокую теоретическую вычислительную сложность, существует большое количество алгоритмов и приложений, основанных на алгоритмах поиска с возвратом, позволяющих решать *SAT*-задачу за приемлемое время даже при количестве переменных порядка 10^6 [6].

Таким образом, в данной работе предложен подход, позволяющий при разработке СУХД АСУ совместить несколько программных решений – хранилищ данных, при этом повышая эффективность совокупной системы за счет подбора оптимального разбиения данных по используемым хранилищам. Предложена модель описания процесса обработки запросов СУХД, критерии эффективности данного процесса, а также методика получения оптимального разбиения. Данный подход позволяет обрабатывать данные с широким диапазоном характеристик, и СУХД, разработанная в соответствии с данным подходом, является эффективным решением задачи хранения данных при проектировании АСУ ВКО.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев В.Н., «5 этапов развития АСУ», Военно-космическая оборона, № 2 (57), 2011.

2. Дэйв Энсор, Йен Стивенсон. «Oracle. Проектирование баз данных» К.:BHV, 1999.

3. Дудаков Н.С., Пирогов Н.Е., Шумилов Ю.Ю., «Гибридная система управления хранением данных», Вестник НИЯУ МИФИ №1 2012.

4. Хинчин А.Я. «Работы по математической теории массового обслуживания», Москва, 1963.

5. Беллман Р., Дрейфус С. «Прикладные задачи динамического программирования», Москва, 1965.

6. Matti Jarvisalo, Daniel Le Berre, Olivier Roussel, «The International SAT Solver Competitions», «www.satcompetition.org».

Д. В. Дымов
ОАО «Информационные спутниковые системы имени академика М. Ф. Решетнева», г. Железногорск

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ БОРТОВЫХ ТЕЛЕМЕТРИЧЕСКИХ СИСТЕМ ДЛЯ СПУТНИКОВ СВЯЗИ ОАО «ИСС»

Приводятся этапы развития бортовых информационно-телеметрических систем космических аппаратов ОАО «ИСС», основные тактико-технические и функциональные характеристики современной телеметрической системы с распределенной структурой, описывается общая структура информационно-измерительной системы с использованием сетевой технологии SpaceWire

Для обеспечения управления космическим аппаратом (КА) важной проблемой является обеспечение в течение всего срока эксплуатации, надежного диагностирования работоспособности и функционального состояния бортовой радиоэлектронной аппаратуры (БРЭА). Такой контроль позволяет оперативно выявить отклонения от штатных режимов работы БРЭА, предотвратить развитие дефектов и своевременно восстановить работоспособность.

Наибольшую актуальность приобретает проблема технической диагностики для современных космических аппаратов (КА), в составе которых используются сложные технические электронные системы, с большим количеством телеметрических параметров различного типа (например, в спутнике связи «Экспресс-АМ5» необходимо контролировать до десяти тысяч телеметрических параметров). Телеметрическую информацию необходимо собрать, обработать, при необходимости запомнить, и передать по служебному радиоканалу командно-измерительной системы (БА КИС) на наземный комплекс управления (НКУ), в котором она должна быть обработана и передана для анализа и принятия решений.

Задача диагностики БРЭА на современном КА решается с помощью системы телеметрического контроля (СТК), состоящей из датчиковой аппаратуры и телеметрической системы. Бортовая телеметрическая система (ТМС) обеспечивает сбор информации от различных служебных и научных датчиков, преобразует выходные сигналы этих датчиков в цифровую форму, обеспечивает хранение информации в период между сеансами связи и формирование телеметрического сообщения на НКУ.

На современном этапе в развитии бортовых телеметрических систем можно выделить несколько направлений:

1) рост объемов данных, получаемых от бортового оборудования КА;

2) сокращение массогабаритных характеристик аппаратуры ТМС;

3) сокращение затрат на разработку и модернизацию ТМС для новых КА,

4) интеграция информационных каналов ТМС в общую информационно-коммуникационную сеть КА, включая распределенную архитектуру сбора информации от датчиковой аппаратуры.

За прошедшие 20 лет, по техническим заданиям и системным проектам ОАО «ИСС», было создано несколько поколений бортовых телеметрических систем, которые обеспечили информационную поддержку и управление всех космических аппаратов разработанных на предприятии (таблица 1).

Таблица 1

Характеристика	ТА932MS/ АМ	ТА932М1М	ТА932МД-01	ТА932МД-233
Измерительные 8-р. каналы:	640	576	480	652
– аналоговые	256	256	128	128
– температурные	192	160	256	432
– цифровые 8р	192	160	96	92
Цифровой интерфейс с БРЭА	-	-	-	2 порта по 576 байт
Измерение цифрового датчика	1р.	1р.	1р.	8р.
Компаратор сигнальных датчиков	Фиксированный на 8 входов			Программный 320 входов
Процессор обработки событий	-	-	ПОС-М ПОС-Б	ПОС-М, ПОС-Б, РКС
Тип ПЗУ управления	Внешняя PROM			Внутренняя EEPROM
Интерфейс с БА КИС	Специальный		2 порта RS232	2 порта RS232 или SpaceWire (опция)
Интерфейс с БЦВК	Специальный	MIL-1553B		MIL-1553B или SpaceWire (опция)
Конструкция ТМС	моноблок			распределенная
Конструкция КА	герметичная		негерметичная	
Масса ТМС	15 кг.	13,5 кг.	7,1 кг.	6,9 кг.
Масса 8р. канала	23,5 г	23,5 г	15 г	10,6 г (3,8)
САС, лет	10,5	10,5	15,25	15,5

В 90-е года прошлого века были созданы первые ТМС, в которых применялись цифровые технологии и специализированные интерфейсы для информационно-логического обмена с БЦВК и БА КИС:

телеметрические системы ТА932М1 с «жесткой аппаратной логикой» для космических аппаратах «Экспресс-А» и «Молния-3К»;

телеметрические системы ТА932MS и ТА932АМ с использованием программируемой логики малой степени интеграции (RH1280, Actel) для спутников связи со сроком эксплуатации 10 лет «SESAT» и ««Экспресс-АМ» первого поколения (АМ1, 2, 3, 22, 33, 44).

В 2002 году, для навигационных спутников серии «Глонасс-М», была разработана телеметрическая система ТА932М1М с информационно-управляющим интерфейсом стандарта MIL-STD-1553B для взаимодействия с БЦВК, открывшим широкие возможности по унификации информационных коммуникаций на борту КА.

В 2011 году завершилась разработка малогабаритных ТМС серии ТА932МД-01, для негерметичных унифицированных платформ «Экспресс-1000», «Экспресс-2000» и созданных на их базе коммерческих спутников связи со сроком эксплуатации 15 лет: «AMOS-5», «TELKOM-3», «Ямал-300», «Ямал-401», «LYBID», «Экспресс-АТ1,2», «Экспесс-АМ5,6,8», «KAZSAT-3». Основным техническим решением, позволившим существенно снизить массогабаритные параметры ТМС, стала реализация функциональных узлов ТА932МД-01 на ПЛИС большой степени интеграции (RTAX1000, Actel) с применением технологий «система на кристалле» и СФ-блоков.

Рассмотренные выше телеметрические системы, позволяя гибко изменять количество измерительных модулей в моноблоке ТМС под задачи контроля определенного КА, имеют существенный недостаток, который ограничивает их дальнейшее развитие – протяженные аналоговые электрические линии связи типа “звезда” с датчиками БРЭА. Упрощенная структурная схема аналоговых линия связи датчиков с ТМС показана на рисунке 1.

Как видно из рисунка 1, аналоговые линии связи, кроме сложной конструкции кабельной сети (экраны, повив), необходимости установки

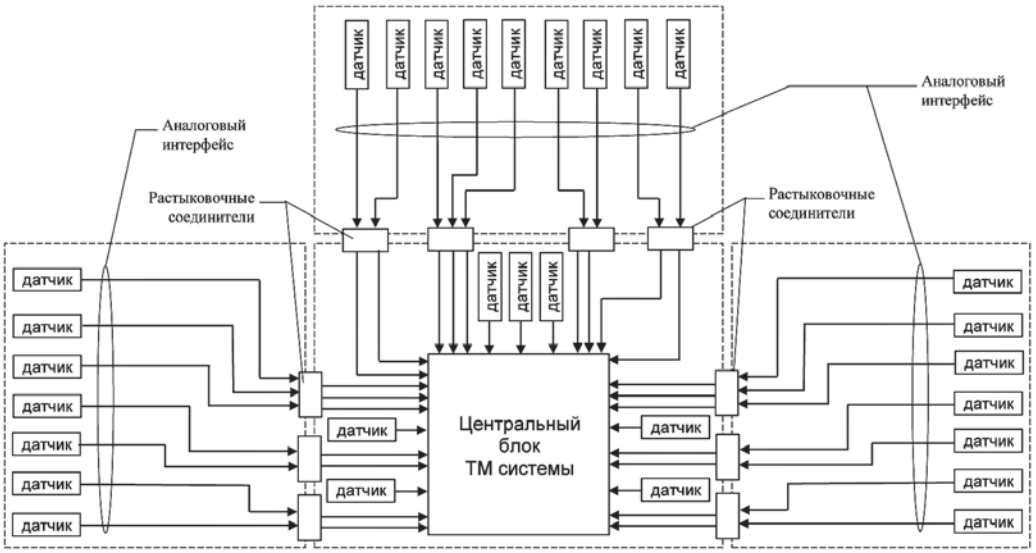


Рис. 1

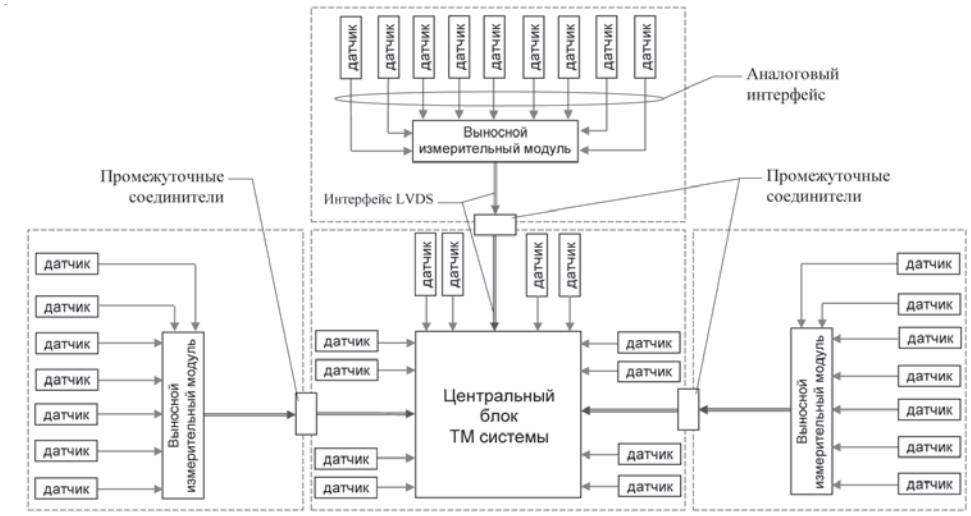


Рис. 2. Информационные связи ТМС с распределенной структурой

большого количества дополнительных соединителей для обеспечения технологии поэтапной сборки и испытания КА, обладают низкой помехоустойчивостью к электромагнитным помехам, снижая общую достоверность диагностики БРЭА.

Для улучшения массогабаритных характеристик ТМС, повышения достоверности результатов измерения сигналов от датчиков, а также удовлетворению возросших потребностей в цифровых стандартных интерфейсах со стороны проектируемой для перспективных проектов БРЭА, в 2012 году началась разработка *телеметрической системы ТА932МД-233 с распределенной структурой*.

При проектировании ТА932МД-233 был проведен большой комплекс проектных работ, результатами которых стали: 1) оптимизированная архитектура «системы на кристалле» центрального блока ТМС; 2) новые функциональные узлы обработки информации от датчиков (320-входовый программируемый логический компаратор, три типа процессоров обработки событий); 3) новые типы универсальных измерительных модулей, позволяющих измерять сигналы от различных типов датчиков; 4) опцион-

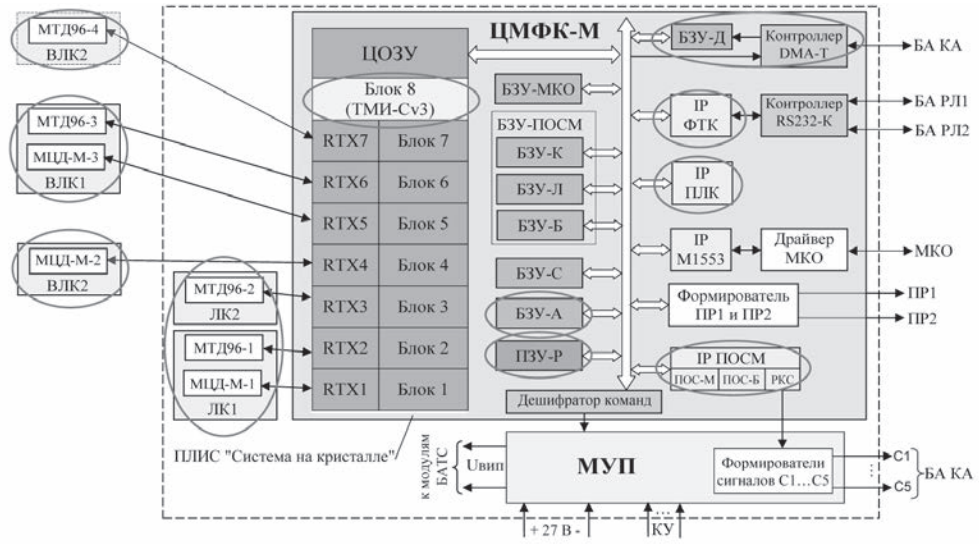


Рис. 3. Структурная схема ТА932МД-233М:
ВЛК – выносной локальный коммутатор, МТД96 – модуль для температурных и аналоговых датчиков, МЦД- модуль для сигнальных, аналоговых и температурных датчиков, ФТК – формирователь транспортных кадров; МКО – ОУ интерфейса MIL-STD-1553B»; ПОС – процессоры обработки событий, РКС – регистратор комплексных событий, МУП – модуль управления и питания

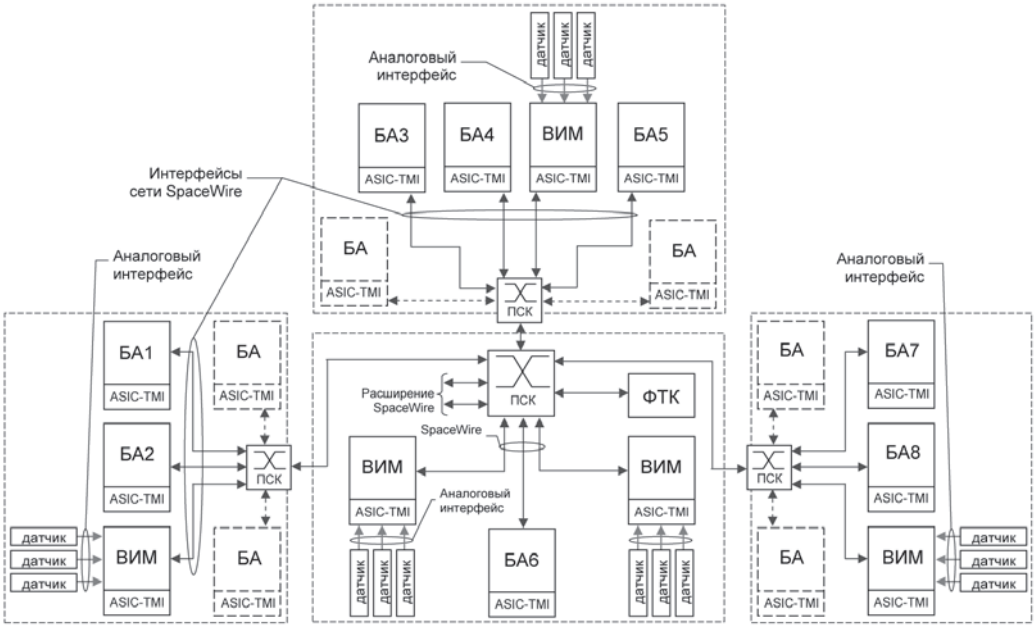


Рис. 4. Сетевая структура информационных связей ТМС
ВИМ – выносной измерительный модуль, ФТК – формирователь транспортных кадров; ПСК – маршрутизирующий коммутатор сети SpaceWire; ASIC-TMI – специализированная БИС для измерения сигналов от датчиков БА

ная поддержка цифровых интерфейсов стандартизованных для применения в КА ОАО «ИСС» (MIL-STD-1553, SpaceWire, RS232, LVDS, DMA-T); 5) малогабаритная механическая конструкция на 30% меньше прототипа; 6) возможность изменять в процессе эксплуатации программ управления функциональными модулями ТМС (применены перепрограммируемые микросхемы ПЗУ устойчивые к ВВФ космического пространства); 7) сокращение аналоговых интерфейсных линий связи (и соответствующее снижение массы бортовой кабельной сети) за счет установки выносных измерительных модулей в местах скопления датчиков (рисунок 2).

Структурная схема телеметрической системы ТА932МД-233М (модификация с интерфейсом MIL-STD-1553B) с выделенными новыми функциональными и структурными элементами показана на рисунке 3.

Дальнейшее развитие радиоэлектронной аппаратуры перспективных КА предполагает создание бортовой информационно-коммуникационной сети, которая в единой аппаратно-программной среде реализует передачу всех видов информации (пакетов данных от БА с телеметрическими параметрами, потоков команд управления, пакетов данных информационно-вычислительных средств, меток системного времени и т.д.). С учетом разрабатываемых информационных технологий, электронной компонентной базы (ЭКБ) и проектных проработок, определена предварительная схема коммуникационной сети платформы КА в которую гармонично включены информационные каналы телеметрического контроля (рисунок 4).

Реализация предложенной распределенной сетевой информационно-коммуникационной сети на основе технологии SpaceWire позволит коренным образом повлиять на решение совокупности основных задач отечественного космического приборостроения, во-первых добиться высокой надежности при приемлемом уровне затрат аппаратного резервирования, во-вторых выдержать жесткие требования к массогабаритным показателям и потребляемой мощности, в третьих добиться унификации интерфейсов передачи данных, и в четвертых достичь необходимых технико-экономических показателей, позволяющих конкурировать на мировом рынке.

А.В. Дьякова
кандидат технических наук, доцент

А.А. Бойко
кандидат технических наук, доцент

Р.С. Яковлев
кандидат технических наук, доцент
НИИЦ РЭБ ВУНЦ ВВС «ВВА им. проф. Н.Е Жуковского и Ю.А. Гагарина» (г. Воронеж)

АЛГОРИТМ ВСКРЫТИЯ УЯЗВИМОСТЕЙ ДЛЯ КОМПЬЮТЕРНЫХ АТАК В ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СРЕДСТВАХ

Предложен алгоритм вскрытия уязвимостей для компьютерных атак (КА) в информационно-технических средствах (ИТС), основанный на использовании автоматизированного метода формальной верификации программного обеспечения (ПО) MODEL CHECKING.

Введение

Сегодня не вызывает сомнения тот факт, что в современных ИТС математическое и реализующее его программное обеспечение обретает все большие объем и сложность, что приводит к лавинообразному увеличению количества ошибок. Ошибки приводят к возникновению уязвимостей, которые могут быть вскрыты и использованы злоумышленником для реализации КА. В таких обстоятельствах очевидна закономерность: чем больше достоверной информации об уязвимостях будет в арсенале разработчика и заказчика на этапе проведения предварительных, приемо-сдаточных (государственных), сравнительных и аттестационных испытаний ИТС, тем более эффективным будет их применение по назначению. Однако, как показывает практика, существующий подход к вскрытию в ИТС уязвимостей и последующей разработке тестовых алгоритмов КА состоит в проверке на наличие наиболее часто встречающихся «шаблонных» уязвимостей (уязвимости при использовании временных файлов, переполнение буфера, переменных, форматной строки, уязвимости, предоставляющие остаточную информацию в оперативной памяти, использующие нарушение синхронизации программных процессов, использующие библиотечные функции, XSS-уязвимости, SQL-уязвимости), а также в поиске экспертом единичных применимых только в специфических условиях КА, способных каким-либо образом нарушить штатный режим функционирования целевого ИТС.

Такой подход не универсален, т.к. не позволяет на основании теоретического обоснования синтезировать наиболее полное для имеющегося объема информации множество тестовых алгоритмов КА на ИТС, из которых для различных условий эксплуатации данных средств возможно выбрать оптимальные и тем самым существенно повысить достоверность оценки их функциональной стабильности. Исходя из этого, задача разработки подхода, позволяющего учитывать недостатки традиционного, является актуальной. В настоящей статье рассматривается алгоритм, который может быть использован в качестве базиса для нового подхода вскрытия уязвимостей для КА в ИТС.

Основная часть

В алгоритме вскрытия уязвимостей для КА в ИТС предлагается использовать автоматизированный метод формальной верификации ПО

MODEL CHECKING [1, 2]. Верификацию предлагается осуществлять с помощью программного средства SPIN (Simple Promela Interpreter) [3], входным языком описания которого является Promela.

Пусть дан фрагмент ПО исследуемого ИТС, представленный на рис. 1 [4]. В этом фрагменте описывается функция, реализующая бесконечный цикл взаимодействия с ядром (посылает сообщения и принимает их от него).

Рассмотрим применение предлагаемого алгоритма вскрытия уязвимостей для КА в ИТС на примере данного фрагмента.

На **шаге 1** задаем требования (спецификацию) к функции. В частности, проверяем выполнимость следующих требований:

1) всегда при вызове sys_irqenable() верно DspVersion[0] < 4;

2) тупики отсутствуют;

3) недостижимый код отсутствует;

4) циклы бездействия, за исключением цикла, связанного с бесконечным выполнением моделируемой функции, отсутствиуют.

На **шаге 2** строим модель функции. На языке Promela модель будет выглядеть следующим образом (рис. 2).

На **шаге 3** формулируем (при необходимости) и проверяем каждое требование спецификации. Требования 2-4 проверяются в SPIN внутренними командами (включением/отключением специальных флагов). Для проверки требования 1 его необходимо выразить на языке LTL (Linear Time Logic).

В ходе **шага 4** анализируем результаты верификации. При проверке требования 1 получили контрпример, который сохранился в файле model_assert.prm (рис. 3).

```
PRIVATE int DspVersion[2];
PRIVATE int dsp_init()
{
	int i, s;
	if(dsp_reset () != OK) {
		dprint("sb16: No SoundBlaster card detected\n");
		return -1;
	}
	DspVersion[0] = DspVersion[1] = 0;
	dsp_command(DSP_GET_VERSION);	/* Get DSP version bytes */
	for(i = 1000; i; i--) {
		if(sb16_inb(DSP_DATA_AVL) & 0x80) {
			if(DspVersion[0] == 0) {
				DspVersion[0] = sb16_inb(DSP_READ);
			} else {
				DspVersion[1] = sb16_inb(DSP_READ);
				break;
			}
		}
	}
	if(DspVersion[0] < 4) {
		dprint("sb16: No SoundBlaster 16 compatible card detected\n");
		return -1;
	}
	dprint("sb16: SoundBlaster DSP version %d.%d detected\n", DspVersion[0],
DspVersion[1]);
	/* set SB to use our IRQ and DMA channels */
	mixer_set(MIXER_SET_IRQ, (1 << (SB_IRQ / 2 - 1)));
	mixer_set(MIXER_SET_DMA, (1 << SB_DMA_8 | 1 << SB_DMA_16));
	/* register interrupt vector and enable irq */
	if ((s=sys_irqsetpolicy(SB_IRQ, IRQ_REENABLE, &irq_hook_id )) != OK)
		panic("SB16DSP", "Couldn't set IRQ policy", s);
	if ((s=sys_irqenable(&irq_hook_id)) != OK)
		panic("SB16DSP", "Couldn't enable IRQ", s);
	DspAvail = 1;
	return OK;
}
```

Рис. 1. Фрагмент ПО исследуемого ИТС

```
#define OK 0
#define NOT_OK 1
#define SYS_IRQPOLICY 1
#define SYS_IRQENABLE 2
int DspVersion[2];
chan to_kernel_channel = [0] of {byte};
chan from_kernel_channel = [0] of {byte};
active proctype kernel()
{
    int msg;
    do
    :: to_kernel_channel?msg ->
    {
        if
        :: (msg == SYS_IRQPOLICY) ->
        {
            if
            :: from_kernel_channel!OK;
            :: from_kernel_channel!NOT_OK;
            fi;
        }
        :: (msg == SYS_IRQENABLE) ->
        {
            if
            :: from_kernel_channel!OK;
            :: from_kernel_channel!NOT_OK;
            fi;
        }
        :: else -> skip;
        fi;
    }
    od;
}
active proctype dsp_init()
{
do
::
    byte result;
    DspVersion[0] = 0;
    DspVersion[1] = 0;
    if
    :: DspVersion[0] = 0;
    :: DspVersion[0] = 1;
    :: DspVersion[0] = 5;
    fi;
    if
    :: DspVersion[1] = 0;
    :: DspVersion[1] = 1;
    fi;
    if :: (DspVersion[0] < 4) ->
    {
        goto return;
    }
```

Рис. 2. Модель фрагмента исследуемого ПО ИТС (неполная)

```
% spin -p -tmodel_assert.prm.trail model_assert.prm
Starting kernel with pid 0
Starting dsp_init with pid 1
spin: couldn't find claim (ignored)
  2:    proc  1 (dsp_init) line  54 "model_assert.prm" (state 1)
[DspVersion[0] = 0]
  4:    proc  1 (dsp_init) line  55 "model_assert.prm" (state 2)
[DspVersion[1] = 0]
  6:    proc  1 (dsp_init) line  60 "model_assert.prm" (state 5)
[DspVersion[0] = 5]
  8:    proc  1 (dsp_init) line  64 "model_assert.prm" (state 8)
[DspVersion[1] = 0]
 10:    proc  1 (dsp_init) line  72 "model_assert.prm" (state 15)       [else]
 12:    proc  1 (dsp_init) line  72 "model_assert.prm" (state 16)       [(1)]
 14:    proc  1 (dsp_init) line  76 "model_assert.prm" (state 19)
[to_kernel_channel!1]
 15:    proc  0 (kernel) line  23 "model_assert.prm" (state 1)
[to_kernel_channel?msg]
 17:    proc  0 (kernel) line  26 "model_assert.prm" (state 2)  [((msg==1))]
 19:    proc  0 (kernel) line  29 "model_assert.prm" (state 3)
[from_kernel_channel!0]
 20:    proc  1 (dsp_init) line  77 "model_assert.prm" (state 20)
[from_kernel_channel?result]
 22:    proc  1 (dsp_init) line  84 "model_assert.prm" (state 24)       [else]
 24:    proc  1 (dsp_init) line  84 "model_assert.prm" (state 25)       [(1)]
 26:    proc  1 (dsp_init) line  88 "model_assert.prm" (state 28)
[call_irqenable = 1]
 28:    proc  1 (dsp_init) line  89 "model_assert.prm" (state 29)
[to_kernel_channel!2]
 29:    proc  0 (kernel) line  23 "model_assert.prm" (state 1)
[to_kernel_channel?msg]
spin: trail ends after 30 steps
#processes: 2
                DspVersion[0] = 5
                DspVersion[1] = 0
                call_irqenable = 1
 30:    proc  1 (dsp_init) line  90 "model_assert.prm" (state 30)
 30:    proc  0 (kernel) line  43 "model_assert.prm" (state 19)
2 processes created
```

Рис. 3. Контрпример

Далее необходимо проверить, является контрпример следствием ошибки моделирования или программирования. Анализируя поученный контрпример, можно установить, что в процессе инициализации параметр DspVersion[0] получил значение 5, и при вызове системной функции sys_irqenable() требование 1 нарушилось (рис. 4).

На 41 строке происходит вызов sys_irqenable(), и, как следствие, спецификация нарушается, что и было выявлено в процессе верификации модели.

```
Строка DspVersion[0]
7      ---
…
12     0
13     0
14     0
15     0
…
35     5
36     5
…
40     5
41     5
На 41 строке происходит вызов sys_irqenable(), и, как следствие, спецификация
нарушается, что и было выявлено в процессе верификации модели.
```

Рис. 4. Нарушение требования 1

Следовательно, с использованием предлагаемого подхода выявлена уязвимость, заключающаяся в потенциальной возможности невыполнения требования 1. Наличие данной уязвимости означает, что при обращении к ядру процессора посредством вызова функции sys_irqenable() происходит прерывание при значениях параметра DspVersion[0] $\geqslant 4$. Такая уязвимость может быть использована злоумышленником в интересах нарушения функциональной стабильности ИТС при реализации КА.

Заключение

Таким образом, предложен алгоритм вскрытия уязвимостей для компьютерных атак в информационно-технических средствах, основанный на использовании автоматизированного метода формальной верификации программного обеспечения MODEL CHECKING, и рассмотрено его применение для фрагмента кода программного обеспечения. Предложенный алгоритм позволит дополнительно к существующей технологии вскрывать уязвимости в многопоточных, распределенных и параллельных алгоритмах функционирования, характерных для программного обеспечения иерархически организованных и распределенных информационно-технических средств. Алгоритм может быть использован в процессе автоматизированного синтеза тестовых алгоритмов компьютерных атак на информационно-технические средства в интересах оценки их функциональной стабильности на этапе предварительных, приемо-сдаточных (государственных), сравнительных и аттестационных испытаний.

СПИСОК ЛИТЕРАТУРЫ

1. Кларк Э.М., Грамберг О., Пелед Д. Верификация моделей программ: Model Checking – М.: МЦНМО, 2002. – 416 с.

2. Карпов Ю.Г. Model Checking. Верификация параллельных и распределенных программных систем – СПб.: БХВ-Петербург, 2010. – 551 с.

3. Документация, дистрибутивы SPIN // http://spinroot.com [Интернет-ресурс]. Дата обращения: 01.09.2013 г.

4. Портал, посвященный программированию // http://esyr.org/wiki/ВПнМ,_примеры_задач/Задача_3 [Интернет-ресурс]. Дата обращения: 01.09.2013 г.

И. В. Иванов
кандидат технических наук МГУПИ
В.Е. Чириков
Академия ФСО России, Орел
М.М Снаров
Академия ФСО России, Орел
К.С. Щуров
ЦИТО Спецсвязь, Москва

ЗАЩИТА АНОНИМИЗИРУЮЩИХ СЕТЕЙ МНОГОСЛОЙНОЙ МАРШРУТИЗАЦИИ ОТ TIMING-АТАК

В данной статье рассмотрены проблема защиты анонимизирующих сетей многослойной маршрутизации от timing-атак. Проанализирована возможность применения timing-атаки на сеть I2P. На основе проведенного исследования авторы выделили условия успешного проведения timing-атаки в сетях многослойной маршрутизации. Выявлены характерные принципы построения защищенных анонимизирующих сетей многослойной маршрутизации.

Анонимность в сетях многослойной маршрутизации достигается путем пересылки сообщений через серию промежуточных узлов, создающих цепочку от отправителя до получателя сообщений. Каждый промежуточный узел должен обеспечить такие параметры выходного потока, которые не позволят установить соответствие входного и выходного потока.

Tor, второе поколение сетей многослойной маршрутизации (Onion Routing), - это анонимная сеть с малыми задержками, в основе которой лежат цепочки промежуточных узлов. В сети Tor применяется контроль перегрузок, технология совершенной прямой секретности, служба каталогов, проверка целостности, настраиваемые правила выхода, точки встречи и скрытые сервисы [1]. В последних версиях разработчики удалили смешивание потоков и использование покрывающего трафика.

«Малозатратная атака», описанная Мёрдочем (Murdoch) и Данезисом (Danezis) в статье “Low-cost traffic analysis of Tor” [2], предполагает, что для успеха нападающему достаточно иметь возможность наблюдать только за частью сети, например, быть одним из Tor-узлов. Мёрдоч и Данезис показали уязвимость Tor к timing-атакам. Цель атаки определить, какие именно узлы сейчас используются для организации Tor-цепочек. Проведенные исследования показали, что владение этой информацией сильно снижает анонимизирующие свойства сети Tor.

В сети Tor считается невозможным наличие глобального наблюдателя, так как нападающий не видит всех связей в сети. Однако злоумышленник способен выступить в роли узла Tor и замерить задержки между собой и всеми другими узлами. Зная эти задержки, можно косвенно оценить объем трафика, который передает каждый узел в определенный момент времени. Обобщая полученные сведения, мы получим распределение объема трафика от времени для всех узлов сети. С помощью распределения можно строить предположения об анонимизирующих цепочках.

Для защиты от этой атаки нужно сделать так, чтобы временные характеристики всех потоков были неразличимы. Чтобы достичь неразличимости временных характеристик, необходимо использовать смешивание с большим количеством входящих сообщений и добавлять большой объем покрывающего трафика (cover traffic).

В сети Tor по соображениям производительности смешивание потоков в промежуточном узле сети было удалено. Таким образом, остается три случая, когда объем трафика будет изменяться:

при устанавливается нового соединения;

при удалении существующего соединения;

при изменении входящего трафика;

Эти изменения отражаются на скорости ответов другим узлам (рис. 1), которые уже имеют или только хотят установить соединение. По этим же самым причинам меняется нагрузка и на других Tor-узлах. Получается, что изменение нагрузки трафика на Tor-узле отражается на нагрузке соединенных с ним узлов. Следовательно, узлы в одной цепочке будут иметь похожие картины распределения нагрузки от времени.

Отметим, изменение нагрузки трафика может возникать не только вышеописанным образом, но и из-за внутренних причин Tor-узла, например нагрузки на CPU — такие задержки не учитываются и могут снизить эффективность атаки. Атака будет еще более эффективной, если нападающий контролирует сервер, к которому подключается пользователь Tor. В этом случае не нужно нападающий сам может видоизменять трафик так, чтобы его легко было обнаружить.

Для проведения атаки нападающий должен получить список всех узлов сети. Затем, он устанавливает соединение с каждым из них и отслеживает возникающие в соединениях задержки. Наблюдение должно вестись некоторое время. На протяжении всего периода наблюдения вредоносный сервер не прекращает слать свой трафик в систему. По окончанию периода наблюдения, результаты замеров задержек в каждом соединении используются для оценки объемов трафиков соответствующих узлов. Затем нагрузки узлов сравниваются с трафиком сервера. Если выявляются совпадения, значит узел входит в анонимизирующую цепочку. Проведя сравнение для всех узлов можно выявить всю цепочку. Таким образом, для успешной атаки должны быть выполнены следующие условия:

Задержки, наблюдаемые вредоносным узлом должны отражать нагрузку других узлов;

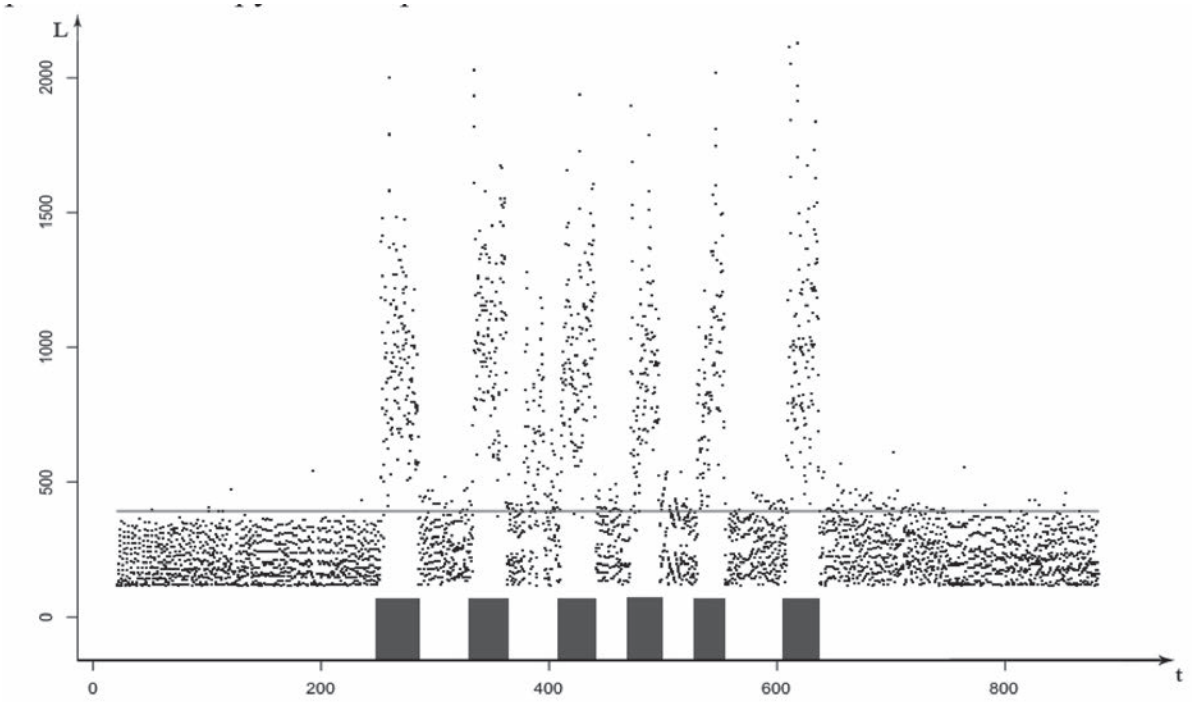


Рис.1. Корреляция задержки (*L) и большого объема входного траффика Tor* узла

Вредоносный узел должен иметь информацию обо всех других узлах сети;

Вредоносный узел должен иметь возможность устанавливать прямые соединения со всеми другими узлами.

Tor подвержен атаке, потому что его архитектура удовлетворяет этим требованиям. Во-первых, разработчики Tor удалили операции смешивания и покрывающий трафик, поэтому временные характеристики потоков сохраняются на протяжении всей цепочки. Это подтвердили эксперименты (Murdoch & Danezis 2004 [2]). Во-вторых, в Tor предусмотрена служба каталогов, с помощью которой Tor-клиент может получить список всех узлов (Tor-серверов) сети. В-третьих, ничего не мешает Tor-клиенту установить соединение со всеми Tor-серверами [3].

Рассмотрим сеть I2P. I2P – это оверлейная децентрализованная анонимная сеть, использующая многослойную маршрутизацию. I2P предназначена для создания изолированной, закрытой сети, без выхода во внешний интернет. В этой сети используется peer-to-peer (p2p) архитектура, с протоколом маршрутизации netDb, используя который, клиент сети может получить информацию фактически о любом узле, а именно входной канал до любого узла.

Существует несколько ключевых особенностей сети I2P.

Во-первых, это полностью децентрализованная сеть, что обеспечивает робастность сети. Маршрутизация внутри сети производится с помощью алгоритма netDb – network database, модификации алгоритма Kademlia DHT. От Kademlia DHT netDb отличается тем, что хранит в себе хешированные адреса узлов сети, зашифрованные AES IP-адреса и публичные ключи шифрования, причём соединения netDb зашифрованы. Сеть предоставляет приложениям простой транспортный механизм для анонимной и защищённой пересылки сообщений друг другу.

Во-вторых, сеть I2P использует разные цепочки узлов сети для передачи и для приема (рис. 2). Каждый узел сети может входить как в цепочку неограниченное количество раз. Различают выходной и входной каналы. Выходной – цепь узлов I2P, от отправителя до точки выхода, входной от точки входа, до получателя соответственно. У отправителя может существовать множество выходных каналов, которые он будет выбирать в соответствии с конечным получателем. Поиск существующих каналов происходит с помощью netDb.

В-третьих, внутри сети данные передаются с помощью протокола SSU - Secure Semireliable UDP, который представляет собой модификацию протокола UDP и модифицированного

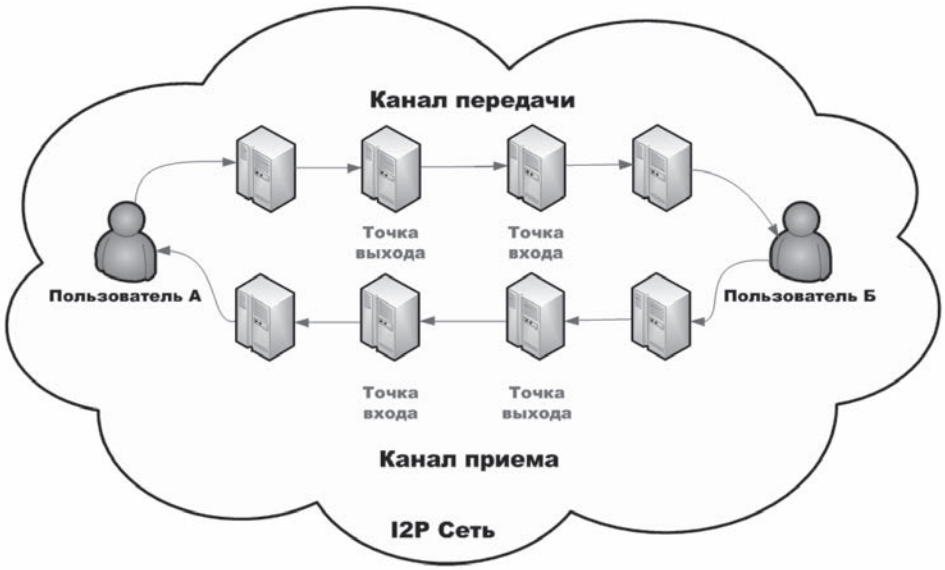


Рис.2. Передача данных в сети I2P

протокола TCP, называемого NTCP. NTCP в данный момент находится еще в стадии разработки, поэтому сейчас может использоваться только для каналов выхода.

В сети I2P timing-атака не может быть проведена. Хотя мы и можем получить карту сети, где будут указаны все узлы сети, но p2p архитектура сети подразумевает динамическое изменение структуры сети, поэтому очень сложно будет построить актуальную карту нагрузок в сети. Предположим, что вредоносных узлов у нас необходимое количество, а структура сети изменяться не будет, но все равно не будет выполняться второе условие, необходимое для проведения атаки. В архитектуре I2P сети отсутствует понятие о прямом соединении, у каждого элемента сети есть входные и выходные туннели, т.е. можно с уверенностью сказать, что снятые данные будут указывать заведомо ложную информацию об узле. Исходя из вышенаписанного можно с уверенностью сказать, что для сети I2P timing-атака, описанная, Мёрдочем и Данезисом не применима.

Заключение

Работая над статьей, мы вывели общие принципы построения защищенных анонимизирующих сетей многослойной маршрутизации от timing-атак:

Использовать p2p архитектуру сети;

Добавлять покрывающий траффик для выходного потока;

Вносить случайную задержку удовлетворяющую требованиям сети;

Использовать смешивание входных и выходных каналов.

СПИСОК ЛИТЕРАТУРЫ

1. R. Dingledine and N. Mathewson. «Tor spec. Technical report», The Free Haven Project, October 11 2011. https://gitweb.torproject.org/tor.git?a=blob_plain;hb=HEAD;f=doc/spec/tor-spec.txt

2. S. Murdoch and G. Danezis «Low-Cost Traffic Analysis of Tor», University of Cambridge, Computer Laboratory, United Kingdom, November 2004

3. A. Christensen «Practical Onion Hacking: Finding the real address of Tor clients», FortConsult's Security Research Team, October 2006

4. M. Ehlert «I2P Usability vs. Tor Usability. A Bandwidth and Latency Comparison», Humboldt University of Berlin, 20 February 2011

5. www.i2p2.de «Invisible Internet Project (I2P) Project Overview» http://www.i2p2.de/_static/pdf/i2p_philosophy.pdf

6. www.i2p2.de «I2P Staff Introducing I2P: A scalable framework for anonymous communication» http://www.i2p2.de/techintro.html (last accessed Feb. 13th 2011)

В.Г. Иванов
кандидат военных наук, Военная академия связи
Д.В. Петрунин
Военная академия связи
В.А. Кутенко
Военная академия связи

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ЭЛЕКТРОННОГО ОБУЧАЮЩЕГО КУРСА ДЛЯ ИЗУЧЕНИИ СОВРЕМЕННЫХ КОМПЛЕКСОВ СВЯЗИ

В статье раскрывается концептуальная модель электронного обучающего курса для изучении современных комплексов связи. Рассмотрены признаки, структура основные этапы по разработке электронных курсов предназначенных для изучения современных комплексов связи и порядок их применения в ходе занятий.

Применение компьютеров в учебном процессе военных учебных заведений привело к появлению нового поколения информационных образовательных технологий, которые позволили повысить качество обучения, создать новые средства воспитательного воздействия слушателей и курсантов, более эффективно взаимодействовать профессорско-преподавательскому составу, слушателям и курсантам с вычислительной техникой.

Под концептуальной моделью электронного-обучающего курса (ЭОК) будем понимать абстрактную модель, содержащую частично формализованное описание требований, структуры, технологий, анализ использования ЭОК в учебном процессе, а также основные вопросы в процессе функционирования [1]. Концептуальная модель ЭОК представлена на рис 1.

При формировании концептуальной модели использовались следующие положения:

Система состоит из отдельных элементов и определяется их свойствами,

Выделение существенных свойств системы зависит от целей исследования.

Сложная система имеет, как правило, многоуровневую структуру.

Каждый элемент системы (и система в целом) непрерывно подвергается некоторым обратимым и необратимым количественным и качественным изменениям, т. е. находится в развитии.

Примером успешной реализации информационно-коммуникационных технологий стало использование Web-технологий в локальной вычислительной сети ВВУЗа с ее практически неограниченными возможностями сбора и хранения информации, передачи ее индивидуально каждому пользователю.

В основе этих курсов должна лежать четкая структура. Контент курса, организованный средствами гипертекста, так же должен иметь структуру. Структура всего курса и его контента зависит не только от содержания обучения, но и от формы обучения. В настоящее время к ЭОК предъявляются следующие требования [2], которые представлены на рис. 1.

Чтобы удовлетворить вышеперечисленные требования, целесообразно использовать при

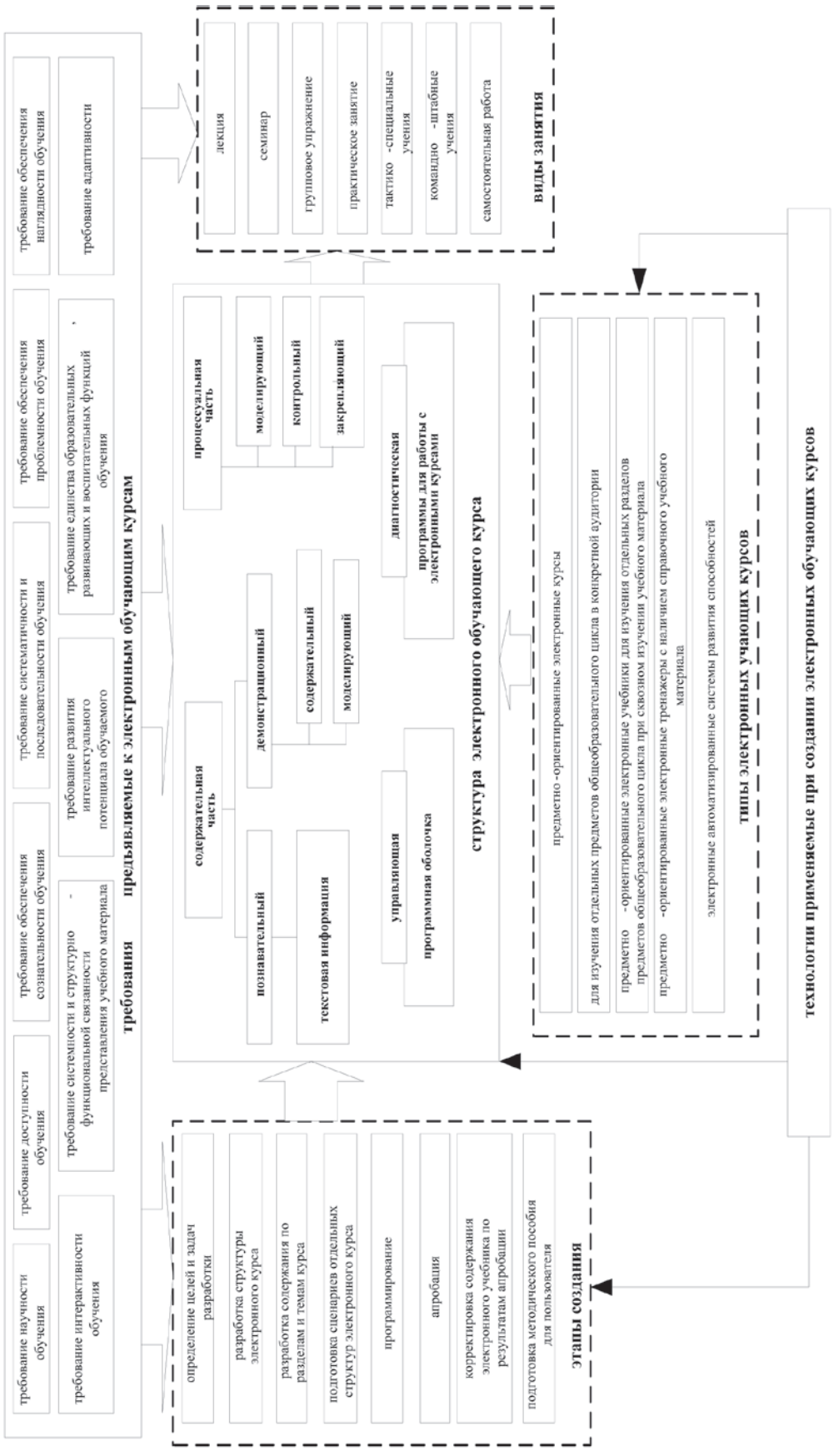


Рис. 1. Концептуальная модель электронного обучающего курса

подготовке ЭОК гипертекстовые и флэш технологии.

Гипертекстовая система – представление информации в виде некоторого графа, в узлах которого содержатся текстовые элементы (предложения, абзацы, страницы или даже целые статьи, либо книги), а между узлами имеются связи, с помощью которых можно переходить от одного текстового элемента к другому.

Использование гипертекстовой технологии удовлетворяет таким предъявляемым к ЭОК требованиям, как структурированность, удобство в обращении. При необходимости такой учебник можно «выложить» на любом сервере и его можно легко корректировать.

Кратко рассмотрим эти этапы разработки ЭОК.

Определение целей и задач разработки. Отправной точкой в создании курсов являются дидактические цели, для достижения и решения которых используются информационные технологии.

В зависимости от целей обучения ЭОК могут быть различных типов рис 1.

При разработке ЭОК необходимо первоначально выработать его структуру, порядок следования учебного материала, вид навигации по разделам, сделать выбор основного опорного пункта будущего курса.

Разработка содержания по разделам и темам ЭОК. Понятие о содержании является частью понятия содержания образования, под которым понимается система знаний, умений, навыков, овладение которыми обеспечивает развитие обучаемого. При разработке содержания отдельных тем необходимо ранжировать учебный материал:

- по степени сложности восприятия,
- по степени сложности подачи.

В ходе этой работы необходимо:

- выделить основное ядро учебного материала,
- выделить второстепенные моменты в изучении учебного материала,
- выделить связи с другими темами учебного курса,
- подобрать практические разно уровневые многовариантные задания по каждой теме,
- подобрать иллюстрации, графики, демонстрации, анимационные видеофрагменты к понятиям, формулировкам, событиям и т.д.

Подготовка сценариев отельных программ ЭОК. Сценарий – это покадровое распределение содержания учебного курса и его процессуальной части в рамках программных структур разного уровня и назначения. Программные структуры разного уровня – компоненты мультимедийных технологий: гипертекст, анимация, звук, графика и т.п.

Использование этих средств носит целенаправленный характер: для развития познавательного интереса, повышения мотивации учения.

Программирование начинается с создания основных шаблонов кадров будущего ЭОК; они различаются в зависимости от назначения кадра: разместить в нем учебный материал, подкрепить его рисунком, анимацией графиком.

Во время апробации выявляются отдельные незамеченные разработчиками ошибки: некорректность, неудобства в эксплуатации и.т.п.

По результатам апробации проводится корректировка программ электронного обучающего курса. Эта работа может касаться и сценарной линии курса, его структуры; она касается неточностей и ошибок в ответах при работе с заданиями и т.п.

Подготовка методического пособия для преподавателя может включать следующие материалы: содержание отдельных программных модулей; задания, тесты, предлагаемые после изучения каждой темы; примерное тематическое планирование с указанием места использования данного электронного обучающего курса; инструкцию для работы с ЭОК; необходимую конфигурацию компьютера для инсталляции ЭОК.

Подготовленный ЭОК может быть использован для проведения различных занятий.

Лекции. Во первых использование электронного обучающего курса может заметно снизить время на подготовку преподавателя к лекциям при его использовании. При подготовке преподавателю нет необходимости придумывать и разрабатывать презентацию, т.к. ЭОК может быть использован в качестве ее. Преподавателю лишь необходимо согласно тематике лекции и ее учебному материалу подобрать последовательность гиперпереходов по различным страницам.

Немаловажным является наличие на страницах ЭОК гиперссылок поясняющих те или иные термины в тексте, таким образом, при

возникновении у обучаемых вопросов по поводу тех или иных непонятных аспектов лекции преподаватель может не просто пояснить устно материал, а переключиться на страницу с соответствующим содержанием. После разъяснения с помощью все тех же гиперпереходов вернуться обратно к материалу лекции. Это существенно повышает интерактивность лекции по сравнению с использованием простой презентации, т.к. преподаватель не может заранее предугадать все возникающие у обучаемых вопросы и при использовании обычной презентации ему приходится тратить время на поиск соответствующего материала.

Практические занятия. ЭОК является достаточно обширным курсом, который включает в себя не только базовые основы по комплексам связи но также в нем приведены технологические карты и порядок настройки отдельных образцов техники связи входящих в состав комплексов связи. Это позволяет использовать ЭОК для проведения практических занятий.

При отработке настройки аппаратуры преподавателю лишь необходимо открыть страницу ЭОК, где рассмотрен процесс настройки подходящий под тему данного практического занятия. При наличии в учебном классе ЭВМ у каждого из обучаемых они могут работать с ЭОК напрямую.

Семинарские занятия. При проведении данных занятий желательно чтобы каждый из обучаемых имел на своем месте ПЭВМ с открытым на нем ЭОК. Таким образом, при коллективном рассмотрении вопросов семинара все обучаемые будут так или иначе задействованы и будут следить за учебным материалом по ходу занятия.

Заключение

Разработка ЭОК по предложенной модели поможет более эффективно разрабатывать учебно-методический материал для подготовки специалистов, повысить наглядность преподаваемого материала, а также предоставить всю необходимую справочную информацию даже касательно монтажа, настройки и эксплуатации средств связи.

Актуальностью создания ЭОК в военно учебных заведениях связи продиктована в быстро идущей заменой устаревших средств связи на новые, но при этом отсутствуют учебные материалы по из освоению. Использование ЭОК в ходе изучения дает возможность быстрого самостоятельного освоения комплексов связи.

СПИСОК ЛИТЕРАТУРЫ

1. Информационные технологии в образовании Электронный ресурс. / Сайт новые информационные технологии в образовании Режим доступа: http://ito.edu.ru

2. Шабанов, Г. И. Методическая система обучения студентов инженерных специальностей обще техническим дисциплинам на основе комплексной информационно-образовательной базы Текст. / Г. И. Шабанов. - Саранск: Изд-во Мордов. ун-та, 2005. 232 с.

М.С. Иванов
кандидат технических наук
А.В. Березин
Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
В.Ф.Волковский
Военно-космическая академия **имени А.Ф.Можайского**

МЕТОДИКА ОРГАНИЗАЦИИ СИСТЕМЫ ЕДИНОГО ВРЕМЕНИ ДЛЯ АБОНЕНТОВ ЛОКАЛЬНОЙ СЕТИ СВЯЗИ С ППРЧ

В статье представлены варианты организации системы единого времени и вхождения в связь для абонентских станций в сети с псевдослучайной перестройкой рабочей частоты. Приведены примеры организации системы локального единого времени для телекоммуникационной системы с псевдослучайной перестройкой рабочей частоты.

Для обеспечения надёжной связи при ППРЧ необходима взаимная привязка абонентов во времени. Синхронизация абонентов по времени является важнейшим и необходимым условием сжатия спектра на приёмной стороне линии связи. Её можно обеспечить различными способами:

– привязкой абонентов к системе единого времени;

– взаимной привязкой абонентов к локальному времени одного из абонентов сети по принципу сверки часов по часам командира.

Система единого времени и эталонных частот развивается на основе Государственной службы времени и частот, обеспечивающей деятельность Государственной системы единого времени и эталонных частот.

Российские средства передачи системы единого времени состоят из:

– КВ, ДВ и СВ станций, расположенных [1] в Москве, Самаре, Иркутске, Нижнем Новгороде, Новосибирске;

– космических аппаратов спутниковой радионавигационной группировки ГЛОНАСС / GPS.

Передающие СВ радиостанции обеспечивают точность привязки шкал времени объектов до 10 мкс по калибровочным трассам и до 35 мкс по любым трассам, время распространения по которым рассчитывается по типовым методикам. Передающие ДВ радиостанции обеспечивают точность привязки шкал времени до 1мкс в зоне действия до 1500 км.

Спутниковая радионавигационная система обеспечивает точность привязки шкалы времени потребителя не хуже 1мкс в любое время суток и года в любой точке земной поверхности и околоземного пространства.

Привязка абонентов к системе единого времени проводится путем сопряжения их аппаратуры с приемниками системы единого времени. Как правило, приемники системы единого времени имеют стандартные интерфейсы, обеспечивающие информационно-командный обмен и выход секундной (минутной) метки для обеспечения аппаратной синхронизации временной шкалы потребителя.

При наличии навигационных приемников GPS у абонентов локальной типового комплекса связи задача взаимной временной привязки абонентов решается полностью. Точность временной привязки приёмников GPS достаточна для организации информационных

сетей, использующих методы расширения спектра и, в частности, ППРЧ.

Однако не всегда абоненты имеют навигационные приемники, которые влияют на ценовые показатели радиосредства и требуется их регистрация в Государственном комитете по радиочастотам. Особенные сложности это создает подвижным радиосредствам локальных типовых комплексов связи (например, носимым радиостанциям), так как требуется дополнительная мощность от автономного источника питания радиостанции.

Для подобного случая можно рассмотреть методику взаимной временной привязки абонентов путем пересылки времени от одной станции к другой (сверка часов по командиру). В этом случае при организации локальной сети связи одна станция выделяется как ведущая, а остальные как ведомые. Ведущая станция может иметь сопряжение с навигационными приемниками и иметь жесткую привязку к системе единого времени. При отсутствии навигационного приемника на ведущей станции, последняя организовывает локальную временную сеть, используя свой тактовый генератор как источник сигналов времени.

Возможна следующая система сигналов локальной временной сети. Ведущая станция каждые t сек. производит излучение сигналов привязки ко времени на нескольких частотных позициях. Например, $t = 10$ сек, а длительность посылок $\tau = 1.666$ мс.

Сначала станция должна передать сообщение о том, на каких частотах будут переданы сигналы отсчётов времени – преамбула. При передаче преамбулы времени станция производит излучение сигналов на нескольких, например, на трех частотных позициях, определяемых датчиком ПСП (ключом, номером сети, частотным набором), и независящих от времени.

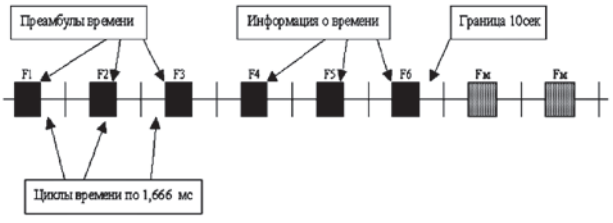


Рис. 1. Пример организации системы локального единого времени для телекоммуникационной системы с ППРЧ

В начале каждой минуты ведущая станция излучает дополнительные, например, две посылки, определяемые датчиком ПСП и текущим временем.

Ведомая станция при вхождении в связь находится в режиме ожидания преамбулы времени. Преамбулы времени излучаются, к примеру, на трех несовпадающих частотах, поэтому ожидание на приемной стороне производится по t сек. на каждой частоте, соответствующей преамбулы.

Трехкратное излучение преамбулы на разных частотах повышает помехоустойчивость от преднамеренных и непреднамеренных помех. Методика организации локальной системы единого времени для станций связи с ППРЧ иллюстрируется на рисунке 1.

Так как значение частот, на которых происходит излучение информации о времени (первые шесть посылок излучения, как показано на рисунке 1), не зависит от времени, то для локальной сети эти значения являются постоянными и зависят только от ключа датчика ПСП, номера сети и частотного набора.

Для помехозащищенной временной привязки абонентов вводится режим корректировки времени, когда по границе каждой минуты ведущая станция излучает минутную преамбулу с дополнительной синхропосылкой. При приёме минутной синхропосылки обеспечивается корректировка времени с привязкой ведомой станции к единому времени локальной сети.

Принцип вхождения в связь в локальных сетях ТКС с ППРЧ

Для локальных информационных сетей, имеющих ограниченное количество абонентов, предлагается следующий вариант вхождения в связь. При ППРЧ используется N парциальных частот в отведенном участке спектра шириной

$$f_1 - \frac{\Delta\Omega}{2} \div f_N + \frac{\Delta\Omega}{2}, \qquad (1)$$

где $\Delta\Omega$ – ширина спектра информационного сигнала.

Поэтому можно заранее выделить для абонентов одну или несколько частот f_{ki} в качестве частот ожидания и передавать на них преамбулы в виде последовательности Голда [2, 3] без модуляции передаваемым сообщением.

Сигнал преамбулы запускает генераторы ПСП приемников, генерирующие взаимно не коррелированные последовательности Голда с одинаковым периодом реализации. После приёма преамбулы синтезаторы частоты приёмников начинают управляться по закону изменения конкретной ПСП и приёмники сети связи перестраиваются по спектру синхронно со своими абонентами.

На рисунке 2 для примера показано, что передача для трех абонентов началась в момент времени $t = 3$. В момент времени $t = 4$ передатчик заканчивает передачу преамбулы на частоте ожидания и приемники, приняв преамбулу, начинают работать синхронно со своими абонентами.

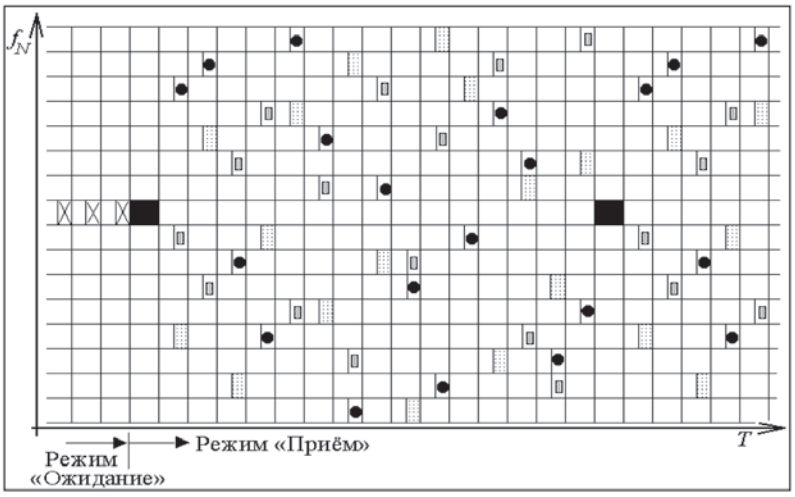
В любой момент времени передаются спектры сигналов многих абонентов сети, но каждый из них перемещается во времени по оси частот по законам некоррелированных между собой последовательностей Голда.

Поэтому после корреляционной обработки [4] на приёмной стороне информационные потоки различных M абонентов не мешают друг другу, в общем случае ухудшая соотношение сигнал/шум на входах приёмников в $(M\text{-}1)/N$ раз. Так как в локальных информационных сетях передачи информации $N >> M$, то это негативное влияние несущественно.

Преамбула передается периодически в первом блоке каждого цикла на частоте ожидания и в течение всего сеанса связи. Длительность цикла определяется длиной используемой последовательности Голда и как правило превышает в 1000 и более раз период тактовой частоты генератора ПСП. С целью маскирования передачи информации и противодействия сосредоточенным помехам дополнительно изменяется структура преамбулы при каждом новом её излучении, и абоненты переходят на работу в разных циклах с новыми реализациями ПСП.

В остальных блоках циклах передаются сигналы данных, группами по m байт каждый. Число байт в цикле зависит от скорости передачи информации в системе, при этом возможны системы ППРЧ как с быстрой, так и с медленной перестройкой рабочей частоты. Характеристики систем в зависимости от скорости перестройки по частотному диапазону значительно различаются [2]. При быстрой перестройке информационные биты дублируются на нескольких участках спектра и за счет избыточности во времени дополнительно реализуется повышенная помехоустойчивость, но и техническая реализация скоростных систем усло-жняется.

После одного периода сигналов ПСП остаётся частотно – временное рассогласование принимаемого и опорного сигналов, определяемое величиной максимального взаимного расхождения счетчиков времени приемного и передающего абонентов за период между двумя коррекциями времени.



– частота ожидания с преамбулой о начале реализации ПСП;
, , – информационные сигналы 1, 2 и 3-го абонентов;
– позиции сигналов абонентов до вхождения в связь

Рис. 2 – Частотно-временная матрица сигналов при вхождении абонентов системы с ППРЧ в связь

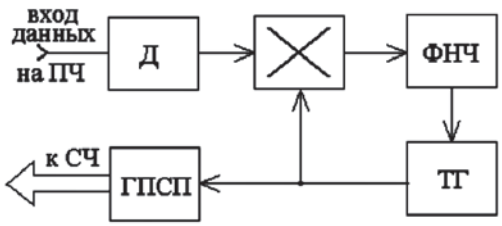


Рис. 3. Схема подстройки задержки сигнала (Д – детектор, ФНЧ – усредняющий фильтр нижних частот, ТГ – тактовый генератор для генератора псевдослучайной последовательности – ГПСП, СЧ – синтезатор частоты)

Для устранения такой ошибки можно использовать следящую схему, показанную на рисунке 3 и основанную на усреднении произведения меандра тактовых импульсов генератора ПСП приёмника и продетектированной огибающей принимаемого сигнала. Результатом перемножения становится знакопеременный сигнал, постоянная составляющая которого пропорциональна задержке входного сигнала относительно тактовых импульсов генератора ПСП.

Анализ модели следящей схемы подстройки сигнала, выполненный на ЭВМ, показал, что в результате усреднения формируется управляющее напряжение для генератора тактовых импульсов ПСП, сводящее после нескольких (3 – 5 циклов, в зависимости от параметров ФНЧ) рассогласование к минимуму. Знак сигнала управления ТГ указывает на направление перестройки, а уровень сигнала – на её величину.

Выигрыш в помехоустойчивости систем с ППРЧ, определяется коэффициентом

$$K = \frac{\Delta f}{\Delta\Omega} \to N \ , \qquad (2)$$

где $\Delta f = f_1 - \frac{\Delta\Omega}{2} \div f_N + \frac{\Delta\Omega}{2}$ – полоса частот, используемая системой связи с ППРЧ.

При многостанционном доступе этот выигрыш в некоторой степени уменьшается, как за счёт использования в каждом цикле служебного блока с сигналами преамбулы, так и за счёт ухудшения помеховой обстановки из-за соседних по своей сети станций. Можно показать, что для локальных телекоммуникационных сетей с N>2000 и с числом абонентов до 100 при корреляционной обработке проигрыш по этим причинам может составить до 10 дБ, что вполне компенсируется выигрышем. Предлагаемый принцип вхождения в связь основывается на ожидании преамбулы, в качестве которой используется последовательность Голда, представляющую собой модулирующую слабо коррелируемую последовательность в 32 бита, передаваемую на соответствующей частоте $F_{\text{пр}}$ в пределах 50 мс интервала времени – сверхцикла, содержащего преамбулу и цикл информационных посылок. Для обеспечения вхождения в связь и осуществление приёма информации необходимо, чтобы излучаемая преамбула попала в интервал ожидания на приемной стороне $T_{\text{ож}}$=50 мс. То есть, взаимное расхождение времен абонентов не должно превышать половины времени ожидания, что составляет менее 25 мс.

Для абонентов, привязанных к системе единого времени, это условие всегда соблюдается автоматически, так как привязка к системе единого времени обеспечивает точность 1мкс. Для абонентов, не имеющих привязку к системе единого времени, время проведения связи ограничивается нестабильностью опорных генераторов. При наличии опорных генераторов с нестабильностью частоты $\Delta f/f = 3\cdot10^{-7}$ время связи определится в виде

$$T_{\text{св}} = \frac{T_{\text{ож}}}{2\cdot\Delta f / f} = \frac{25\cdot10^{-3}}{2\cdot3\cdot10^{-7}} = \\ = 4{,}166(6)\cdot10^{4}\ \text{сек} = 11{,}574\ \text{ч}. \qquad (3)$$

Поэтому для поддержания надёжной связи при предлагаемом методе вхождения в связь необходимо проводить не реже одного раза в 11 часов дополнительную синхронизацию абонентов путем нового ввода или коррекции времени.

СПИСОК ЛИТЕРАТУРЫ

1. Бернюков А.К. Дискретная и цифровая обработка информации. Изд. ВлГУ, Владимир, 2002. – 160 с.

2. Финк Л.М. Теория передачи дискретных сообщений. М.: Сов радио, 1970. – 728 с.

3. Злотник Б.М. Помехоустойчивые коды в системах связи. – М.: Радио и связь, 1989, 232с.

4. Стейн С., Джонс Дж. Принципы современной теории связи и их применение к передаче дискретных сообщений. М.: Связь, 1971. – 376 с.

В.Г. Иванов
кандидат военных наук, Военная академия связи

Д.В. Петрунин
Военная академия связи

К.А. Хвостова
Военная академия связи

ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ПРИМЕНЕНИЮ ТЕХНОЛОГИЙ ВИРТУАЛЬНЫХ ИНТЕРАКТИВНЫХ 3D ПАНОРАМ ПРИ ИЗУЧЕНИИ УЗЛОВ СВЯЗИ ПУНКТОВ УПРАВЛЕНИЯ

В статье рассматриваются положения по применению технологий виртуальных интерактивных 3D панорам при изучении узлов связи пунктов управления. Рассмотрены возможности применения данных технологий в ходе проведения занятий, которые позволят создать виртуальный тренажер по изучения узлов связи и комплексов связи.

В настоящее время идёт активное поступлением новейших средств связи в части связи, для повышения качества их изучения необходимо использовать новейшие технологии, которые позволят повысить восприятие учебного материала. К таким технологиям можно отнести технологий виртуальных интерактивных туров. 3D панорамы и технологии их изготовления только начинают развиваться, хотя плоская панорамная фотография существует уже более 150 лет. Это объясняется тем, что ранее процесс создания таких фотографий был относительно трудоёмким. С появлением цифровой фотографии развитие 3D панорам получило новый импульс для развития, а обработка отснятого материала стала намного проще. Но настоящей причиной столь активного развития является значительно возросшая производительность современных компьютеров, что позволяет выполнять сложные математические расчёты в реальном времени. Панорама позволяет представить человеку окружающее пространство точно так же, как если бы он находился в месте съёмки панорамы – он может вращаться относительно точки съёмки в любую сторону и рассматривать любой участок панорамы, увеличивая его (вплоть до гигапиксельных разрешений High Definition, HD панорамы) [1]. Современный уровень развития Web-технологий позволил значительно расширить возможности панорам, добавив при этом возможность внедрения в них интерактивных эффектов.

Интерактивные эффекты позволяют создавать целые информационные системы внутри одной панорамы, включающих в себя видеоматериал, анимацию, звук, информационные окна и меню, а также различные специальные эффекты. В свою очередь, виртуальный 3Dтур – это набор таких панорам, перемещение между которыми происходит посредством специальных участков на панораме.

Достаточно только щёлкнуть мышью по такой точке или области и возникнет эффект перемещения на другую панораму. Всё это создаёт уникальные возможности по созданию виртуальных туров по известным местам, музеям и галереям с полным погружением в виртуальную реальность.

Виртуальные туры и сферические 3D панорамы, в которых используется 360°x180° панорамная проекция и интерактивное управление, являются современной и эффекти-

вной формой презентации пространства. Для просмотра 3D панорам и виртуальных туров не требуется высокой скорости для передачи данных, что позволяет размещать и активно продвигать их в сети. Для более удобной навигации можно перейти в режим полноэкранного просмотра.

В отличие от обычной видеосъёмки, обучаемый, просматривающий изображение, не зависит от того, куда направлял камеру оператор, оно находится полностью под его контролем. 3D панорама может дополняться любым текстом, звуковым сопровождением, видео роликом, всплывающими картинками и т.п.

Всего одним кликом на указателе в 3D панораме пользователь совершает настоящее путешествие, перемещаясь от одной панорамы к другой (например, боевые посты стационарного узла связи, полевые аппаратные связи). Для более удобной ориентации виртуальные туры могут сопровождаться интерактивной картой имеющей “радар”, который показывает текущее местоположение, положение камеры, а также угол зрения.

Виртуальные туры и 3D-панорамы могут стать крайне полезны для проведения занятий, которые идут в ногу со временем, не отстающих от прогресса и стремящихся вести обучение наиболее современным способом. Сфера применения виртуальных туров и 3D панорам в образовании очень широка.

Модель интерактивной 3D панорамы представлена на рис. 1. которая показывает взаимосвязь программного комплекса для разработки 3D панорам и процесса изучения дисциплины.

Просматривая 3D панораму, слушатель или курсант может получить гораздо больший объем визуальной информации, чем рассматривая обычную фотографию или презентацию. Виртуальные панорамы имеют настолько высокой способностью отражать реальность, что могут практически заменить физическое посещение объекта, будь то стационарный или полевой узел связи. Обучаемый имеет возможность изучить материал в наглядном и удобном виде самостоятельно, не выходя из класса, в удобное время.

Несколько сферических панорам, которые объединены со схемой-картой в виртуальную презентацию, могут отлично показать планировку элементов узла связи и аппаратных связи, объем помещений (аппаратной) и, помогая создать представление об объекте .

Рис. 1. Обобщенная модель функционирования интерактивной 3D панорамы

Виртуальные туры помогают создать иллюзию присутствия обучаемого на объектах узлов связи, с использованием механизмов интеграции изучить состав его элементов и даже необходимых типов аппаратуры. При использовании flash-модулей перейди к непосредственной настройки аппаратуры на виртуальном стенде.

Виртуальная панорама позволит отлично демонстрировать состав, размещение аппаратуры аппаратной или боевого поста. Даже с небольшим размером.

Панорамная 3D фотография и виртуальный туры обладают множеством преимуществ перед другими способами представления. Главными преимуществами являются – фотореалистичность, интерактивность, наглядность. Данное сочетание выгодно отличает виртуальные туры от других средств визуализации.

Даже современная фотография с использованием новейшей техники не может обеспечить интерактивности, и не даёт полностью погрузиться в получаемое изображение. Виртуальная панорама к тому же позволяет в одно изображение поместить весь объем пространства, показать взаимное расположение предметов, лучше передать перспективу. Изображение можно рассматривать под любым угодно углом и сколько угодно времени.

Виртуальный тур, созданный основе панорамных фотографий интерактивен - даёт возможность нелинейного просмотра, переходя от из одного помещения в любое другое. Данное качество особенно ценно для создания Web-презентаций, где есть возможность показать все и просмотреть только то, что необходимо. Компьютерные 3D-модели, которые созданы посредством 3dmax, ArCon и других программ предназначенных для архитектурного проектирования, по сравнению с виртуальными турами и панорамными фотографиями обладают гораздо меньшей фотореалистичностью.

Готовый виртуальный тур для изучения узлов связи пунктов управления может представлять собой:

– исполняемый файл Windows, для просмотра на компьютере с диска или flash-карточки;

– готовый к публикации на сайте модуль, который можно включить в любой сайт для просмотра;

– виртуальный тур можно оптимизировать и настроить для демонстрации на планшетных компьютерах.

Заключение

Используемое программное обеспечение для демонстрации тура на сайте или локальном ресурсе ВВУЗа подобрано таким образом, чтобы экономить амортизацию внешних носителей при просмотре панорам за счёт создания многослойной – «шахматной» системы загрузки изображений.

При просмотре панорамы загружается лишь та область, которая используется в данный момент, что экономит интернет трафик и позволяет уменьшить место для хранения и воспроизведения виртуальных туров.

В виртуальном туре возможна демонстрация фотографий, видеороликов, вывод текстовой информации, логика действий и запрограммированные последовательности показа, что незаменимо для презентаций.

Предлагаемая технология позволяет погружать обучаемых в виртуальное пространство узла связи пункта управления или его элемент. Даёт возможность усилить восприятие учебного материала.

СПИСОК ЛИТЕРАТУРЫ

1. Панорамный мир. 2010. URL: http://panoworld.narod.

2. Дорофеев С.Ю., Тюгаев Д.Н. Создание аппаратно-программного комплекса для изготовления виртуальных туров на основе интерактивных 3Dпанорам // Инновационные технологии кафедры КСУП: Научно- практическая конференция. - Томск, 2008.

А.А. Иванов
кандидат технических наук

А.В. Огоцкий
Военно-космическая академия имени А.Ф. Можайского

ВАРИАНТЫ АДАПТАЦИИ ПРОГРАММНО-АЛГОРИТМИЧЕСКОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ К ИЗМЕНЕНИЮ «ВНЕШНЕЙ» СРЕДЫ

В статье рассмотрен вопрос адаптации программно-алгоритмического обеспечения автоматизированных систем управления (АСУ) к изменению факторов «внешней» среды. Рассмотрены основные посылки к созданию единого информационного пространства (ЕИП) и имеющиеся при этом ограничения.

Введение

Расширение задач Войск Воздушно-космической обороны (ВВКО), увеличение пространственного охвата системами разведки, освещения обстановки и связи выдвигают проблему качественного улучшения процесса управления силами и средствами ВВКО.

Необходимость совершенствования АСУ требует разрешения сложной задачи, связанной, с одной стороны, с разработкой надёжных, быстродействующих средств вычислительной техники, с другой - с разработкой и реализацией на этих средствах большого числа математических моделей воздушных и космических операций, адекватных фактическим действиям сил и процессу управления ими в боевых условиях.

Основные ограничения создания единого информационного пространства

Предполагается, что достигнуть качественно нового уровня в автоматизации процессов управления средствами ВВКО можно путём интеграции всех управляющих систем и комплексов в ЕИП. Для создания ЕИП могут привлекаться информационные средства систем предупреждения о ракетном нападении, контроля космического пространства, противоракетной обороны, а также средства систем разведки взаимодействующих видов ВС.

Вместе с тем использование уже имеющихся управляющих структур и связей между ними имеет ряд ограничений, таких как: - отсутствие полной совместимости информации, циркулирующей в АСУ различных уровней; - отсутствие единого подхода в формировании и использовании информационных ресурсов; - отсутствие гарантированных механизмов доступа и управления доступом к информационным ресурсам; – отсутствие единого стандарта при проектировании и разработки средств информационного управления.

Кроме этого, основными источниками случайных воздействий на работу АСУ являются факторы «внешней» среды и отклонения от нормальных режимов функционирования (ошибки, шумы и т.д.), возникающие внутри системы [2, 4].

Существенным фактором является случайное колебание нагрузки, вызываемое увеличением числа абонентов и соответственно потока событий. Это предъявляет повышенные требования к пропускным способностям элементов системы, к оперативности управления её функционированием и может привести к снижению качества работы, поэтому устойчивость к входным перегрузкам – одно из важнейших требований к современным АСУ военного назначения.

К выбору вариантов адаптации ПАО

Известны методы [4], используемые для адаптации ПАО к изменению характеристик «внешней» среды: параметрический, функциональный, организационный и структурный, а также методы «размножения» и «развития», присущие перспективным самоорганизующимся системам.

Более простым вариантом адаптации является параметрический, заключающийся в изменении параметров, определяющих поведение и функционирование ПАО. В этом случае выбор приемлемого способа обработки колебаний нагрузки (перегрузок) возможен путём буферизации входных потоков, при этом размер буфера зависит от характеристик обслуживаемых абонентов и параметров самого вычислительного комплекса АСУ.

В работе [3] предложен алгоритм регулирования размера демпфирующего буфера, базирующийся на периодическом итеративном расчёте его величины. На этапе настройки, устанавливается некий исходный размер, а на этапе эксплуатации он итеративно корректируется по измеренным характеристикам.

Алгоритм приемлем в системах, где периоды повторяющегося поведения могут составлять от суток до года и более [1] и совсем не подходит для АСУ военного назначения, где период повторения событий составляет минуты и даже доли секунд.

Другим вариантом адаптации может стать увеличение темпа обработки событий при увеличении входного потока сообщений.

В этом случае необходим переход к концепции «активного слежения» за потоками входной информации, осуществляемого с помощью специализированной управляющей ЭВМ («диспетчера»). Суть работы такова, что когда «диспетчером» запланирован приём новых сообщений от абонентов, аппаратура приёма и обработки ожидает поступление информации с указанного ЭВМ направления.

Заключение

Таким образом, исходя из замысла построения ЕИП, в его основу будут положены пункты и центры сбора и обработки разведывательной информации, объединённые информационно-управляющей сетью, что даст возможность сбора, обработки и оперативного доведения разведывательных данных до потребителей. В условиях жестких временных ограничений на принятие решений, вопрос о увеличении продолжительности безотказной работы АСУ является актуальным.

СПИСОК ЛИТЕРАТУРЫ

1. Бесекерский В.А. Теория систем автоматического регулирования / В.А. Бесекерский, Е.П. Попов. – М.: Наука, 1975. – 768 с.

2. Мамиконов А.Г. Основы построения АСУ. – М.: «Высшая школа», 1981. – 248 с.

3. Лукин Д.В. Адаптация систем сбора данных к входным перегрузкам. Известия ВУЗ №2, 2008. 47 – 55 с.

4. Шеннон Р. Имитационное моделирование систем – искусство и наука / Под ред. Е.К. Масловского. – М.: Изд. Мир, 1978. – 411 с.

А.А. Кокуев
инженер-программист ОАО «Концерн «Системпром»

МЕТОДЫ ОПТИМИЗАЦИИ В ЗАДАЧЕ САМОСТОЯТЕЛЬНОГО ПОИСКА СРЕДСТВ ВОЗДУШНОГО НАПАДЕНИЯ ПРОТИВНИКА

Пусть в некоторой области происходит налет средств воздушного нападения (СВН) противника (см. рис. 1). Налет осуществляется на некоторой высоте, летательные аппараты движутся со скоростью v. Перпендикулярно налету очерчивается фронт, который, не будучи обнаруженной, не должен пересечь ни один летательный аппарат противника. В распоряжении имеется m аэродромов, на каждом из которых в боевой готовности находится некоторое количество истребителей k_j, где j – номер аэродрома.

Задача самостоятельного поиска [1] СВН противника заключается в создании оптимального плана дежурства истребителей в районе налета, при котором все ракеты будут обнаружены до того, как они пересекут заданный фронт. Область налета можно разделить на некоторое

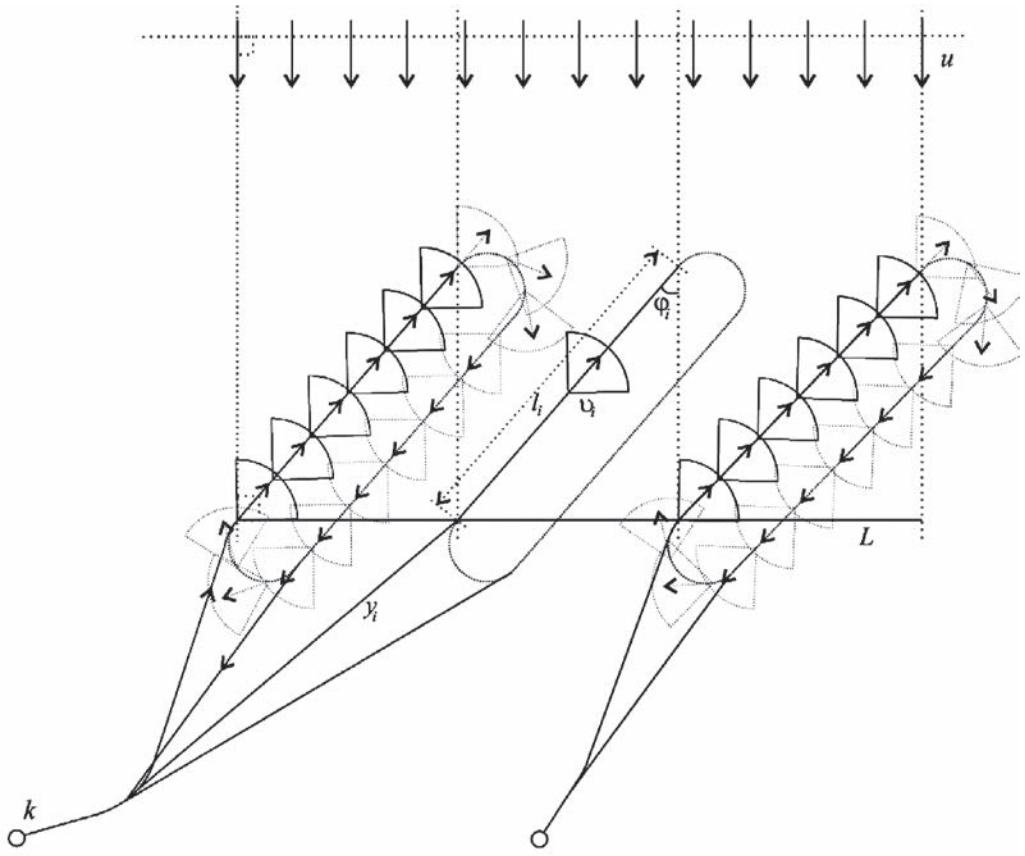


Рис. 1. Процесс поиска летательных аппаратов

количество зон n. В каждой i-ой зоне осуществляют дежурство некоторое количество истребителей y_i. Каждый истребитель просматривает определенную территорию, прикрывая тем самым определенную часть фронта. Поскольку истребитель находится в движении, территория, которую он просматривает, также движется. Для того, чтобы просматривать территорию постоянно необходимо, чтобы следом по такой же траектории следовал другой истребитель. Таким образом, образуется цепочка, состоящая из y_i истребителей.

Поскольку требуется обеспечить, чтобы ни одно СВН не пересекло фронт не будучи обнаруженным, необходимо рассмотреть какая ширина фронта просматривается одним истребителем. Если все истребители в совокупности просматривают всю ширину фронта, то ни одно СВН не сможет пролететь необнаруженным и фронт будет прикрыт. Если предположить, что в одной зоне дежурят истребители одного типа, то критерием качества поиска является ширина прикрываемого в процессе поиска фронта $h(\varphi_i)$. Тогда критерий качества в задаче поиска можно сформулировать следующим образом:

$$\max J(y_{ij}) = h(\varphi)\sum_{j=1}^{m}\sum_{i=1}^{n} y_{ji}.$$

Основным ограничением при самостоятельном поиске является запас топлива. Топливо необходимо для совершения маневров. Топливо расходуется как для того, чтобы долететь до зоны поиска, так и для осуществления поиска. Запас топлива является ограничением при выполнении поиска, влияя на количество времени, которое каждый истребитель может провести в зоне поиска.

Истребитель имеет ограниченный запас топлива в баках. Пусть у истребителя перед взлетом есть определенный запас топлива Q_i^0. Чтобы взлететь и долететь до точки начала поиска, а также чтобы вернуться обратно истребителю нужно некоторое количество топлива Q_i^1. После посадки должен остаться определенный запас топлива Q_i^2. На участке поиска известен километровый расход топлива q_i. Можно оценить максимальную длину траектории истребителя в зоне поиска:

$$l_i^{общ} \le \frac{Q_i^0 - Q_i^1 - Q_i^2}{q_i}.$$

В каждой зоне поиска находится y_i истребителей, в то время, как максимальное число истребителей на одном аэродроме равно k:

$$\sum_{i=1}^{n} y_i \le k.$$

В каждой зоне дежурства необходимо обеспечить непрерывное наблюдение, для этого истребители должны осуществлять полет колонной, поддерживая определенную дистанцию d_i между собой. А это значит, что длину рабочей прямой и количество истребителей в зоне можно связать равенством:

$$l_i^{общ} = d_i y_i.$$

Ширину прикрываемого фронта можно оценить как сумму проекций рабочих прямых на весь фронт:

$$\sum_{i=1}^{m} l_i \sin\varphi_i.$$

При этом ширина прикрываемого фронта не должна превышать ширины всего фронта:

$$\sum_{i=1}^{m} l_i \sin\varphi_i \le L$$

С учетом рассмотренных критерия качества и ограничений, задача самостоятельного поиска может быть сведена к следующей задаче оптимизации:

$$\max J(y_{ij}) = h(\varphi)\sum_{j=1}^{m}\sum_{i=1}^{n} y_{ji},$$

$$\begin{cases} y_{ij} > 0, \ \forall i \in 1,\dots,n, \ \forall j \in 1,\dots,m \\ y_{ij} \le q_{ij}, \ \forall i \in 1,\dots,n, \ \forall j \in 1,\dots,m \\ \sum_{i=1}^{n} y_{ij} \le k_j, \ \forall j \in 1,\dots,m \\ \sum_{i=1}^{n}\sum_{j=1}^{m} y_{ij} \le l(\varphi). \end{cases}$$

Предложенная задача оптимизации является задачей нелинейного программирования, поскольку в критерии качества и в одном из ограничений присутствуют элементы, нелинейно

зависящие от угла поиска φ. Если же угол φ считать постоянным, то задачу можно будет отнести к классу задач линейного программирования. Таким образом, предложенную задачу нелинейного программирования можно решить путем перебора по всем углам φ и решении для каждого из них задачи линейного программирования. После чего из полученных значений критерия качества необходимо выбрать максимальный, что определит угол поиска, а соответствующее этому углу решение задачи линейного программирования определит количество истребителей участвующих в поиске. Предлагаемый способ решения является реализацией метода градиентного спуска [2].

Задача линейного программирования может быть решена различными способами. Одним из таких методов является симплекс-метод [3-5]. Другим способом решения задач линейного программирования является метод построения дерева решений [6]. Метод дерева решений предполагает предварительный расчет возможных решений задачи линейного программирования, с учетом известных и постоянных элементов задачи, таких как коэффициенты в матрице ограничений, столбце свободных членов и критерии качества. К преимуществам метода дерева решений можно отнести крайне высокую скорость работы по сравнению с симплекс-методом. Основным его недостатком является необходимость предварительных достаточно ресурсоемких расчетов.

При решении задачи самостоятельного поиска было проведено сравнение быстродействие этих двух методов на испытательном стенде.

Стенд состоял из персональной ЭВМ со следующей конфигурацией:

• Микропроцессор: Intel Core 2 Duo CPU E6850 @ 3,00 GHz,

• ОЗУ: 3,25 Гб (PC2-6400).

Измерение быстродействия проводилось с использованием счетчика тактов, встроенного в микропроцессор, т.к. это единственный из существующих методов измерения, позволяющий измерить время выполнения небольших участков кода [7]. Для того, чтобы измерить количество прошедших тактов процессора, необходимо получить количество тактов до начала процедуры и после ее завершения. Разница между этими двумя значениями и есть количество прошедших тактов процессора.

Измерялось время решения одной задачи с заданным количеством используемых аэродромов. Чтобы избежать влияния программного и аппаратного непостоянства, эксперимент повторялся для каждой размерности примерно 8000 раз. После чего отбрасывались измерения отличающиеся от среднего более чем в 20 раз. Результаты измерения представлены в таблице 1.

Таблица 1.

Результаты сравнения быстродействия алгоритмов с использованием дерева решений и симплекс-метода

Количество аэродромов	Симплекс-метод	Дерево решений	Прирост быстродействия
1	$(160\pm2)\cdot10^2$ тактов	272±1 тактов	в 59 раз
2	$(186\pm2)\cdot10^2$ тактов	296±1 тактов	в 63 раза
3	$(196\pm2)\cdot10^2$ тактов	298±1 тактов	в 66 раз
4	$(212\pm2)\cdot10^2$ тактов	308±1 тактов	в 69 раз
5	$(266\pm2)\cdot10^2$ тактов	315±1 тактов	в 84 раза
6	$(281\pm2)\cdot10^2$ тактов	320±1 тактов	в 88 раз
7	$(279\pm3)\cdot10^2$ тактов	326±1 тактов	в 86 раз
8	$(268\pm3)\cdot10^2$ тактов	332±2 тактов	в 81 раз
9	$(261\pm3)\cdot10^2$ тактов	339±1 тактов	в 77 раз
10	$(364\pm5)\cdot10^2$ тактов	345±2 тактов.	в 105 раз

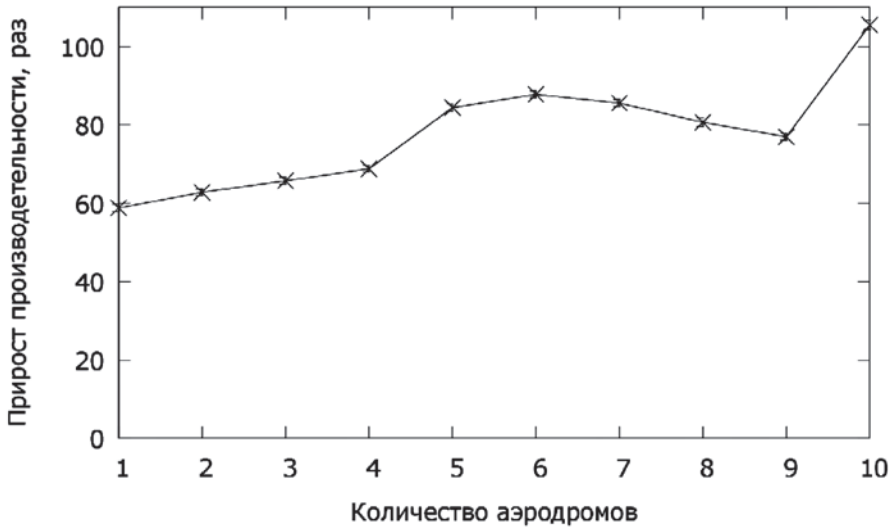


Рис. 2. График зависимости прироста производительности от количества аэродромов

По данным из таблицы 1 был построен график зависимости прироста производительности от количества аэродромов.

Из графика и таблицы видно, что быстродействие алгоритма использующего дерево решений более предсказуемо, чем алгоритма использующего симплекс-метод. Кроме того, алгоритм использующий дерево решений работает значительно быстрее, чем алгоритм использующий симплекс-метод: средний прирост быстродействия составил: 78 раз.

СПИСОК ЛИТЕРАТУРЫ

1. Авиация ПВО России и научно-технический прогресс: боевые комплексы и системы вчера, сегодня, завтра: монография / Под ред. Е. А. Федосова. – М.: Дрофа, 2005. –– 815 с.

2. Химмелблау Д. Прикладное нелинейное программирование / Под ред. М. Л. Быховский. – М. : Издательство «Мир», 1973. –– 526 р.

3. Таха Хэмди А. Введение в исследование операций. – 7 изд. – М. : Издательский дом «Вильямс», 2007. – 912 с.

4. Ашманов С. А. Линейное программирование. –М. : Наука, 1981. – 340 с.

5. Методы математического программирования в задачах оптимизации сложных технических систем / А. М. Загребаев, Н. А. Крицына, Ю. П. Кулябичев, Ю. Ю. Шумилов. – М. : МИФИ, 2007. – 332 с.

6. Кокуев А. А., Ктитров С. В. Построение дерева решений в задачах линейного программирования // Тезисы докладов XX международного научно-технического семинара «Современные технологии в задачах управления, автоматики и обработки информации». – М. : Изд-во ПГУ, 2011. – С. 321–322.

7. Касперски К. Техника оптимизации программ. Эффективное использование памяти. – СПб. : БХВ-Петербург, 2003. – 464 с.

А.С. Корсунский
кандидат технических наук
Федеральный научно-производственный центр ОАО «НПО «Марс»

Т.Н. Масленникова
кандидат технических наук
Федеральный научно-производственный центр ОАО «НПО «Марс»

ЗАЩИЩЕННЫЙ ОБМЕН МЕЖДУ АВТОМАТИЗИРОВАННЫМИ РАБОЧИМИ МЕСТАМИ НА БАЗЕ ПЛАНШЕТНЫХ КОМПЬЮТЕРОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

В статье рассмотрен подход к обеспечению защищенного обмена по беспроводному интерфейсу между автоматизированными рабочими местами (АРМ) на базе планшетных персональных компьютеров в автоматизированных системах (АС) различного назначения. Данный подход исключает наличие в планшетном персональном компьютере аппаратных средств защиты информационного обмена.

Введение

Бурное развитие информационно-телекоммуникационных технологий, рост производительности и миниатюризация микропроцессорной техники предопределяют внедрение в состав АС различного назначения новых устройств, таких как планшетные персональные электронно-вычислительные машины (ПЭВМ), смартфоны и т.д. [1]. Взаимодействие данных устройств осуществляется по беспроводному интерфейсу (например, по технологии 802.11a/b/g/n и др.). Ни для кого не секрет, что ряд АС может обрабатывать конфиденциальную информацию или информацию, составляющую коммерческую тайну. Поэтому актуальной является задача обеспечения защищенного обмена между АРМ таких АС.

Подход к защищенному обмену между АРМ на базе планшетных компьютеров

Предлагаемая к рассмотрению система обеспечения безопасности информации состоит из станции управления ключевой информацией, модуля управления беспроводным соединением и клиентской частью, представляющей собой планшетный компьютер с установленным специализированным программным обеспечением (рис.1).

Клиентское оборудование представляет собой планшетный компьютер, функционирующий под управлением доверенной операционной системы. В выключенном состоянии основные модули операционной системы и данные находятся в зашифрованном состоянии. При включении после удачного прохождения процедуры аутентификации и получения ключей загрузчик клиентского устройства осуществляет расшифрование модулей операционной системы и данных и загрузку операционной системы. Ключевая информация, расшифрованные модули операционной системы и данные хранятся в оперативной памяти клиентского оборудования и после выключения питания теряются. Благодаря этому клиентское оборудование в выключенном состоянии не содержит в себе сведений конфиденциального характера.

Станция управления ключевой информацией выполняет следующие задачи:

хранение ключей парной связи для всех комплектов клиентского оборудования в базе данных устройства в зашифрованном виде;

поэкземплярный учет ключей, сроков их действия;

Рис. 1. Обобщенная схема системы обеспечения безопасности информации

стирания;

создание и хранение логина и кодового слова (пароля) для аутентификации пользователей клиентского оборудования;

генерацию и хранение и удаление открытого и закрытого ключей для передачи клиентской части ключей парной связи;

управление сеансом идентификации и аутентификации, передачу ключей парной связи клиентскому оборудованию;

добавление, удаление ключей парной связи из базы данных устройств;

ведение в зашифрованном виде журнала регистрации событий на устройстве для ведения аудита безопасности;

ввод информации для проверки целостности программного обеспечения с отображением результатов проверки на подключаемом мониторе.

Модуль управления беспроводным соединением должен обеспечивать взаимодействие клиентских устройств по беспроводному интерфейсу с аутентификацией каждого из устройств и взаимодействие со станцией управления ключевой информацией.

Процедура аутентификации и получения ключевой информации с использованием концепции открытого распределения ключей показана на рис.2.

В рассматриваемом случае клиентское оборудование в выключенном состоянии не хранит ключевой информации. При включении клиентского оборудования и установлении сетевого соединения загрузчик клиентского оборудования посылает станции управления ключевой информацией аутентифицирующую информацию (полученная ранее оператором клиентского оборудования кодовая фраза, которую необходимо ввести при аутентификации, электронный ключ, содержащийся, например, на флеш-носителе, либо что-то еще) и запрос на получение ключа для расшифровки программного обеспечения и данных. После успешного прохождения аутентификации станция управления ключами передает в зашифрованном виде закрытый ключ для расшифрования ключа шифрования модулей операционной системы и данных. После успешного получения закрытого ключа клиентское оборудование осуществляет его расшифрование (ключем для расшифрования является кодовая фраза, получаемая оператором от администратора станции управления ключами). После успешного расшифрования ключа для расшифрования модулей операционной системы и данных клиентское оборудование осуществляет расшифрование модулей операционной системы и данных, после чего осуществляется загрузка операционной системы. По окончании загрузки операционной системы клиентское оборудование передает станции управления ключами сообщение о завершении расшифрования модулей операционной системы и данных. После получения этого сообщения станция управления ключами отправляет запрос на получение кодовой последовательности, которая была расшифрована вместе с данными. Клиентское оборудование передает кодовую по-

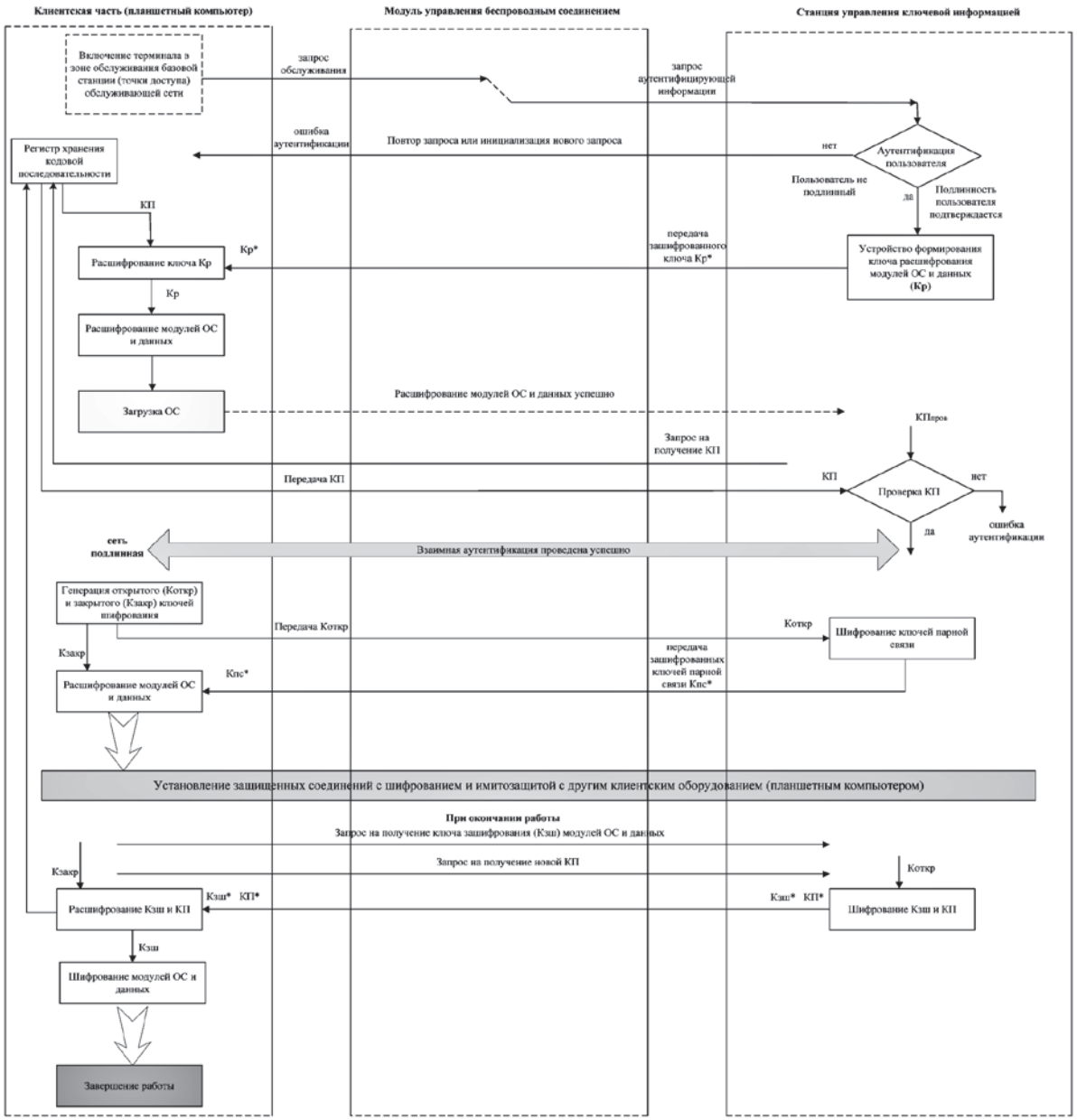


Рис. 2. Процедура аутентификации и получения ключевой информации с использованием концепции открытого распределения ключей

следовательность станции управления ключами, после чего ожидает сообщения об успешном прохождении аутентификации. После сообщения об успешном прохождении аутентификации клиентское оборудование создает открытый и закрытый ключи для шифрования ключей парной связи и отправляет открытый ключ. Станция управления ключами при помощи открытого ключа зашифровывает ключи парной связи и отправляет клиентскому оборудованию. Приняв зашифрованные ключи парной связи, клиентское оборудование расшифровывает их при помощи закрытого ключа.

В дальшейшем взаимодействие с комплектами клиентского оборудования осуществляется с использованием ключей парной связи. Перед завершением работы клиентское оборудование отправляет станции управления ключами запрос на получение ключа для зашифрования модулей операционной системы и данных, а так же новой кодовой последовательности. Станция управления ключами шифрует новые

ключ для зашифрования операционной системы и данных и кодовую последовательность на полученном при начале сеанса работы от клиентского оборудования открытом ключе и передает зашифрованные данные клиентскому оборудованию. Клиентское оборудование осуществляет расшифрование полученных от станции управления ключами ключа и кодовой последовательности, а так же сохранение кодовой последовательности. После этого клиентское оборудование на полученном ключе зашифровывает модули операционной системы и данные и завершает сеанс работы. В начале следующего сеанса работы станция управления ключами на запрос клиентского оборудования передает тот ключ шифрования модулей операционной системы и данных, на котором осуществлялось зашифрование модулей операционной системы и данных при завершении предыдущего сеанса работы [2-5].

В данном случае возможны два варианта исполнения станции управления ключами: на базе промышленной ПЭВМ, с возможностью подключения по мере необходимости монитора, клавиатуры и мыши, с разработкой доверенной операционной системы, либо разработка специализированной аппаратуры.

Заключение

Необходимо отметить, что существуют еще ряд подходов к обеспечению защищенного обмена между ПЭВМ на базе планшетных компьютеров. Так, например, это может быть реализовано путем физического распределения ключей расшифрования модулей операционной системы, данных и ключей парной связи, либо размещением модулей операционной системы и данных на flash-накопителе. Представленный выше подход к обеспечению защищенного обмена между АРМ на базе планшетных компьютеров направлен в первую очередь на исключение из их состава аппаратной компоненты системы шифрования, что значительно облегчает работу службе эксплуатации и службе экономической безопасности организации.

СПИСОК ЛИТЕРАТУРЫ

1. Оков И.Н. Аутентификация речевых сообщений и изображений в каналах связи / под ред. В.Ф. Комаровича. –СПб.: Изд-во Политехн. ун-та, 2006.

2. Комарович В.Ф., Оков И.Н., Корсунский А.С. Защита подлинности информации в ССПО. Сборник материалов НТК «Проблемы совершенствования и развития специальной связи и информации, предоставляемых государственным органам», Орел, Академия ФСО, 2007.

3. Корсунский А.С. Анализ методов обеспечения подлинности и доступности информации и услуг в сетях подвижной радиосвязи//Научно-технические ведомости СПбГПУ–2008,–№ 2–с.55–59.

4. Корсунский А.С., Маттис А.В., Масленникова Т.Н. Подход к реализации защищенного обмена между АРМ на базе планшетных ПЭВМ в АСУ различного назначения. - Материалы межотраслевой НПК, «ВОКОР-2012» , НИИ К и В ВУНЦ ВМФ «ВМА», С.-Петербург, 2012.

5. Корсунский А.С., Масленникова Т.Н., Лучков Н.В. Обеспечение защищенного обмена между АРМ на базе планшетных ПЭВМ в АСУ различного назначения. - Сборник материалов НТК «Состояние, проблемы и перспективы создания корабельных информационно-управляющих комплексов», ОАО «Концерн «Моринформсистема-Агат», Москва, 2013.

М. А. Коцыняк
И.А. Кулешов
***О.С.** Лаута*

ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ КОМПЬЮТЕРНОЙ АТАКИ ТИПА «ЛОГИЧЕСКАЯ ПОДМЕНА СЕРВЕРА»

В статье рассматривается модель, предназначенная для определения вероятностно-временных характеристик компьютерной атаки типа «Логическая подмена сервера»

Одной из проблем безопасности распределенной информационно-телекоммуникационной сети (ИТКС) является недостаточная идентификация и аутентификация ее удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в распределенных ИТКС эта проблема решается в процессе создания виртуального канала объекты ИТКС обмениваются определенной информацией, уникально идентифицирующей данный канал. Однако, не всегда для связи двух удаленных объектов в ИТКС создается виртуальный канал, зачастую, особенно для служебных сообщений, используется передача одиночных сообщений, не требующих подтверждения.

Для адресации сообщений в распределенных ИТКС используется сетевой адрес, который уникален для каждого объекта ИТКС. Сетевой адрес также может использоваться для идентификации объектов ИТКС. Однако сетевой адрес достаточно просто подделывается и поэтому возможна реализация компьютерной атаки типа «Логическая подмена сервера» [1].

Компьютерные атаки (КА) обладают вероятностно-временными характеристиками (ВВХ), определение которых позволяет оценить степень их опасности, выбрать и реализовать меры защиты.

Для исследования и определения ВВХ КА необходима разработка ее модели. Одним из подходов к решению этой задачи является разработка модели (профильной, математической) компьютерной атаки.

Профильная модель компьютерной атаки типа «Логическая подмена сервера».

Злоумышленник осуществляет КА в следующей последовательности:

– запуск программно-аппаратного комплекса (сетевого сканера) за среднее время $\overline{t}_{зап}$ с функцией распределения времени *W(t);*

– перехват с вероятностью P_n сетевого адреса атакуемой ИТКС за среднее время $\overline{t}_{перех}$ с функцией распределения времени *M(t);*

– формирование ложного сетевого адреса за среднее время $\overline{t}_{адрес}$ с функцией распределения времени *D(t);*

– направление запроса с ложным сетевым адресом на маршрутизатор атакуемой ИТКС за среднее время $\overline{t}_{запрос}$ с функцией распределения времени *L(t);*

– получение запроса (сообщения) маршрутизатором и внесение изменений в таблицу маршрутизации за среднее время $\overline{t}_{изм}$ с функцией распределения времени *Q(t);*

Если сетевой адрес не перехвачен, то с вероятностью (1-P_n) будет повторно организован его перехват за среднее время $\overline{t}_{повт}$ с функцией распределения времени *Z(t)*.

Математическая модель КА типа «Логическая подмена сервера» (рис. 1).

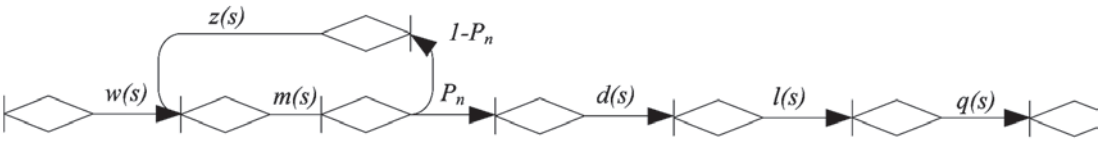


Рис. 1. Стохастическая сеть компьютерной атаки типа «Логическая подмена сервера»

Используя уравнение Мейсона, преобразование Лапласа, разложение Хевисайда и метод топологического преобразования стохастических сетей [2], функцию распределения вероятности времени реализации КА можно определить следующим образом

$$F(t)=\sum_{k=1}^{6}\frac{w\cdot m\cdot P_n\cdot d\cdot l\cdot q\cdot(z+s_k)}{\varphi'(s_k)}\cdot\frac{1-\exp[s_k t]}{-s_k}, \quad (1)$$

а среднее время $\overline{T}$, затрачиваемое на реализацию компьютерной атаки:

$$\overline{T}=\sum_{k=1}^{6}\frac{w\cdot m\cdot P_n\cdot d\cdot l\cdot q\cdot(z+s_k)}{\varphi'(s_k)}\cdot\frac{1}{(-s_k)^2}, \quad (2)$$

где: $w(s)=\int_0^\infty \exp(-st)d[W(t)]=\frac{w}{w+s}$ – преобразование Лапласа функции распределения времени запуска сетевого сканера;

$m(s)=\int_0^\infty \exp(-st)d[M(t)]=\frac{m}{m+s}$ – преобразование Лапласа функции распределения времени перехвата сетевого адреса;

$d(s)=\int_0^\infty \exp(-st)d[D(t)]=\frac{d}{d+s}$ – преобразование Лапласа функции распределения времени формирования ложного сетьевого адреса;

$l(s)=\int_0^\infty \exp(-st)d[L(t)]=\frac{l}{l+s}$ – преобразование Лапласа функции распределения времени направления запроса с ложным сетевым адресом;

$q(s)=\int_0^\infty \exp(-st)d[Q(t)]=\frac{q}{q+s}$ – преобразование Лапласа функции распределения времени внесения изменений в таблцу маршрутизации;

$z(s)=\int_0^\infty \exp(-st)d[Z(t)]=\frac{z}{z+s}$ – преобразование Лапласа функции распределения времени повторного перехвата сетевого адреса;

$W(t)=1-\exp[-wt]$ – функция распределения времени запуска сетевого сканера;

$M(t)=1-\exp[-mt]$ – функция распределения времени перехвата сетевого сканера;

$D(t)=1-\exp[-dt]$ – функция распределения времени формирования ложного сетевого адреса;

$L(t)=1-\exp[-lt]$ – функция распределения времени направления запроса с ложным сетевым адресом;

$Q(t)=1-\exp[-qt]$ – функция распределения времени внесения изменений в таблицу маршрутизации;

$Z(t)=1-\exp[-zt]$ – функция распределения времени повторного прехвата сетевого адреса;

$w=1/\overline{t_{\text{зап}}}, m=1/\overline{t_{\text{перех}}}, d=1/\overline{t_{\text{адрес}}}, q=1/\overline{t_{\text{запрос}}}, \quad =1/\text{ изм},$ $q=1/\overline{t_{\text{изм}}}, z=1/\overline{t_{\text{повт}}}$ – параметры распределения; $\overline{t_{\text{зап}}}$, $\overline{t_{\text{перех}}}$, $\overline{t_{\text{адрес}}}$, $\overline{t_{\text{запрос}}}$, $\overline{t_{\text{изм}}}$, $\overline{t_{\text{повт}}}$ – среднее время каждого процесса КА; $\varphi'(s_k)$ – значение производной многочлена знаменателя в точке s_k.

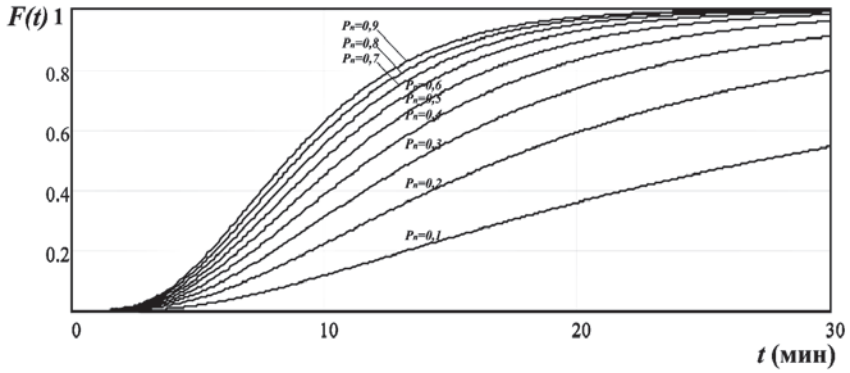
Зависимости функции распределения вероятности $F(t)$ и среднего времени представлены на рисунке 2. В качестве исходных данных используются следующие значения времени и вероятности, соответствующие профильной модели компьютерной атаки типа «Логическая подмена сервера»

$$\overline{t_{\text{зап}}}=2\text{ мин}, \overline{t_{\text{перех}}}=1\text{ мин}, \overline{t_{\text{адрес}}}=1\text{ мин},$$
$$\overline{t_{\text{запрос}}}=3\text{ мин}, \overline{t_{\text{изм}}}=2\text{ мин}, P_n=0{,}1\ldots0{,}9.$$

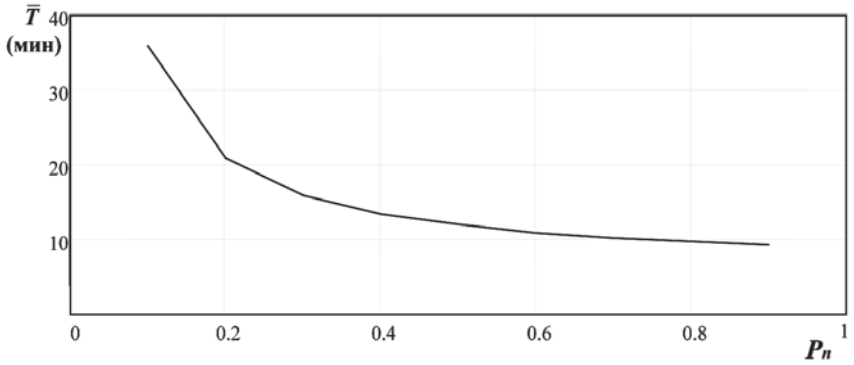
Анализ полученных результатов позволяет сделать выводы:

– среднее время реализации компьютерной атаки «Логическая подмена сервера» с вероятностью P_n=0,1 составляет 35 мин. и 9 мин. при P_n=0,9;

– полученные зависимости позволяют оценить влияние вероятности перехвата сетевого адреса атакуемой ИТКС на показатель эффективности реализации компьютерной атаки. Видно, что увеличение вероятности P_n повышается эффективность компьютерной



а) зависимость интегральной функции распределения вероятностей от времени реализации компьютерной атаки



б) зависимость среднего времени реализации компьютерной атаки от вероятности перехвата сетевого адреса

Рис. 2. Вероятностно-временные характеристики компьютерной атаки типа «Логическая подмена сервера»

атаки. Однако, по мере возрастания значения P_n степень влияния на интегральную функцию распределения $F(t)$ уменьшается и при преодолении значения P_n>0,4 степень влияния пренебрежимо мала;

– результаты моделирования могут быть использованы при обосновании направлений разработки системы защиты ИТКС, целью которой является предотвращение (затруднение) реализации компьютерной атаки.

СПИСОК ЛИТЕРАТУРЫ

1. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через INTERNET - СПб: Мир и семья-95, 1998. – 296 с.

2. Привалов А.А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. – СПб: ВМА, 2000 г.

Ю.Л.Кругляк
кандидат технических наук доцент
Д.О.Петрич
кандидат технических наук
Ю.А.Загрутдинов
Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военно-космическая академия имени А.Ф.Можайского» Министерства обороны Российской Федерации

МНОГОУРОВНЕВЫЙ ПОДХОД И ДЕКОМПОЗИЦИЯ ПРИ МОДЕЛИРОВАНИИ СИСТЕМЫ ПАМЯТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ВОЕННОГО НАЗНАЧЕНИЯ

В работе описан научно-методический подход к моделированию многоуровневой системы памяти, приведены выражения для расчета основных показателей надежности. Представленную модель целесообразно использовать для проведения сравнительной оценки различных методов повышения надежности при разработке систем памяти перспективных вычислительных средств автоматизированных систем управления военного назначения.

Запоминающие устройства (ЗУ) в отношении повторяемости элементов являются наиболее однородными и регулярными структурами по сравнению с другими устройствами вычислительной системы (ВС).

С развитием вычислительной техники наблюдается устойчивая тенденция увеличения информационной емкости ЗУ. Повышение быстродействия процессоров и стремление к миниатюризации радиоэлектронной аппаратуры предъявляют трудно совместимые требования к ЗУ. Система памяти универсальной ВС должна иметь информационную емкость $10^9...10^{12}$ бит и больше при времени обращения менее 5 нс и потребляемой мощности около 1 мкВт/бит. Эти характеристики должны сочетаться с высокой надежностью, приемлемой стоимостью, малыми габаритами и массой. Вследствие этого ЗУ современных ВС имеет весьма сложную многоуровневую (иерархическую) структуру, позволяющую в определенной мере удовлетворить все необходимые требования при ограниченном наборе технических средств [1, 2].

Типичная иерархическая структура системы памяти современной ВС представлена на рис.1.

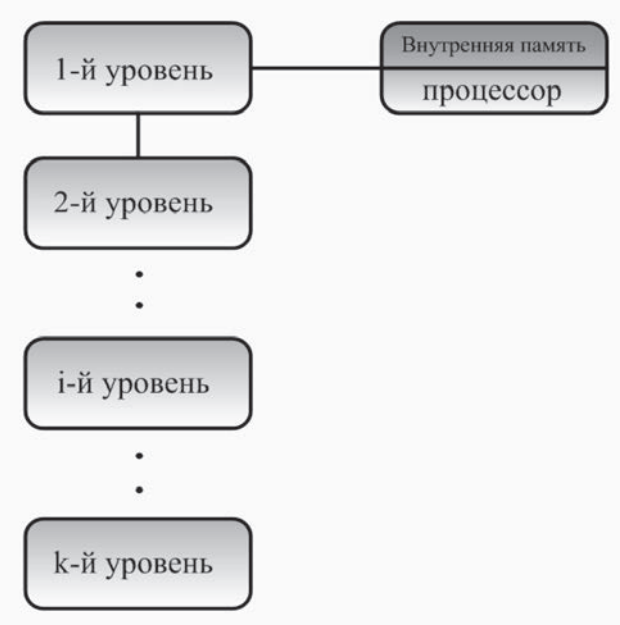


Рис.1. Иерархическая структура системы памяти современной ВС

Непосредственно связанные с процессором устройства памяти составляют верхние уровни иерархии. Они имеют максимальное быстродействие, но относительно малую информационную емкость. На остальных уровнях иерархии устройства памяти располагаются по мере увеличения информационной емкости и связанного с этим уменьшения быстродействия.

Таким образом, рассмотренная структура системы памяти позволяет использовать для решения задач математического моделирования ЗУ перспективных ВС многоуровневый подход и декомпозицию [3, 4].

Декомпозиция предполагает:

1. Разбиение сложной задачи (системы) на несколько простых задач (модулей).

2. Четкое определение функций каждого модуля, решающего отдельную задачу.

3. Определение правил взаимодействия между модулями.

При многоуровневом подходе:

1. Все множество модулей разбивается на уровни (при этом функции всех уровней четко определены).

2. Уровни образуют иерархию (т.е. существуют верхние и нижние).

3. Для решения своих задач каждый уровень обращается с запросами только к модулям непосредственно примыкающего нижнего (верхнего) уровня.

4. Результаты работы модулей уровня могут быть переданы только соседнему уровню.

Такой подход позволяет достичь упрощения решения задач анализа сложных систем.

С учетом вышеизложенного далее производится моделирование и расчет основных показателей надежности для одного уровня памяти с коррекцией ошибок.

В [5] память рассматривается как канал хранения данных, в котором информация распространяется не в пространстве, а во времени. Обобщенный канал хранения данных представлен на рис.2.

При этом кодеру известны подмножества $S'_0 \in S_0$ и $S'_1 \in S_1$ элементы которых соответствуют разрядам ячеек, отказавших соответственно в «0» и «1» до записи данных в память. Декодеру известны подмножества $S''_0 \in S_0$ и $S''_1 \in S_1$, элементы которых соответствуют разрядам ячеек, отказавших соответственно в «0» и «1» до записи данных, а также подмножества $R''_0 \in R_0$ и $R''_1 \in R_1$, элементы которых соответствуют разрядам ячеек, отказавших соответственно в «0» и «1» после записи данных в память.

Обобщенный канал (рис. 2), характеризуемый множествами $S'_0, S'_1, S''_0, S''_1, R''_0, R''_0, S''_0 \bigcup R''_0$, $S''_1 \bigcup R''_1$, множеством отказов переданных кодеру Zдк и словом e, моделирующим ошибки в канале достаточно хорошо описывает все возможные ситуации, которые могут реально возникнуть в памяти.

Однако данная модель не учитывает возможности применения современных схем уменьшения кратности корректируемой

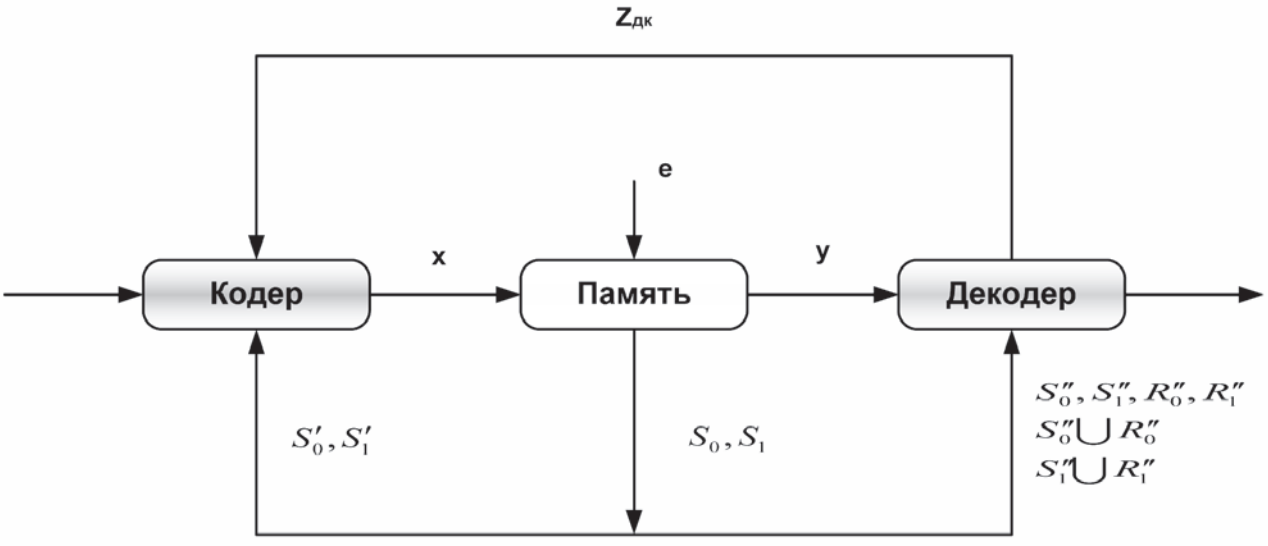


Рис.2. Обобщенный канал хранения данных

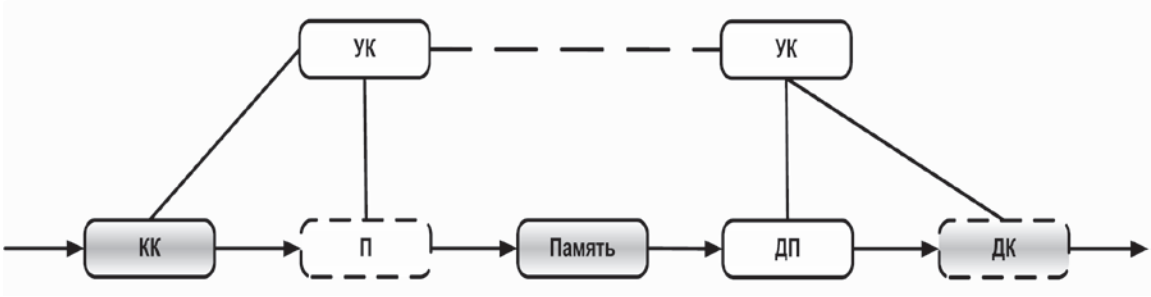


Рис. 3. Структурная схема канала памяти

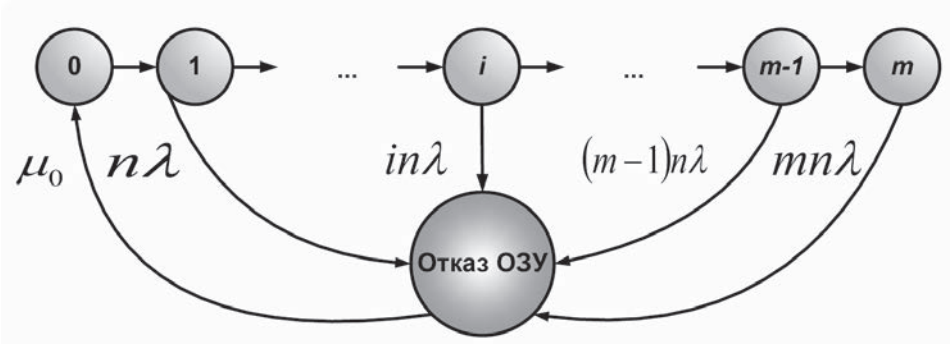


Рис. 4. Граф функционирования ОЗУ с реконфигурацией отказавших разрядов накопителя (r = 1)

ошибки, путем разнесения ошибок в слове по разным адресам (перемежения).

С учетом этого предлагаемая структурная схема канала памяти представлена на рис.3.

Перечислим блоки, входящие в структурную схему.

КК (ДК) – кодер (декодер) канала, обеспечивает корректирующее кодирование с целью защиты от ошибок.

П (ДП) – перемежитель (деперемежитель), обеспечивает перемежение с целью декорреляции ошибок.

УК – средства управления каналом памяти.

Покажем, что решение задачи определения параметров такого канала памяти непосредственно из обобщенного канала хранения данных является принципиально возможной.

Для оценки надежности такого ОЗУ предположим, что отказы микросхем (МС) памяти независимы и равновероятны, время до отказа распределено по экспоненциальному закону, а в начальный момент времени все МС памяти исправны. Надежность общего оборудования считаем идеальной.

Очевидно, что отказ такого ОЗУ наступит в случае появления в одной из линеек памяти (ЛП) более r отказавших разрядов, превышающих возможности схемы реконфигурации.

Граф функционирования такой системы при r=1 приведен на рис.4. Возможными состояниями устройства являются следующие:

0 – все оборудование ОЗУ работоспособно;

1 – отказала одна МС памяти в одной из *m* линеек, реконфигурация отказавшего разряда;

...

i – отказало по одной МС в *i* линейках, реконфигурация отказавших разрядов;

...

m – отказало по одной МС во всех линейках, реконфигурация отказавших разрядов резервными;

m+1 – отказали две МС в одной линейке (событие «Отказ ОЗУ»).

По графу состояний можно получить систему дифференциальных уравнений:

$$
\begin{cases}
\dfrac{dp_0(t)}{dt} = \mu_0 p_{m+1}(t) - mk\lambda p_0(t); \\
\dfrac{dp_1(t)}{dt} = mk\lambda p_0(t) - (mk-1)\lambda p_1(t); \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\dfrac{dp_i(t)}{dt} = k(m-i+1)\lambda p_{i-1}(t) - (mk-i)\lambda p_i(t); \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\dfrac{dp_m(t)}{dt} = k(m-m+1)\lambda p_{m-1}(t) - \\
-(mk-m)\lambda p_m(t); \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\dfrac{dp_{m+1}(t)}{dt} = -\mu_0 p_{m+1}(t) + (mk-m)\lambda p_m(t) + \\
+\sum\limits_{i=1}^{m-1} i(k-1)\lambda P_i(t); \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\sum\limits_{i=0}^{m+1} P_i(t) = 1.
\end{cases}
\qquad (1)
$$

Для нахождения стационарных вероятностей пребывания устройства в каждом состоянии из системы дифференциальных уравнений можно получить и решить систему алгебраических уравнений.

Поскольку для рассматриваемой системы состояниями работоспособности являются состояния 1,1,...,*m* коэффициент готовности для этой системы равен сумме вероятностей пребывания во всех этих состояниях

$$K_{\Gamma} = \sum_{i=0}^{m} p_i .$$

Из (1) следует, что

$$P_i = \frac{(m-i+1)k}{mk-i} P_{i-1} \qquad (2)$$

Учитывая (2), $P_i (i = 1,...m)$ можно выразить через P_0

$$P_i = P_0 \chi_i \qquad (3)$$

где

$$\chi_i = \prod_{j=1}^{i} \frac{i(m-j+1)k}{mk-j} \qquad (4)$$

Из первого уравнения системы (1) следует, что

$$P_{m+1} = \frac{mk\lambda}{\mu_0} P_0 . \qquad (5)$$

Учитывая условие нормировки и соотношения (2) – (5), можно найти, что

$$P_0 = \frac{1}{1 + \sum\limits_{i=1}^{m} \chi_i \dfrac{mk\lambda}{\mu_0}} . \qquad (6)$$

С учетом (3) коэффициент готовности находится по формуле

$$K_r = P_0 + \sum_{i=1}^{m} P_0 \chi_i ,$$

а после подстановки выражений (4) и (6)

$$K_r = \frac{1 + \sum\limits_{i=1}^{m} \chi_i}{1 + \sum\limits_{i=1}^{m} \chi_i + \dfrac{mk\lambda}{\mu_0}} . \qquad (7)$$

Средняя наработка $T_{\text{н}}$ до отказа ОЗУ равна математическому ожиданию времени пребывания устройства в множестве работоспособных состояний 0,1,...,*m* при условии, что в начальный момент времени оно находилось в нулевом состоянии, т.е. $P_0(0) = 1$.

Проведя ряд преобразований, получаем

$$T_{\text{н}} = \frac{1}{mk\lambda} + \frac{1}{\lambda} \sum_{i=1}^{m} \frac{k^i}{mk-i} \prod_{j=1}^{i} \frac{m-j+1}{mk-j+1} . \qquad (8)$$

Полученные соотношения позволяют оценить влияние параметров ОЗУ на показатели надежности.

Заключение

Таким образом, центральным моментом при рассмотренном подходе является выбор модели канала памяти. Представленная модель достаточно точно отражает статистику ошибок в канале, дает возможность быстрого определения ее параметров по статистике и не требует значительных вычислительных ресурсов для проведения дальнейших расчетов, что особенно важно в адаптивных системах.

СПИСОК ЛИТЕРАТУРЫ

1. Горшков В.Н. Расчет надежности оперативных запоминающих устройств / В.Н.Горшков, Ю.Л.Кругляк. – Учеб. пособие. – Пушкин: ВИ(СиСОВ) ВКА имени А.Ф. Можайского, 2007. – 52 с.

2. Соломенчук В.Г. Железо ПК / В.Г.Соломенчук, П.В.Соломенчук – СПб.: БХВ – Петербург, 2011. – 448 с.

3. Мелентьев О.Г. Теоретические аспекты передачи данных по каналам с группирующимися ошибками / Под редакцией профессора В.П. Шувалова. – М.: Горячая линия - Телеком, 2007. – 232 с.

4. Альянах И.Н. Моделирование вычислительных систем. – Л.: Машиностроение, 1988. – 223 с.

5. Горшков В.Н. Методология повышения надежности оперативной памяти ЭВМ // Петербургский журнал электроники. – № 1. – 1996.

С.В. Куликов
капитан, преподаватель,

А.В. Зеленков
подполковник, старший преподаватель,

Д.А.Скворцов
старший лейтенант, оперативный дежурный Военно-космическая академия им. А.Ф. Можайского.

АДАПТИВНЫЕ СОГЛАСУЮЩИЕ УСТРОЙСТВА С РЕГУЛИРУЕМЫМИ ПАРАМЕТРАМИ

ФАР состоят из большого количества излучателей, размещенных на сравнительно большом расстоянии друг от друга, что приводит к взаимному влиянию между ними. Взаимодействие между излучателями в решётке проявляется следующим образом:

– входное сопротивление излучающего элемента ФАР отличается от его сопротивления в свободном пространстве и является функцией угла сканирования;

– увеличиваются потери сигнала при сканировании лучом ДНА в пространстве;

– изменяется форма диаграммы направленности излучателя;

– снижается коэффициент усиления антенной решетки.

Поэтому задача разработки адаптивных согласующих устройств СВЧ для РЛС РТВ с ФАР, позволяющих уменьшить влияние факторов, обусловленных изменением входного сопротивления излучающего элемента в ФАР при сканировании и взаимным влиянием излучателей друг на друга в решетке, является актуальной.

Под адаптивным согласующим устройством СВЧ (АдСУ СВЧ) в диссертации понимается устройство, выполненное на отрезках линий передачи, способное подстраивать свою структуру и параметры при изменении комплексного сопротивления нагрузки с целью снижения потерь высокочастотного сигнала.

Известно много реализаций устройств, с помощью которых обеспечивается согласование входного сопротивление антенн. Согласующие устройства на шлейфах (ферритовые вентили, циркуляторы и др.).

Адаптивные согласующие устройства не применялись, поскольку до настоящего времени не было необходимости обеспечивать согласование изменяющейся комплексной нагрузки.

Наиболее близким аналогом предлагаемой полезной модели является согласующее устройство на шлейфах, состоящих из отрезков линий, которые обеспечивают согласование для фиксирующего значения комплексного сопротивления нагрузки [3]. Недостаток данного устройства состоит в том, что оно обеспечивает наименьшее значение коэффициента отражения только для одного значения комплексного сопротивления нагрузки.

Цель работы – повысить качество согласования входного комплексного сопротивления антенны с линией передачи при изменении положения луча диаграммы направленности в пространстве. Для достижения цели согласующее устройство СВЧ в полосковом или микрополосковом исполнении разбивается на отдельные отрезки линии передачи с различными параметрами (электрическая длина отрезка и его волновое сопротивление), которые

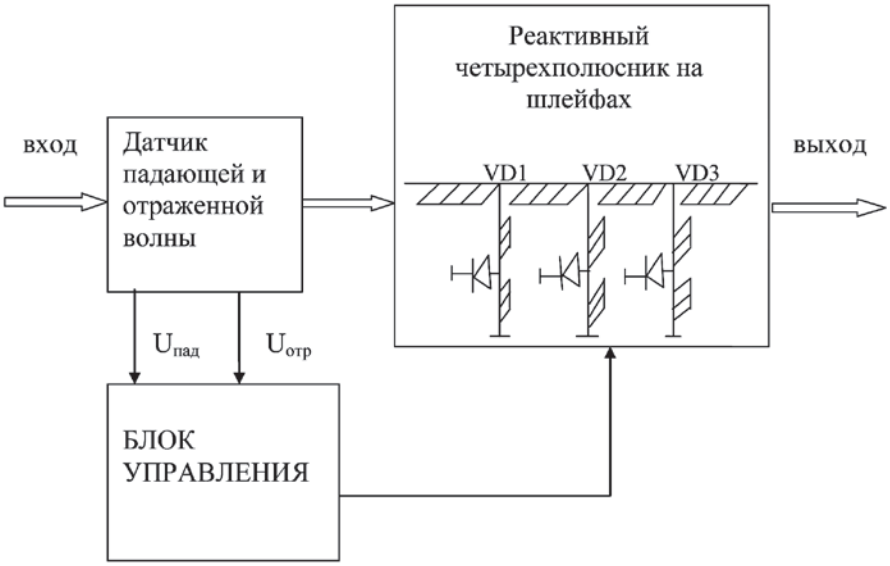


Рис. 1. Адаптивное согласующее устройство

коммутируются при помощи полупроводниковых регулируемых элементов (pin-диодов). Управление элементами коммутации адаптивного согласующего устройства осуществляется на основе анализа падающей и отражённой волны поступающей от соответствующего датчика в блок управления (рис.1). Блок управления реализован на основе микроконтроллера с управляющей программой, рассчитывающий изменение коэффициента стоячей волны [4] и формирующий на основе его значения управляющее напряжение, которое подаётся на коммутирующие элементы согласующего устройства, и обеспечивают подстройку его структуры и параметров под изменение входного сопротивления антенны. Учёт изменения входного сопротивления антенны при изменении луча диаграммы направленности в пространстве осуществляется на основе формулы для расчёта взаимного влияния соседних антенн в антенной решётке [5].

Коэффициент стоячей волны рассчитывается в соответствии с формулой:

$$Ксв = \frac{U_{под} - U_{отр}}{U_{под} + U_{отр}};$$

где $U_{пад}$ – напряжение падающей волны; $U_{отр}$ – напряжение отраженной волны

Разбиение реактивных шлейфов на отрезки линий осуществляется с помощью симметричного деления на равные части. Коммутирующие элементы, установлены между отрезками линий каждого реактивного шлейфа в реактивном четырехполюснике, которые обеспечивают подстройку структуры и параметров согласующего устройства под изменение комплексного сопротивления нагрузки.

Техническим результатом является увеличение функциональных возможностей согласующего устройства СВЧ за счет использования в устройстве коммутирующих элементов и устройства управления ими. Это позволит использовать его в многоканальных антенных системах, где используют электронное управление положения луча в пространстве, для согласования изменяющегося входного сопротивления антенн.

СПИСОК ЛИТЕРАТУРЫ

1. Матей Д.Л., Янг Л., Джонс Е.М.Т., Фильтры СВЧ, согласующие цепи и цепи связи.- М.: Связь, 1971., 1т.-439с.

2. Матей Д.Л., Янг Л., Джонс Е.М.Т., Фильтры СВЧ, согласующие цепи и цепи связи. -М.: Связь, 1972., 2т.- 494с.

3. Устройства СВЧ и антенны Д.И. Воскресенский 2008 г.

4. Антенны и устройства СВЧ проектирование фазированных антенных решеток, под редакцией Д.И. Воскресенского 1994 г.

5. Антенны с электрическим сканированием О.Г. Вендик, М.Д. Парнес под редакцией Л.Д. Бахраха 2001 г.

Г.В. Куликов
заместитель директора Центра ОАО «НПО РусБИТех», к.т.н, доцент

ПРОБЛЕМНЫЕ ВОПРОСЫ СОЗДАНИЯ ДОВЕРЕННЫХ ПРОГРАММНО-АППАРАТНЫХ ПЛАТФОРМ ДЛЯ ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Одной из проблем обеспечения безопасности информации в автоматизированных системах в защищенном исполнении является то, что современные ОС содержат от 3 до 10 млн. строк исходного кода, среди которых можно разместить команды, реализующие недокументированные возможности, с помощью которых можно нарушить безопасность информации, обрабатываемой автоматизированными системами органов государственного и военного управления.

В ОС с открытым исходным кодом гораздо проще выявлять и предотвращать наличие подобных недокументированных команд. Указанное обстоятельство обуславливает принятие во многих государствах, обладающих различным экономическим потенциалом и имеющих разный уровень развития информационных технологий (Китай, Корея, Индия, Венесуэла, Бразилия, Нидерланды, Германия, Испания, Франция, Италия и т.д.) планов перехода государственных структур на использование открытых операционных систем на базе Linux. В ряде стран в органах государственного управления уже применяются крупные коммерческие дистрибутивы ОС Novell SUSE, RedHat, Ubuntu, Mandriva.

Минкомсвязи России также разрабатывает программу перехода органов государственной власти на использование свободного программного обеспечения на платформе Linux.

Переход на использование защищенного программного обеспечения на базе свободного программного обеспечения позволяет:

1) Исключить технологическую зависимость критичных сегментов информационно-телекоммуникационной системы России от иностранных производителей;

2) Экономить расходы бюджета на покупки иностранного ПО, стоимость которого на порядок выше отечественных разработок на базе платформы Linux;

3) Предоставят контролирующим органам возможность иметь полную и достоверную информацию о содержимом исходного кода;

4) Развивать отечественную отрасль информационных технологий и разработку аппаратных средств.

5) Не содержать большой штат разработчиков для всех компонентов ОС, поскольку их разработкой уже занимаются многочисленные открытые сообщества разработчиков.

Другой важной проблемой является то, что для построения автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую государственную тайну и персональные данные необходимо наличие защищенной ОС.

Существуют два общепринятых отечественными разработчиками подхода к созданию защищенных ОС – фрагментарный и комплексный.

При фрагментарном подходе за основу защищенной ОС берется незащищенная ОС иностранного производителя, как правило ОС семейства Windows, которая затем дополняется различными программно-аппаратными средствами защиты информации, которые позволяют обеспечить формальное выполнение требований руководящих документов России по защите информации.

Основной недостаток данного подхода очевиден – система защиты информации защищенной ОС, построенной с использованием фрагментар-

ного подхода практически не интегрирована с базовыми подсистемами ОС, обеспечивающими работу оборудования и ответственными за взаимодействие с пользователем.

При комплексном подходе функции и механизмы системы защиты, вносятся в ОС на этапе проектирования архитектуры системы защиты ОС и являются ее неотъемлемой частью. Все механизмы защиты ОС, созданной на основе комплексного подхода тесно взаимодействуют друг с другом и с базовыми подсистемами ОС и обеспечивают непрерывную защиту информации.

Все встраиваемые в ОС семейства Windows средства защиты информации отечественных производителей, позволяющие формально выполнять требования руководящих документов России по защите информации, включая информацию содержащую государственную тайну, обеспечивают защиту только на основе фрагментарного подхода, что учитывая недостатки указанного подхода является недопустимым. Это связано с тем, что для создания на базе ОС семейства Windows защищенной ОС с использованием комплексного подхода необходимо наличие у разработчиков отечественных средств защиты исходных текстов указанных ОС, что не представляется возможным в соответствии с политикой фирмы Microsoft, являющейся разработчиком указанных ОС.

Кроме того, в соответствии с требованиями руководящих документов по обеспечению безопасности информации ФСБ России, Минобороны России и ФСТЭК России все компоненты системы защиты информации в защищенной ОС должны пройти исследования по контролю отсутствия недекларированных возможностей, что в отношении ОС семейства Windows не представляется возможным.

Для решения указанных проблем ОАО «НПО РусБИТех» разработало в инициативном порядке основные составляющие доверенной программно-аппаратной платформы для построения автоматизированных систем в защищенном исполнении, предназначенных для обработки информации, содержащей государственную тайну:

– защищенную операционную систему;

– защищенную реляционную СУБД;

– защищенные сервер и клиент электронной почты;

– защищенный сервер гипертекстовой обработки информации и web-браузер;

– аппаратно-программный модуль доверенной загрузки.

Программные компоненты платформы основаны на свободном программном обеспечении, в которые встроены механизмы защиты информации, удовлетворяющие требованиям руководящих документов Российской Федерации по безопасности информации.

Проведена сертификация программных компонентов платформы:

по 3 классу защищенности СВТ и 2 уровню отсутствия недекларированных возможностей в системе сертификации Минобороны России и ФСТЭК России;

на соответствие требованиям ФСБ России.

Основными преимуществами доверенной программно-аппаратной платформы являются:

– использование в качестве основы свободного программног обеспечения;

– наличие исходных текстов всех составных частей;

– интеграция механизмов защиты информации в ядро операционной системы;

– использование встроенных в ядро операционной системы механизмов защиты информации всеми компонентами общего программного обеспечения из состава доверенной программной платформы.

С.В. Куликов
майор, преподаватель

А.В. Зеленков
подполковник, старший преподаватель

Д.А.Скворцов
старший лейтенант, оперативный дежурный Военно-космическая академия им. А.Ф. Можайского.
г. Санкт-Петербург

СИНТЕЗ АДАПТИВНЫХ СОГЛАСУЮЩИХ УСТРОЙСТВ СВЧ

Синтез адаптивных согласующих устройств СВЧ для РЛС с АФАР новая. Она построена на основе классического подхода к синтезу устройств СВЧ, основанного на методе Кона, суть которого заключается в переходе от низкочастотного прототипа к схеме с распределёнными параметрами. Методика разработана для комплексных нагрузок и позволяет осуществить выбор структуры и параметров согласующих устройств, обеспечивающих минимальный коэффициент стоячей волны по напряжению при изменении входного комплексного сопротивления излучателя при заданных ограничениях на массогабаритные характеристики согласующих устройств. В отличие от известных методик, в ней используется возможность управления параметрами реактивного четырехполюсника при изменении входного комплексного сопротивления излучателя при сканировании, возникающее из-за их взаимного влияния.

1. Задаются исходные данные для расчёта СУ, среди которых частоты, определяющие центральную и граничные частоты полосы пропускания (ПП) и уровни пульсаций в ПП.

Исходными данными являются: линейная центральная резонансная частота f_0 (или длина волны); *w*– относительная ширина основной полосы пропускания, где $w = \Delta\omega/\omega_0$, $\Delta\omega$ – абсолютная протяженность полосы пропускания на резонансной частоте, $\omega_0=2\pi f_0$ – круговая центральная частота полосы пропускания, P_C – мощность сигнала на входе согласующего устройства, $Z_И$ –сопротивление источника питания, Δf – диапазон перестройки рабочих частот, $\Delta\varepsilon = \varepsilon_2 - \varepsilon_1$ – диапазон перемещения луча диаграммы направленности антенны по углу места, $R_Н=R_Г=1$ – нормированные сопротивления нагрузки и генератора; уровень пульсаций в полосе пропускания L_r.

2. Выбирается вид аппроксимации требуемой характеристики затухания и расчёт требуемого

Рис. 1. Общая схема методики синтеза АдСУ

числа элементов лестничной схемы фильтра прототипа. *Выбор структуры СУ* заключается в определении общего количества резонаторов N.

3. На основе метода низкочастотного прототипа, определяются g – параметры, по которым рассчитываем параметры отрезков линии СУ, определяем волновое сопротивление каждого отрезка и его электрическую длину. В зависимости от выбранного вида аппроксимации определяются значения g-параметров [6].

4. По соотношениям (1-2) определяются значения коэффициентов инверторов проводимости. От уровня пульсаций L_r зависят значения g-параметров элементов НЧ прототипа (g_0... g_{n+1}), параметры инверторов зависят от относительной полосы пропускания *w*.

$$S = \sqrt[n-2]{\frac{R_A}{R_B}};\ C_2 = g_2;\ C_k\left|\begin{array}{l} k = 3 \div n-1 \\ \text{если},\ n = 3 \end{array}\right.$$

$$\text{при}\ \ n > 3 = 2dg_2 s^{k-2};\ \ C_n\Big|_{n\geq 3} = g_0 g_n g_{n-1}\frac{R_A}{R_B};$$

$$C_n\Big|_{n\geq 3} = g_0 g_n g_{n-1}\frac{R_A}{R_B};\ \ C_2' = g_2(1-d),\ C_2'' = dg_2,$$

$$C_k'\Big|_{k=3\div n} = C_{k-1}'',\ C_k'' = C_k - C_k' \qquad (1)$$

$$G_A = \frac{1}{R_A};\ J_{23} = \frac{1}{g_0}\sqrt{\frac{C_2 C_3}{g_2 g_3}};$$

$$N_{23} = \sqrt{\left(\frac{J_{23}}{G_A}\right)^2 + \left(\frac{C_3'' tg\theta_1}{g_0}\right)^2};$$

$$\theta_1 = \frac{\pi}{2}\left(1 - \frac{w}{2}\right);\ \ w = (f_2 - f_1)/f_0;$$

Параметры инверторов, нормированные относительно волновой проводимости нагрузки, равны

$$\frac{J_{12}}{Y_a} = g_0\sqrt{\frac{C_a}{g_2}},\ \frac{J_{k,k+1}}{Y_a}\Big|_{k=2,\ldots n-2} = \frac{g_0 C_a}{\sqrt{g_k \cdot g_{k+1}}},$$

$$\frac{J_{n-1,n}}{Y_a} = g_0\sqrt{\frac{C_a g_{n+1}}{g_0 \cdot g_{n-1}}}. \qquad (2)$$

где $C_a = 2dg_1$, d = 1, g_o , g_1,... g_{n+1} значения элементов фильтра-прототипа нижних частот.

Волновые проводимости параллельных шлейфов определяются формулами [6];

$$Y_{11} = g_0 Y_a \omega_1'(1-d)g_1 tg\theta_1 + Y_a(N_{12} - J_{12}/Y_a);$$

$$Y_n\Big|_{k=2,\ldots n-1} = Y_a(N_{k-1,k} + N_{k,k+1} - \qquad (3)$$

$$-J_{k=1.k}/Y_a - J_{k,k+1}/Y_a)$$

$$Y_n = Y_a\omega_1'(g_n g_{n+1} - dg_0 g_1)tg\theta_1 + Y_a(N_{n-1,n} - J_{n-1,n}/Y_a);$$

$$\theta_1 = \frac{\pi\omega_1}{2\omega_0} = \frac{\pi}{2}(1 - \frac{w}{2}); \qquad (4)$$

$$N_{k,k+1}\Big|_{k=1,\ldots n-1} = \sqrt{\frac{(J_{k,k+1})^2}{Y_a{}^2} + \frac{(g_0\omega_1' C_a tg\theta_1)^2}{4}}, \qquad (5)$$

где ω_1' – частота среза фильтра нижних частот; w= (ω_2 – ω_1)/ ω_o – относительная ширина полосы пропускания; ω_2, ω_1 – верхняя и нижняя граничные частоты полосы пропускания на уровне пульсаций характеристики затухания; ω_o – центральная частота. Волновые проводимости соединительных линий (инверторов) равны

$$Y_{k,k+1}\Big|_{k=1,\ldots n-1} = Y_a(J_{k,k+1}/Y_a). \qquad (6)$$

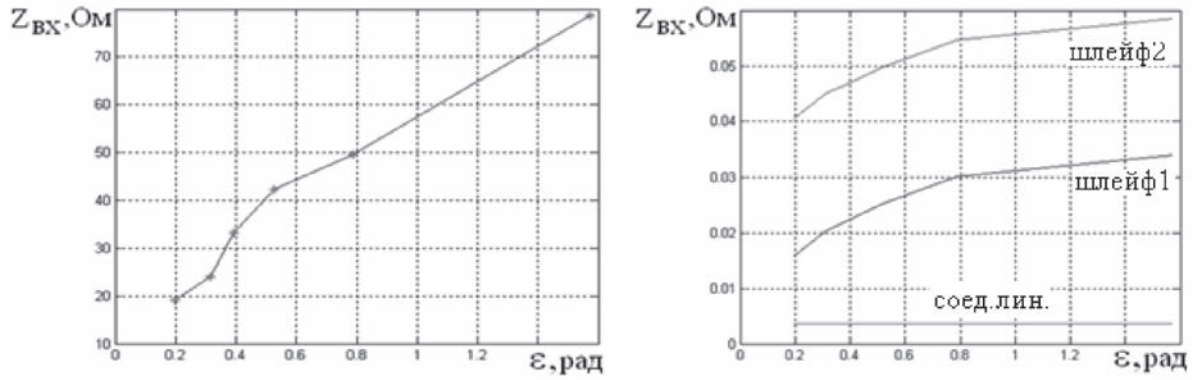


Рис. 2. Изменение параметров шлейфов при различном положении луча в пространстве а) изменение входного сопротивления б) изменение параметров шлейфа

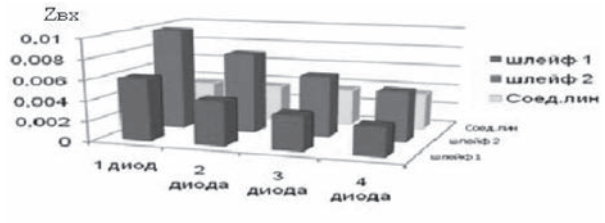


Рис. 3 Зависимость изменения входного сопротивления шлейфа от количества элементов коммутации

5. По рассчитанным значениям коэффициентов инверторов осуществляется расчёт значений длин участков соединительных линий, выступающих в качестве элементов связи.

На рисунке (2а,б) приведены результаты моделирования параметров отрезков линий согласующего устройства при изменении положения луча в пространстве.

Из рисунка 3 видно, что при увеличении числа диодов точность подстройки увеличивается, за счет изменения входного сопротивления и уменьшения его к требуемому значению, что в свою очередь приводит к снижению коэффициенту стоячей волны и к улучшению качества согласования.

Таким образом, подключение коммутирующих элементов в отрезок линии позволяет обеспечить, достаточный уровень коэффициента стоячей волны.

6. Приступаем к этапу моделирования и получения характеристик синтезированного АдСУ.

Определение входного сопротивления СУ осуществляется путем пересчёта сопротивления нагрузки Z через соответствующий отрезок передающей линии по известной формуле

$$Z_{BX.} = W\frac{Z+jWtg\theta}{W+jZtg\theta},$$

где W – волновое сопротивление линии, θ – электрическая длина отрезка передающей линии.

Из рисунка 4 видно, что при отклонении луча диаграммы направленности от нормали, входное сопротивление СУ изменяется, что приводит к изменению выходных характеристик СУ и приводит к потерям мощности сигнала.

Построение выходных характеристик СУ заключается в вычислении зависимостей коэффициента отражения Г, коэффициента стоячей

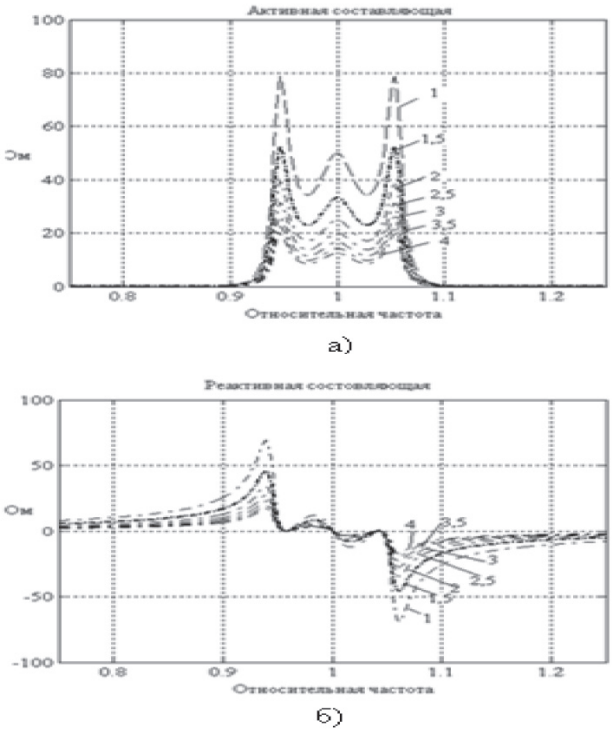


Рис. 4. Определение активной а) и реактивной б) составляющей при отклонении положения луча от нормали

волны КСВН, затухания в полосе пропускания и фазовой характеристики Ф от частоты. Расчёт этих характеристик проводится по известным формулам.

$$\Gamma = \left|\frac{R_\Gamma - Z_{BX}}{R_\Gamma + Z_{BX}}\right|,\ KCBH = (1+\Gamma)/(1-\Gamma),$$

$$L = 10\lg[1/(1-|\Gamma|^2)],\ \Phi = (Jm\Gamma)/(\mathrm{Re}\,\Gamma).$$

7. Результаты моделирования показали, что при увеличении нагрузки растет влияние входных сопротивлений СУ и следствие ведет к ухудшению характеристик АР.

Применение АдСУ позволило улучшить характеристики АР за счет применения коммутирующих элементов.

8. Проверка условия удовлетворяет ли СУ предъявляемым требованиям, при положительном решении можно переходить к этапу практической реализации и проведении эксперимента (п.10). При отрицательном исходе нужно вернуться к 4 и 5 этапам и провести анализ характеристик с откорректированными размерами (п.9). Особенности этапа реализации будут рассмотрены в разделе 3.

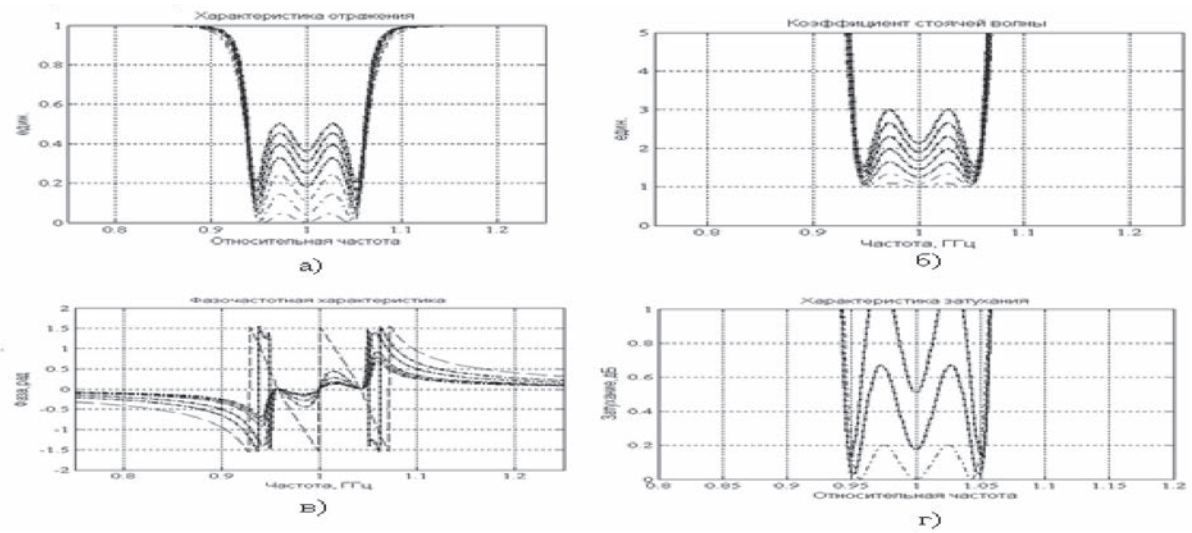


Рис. 5. Зависимости коэффициента отражения Г а), коэффициента стоячей волны КСВН б), затухания в полосе пропускания в) и фазовой характеристики Ф от частоты г)

Новизна данной методики, заключается в увеличении функциональных возможностей согласующего устройства СВЧ за счет использования в устройстве коммутирующих элементов и устройства управления ими. Это позволит использовать его в многоканальных антенных системах, где используют электронное управление положением луча в пространстве, для согласования изменяющегося входного сопротивления антенн.

СПИСОК ЛИТЕРАТУРЫ

1. Бердышев В.П., Синицын А.В. Развитие методов синтеза и построения фильтрующих устройств СВЧ на неоднородных линиях. Часть 1. - Тверь: ВУ ПВО, 2001, - 184 с.

2. Бердышев В.П., Синицын А.В. Развитие методов синтеза и построения фильтрующих устройств СВЧ на неоднородных линиях. Часть 2. - Тверь: ВУ ПВО, 2002, - 218 с.

3. Фильтры и цепи СВЧ. Пер. с англ. Л.В.Алексеева, А.Е.Знаменского, В.С.Полякова.- М.: Связь, 1976.-248 с.

4. Вай Кайчень. Теория и проектирование широкополосных согласующих цепей.- М.: Связь, 1979.-287 с.

5. Мазепова О.И., Мещанов В.П., Прохорова Н.И., Фельдштейн А.Л., Явич Л.Р. Справочник по элементам полосковой техники / под редакцией Фельдштейна. – М.: Связь, 1979г.-336 с.

6. Д.И.Воскресенский, и др., Антенны и устройства СВЧ (проектирование фазированных антенных решеток).- М.: Радио и связь, 1981. - 431 с.

7. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. - СПб.: Лань, 2003, - 832 с.

В.Н. Лазарев

ПРОБЛЕМЫ ОБРАБОТКИ ФОТОИЗОБРАЖЕНИЙ МЕТОДОМ ЛИНЕЙНОЙ ФИЛЬТРАЦИИ

Для решения задач слежения за аэродинамическими и космическими объектами и их распознаванием целесообразно привлекать как РЛК, так и оптико-электронные средства. Последние позволяют получить более точную информацию о форме, размерах и параметрах исследуемых объектов. Изображения объектов могут быть получены средствами космической разведки путём применения на околоземных орбитах разведывательных космических аппаратов, которые обеспечивают получение специальной фото и видео информации и передачи её на Землю. Однако качество полученных фото изображений порой оставляет желать лучшего. Для повышения качества и контрастности полученных снимков порой целесообразно применять методы линейной фильтрации.

Обычно изображения, сформированные информационными системами, искажаются действием помех. Это затрудняет как их визуальный анализ человеком-оператором, так и автоматическую обработку в ЭВМ.

Фундаментальной проблемой в области обработки изображений является эффективное удаление шума при сохранении важных для последующего семантического описания/ распознавания деталей изображения. Основные источники шума на цифровом изображении – это сам процесс его получения (оцифровки), а также процесс передачи. Например, в процессе получения изображения с помощью фотокамеры с ПЗС-матрицей, основными факторами, влияющими на величину шума, являются уровень освещённости и температура сенсоров.

В процессе передачи изображения могут искажаться помехами, возникающими в каналах связи. Например, при передаче изображения с использование беспроводной связи, оно может быть искажено в результате разряда молнии или других возмущений в атмосфере. **Сложность решения данной задачи существенно зависит от рассматриваемой модели шума.**

При восстановлении делается попытка реконструировать или воссоздать изображение, которое было до этого искажено, используя априорную информацию о явлении, которое вызвало ухудшение изображения. Поэтому методы восстановления основаны на моделировании процессов искажения и применении обратных процедур для воссоздания исходного изображения.

Этот подход обычно включает разработку критериев качества, которые дают возможность объективно оценить полученный результат. Напротив, методы улучшения изображений в основном представляют собой эвристические процедуры, предназначенные для такого воздействия на изображение, которое позволит затем использовать преимущества, связанные с психофизическими особенностями зрительной системы человека. Например, процедура усиления контраста рассматривается как метод улучшения, поскольку в результате её применения изображение, в первую очередь, становится более приятным для глаза, тогда как процедура обработки смазанного изображения, основанная на применении обратного оператора, рассматривается как метод восстановления.

Задача восстановления рассматривается лишь с момента получения уже искажённого

цифрового изображения; поэтому вопросы, касающиеся природы искажений, вносимых чувствительными элементами, цифровыми преобразователями и воспроизводящими устройствами, затрагиваются лишь поверхностно [1].

Как показано на рисунке 1, принятая модель процесса искажения предполагает действие некоторого искажающего оператора H на исходное изображение $f(x,y)$, что после добавления аддитивного шума даёт искажённое изображение $g(x,y)$.

Задача восстановления состоит в построении некоторого приближения $\hat{f}(x,y)$, исходного изображения по заданному (искажённому) изображению $g(x,y)$, некоторой информации относительно искажающего оператора H, и некоторой информации относительно аддитивного шума $\eta(x,y)$. Желательно чтобы наше приближение было как можно ближе к исходному изображению, и, в принципе, чем больше мы знаем об операторе H и о функции η, тем ближе будет функция $\hat{f}(x,y)$ к функции $f(x,y)$.В основе подхода, применяемого в курсовом проекте, лежит использование операторов (фильтров), восстанавливающих изображение.

Искажённое изображение может быть представлено в пространственной области в виде:

$$g(x,y)=h(x,y)*f(x,y)+\eta(x,y), \qquad (1)$$

где: $h(x,y)$ – функция, представляющая искажающий оператор в пространственной области, а символ «*» используется для обозначения свертки.

Если иметь дело только с искажениями, вызванными наличием шума, то выражение (1) можно записать в виде:

$$g(x,y)=f(x,y)+\eta(x,y). \qquad (2)$$

Наиболее удобной моделью искажения изображений для исследования методов их восстановления является добавление аддитивного белого гауссова, а также импульсного шума к исходному изображению. Такая модель наиболее близка к реальному действию шумов, когда сигнал изображения подвергается воздействию множества различных случайных факторов [2].

Аддитивный гауссов шум характеризуется добавлением к каждому пикселю изображения значений из соответствующего нормального распределения с нулевым средним значением. Такой шум обычно вводится на этапе формирования цифровых изображений. Импульсный шум характеризуется заменой части пикселей на изображении значениями фиксированной или случайной величины. Такая модель шума связана, например, с ошибками при передаче изображений.

Простейшим методом ослабления аддитивного гауссова белого шума на изображениях является его фильтрация посредством линейного фильтра. В результате такой фильтрации ослабляется энергия шума. Также с помощью метода линейной фильтрации достигается расфокусировка изображения.

Расфокусировка может применяться как предварительный шаг обработки изображения, например, для удаления мелких деталей перед обнаружением больших объектов (задача распознавания космических объектов для войск ВКО).

Множество подходов к улучшению изображений распадается на две большие категории: методы обработки в пространственной области (пространственные методы) и методы обработки в частотной области (частотные методы). Термин пространственная область относится к

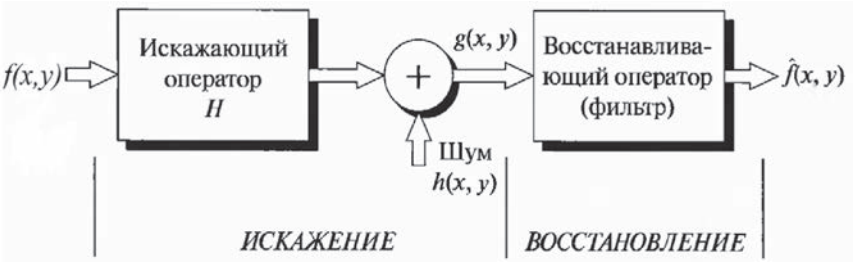


Рис. 1. Модель процесса искажения/восстановления фотоизображения

плоскости изображения как таковой, и данная категория объединяет подходы, основанные на прямом манипулировании пикселями изображения. Методы обработки в частотной области основываются на модификации сигнала, формируемого путём применения к изображению преобразования Фурье.

Поскольку пространственный метод обработки фильтруемого изображения требует меньших вычислительных затрат он будет наиболее предпочтительнее. Процессы пространственной обработки описываются уравнением:

$$g(x,y) = T\left[f(x,y)\right], \qquad (3)$$

где: $f(x,y)$ – входное изображение; $g(x,y)$ – обработанное изображение; T – оператор над f, определённый в некоторой окрестности точки (x,y).

Главный подход в определении окрестности вокруг точки (x,y) заключается в использовании квадратной или прямоугольной области – подмножества изображения, центрированного в точке (x,y).

Центр данного подмножества передвигается от пикселя к пикселю, начиная, скажем, с верхнего левого угла. Оператор T выполняется в каждой точке (x,y), давая в результате выходное значение g для данной точки.

Чаще всего маска представляет собой небольшой (как правило 3*3 элемента) двумерный массив, значения коэффициентов маски внутри которого определяют существо процесса.

Процесс пространственной фильтрации основан на простом перемещении маски фильтра от точки к точке изображения, в каждой точке (x,y) отклик фильтра вычисляется с использованием предварительно заданных связей. В случае линейной пространственной фильтрации отклик задаётся суммой произведений коэффициентов фильтра на соответствующие значения пикселей в области, покрытой маской фильтра [3].

Важным вопросом при реализации операций пространственной фильтрации по окрестности является рассмотрение ситуации, когда центр фильтра приближается к границам изображения. Если же центр маски приближается к границе, то одна или несколько строк или столбцов маски будут находиться вне изображения. Существует несколько способов учесть это обстоятельство.

Как уже ранее было отмечено в данной работе рассматривается улучшение фотоизображений с аддитивным белым гауссовым и импульсным шумом, которое может быть осуществлено как программными, так и аппаратными методами.

СПИСОК ЛИТЕРАТУРЫ

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений / Перевод с английского под редакцией Чочиа П.А. – Москва: Техносфера, 2005г. – 1072 с.

2. Хуанг Т. Обработка изображений и цифровая фильтрация / Перевод с английского к.т.н. Сорокин Е.З. и к.т.н. В.А. Хлебородова. – Москва: «Мир», 1979г. – 320 с.

3. Яне Б. Цифровая обработка изображений. – Москва: Техносфера, 2007г. – 584 с.

В.А. Бабошин
Начальник отдела ОАО «НИИ «Рубин», кандидат технических наук, доцент
К.Е.Легков
Заместитель начальника кафедры технологий и средств технического обеспечения и эксплуатации АСУ (войсками) Военно-космической академии имени А.Ф. Можайского, кандидат технических наук

К ВОПРОСУ О СОЗДАНИИ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Инфокоммуникационная система специального назначения (ИКС СН) представляет собой совокупность автоматизированных цифровых сетей связи общего пользования и телекоммуникационных сетей следующего поколения (NGN) с системами обмена и хранения данных, построенных на основе конвергентных инфокоммуникационных технологий, объединенных единой системой управления и обеспечивающих предоставление пользователям услуг обмена, доступа, размещения и поиска информации различных типов в единой среде межвидового (межведомственного) вертикального и горизонтального электронного взаимодействия вне зависимости от места нахождения абонентов и информации [1].

Одной из основных задач создания ИКС СН является резкое улучшение способности к взаимодействию, т.е. способности систем, органов управления (ОУ) или сил представлять данные, информацию, услуги и принимать их из других систем, ОУ или сил, а также использовать эти данные, информацию и услуги для эффективного совместного решения поставленных задач.

Анализ текущего состояния и ведущихся разработок показывает, что в ходе создания ИКС СН необходимо учитывать современные подходы к построению подобных систем на основе:

унифицированных способов построения аппаратно-программных комплексов, обеспечения их взаимодействия и организации на их основе служб управления;

набора базовых аппаратно-программных средств, различные сочетания которых позволяют создавать масштабируемые вычислительные сети, службы связи и управления;

адаптации служб управления к решаемым задачам и условиям их решения при сохранении инвариантного характера реализации специального программного обеспечения на основе методов метауправления функциональностью.

В целом для современных ИКС СН характерны:

интеграция информационных и телекоммуникационных сервисов;

ориентация на потребителя;

конвергенция технологий, сегментов, систем;

уменьшение грани между информационными и телекоммуникационными сетями, их системами управления;

развитие автоматизированных систем управления связью (АСУС) в системы класса Operating Support System (OSS) и Business Support System (BSS);

рост приоритета интеграционных процессов, обеспечения полной наблюдаемости и управляемости;

стремление к унификации используемых технологий и средств, выделению и развитию инварианта.

Под инвариантом понимаются унифицированные компоненты – множество изделий, пригодных к совместному применению в комплексах средств связи и автоматизации

информационно-телекоммуникационных ведомственных и межведомственных систем различного назначения.

Накопленный опыт работ по созданию программных и программно-аппаратных комплексов и систем в интересах создания телекоммуникационных платформ различного назначения и АСУС позволяет в первом приближении выделить следующие основные составляющие инварианта любой инфокоммуникационной системы:

средства вычислительных сетей и систем;

базовые средства и сервисы безопасности;

базовые инфотелекоммуникационные и типовые прикладные сервисы [2].

Целесообразность выделения и использования инвариантных составляющих, единых для прикладных информационных систем (ИС) и их телекоммуникационной платформы (ТКП), очевидна – это минимизация сроков и затрат на создание систем. Собственно инвариантные изделия образуют унифицированную платформу создания ИКС СН и предполагают наращивание этой платформы в рамках единой интеграционной дисциплины, основу которой составляют информационная безопасность (ИБ) и управление.

В общем случае интеграционные процессы можно рассматривать с точки зрения технологии порталов обеспечивающих (рис. 1):

поддержку сеансовой связи, интеграция «традиционной» и новых составляющих ТКП – через телекоммуникационные порталы;

интеграцию прикладных ИС – через порталы информационного доступа (ПИД);

интеграция информационных и телекоммуникационных услуг для конечного пользователя – через сервисные порталы (порталы сервисного доступа) [2].

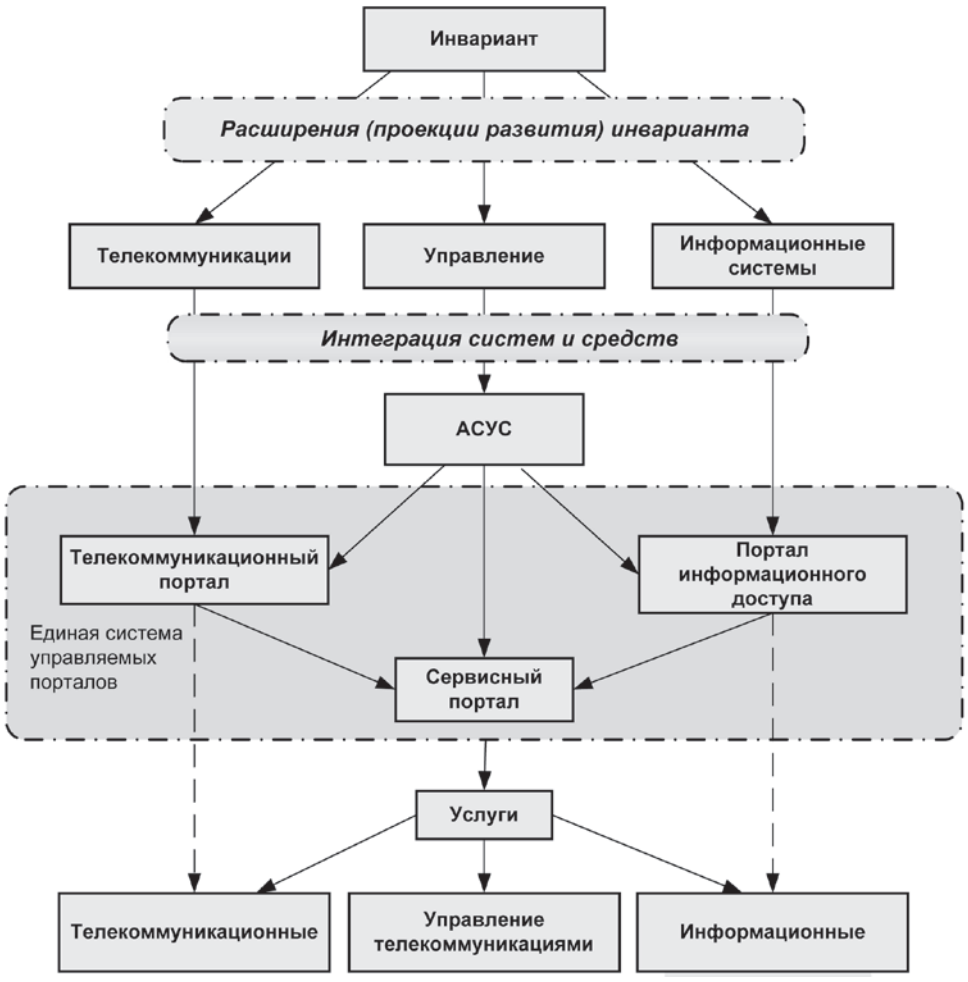


Рис. 1. Контекст системы порталов

Существенно, что в настоящее время в качестве основы для выделения инвариантной составляющей следует рассматривать ТКП – как механизм, единый для всех использующих его прикладных ИС. В этом механизме представлены фактически все составляющие инвариантной платформы, которые можно распространить на уровень прикладных ИС, сохранив единство решений по управлению и ИБ.

На рис. 2 показаны уровни типовой инвариантной платформы, составляющие ее многоуровневую архитектуру, для которой телекоммуникационные сервисы (перенос трафика различными способами с требуемыми степенью защиты и показателями качества обслуживания) предоставляет распределенная телекоммуникационная среда – транспортные сети и сети доступа (локальные вычислительные сети, структурированные кабельные сети, объектовые сети) [2]. Средства каждого уровня в общем случае обеспечивают как услуги конечного пользователя, так и сервисы для

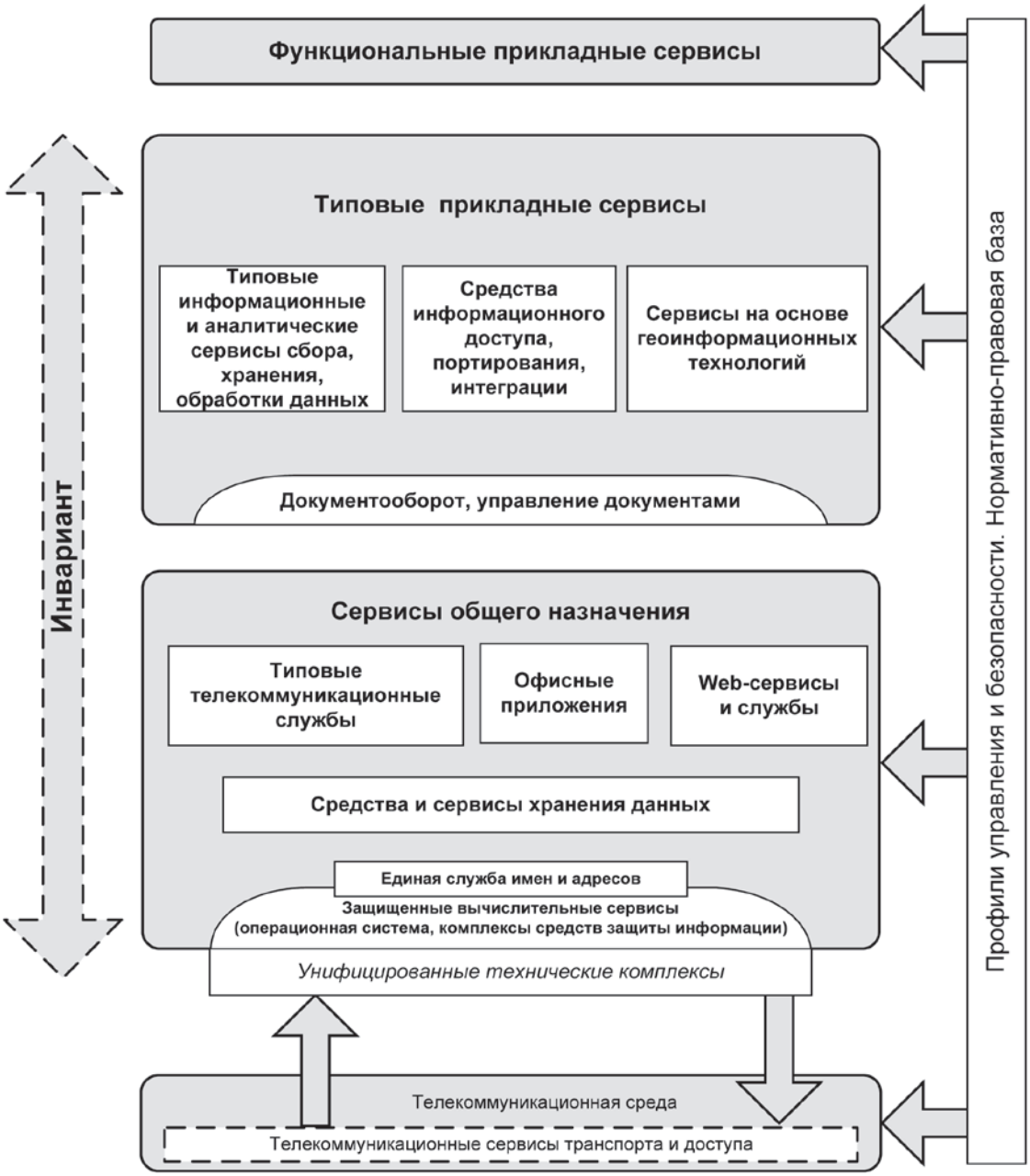


Рис. 2. Уровни типовой инвариантной платформы

средств своего и более высоких уровней. Следует отметить, что современные инфокоммуникации оперируют интегрированным IP-трафиком от различных источников с косвенной привязкой к роду связи через параметры качества обслуживания. В классической телекоммуникационной сети оперируют собственными типами трафика с привязкой к конкретным службам связи, что требует унификации систем управления [3].

Кроме этого, в рамках создания ИКС СН предполагается создать сетеориентированное окружение, которое обеспечит повышение эффективности действий должностных лиц (ДЛ) на всех уровнях управления.

При создании сетеориентированного окружения необходимо обеспечить:

робастную техническую связность;

управление информацией и доступ к ней.

Первая проблема состоит в невозможности в настоящее время «бесшовно» распространять информацию по робастной, защищенной сети, охватывающей все объекты и субъекты системы управления.

Вторая проблема заключается в достижении состояния, когда адекватная потребностям конкретного ДЛ информация становится ему доступной в нужное время и в нужном контексте.

Для понимания взаимоотношения двух областей необходимо отметить, что в сетеориентированном окружении информация не должна рассматриваться как неотъемлемая часть технической инфраструктуры, так же как и принадлежащей приложениям инфраструктуры. В сетеориентированном окружении данные выталкиваются в распределенное пространство и могут быть доступны любым авторизованным пользователям.

Чем больше охват сети, тем больше в ней может быть потенциальных пользователей. Чем ценнее информация, имеющаяся в сети, тем большее число потенциальных пользователей будут пользоваться сетью и распространять в ней информацию. Поэтому при разработке ИКС СН необходимо решить две взаимосвязанные, но существенно разные задачи:

разработать робастную потенциально полносвязную сеть для предоставления исчерпывающего набора услуг по обмену всеми типами информации;

обеспечить средства размещения, поиска и доступа ко всей информации, имеющейся в системе управления (СУ).

Необходимо отметить, что ценность ИКС СН для системы управления будет расти пропорционально квадрату числа пользователей. Рост числа пользователей будет зависеть не только от директивных документов, но прежде всего от качества услуг и их реальной востребованности должностными лицами ОУ. В качестве примера, подтверждающего это утверждение, можно рассматривать эволюционное развитие системы обмена электронной корреспонденции.

Рост числа пользователей приведет к росту объема информации, размещенной и доступной в ИКС СН, что приведет к синергетическому росту возможностей системы управления, как показано на рис.3.

Первым шагом на пути создания сетеориентированного окружения в СУ будет являться сопряжение существующих автоматизированных систем (АС) и автоматизированных систем

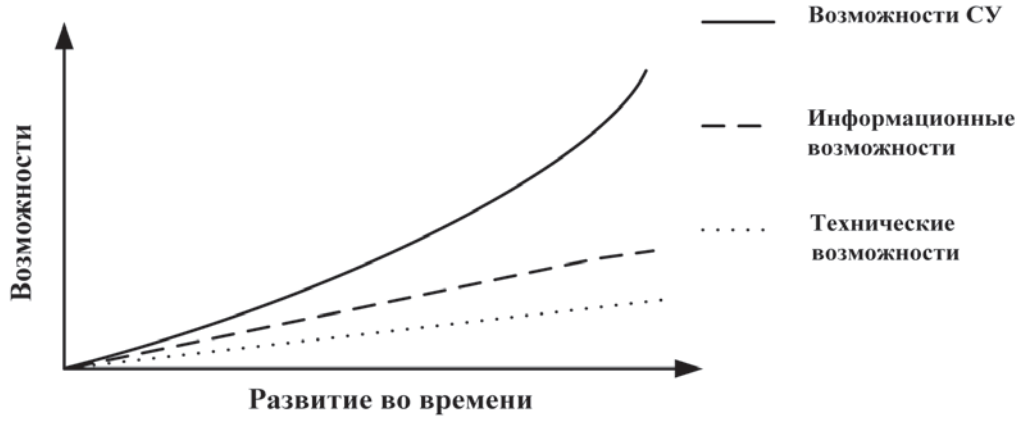


Рис. 3. Рост возможностей системы управления

управления (АСУ) с ИКС СН с целью интеграции пользователей и приложений в общую инфраструктуру обмена информацией в СУ.

Сопряжение всех АСУ с ИКС СН позволяет унифицировать взаимодействие и на порядок уменьшить число шлюзов (до N), необходимых для полносвязного взаимодействия. Поэтому появится реальная возможность перейти от автономной «стволовой» архитектуры к взаимосвязанным системам.

Однако использование механизма сопряжения с помощью шлюзов имеет существенные ограничения и должно применяться только для существующих АСУ. Ограничения заключаются в потере «прозрачности» взаимодействия и неизбежном ограничении услуг, «проходящих» через шлюз сопряжения. Ограничения могут быть вызваны как несовпадением услуг ИКС и взаимодействующей АСУ, так и возможностями шлюза.

Поэтому наиболее оптимальным является непосредственное использование услуг ИКС. Для этого вновь разрабатываемые и модернизируемые системы должны включать в свой состав средства обеспечения доступа к услугам ИКС и являться абонентскими КСА, непосредственно использующими услуги ИКС для решения прикладных задач по своему функциональному предназначению. Помимо отсутствия необходимости в разработке шлюзов, такое решение обеспечивает:

предоставление пользователям широкого набора унифицированных инфраструктурных услуг по обмену информацией и совместному использованию данных, не зависящих от подчиненности ОУ, их принадлежности к звеньям управления и выполняемых ими задач;

высокое качество предоставляемых услуг, так как в ИКС предполагается использовать продукты (изделия) не одного предприятия, а все лучшее, что разработано предприятиями военно-промышленного комплекса (ВПК);

«прозрачность» взаимодействия между всеми абонентами, имеющими доступ к услугам ИКС;

повышение эффективности совместного использования данных на основе обеспечения их глобальной видимости, доступности и понятности;

возможность интеграции и гибкого приспособления КСА и средств автоматизации под решение задач в соответствии с конкретными составом группировки войск (сил) и условиями обстановки.

В предельном случае будет создано такое сетеориентированное окружение, в котором станет возможным «бесшовное» полносвязное взаимодействие «точка – точка» и в которое будут интегрированы все источники и потребители данных вне зависимости от их подчиненности и дислокации, станет возможным взаимодействие «многие – со многими», ограниченное только требованиями безопасности информации.

Создание инфраструктуры, в которой поддерживается адаптивная полносвязность, и совместное использование данных большого числа объектов и субъектов СУ является сложной задачей, которая в принципе не решается в рамках традиционной архитектуры технической основы СУ. Однако в технологическом плане такая задача уже решалась в коммерческих проектах, но в них предъявлялись более низкие требования к обеспечению безопасности информации и отсутствовали требования технологической независимости, существенные для СУ сил специального назначения.

Современные инфокоммуникационные технологии дают возможность рассеять «туман войны» на основе существенного расширения области распространения информации, повышения качества информации и информационного взаимодействия. Становится достижимым состояние, когда информация высокого качества может быть «прозрачно» распределена среди всех, кому она необходима для выработки совместной осведомленности, понимания обстановки и намерений противника и синхронизации действий, как показано на рис.4. Таким образом, можно говорить о некоторой новой оперативной концепции, основанной на достижении информационного превосходства, которое трансформируется в увеличение боевой мощи (потенциала) на основе эффективного связывания объектов и субъектов в системе управления в единое информационное пространство на театре военных действий [4].

Вышесказанное легко проецируется на взаимодействие сил в составе разновидовых

группировок. Взаимодействие, по сути, является разрешением противоречий между централизацией и гибкостью управления, что обусловлено следующими причинами:

необходимость во взаимодействии возникает в условиях, когда командир не имеет возможности в условиях быстро изменяющейся обстановки эффективно управлять силами ввиду большого количества объектов управления и квадратичного числа связей между ними;

для организации взаимодействия необходимо упорядочить отношения между органами управления, которые не находятся в отношениях подчиненности между собой, но должны совместно решать общую задачу в условиях, когда действия одного субъекта взаимодействия непосредственно отражаются на состоянии или действиях другого субъекта;

в случае горизонтального взаимодействия объекты управления, не находящиеся в отношениях подчиненности, должны самостоятельно без участия вышестоящей инстанции решать отдельные управленческие задачи.

Таким образом, взаимодействие следует рассматривать как взаимную поддержку сил и как деятельность ОУ, не находящихся между собой в отношениях подчиненности, но совместно выполняющих задачи по упорядочению и согласованию своих действий в интересах выполнения общих задач.

Для обеспечения взаимодействия инфокоммуникационные технологии должны обеспечить возможность достижения совместной осведомленности об обстановке всех участников взаимодействия и предоставить возможность их сотрудничества, а на основе сотрудничества обеспечить синхронизацию действий.

С развитием вычислительных мощностей компьютеров, переходом на цифровые технологии коммутации пакетов с возможностью выделения «полосы пропускания по требованию» становится возможным переход к парадигме «публикация данных до обработки». В соответствии с этой парадигмой данные от всех источников помещаются в сетеориентированное окружение, где они становятся доступными всем участникам взаимодействия вне зависимости от их дислокации и организационной подчиненности. Тем самым обеспечивается возможность перехода от традиционного информационного взаимодействия «точка – точка» к взаимодействию «многие – со многими», что обеспечит возможности достижения совместной осведомленности, сотрудничества, децентрализации

Рис. 4. Достижение превосходства на основе сетеориентированного окружения

центров принятия решения и, в предельном случае, самосинхронизации действий.

В современной войне очень трудно предсказать развитие обстановки, более того, очень трудно собрать информацию, необходимую для заблаговременного планирования. Будущие операции будут противоборством в адаптивности – победителем будет тот, кто более эффективно использует свои силы в соответствии с оперативной обстановкой.

Таким образом, применение инфокоммуникационных технологий должно придать перспективной системе управления следующие характеристики:

все элементы системы управления охвачены робастной сетью, которая обеспечивает обмен всеми типами информации;

войска имеют возможность совместного защищенного использования данных из многочисленных источников;

войска имеют возможность качественного информационного взаимодействия, включая возможность сотрудничества;

войска имеют возможность выработать и поддерживать высокий уровень осведомленности обо всех видах обстановки и трансформировать его в совместное планирование;

войска имеют возможность развивать совместное понимание обстановки, включая намерения командования, и на этой основе принимать самостоятельные решения (децентрализация центров принятия решений);

войска имеют возможность самосинхронизации своих действий.

Стремительное развитие инфокоммуникационных технологий свидетельствует о том, что человечество вступает в новый век – век информации. Во всех сферах человеческой деятельности доступность информации, ее качество и качество информационного взаимодействия будут решающим фактором успеха. В области применения сил и средств специального назначения решающим фактором успеха становится достижение информационного преимущества. Достижение информационного преимущества возможно только тогда, когда информационные возможности, предоставляемые инфокоммуникационными технологиями, соответствуют информационным потребностям командиров и подчиненных. Применение современных инфокоммуникационных технологий в силах специального назначения должно сопровождаться соответствующими изменениями в концепции проведения боевых действий, тренировок и обучения. В век информации инновации и экспериментирование, созидание, а не приспособление будут определять развитие системы управления и успех применения технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Легков К.Е. Цели и задачи создания инфокоммуникационной системы военного назначения //Актуальные проблемы информационного обеспечения деятельности Войск воздушно-космической обороны. – 2013. – № 1 - С.22–30.

2. Шестаков А. В., Шерстюк Ю. М., Кривов О. А. Системно-техническая платформа построения и развития технической основы систем управления связью специальных потребителей. Телекоммуникационные технологии. Вып. 5. СПб.: ФГУП «НИИ «Рубин», 2010. –С.33–41

3. Бабошин В.А., Павлович А.А., Романюк И.А. Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2011. С. 150–153.

4. Легков К.Е. Применение сетеориентированных информационных услуг при проведении операций и ведении боевых действий //Сборник трудов ВНК ВКА им.А.Ф.Можайского. – 2013. –С.16–21.

В.А. Бабошин
К.Е. Легков

О МЕХАНИЗМЕ УПРАВЛЕНИЯ ПРЕДОСТАВЛЕНИЕМ УСЛУГ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В настоящее время в системах связи специального назначения широко используются мультисервисные сети широкополосного беспроводного доступа. С учетом возросших требований к перечню услуг мультисервисной сети, удельный мультимедийный трафик поглощает значительную часть её пропускной способности и повышает требования как к качеству информационного обмена, так и к качеству управления предоставлением услуг. В рамках реализации концепции AMS (Advanced Multimedia System) предлагается новый метод управления процессом предоставлением услуг.

Данная статья посвящена оценке качественных возможностей по управлению инфокоммуникационными услугами системы связи специального назначения в приложении к сетям беспроводного широкополосного доступа.

Ключевые слова: сети специального назначения, контейнер, мультисервисная сеть, трафик, беспроводный широкополосный доступ, коллизионные потери, доступный перечень услуг

В контексте дальнейшего технологического развития телекоммуникационной отрасли ближайшей перспективой является внедрение концепции AMS (Advanced Multimedia System), для чего необходимо переосмысление процесса управления предоставлением услуг должностным лицам органов управления (ДЛ ОУ) в системе связи специального назначения (СССН), неотъемлемой частью которой является мультисервисная сеть широкополосного беспроводного доступа [1]. Доступность, качество и своевременность предоставления услуг непосредственно зависит от системы управления и используемых в ней протоколов сигнализации. Так, например, в IP-сетях процедуры управления вызовами выполняются специализированными протоколами сигнализации, а непосредственная маршрутизация трафика обеспечивается другими сетевыми протоколами. В общем виде механизм сигнализации для IP-телефонии может иметь вид, представленный на рис. 1. [2].

Рис. 1. Механизм сигнализации в сетях IP-телефонии

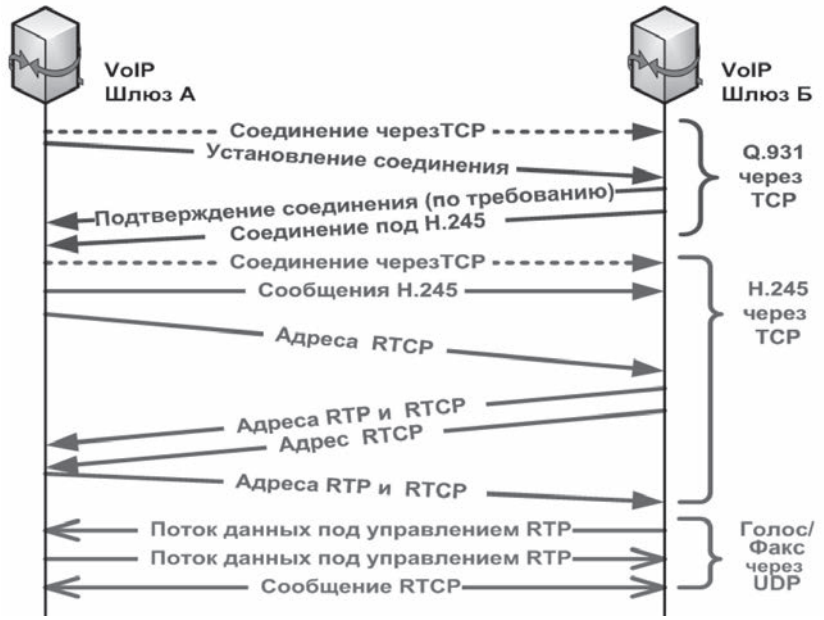


Рис. 2. Основные фазы межшлюзового взаимодействия протокола H.323

Существенным недостатком данных решений является необходимость многопротокольного обмена на разных фазах передачи информации, что приводит к возрастанию объема служебных сообщений, что проиллюстрировано примером межшлюзового взаимодействия протокола H.323 (рис.2).

Кроме того, протокол H.323 использует до 100 информационных полей в сообщениях. Протокол сигнализации SIP (Session Initiation Protocol) использует несколько десятков полей, а для организации базового соединения необходимо всего три типа запросов (INVITE, BYE и ACK) и несколько полей (To, From, Call-ID, CSeq). SIP обеспечивает ряд основных функций, включая определение местоположения и доступности пользователя, возможности станции, установления и управления сеансом, однако и этот протокол требует достаточно большого объема служебной информации. Время установления соединения в условных единицах RTT (round trip time) составляет для протокола SIP 1,5+2,5 RTT, а для протокола H .323 6-7 RTT, что связано с тем, что в запросе SIP INVITE содержатся все сведения, необходимые для организации сессии, а для H.323 обмен проводится неоднократно.

В соответствии с концепцией AMS создается универсальная коммуникационная платформа, позволяющая пользователям получать мультимедийные услуги в любом месте и на любом устройстве. Она предоставляет возможности (в зависимости от контекста) по обнаружению устройств и сервисов, организации бесшовных сессий передачи, автоматической настройке, адаптации и изменению характеристик этих сессий. Для этого используется принцип декомпозиции, согласно которого персональное терминальное устройство пользователя описывается как контейнер (container), использующий универсальное звено сигнализации [1,3]. Подобным контейнером является и мобильное устройство (телефон, коммуникатор), позволяющее управлять целым набором услуг в рамках одного канала (звена) сигнализации с использованием универсального протокола (рис.3).

Совокупность контейнера и зарегистрированных в нем приложений называется AMS Assemblage – сборка AMS, конфигурация которой и определяет, какие услуги доступны пользователю устройства-контейнера (рис.4) [1]. Из рисунка видно, что компоненты AMS Assemblage могут присутствовать в одном устройстве (мультимедийный терминал) или находиться и в физически разнесенных устройствах.

Очевидно, что данный подход требует совершенствования механизма управления процессом предоставления услуг. Функциональная структура AMS Assemblage подразумевает деление на два основных уровня: транспортный

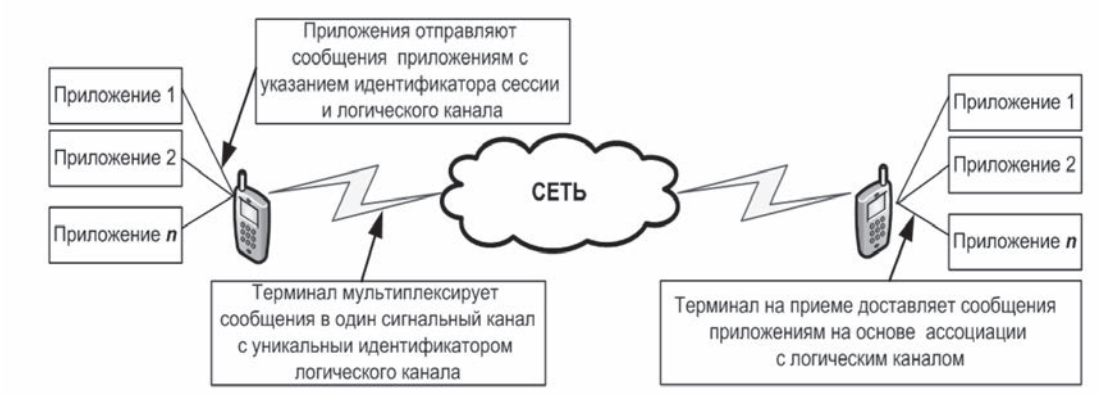


Рис. 3. Взаимодействие приложений в AMS

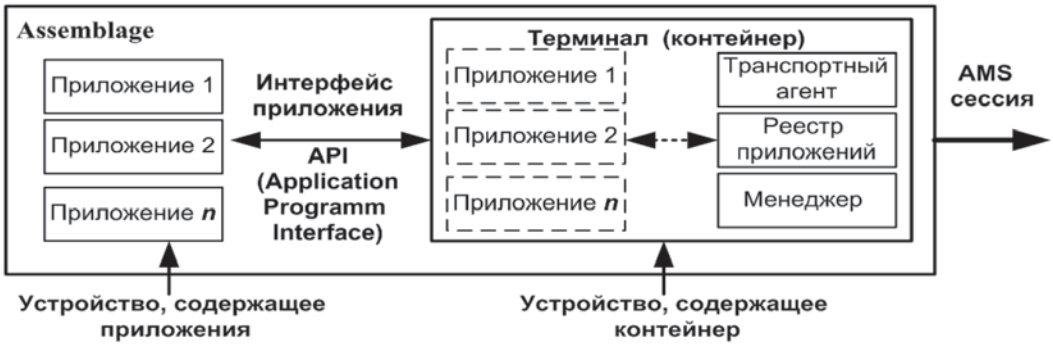


Рис. 4. Структура AMS сборки

и приложений. Транспортный уровень состоит из подуровней сигнализации и передачи данных. Уровень приложений представляет собой набор приложений, каждое из которых выполняет какую-то задачу, например, аутентификацию, тарификацию, определение местоположения или управление конфигурацией [3]. При этом приложения могут взаимодействовать друг с другом, как локально (активировать тот или иной элемент интерфейса, скопировать файл), так и удаленно (при осуществлении голосовой и видеосвязи, при передаче данных), а также одновременно (локально и удаленно), например, перевести голосовой вызов с мобильного телефона на стационарный, перенести видеосессию с коммуникатора на телевизор и т. п.

Следует отметить, что с учетом возросших требований к перечню услуг, удельный вес различных видов трафика значительно меняется, причем мультимедийный трафик поглощает значительную часть пропускной способности сетей и повышает требования к качеству информационного обмена.

Особенно актуальна эта задача применительно к мультисервисным сетям беспроводного широкополосного доступа, функционирование которых зависит от условий распространения радиоволн, а также наличия как непреднамеренных, так и преднамеренных помех, что требует, в том числе, оценки уровня помехозащищенности приёма сигналов, от которого будет зависеть возможность предоставления той или иной услуги. Радиус действия отдельного терминала определяется пороговым значением мощности сигнала $P_{\text{с пор}}$, обеспечивающим правильный прием пакета в точке приёма. При этом в зоне радиодоступа, ограниченной радиусом R, вероятность ошибки при поэлементном приеме пакетной информации не превышает минимально допустимое значение $P_{k\ min}$, фактически определяющее возможность предоставления той или иной услуги. Очевидно, что если исключить влияние местности и помех, зона доступности к определенному перечню услуг (относительно базовой станции) может быть представлена в виде совокупности $\Phi=\{\Phi_1, ...\Phi_к, ...\Phi_К\}$, состо-

ящей из K подзон, в которых обеспечивается передача пакетов с определенной полосой пропускания, то есть K определяет доступный перечень разнородных услуг $\Omega=\{\Omega_1,...\Omega_к,...\Omega_K\}$. В реальных условиях существует задача рационального распределения общего ресурса, в случае, когда пользователи услуг сети находятся в различных условиях ведения связи (удаленности абонентов от точки доступа, условий распространения радиоволн, воздействия помех, требований к предоставлению услуг, приоритета пользователей, требований по своевременности, достоверности и т.д.). Очевидно, что наибольший интерес представляет определение практической пропускной способности сети. Так, согласно модели Бьянки при распределенном механизме управления доступом DCF (distributed coordination function), моменты времени t и $(t+1)$ соответствуют началам следующих друг за другом виртуальных слотов (ВСл). Предполагается, что вначале ВСл каждая станция пытается отправить пакет с вероятностью τ, определяемой как (1):

$$\tau=\frac{2q(1-p^{m+1})}{q(1-p^{m+1})+W_0[1-p-p(2p)^{m'}(1+p^{m-m'}q)]}, \quad (1)$$

где $q=1-2p$, W_0 – минимальный размер конкурентного окна; m – максимальное число попыток передачи; m' – номер попытки передачи при максимальном размере конкурентного окна, $m \leqslant m'$; p – условная вероятность потери пакета.

При нахождении терминалов в зоне взаимной радиовидимости (функция DCF) попытки передачи происходят в одинаковых для всех узлов временных интервалах и условная вероятность потери пакета определяется как:

$$p=1-(1-\tau)^{n-1}, \quad (2)$$

где n – общее количество терминалов (контейнеров) [3].

В многоскачковых сетях (при отсутствии взаимной радиовидимости), могут возникать потери пакетов из-за работы протокола MAC. Для рассмотрения влияние работы протокола MAC на условную вероятность p, рассмотрим упрощенную модель физического уровня. Таким образом, представим, что дальность передачи R_T каждого узла фиксирована и все узлы передают с одинаковой мощностью; только терминалы в пределах подзоны Φ_K от передающего терминала могут правильно принимать и декодировать пакеты; дальность контроля несущей каждым узлом фиксирована в пределах радиуса R_S; нет эффекта энергетического захвата: пакет не может быть получен узлом, если он коллизирует ходя бы с одним пакетом, переданным любым узлом в пределах данного радиуса; канал связи без ошибок: полученный пакет всегда декодируется правильно при отсутствии коллизий. Введение этих ограничений позволит выделить проблемы, связанные непосредственно с работой протоколов MAC уровня в сетях с произвольным множественным доступом к среде, например 802.11 DCF.

Можно определить четыре различных категории потерь пакета из-за работы протокола MAC:

– потери из-за коллизий между скоординированными терминалами, происходящие из-за коллизии при одновременном получении пакетов от нескольких терминалов, находящихся в зоне радиовидимости;

– потери из-за информационной асимметрии: связь $l(i, j)$, страдает из-за связи $l'(i', j')$ по причине эффекта информационной асимметрии, если удовлетворены следующие геометрические зависимости: $d(i,j)>R_S$, $d(i, i')>R_S$,; передающие терминалы связей l и l' вне зоны радиовидимости друг друга; $d(j, i')>R_S$,: принимающий терминал l находится в зоне радиовидимости передающего l'; $d(i, j')>R_S$, принимающий l' не находятся в зоне радиовидимости передающего терминала l', где $d=(m, n)$ – евклидово расстояние между узлами m и n. Вероятность потери пакета обозначим $p_{ia}^{(i)}$;

– потери из-за близких скрытых терминалов. Подобные потери происходят между двумя связями $l(i, j)$ и $l(i', j')$ когда: $d(i, i')>R_S$: передающие терминалы l и l' вне зоны радиовидимости; $d(i, j')<R_S$: принимающий l находится в зоне радиовидимости терминала l'; $d(i, j')<R_S$ принимающая станция l находятся в зоне радиовидимости станции l, $p_{nh}^{(i)}$ – вероятность потери пакета;

– потери из-за удаленных скрытых терминалов происходят между двумя связями $l(i, j)$ и $l'(i', j')$ когда $d(i, i')>R_S$: передающие терминалы l и l' вне зоны радиовидимости; $d(j, i')>R_S$: принимающий терминал l находится вне зоны радиовидимости передающего терминала l'; $d(i, j')<R_S$ принимающий терминал l› находятся в зоне радиовидимости терминала l.

В этом случае пакеты управления, посланные одной приемной станцией, интерферируют с приемом пакетов в другой. Хотя теоретически конфигурация симметрична, потери пакетов неравнозначны, так как узел, начавший передачу первым, может закончить её успешно. Полную вероятность потери пакета узла i можно рассчитать согласно выражения (3):

$$p(i) = 1 - [1 - p_{co}(i)][1 - p_{ia}(i)][1 - p_{nh}(i)][1 - p_{fh}(i)]. \quad (3)$$

Приведенная классификация является достаточно полной для описания возможных коллизионных потерь между любыми двумя связями в сети беспроводного широкополосного доступа СССН.

Таким образом, совершенно очевидно, что при прямой коррелированности R_S и Φ_K, предоставляется возможность сформировать алгоритм управления инфокоммуникационными услугами системы на основе описанной концепции AMS, а также определить вероятность предоставления определенного перечня услуг в зависимости от конкретных условий ведения связи.

СПИСОК ЛИТЕРАТУРЫ

1. Бабошин В.А., Павлович А.А., Романюк И.А. Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения // Труды Северо-Кавказского филиала МТУСИ. Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2011. С. 50–153.

2. Гольдштейн Б. С. Сигнализация в сетях связи. – М.: Радио и связь, 1997.

3. A.H. Salden, "Multimedia system analysis and processing," In Proceedings of 2001 IEEE International Conference on Multimedia and Expo, ICME2001, August 22-25, 2001, Waseda University, Tokyo, Japan

4. Бабошин В. А., Яковицкая М. В., Павлович А. А. Система управления инфокоммуникационными услугами в мультисервисных сетях специального назначения // Материалы 7-й научно-практической конференции «Проблемы развития технологических систем государственной охраны, специальной связи и информации». 3–4 марта. В 10 ч. Ч. 2 / Под общ. ред. В. В. Мизерова. Орел: Академия ФСО России. 2011. С. 114–118.

К.Е. Легков
О.А. Скоробогатова

НАПРАВЛЕНИЯ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СИЛ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Главное направление разрешения информационно-управленческих проблем строительства и применения сил специального назначения (СН) – это информационно-техническое объединение всех имеющихся и перспективных средств в единое информационное пространство (ЕИП) за счет развертывания базовой информационно-управляющей системы, их интеграции в систему оружия и органов управления.

Такое объединение потребует соответствующего совершенствования средств связи и передачи данных, всех видов информационного обеспечения, автоматизации и информатизации управления.

Очевидно, что создание столь сложной, пространственно-распределенной системы невозможно без решения целого ряда проблем технического и организационного характера.

Техническую основу сегмента сил СН в едином информационном пространстве должна составить многомерная защищенная высокоскоростная сеть, включающая в свой состав следующие информационные средства: добывания информации, ее обработки и передачи, а также синхронизации и передачи сигналов точного времени.

Ключевые слова: система управления, информационное взаимодействие, система связи, инфокоммуникационная система, алгоритм

Одной из перспективных задач развития автоматизированных систем управления (АСУ) становится задача предвидения возможного развития оперативной и боевой обстановки, формирования рациональных способов боевых действий. При этом необходимо обеспечивать соответствие между возможностями комплекса средств автоматизации (КСА) по формированию способов боевых действий, с одной стороны, и обязанностями, правами, ответственностью должностных лиц в каждом звене управления, с другой.

В иерархической системе управления формирование способа боевых действий сил заключается в определении пространства, времени и форм боевых действий, оперативного построения, маневра сил и средств подчиненных частей и подразделений для решения специальных задач.

Таким образом, как в повседневной деятельности сил, так и в компьютерных моделях поддержки принимаемых решений должны отражаться принципы управления, в частности:

принцип единоначалия;

принцип централизации управления с предоставлением подчиненным инициативы в определении способов выполнения поставленных специальных задач;

принцип личной ответственности должностных лиц за принимаемые решения на применение подчиненных сил и результаты выполнения ими поставленных специальных задач.

Наряду с вышеизложенным, необходимо учитывать и достаточно важную тенденцию в развитии автоматизированных систем управления силами, на основе информационно-управляющих систем реального времени (ИУС РВ).

Основу ИУС РВ составляют пространственно разнесенные источники информации, действующие на различных физических принципах и обеспечивающие сбор, сверхбыструю обработку

информации компьютерные сети (сетецентрические технологии).

Функциональные подсистемы перспективной АСУ сил СН должны обеспечивать автоматизацию как целевых процессов управления применением сил, так и функций управления органов управления, а инфраструктурные подсистемы должны обеспечивать базовый набор услуг по управлению информационными и вычислительными ресурсами АСУ в интересах работы всех функциональных подсистем. Они должны создаваться в контексте единых архитектурных решений, использовать максимально унифицированные программные компоненты и общую технологическую и информационную среду совместного применения и функционирования данных программных компонентов.

Использование инфраструктурных систем позволит повысить технологичность разработки перспективной АСУ сил СН и функциональных подсистем, как ее компонентов. Применение унифицированных программных компонентов, разработанных в рамках инфраструктурных систем, должно позволить разработчикам функциональных подсистем максимально сосредоточиться на решении поставленных задач, стоящих перед конечными пользователями АСУ сил СН. При этом разрабатываемыми средствами должно обеспечиваться сопряжение с существующими и перспективными системами освещения обстановки и управления.

Работа перспективной АСУ сил СН должна обеспечиваться ИКС СН.

Основой создания АСУ сил СН должна стать реализация концептуальной модели сервис-ориентированной архитектуры, основными достоинствами которой являются возможность эволюционного развития, обеспечение совместимости между отдельными элементами, многократное (повторное) использование программных компонентов.

Эта модель должна состоять из следующих основных компонент:

презентационный уровень описывает интерфейсные сервисы для взаимодействия пользователей с информационной системой, включая закрытые и открытые порталы, доступ с мобильных устройств, а также различные преобразования информации при взаимодействии с внешними системами и устройствами;

на уровне функциональных сервисов формируются модели и осуществляется управление выполнением процессов АС с использованием специализированных средств (типа BPEL), а также координация автоматизированных и «ручных» операций;

интеграционные сервисы обеспечивают взаимодействие между приложениями, которое может быть реализовано, в частности, с использованием средств обмена сообщениями или в рамках единой среды исполнения, такой как сервер приложений J2EE;

сервисы уровня данных реализуют средства извлечения и повторного использования данных из СУБД и приложений. Явное выделение такого уровня позволяет изолировать вышестоящие компоненты архитектуры от изменений в технологиях, а также обеспечить единый унифицированный подход к выполнению операций с данными;

уровень инфраструктуры, приложений и СУБД является как бы основой для всей структуры, и именно здесь концентрируются основные инвестиции в ИТ.

Взаимодействие между этими уровнями, однако, осуществляется не напрямую, а через сервисы, выделенные на уровень обработки событий. Сервисы этой компоненты архитектуры обеспечивают сбор данных о событиях в масштабе АСУ, необходимое преобразование и маршрутизацию этих данных между разными уровнями, а также «обратную связь» между сервисами каждого отдельного уровня.

При формировании функциональных подсистем АСУ сил СН наиболее важным становится принцип, при котором каждый процесс должен автоматизироваться однократно, вне зависимости от принадлежности к виду и уровню управления. Для обеспечения специфики вида деятельности, налагаемой видовой принадлежностью или уровнем управления, необходимо обеспечить широкие возможности настройки ПО (по видам и источникам информации, применяемым информационно-расчетным задачам, УФД и т.д.).

В настоящее время в силах СН на вооружении находится множество систем и комплексов, с той или иной степенью эффективности решающих различные задачи управления силами и средствами СН. Однако имеет место большая избыточность поступающих данных, сложность,

а зачастую и невозможность организации взаимодействия и оперативной совместимости различных систем, а также несовершенство механизма распределения конечных результатов.

С технической точки зрения причиной изолированности систем и комплексов является излишнее разнообразие аппаратных и программных средств, платформ, архитектур и технологий, различие интерфейсов и протоколов, а также отсутствие изначально заложенных механизмов взаимодействия систем.

Необходима разработка и внедрение аппаратно-программных средств, обеспечивающих комплексирование информации от разнородных источников, автоматизацию процессов обработки и интерпретации поступающей информации, а также формирование общей базы данных с распределенным доступом к ней, что позволит создать единое информационное пространство, снизить избыточность поступающей информации, повысить качество ее представления, скорость поиска данных и их доведения до конечного пользователя.

Предусмотреть возможность эффективного решения сложных вычислительных задач, обеспечения взаимодействия программных комплексов и систем путем организации распределенных вычислений в сетях на основе рационального использования сетевых ресурсов – процессоров, памяти, коммуникационного оборудования, алгоритмов и программ.

Функциональные подсистемы (ФПС) АСУ, должны быть определены как наборы унифицированных и не унифицированных программных компонентов – Функциональных сервисов, способных работать совместно, в соответствии с установленным формализованным регламентом деятельности. Функциональные подсистемы рассматриваются, как совокупности слабо связанных Функциональных сервисов, применяемый набор которых определяется задачей по управлению АСУ.

Инфраструктурные системы (ИС) обеспечивают предоставление функционально независимых услуг абонентам и элементам АСУ. Инфраструктурные системы должны рассматриваться как наборы Инфраструктурных сервисов, предназначенные для реализации технологической основы для Функциональных сервисов. Инфраструктурные сервисы должны предоставлять возможности функциональным подсистемам реализовывать свое назначение путем манипулирования набором применяемых Инфраструктурных систем и использования их функциональных возможностей. Инфраструктурные сервисы скрывают техническую реализацию от Функциональных сервисов, а специфицирование (описание и следование описанию) интерфейсов обеспечивает необходимую гибкость, возможности масштабирования, а также постепенного улучшения и наращивания функциональности подсистемы, путем замены реализации Инфраструктурного сервиса, без необходимости внесения изменений в Функциональную подсистему.

Обеспечение информационно-технического взаимодействия АСУ со сторонними (существующими, унаследованными) системами производится путем их интеграции в единую распределенную среду информационного взаимодействия через унифицированный механизм адаптеров. Далее этот механизм может быть применен как способ интеграции в АСУ СН.

Рабочее пространство пользователя (РПП) должно обеспечивать единую рабочую область для всех Функциональных подсистем, которые использует пользователь в рамках своей деятельности. Использование Рабочего пространство пользователя должно обеспечить преимуществом сквозной идентификации пользователя для различных Функциональных подсистем, при выполнении всех функций АРМ, применяемых пользователем в рамках единой рабочей области. Для полного и эффективного взаимодействия пользователя с АСУ необходимо реализовать РПП на основе концепции «толстого» клиента. Для простого взаимодействия пользователя с АСУ и улучшения мобильности пользователя необходимо реализовать РПП на основе концепции «тонкого» клиента.

Реализация указанных направлений развития системы управления сил СН позволит:

обеспечить планируемое повышение эффективности средств поражения до требуемых показателей;

обеспечить создание системы разведки и контроля, позволяющую контролировать 100% зон ответственности;

обеспечить автоматизированное решение 100% задач управления силами СН с высоким качеством реализации циклов управления силами.

Очевидно, что создаваемая система должна иметь открытую архитектуру и обеспечивать возможность оперативной адаптации к изменениям состава и структуры сил СН в целом и отдельных группировок, в частности, в том числе и оперативно формируемых на отдельных направлениях.

СПИСОК ЛИТЕРАТУРЫ

1. Легков К.Е. Применение сетеориентированных информационных услуг при проведении специальных операций //Сборник трудов военно-научной конференции ВКА им.А.Ф.Можайского. – 2013. –С.16–21.

2. Трушин В.В. О сущности взаимодействия войск в операции (бою) // Военная мысль. – 2007. – № 4. – С. 16–18.

3. Шеремет И.В. «Сетецентрическая война»: истоки и технические аспекты // Военно-промышленный курьер. – 2006. – № 7. – С. 22–24.

К.Е.Легков
Врио начальника кафедры технологий и средств технического обеспечения и эксплуатации АСУ (войсками) Военно-космической академии имени А.Ф. Можайского, кандидат технических наук
А.Б.Зверев
ЗАО НПЦ ИРС

ОСНОВНЫЕ ПОДХОДЫ К ПОСТРОЕНИЮ ТЕХНИЧЕСКОЙ ОСНОВЫ СИСТЕМЫ УПРАВЛЕНИЯ НА БАЗЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ РАЗЛИЧНОГО НАЗНАЧЕНИЯ

Анализ существующей технической основы системы управления показывает, что на сегодняшний день она не в полной мере удовлетворяет предъявляемым к ней требованиям по обеспечению единого централизованного руководства всеми разновидовыми и разноведомственными силами, в мирное время (в том числе, при проведении специальных операций и действиях в чрезвычайных ситуациях) а так же при переводе сил с мирного на военное положение, в военное время.

Основные недостатки:

существующие автоматизированные системы (АС) и автоматизированные системы управления (АСУ) разновидовых и разноведомственных сил специального назначения ориентированы на поддержку управления только силами, в интересах которых они функционируют. Используют ресурсы связи монопольно в интересах каждого из обеспечиваемых органов управления;

существующие и создаваемые АС и АСУ, как правило, не поддерживают информационно-технического сопряжения между собой и с комплексами средств автоматизации (КСА) высшего звена управления (ВЗУ);

не обеспечивается быстрая реконфигурация технической основы системы управления в соответствии с изменениями в организационно-штатной структуре органов управления в мирное и военное время, особенно в оперативном звене управления. Это существенно усложняет развертывание системы управления силами и увеличивает время ее перевода с мирного на военное положение в условиях резкого обострения обстановки или внезапной агрессии противника;

в штабах и на пунктах управления не обеспечиваются автоматизированные сбор, обобщение, распределение и своевременное доведение данных обстановки;

возможности автоматизированного информационного взаимодействия между органами управления формирований различной ведомственной принадлежности в ходе принятия (уточнения) решения, определения и постановки задач силам, разработки документов не обеспечивают своевременное принятие эффективных решений;

средства автоматизации (системы, комплексы) управления силами специального назначения используются разрозненно и информационное взаимодействие между ними практически отсутствует;

управление частями и подразделениями осуществляется, как правило, без использования автоматизированных средств обмена информацией с использованием неавтоматизированных средств управления;

доведение приказов (команд, сигналов) боевого управления с вышестоящих пунктов

управления до нижестоящих осуществляется неавтоматизированным способом;

автоматизированный обмен информацией между средствами разведки, управления и поражения оперативного и тактического звеньев практически отсутствует, что ориентировочно на 25–30 % снижает степень реализации боевых возможностей сил специального назначения;

инфокоммуникационное взаимодействие не унифицировано не только в масштабах сил специального назначения, но зачастую даже в пределах одного звена управления.

Как составная часть технической основы системы управления система связи сил специального назначения не соответствует современным условиям и сдерживает внедрение современных инфокоммуникационных технологий.

С другой стороны, каждая существующая АС и АСУ, как правило, имеет свою систему обмена данными и использует выделенные ресурсы связи только в собственных интересах. Продолжение такой политики приведет к тому, что переход на высокоскоростные цифровые каналы связи не даст существенного приращения в эффективности использования ресурсов связи и, соответственно, повышении эффективности системы управления, а также не обеспечит совокупное снижение стоимости аренды канальных ресурсов.

В ожидаемых условиях ведения боевых действий устойчивость существующей системы связи является недостаточной, что обусловлено:

низкой помехозащищенностью радиоканалов различных диапазонов в условиях радиоэлектронного поражения;

жестким закреплением каналов за направлениями связи;

высокой подверженностью кабельных линий связи поражающим факторам ядерного оружия (особенно электромагнитное излучение);

невозможностью организации обходных направлений с помощью сохранившихся после воздействия узлов и каналов связи, а также использования связных ресурсов узлов связи в интересах смежных пунктов управления.

Оценки устойчивости системы связи и предложения по способам ее повышения при переходе на цифровые коммуникационные технологии, в том числе на аренду виртуальных каналов у операторов связи ЕСЭ РФ, отсутствуют.

В настоящее время фактически отсутствует единый взгляд на облик (архитектуру) технической основы системы управления и ее элементов. Более того, руководящие нормативные документы, определяющие требования к перспективным средствам управления, в значительной степени противоречивы. Отсутствуют документы, регламентирующие оперативное и функциональное взаимодействие различных АС и АСУ в различных условиях обстановки.

Таким образом, техническая основа системы управления не в полной мере соответствует предъявляемым к ней современным требованиям по тактико-техническим (включая вероятностно-временные) характеристикам, в том числе по возможностям интеграции процессов управления силами специального назначения, пропускной способности, разведзащищенности, устойчивости и мобильности, возможностям информационного взаимодействия. Она не обеспечивает не только эффективную поддержку совместного применения разновидовых и разнородных сил и средств в совместных операциях, но и осуществление повседневной деятельности.

В значительной степени такое состояние технической основы системы управления обусловлено ориентацией на устаревшие технологии и подходы в области инфокоммуникационных технологий.

Традиционный подход к построению технической основы системы управления (СУ) на базе АС и АСУ различного назначения ориентирован на создание автономных «островков автоматизации», автоматизирующих ограниченный набор регламентированных процессов (функций) управления на основе использования жестко детерминированных алгоритмов обработки данных, при этом:

под каждую АСУ, как правило, создается собственная система обмена данными, основанная на специализированных протоколах обмена;

каждая АСУ имеет собственные частные решения по информационному взаимодействию внутри АСУ;

каждая АСУ оперирует собственными структурами данных, жестко завязанными на приложения конкретной АСУ;

собственные решения по обмену данными и информационному взаимодействию, а также

собственные данные делают практически невозможным полноценное взаимодействие между различными АСУ.

АСУ охватывают некоторые процессы управления в одной из областей деятельности по нескольким уровням управления. В предельном случае для полной связности N систем необходимо специфицировать и реализовать N * (N – 1)/2 шлюзов (рис.1). Таким образом, мы имеем квадратичный рост сложности АСУ сил специального назначения при включении в ее состав новых систем. Полная связность, во многих случаях, является избыточной, но это ненамного упрощает задачу.

Фактически, должностные лица органов управления становятся заложниками таких систем, они не имеют доступа к первичным данным и зачастую не могут организовать информационное взаимодействие и совместное использование информации от различных систем. Это связано с тем, что архитектура АСУ разрабатывается на принципе автономности, что создает барьеры на пути информационных потоков, связанных с взаимодействием должностных лиц – пользователей различных систем, как в повседневной деятельности, так и при ведении боевых действий. В частности, «стволовая» архитектура АСУ делает практически невозможным полноценное горизонтальное взаимодействие.

Данные, циркулирующие в АСУ, предназначены для органов управления определенного звена и определенного круга должностных лиц (ДЛ), а также решения задач по предназначению конкретной АСУ. Очевидно, что при таком подходе, на фоне дублирования информации в различных АСУ, порождаются информационные, организационные, функциональные и технические барьеры, которые препятствуют эффективному использованию совокупности АСУ в интересах повышения эффективности СУ в целом.

Таким образом, техническая основа СУ, построенная на основе АСУ, не может обеспечить полносвязное взаимодействие на всех уровнях управления, гибко подстраиваться под изменения структуры сил специального назначения, а тем более под структуру разновидовых группировок, не может охватить все разнообразие задач

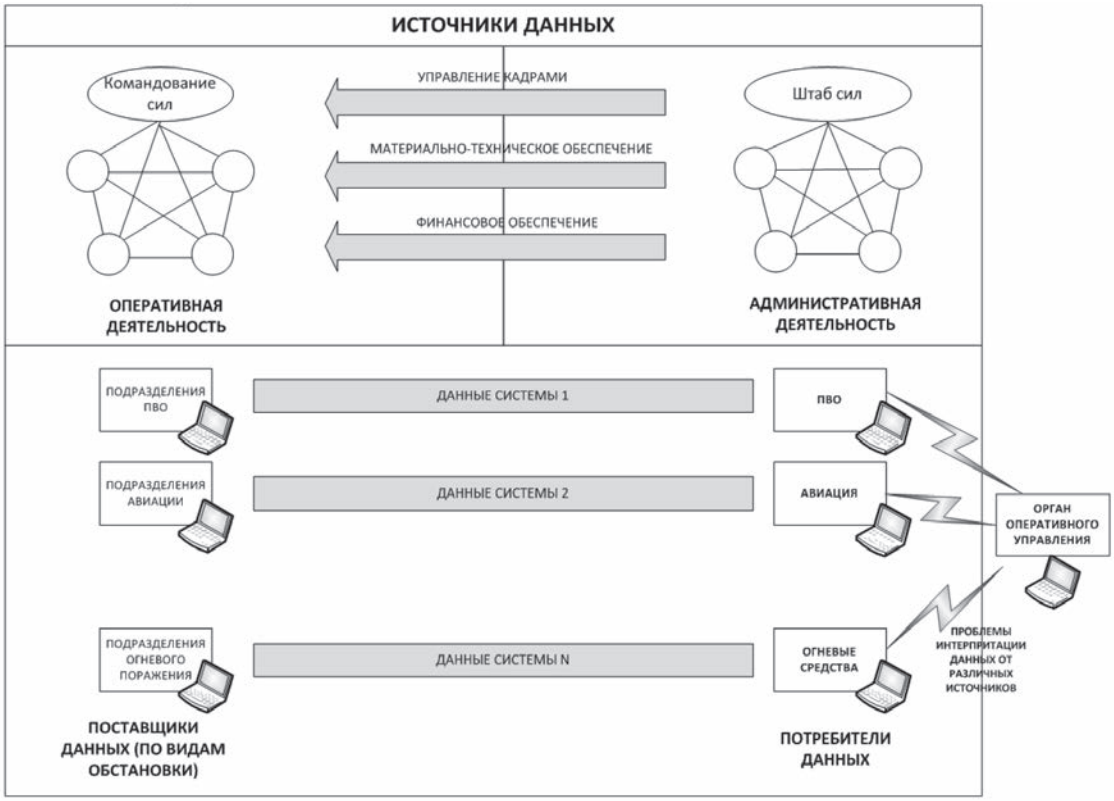


Рис. 1 Модель взаимодействия на базе АСУ

подготовки и применения сил в различных условиях обстановки.

Развитие инфокоммуникационных технологий формирует новые информационные возможности и концепции их применения, при этом изменяется также и природа самих технологий и возрастает скорость самих изменений. Природа изменений, в сочетании с высокой скоростью изменений и очень высокой ценой ошибок, затрагивающих вопросы обороноспособности, создает комплекс сложных проблем, связанный с применением «разрушительных новшеств». Это значит, что их применение может быть малоэффективным, если оно не сопровождается одновременными изменениями в доктрине, концепциях ведения боевых действий и управления силами, подготовки и обучения личного состава.

Тем не менее, традиционный подход к построению технической основы СУ фактически исчерпал возможности повышения эффективности системы управления. Сохранение этого подхода, при одновременном качественном росте объемов информации, делает практически недостижимым обеспечение «прозрачности» информационного взаимодействия между всеми ДЛ и/или приложениями различных АСУ.

АСУ, обеспечивая существенное повышение эффективности некоторых процессов управления, не могут интегрально существенно улучшить эффективность системы управления в целом, а поэтому в будущем традиционная архитектура АСУ должна применяться только для автоматизации наиболее критичных, жестко определенных процессов и процессов реального времени. Это не означает, что не должны разрабатываться функциональные системы, реализующие широкий спектр информационных и расчетных задач, но они должны применяться в архитектуре, отличной от архитектуры традиционных АСУ, и должны работать не с собственными информационными ресурсами, а с информационными ресурсами, доступными во всей системе управления.

Таким образом, дальнейшее повышение эффективности системы управления может быть обеспечено не в рамках продолжения создания традиционных АСУ и постоянных совещаний по вопросам информационно-технического сопряжения, а в рамках изменения подхода к автоматизации и информации.

Вторая существенная проблема связана с невозможностью, в рамках существующей архитектуры технической основы СУ, адекватно использовать ресурсы связи. Необходимо создать сетевую инфраструктуру, которая обеспечит:

эффективное использование всех доступных ресурсов связи;

быструю адаптацию в условиях разрушающих воздействий, компенсируя низкую устойчивость системы связи;

необходимый уровень защиты информации при передаче ее по любым каналам связи и транспортным сетям;

предоставление всем системам возможности использования унифицированного набора сетевых услуг;

возможность единого адресования объектов и субъектов в масштабах.

Силы специального назначения для достижения превосходства в принятии эффективных решений должны иметь быстрый доступ к релевантной, точной и своевременной информации, возможность автоматизированной выработки и распространения знаний в устойчивом инфокоммуникационном окружении в условиях быстроменяющейся обстановки. В этом плане создание инфокоммуникационной системы специального назначения (далее – ИКС СН) предполагает собой создание робастного (устойчивого) инфокоммуникационного окружения (сетеориентированного окружения (СО), обеспечивающего приемлемую скорость доступа к релевантной, своевременной информации, и в создании фундамента для обеспечения возможностей автоматизированной выработки и распространения знаний.

СПИСОК ЛИТЕРАТУРЫ

1. Легков К.Е. Применение сетеориентированных информационных услуг при проведении операций и ведении боевых действий //Сборник трудов военно-научной конференции ВКА им.А.Ф.Можайского. – 2013. –С.16–21.

2. Легков К.Е. Цели и задачи создания инфокоммуникационной системы военного назначения // Актуальные проблемы информационного обеспечения деятельности Войск воздушно-космической обороны. – 2013. – № 1 – С.22–30.

К.В. Марченко
ООО «Т8»

ПОСТРОЕНИЕ СКОРОСТНЫХ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ СВЯЗИ НА ОСНОВЕ КОГЕРЕНТНОЙ DWDM-СИСТЕМЫ «ВОЛГА» В ИНТЕРЕСАХ СПЕЦПОЛЬЗОВАТЕЛЕЙ

Показана актуальность перехода к когерентным каналам 100 Гбит/с с сохранением существующей инфраструктуры сети. Описаны преимущества когерентных систем: повышение скорости магистральной сети в 5 раз, снижение цены за 1 Гб переданной информации, надёжная коммутация каналов с использованием ROADM, снижение рисков несанкционированного доступа к системе управления. Представлена система «Волга» российского производства, которая позволяет строить скоростные сети связи с пропускной способностью до 9,6 Тбит/с с возможным апгрейдом.

Введение

Один из основных выводов масштабных военных учений, проведённых в 2013 г. – необходимость глубокой модернизации военных систем связи. Министр обороны РФ С.К. Шойгу оценил эффективность системы военной связи на уровне 18%, назвав её «одной из наших серьёзных проблем». В частности, было отмечено неудовлетворительное состояние волоконно-оптической сети связи Министерства обороны РФ. Она обладает крайне низкой пропускной способностью, которая не соответствует потребностям, предъявляемым со стороны современных средств вооружений.

По оценкам экспертов, для обеспечения потребностей ГУС МО пропускная способность магистральных каналов между регионами должна составлять на сегодняшний день не менее 300-400 Гбит/с. Сеть должна обеспечивать возможность многократного резервирования трафика, возможность коммутации и доставки трафика в точку назначения разными путями. Кроме того, система управления сети должна быть устойчива к сторонним информационным атакам. Поведение сети, построенной на оборудовании и программном обеспечении зарубежного производства, в условиях чрезвычайной ситуации практически непредсказуемо из-за наличия не декларированных возможностей (НДВ) иностранного оборудования.

Очевидно, что Министерству обороны РФ необходимо модернизировать магистральную волоконно-оптическую сеть. Прежде всего, необходимо оборудовать скоростные каналы 100 Гбит/с на уровне ядра сети (7 УАК «каждый с каждым»), и на уровне «ядро — узлы внутризоновых сетей» (не менее двух разнесённых оптоволоконных трасс к каждому узлу).

Современные волоконно-оптические системы передачи данных со скоростью 100 Гбит/с основаны на когерентных оптических технологиях. Они имеют целый ряд преимуществ перед некогерентными системами, которые использовались до сих пор. Помимо увеличения скорости передачи (с 10 Гбит/с или 40 Гбит/с до 100 Гбит/с), когерентные технологии позволяют строить более протяжённые линии связи без компенсаторов дисперсии, с меньшим количеством усилителей и пунктов регенерации сигнала. Уменьшение количества оборудования снижает затраты на построение и дальнейшее развитие сети, повышает её надёжность и удобство управления.

Помимо увеличения пропускной способности, необходимо также минимизировать уязвимость сети, снизить риски несанкционирован-

ного доступа к системе управления. Этого можно добиться за счёт использования отечественного оборудования и программного обеспечения, а также за счёт упрощения архитектуры сети и отказа от сложных электронных компонентов в пользу более простых и надёжных решений. В частности, для коммутации каналов на верхнем уровне вместо электронных матриц коммутации можно использовать настраиваемые оптические мультиплексоры ввода-вывода каналов (reconfigurable optical add-drop multiplexer, ROADM).

Система «Волга»

Единственным российским производителем когерентных систем 100 Гбит/с, удовлетворяющих представленным требованиям, является компания «Т8». Флагманский продукт компании – система «Волга». Сборка системы «Волга» полностью осуществляется в России, из взаимозаменяемых компонентов зарубежных производителей (процессоры, интегральные микросхемы и проч.). Программное обеспечение для системы управления также пишется в России. Система сертифицирована Минсвязи РФ и успешно работает на сетях связи российских операторов связи. Пропускная способность системы «Волга» в существующем сертифицированном исполнении составляет до 9,6 Тбит/с на волокно (96 каналов DWDM по 100 Гбит/с в каждом канале). В 2012 г. этой системой было поставлено два мировых рекорда:

- мировой рекорд по дальности передачи сигнала 100 Гбит/с без компенсации дисперсии и без регенерации (4000 км);
- мировой рекорд по дальности передачи сигнала 100 Гбит/с в однопролётной линии без промежуточных пунктов усиления сигнала, требующих электропитания (500 км).

В настоящее время ведётся работа по увеличению пропускной способности системы «Волга» до 25 Тбит/с. В 2013 г. этот проект был признан лучим российским ИТ проектом в рамках «Сколково Startup Village».

Актуальность внедрения когерентных систем

В обычной системе передачи, приёмник детектирует только амплитуду приходящего оптического сигнала (прямое детектирование). В когерентной системе, приёмник определяет амплитуду, фазу и частоту сигнала (когерентное детектирование). Использование когерентных технологий позволяет не только увеличить скорость в линии, но также отказаться от использования компенсаторов дисперсии, уменьшить число оптических усилителей и пунктов регенерации сигнала, увеличить протяжённость сегментов сети. Это даёт заметную экономию средств и повышает надёжность сети.

Для когерентного детектирования, необходимо на стороне приёмника смешать принятый сигнал с опорным излучением, полученным с локального опорного лазера. Долгие годы эта задача не имела удовлетворительного технического решения для оптических линий связи. Попытки создания аналоговых когерентных систем в начале 1990-х гг. не привели к успеху, и разработки в этой области были надолго приостановлены.

В последние годы (конец 2000-х – начало 2010-х) произошёл настоящий прорыв в разработке цифровых когерентных систем, связанный с появлением высокостабильных узкополосных источников излучения и мощных цифровых сигнальных процессоров (DSP, digital signal processor). Благодаря этому, в мире началась настоящая «когерентная революция», которая позволяет, прежде всего, радикально модернизировать сети дальней связи.

Преимущества когерентных систем

Суть предлагаемого решения состоит в переходе от существующих DWDM систем с каналами 2,5/10/40 Гбит/с к DWDM системам с когерентными каналами 100 Гбит/с с сохранением существующей кабельной инфраструктуры и сохранением расположения пунктов установки оборудования, и с использованием оптических мультиплексоров ROADM для надёжной коммутации каналов без электронных матриц коммутации. Основные преимущества когерентных систем:

- в пять раз повышается пропускная способность магистральной сети;
- на 30% снижается стоимость CAPEX сети (по сравнению с достижением той же ёмкости некогерентными технологиями), настолько же снижается стоимость 1 Гб переданной информации;
- снижается стоимость OPEX – эксплуатационных расходов за счет уменьшения энергопотребления и экономии места в стойках;

• запас по емкости – обеспечивается возможность оперативного и экономичного добавления новых DWDM каналов при развитии сети вплоть до 9,6 Тбит/с с возможным апгрейдом до 25 Тбит/с;

• надёжная коммутация каналов с использованием ROADM, снижение рисков несанкционированного доступа к системе управления.

Существующая конфигурация типовой сети обеспечивает максимальную ёмкость DWDM сети 1,6 Тбит/с по паре волокон (40 каналов по 40 Гбит/с) или стандартную ёмкость 400 Гбит/с (40 каналов по 10 Гбит/с), а на некоторых сегментах – 160 Гбит/с по паре волокон (16 каналов по 10 Гбит/с). Переход к когерентным системам позволяет повысить скорость в канале с 2,5/10/40 Гбит/с до 100 Гбит/с без изменения системных требований к линии, и передавать до 96 каналов по паре волокон в DWDM системе. Таким образом, максимальная ёмкость сети при переходе на когерентную технологию передачи возрастает более чем в 5 раз – до 9,6 Тбит/с.

Переход к когерентным технологиям позволяет не менее чем на 30% снизить затраты на построение магистральной сети. Этот экономический эффект достигается за счёт двух основных факторов.

1. Стоимость транспондера или мукспондера на 100 Гбит/с примерно на 10-15% ниже, чем для 10 каналов по 10 Гбит/с (5 сдвоенных блоков 10G).

2. Отказ от использования компенсаторов дисперсии, уменьшение количества оптических усилителей снижает затраты на построение сети ещё на 10%.

Дополнительная экономия в 5-10% может быть достигнута с учётом косвенного снижения издержек:

3. При отказе от компенсаторов дисперсии, улучшается OSNR и снижаются требования к количеству и мощности усилителей.

4. Сокращается количество мультиплексоров на линии, в расчёте на 1 Гб передаваемой информации.

5. Снижаются операционные расходы на обслуживание сети за счёт снижения количества транспондеров, экономии места в стойках и сокращения потребления электричества.

Исключительные технические характеристики предлагаемого оборудования позволяют увеличить скорость передачи в канале с 10 до 100 Гбит/с без замены существующего волокна и пунктов обслуживания. В системе «Волга» для работы на скорости 100 Гбит/с требуется OSNR всего 12,5 дБ (при BER=10^{-12}). Примерно только же требуется некогерентным системам предыдущего поколения для работы на скорости 2,5G без FEC и 10 Гбит/с со стандартным FEC. Таким образом, канал 100 Гбит/с будет работать на той же кабельной инфраструктуре, на которой сейчас работают каналы 2,5/10/40 Гбит/с.

Дальность работы когерентных систем передачи без регенерации сигнала, на каскаде оптических усилителей, может составлять тысячи километров, что является важнейшим отличием от некогерентных систем. При развитии сети можно добавлять новые магистральные каналы DWDM без замены усилителей на линии, что многократно снижает стоимость добавления новых каналов. Например, для добавления нового канала 100 Гбит/с «Санкт-Петербург - Архангельск» достаточно будет установить два транспондера в конечных точках канала. Замена усилителей на линии при этом не потребуется.

Современные высокоскоростные сети связи имеют сложную архитектуру с большим трафиком, с большим количеством каналов DWDM и подключенных клиентов. Для того, чтобы упростить администрирование таких сетей, применяются оптические мультиплексоры ROADM. Однако они вносят дополнительный шум (cross-talk) в каналы связи. Поэтому для их гибкого применения необходим дополнительный запас по OSNR. Когерентные технологии обеспечивают больший запас по OSNR, по сравнению с некогерентными системами, и позволяют широко применять ROADM.

Перестраиваемый оптический мультиплексор ввода-вывода каналов (reconfigurable optical add-drop multiplexer, ROADM) позволяет гибко изменять число выводимых каналов из спектра DWDM без перерыва трафика независимо от сложности сети. Устройство производит селективное мультиплексирование для организации выделения оптических каналов в сетке DWDM с шагом 50 ГГц или 100 ГГц в промежуточных пунктах двунаправленной линии связи. Управление модулем осуществляется при помощи системы управления шасси. Благодаря использованию ROADM, можно легко пробрасывать через сеть DWDM новые клиентские маршруты.

В сложных MESH сетях технология ROADM может не только использоваться для быстрого проброса клиентских интерфейсов, но и позволяет реализовать эффективное резервирование линий связи с гибким выбором путей резервирования. Время переключения на резервный канал 100 Гбит/с составляет 20 миллисекунд.

Заключение

Переход к когерентным каналам 100 Гбит/с позволяет эффективно модернизировать волоконно-оптическую сеть связи с сохранением существующей кабельной инфраструктуры. Применение когерентных технологий обеспечивают экономию до 30% по сравнению с аналогичной сетью на некогерентных системах. Оборудования российского производства «Волга» обеспечивает построение сетей с высокой пропускной способностью, надёжным резервированием трафика, устойчивой системой управления, — в том числе, в интересах спецпользователей.

С.С. Махров
Аспирант, Московский технический университет связи и информатики, г. Москва

БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИ В ВОЕННО-ТАКТИЧЕСКИХ ЗАДАЧАХ

Введение

Беспроводная сенсорная сеть (БСС) - это множество самоорганизующихся беспроводных узлов, имеющих датчики, и объединенных посредством радиоканала. Узлы являются автономными в отношении электропитания, которое ограничено встроенными в каждый узел источниками энергии. Основной целью такой сети является измерение физических параметров из внешней среды. Но БСС могут служить не только средствами мониторинга, но и контроля. Данные, собранные узлами сети, передаются на базовую станцию (БС), в качестве которой может выступать любое устройство с

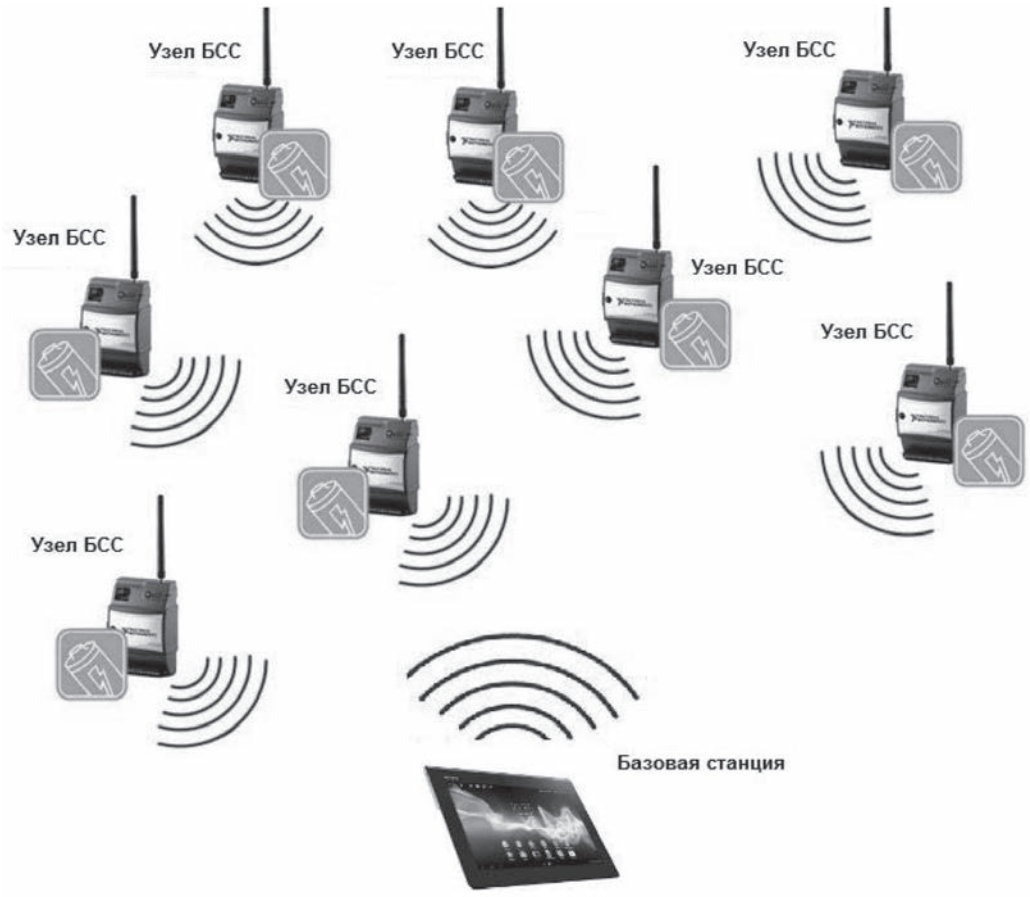


Рис. 1. Беспроводная сенсорная сеть

приёмопередатчиком, процессором, устройством памяти, средствами управления и отображения, например, персональный компьютер или планшет (рис. 1). БСС имеют множество сфер применения, одной из которых является военная сфера[1].

Современные достижения в области нанотехнологий, микро-электро-механических систем (MEMS), радиотехники, цифровой электроники, цифровой обработки сигналов и беспроводных сетей позволяют создавать миниатюрные и интеллектуальные датчики. Миниатюризация позволяет расширять возможности применения и интеграции БСС.

Таким образом, БСС представляют собой некоторое множество беспроводных сенсоров (в зависимости от задачи), которые могут быть дислоцированы в целевую область для осуществления её мониторинга и контроля. Задача мониторинга и контроля является достаточно актуальной для военной сферы.

Военное применение сенсорных сетей

Военный аспект применения сенсорных сетей ставит перед разработчиками широкий круг задач, начиная от мониторинга периметра базы и заканчивая поддержкой боевых единиц при выполнении тактических задач.

Можно выделить следующие основные задачи военного применения, которые могут быть решены с помощью БСС:

- мониторинг периметра базы;
- защита объекта (мониторинг очищенных локаций от новых вторжений противника, ключевых точек, дорог);
- разведка;
- шпионаж;
- обнаружение и локализация снайперов;
- химическая диагностика;
- бактериологическая диагностика;
- ядерная и радиационная диагностика;
- передача данных между наземными, воздушными и морскими силами.

Рассмотрим задачу мониторинга периметра базы. После того как она будет развернута в зоне боевых действий, необходимо иметь возможность предупредить нападения врага. Окружающий ландшафт может быть волнистым или гористым, а также может иметь преграды в виде деревьев и растительности. Атака может прийти в виде пеших групп боевых единиц или на транспорте. В целях облегчения раннего выявления, охраны периметра (рис. 2), БСС должна охватывать пе-

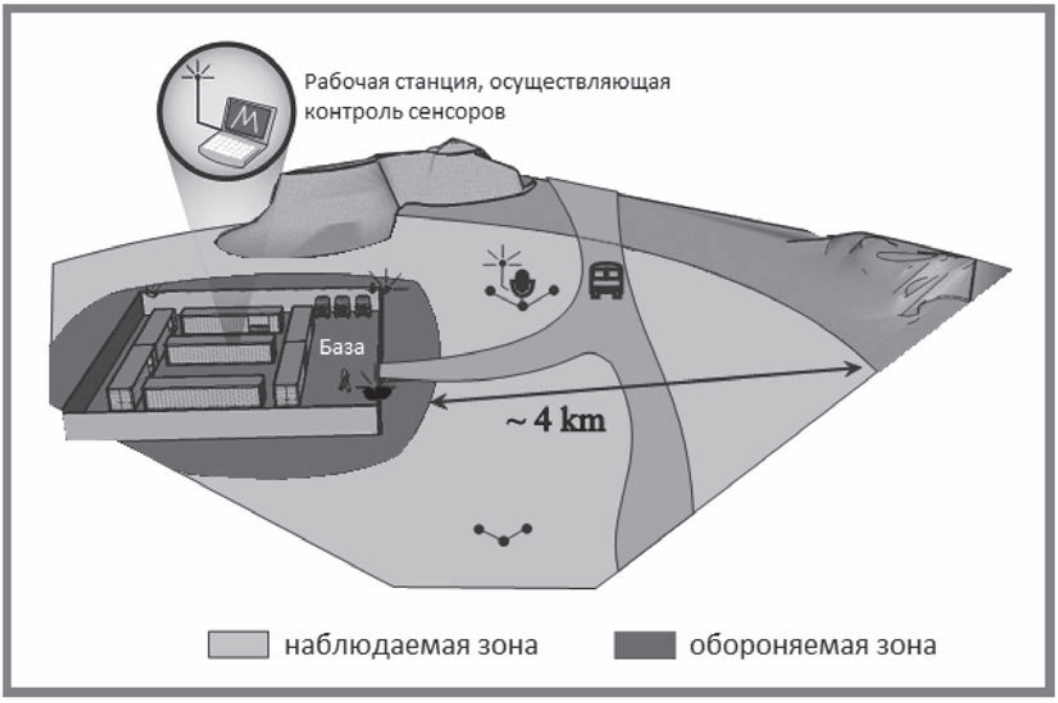


Рис. 2. БСС защищает периметр базы путем обнаружения вторжений

риметр вокруг базы радиусом до 4 км, в то время как на практике требуется такая дальность как до 10 км. Обнаружение может быть необходимо именно на такой дальности, в то время как конкретная идентификация типов объектов необходима на расстоянии 1-2 км вокруг базы.

БСС для определения вторжения врага могут использовать различные типы сенсоров:

- акустические;
- сейсмические;
- магнитные;
- инфракрасные;
- электро-оптические;
- электромагнитные.

Значительные усилия необходимы для правильной интеграции сенсоров в крупномасштабные сенсорные сети, и одной из самых сложных задач является повышение точности сенсоров в поддержании минимального уровня ложных срабатываний. Необходимость надежного обнаружения приводит к использованию мультимодальных сенсоров. Разумное сочетание сенсоров и их точностей в будущем обеспечат надежные программно-аппаратные комплексы. Кроме того, использование мультимодальных сенсоров может свести к минимуму потребление энергии, а также генерацию трафика, например, если видеокамера включается по срабатыванию акустических или инфракрасных сенсоров[2].

При использовании БСС для определения вторжения вражеских боевых единиц в заданную зону, возможно также определения типов боевых единиц, путем анализа данных сенсора. Например, если используется акустический сенсор, то здесь необходимо производить спектральный анализ звука и сравнивать измеренные значения с типовыми для каждого заранее заданного типа боевой единиц (танк, пехота, вертолет, самолет).

Благодаря миниатюрным размерам, сенсорные узлы будут достаточно скрытным и удобным в дислокации средством мониторинга[3,4].

Одними из способов дислокации сенсорных узлов в целевую область являются:

- ручная установка узлов путем разбрасывания;
- жесткий монтаж к поверхности;
- авиация;
- использование в качестве снаряда.

Требования безопасности к военным БСС

Применение БСС в военных условиях, выставляет соответствующие требования к проектированию таких сетей и всех сопутствующих компонентов. БСС должна отвечать следующим требованиям информационной безопасности:

Защита от прослушивания - враг может перехватить и декодировать сообщения, циркулирующие между узлами сети. Для предотвращения прослушивания необходимо стойкое шифрование передаваемых данных.

Защита от спуфинга - враг может свой узел выдать в качестве санкционированного узла сети и тем самым произвести диверсию. Соответственно, необходимо использование механизмов аутентификации узлов в сети.

Защита целостности данных - способность сообщений, циркулирующих между узлами, оставаться без изменения и модификаций в течении всего продвижения по сети. На протяжении всего пути, по которому следует пакет, маршрут также должен оставаться неизменным. Криптографическая защита и мощная проверка целостности (например, MD5 Hash, SHA) могут обеспечить надежную защиту от фальсификации сообщений и атак воспроизведения.

Защита от отказа в обслуживании - предотвращение создания условий, при которых узлы не могут получить доступ и использовать сеть для передачи сообщений.

Защита от геолокационного обнаружения - враг может определить местонахождение географического положения узлов сенсорной сети путем обнаружения излучений устройств. Сокращение частоты и продолжительности передачи данных до абсолютного минимума и продолжительности уменьшит шанс того, что сеть будет обнаружена. Тем не менее, всегда будет вероятность обнаружения, особенно, если противник знает, что в данной области располагается сенсорная сеть.

Защита физических компонентов - враг может извлечь собранные данные из сенсорного узла, механически вскрыв его корпус. Необходимо использование корпусов с особой технологией демонтирования креплений, без знания которой критически повреждаются элементы памяти и не подлежат восстановлению.

Сопротивление условиям внешней среды – корпус сенсорного узла должен быть защищен от различного рода воздействий окружающей среды: температура, помехи, вода и .т.д[5].

Заключение

Беспроводные сенсорные сети являются превосходным инструментом, который может использоваться в военно-тактических задачах. Создание миниатюрных беспроводных узлов, отвечающих требованиям информационной безопасности, функционирующих под управлением соответствующего энергосберегающего протокола, позволит строить эффективные системы защиты, мониторинга, контроля и исследования целевых областей.

В данной работе произведен анализ возможностей и способов применения БСС в военной сфере, которые накладывают в свою очередь ряд требований. Проектирование таких сетей в свою очередь должно производиться с их учетом.

СПИСОК ЛИТЕРАТУРЫ

1) Dargie, W. and Poellabauer, C., «Fundamentals of wireless sensor networks: theory and practice», John Wiley and Sons, 2010 ISBN 978-0-470-99765-9, pp. 168–183, 191–192

2) Kushwaha, M., Amundson, I., Volgyesi, P., Ahammad, P., Simon, G., Koutsoukos, X., Ledeczi, A., Sastry, S. 2008. Multi-modal target tracking using heterogeneous sensor networks. In: Proc. of ICCCN.

3) Alhmiedat, T., and Yang, S 2007. A Survey: Localization and Tracking Mobile Targets through Wireless Sensor Network, PGNet International Conference, ISBN: 1-9025-6016-7.

4) Meesookho, C., and Mitra, U. 2008. On energy-based acoustic source localization for sensor networks, IEEE Trans. Signal Process., vol. 56, no. 1, pp. 365–377.

5) Capkun, S., Hubaux, J.P.: Secure positioning of wireless devices with application to sensornetworks. In: Proceedings of IEEE INFOCOM (2005)

А.А. Миняев
научный сотрудник, к.т.н.

К.Г. Масленников
научный сотрудник

С.В. Морковин
научный сотрудник,
Академия ФСО России, г. Орел.

ПОСТАНОВКА ЗАДАЧИ НА РАЗРАБОТКУ МЕТОДА ОБРАБОТКИ ВИДЕОДАННЫХ В СИСТЕМАХ МОНИТОРИНГА КАНАЛОВ СВЯЗИ

В последнее время лидирующие позиции в общем объеме трафика телекоммуникационных систем занимают данные различных систем медиавещения. После прохождения процедур устранения избыточности и упаковки в контейнеры сетевых протоков эти данные имеют строго определенную структуру, существенно неустойчивую к воздействию ошибок в канале связи. Последствия ошибок могут иметь как локальный характер, так и приводить к полной невозможности корректного декодирования видеоданных. Существующие методы восстановления искаженных видеоданных ориентированы на узкий круг критических ситуаций и не могут быть в полной мере применены для решения задач обработки видеоданных в системах мониторинга каналов связи. В частности, существующие методы не учитываю типичную для современных телекоммуникационных систем ситуацию трансляции данных по различным физическим каналам и невозможности наблюдения всей совокупности физических каналов в системах мониторинга. Это приводит к необходимости разработки и реализации в современных системах мониторинга каналов связи методов и алгоритмов обработки видеоданных в условиях их искажения. В статье рассматривается поставка задачи обработки искаженных видеоданных применительно к условиям функционирования систем мониторинга каналов связи. Сформулированы существующее противоречие, научная проблема и гипотеза исследования.

Ключевые слова: видеосжатие, видеокодирование, *агрегация каналов, маскирование искажений,* медиавещание.

Трансляция видеоданных в современных системах связи описывается общей моделью системы передачи информации, одним из основных элементов которой является кодер источника сообщений (рис. 1):

Основная цель кодера – сокращение избыточности видеоданных (т.е. сжатие видеоданных) на основе учета внутрикадровой и межкадровой корреляции подвижных изображений. Этапы сжатия видеоданных представлены на рисунке 2:

При этом, отправляемая в канал последовательность кадров подвижного изображения имеет строго определенную структуру (рис 3). Первым в последовательности следует так называемый опорный кадр, при сжатии которого используется информация только из пространственной области этого кадра. Кодирование всех последующих кадров (вплоть до следующего опорного) производится относительно предыдущего и последующего кадров на основе учета разницы между предсказанными и действительными коэффициентами векторов движения объектов на кодируемой графической сцене.

Рассматриваемая структура последовательности позволяет достичь существенных коэффициентов сжатия видеоданных, но обладает неустойчивостью к ошибкам в канале связи. Искажение единичного элемента кадра приво-

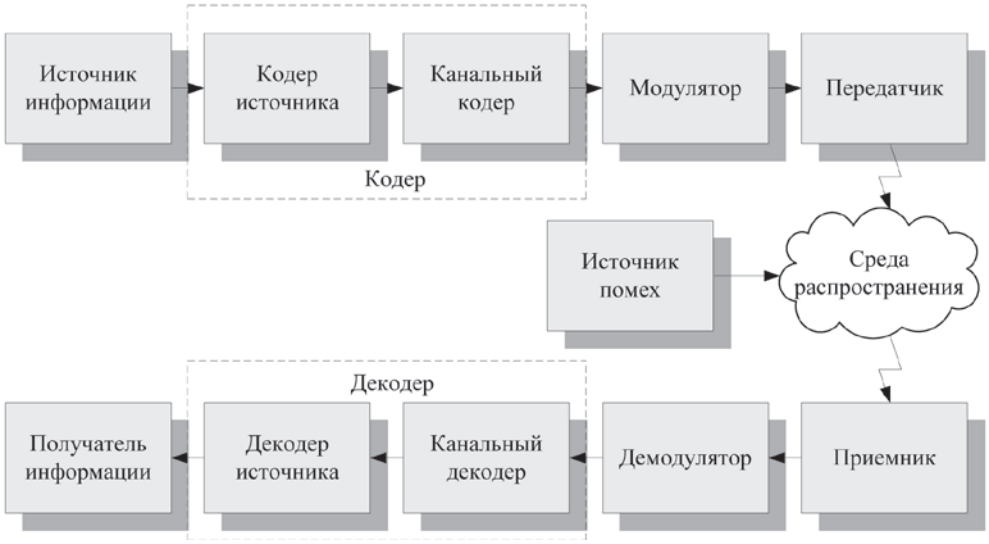


Рис. 1. Модель системы передачи информации

Рис. 2. Этапы сжатия подвижных изображений

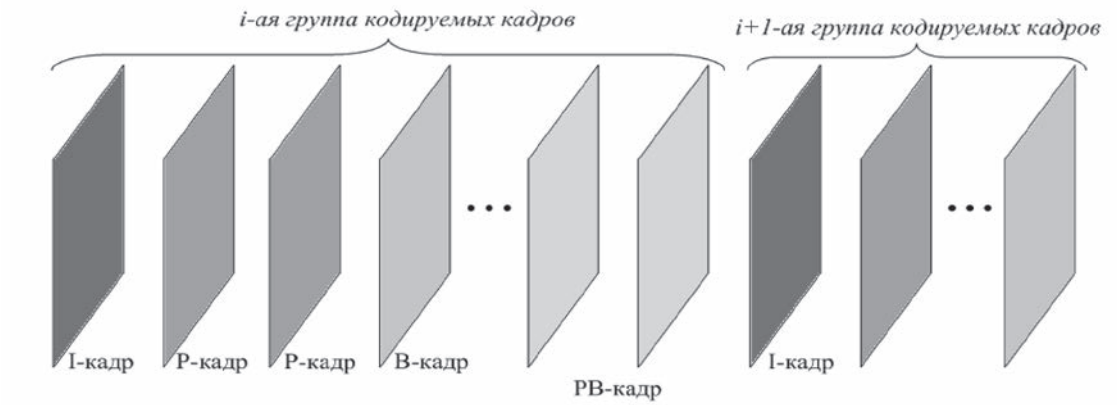


Рис. 3. Разбиение кадров подвижного изображения по типам

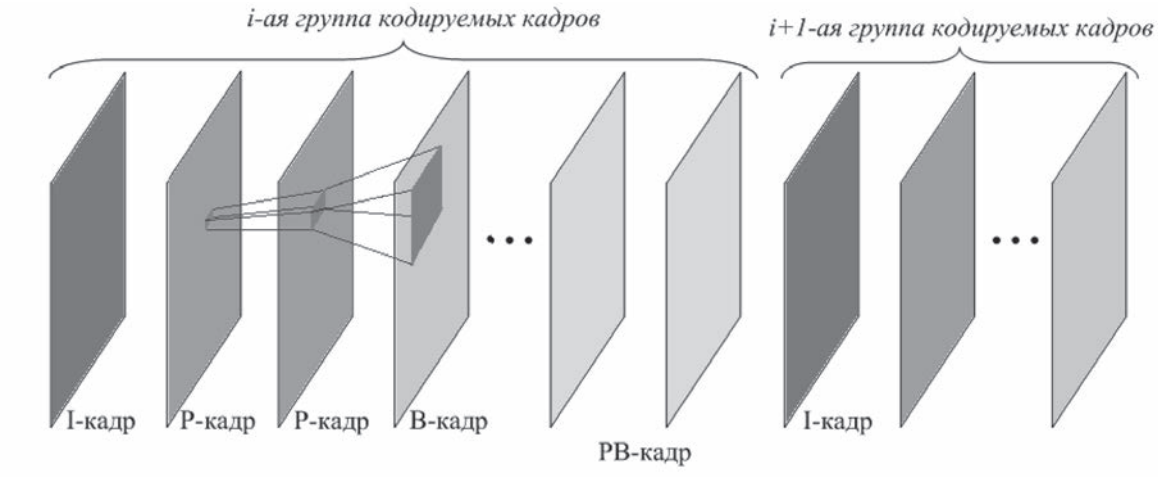


Рис. 4. Распространение единичной ошибки в зависимых кадрах

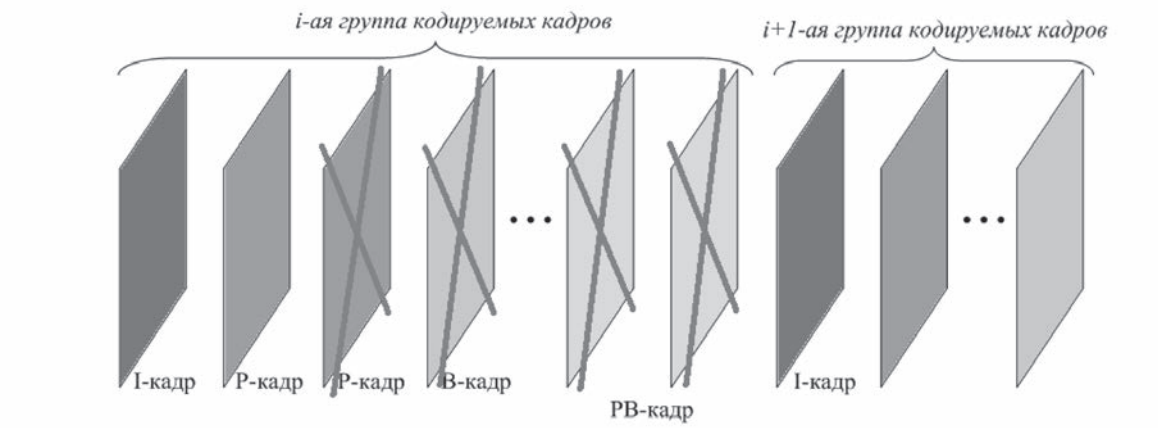


Рис. 5. Распространение единичной ошибки, связанной с потерей промежуточного кадра

дит к искажению всех зависимых от него элементов в последующих кадрах – т.е. к распространению ошибки (рис. 4).

А потеря целого кадра приводит к сбою в работе декодера и невозможности восстановления видеоданных вплоть до следующего опорного кадра (рис. 5).

Классификация известных подходов к восстановлению искаженных видеоданных представлена на рисунке 6. Группы **традиционных для систем передачи данных методов** и методов, относящихся к классу **кодирование, устойчивое к ошибкам,** основываются на специальных правилах организации канала связи и не могут быть применены при проектировании систем мониторинга.

Методы **маскирования искажений** восстанавливают только ограниченные области искаженного кадра и применяются при воздействии одиночных или локализованных групповых ошибок.

Однако, анализ условий функционирования систем мониторинга показывает, что современные системы ПДПК зачастую строятся на **принципах агрегации каналов,** когда данные могут быть переданы по разным **физическим** каналам. При этом, в случае наблюдения в системе мониторинга не всей совокупности физических каналов (рис. 7), корректное декодирование видеоданных становится невозможным.

Таким образов, возникает **Противоречие** между применением в зарубежных системах передачи информации процедур сокращения избыточности (сжатия) видеоданных и отсутствием в системе мониторинга методов их корректной обработки. Разрешение противоречия требует проведения исследования по разработке

Рис. 6. Методы борьбы с искажениями видеоданных

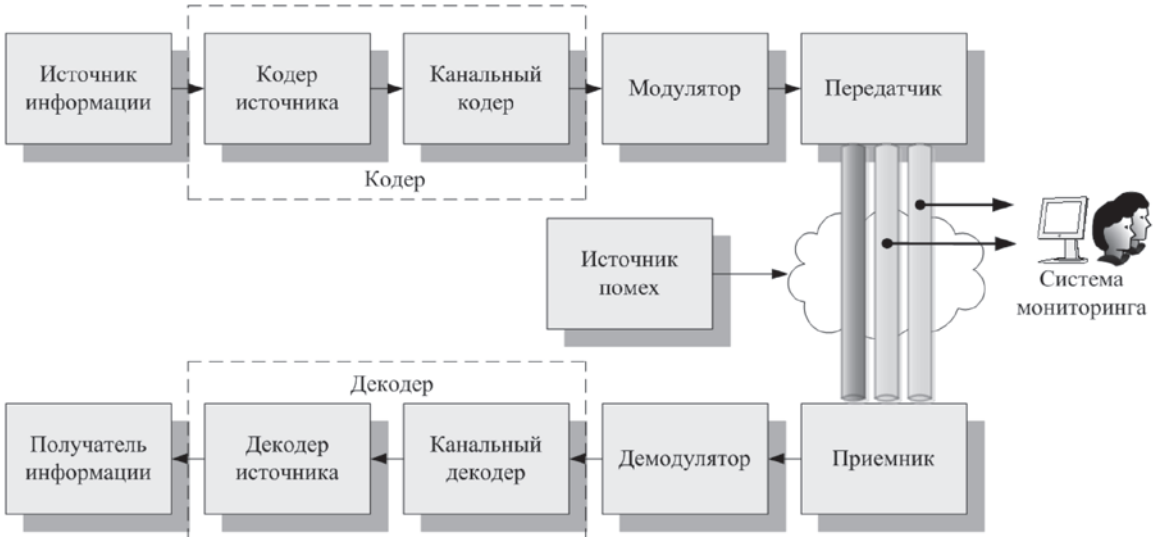


Рис. 7. Модель наблюдения системы передачи информации с агрегацией каналов в системе мониторинга

теоретических основ обработки видеоданных применительно к условиям функционирования систем мониторинга.

Научная проблема исследования: разработка теоретических основ обработки видеоданных применительно к системам мониторинга каналов связи.

Решение научной проблемы возможно путем выдвижения гипотезы о существовании взаимосвязей (корреляций) между параметрами и элементами неискаженных и искаженных (отсутствующих) кодовых слов, позволяющих выполнить восстановление синхронизации видеодекодера без участия следующего опорного кадра.

Формализованная постановка задачи исследования представлена на рисунке 8.

Исходные данные:

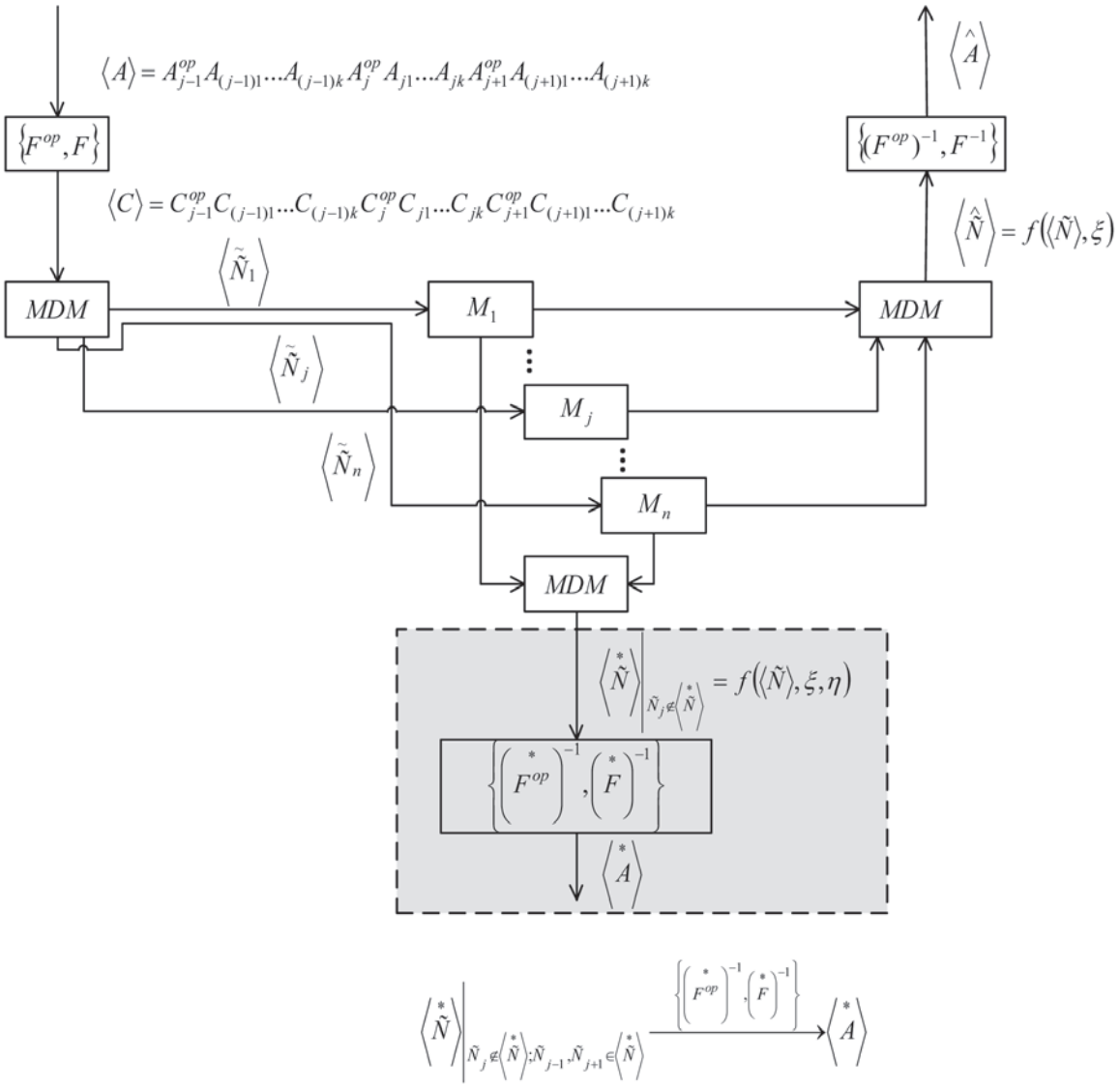


Рис. 8. Постановка задачи исследования

1 . $\langle A\rangle = A^{op}_{j-1}A_{(j-1)1}...A_{(j-1)k}A^{op}_{j}A_{j1}...A_{jk}A^{op}_{j+1}A_{(j+1)1}...A_{(j+1)k}$ – исходные видеоданные (последовательность подвижных изображений), поступающие на вход системы передачи информации от источника видеоданных.

2. $\langle C\rangle = C^{op}_{j-1}C_{(j-1)1}...C_{(j-1)k}C^{op}_{j}C_{j1}...C_{jk}C^{op}_{j+1}C_{(j+1)1}...C_{(j+1)k}$ – переданная в канал связи последовательность кодовых слов $\langle C\rangle$, полученная в результате применения комплекса $\{F^{op},F\}$ операторов устранения избыточности исходных видеоданных $\langle A\rangle$, где:

– F^{op} – оператор обработки опорного кодового слова;

– F – оператор обработки промежуточных кодовых слов;

3. $\left\langle \overset{*}{C}\right\rangle\Big|_{C_j\notin\left\langle \overset{*}{C}\right\rangle} = f(\langle C\rangle,\xi,\eta)$ – поступившая на вход СРР неполная последовательность кодовых слов, подверженная действию шумов канала связи – η, и особенностям организации канала связи – ξ;

4. Особенности организации канала связи ξ заключаются в использовании нескольких независимых физических каналов, образующих связанную логическую группу передачи последовательности кодовых слов $\left\{\left\langle \tilde{C}_1\right\rangle,...,\left\langle \tilde{C}_j\right\rangle,...,\left\langle \tilde{C}_n\right\rangle\right\}$.

Необходимо:

1. Разработать комплекс операторов $\left\{\left(\overset{*}{F^{op}}\right)^{-1},\left(\overset{*}{F}\right)^{-1}\right\}$ обеспечивающих обработку и восстановление искаженных видеоданных

$$\left\langle \overset{*}{C}\right\rangle\Big|_{C_j\notin\left\langle \overset{*}{C}\right\rangle;C_{j-1},C_{j+1}\in\left\langle \overset{*}{C}\right\rangle}\xrightarrow{\left\{\left(\overset{*}{F^{op}}\right)^{-1},\left(\overset{*}{F}\right)^{-1}\right\}}\left\langle \overset{*}{A}\right\rangle$$

при ведении РР;

Требования к комплексу операторов:

1. Время обработки одного объекта $\left\langle \overset{*}{C}\right\rangle$ не превышает требуемого значения $T_{обр}\to T_{обр}^{TP}$.

Ограничения и допущения:

1. Характер воздействия канала связи $\left\langle \overset{*}{C}\right\rangle=f\left(\langle C\rangle,\xi,\eta\right)$ ограничивается отсутствием искажений двух подряд идущих кодовых слов $\left\langle \overset{*}{C}\right\rangle\Big|_{C_j\notin\left\langle \overset{*}{C}\right\rangle;C_{j-1},C_{j+1}\in\left\langle \overset{*}{C}\right\rangle}$

Заключение

В статье рассмотрена типичная для систем мониторинга каналов связи критическая ситуация наблюдения неполной группы физических каналов, приводящая к невозможности корректного декодирования видеоданных. Выявлено противоречие, сформулирована научная проблема и поставлена задача на проведение исследования, направленного на решение этой проблемы.

СПИСОК ЛИТЕРАТУРЫ

1. Ян Ричадсон. Видеокодирование H.264 и MPEG-4 - стандарты нового поколения. Техносфера, 2005. - с.47-112.

2. ITU-T recommendation by standard of joint video specification (ITU-T Rec. H.264/ISO/IEC 14 496-10 AVC). Joint Video Team (JVT) of ISO/IEC MPEG and ITU-T VCEG, JVTG050, 2003.

3. M. Oliveira, B. Bowen. Fast digital image inpainting. Proc. International Conf. on Visualization, Imaging and Image Processing – Marbella, Spain, 2001. – Pp. 161-232.

4. Lin Liang, Ce Liu. Real-time texture synthesis by paych-based sampling. ACM Trans. Graph. – 2001. – July. Vol. 20, no. 3. – Pp. 67-152.

5. M. Bertalmio, L. Vese. Simultaneous structure and texture image inpainting. Image Processing, IEEE Transactions on. – 200. – Vol. 12, no. 8. – Pp. 882-889.

В.И. Мирошников
доктор техничеких наук
К.З. Билятдинов
кандидат военных наук
А.Г. Фортинский
кандидат технических наук

ПОВЫШЕНИЕ КАЧЕСТВА УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

Рассмотрены общие вопросы повышения качества управленческих решений. Описаны основные показатели и формулы, применимые для оценки качества решений. Определены возможные направления и методы повышения качества управленческих решений.

Ключевые слова: система, управление, качество, решение, оценка.

Управление любой системой предусматривает принятие управленческих решений. От качества этих решений зависит степень достижения цели функционирования системы.

Таким образом, повышение качества управленческих решений является одной из актуальных задач в процессе управления.

Любое решение направлено на достижение определенной цели. Оно обеспечивает некоторый полезный эффект, связанный, в свою очередь, с затратами. Сопоставление полезного эффекта с затратами на его получение позволяет судить о качестве решения. [3, С.151]

Поэтому наиболее распространенный показатель качества решений — интегральный, составленный как отношение полезного эффекта (Э) к суммарным затратам на его получение (З). Он называется целевой функцией:

$$Ц = \frac{Э}{З}. \qquad (1)$$

Естественно, что решение, максимизирующее целевую функцию, является наилучшим по критерию оптимальности (2).

$$Ц = \frac{Э}{З} = \max \qquad (2)$$

Синтез оптимального решения по критерию максимума целевой функции (2) предполагает две возможности.

Первая из них состоит в выяснении условий, максимизирующих полезный эффект при фиксированных затратах. Вторая сводится к минимизации затрат, обеспечивающих один и тот же полезный эффект. Таким образом, критерий (2) распадается на два частных критерия, которым удовлетворяют два разных решения (3) и (4):

$$Ц_1 = \frac{Э = \max}{З = const} \qquad (3)$$

$$Ц_2 = \frac{Э = const}{З = \min} \qquad (4)$$

Если есть выбор, то в качестве оптимального выбирают решение, обеспечивающее большее значение целевой функции.

Разнообразие практических задач и множество подходов к их решению не позволяет далее рассматривать этот вопрос с позиций общей теории. В каждом конкретном случае разрабатывается частная методика синтеза оптимального решения по критерию максимума целевой функции. [3, С.151]

В общем случае направления повышения качества управленческих решения можно выбрать на основе улучшения наиболее значимых показателей качества управления.

В нашей работе такими основными показателями будут являться:

1) Степень достижения цели функционирования системы, вследствие выполнения оцениваемого управленческого решения.

2) Количество затраченных ресурсов на принятие и выполнение оцениваемого управленческого решения.

3) Количество времени, затраченного на принятие и выполнение оцениваемого управленческого решения.

Степень достижения цели функционирования для сложных организационно-технических систем можно выразить количественно в виде комплексного показателя, учитывающего все важные частные показатели (5).

В результате, можно обоснованно оценить степень достижения цели функционирования для сложных организационно-технических систем:

$$Q_j = \sum_{l=1}^{n} q_j g_l \qquad (5)$$

где Q_j – комплексная оценка степени достижения цели; q_j – выбранный частный показатель для оценки; g_j – нормированный весовой коэффициент этого показателя.

Количественное значение нормированного весового коэффициента (g_j) может быть определено с помощью:

1) установления приоритетов выполняемых системой задач, необходимых для достижения требуемой цели;

2) на основе учета мнений компетентных должностных лиц (экспертов).

В первом случае g_j может быть определено на основе статистических данных о функционировании системы, с помощью которых можно сделать выводы о том какие частные задачи наиболее важны для достижения требуемой цели.

Во втором случае можно использовать формулу (6), при условии сравнительно одинаковой компетенции должностных лиц (экспертов), то есть при равных значений весовых коэффициентов должностных лиц (экспертов):

$$g_i = \sum_{j=1}^{m} r_{ij} \Big/ \sum_{i=1}^{n} R_i \ , \qquad (6)$$

В формуле (6) в числителе – сумма оценок, проставленная i-тому показателю всеми m – должностными лицами (экспертами), а в знаменателе – общая сумма оценок, проставленная m экспертами всем n– показателям (r_{ij} – оценка, проставленный j-м экспертом i-тому показателю).

Если определено, что при любом оцениваемом решении цель достигается, то для последующей оценки качества этих решений используют только количество затраченных ресурсов и времени.

При расчете количества затраченных ресурсов на принятие и выполнение оцениваемого управленческого решения необходимо понимать, что такие ресурсы, включают в себя долговременные и преобразуемые ресурсы.

Долговременные ресурсы (или ресурсы длительного пользования): люди (личный состав, персонал, работники), технические устройства, программное обеспечение, методы достижения цели (работы), здания и сооружения.

Преобразуемые ресурсы: финансовые и материальные ресурсы, электрическая энергия, горюче-смазочные материалы, расходные материалы и комплектующие, запасные инструменты и принадлежности т.п.

Разделение ресурсов на долговременные и преобразуемые важно для упрощения оценки управленческих решений и в последующем для повышения качества этих управленческих решений.

Так если при выполнении разных решений, направленных на достижение одной и той же цели, использовались одни и те же долговременные ресурсы (то есть количество личного состава (персонала), аппаратуры, транспортных средств, одни и те же здания и сооружения), то при последующем сравнении этих решений долговременные ресурсы можно принять за постоянную величину. И в последующих расчетах учитывать только затраченные преобразуемые ресурсы.

При расчете времени (Т) целесообразно учитывать количество времени, непосредственно

затраченное с момента получения приказа (распоряжения) от вышестоящей системы (органа управления) до момента его выполнения и (или) получения вышестоящей системой доклада о выполнении этого приказа (7):

$$T = t_{си} + t_{пр} + t_{вр} + t_{д} \qquad (7)$$

где: $t_{си}$ – количество времени, затраченное на сбор исходных данных и оценку обстановки; – количество времени, затраченное непосредственное на принятие оцениваемого управленческого решения; $t_{вр}$ – количество времени, необходимое для выполнения решения; $t_{д}$ – количество времени на доклад в вышестоящую систему о выполнении решения (достижения цели).

Таким образом, задача повышения качества управленческих решений сводится к улучшению значений трех вышеперечисленных показателей, а именно: повышение степени достижения цели, уменьшение количества затраченных ресурсов, уменьшение времени на принятие решения и его выполнение.

Данную задачу целесообразно комплексно решать в процессе подготовки и принятия управленческого решения на организационном и техническом уровнях.

Организационный уровень предусматривает регламентацию процесса принятия решения и установление приоритетов с целью повышения качества управления. На техническом уровне происходит применение технических устройств (программно-аппаратных средств) с той же целью.

В процессе повышения качества управленческих решений важную роль могут играть статистические методы. В особенности, когда необходим анализ выборки данных и (или) массивов информации и (или) информация о состоянии системы неполная для принятия обоснованного решения.

Кроме того статистические методы для обоснования решений руководителя могут эффективно применятся, когда другие методы, например: экспертные оценки, не дают необходимых результатов и (или) их выводы расплывчаты и требуют дальнейшей проверки. Например: одним из статистических методов, используемым при этом могут быть контрольные карты. При практическом использовании контрольных карт целесообразно руководствоваться соответствующими стандартами, например:

– ГОСТ Р 50779.40-96 (ИСО 7870-93) Статистические методы. Контрольные карты. Общее руководство и введение;

– ГОСТ Р 50779.42-99 (ИСО 8258-91) Статистические методы. Контрольные карты Шухарта;

– ГОСТ Р 51814.3-2001 Методы статистического управления процессами. [4]

Если для повышения качества управленческих решений надо решить задачу обоснованного выбора из множества альтернатив или выборок статистических данных, то возникает необходимость сопоставления двух (или более) рядов выборочных значений по частоте встречаемости какого-либо признака. В этом случае считается рациональным выбор и применение многофункциональных непараметрических статистических критериев, которые помогут решить эту задачу по отношению к самым разнообразным данным, выборкам и задачам, что существенно повысит обоснованность решений. [2, С.204]

Однако в некоторых случаях необходимо принимать сложные решения в условиях недостаточно высокого качества и количества имеющейся информации (исходных данных). Основные трудности, возникающие при принятии таких сложных решений, можно подразделить на пять групп:

Во-первых, исходная статистическая информация зачастую бывает недостаточно достоверной.

Однако даже при наличии достоверных данных о прошлом они не всегда могут служить надежной базой для принятия решений, направленных в будущее, поскольку существующие условия и обстоятельства могут в дальнейшем измениться.

Во-вторых, некоторая часть информации имеет качественный характер и не поддается количественной оценке.

В-третьих, в практике подготовки решений часто возникают ситуации, когда в принципе необходимую информацию получить можно, однако в момент принятия решения она отсутствует, поскольку это связано с большими затратами времени или средств.

В-четвертых, существует большая группа факторов, которые могут повлиять на реали-

зацию решения в будущем, но их нельзя точно предсказать.

В-пятых, одна из наиболее существенных трудностей при выборе решений состоит в том, что любая научная или техническая идея содержит в себе потенциальную возможность различных схем ее реализации, а любое действие может приводить к многочисленным исходам. [1, С.4]

Проблема выбора наилучшего варианта решения может возникнуть и потому, что обычно существуют ограничения в ресурсах, а следовательно принятие одного варианта всегда связано с отказом от других (нередко достаточно эффективных) решений.

И наконец, при выборе наилучшего решения мы нередко сталкиваемся с многозначностью обобщенного критерия, на основе которого можно произвести сравнение возможных исходов. Многозначность, многомерность и качественное различие показателей является серьезным препятствием для получения обобщенной оценки относительной эффективности, важности, ценности или полезности каждого из возможных решений. [1, С.5].

При вышеназванных условиях для повышения качества сложных управленческих решений целесообразно применять метод групповых экспертных оценок.

Сегодня экономия ресурсов и времени на достижение цели становится все более важной задачей управления, но качество управленческого решения в первую очередь должно влиять на степень достижения цели.

Таким образом, повышение качества управленческих решений представляет собой постоянную деятельность должностных лиц, направленную на повышение степени достижения цели при условии уменьшения расхода ресурсов и времени. При этом целенаправленная деятельность по повышение качества управленческих решений требует специальной организации и оценки результатов этой деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Билятдинов К.З. Обоснование выбора метода групповых экспертных оценок... // Деп. в ЦВНИ МО РФ. Инв. № В6879. Справка №15966, Серия Б. Вып. № 84. М., 2008.

2. Билятдинов К.З., Кривчун Е.А. Обоснование выбора при контроле изделий // European Applied Sciences, November-December, 2012, 1 (2) – pp. 204-206.

3. Станякин В.М., Шишкин И. В. Квалиметрия и управление качеством – М.: ВЗПИ, 1992, 159с.

4. http://www.standard.ru/.

Р.Л. Михайлов
Военно-космическая академия **имени А.Ф.Можайского**

Е.С. Владимиров
Военная академия Министерства обороны (филиал, г. Череповец)

МЕТОДИКА ОБОСНОВАНИЯ ПОКАЗАТЕЛЯ УСТОЙЧИВОСТИ СВЯЗИ

В статье рассмотрены понятие устойчивости связи и методика ее оценки. Дано определение устойчивости связи согласно руководящих документов. Проведен анализ исследований в данной области, систематизированы различные подходы к расчету показателя устойчивости связи. Обоснован выбор показателя устойчивости связи и обоснована методика его расчета.

Введение

Актуальность вопросов повышения устойчивости связи обусловлена все более возрастающими требованиями к качеству обслуживания, предъявляемыми к современным сетям связи (СС), в условиях функционирования их в неблагоприятной среде.

Под устойчивостью связи, согласно ГОСТ [1], понимается способность СС выполнять свои функции при выходе из строя части ее элементов в результате воздействия дестабилизирующих факторов.

Дестабилизирующими факторами (ДФ) являются воздействия на СС, источником которых является физический или технологический процесс внутреннего или внешнего характера, приводящие к выходу из строя элементов СС [1]. В соответствии с этим различают:

– внутренние ДФ;

– внешние ДФ.

При этом способность СС противостоять внутренним ДФ определяет свойство ее надежности, а способность противостоять внешним ДФ свойство живучести [1].

Показатели устойчивости в общем виде

В соответствии с действующим в настоящее время ГОСТом [1] показателем устойчивости СС является значение вероятности связности информационного направления связи (ИНС), под которым понимается вероятность того, что на заданном направлении существует хотя бы один путь, по которому возможна передача информации с требуемым качеством (QoS – Quality of Service – качество обслуживания) и объемом:

$$P_{св} = P\left(l \geq 1 \middle| \{Q_l\} \in \left\{Q^{треб}\right\}\right), \qquad (1)$$

где $P_{св}$ – показатель вероятности связности ИНС, l – количество работоспособных путей на заданном ИНС, Q_l – качество обслуживания, обеспечиваемое путями (путем) на заданном ИНС, $Q^{треб}$ – требуемый уровень качества обслуживания.

Вместе с тем данное определение связности не учитывает важность отдельных ИНС, количество и распределение в них путей, а также особенности воздействия на них ДФ.

В связи с этим в работе [2] в качестве показателя устойчивости сети предложено использовать среднесетевую вероятность связности $P_{У\,ср}$ [2]:

$$P_{У\,ср} = \frac{1}{N}\sum_{i=1}^{N} P_{У\,i}\ , \qquad (2)$$

где: N – количество ИНС в СС; $P_{У\,i}$ – устойчивость i-го ИНС $i = \overline{1, N}$.

Устойчивость каждого i-ого ИНС $Р_{У\,i}$ определяется в соответствии с выражением [2]:

$$P_{У\,i} = K_{Г\,i} P_{св\,i}\,, \qquad (3)$$

где $К_{Г\,i}$ коэффициент готовности i-ого ИНС; $Р_{св\,i}$ вероятность связности i-ого ИНС, в условиях воздействия на нее ДФ.

В выражении (3) коэффициент готовности $К_{Г\,i}$ определяет временные параметры процесса отказов/восстановлений ИНС при воздействии на нее ДФ, а вероятность связности ИНС $Р_{св\,i}$ – структурно-вероятностные параметры этого процесса.

Необходимо отметить, что при использовании показателя устойчивости в виде (2) вводиться допущение о равнозначности ИНС при определении устойчивости сети. Однако, различные ИНС имеют различную важность и для учета их разного вклада в общий показатель устойчивости (в выражении (2)) вводят соответствующие весовые коэффициенты α_i [3]:

$$P_{У\,ср} = \sum_{i=1}^{N} \alpha_i P_{Уi},$$

$$\text{условие нормировки } \sum_{i=1}^{N} \alpha_i = 1\,, \qquad (4)$$

где $Р_{У\,ср}$ среднесетевая вероятность связности; $Р_{У\,i}$ – устойчивость i-го ИНС $i = \overline{1, N}$; α_i весовой коэффициент, учитывающий важность i-го ИНС.

В работе [3] предполагается, что весовые коэффициенты α_i в выражении (4) задаются исходя из конкретных условий и целей функционирования СС. Однако в этой работе не указываются конкретные подходы к вычислению коэффициентов важности.

В работе [2] коэффициенты важности i-го ИНС предложенно определять исходя из циркулирующей по ним доли трафика [2]:

$$\alpha_i(\lambda_i) = \frac{\lambda_i}{\sum_{i=1}^{N} \lambda_i}\,, \qquad (5)$$

где λ_i - трафик, передаваемый в i-том ИНС; N – количество ИНС в СС.

Учет структурно-вероятностных параметров при оценке показателя устойчивости

Рассмотрим более подробно факторы, определяющие вероятность связности отдельного i-ой ИНС $Р_{св\,i}$, в выражении (3) при определении показателя устойчивости СС.

Для учета специфики воздействующего ДФ в работе [2] вероятность связности $Р_{св\,i}$ каждого отдельного i-го ИНС из выражения (3) предложено определять в следующем виде:

$$P_{св\,i} = \left(1 - P_{ИТВ\,i}\right)\left(1 - P_{РЭП\,i}\right)\left(1 - P_{ФП\,i}\right)\left(1 - P_{отк\,i}\right), \qquad (6)$$

где $P_{ИТВ\,i}$ - вероятность отказа элементов СС (каналов и узлов связи) вследствие информационно-технических воздействий (ИТВ); $P_{РЭП\,i}$ – вероятность подавления количества каналов связи СС большего, либо равного величине реберной связности x_v подграфа $G_{ИНС\,i}$; $P_{ФП\,i}$ – вероятность физического поражения (ФП) узлов связи СС большего, либо равного величине вершинной связности x_u подграфа $G_{ИНС\,i}$; $P_{отк\,i}$ – вероятность отказа элементов СС (каналов и узлов связи) вследствие воздействия внутренних ДФ и естественных процессов надежности.

При этом считается, что каждое из учитываемых в выражении (6) воздействий переводит подграф $G_{ИНС\,i}$, формализующий i-ую ИНС в несвязное состояние.

В работе [4] вероятность работоспособного состояния j-го пути $Р_{раб\,j}$ в составе i-го ИНС состоящего из z_j элементов (m_j каналов и n_j узлов связи) предложено определять через вероятности работоспособного состояния $P_{раб.\,эл.\,v}$ всех v-ых элементов в составе пути с учетом особенностей воздействия ДФ:

$$P_{раб\,j} = \prod_{v=1}^{z_j} P_{раб.\,эл.\,v}\,, \qquad (7)$$

$$P_{раб.\,эл.\,v} = \left(1 - P_{ИТВ\,v}\right)\left(1 - P_{РЭП\,v}\right) \times \left(1 - P_{ФП\,v}\right)\left(1 - P_{отк\,v}\right) \qquad (8)$$

где $z_j = m_j + n_j$ – количество элементов (каналов и узлов связи) в составе пути; переменные, $P_{ИТВ\,v}$ $P_{РЭП\,v}$, $P_{ФП\,v}$, $P_{отк\,v}$ соответствуют вероятностям воздействия соответствующих ДФ, в результате которых отказывает v-ый элемент j-го пути.

В этом случае связность i-го ИНС будет определяться работоспособным состоянием всех l_i -ых путей, каждый из которых содержит z_j элементов ($j = \overline{1, l}$) и будет равна:

$$P_{св\,i} = 1 - \prod_{j=1}^{l}\left(1 - P_{раб\,j}\right) = 1 - \prod_{j=1}^{l}\left(1 - \prod_{v=1}^{z_j} P_{раб.\,эл.\,v}\right). \qquad (9)$$

Зачастую в практике построения современных СС используется резервирование путей в ИНС, когда один путь является основным, а остальные – резервными. В этом случае вероятность связного состояния ИНС из одного основного и (l–1) резервных путей (соответственно из $z_{осн}$ и z_j элементов, где $j = \overline{2, l}$), будет определяться как:

$$P_{св\,i} = 1 - \left(\left(1 - \prod_{v=1}^{z_{осн}} P_{раб.эл.v} \right) \prod_{j=1}^{l-1} \left(1 - \prod_{v=1}^{z_j} P_{раб.эл.v} \right) \right). \quad (10)$$

Так как для любого j-го пути $P_{\text{раб. эл. v}} \leqslant 1$, то для любого ИНС добавление резервных путей будет увеличивать вероятность его связности.

Вместе с тем, выражение (10) не учитывает возможные пересечения путей на элементах подграфа ИНС. Зависимость вероятности связности i-го ИНС $\text{Р}_{\text{св } i}$ от количества путей l на ИНС с учетом их пересечений по общим элементам сети показана в работе Ковалькова Д.А. [5].

В случае если первыми l путями обеспечивается вероятность связности $P_{св\,l}$, то добавление очередного пути (l+1) приведет к увеличению вероятности связности ИНС до $P_{св\ l+1}$. Вероятность $P_{св\ l+1}$ будет определяться вероятностью двух событий: исправен хотя бы один из первых l путей или исправен (l+1)-й путь, в соответствии с рекуррентной формулой [5]:

$$P_{св\,i} = P_{св\,l} + P_{св\,l+1} - P_{св\,l+1} * P_{св\,l}\,, \quad (11)$$

где знак «*» – означает, что при перемножении вероятностей связности путей в составе ИНС при наличии общих элементов связность, обеспечиваемая элементами, входящими в первые l путей и общими с новым (l+1)-м путем, заменяется единицей.

Учет временных параметров при оценке показателя устойчивости

Надежность каналов передачи характеризуется коэффициентом готовности $\text{К}_{\Gamma\,i}$ который является временным параметром устойчивости i-го ИНС и определяется наработкой на отказ $\text{Т}_\text{О}$ и временем восстановления $\text{Т}_\text{В}$ (12).

Время восстановления $\text{Т}_{\text{В}\,i}$ согласно [6], состоит из: времени диагностики отказа $\text{Т}_{\text{диагн}\,i}$; времени ожидания восстановления связи (удержания конфигурации ИНС) $\text{Т}_{\text{ож}\,i}$; временем уведомления узла, ответственного за изменение конфигурации путей ИНС $\text{Т}_{\text{увед}\,i}$; длительности резервирования и реконфигурации путей в ИНС $T_{\text{рек}\,i}$; времени переключения информационных потоков с активных путей на резервные пути в составе ИНС $T_{\text{перекл}\,i}$:

$$K_{\Gamma\,i} = \frac{T_{O\,i}}{T_{O\,i} + T_{B\,i}} = \frac{T_{O\,i}}{T_{O\,i} + \left(T_{диагн\,i} + T_{ож\,i} + T_{увед\,i} + T_{рек\,i} + T_{перекл\,i} \right)}. \quad (12)$$

Время уведомления $\text{Т}_{\text{увед}\,i}$ в ИНС зависит от времени передачи между отдельными узлами сообщения об отказе $T_{пер}$ и от количества участков сети d_{ij}, между узлом, обнаружившим отказ пути (узел a), и узлом, ответственным за переключение путей в ИНС (узел b).

$$T_{увед\,i} = T_{пер}\, d_{ab}\,. \quad (13)$$

Для повышения временных параметров устойчивости ИНС, как следует из выражения (13), необходимо максимально сократить длительность *восстановления связи* ($\text{Т}_{\text{В}\,i}$). Это достигается применением протоколов маршрутизации, которые обеспечивают быстрое обнаружение отказа ($\text{Т}_{\text{диагн}\,i}$) и уведомление о нем узла, ответственного за переключение, либо принятие решения о переключении на самом узле, ближайшем к отказавшему элементу СС. Заблаговременное резервирование маршрутов позволит сократить временные интервалы $\text{Т}_{\text{диагн}\,i}$ и $T_{\text{перекл}\,i}$. Анализ выражения (13) показал, что введение дополнительной структурной избыточности ведет к увеличению d_{ab} *и, как следствие, приводит к ухудшению надежности по показателю коэффициента готовности*.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 5311 – 2008. «Устойчивость функционирования сети связи общего пользования».

2. Назаров А.Н., Сычев К.И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. – Красноярск: Поликом, 2010. – 389 с.

3. Боговик А.В., Игнатов В.В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.

4. Макаренко С.И. Анализ воздействия преднамеренных помех на функционирование расширенного протокола маршрутизации внутреннего шлюза (EIGRP) // Информационные технологии моделирования и управления. 2010. №2 (61). С. 223-229.

5. Ковальков Д.А. Математические модели оценки надежности мультисервисного узла доступа // Радиотехнические и телекоммуникационные системы. 2011.№2. С. 64-71

17. Егунов М.М., Шувалов В.П. Анализ структурной надежности транспортной сети // Вестник СибГУТИ. 2012. №1. С. 54-60.

С. Е. Мищенко[1]
доктор техничеких наук

В. В. Шацкий[1]
кандидат техничеких наук, с.н.с.

С.В. Землянский[2]
кандидат техничеких наук
[1]ФГУП «Ростовский-на-Дону НИИ радиосвязи» ФНПЦ,
[2]Военная академия связи (филиал, г. Краснодар)

ШИРОКОПОЛОСНАЯ АНТЕННА ДЛЯ СИСТЕМЫ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ИНФОРМАЦИИ

Рассмотрен синтез широкополосного векторного излучателя на основе модели векторной антенны, в которой ортогональные компоненты токов являются независимыми.

Введение

Системы радиотехнической разведки (СРР) в процессе сбора и обработки информации в информационном поле должны отвечать требованиям по широкополосности. Поскольку антенна связана со звеньями радиоканала, ее свойства в полосе частот являются существенными. Поэтому при проектировании антенн СРР необходимо уметь синтезировать их требуемые свойства.

В соответствии с [1-3] широкополосные свойства антенны определяются степенью постоянства ее двух параметров: диаграммы направленности (ДН) и коэффициента отражения (КО) на входе фидера. При этом основным способом решения проблемы широкополосности является создание излучателей с медленно меняющимся входным импедансом (ВИ) в полосе частот (ПЧ). Одним из приемов является усложнение распределения тока в излучателе за счет перехода от линейной антенны к плоскому или трехмерному векторному излучателю.

Цель исследования – разработка математического аппарата синтеза широкополосных излучателей на основе модели векторной антенны (ВА).

Синтез излучателей с улучшенными диапазонными свойствами

В [4-6] под ВА понимается совокупность трёх взаимно ортогональных излучателей с совмещенными фазовыми центрами. Управление параметрами антенны: комплексными амплитудами возбуждения элементов или их размерами – позволяет формировать заданные характеристики направленности. Однако в работах, посвященных ВА, свойства таких антенн в ПЧ не исследованы.

Рассмотрим систему (рис. 1) из трех тонких взаимно ортогональных симметричных вибраторов длиной l_a $(a = x, y, z)$ и радиусом r_a с совмещенными фазовыми центрами. Пусть фидерный тракт состоит из равномерного сумматора «на три» (1 вход сумматора имеет волновое сопротивление (ВС) 50 Ом, а остальные – 150 Ом), четвертьволновых трансформаторов сопротивлений линий передачи с ВС Z_{0a} к ВС 150 Ом и отрезков линий передачи с ВС Z_{0a} и длиной L_a, необходимых для согласования линии передачи с вибраторами. Входное сопротивление вибраторов с отрезком линии передачи и ρ_a – комплексный

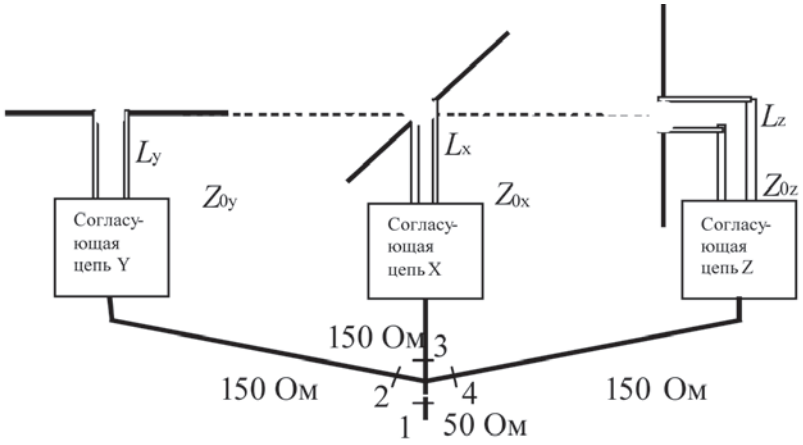


Рис. 1. Векторная антенна

коэффициент отражения (КО) на входе вибратора могут быть найдены по формулам [3]:

$$Z_{ina} = Z_{0a}\frac{1+\rho_a \exp(-i2kL_a)}{1-\rho_a \exp(-i2kL_a)};\ \rho_a = \frac{Z_0 - Z_a}{Z_0 + Z_a};$$

$$Z_{in-a} = 150\frac{1+\rho_a \exp(-i2kL_a)}{1-\rho_a \exp(-i2kL_a)}, \qquad (1)$$

где Z_a – входное сопротивление соответствующего вибратора; Z_{in-a} – сопротивление после трансформации в каждом плече. При подключении трех вибраторов ко входам сумматора входное сопротивление ВА примет вид:

$$Z = \left(\sum_{a=x,y,z}\frac{1}{Z_{in-a}}\right)^{-1} =$$

$$= \frac{Z_{in-x}Z_{in-y}Z_{in-z}}{Z_{in-x}Z_{in-y} + Z_{in-x}Z_{in-z} + Z_{in-y}Z_{in-z}} = \cdot \qquad (2)$$

$$= Z_{in-x}Z_{in-y}Z_{in-z}A^{-1}$$

Результирующий КО и длина линии передачи описываются выражениями вида:

$$\rho = \frac{50 - Z}{50 + Z} = \frac{50A - Z_{in-x}Z_{in-y}Z_{in-z}}{50A + Z_{in-x}Z_{in-y}Z_{in-z}}$$

$$k_a L_a = \pi + \frac{\arg\rho_a}{2}, \qquad (3)$$

где L_a – длина линии передачи при узкополосном согласовании на выбранной частоте, для которой сопротивление равно действительной части входного сопротивления вибратора [3]; k_a – волновое число. Однако в широкой полосе частот при узкополосном согласовании необходимо каждый раз менять величины Z_{0a} и L_a, что является неудобным с инженерной точки зрения. Поэтому для определения параметров воспользуемся сначала известным подходом [8]:

$$Z_{0a} = \frac{1}{\omega_2 - \omega_1}\int_{\omega_1}^{\omega_2} \mathrm{Re}\left(Z_a(\omega)\right)d\omega;$$

$$L_a = \frac{1}{\omega_2 - \omega_1}\int_{\omega_1}^{\omega_2} \frac{\pi + 0{,}5\arg\left(\rho_a(\omega)\right)}{\omega}d\omega, \qquad (4)$$

где ω_2 и ω_1 – верхняя и нижняя частоты заданного диапазона.

Для произвольного тока в элементе ВА задача определения ВИ может быть решена с помощью различных подходов [1], [9]. Для антенны рис.1 в виду простоты целесообразно использовать подход метода эквивалентных схем [1, 2].

ВИ тонкого симметричного вибратора, ориентированного вдоль орта e_a декартовой системы координат, описывается выражением [1]:

$$Z_{ina} = Z_{0a}\left(1 - i\frac{\alpha_a}{k}\right)\mathrm{cth}\left(\alpha_a l_a + j\beta l_a\right);$$

$$Z_{0a} = 120\left(\ln\frac{l_a}{r_a} - 1\right); \qquad (5)$$

$$\alpha_a = \frac{R_{1a}}{W_{wa}};\quad R_{1a} = R_{\Sigma\Pi a}\Big/ l_a\left(1 - \frac{\sin 2k_1 k l_a}{2k_1 k l_a}\right), \qquad (6)$$

где – ВС вибратора; r_a – радиус вибратора; α_a – эквивалентный коэффициент затухания; R_{1a} – погонное активное сопротивление потерь одного проводника линии; l_a – длина плеча вибратора; $\beta = kk_1$ – эквивалентное волновое число; k_1 –

поправочный множитель [1]; $R_{\Sigma Па}$ – сопротивление излучения вибратора, отнесенное к пучности тока, рассчитываемое по формуле Баллантайна [1,2].

Рассмотрим задачу конструктивного синтеза широкополосного векторного излучателя с ортогональными компонентами токов в следующей постановке. Для заданного диапазона частот и антенны на рис.1 необходимо найти девять параметров: l_a r_a, L_a, обеспечивающих минимизацию функционала вида:

$$Q = \int_{\omega_1}^{\omega_2} \left|\rho\left(l_a, r_a, L_a, \omega\right)\right|^2 d\omega \,. \qquad (7)$$

Функционал (7) согласуется с определением широкополосной антенны [1, 2] и является дифференцируемым. Решение задачи синтеза определяется частотной зависимостью ВИ элементов антенны. Компоненты градиента функционала (7) используются для организации итерационного процесса:

$$\gamma_a^{\langle t+1\rangle} = \gamma_a^{\langle t\rangle} - v^{\langle t\rangle} \frac{\partial Q^{\langle t\rangle}}{\partial \gamma_a}; \quad Q^{\langle t+1\rangle} < Q^{\langle t\rangle}, \quad (8)$$

где $v^{\langle t\rangle}$ – скорость приближения к экстремуму. На каждом шаге t итераций проверяется выполнение условия (8). При его нарушении осуществляется дробление шага $v^{\langle t\rangle}$ для нахождения экстремума функции Q с заданной точностью.

Итак, особенность предлагаемого аппарата состоит в том, что искомые параметры оказывают различное влияние на широкополосные свойства ВА. Следовательно, при реализации процедуры (8) параметр скорости приближения $v^{\langle t\rangle}$ должен отличаться для каждой группы параметров: l_a r_a, L_a.

Численное моделирование

Каждый шаг итерационного процесса содержит три последовательные процедуры (8) для каждой группы параметров. Для решения задачи синтеза ВА потребовалось 26 итераций и была сформирована такая частотная зависимость входного сопротивления системы на рис. 1, у которой реальная часть в заданном интервале частот от 196 до 396 МГц (центральная частота 296 МГц) практически неизменна и колеблется вблизи 50 Ом, а мнимая часть колеблется вблизи нулевого уровня. Данному ВИ соответствует зависимость КО на рис. 2.

Сплошная кривая - синтезированная антенна, а пунктирная – антенна с начальными параметрами. Исходные и конечные параметры сведены в таблицу 1 (строки 1 и 2). Перед оптимизацией основной вклад в ДН вносит вибратор, ориентированный вдоль оси $0x$. После оптимизации размеры всех вибраторов примерно одинаковы, что приводит к изменению формы ДН по сравнению с торроидальной ДН. В рассматриваемой полосе частот ДН ВА сохраняется.

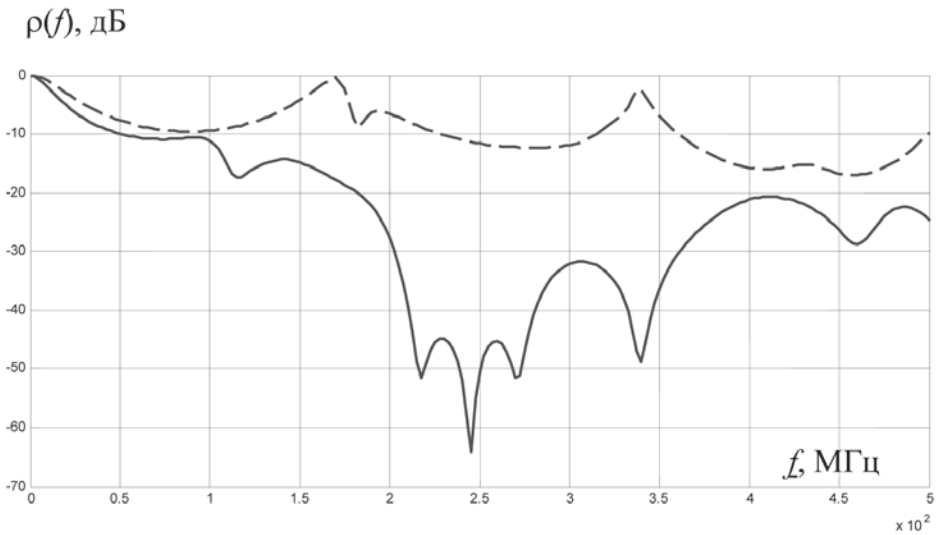


Таблица 1

Начальные (1) и конечные (2) значения параметров оптимизации

№	Длины плеч вибратора, м			Радиусы проводов, м			Длины фидера, м		
	l_x	l_y	l_z	r_x	r_y	r_z	L_x	L_y	L_z
1	0,25	0,1	0,17	0,013	0,050	0,008	0,711	0,865	0,827
2	0,4936	0,458	0,464	0,039	0,064	0,048	0,614	0,814	1,006

Заключение

Таким образом, полученные результаты подтверждают возможность применения узкополосного согласования для отдельных антенных элементов системы излучателей с целью расширения рабочей полосы всей системы (на рис.2 расширение составило 60 %). Предлагаемый математический аппарат позволяет при определенных модификациях и ограничениях стать основой для решения целого ряда практически важных задач конструктивного синтеза антенн.

СПИСОК ЛИТЕРАТУРЫ

1. Марков Г.Т., Сазонов Д.М. Антенны: Учебник для вузов.-М.: Энергия. 1975.

2. Марков Г.Т. Антенны. - М.: Госэнергоиздат. 1960.

3. X. Ding, B.-Z. Wang, G.-D. Ge and D. Wang. A Broadband VHF/UNF Double-WHip Antenna. // IEEE Transaction on Antennas and Propagation. 2012/ V. 60. NO2. Pp. 719-724.

4. Балзовский Е.В., Буянов Ю.И., Кошелев В.И. Векторная приемная антенна для измерения поляризационной структуры сверхширокополосных электромагнитных импульсов // Радиотехника и электроника, 2005. Т.50. № 8. С.863-872.

5. Габриэльян Д.Д., Мищенко С.Е., Шацкий В.В. Возможности формирования нуля диаграммы направленности на основе излучателя из трех ортогональных вибраторов. // Радиотехника. – 1995. №7-8. С. 81-83.

6. Пат. 2393597 Российская Федерация, H 01 Q 21/24. Антенна [Текст] / Колесников В.Н., Мищенко С.Е., Шацкий В.В., Шацкий Н.В. // опубл. 27.06.10, Бюл. № 18. –.7 с.: ил.

7. Макурин М.Н., Кирьяшкин В.В., Чубинский Н.П. Эквивалентная схема, моделирующая входной импеданс биконической антенны // Труды III Всероссийской конф. «Радиолокация и радиосвязь». ИРЭ РАН. 26-30 октября 2009 г. С. 12-16.

8. Вендик О.Г., Парнес М.Д. Антенны с электрическим сканированием. Введение в теорию / Под ред. Л.Д. Бахраха. С.-Петербург. 2001.

Ю.Н. Музелин
кандидат техничеких наук
Д.А. Рычков
Г.Н. Юрьев
ОАО «ВНИИРА»

ПЕРЕДАЧА ЦИФРОВЫХ СИГНАЛОВ В РЕАЛЬНОМ ВРЕМЕНИ ПО ВОЛОКОННО-ОПТИЧЕСКОМУ КАНАЛУ.

В докладе рассмотрены вопросы передачи и приема в масштабе реального времени многоканальных цифровых сигналов по волоконно-оптическому каналу. Рассмотрены методы и средства мультиплексирования сигналов частотой до 50 МГц, передачи по волоконно-оптической линии связи (ВОЛС) на частотах до 2,5 ГГц и их обратное демультиплексирование. Предложены технические средства для реализации. Описаны характеристики опытного образца аппаратуры.

Введение

В современных радиолокаторах существует проблема передачи данных с приемного устройства в системы первичной обработки сигналов, особенно в тех случаях, когда модуль фазированной антенной решетки (ФАР) является самостоятельным малогабаритным устройством и находится в обтекателе летательного аппарата (ЛА) ограниченного объема, а система первичной обработки сигналов вынесена в фюзеляж ЛА и соединена с модулем ФАР через вращающееся сочленение. В таком случае простым выходом может оказаться передача сигнальных линий существующих интерфейсов по оптоволокну.

В данной статье рассмотрено решение задачи по передаче сигналов нескольких интерфейсов через волоконно-оптический канал. В исходном интерфейсе имеются как синхронные последовательные кадрированные каналы («frame», «data», «clock») частотой 50 МГц в уровнях LVDS, так и сигналы типа «разовая команда» TTL-уровня, а также двунаправленные полудуплексные линии стандарта RS-485. Задача устройства преобразования среды передачи данных состоит в том, чтобы мультиплексировать цифровые линии в последовательные данные ВОЛС, затем произвести обратную операцию – демультиплексирование данных. Необходимо обеспечить реальное время передачи сигналов, т.е. минимизировать постоянную и переменную составляющую задержки демультиплексированных данных относительно мультиплексированных. В конкретном случае допустимая постоянная составляющая задержки равна 500 нс, а переменная – 10 нс. Повторный запрос на передачу данных в случае их искажения не предусмотрен. Поэтому, даже редко случающееся искажение передаваемой информации недопустимо.

Теоретические соображения

При передаче высокоскоростных сигналов важным условием является сбалансированное количество логических нулей и единиц. Соответственно, необходимо выбрать механизм кодирования данных: скремблирование или изменение данных с помощью кодирующих таблиц[1].

Мультиплексирование и последующее демультиплексирование сигнала осуществляется

на однотипных, но все же разных устройствах, поэтому тактовые частоты, генерируемые в этих устройствах, неизбежно будут различаться. Особенно в условиях разницы температур между обтекателем и фюзеляжем. Следовательно, необходимо либо выделять отдельную тактирующую линию, либо выбрать механизм синхронизации двух устройств.

Входные сигналы должны считываться устройством с частотой, превышающей их собственную частоту более чем в 2 раза. Для сохранения всех качеств синхронного интерфейса нельзя просто считывать такты и данные – различие фазовых задержек в линиях приведет к потере данных. Поэтому, в соответствии с протоколом, необходимо считывать данные строго по фронту тактового сигнала.

Реализация мультиплексирования полудуплексного режима линий RS-485 требует определенного механизма переключения направления передачи данных.

Практическая реализация

Главным элементом, необходимым для реализации проекта, была выбрана программируемая логическая интегральная схема (ПЛИС) фирмы Xilinx семейства Virtex5. Эти ПЛИС предоставляют широкие возможности для реализации высокоскоростных последовательных интерфейсов. Входящие в их состав модули Rocket IO GTX позволяют передавать данные на скоростях до 6.5 Гбит/с [3], используя стандартные интерфейсы (Ethernet, SATA, PCI-E и т.д.), либо интерфейсы собственной разработки. Микросхемы Virtex5 содержат до 48 дифференциальных высокоскоростных приемопередатчиков[2]. К достоинствам данной ПЛИС также следует отнести наличие в своем составе механизмов кодирования 8b/10b и 64b/66b. Имеющийся эластичный буфер позволяет реализовать коррекцию тактов (Clock correction), необходимую для устранения разности частот задающих генераторов на передающей и приемной сторонах, а также осуществить связывание каналов (Channel bounding) - устранить разницу задержки распространения сигнала в различных каналах [3].

Применение кодека 64b/66b создает меньшую избыточность (3% вместо 25% у 8b/10b), однако этот алгоритм более сложный, выравнивание данных занимает более длительное время, а также возможен незначительный дисбаланс логических уровней. Поэтому в приемопередатчиках используется кодирование 8b/10b. В таком случае при работе на частоте 1,25 ГГц мы получаем скорость 1 Гбит/с. Избыточность передаваемой информации компенсируется возможностью простого и быстрого выравнивания данных на приемной стороне и коррекции тактов. Для этого требуется с некоторой периодичностью посылать специальные символы (т.н. запятые) и символы коррекции тактов. Выбирать эти символы следует из набора доступных для 8b/10b управляющих символов (K-символов).

Структура проекта представлена на рисунке 1.

Данные на вход приемопередатчиков поступают по 8-битной шине (для варианта со скоростью 2,5 Гбит/с – 16 бит) с частотой 125 МГц. Так как необходимо вставлять в поток считываемых данных управляющие символы, мы должны выполнять дискретизацию входного сигнала с частотой меньше 125 МГц. Была выбрана частота 120 МГц, так как это позволяет на один блок из 24 отсчетов передать один управляющий символ. Это (поочередно) либо символ запятой, либо символ коррекции тактов. Кроме того, используя доступные в Virtex5 блоки ФАПЧ (PLL), легко получить синфазные тактовые сигналы частотой 120 и 125 МГц.

Для компенсации разницы частот считывания и передачи используется выходной буфер типа FIFO. Так как разница частот невелика, FIFO не должно быть глубоким – 16 слов достаточно. Считывание данных из FIFO происходит быстрее, чем запись, следовательно, необходимо предварительно накопить несколько слов в памяти, прежде чем разрешить их считывание и передачу.

По одной линии данных можно поочередно передавать отсчеты с двух (либо четырех и т.д.) цифровых входов. Таким образом, частота дискретизации уменьшится в два (четыре) раза, что повлечет за собой уменьшение максимальной частоты сигналов до 25 МГц (12,5 МГц).

На приемной стороне нельзя использовать FIFO для исключения управляющих символов, так как символы коррекции тактов могут либо дублироваться, либо пропускаться (в этом заключается принцип коррекции тактов). Поэтому сигналы просто восстанавливаются с частотой

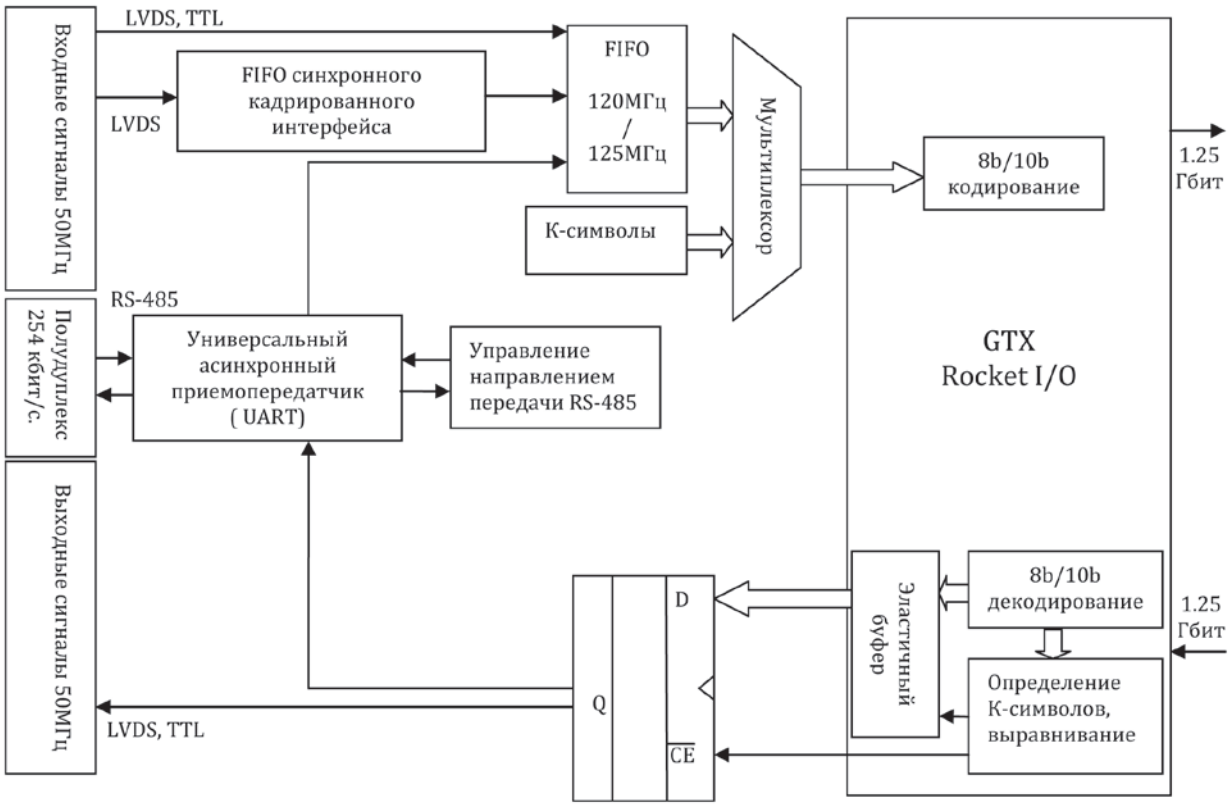


Рис. 1. Структура проекта ПЛИС.

125 МГц, а во время передачи К-символа остаются неизменными.

Чтобы минимизировать задержку передачи, данные синхронного кадрированного последовательного интерфейса необходимо передавать сразу по мере получения. Для этого используется однобитное FIFO глубиной 16 бит. При наличии принятых данных в FIFO, на соответствующих линиях 120 МГц шины выставляются данные, а линия тактов сбрасывается в низкий уровень. При следующем фронте 120 МГц тактов сигнал «clock» синхронного интерфейса устанавливается в состояние логической единицы. При этом происходит подсчет количества переданных бит, и после передачи 32 бит сигнал «frame» сбрасывается. При этом все сигналы соответствуют синхронному кадрированному последовательному протоколу, с той разницей, что сигнал «clock» представляет собой не меандр – длительность высокого и низкого уровня различна, и составляет (на выходе приемной стороны) 8 или 16 наносекунд.

Для линий RS-485 используется универсальный асинхронный приемопередатчик (UART). Данные передаются как «разовые команды», но при этом происходит анализ первого байта сообщения на передающей и приемной стороне. В соответствии с протоколом обмена, по первому байту сообщения однозначно определяется время переключения направления передачи. После выполнения запроса передатчик переключается на прием либо до окончания ответного пакета, либо до превышения допустимого времени ожидания.

Тактирование приемопередатчиков выполняется от опорного генератора частотой 100 МГц, подключенного к выделенным линиям модуля GTX. Частоты 120 и 125 МГц (а также 240 и 250 МГц для встроенного логического анализатора) синтезируются с помощью двух модулей ФАПЧ, синхронизированных от опорного тактового сигнала GTX. От сигнала частотой 120 МГц тактируется блок синхронного кадрированного интерфейса и входная память типа FIFO.

Память FIFO для сопряжения шин 120 и 125 МГц выполнена на аппаратном модуле, входящем в состав Virtex5. Память FIFO, входящая в блок

Таблица 1

Характеристики блока передачи и приема цифровых сигналов

Частота ВОЛС, ГГц	Частота цифровых линий, МГц	Частота дискретизации, МГц	Количество цифровых линий	Постоянная задержка*, нс	Переменная задержка, нс
1,25	50	120	8	550	8,3
	25	60	16		16,7
	12,5	30	32		33,3
2,5	50	120	16	330	8,3
	25	60	32		16,7
	12,5	30	64		33,3

*Указанные задержки означают суммарное время прохождения от входных LVTTL (LVDS, RS-485) выводов на одном устройстве выходных выводов на втором устройстве.

кадрированного синхронного интерфейса, реализована на распределенной однобитной памяти с использованием соответствующего примитива.

Мультиплексор данных и управляющих символов для приемопередатчика GTX выполнен с помощью счетчика, который каждое 25-е и 50-е слово данных наполняет управляющим символом, а остальные считывает из FIFO.

Полученные результаты

Разработка блока передачи и приема цифровых сигналов на ПЛИС Xilinx Virtex5 заняла четыре месяца. В результате было получено гибкое решение, воплощенное в реальной аппаратуре:

Дальнейшее развитие проекта возможно и подразумевает введение в протокол механизма связывания каналов. Эта функция, как уже отмечалось выше, поддерживается GTX Rocket IO и позволяет связывать каналы, выравнивая время передачи данных по нескольким ВОЛС с удержанием взаимного фазового разбега в требуемых пределах. Для связывания каналов необходимо кроме передачи символов запятой и коррекции тактов передавать символ связывания каналов. В таком случае цикл работы счетчика мультиплексирования данных и К-символов увеличивается до 75: каждый 25-й, 50-й и 75-й символы являются управляющими.

Заключение

Используя современную элементную базу, удалось в короткие сроки реализовать передачу цифровых сигналов отработанного интерфейса обмена данными через волоконно-оптический канал. При этом решение получилось гибким, позволяющим быстро переконфигурировать входы и выходы на различные комбинации интерфейсов.

СПИСОК ЛИТЕРАТУРЫ

1. High-Speed Serial I/O Made Simple. A Designer's Guide with FPGA Application – Abhijit Athavale, Carl Christensen. 2005.

2. Vertex-5 Family Overview. Datasheet. (www.xilinx.com)2009г.

3. Virtex-5 FPGA Rocket IO GTX Transceiver. User Guide. (www.xilinx.com) 2009г.

В.В. Мышко
кандидат технических наук, доцент

А.Н. Кравцов
кандидат технических наук

В.В. Ткаченко
кандидат технических наук
ФКГВОУ ВПО «Военно-космическая академия имени А.Ф. Можайского», г. Санкт-Петербург

ПРЕДУПРЕЖДЕНИЕ НЕШТАТНОГО ФУНКЦИОНИРОВАНИЯ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ С УЧЕТОМ ПРОГНОЗА РИСКОВ ВОЗНИКНОВЕНИЯ ОТКАЗОВ

Обосновывается необходимость своевременного предупреждения нештатных ситуаций в работе сложных технических систем на этапе целевого применения по результатам анализа их частично определенных параметров состояний. Представлены предложения по совершенствованию методического обеспечения контроля функционирования сложных технических систем.

Введение

Понятие технического состояния в теории контроля и технической диагностики является ключевым и определяется как совокупность подверженных изменению в процессе производства и эксплуатации свойств объекта, характеризуемая в определенный момент времени признаками, установленными технической документацией на этот объект. Между тем, указанные признаки не могут характеризовать свойства объекта, так как последние объективно существуют (присущи объекту) независимо от того, охарактеризованы они извне или нет. В технической документации могут быть указаны лишь в той или иной форме требования к свойствам объекта, обеспечивающие проверяемость этих свойств.

В этом смысле более конструктивным является определение технического состояния как совокупности свойств технического объекта, фиксируемых в определенный момент времени при определенных условиях внешней среды [1].

Для решения указанных задач необходим контроль функционирования сложных технических систем (СТС), осуществляемый информационно-управляющими системами специального назначения (ИУС СН) на всех этапах жизненного цикла СТС, а именно, контроль совокупности взаимосвязанных процессов последовательного изменения состояния СТС [2].

В общей структуре ИУС СН важную роль играет система информационно-телеметрического обеспечения (СИТО) технологических процессов. Предупреждение нештатного функционирования СТС из-за увеличения числа возникающих отказов на этапах испытания и целевого применения СТС при росте интенсивности задействования особо актуальным становится в период изменения обстановки. Особую роль в этих условиях приобретает обработка телеметрической информации (ТМИ) в режиме реального времени.

Результаты обработки ТМИ обеспечивают не только возможность выявления неисправ-

ностей, но позволяют формировать исходные данные для диагностического контроля с целью предупреждения развития отказов СТС. При этом к результатам обработки ТМИ предъявляются повышенные требования по оперативности их представления с учетом максимальной достоверности и точности локализации неисправностей.

Тенденции развития методов предупреждения нештатного функционирования сложных технических систем с учетом прогноза рисков возникновения отказов

Тенденции развития теории и практики создания ИУС СН предполагают обеспечение средств, включающих в свой состав не только контроль, но и прогнозирование поведения контролируемых параметров. При этом в целях обеспечения надежности подготовки СТС требуется формирование предложений по изменению количества и порядка анализируемых параметров, обеспечивающих полную наблюдаемость и прогнозируемость технического состояния (ТС) СТС.

Известные подходы к решению задач контроля и диагностирования ТС СТС, построенные на основе матричного, ситуационно-диагностического, автоматно-лингвистического, структурно-логического методов, а также метода с использованием временной расстановки событий имеют значительные ограничения по практическому применению, связанные с присущей им «жесткостью» схем обработки информации, слабыми возможностями по учету предыстории (накоплению и использованию знаний о возможных ТС), необходимостью проведения существенных доработок при изменении состава и логики функционирования СТС. В настоящее время широко применяется научно-методический аппарат, позволяющий обеспечить высокие требования по диагностированию неисправностей, но не в полной мере проработаны возможности предупреждения нештатного функционирования СТС по результатам диагностического контроля. Например, существующий научно-методический аппарат не позволяет обеспечить идентификацию возможных неисправностей СТС по пограничным классам состояний, характеризуемых по результатам частично определенных параметров состояний и функционирования существующей ИУС СН.

В настоящее время назрела необходимость разработки научно-методологических подходов к обоснованию и расчету обобщенной значимости телеметрируемых параметров (ТМП), используемых при диагностировании ТС СТС. Необходимость разработки таких подходов связана с усложнением структуры СТС и увеличением интенсивности задействования в период изменения обстановки.

При формировании требований к перспективной ИУС СН возникает проблемная ситуация, состоящая в необходимости своевременного предупреждения нештатных ситуаций в работе СТС при росте интенсивности использования и несовершенство моделей и методов контроля и диагностирования возможных отказов СТС по результатам анализа их частично определенных параметров состояний. Разрешение указанного противоречия предлагается осуществить путем разработки методического, математического обеспечения и системотехнических решений для ИУС СН.

Для получения максимально информативного результата анализа ТС СТС, без потери достоверности диагностирования, необходимо изменение последовательности анализа ТМП.

Системный анализ структуры и задач, решаемых ИУС СН, позволил сделать вывод о необходимости использования результатов экспресс– и оперативной обработки информации по аналогичным объектам, при подготовке исходных данных (ИД) для анализа ТС СТС нового однотипного изделия. Пути снижения рисков возникновения нештатных ситуаций в работе СТС могут основываться на применении агрегированных моделей анализа технического состояния. Данный подход позволяет в процессе контроля ТС СТС выявлять пограничные классы состояний (с учетом априорных данных) и оценивать риск возникновения нештатных ситуаций. В роли показателя риска возникновения нештатных ситуаций может выступать вероятность возникновения отказов СТС.

Перспективным направлением совершенствования ИУС СН является разработка системы оценивания значимости ТМП на основе формирования обобщенных показателей значимости с использованием результатов синтеза программ диагностирования (ПД) по критериям максимума достоверности и информативности

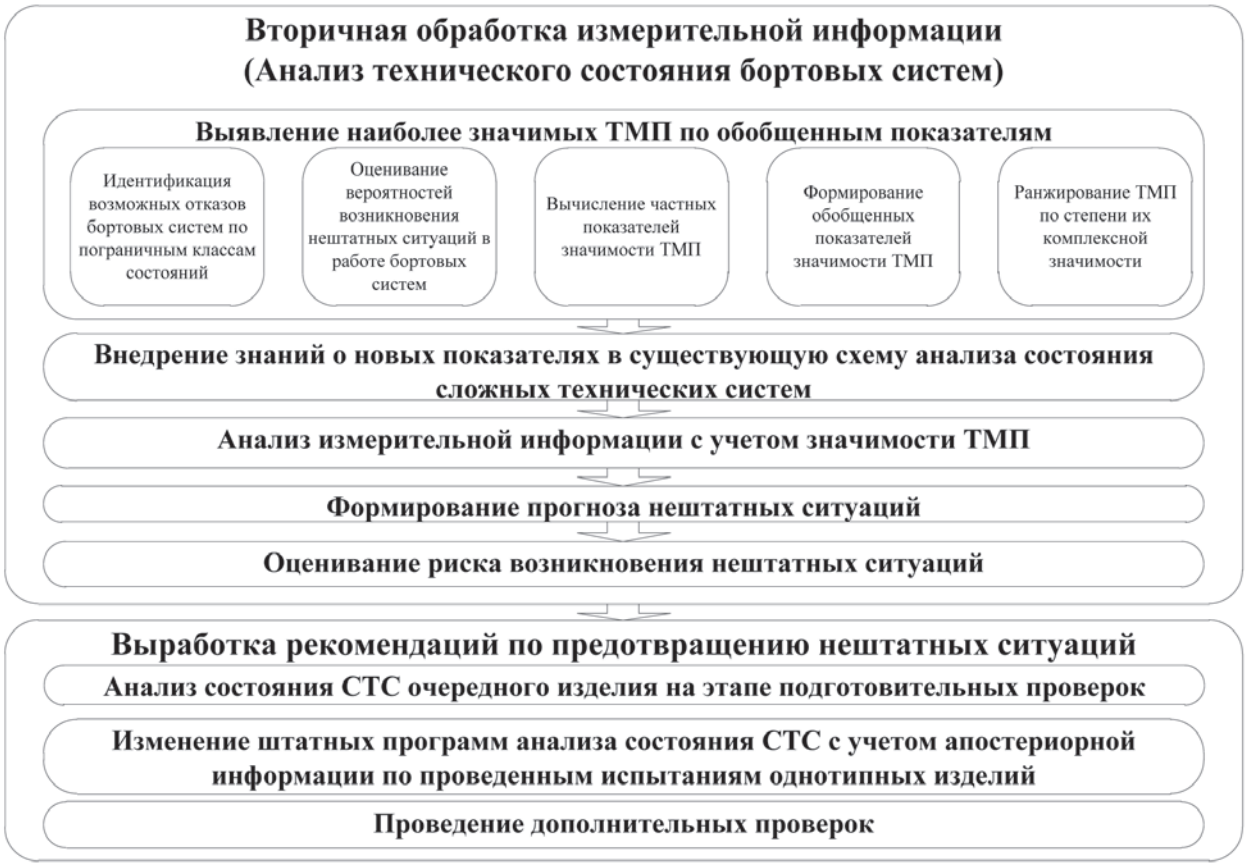


Рис. 1. Методика предупреждения нештатного функционирования сложных технических систем

программ диагностирования и учетом погрешности вычисления ДП.

Решение задачи определения значимости ТМП представляет собой совокупность алгоритмов, основанных на решении задач диагностирования методом динамического программирования. Показатели обобщенной значимости формируются на основе ИД по предшествующим испытаниям и применяются при диагностическом контроле на этапе подготовки очередного изделия [3, 4].

Структурная схема методики предупреждения нештатного функционирования сложных технических систем представлена на рисунке 1.

Заключение

Таким образом, тенденции развития теории и практики создания информационно-управляющих систем специального назначения показывают, что исследования целесообразно вести по следующим направлениям:

разработка методов идентификации ТМИ и оценивания основных характеристик СТС на основе интеллектуальных систем;

обоснование учета, в качестве инструментальной погрешности вычисления, тактико-технических и точностных характеристик отечественной датчиковой аппаратуры;

исследование методов преобразования множества ДП с целью уменьшения погрешности их вычисления;

исследование применимости при формировании множества изображений эталонных типов ТС положений теоремы отделимости;

дальнейшее развитие методической основы вычисления вероятностей ошибочного решения при определении исхода проверок ДП;

анализ способа вычисления ошибок первого и второго родов при определении исхода проверок ДП без использования приближенных номограмм, но с помощью таблиц или функционального уравнения.

СПИСОК ЛИТЕРАТУРЫ

1. Кравцов А.Н., Мышко В.В., Самойлов Е.Б., Ткаченко В.В. Обучение распознаванию технического состояния сложных технических систем / Тр. второй науч.-технич. конф. молодых специалистов «Старт в будущее». – СПб.: КБСМ, 2011. – С. 235-238.

2. Мышко В.В., Окуловский О.И., Ткаченко В.В. Программный комплекс анализа технического состояния бортовых систем на основе информации телесигнализации/Сб.«Изв. РАРАН» – М.: РАРАН, 2011. Вып. №1 (68). – С. 67-71.

3. Мышко В.В., Ткаченко В.В. Применение коллективных статистических решений для синтеза метода распознавания образов в задачах контроля и технического диагностирования / Тр. 13 Всерос. науч.-практич. конф. «Актуальные проблемы защиты и безопасности». Т. 1: Вооружение и военная техника. Прил. к журн. «Изв. РАРАН». – СПб.: НПО СМ, 2010. С. 245-249.

4. Ткаченко В.В. Реализация последовательного метода распознавания на примере объектов локации / Сб. тр. 12 Всерос. науч.-практич. конф. «Актуальные проблемы защиты и безопасности». Т. 2 : Вооружение и военная техника. Прил. к журн. «Изв. РАРАН». – СПб.: НПО СМ, 2009. – С.298-300.

О.В. Новиков
ОАО «Научно-исследовательский институт систем связи и управления»

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АСУВ ТАКТИЧЕСКОГО И ОПЕРАТИВНО-ТАКТИЧЕСКОГО УРОВНЯ УПРАВЛЕНИЯ

Файл слайдовой поддержки: Доклад НИИС-СУ.ppt

Слайд № 1

В ходе работы над созданием мобильно-стационарной системы управления силами специальных операций коллектив нашего института стремился создать такую систему, которая в полной мере отвечала бы требованиям полученного технического задания, а также основополагающим требованиям, предъявляемым ко всем системам управления войсками, изложенным в руководящих документах Министерства обороны.

Слайд № 2-3

За время работы и опытной эксплуатации элементов системы мы пришли к выводу о том, что основными критериями, определяющими эффективность автоматизированной системы управления военного назначения, являются:

во-первых - **сокращение цикла боевого управления**, то есть оперативность ее работы,

а во-вторых - **повышение качества решения управленческих задач**, выполняемых оперативным (боевым) составом пунктов управления.

Слайд № 4

Поэтому основным вопросом, который мы задавали себе при создании различных компонентов программного обеспечения, был: «А насколько уменьшатся продолжительность конкретной операции, выполняемой конкретным должностным лицом органа управления при использовании им нашей программы, по сравнению с неавтоматизированным выполнением той же операции?»

При этом нами учитывалось, помимо прочего, характер каждой выполняемой операции, ее место и роль в коллективной работе боевого состава соответствующего органа управления, а также степень влияния ее выполнения на общее время, потребное на выработку решения и постановку задач подчиненным.

Ввиду того, что опытный дивизионный комплект системы, которым мы оснастили 7-ю десантно-штурмовую дивизию (горную) активно использовался при проведении мероприятий боевой и оперативной подготовки у нас не было недостатка в материалах для такого анализа.

Очень скоро, мы пришли к выводу о том, что существует ряд задач, которые являются ключевыми в боевой работе должностных лиц органов управления, без «ускорения» решения которых, добиться сколько-нибудь существенного сокращения цикла боевого управления не удастся в принципе.

К такого рода задачам, в первую очередь, относится визуализация оперативно-тактической информации. Говоря другими словами – отображение тактической обстановки на электронной карте.

Слайд № 5

Помимо того, что на эту задачу замыкаются подавляющее большинство расчетных и расчетно-аналитических задач, работа на карте яв-

ляется для подавляющего большинства должностных лиц наиболее трудоемкой и сложной задачей.

В ходе мероприятий оперативно-тактической подготовки, проводимых в соединениях и воинских частях ВДВ с использованием средств АСУВ, мы неоднократно могли убедиться, что отсутствие инструмента, который позволил бы должностным лицам органов управления быстро отображать тактическую обстановку на электронной карте и в автоматическом режиме обмениваться этими данными, приводит к невозможности выполнения нормативов, установленных даже для ручного(!) способа работы.

И это при наличии оперативного состава достаточно подготовленного, как в военном отношении, так и в вопросах использования применяемых программно-технических средств!

Как выяснилось, столь же «системоообразующими» были вопросы сбора данных обстановки от подчиненных подразделений, доведения до них боевых задач, а также контроля выполнения поставленных боевых задач в режиме реального времени.

Слайд № 6

Практика многих учений показала, что использование для этих целей радиостанций Р-168 МРА не отвечает требованиям по устойчивости системы управления.

Ввиду этого, в качестве основных радиосредств, используемых в нашей системе для передачи информации в тактическом звене, были выбраны радиостанции УКВ-диапазона.

Относительно низкая пропускная способность УКВ-радиосредств в реальных боевых условиях весьма ограничивает возможности системы по передаче этой информации с гарантией ее получения.

Исходя из вышесказанного, мы определи для себя в качестве приоритетных следующие направления, при создании компонентов программного обеспечения:

Слайд № 7

1.Создание простого и надежного средства для отображения динамической тактической обстановки.

2. Поиск программных решений, позволяющих максимально уменьшить объемы графической информации, передаваемой по каналам связи.

3. Создание специальных программных средств, осуществляющих в реальном времени мониторинг возможностей каналов связи по передаче информации.

4. Разработка средств почтового обмена (электронной почты), гарантированно осуществляющих передачу информации с использованием неустойчивых каналов связи.

5. Создание программ, обеспечивающих в автоматическом режиме сбор и отображение данных о положении и состоянии объектов, имеющих средства глобального позиционирования (как бронеобъектов, так и отдельных военнослужащих).

6. Создание единых форматов передачи данных и программных продуктов обеспечивающих полностью замкнутый разведывательно-огневой контур.

Кроме того, в рамках работ по созданию программного обеспечения мы стремились сделать все программные компоненты максимально простыми в изучении и применении. Другими словами - дружелюбными для пользователя, что в конечных продуктах выразилось в интуитивно понятных пользовательских интерфейсах, не требующих изучения инструкций.

При этом, мы отдаем себе отчет, что по сути пока создали автоматизированную систему только класса С2. То есть, способную обеспечить командиру сбор и отображение данных обстановки, быстрое отображение (визуализацию и вербализацию) принятого им решения, гарантированное доведение его до подчиненных и контроль выполнения ими поставленных задач в автоматизированном режиме.

Пока в нашей системе не полностью реализован функционал, который можно было бы назвать «интеллектуальной поддержкой принятия решений». Но основа, или «фундамент» для проведения работ по созданию такой системы создан.

В настоящее время результат нашей работы по созданию системы подтвержден Государственными испытаниями, а также рядом учений, проведенных в последнее время. На этих учениях активно применялись компоненты нашей системы.

Слайд № 8

В плане сокращения цикла боевого управления, результаты, достигнутые и зафиксированные в ходе проведения учения «Кавказ-2012», а также ДКШУ с 7 десантно-штурмовой дивизией в апреле этого года представлены на слайдах:

Вам представлены этапы работы органов управления на примере тактического звена (полк-батальон-рота-взвод-отделение). На слайдах указано, за счет чего и какой достигнут выигрыш по времени при организации работы по подготовке боя.

Слайд № 9

На этом слайде и далее, использование компонентов программного обеспечения проиллюстрированы фотографиями, а также снимками экранов автоматизированных рабочих мест с отображением интерфейсов соответствующих программных продуктов.

Слайд № 10

Так, например, за счет использования графических данных, передаваемых вышестоящим штабом в качестве боевой задачи полку сокращение времени на Уяснение задачи, ориентирование должностных лиц и подчиненных командиров может достигать двух и более раз.

Слайд № 11

На данном слайде представлены интерфейсы программ **«Электронная почта», Контакты» и «Радиочат»,** которые используются для организации обмена сообщениями, а также для пересылки электронных файлов любого формата. Программа **Электронная почта»** при этом обеспечивает гарантированное доведение почтовых сообщений вне зависимости от текущего состояния и устойчивости каналов связи.

Слайд № 12

Реализация сетецентрических принципов построения системы связи позволяет (при соответствующей ее настройке) обмениваться информацией с нижестоящими уровнями управления минуя промежуточные уровни, что резко ускоряет информационный обмен на этапе сбора (добывания) данных обстановки. Кроме того, такой процесс в системе становится реально непрерывным.

Слайд № 13

Реализация принципа многопользовательского доступа с разграничением прав пользователей по слоям дает большие преимущества оперативному составу органов управления, как в плане ускорения обмена текущей графической информацией, так и в плане сохранения уже обработанной информации.

Слайд № 14

Основным преимуществом, которое дает система в плане организации работы параллельным методом, является возможность передачи подчиненным наиболее востребованной ими информации еще до «официального» получения ими боевых задач. Это обеспечивает подключение их к работе в значительно более ранние сроки, чем при ручном способе управления.

Слайд № 15

На данном слайде показана работа органа военного управления (полка), деятельность которого организована с использованием подвижных модулей, входящих в состав системы.

Слайд № 16

Многопользовательский доступ реализован по серверному принципу, при этом сервером может быть назначен компьютер любого должностного лица. Перестройка работы должностных лиц управления полка на резервный сервер, в случае выхода из строя основного, может быть произведена менее чем за минуту без потери текущей информации, которая сохраняется на каждом рабочем месте, имевшем ранее подключение к серверу.

Слайд № 17

На данном слайде показан интерфейс графического редактора с открытым окном серверной программы.

Слайд № 18

Сам принцип работы в многопользовательском доступе показан на данном слайде.

Слайд № 19

На этапе определения замысла и выработки решения командиром, помимо применения многопользовательского доступа, он имеет возможность пользоваться сенсорным экраном с функциями интерактивной доски (функция «Карандаш»). Данная функция используется для чернового отображения (визуализации) замысла (решения) командира и быстрого доведения до должностных лиц их вариантов.

Слайд № 20

На данном слайде работа командира и должностных лиц управления полка по выработке решения показана желтым цветом. Дело в том, что процесс выработки решения является наиболее творческой работой всех должностных лиц, которая крайне трудно поддается алгоритмизации. Особенно это характерно для низовых тактических звеньев.

Решающими факторами, могущими оказать влияние на ход и исход боя в тактике, как в составной части военного искусства, могут ока-

заться отнюдь не расчеты соотношения сил и средств, опирающиеся на боевые потенциалы, а дерзость принятого решения, внезапность действий, разнообразие тактических приемов, упреждение противника и другие, достаточно трудные для математического описания.

Кроме того, как показывает опыт, для корректного расчета, например, ожидаемых потерь, или темпов продвижения в наступлении с учетом противодействия противника, на этапе принятия решения, как правило, не хватает подтвержденных разведывательных данных.

Поэтому мы считаем, что на данном этапе работы пока рано говорить о замене опыта, военной интуиции, и таланта командира каким-либо программным продуктом.

Слайд № 21

На следующем слайде показан командно-наблюдательный пункт десантно-штурмового батальона десантно-штурмового полка 7 дшд(г), принимавшего участие в учении «Кавказ-2012».

Слайд № 22

Комплекс программных продуктов, используемых в системе, обеспечивает командиру весь спектр мультимедийных услуг – электронная почта, телефонная связь, в том числе – гарантированной стойкости, закрытая видеоконференцсвязь, а также КВ и УКВ радиосвязь. Доклад решения старшему начальнику может быть осуществлен с использованием любого из них, либо сочетанием нескольких.

Слайд № 23

Для постановки задач также могут быть использованы все доступные виды связи и программные компоненты, обеспечивающие их работу.

Слайд № 24

На слайде представлены фотографии должностных лиц управления 7 дшд(г) при постановке задач подчиненным частям и подразделениям. В центре – фотография группы направлений.

Слайд № 25

На этапе планирования боя, т.е. детализации решения командира на две ступени ниже наиболее трудоемким процессом является оформление планов по видам обеспечения и планов применения частей и подразделений родов войск и служб. Помимо трудоемкости данного процесса, принципиальное значение имеет согласованность отображаемой на планах информации. Дело в том, что в условиях работы с использованием бумажных карт в них неизбежно будут накапливаться расхождения. Иногда очень значительные. Использование электронных карт и многопользовательского доступа на данном этапе, помимо сокращения времени на проводимые работы дает еще очень ощутимый прирост качества исполняемых документов. В первую очередь – графических.

Слайд № 26

Программное обеспечение созданное в рамках ОКР «Андромеда-Д» предоставляет возможность применить новые способы работы командира и штаба по организации боя. В том числе – по организации взаимодействия.

Так, Использование средств «Электронная почты», реализация принципа многопользовательского доступа, а также использование функции «Карандаш» в графическом редакторе позволяет провести работу по организации взаимодействия методом «по карте» без сбора командиров подразделений.

Слайд № 27

Вообще говоря, в соответствии с законом зависимости способов управления от средств управления, при наличии комплекса средств автоматизации должны быть выработаны и использованы принципиально новые способы организации работы боевого состава, методы сбора, обработки, отображения и доведения информации. При этом, способы работы боевого состава командных пунктов, оснащенных средствами АСУ, будут иметь целый ряд принципиальных отличий от алгоритмов, применяемых на пунктах управления не имеющих таких средств.

Следует учитывать, что попытки использования «ручных» способов управления в автоматизированной системе могут привести не к ожидаемому сокращению цикла боевого управления, а к абсолютно обратному эффекту. Организация работы боевого состава обычными методами в условиях использования АСУВ может стать причиной превышения нормативных сроков подготовки к выполнению боевой задачи,

Слайд № 28

К счастью, командование ВДВ и абсолютное большинство командиров соединений и воинских частей это хорошо понимают и стремятся выработать и использовать в практической деятельности такие способы и методы. Естественно, с учетом и применительно к тем возможностям,

которые предоставляют им соответствующие аппаратно-программные средства.

Замечено, кстати, что желание военных использовать средства АСУВ прямо пропорционально простоте программных средств и степени дружелюбности их интерфейсов.

Слайд № 29

На следующем слайде представлена схема, иллюстрирующая достигнутое в системе общее сокращение организационной части цикла боевого управления, а также отдельных его этапов, применительно к уровню дивизии.

Слайд № 30

Что касается управления подразделениями и частями непосредственно в бою, то все те программные компоненты, о которых было рассказано выше, могут применяться и на этой стадии цикла. Кроме того, в составе комплекса ПО есть специальное средство, которое обеспечивает контроль положения объектов, имеющих средства глобального позиционирования на фоне топографической основы и нанесенной на нее тактической обстановки.

В качестве примера на данном слайде представлена фотография отображения в главном оперативном управлении ГШ ВС РФ (г.Москва) данных о бронеобъектах, действующих в ходе этапа розыгрыша при проведении командно-штабного учения с 7 дшд(г) на полигоне «Раевская» под Новороссийском.

Кстати, аналогичная трансляция осуществлялась в главное здание ГШ при проведении учения «Кавказ-2012» с полигона «Ашулук», а также в ходе проведения исследовательской КШТ с 98 вдд в декабре 2012 года из Ивановской области.

Слайды №№ 31-38

Это программа «Навигатор», которая обеспечивает в автоматическом режиме сбор и отображение данных о положении бронеобъектов и отдельных военнослужащих. При этом, трансляция этого отображения может быть во-первых осуществлена на неограниченные расстояния и на любой пункт управления, на котором будут развернуты соответствующие средства связи и аппаратно-программные комплексы.

Во-вторых, в комплексе с программой графического редактора оперативно-тактической обстановки, а также системой электронной почты можно вносить изменения в тактическую обстановку, применительно к конкретным действиям войск в реальном масштабе времени и обмениваться информацией с любым бронеобъектом, отображенным на карте. При этом адресация сообщения производится простым выделением нужного объекта непосредственно на экране.

Слайд № 39

Как я уже говорил, одним из приоритетных направлений в создании программного обеспечения для нас являлось создание полностью замкнутого автоматизированного разведывательно-огневого контура.

Эта задача в данный момент выполнена по следующим направлениям:

органы войсковой разведки – общевойсковой командир (начальник) – артиллерийский командир – огневое средство;

органы артиллерийской инструментальной разведки – общевойсковой (артиллерийский) командир – огневое средство;

общевойсковой командир (звена отделение, взвод, рота) – артиллерийский командир – огневое средство.

Слайд № 40

В данных направлениях применяются единые форматы обработки, хранения, отображения и передачи данных, что позволяет обмениваться разведданными об объектах поражения (целях) между всеми участниками данных направлений, причем как в направлении «снизу-вверх», так и по «горизонтали».

Слайды №№ 41-44

На слайдах представлен интерфейс программы «Навигатор», работающий в режиме целеуказания.

Таким образом, в подсистемах разведки, командира и штаба, а также в подсистеме огневого поражения происходит бесшовный обмен информацией об объектах огневого поражения, в том числе данных, полученных при помощи ДПЛА, лазерных дальномеров, (как артиллерийских, так и используемых войсковыми разведчиками), а также радиолокационных средств («Фара-СВ»).

Слайды № 45

В качестве выводов моего доклада представлены те возможности, которые предоставляются командирам всех степеней и другим должностным лицам нашим программным обеспечением, грамотное использование которых позволит существенно сократить цикл боевого управления.

А. А. Олимпиев,
ЗАО «Институт инфотелекоммуникаций»

Ю. М. Шерстюк
доктор технических наук, доцент, ОАО «Научно-исследовательский институт «Рубин»

ПРЕДЛОЖЕНИЯ ПО УСОВЕРШЕНСТВОВАНИЮ МОДЕЛИ ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ ОПЕРАТИВНО-ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ ИНФОТЕЛЕКОММУНИКАЦИЯМИ

В статье приведены рекомендации по развитию модели интерфейса пользователя в службе оперативно-технологического управления, базирующиеся на объектном представлении инфотелекоммуникационных сетей. Изложены предложения по применению дискриптивных описаний оконных форм интерфейса пользователя. Рекомендации направлены на гибкости и информационного охвата интерфейса пользователя.

Введение

Стремительное развитие мультисервисных инфотелекоммуникационных сетей (МИТКС), а также автоматизированных систем управления такими сетями (АСУС), обусловливает необходимость переосмысления существующего опыта разработки программных средств, предназначенных для визуального представления информационной модели управляемой сети связи.

В общемировой практике развития АСУС наблюдаются тенденции по переходу от систем, создаваемых в рамках концепций и стандартов Telecommunication Management Network (TMN), к системам функциональность класса Operation Support System (OSS) и далее к Business Support System (BSS) (см. например [1]). Перспективный переход от двухуровневой системы управления, состоящей из двух самостоятельных служб оперативно-технического и технологического управления к комплексному решению — службы оперативно-технологического управления инфотелекоммуникациями (СОТУ ИТК) — описан, например в [2].

В качестве средства построения информационной модели СОТУ ИТК может быть положен подход, описанный в [3], базирующийся на сочетании учетной и объектной моделей представления МИТКС с учетом гетерогенности ее компонентов. Объектная модель предполагает представление МИТКС в виде множества взаимодействующих объектов (абстрактных автоматов). Каждый объект является экземпляром некоторого класса, который в свою очередь является описателем логического или физического элемента сети, то есть поставлен ему в соответствие. Эффективное применение данного подхода во многом зависит от того, какие возможности предоставляет интерфейс пользователя средств СОТУ ИТК по визуализации объектов и существующих между ними отношений с позиций полноты и адекватности отображаемых сведений, способов и форм отображения этих сведений, доступных операций навигации по элементам объектной модели. С этих позиций интерес может представлять формальная модель интерфейса пользователя, учитывающая его соотношение с элементами объектной модели.

Рекомендации по расширению формальной модели интерфейса пользователя

Формальная модель интерфейса пользователя, описанная в [4], при переходе к оператив-

но-технологическому управлению инфотелекоммуникациями становится недостаточной, так как рассчитана на строго иерархическую модель представления сети. Однако она может быть расширена посредством внедрения дополнительных методов отображения.

В общем случае, множество объектов, составляющих объектную модель МИТКС, должно представлять собой лес – множество иерархий, каждая из которых имеет одну и только одну корневую вершину. Каждая из таких иерархий соответствует одной из точек зрения на структуру МИТКС. Примером иерархии могут служить, например:

- организационная структура МИТКС;
- логическая структура МИТКС;
- физическая топология МИТКС;
- потребители, службы, услуги и другие.

Любой объект может быть рассмотрен с разных позиций и, следовательно, должен иметь соответствующие бинарные отношения с объектами разных иерархий.

В каждой иерархии, выступающей в качестве наиболее общего объекта мониторинга с точки зрения организации сети, в общем случае, могут быть узлы связи (УС) и узлы коммутации (УК). Предполагается, что любой узел коммутации всегда находится в зоне ответственности одного и только одного УС. Тогда все объекты могут быть представлены следующими методами визуализации:

1. Отображение МИТКС в целом (представление иерархии на схеме сети):

– УС либо объекты, являющиеся их компонентами (внутриузловые объекты);

– объекты, соответствующие линиям, каналам, трактам и т.д. между узлами (межузловые коммуникационные объекты);

– объекты, агрегирующие внутриузловые и/или межузловые коммуникационные объекты (сеть телефонной связи, сеть линий прямой связи и т.д.) (межузловые агрегирующие объекты).

2. Отображение физической структуры УС (представление иерархии на схеме УС):

– УК либо объекты, являющиеся их компонентами (оборудование, размещенное внутри стойки, блок внутри оборудования и т.п.);

– объекты, соответствующие линиям, каналам, трактам и т.д. между узлами коммутациями (внутриузловые коммуникационные объекты);

– объекты, соответствующие исходящим и входящим направлениям информационного обмена (межузловые коммуникационные объекты).

3. Отображение в виде иерархии одного из поддерживаемых типов.

Для визуального отображения каждого отдельного объекта, принадлежащего некоторому классу, может быть выбран механизм, применяющийся для визуализации классов сетевых элементов уровня технологического управления. Данный механизм описан в [5] и предполагает включение в информационную модель метаописаний экранных форм, позволяющих управлять экранными формами без изменения программного кода пользовательских приложений.

Согласно предлагаемому механизму описание интерфейса пользователя для отображения состояния объекта в интерактивном приложении представляет собой совокупность сведений декларативного характера, посредством интерпретации которых интерактивное приложение осуществляет взаимодействие с пользователем.

Структура интерфейса пользователя может быть представлена ориентированным графом, вершинам которого соответствуют экранные формы, а переходам – возможные смены форм. Формы содержат различные элементы управления, предусмотренные разработчиком компонентов метаинформации – кнопки, таблицы, списки выбора и т.д.

Общая схема ведения диалога с пользователем может быть описана следующим образом:

– выполняется создание экранной формы (фрейма или окна диалога) и имеющихся в ней компонентов;

– выполняется запрос к серверу для получения значений всех параметров объекта и его отношений с другими объектами, ссылки на которые имеются в описании действий по инициализации компонентов формы – результатом выполнения этого запроса является ассоциативный список имен-значений объектов и параметров;

– обрабатываются описания действий по инициализации компонентов формы;

– обрабатываются события, инициируемые пользователем над управляющим компонентами формы – при наличии описания действий как реакции на эти события.

В качестве реакции могут быть, в частности, использованы:

– закрытие формы – завершение ее работы и передача управления обработчику событий вызывающей (старшей) формы;

– вызов другой формы – возможно, с передачей ей параметров;

– выполнение воздействия на объект (например, установка флага о игнорировании объекта при вычислении состояний контейнеров) – как вызов соответствующей функции сервера.

Интерактивное приложение осуществляет буферное хранение описаний интерфейсов пользователя. Каждый раз, когда такое описание должно быть обработано, проверяется наличие описаний экранных форм данного класса объектов в буфере, и при отсутствии такового происходит обращение к серверу для его получения.

Заключение

Предлагаемые решения позволяют расширить возможности программных средств, предоставляющих пользовательский интерфейс к объектной модели МИТКС, а также сделать данные программные средства более гибкими и адаптированными к изменениям структуры МИТКС и применяемым классам технических средств.

СПИСОК ЛИТЕРАТУРЫ

1. **Гребешков А.Ю**. Стандарты и технологии управления сетями связи [Текст] : Рукопись. – М.: Эко-Трендз, 2003. – 288 с.

2. **Шерстюк Ю.М.** Оперативно-технологическое управление инфотелекоммуникациями [Текст] / Шерстюк Ю. М., Воронков К.Л., Олимпиев А.А., Рожнов М.Д. // Телекоммуникационные технологии. 2010. Вып. 6. С. 109-121.

3. **Олимпиев А.А.** Унификация представления сетей связи на основе объектного подхода [Текст] / Олимпиев А.А., Рожнов М.Д., Шерстюк Ю.М. // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России-2007 (ИБРР-2007)», Санкт-Петербург, 23-25 октября 2007 г.: Труды конференции, секция Информационная безопасность телекоммуникационных сетей. – СПб.: СПОИСУ, 2008, с.60-66.

4. **Олимпиев А.А.** Отображение объектной модели сети связи в интерфейсе пользователя [Текст] / Олимпиев А.А., Шерстюк Ю.М. // Телекоммуникационные технологии. 2007. Вып. 3. С.28-33.

5. **Шерстюк Ю. М.** Архитектура средств технологического управления телекоммуникациями [Текст] / Шерстюк Ю. М., Зарипов В. Д., Рожнов М.., Савельев И. Л. // Телекоммуникационные технологии. 2006, вып. 2, инв. В-3547. С.33-40

А.Н. Павлов
Федеральное государственное казенное военное образовательное учреждение высшего профессионального образования «Военная академия войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А.М. Василевского» Министерства обороны Российской Федерации

К ВОПРОСУ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЛЕКСАХ СРЕДСТВ АВТОМАТИЗАЦИИ ВОЙСКОВОЙ ПВО

В статье обоснована актуальность применения современных информационных технологий в аспекте компьютерных форм, описаны свойства защищенности информационных ресурсов, представлена классификация угроз защищенности системы при применении нарушителем несанкционированных воздействий и возможные последствия их успешной реализации относительно основных свойств защищенности. Представлена классификация уязвимостей аппаратных и программных средств компонентов распределенной вычислительной системы.

Осознание на государственном уровне важности и необходимости защиты информационных ресурсов различной степени секретности от разнообразных форм и способов несанкционированных воздействий и непреднамеренных действий должностных лиц явилось основанием для появления и дальнейшего развития федерального законодательства, к которому, в первую очередь, относится действующий уголовный кодекс, а также Федеральные законы: «О государственной тайне» от 21 июля 1993 г. №5485-1, «Об информации, информатизации и защите информации» от 25 января 1995 г. (25 февраля 1995 г.) № 24-ФЗ, «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. № 149-ФЗ и другие. Следует отметить, что в уголовном кодексе преступления в сфере компьютерной информации относятся к преступлениям против общественной безопасности и общественного порядка. В иерархии приоритетных направлений уголовного законодательства составы преступлений, регламентирующие данную главу 28 расположены в уголовном кодексе ранее преступлений, совершенных против государственной власти. Это позволяет сделать вывод о том, что преступления в сфере компьютерной информации являются более приоритетным направлением на стыке гуманитарных и технических предметных областях.

Неотвечающий потребностям практики уровень защищенности системы является серьезным препятствием для применения ПЭВМ с секретной (конфиденциальной) информацией.

В условиях современного развития Вооруженных Сил в части автоматизации процесса выработки и принятия решений необходим поиск новых путей и способов качественного функционирования органов управления, в особенности оперативных звеньев. При этом возрастает актуальность проблемы информационной защиты ресурсов, циркулирующих в комплексах средств автоматизации (КСА) войсковой ПВО, которая, в частности, обусловлена:

возрастающим значением в достижении целей вооруженного противоборства параметров защищенности ресурсов органов военного управления;

существующим противоречием между возможностями систем защиты информационных ресурсов распределенных вычислительных систем и задачами, стоящими перед ними в процессе подготовки и в ходе вооруженного противоборства с противником;

современным состоянием научно-методического аппарата оценки эффективности защиты информационных ресурсов распределенных КСА войсковой ПВО не обеспечивающим рациональную реализацию функций поддержания его параметров на заданном уровне;

недостаточным развитием теории и практики защиты информационных ресурсов КСА войсковой ПВО и отсутствием рекомендаций по практической реализации комплекса мер, направленных на поддержание их защищенности.

Учитывая, что в основу функционирования КСА положены процессы приема, обработки, преобразования и передачи информационных ресурсов различной степени секретности между автоматизированными рабочими местами должностных лиц органов управления распределенной вычислительной системы, практическое внедрение связано с обеспечением безопасности обмена этих циркулирующих ресурсов, то есть их защиты от несанкционированных воздействий внешнего и внутреннего нарушителя (посредством непреднамеренных действий должностных лиц органов управления). Информационные ресурсы представляют собою непосредственно хранящиеся и циркулирующие в системе сами данные, а также аппаратные и программные средства (алгоритмы, программы, процедуры) технологии процессов их сбора, передачи, обработки, хранения и использования на автоматизированных местах должностных лиц органов управления.

Основанием для построения комплексной защищенной системы и, как следствие, повышения эффективности защиты информационных ресурсов различной степени секретности (конфиденциальности) являются факторы, представленные рисунком 1.

Разнесенность компонентов распределенной вычислительной системы, интенсивный обмен информационными ресурсами между ее сегментами с использованием стандартных протоколов передачи, участие в процессе обработки большого количества должностных лиц, имеющих различные степени допуска к ресурсам, а также отсутствие в системе необходимой поддержки интегрированных встроенных средств защиты является основополагающим фактором, в общем смысле называемым – особенности информационного обмена.

Проведенный анализ моделей обеспечения безопасности информационных ресурсов КСА показывает, что любая автономная или в составе системы ПЭВМ является уязвимой без достаточного количества установленных средств защиты. Нарушитель использует несанкционированный доступ с целью дальнейшего разглашения семантической составляющей информации относительно свойств защищенности информационных ресурсов – доступности, целостности и конфиденциальности (рис. 2). Доступностью является свойство системы, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующим им информационным ресурсам и готовностью соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов.

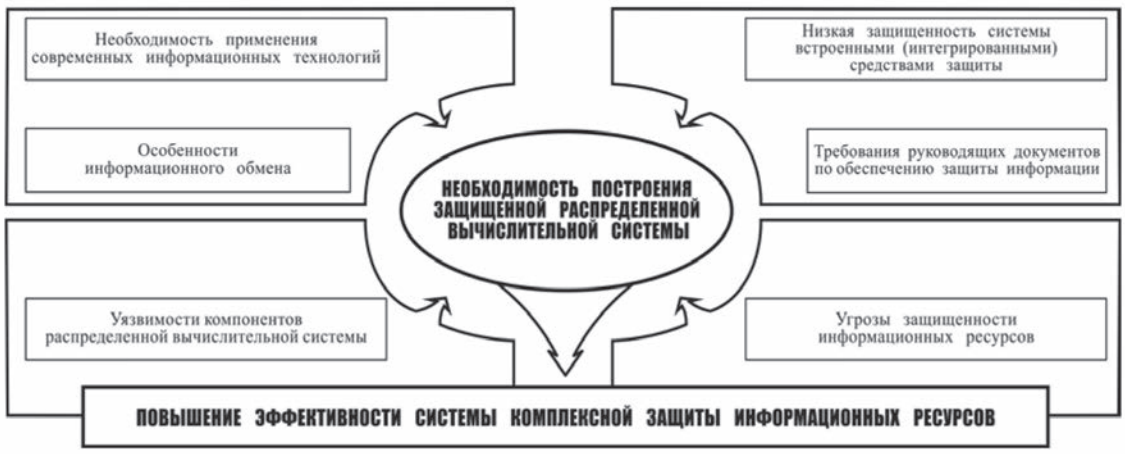


Рис. 1. Факторы, определяющие необходимость построения и повышения эффективности системы комплексной защиты КСА

Рис. 2. Круговые схемы Эйлера, описывающие свойства защищенности информационных ресурсов

Целостностью называется свойство информационных ресурсов, заключающееся в существовании в неизменном по отношению к некоторому фиксированному состоянию в процессе их хранения и перемещения. Конфиденциальность – свойство информационных ресурсов, определяющее статус важности, указывает на необходимость введения ограничений на круг субъектов, имеющих право доступа и определяет требуемую степень их защищенности в тайне от субъектов, не имеющих полномочий на их использование. Защищенной системой является система, с установленными средствами защиты, успешно и эффективно противостоящая несанкционированным воздействий нарушителя.

В ограниченном количестве, имеющейся в распределенной вычислительной системе, встроенных средств защиты используются стандартные методы и механизмы защиты, которые не в полной мере способны эффективно противостоять разнообразным способам и методам несанкционированных воздействиям. Это является следствием противоречия между возросшей необходимостью расширения сфер применения ПЭВМ и недостаточным качеством решения задач по обеспечению защиты информационных ресурсов.

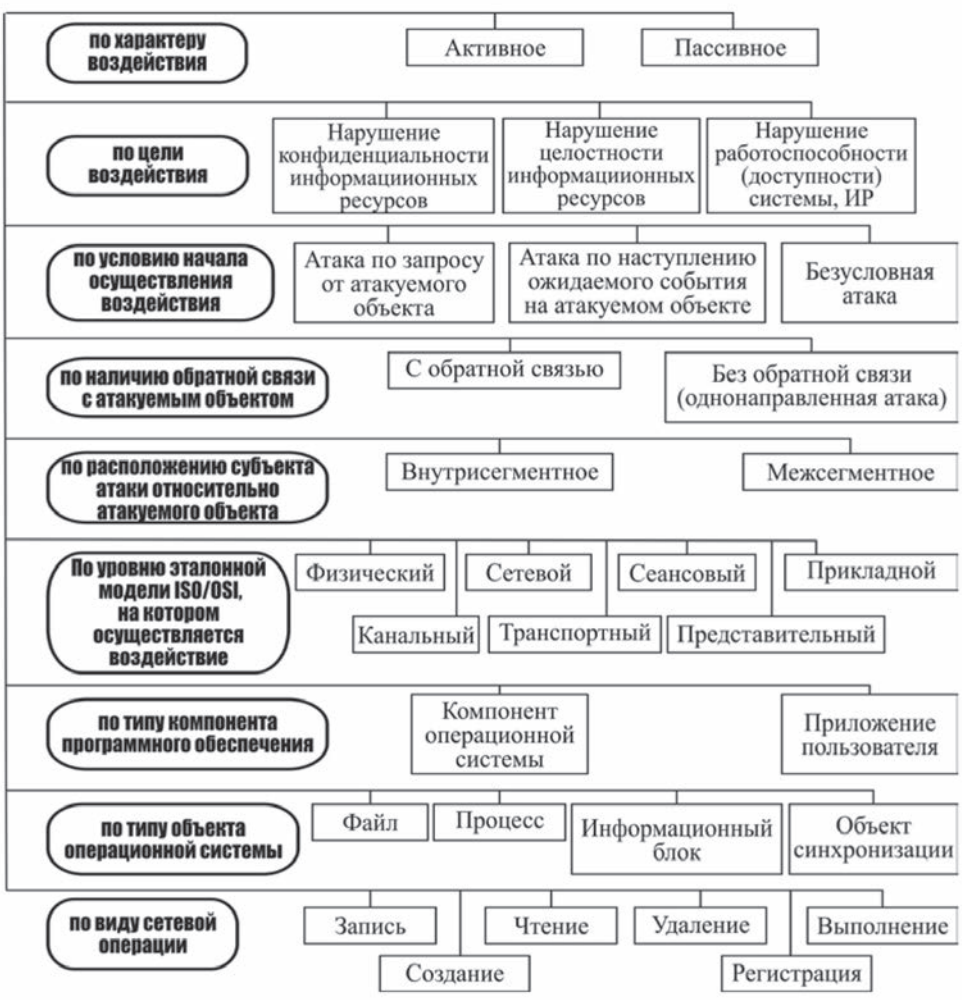


Рис. 3. Классификация угроз защищенности информационных ресурсов

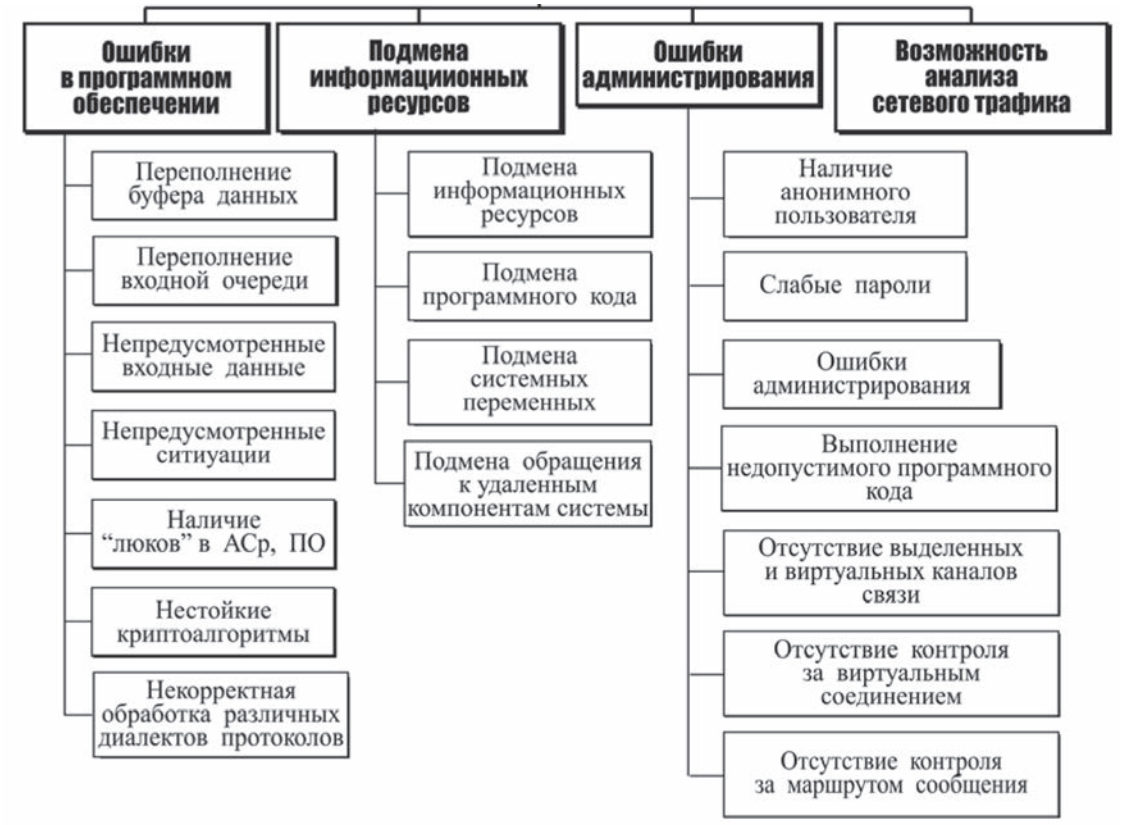


Рис. 4. Классификация уязвимости компонентов распределенной вычислительной системы

Изменение установленных в системе свойств защищенности информационных ресурсов достигается реализацией нарушителем угроз (рис. 3) посредством несанкционированных воздействий с целью их модификации (изменения), блокирования (нарушение функционирования аппаратных и программных средств) компонентов распределенной вычислительной системы, копирования (разглашения), уничтожения (удаление без возможности восстановления). Под угрозой защищенности системы подразумевается потенциальная возможность нарушения основных свойств защищенности информационных ресурсов.

Несанкционированные воздействия нарушителя направлены на уязвимости компонентов КСА (аппаратные средства и программное обеспечение) распределенной вычислительной системы (рис. 4).

Уязвимость системы – это свойства аппаратных и программных средств системы, на которые может воздействовать нарушитель при реализации несанкционированных воздействий, приводящие к нарушению ее защищенности.

Защита информационных ресурсов от несанкционированных воздействий и непреднамеренных действий должностных лиц достигается перекрытием уязвимостей системы посредством применения совокупности способов и методов информационной защиты, реализованных в средствах защиты относительно свойств защищенности системы.

Различные методы защиты информационных ресурсов реализованы в сертифицированных средствах защиты. Одной из важнейших задач повышения эффективности защиты информационных ресурсов КСА и в последующем синтеза системы комплексной защиты является выбор из множества имеющихся таких средств защиты, которые позволяют получить наиболее рациональную структуру системы защиты.

Таким образом, научная статья отражает описание актуальной задачи в развитии форм оперативно-тактической подготовки.

М.А. Перегудов
А.А. Бойко
кандидат технических наук, доцент
НИИЦ РЭБ ВУНЦ ВВС «ВВА им. проф. Н.Е Жуковского и Ю.А. Гагарина» (г. Воронеж)

ОБ АДАПТИВНОЙ ЗАЩИТЕ ТРАНКОВЫХ СЕТЕЙ СВЯЗИ СТАНДАРТА TETRA ОТ ДЕСТРУКТИВНОГО ПРОГРАММНОГО ВОЗДЕЙСТВИЯ

Предложен подход к организации адаптивной защиты транковых систем связи (ТрСС) стандарта TETRA от деструктивного программного воздействия (ПВ), нацеленного на технологические уязвимости этих систем в процедуре множественного доступа к радиоканалу.

Введение

Одним из наиболее востребованных стандартов ТрСС для создания сетей связи служб безопасности, спасения, вооруженных сил, полиции в настоящее время является TETRA [1, 2]. Процедура множественного доступа абонентских терминалов (АТ) ТрСС стандарта TETRA к радиоканалу уязвима для деструктивного ПВ. Она не предусматривает аутентификации и позволяет осуществлять семантический анализ передаваемых в эфире служебных данных канального уровня эталонной модели взаимодействия открытых систем. Подходы к устранению таких технологических уязвимостей не известны. Поэтому задача разработки адаптивной защиты ТрСС стандарта TETRA от деструктивного ПВ, использующего уязвимости в процедуре множественного доступа к радиоканалу, является актуальной.

Основная часть

Процедура случайного доступа в сетях связи, построенных по принципу макро/микросотовой структуры, предназначена для инициализации передачи служебной информации от абонентов к средствам управления и коммутации сети.

Отличительными особенностями процедуры случайного доступа ТрСС стандарта TETRA являются присваивание каждому АТ одного из четырех кодов доступа (A, D, C, D), с помощью которых возможно реализовать вертикаль подчиненности между АТ, а также семи приоритетов сообщений сигнализации, отвечающих за инициализацию всех транзакций в сети [3]. Для адаптивного управления коллизиями в общем канале сигнализации процедурой случайного доступа предусмотрено два сообщения управления: ACCESS-DEFINE и ACCESS-ASSIGN, которые широковещательно передаются базовой станцией (БС). Вариация значений параметров указанных сообщений непосредственно влияет на эффективность функционирования ТрСС стандарта TETRA.

Сообщение ACCESS-DEFINE содержит информацию: о привязке к коду доступа приоритета сообщения сигнализации и возможных идентификационных данных АТ; параметр разрешения немедленного доступа для первой передачи; время ожидания повторного запроса случайного доступа; разрешенное число повторений произвольного доступа; умножающий фактор поиска следующего кадра. Коды доступа в сообщении ACCESS-DEFINE по мере необходимости динамически меняются БС оператором сети.

Сообщение приглашения к доступу ACCESS-ASSIGN содержит карту доступа соответствующих восходящих временных интервалов для каждого кадра. Таким образом, приглашение относится только к тем АТ, которым присвоен соответствующий код в ACCESS-DEFINE.

В соответствии с [3] в ТрСС стандарта TETRA процедура случайного доступа состоит из широковещательной рассылки БС в общем канале сигнализации сообщений ACCESS-ASSIGN в каждом нисходящем пакете (временном интервале) и сообщений ACCESS-DEFINE, периодичность рассылки которых определяется оператором сети связи. С учетом информации, содержащейся в данных сообщениях, АТ по восходящему каналу сигнализации отправляет запрос о случайном доступе, содержащий информацию о необходимом временном ресурсе для дальнейшей отправки сообщения сигнализации зарезервированным доступом. Затем АТ ожидает ответ от БС, сканируя нисходящий трафик. Получив подтверждение случайного доступа, АТ отправляет сообщение сигнализации заданного приоритета в ACCESS-DEFINE в восходящем временном интервале, заданным в ACCESS-ASSIGN, и ожидает ответа от БС. Например, сообщением сигнализации может быть команда об установлении соединения или об окончании сеанса связи. В процессе передачи сообщения сигнализации одним АТ возможна конфликтная ситуация, когда другой АТ передает сообщение в том же временном ресурсе. БС может разрешить этот конфликт в пользу одного из АТ, передав ему ответ на сообщение сигнализации. После этого процедура случайного доступа считается завершенной.

В таких условиях возможны следующие алгоритмы деструктивных ПВ.

Алгоритм 1 (фальсификация запроса на соединение)**.**

Шаг 1. Поиск в ходе анализа трафика в нисходящем канале сигнализации ответов от БС о подтверждении доступа легитимным АТ.

Шаг 2. Использование выделенного легитимной АТ временного ресурса для отправки фальсифицированного сообщения сигнализации. К примеру, производится отправка сообщения с запросом на повторное установление соединения. При этом идентификационные данные нелегитимного и легитимного АТ должны отличаться. Поскольку БС не может идентифицировать АТ, запрашивающий повторное соединение, она это соединение отвергает.

Шаг 3. Если время деструктивного ПВ не исчерпано, переход к шагу 1.

Алгоритм 2 (непредставление ответа на соединение)**.**

Шаг 1. Копирование в ходе анализа трафика в нисходящем канале сигнализации запросов о получении доступа легитимных АТ.

Шаг 2. Отправка фальсифицированных запросов о доступе во временных интервалах, выделенных легитимным АТ. При этом ответы на данные запросы должны прийти в нисходящих временных интервалах, определяемых восходящими временными интервалами и значениями параметра WT сообщения ACCESS-DEFINE. БС идентифицирует АТ, обрабатывает полученные запросы и, не подозревая их ложность, сообщает по нисходящему каналу ответы о подтверждении случайного доступа, содержащие информацию о выделенных временных ресурсах на восходящем канале сигнализации.

Шаг 3. Игнорирование полученных ответов в течение заданного времени.

Шаг 4. Если время деструктивного ПВ не исчерпано, переход к шагу 1.

Алгоритм 3 (комбинированный).

Выполняется алгоритм 2, но вместо игнорирования ответов о подтверждении случайного доступа выполняется модифицированный алгоритм 1, в котором на БС отправляются фальсифицированные сообщения сигнализации от имени множества одних легитимных АТ на установление соединений с коммутацией каналов с равным по численности множеством других легитимных АТ. В результате БС отправляет сообщение о согласии на установление требуемых соединений. При этом выделяются частоты из имеющегося частотного ресурса и БС сообщает об этом легитимным АТ, «инициировавшим» запрос на установление соединения. В результате множество легитимных АТ, получив сообщения о выделении им частотного ресурса, игнорируют эти сообщения. Таким образом, алгоритм 3 позволяет в течение заданного времени за счет нарушения доступности легитим-

ных АТ к временному и частотному ресурсу снижать эффективность функционирования ТрСС.

Исходя из этого, предлагается использовать адаптивную защиту ТрСС стандарта TETRA от деструктивных ПВ, маскирующую процедуру установления соединения АТ.

Адаптивную защиту предлагается основывать на системе показателей эффективности функционирования ТрСС стандарта TETRA. Система включает интегральный, определяемый для организованной системы связи в целом, и частные показатели эффективности, определяемые для каждой конкретной процедуры использования случайного доступа АТ. Для алгоритма 1 частным показателем эффективности функционирования легитимного АТ будем считать отношение количества инициированных им и не блокированных запросов на доступ к общему количеству запросов этого АТ в течение времени деструктивного ПВ. Для алгоритма 2 показателем эффективности легитимного АТ будет результат отношения выделенного этому АТ и используемого им временного ресурса к общему выделенному ему временному ресурсу в течение деструктивного ПВ. Для алгоритма 3 показатель будет определяться аналогично показателю алгоритма 2 с учетом частотного ресурса. Интегральный показатель будет определяться как среднее арифметическое всех частных показателей за интервал времени, в течение которого реализуется деструктивное ПВ. Значения показателей подсчитываются и запоминаются в БС.

Значение интегрального показателя эффективности функционирования ТрСС стандарта TETRA предлагается контролировать в режиме реального времени. Если оно станет ниже порогового значения, установленного на основе статистических данных о результатах функционирования ТрСС в нормальных условиях, то случайным образом из интервала 1..3 будет сгенерировано значение функции смещения значений кодов доступа и приоритетов сообщений сигнализации (в нормальных условиях функционирования сети данное значение будет равно нулю). Каждое значение функции смещения предлагается, не изменяя структуру кадра, присваивать значению параметра рассылаемого БС сообщения ACCESS-DEFINE, которое не используется для управления коллизиями в процедуре случайного доступа.

Если значение обобщенной эффективности остается ниже порогового в течение заданного временного интервала, то функция смещения случайным образом меняет свое значение на любое из оставшихся чисел из интервала 1..3.

В случае превышения значением интегрального показателя эффективности порогового значения (или равенства ему), функция смещения меняет свое значение на ноль, что сигнализирует о переходе ТрСС стандарта TETRA в штатный режим функционирования.

Изменяя значения функции смещения кодов доступа и приоритетов сообщений сигнализации адаптивная защита ТрСС стандарта TETRA позволяет идентифицировать злоумышленника и блокировать направленные с его стороны деструктивные ПВ, описанные алгоритмами 1-3.

Реализация предлагаемой адаптивной защиты ТрСС стандарта TETRA, позволяющей определять изложенные выше деструктивные ПВ, может быть представлена в виде трех взаимосвязанных блоков программного кода.

В **блоке 1** сравнивают содержащиеся в сообщении ACCESS-ASSIGN значения выделенных временных интервалов восходящего канала сигнализации со значениями временных интервалов, в течение которых были переданы запросы о получении случайного доступа от АТ с учетом текущего значения функции смещения. Если значения совпадают, то запросы переданы легитимными АТ, в противном случае имеет место факт деструктивного ПВ.

В **блоке 2** защиты сравнивают количество содержащихся в сообщении ACCESS-DEFINE временных интервалов, требуемых для отправки сообщения сигнализации с заданным приоритетом, с количеством временных интервалов, содержащихся в запросе на получение доступа АТ. Если значения совпадают, то запросы переданы легитимными АТ, в противном случае имеет место факт деструктивного ПВ. Для повышения достоверности распознавания запросов предлагается для каждого приоритета сообщения сигнализации ввести однозначно определяющее количество временных интервалов.

В **блоке 3** сравнивают значения приоритетов сообщений сигнализации, содержащиеся в сообщениях ACCESS-DEFINE, со значениями

приоритетов сообщений, передаваемых по общему каналу сигнализации. Если значения совпадают, то сообщения переданы легитимными АТ, в противном случае имеет место факт деструктивного ПВ.

Если в восходящем временном интервале содержится запрос о получении случайного доступа АТ, то для определения его легитимности задействуются блоки 1, 2. Для блокирования деструктивного ПВ достаточно, чтобы хотя бы один из этих блоков определил фальсифицированный запрос о получении доступа. В случае определения блоком 3 в восходящем временном интервале ложного сообщения сигнализации, БС игнорирует данное сообщение.

Заключение

Таким образом, предложен подход к организации адаптивной защиты ТрСС стандарта TETRA, позволяющий с учетом результатов контроля интегрального и частных показателей эффективности функционирования сети в режиме реального времени блокировать деструктивные ПВ, нацеленные на использование технологических уязвимостей этих систем в процедуре множественного доступа к радиоканалу.

СПИСОК ЛИТЕРАТУРЫ

1. Чивилев С. Профессиональная радиосвязь на предприятии // http://www.m-forum.ru/news/article/062756.htm [Интернет-ресурс]. Дата обращения: 02.05.13.

2. Молдаванов А. Безопасность как стиль жизни – стандарт XXI века // http://www.connect.ru/journal_archieve.asp?journalid=508 [Интернет-ресурс]. Дата обращения: 02.05.13.

3. EN 300 392-2 V3.4.1 (2010-08). Terrestrial Trunked Radio (TETRA). Voice plus Data (V+D). Part 2: Air Interface (AI) // http://pda.etsi.org/ [Интернет-ресурс]. Дата обращения: 15.10.2012 г.

4. Система ELETTRA. 1999 г. // http://www.osp.ru/nets/1999/04/144021/ [Интернет-ресурс]. Дата обращения: 10.09.2012 г.

А.В. Сафонов
Кандидат технических наук, доцент

Д.Ю. Щетинин
Тюменское высшее военно-инженерное командное училище

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ПРОТИВОБОРТОВОЙ МИНОЙ ТМ-83

В статье обосновывается целесообразность разработки нового устройства управления инженерным боеприпасом. Актуальность работы в данном направлении определяется рядом критичных недостатков существующей системы управления боеприпасом. Приведен один из подходов для решения задачи определения момента начала вычислительной процедуры. Решение на приведение в действие принимается на основе корреляционной обработки. Приведены оценки вероятности принятия решения.

В настоящее время все более необходима замена устаревающих образцов инженерного вооружения в инженерных войсках России. Особенно это актуально применительно к инженерным боеприпасам (минам), а именно – в части касающейся алгоритмов приведение их в действие. Вследствие не всегда возможного финансирования вновь разрабатываемых проектов становится актуальной модернизация исполнительных и командно-передающих приборов указанных выше боеприпасов, преимущественно предназначенных для уничтожения автобронетанковой техники.

Поэтому целью статьи является описание метода селекции подвижных объектов по их двумерному изображению в интересах повышения избирательности инженерного боеприпаса.

Авторами предлагается провести усовершенствование комплекта мины ТМ-83, которая предназначена для уничтожения автобронетанковой техники противника. Известно, что данная мина в своем составе имеет два датчика: сейсмический и инфракрасный. Таким образом, при пересечении линии прицеливания тяжелой техникой происходит выдача сигнала командно-передающим прибором (КПП) сигнала на подрыв. Уничтожение объекта коммулятивной струей происходит вне зависимости от того, какого типа объект пересек линию прицеливания. Однако возможны ситуации, когда требуется из состава колонны уничтожить строго определенный тип техники вне зависимости от его нахождения в составе колонны (причем это не всегда танк). Для решения данной задачи авторами предлагается дополнить комплект мины инфракрасной камерой низкого разрешения и программным вычислителем (Рис. 1.)

Принцип функционирования комплекта будет заключаться в следующем. Сигнал в инфракрасном диапазоне длин волн от цели поступает на вход видеомодуля. Сигнал в видеомодуле представляет собой матрицу

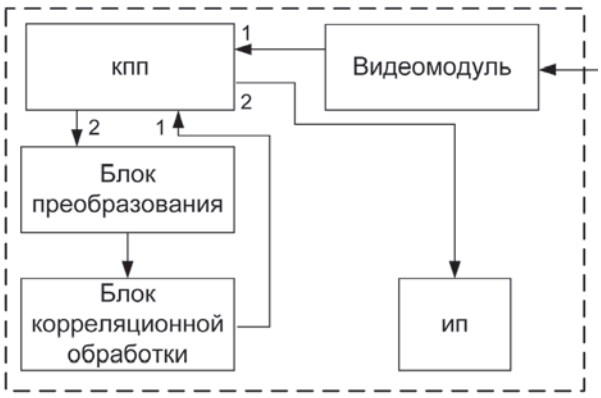


Рис. 1. Модернизованный комплект мины

цифровых значений элемента изображения. Причем каждый элемент матрицы содержит некоторое число, соответствующее значению яркости элемента цели. Таким образом, можем записать сигнал, имеющий в своем составе полезную информацию о цели как некоторую функцию от двух аргументов – номера столбца y и строки x

$$S = M_{x,y}.$$

Сигнал с выхода видеомодуля поступает на первый вход КПП, который передает (транслирует) данный сигнал на вход блока преобразования. Сигнал с выхода видеомодуля представляет собой сигнал, продискретизированный по времени и квантованный по амплитуде. Шаг квантования по амплитуде равен единице (разница между соседними значениями яркости). Шаг дискретизации по времени определяется шагом изменения порядкового номера смежных ячеек матрицы. Определимся, что формирование вектора яркости осуществляется по правилу

$$s_n = \bigcup_{x=1}^{X} \bigcup_{y=1}^{Y} \left(M_{x,y} \right),$$

где X – максимальное число столбцов, Y – максимальное число строк, $n = XY$.

Уровни квантования могут изменяться в зависимости от числа возможных значений яркости используемого видеомодуля.

Известно, что при анализе степени схожести сигналов используют взаимокорреляционную функцию, записываемую для сигналов $s_1(t)$ и $s_2(t)$ в следующем виде

$$R_{12}(\theta) = \int_{-\infty}^{\infty} s_1(t) s_2(t+\theta) dt.$$

В нашем случае сигнал, во-первых, является дискретным. Во-вторых необходим второй сигнал, с которым мы будем сравнивать тот, что получен из изображения на входе видеомодуля. В качестве данного сигнала мы будем использовать эталоны, которые на этапе проектирования заранее будут запоминаться в памяти блока корреляции. Следовательно, указанная выше формула может быть записана, в виде

$$R_{12}(\theta) = \sum_{n=1}^{N} s'_n s_{n-\Theta},$$

здесь Θ – смещение на один отсчет принятой реализации сигнала, s'_n – эталонный дискретный сигнал, полученный при моделировании.

Сигнал с выхода блока корреляционной обработки поступает на второй вход КПП, в котором полученное значение сравнивается с имеющимся в памяти. В случае, если сигналы будут максимально схожи, значение взаимокорреляционной функции будет максимальным, в противном случае – минимальным, либо значительно меньше граничного, при превышении которого КПП принимает решение в пользу κ-й цели. Если на этапе подготовки комплекта КПП заранее запрограммирован так, что при превышении порога выдается сигнал на приведение в действие исполнительного прибора.

Для получения оценок вероятности распознавания целей на изображении проводилось математическое моделирование (ММ).

В процессе моделирования решались три смежных задачи – обнаружение объекта, определение момента принятия решения и, собственно, принятие решения на приведение мины в действие. Моделировались ситуации пересечения линии прицеливания тремя типами объектов – танком, БМП и транспортным автомобилем. В качестве фоновых использовались тепловизионные изображения объектов для наиболее вероятных типов местности: лесистой, степной, городской и гористой. Также имитировалось движение объекта в кадре. Движение задавалось различным положением самого объекта относительно центрального столбца изображения (Рис. 2).

Двумерное изображение соответствовало по характеристикам тепловизионному модулю с разрешением 640×480 точек. Для определения наличия цели в кадре использовался профиль яркости (ПЯ) (Рис. 3). Вектор ПЯ формировался из строки с номером $Y/2$. Однако выбор средней строки не всегда приводил в положительному результату. Это следовало из того, что положение центра кадра относительно края полотна дороги не всегда выставляется точно.

Поэтому положение объекта по его профилю определялось автоматически, для чего использовался следующий алгоритм:

1. Формировался ПЯ $p(y)$ для всех строк матрицы изображения.

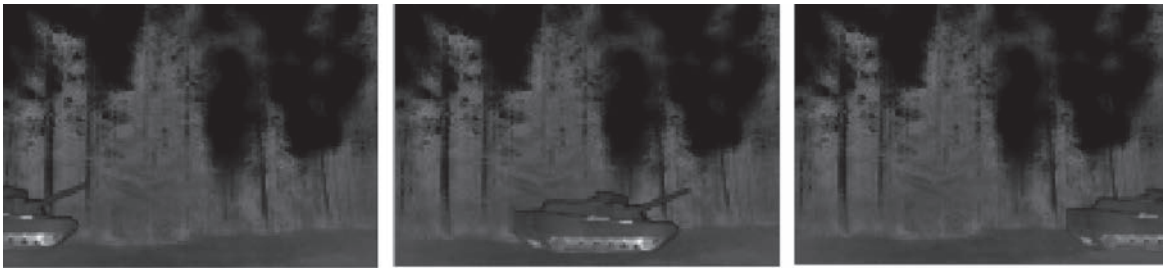


Рис. 2. Пример изображения участка местности с имитацией движения танка

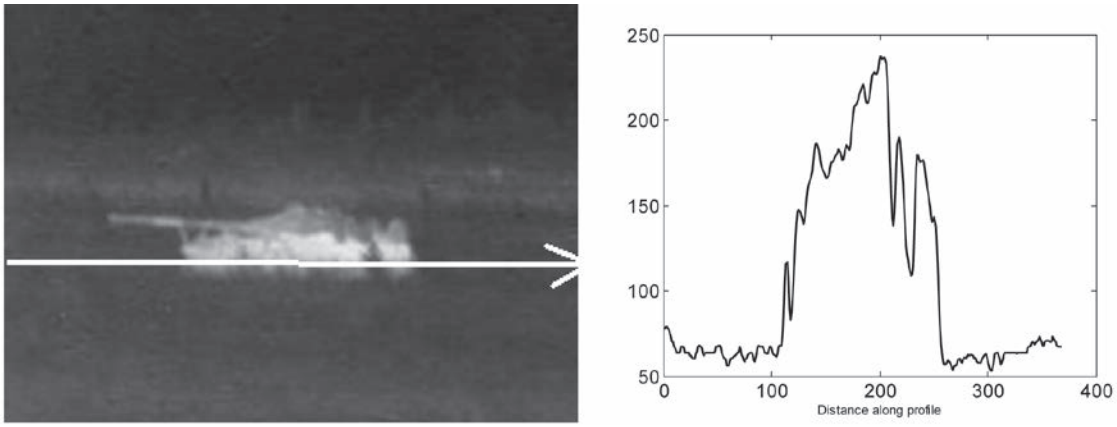


Рис. 3. Изображение танка, путь построение ПЯ и вектор ПЯ

2. Проводился поиск элементов ПЯ со значениями более 0,707 от максимального – $\tilde{p}(y)$.

3. Проводится поиск следующих за найденным элементов вектора со значениями равными или большими найденного.

4. Подсчитывались найденные элементы.

5. Если значение элемента смежного с запомненным меньше, то подсчитывалась протяженность разрыва. Если она составляла менее 30 элементов и падение яркости не более чем 18-20 единиц (10%), то протяженность интервала включалась в общую сумму. Если условия не выполнялись, то подсчет начинался заново.

6. Предварительное решение о наличии объекта в кадре принималось в случае, если число элементов со значением яркости $\tilde{p}(y)$ (для длины строки 480 точек).

7. Осуществлялось построение ПЯ по столбцам матрицы изображения.

8. Проводился поиск элементов со значениями более 130.

9. Проводился поиск следующих за найденным элементов профиля со значениями равными или большими найденного.

10. Осуществлялся подсчет найденных элементов.

11. Осуществлялся расчет по аналогии с п.5, за исключением того, что число элементов разрыва уменьшалось вдвое, так как протяженность самого профиля по вертикали меньше.

12. Вычислялось отношение протяженности интервала с максимумами яркости, рассчитанному в п. 11 к величине, рассчитанной в п. 5. Если полученное значение находится в интервале 0,9...1, то принималось решение, что на кадре засветка. В противном случае принималось решение о наличии объекта в кадре.

Немаловажным являлось определение момента для принятия решения, так как цель движется. Наилучший результат достигался в случае, когда объекта находился в центре растра изображения. Момент принятия решения рассчитывался для нескольких изображений с различным положением «контура» цели относительно центрального столбца. Для этого по уже описанному выше алгоритму запоминался номер первого элемента y_1 со значением $\tilde{p}(y)$. После этого запоминался номер последнего элемента y_2 с аналогичным значением. После

этого проверялось условие приблизительного равенства числа элементов вектора ПЯ, соответствующих фону до «контура» цели и после него $\left|\left(Y\text{-}y_2\right)-y_1\right| \le Y/10$. В идеальном случае их число должно быть равным нулю. При выполнении условия рассчитывался коэффициент взаимной корреляции.

Результаты моделирования показали, что при отсутствии очагов засветки на изображении (городские условия местности с очагами возгорания) оценки вероятности правильного принятия решения составили значение для бронеобъекта типа «танк» – 0,78, для объекта типа «грузовик» – 0,67.

Таким образом, предложенный подход позволит повысить устойчивость к случайному срабатываю боеприпаса, а также использовать селекцию объектов поражения. Однако необходимо проводить поиск путей повышения оценок правильного принятия решения для различных условий местности, погодных условий, наличия шумовых воздействий.

С.С. Семенов
Кандидат технических наук, доцент, доцент кафедры
А.А. Бурлаков
кандидат военных наук, преподаватель кафедры
Военная академия связи имени Маршала Советского Союза *С.М. Буденного, г. Санкт-Петербург*

МОДЕЛЬ ГЕНЕРАЦИИ МНОЖЕСТВА ВАРИАНТОВ СТРУКТУР И ВЗАИМОДЕЙСТВИЯ СИСТЕМЫ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ И СИСТЕМЫ ВОЕННОЙ СВЯЗИ

В докладе рассмотрена актуальность разработки модели генерации множества вариантов структур и взаимодействия системы связи общего пользования и системы военной связи. Показаны основные алгоритмы функционирования разработанной модели и представлены примеры результатов обработки данных на модели.

В настоящее время система связи военного назначения развивается в сторону интеграции с ЕСЭ РФ (система связи общего пользования ССОП). При этом вопросам взаимодействия этих двух совершенно разных, как по структуре, так и по техническому наполнению систем, должного внимания не уделяется. Для разработки модели, описывающей функционирование системы военной связи (СВС) в условиях интеграции с ССОП, первым этапом должно быть описание (генерация/задание) обобщенной структуры системы связи. Усложняет ситуацию тот факт, что СВС не имеет постоянной структуры и динамически изменяется как по составу, так и по связанности, в реальном масштабе времени. ССОП, в свою очередь, имеет постоянную, но неоднородную, в зависимости от региона, структуру.

Таким образом, возникает актуальная задача моделирования структур интегрированных систем связи военного назначения (ИСС ВН) в различных регионах и в различных условиях функционирования СВС, расчет вероятности обеспечения связью информационных направлений для сформированной структуры ИСС ВН [1, 2].

Выходными данными разработанной модели являются:

Структура ИСС ВН, описываемая графом, в котором вершины соответствуют узлам, а дуги линиям связи и набором матриц, содержащих значения пропускных способностей, живучести и помехозащищенности элементов системы. Также каждая итерация модели выдает матрицу, содержащую информацию о наличии маршрута между абонентами информационных направлений, удовлетворяющего выдвинутым требованиям, в виде логической «1» в случае существования маршрута или логического «0» в случае его отсутствия.

При большом количестве итераций модели с неизменными данными об абонентах и информационных направлениях можно получить вероятность существования маршрута для абонентов информационного направления (ИН), удовлетворяющего выдвинутым требованиям в заданном регионе по формуле (1).

$$P_{ин}(n) = \frac{\sum_{n}^{i=1} ИН_i}{n}, \qquad (1)$$

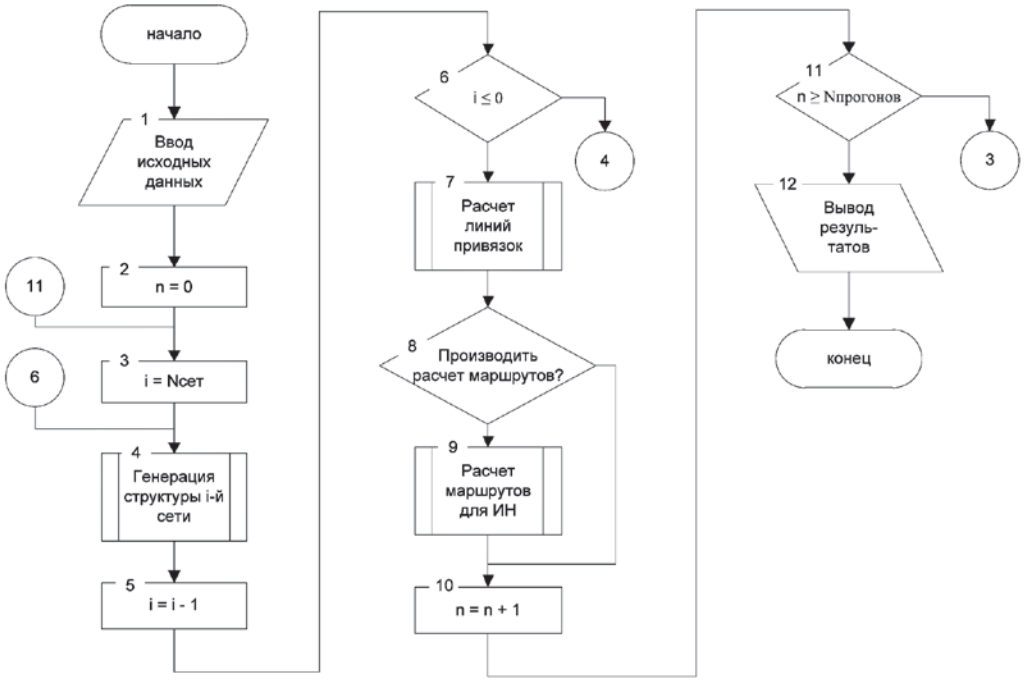


Рис. 1. Обобщенный алгоритм модели формирования взаимодействия ССОП и СВС

где $ИН_i$ – бинарное отображение наличия маршрута для ИН в i-й итерации; n – количество итераций.

Модель сформирована в виде взаимосвязанных модулей, представленных в виде алгоритмов. Обобщенный алгоритм модели представлен на рисунке 1.

В блоке 1 производится ввод исходных данных. Во втором блоке устанавливаются счетчики количества прогонов модели равным нулю.

В блоке 3 устанавливается счетчик количества сетей.

В блоке 4 формируется структура i-й сети.

В блоке 5 происходит уменьшение счетчика сетей (переход к следующей сети).

В блоке 6 происходит сравнение счетчика сетей с нулем, если счетчик достиг нуля (сгенерированы структуры всех сетей), то осуществляется переход к блоку 7, иначе осуществляется переход к блоку 4.

В блоке 7 происходит расчет и генерация линий привязок узлов СВС к ССОП и к сетям других силовых министерств и ведомств.

В блоке 8 происходит разветвление алгоритма. В случае, если в качестве результатов работы модели достаточно получить структуру ИСС ВН, то осуществляется переход к блоку 10, если требуется расчет наличия маршрутов для информационных направлений, то осуществляется переход к блоку 9.

В блоке 9 производится расчет маршрутов для каждого из ИН.

В блоке 10 производится увеличение счетчика прогонов модели.

В блоке 11 производится сравнение счетчика прогонов с заданным количеством прогонов. Если счетчик достиг этого количества, то осуществляется переход к блоку 12, иначе переход к блоку 3 (очередной прогон модели).

В блоке 12 производится вывод результатов моделирования.

Рассмотрим алгоритм генерации структуры ИСС, представленный на рисунке 2. В блоке 4.1 происходит генерация количества узлов связи в моделируемой сети. В этом же блоке обнуляется счетчик узлов j.

В блоке 4.2 генерируются характеристики j-го узла, а именно координаты по оси X и Y, ранг узла - R, пропускная способность узла – V и параметр, характеризующий живучесть узла – G, так же в этом блоке происходит увеличение счетчика узлов j.

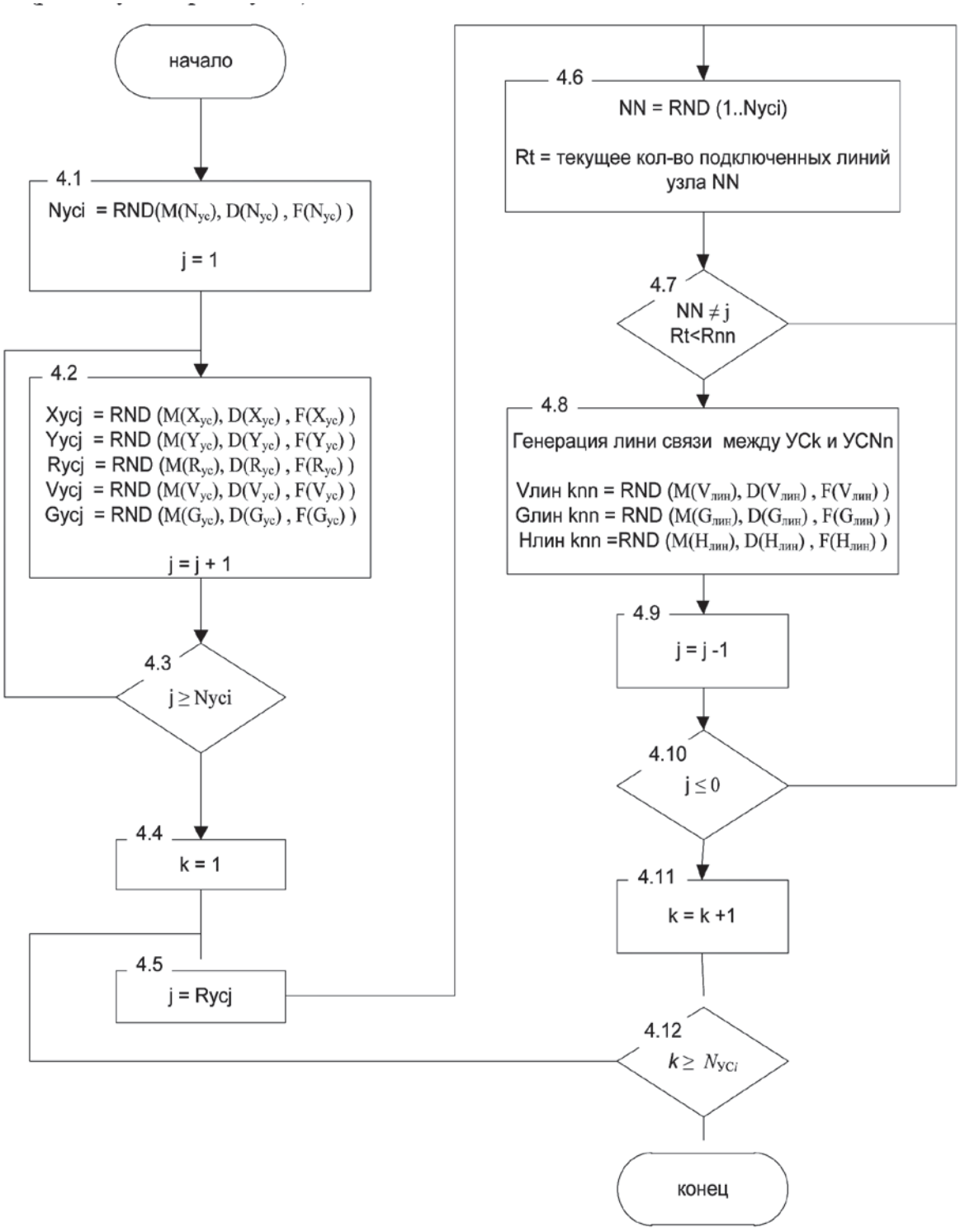


Рис. 2. Алгоритм генерации структуры ИСС

В блоке 4.3 происходит сравнение счетчика узлов с количеством узлов в сети, если счетчик достиг количества узлов в сети, то управление передается в блок 4.4, иначе происходит переход к генерации характеристик следующего узла (блок 4.2).

В блоке 4.4 происходит обнуление счетчика узлов в сети -*k*, для генерации линий связи.

В блоке 4.5 выставляется счетчик *j* подключенных линий связи к *k*-му узлу связи (реализуется ранг узла).

В блоке 4.6 генерируется номер узла связи к которому будет производится подключение линии связи и вычисляется текущее количество подключенных линий к узлу, номер которого сгенерирован.

В блоке 4.7 проверяется условие, что сгенерированный номер узла не равен номеру текущего узла – чтобы не получилась петля и что текущее количество подключенных линий связи к узлу *NN* меньше ранга этого узла. Если условие выполнено, то управление передается в блок 4.8, иначе генерируется другой номер узла (переход в блок 4.6).

В блоке 4.8 производится генерация линии связи между *k*-м и *nn*-м узлами связи в сети, для чего генерируется пропускная способность линии, ее помехозащищенность и параметр, описывающий ее живучесть.

В блоке 4.9 производится уменьшение счетчика *j* (переход к следующей лини связи для *k*-го узла).

В блоке 4.10 происходит проверка ранга узла (достиг ли счетчик *j* нуля). Если условие выполняется, то управление передается блоку 4.11, иначе осуществляется переход к блоку 4.6 (генерация следующей линии связи для *k*-го узла сети).

В блоке 4.11 происходит приращение счетчика *k* (переход к следующему узлу).

В блоке 4.12 производится сравнение счетчика *k* с количеством узлов в сети. Если счетчик достиг значение количества узлов в сети (для всех узлов линии связи сгенерированы), то алгоритм заканчивает работу, иначе осуществляется переход к блоку 4.5 (переход к следующему узлу).

Проведение на модели ряда экспериментов позволило получить зависимость выходного параметра модели – вероятности связности двух абонентов сети ($P_{св}$) от входных параметров. В качестве выходных данных модель предоставляет сгенерированные варианты ССОП и СВС для использования их в дальнейших исследованиях. Варианты полученных структур приведены на рисунках 3 и 4.

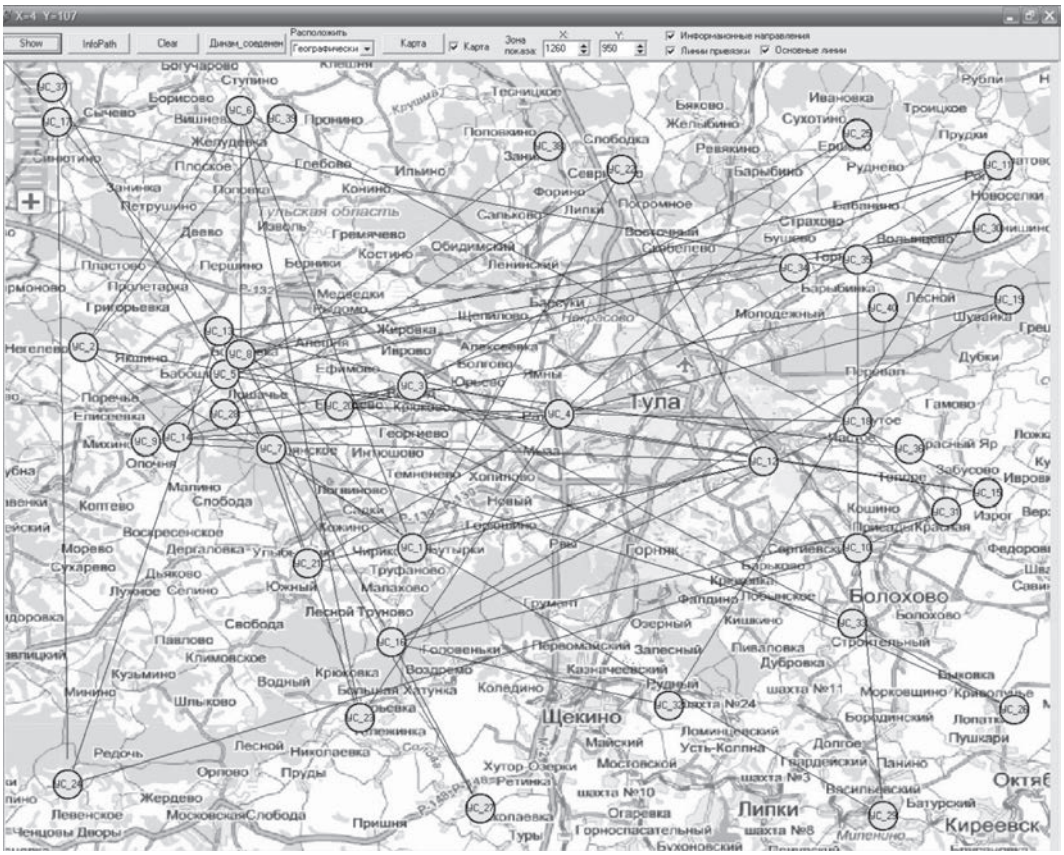


Рис.3. Вариант сгенерированной структуры ССОП

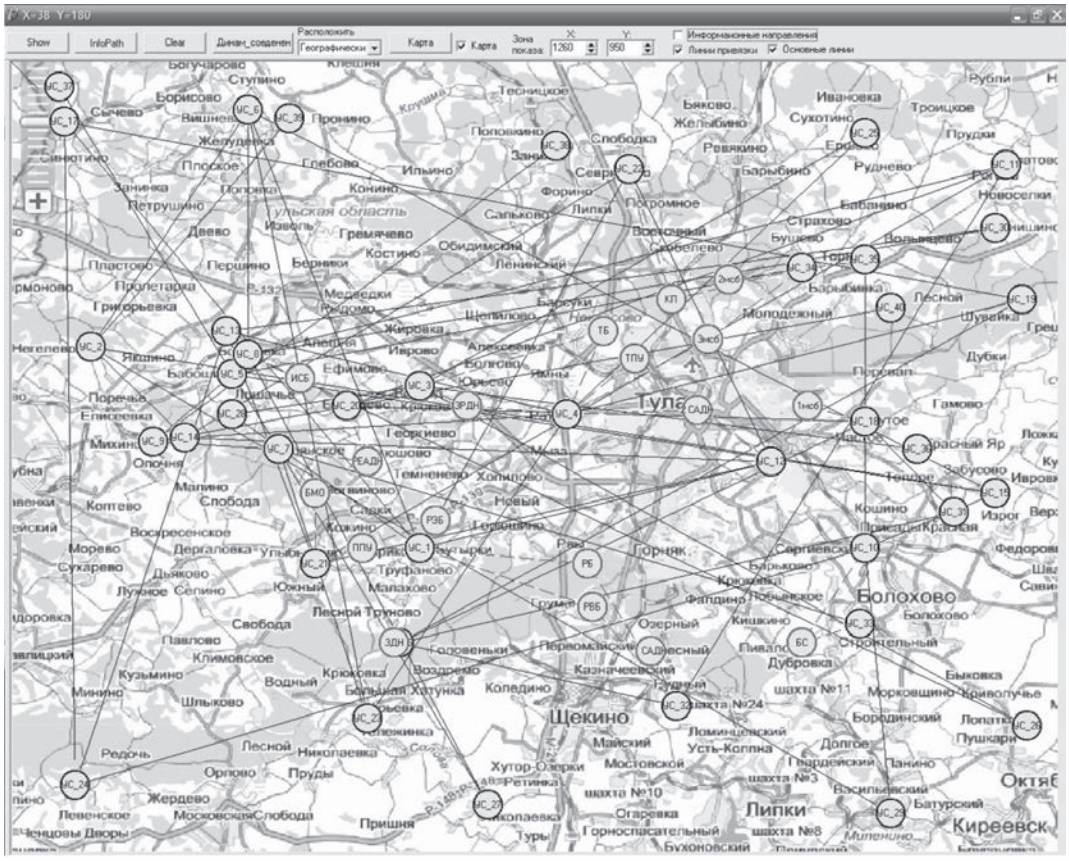


Рис.4. Вариант сгенерированной структуры ССОП и СВС

Модель генерации множества вариантов структур и взаимодействия системы связи общего пользования и системы военной связи доведена до программной реализации [3, 4] и реализована в виде заявки на предполагаемое изобретение [5].

Практическое использование разработанной модели позволит значительно сократить объем работы должностных лиц и время, затрачиваемое на разработку структур интегрированных систем связи военного назначения в различных регионах с учетом конкретных условий функционирования СВС, а также позволит повысить вероятность принятия оптимальн

СПИСОК ЛИТЕРАТУРЫ

1. Семенов С.С., Стародубцев Ю.И. Постановка задачи на разработку способа моделирования структуры интегрированной системы связи военного назначения. Депон. в ЦВНИ МО РФ. М., 2012. 9 с. Выпуск № 3(116) Сер. А. Инв. А31470.

2. Семенов С.С. Способ моделирования структуры интегрированной системы связи военного назначения. Депон. в ЦВНИ МО РФ. М., 2012. 23 с. Выпуск № 3(116) Сер. А. Инв. А31465.

3. Семенов С.С, Гусев А.П., Милый Д.В. Программа генерации структуры системы управления для различных звеньев управления: свидетельство об официальной регистрации программы для ЭВМ № 1215. СПб.: ВАС, 2012.

4. Семенов С.С, Гусев А.П., Баленко О.А. Программа моделирования структуры интегрированной системы связи военного назначения: свидетельство об официальной регистрации программы для ЭВМ № 1219. СПб.: ВАС, 2012.

5. Семенов С. С., Гусев А. П., Баленко О. А., Стародубцев Ю. И. Способ моделирования сети связи: заявка на изобретение РФ. № 2012106099. Заявл. 20.02.12. 33 с.

М. А. Семисошенко
доктор технических наук, профессор
Военная академия связи
Д. В. Кржижокольский
Военная академия связи

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ПРИ РАСПРЕДЕЛЕНИИ ЧАСТОТНОГО РЕСУРСА В СЕТИ ПАКЕТНОЙ ДЕКАМЕТРОВОЙ РАДИОСВЯЗИ

В статье рассмотрены особенности построения системы управления при распределении частотного ресурса и задача централизованного управления общим частотным ресурсов сети пакетной декаметровой радиосвязи при ее функционировании в условиях воздействия непреднамеренных и преднамеренных помех, создаваемых комплексом радиоподавления, и использовании методов случайного многостанционного доступа к среде передачи.

Введение

Декаметровая радиосвязь, несмотря на ряд известных недостатков, продолжает оставаться важным средством в обеспечении устойчивого управления войсками. Одним из перспективных направлений развития декаметровой радиосвязи является использование пакетного режима передачи информации. В наибольшей степени преимущества пакетного режима передачи информации в декаметровой радиосвязи реализуются при построении сети пакетной радиосвязи (СПР), которая представляет собой совокупность автоматизированных пакетных радиосетей (ПРС), использующих для передачи пакетов как прямые, так и составные радиоканалы, образованные через удаленные радиоцентры-ретрансляторы [1].

Реализация потенциальных возможностей СПР предусматривает создание автоматизированной системы управления (АСУ) сетью пакетной радиосвязи, осуществляющей динамическое управление ресурсами сети (частотным, маршрутным, аппаратурным, энергетическим, потоковым) на различных иерархических уровнях. При этом АСУ СПР имеет иерархическую структуру и содержит несколько иерархических уровней управления:

1) уровень управления установками пакетной радиосвязи, который является нижним уровнем управления АСУ сетью пакетной радиосвязи;

2) уровень управления автоматизированным радиоцентром (АРЦ), объединяющим несколько установок пакетной радиосвязи, осуществляющих передачу информации по радиоканалу в интересах пользователей определенного пункта управления войсками;

3) уровень управления пакетной радиосетью, объединяющей совокупность автоматизированных радиоцентров, расположенных в определенном регионе;

4) уровень управления сетью пакетной радиосвязи, объединяющей совокупность пакетных радиосетей.

На первом (нижнем) уровне управления осуществляется управление ресурсами отдельных установок пакетной радиосвязи (установление, ведение и восстановление радиосвязи, оперативный контроль процесса передачи информации по радиоканалу, использование оптимальных режимов работы радиосредств в динамике ведения связи).

На втором иерархическом уровне управления осуществляется управление ресурсами ав-

томатизированного радиоцентра (выбор радиосредств и их распределение между установками пакетной радиосвязи, формирование высокочастотных трактов передачи и приема, анализ и распределение частот, управление энергетическим ресурсом АРЦ).

На третьем уровне управления решаются задачи управления пакетной радиосетью.

На четвертом (верхнем) уровне управления реализуются задачи управления ресурсами сети пакетной радиосвязи, которые заключаются в распределении общего ресурса между пакетными радиосетями (частотного, маршрутного).

Автоматизированная система управления сетью пакетной радиосвязи может быть построена с использованием способов как централизованного, так и децентрализованного управления [1,2,3].

При централизованной системе управления сетью пакетной радиосвязи служебная информация о функционировании всех ПРС поступает в автоматизированную систему контроля и управления (АСКУ) одного из автоматизированных радиоцентров сети, который назначается главным, и обрабатывается в АСКУ главного АРЦ в интересах пользователей всех пакетных радиосетей. На основе поступающей информации о состоянии сети пакетной радиосвязи в АСКУ главного АРЦ формируются управляющие воздействия, которые по каналам передачи служебной информации (командным каналам) передаются подчиненным автоматизированным радиоцентрам. При децентрализованной системе управления сетью пакетной радиосвязи управление ресурсами СПР осуществляется каждой пакетной радиосетью в соответствии с локальными критериями оптимальности.

Приведем математическую постановку задачи распределения частотного ресурса в сети пакетной радиосвязи при централизованном способе построения автоматизированной системы управления СПР.

Пусть сеть пакетной радиосвязи, состоящая из совокупности N независимых пакетных радиосетей, функционирует в условиях воздействия непреднамеренных и преднамеренных помех, создаваемых комплексом радиоподавления противостоящей группировки радиоэлектронной борьбы. Сети пакетной радиосвязи выделено Q частот (частотных полос), которые необходимо распределить между пакетными радиосетями для обеспечения экстремума выбранного показателя эффективности Ф, причем $N \le Q$. При этом каждой пакетной радиосети необходимо назначить $q_n > 1$ ($n = \overline{1, N}$) частот (частотных полос) Во всех пакетных радиосетях осуществляется случайный доступ к общему для всех корреспондентов данной ПРС радиоканалу на основе протоколов случайного многостанционного доступа *S-Aloha* [1].

Введем следующие ограничения:

общий поток пакетов, передаваемых в каждой n-той пакетной радиосети, имеет пуассоновское распределение с интенсивность λ_n ($n = \overline{1, N}$);

характеристики радиоканалов, определяемые вероятностью радиосвязи с достоверностью не хуже заданной в условиях воздействия непреднамеренных помех для любого из корреспондентов n-той ПРС при его работе на q-той частоте $p_{nq}(D \ge D_{\text{доп}})$, являются одинаковыми, где $n = \overline{1, N}$; $q = \overline{1, Q}$; D достоверность радиосвязи; $D_{\text{доп}}$ допустимая достоверность радиосвязи;

в случае неудачной попытки передачи кадра на предыдущем временном интервале повторная передача кадра, формируемого из пакета на канальном уровне, производится на новой частоте (полосе частот), при этом события, заключающиеся в успешной передаче кадра на i-том и на (i+1)-том временных интервалах (i = 1,2,...), являются независимыми событиями;

передача служебной информации об успешном приеме кадра каждым из корреспондентов СПР осуществляется по идеальному командному каналу;

противостоящий комплекс радиоподавления на длительности передачи кадра $\Delta T_{\text{кдр}}$ осуществляет гарантированное подавление одновременно $Q_{\text{рп}}$ частот (частотных полос), выбираемых случайным образом из числа используемых частот с равномерной функцией распределения.

Дополнительными исходными данными, необходимыми для решения задачи распределения частот (частотных полос) в сети пакетной радиосвязи, являются:

матрица вероятностей радиосвязи с достоверностью не хуже заданной для корреспондентов N ПРС при использовании выделенных частот в условиях воздействия непреднамеренных помех $\left\| p_{nq}(D \ge D_{\text{доп}}) \right\|_{N \times Q}$;

матрица средних длительностей пригодного состояния радиоканала для передачи кадра с достоверностью не хуже заданной корреспондентами N пакетных радиосетей при использовании ими каждой из Q частот в условиях воздействия непреднамеренных помех $\left\|\tau_{\text{пр}(nq)}(D \ge D_{\text{доп}})\right\|_{N\times Q}$;

$\lambda_{\text{пвт}(nq)}$ – интенсивность повторной передачи кадров корреспондентами n-той пакетной радиосети, функционирующей на q-той частоте, обусловленная возникновением конфликтов при использовании методов случайного многостанционного доступа к общей для всех корреспондентов ПРС среде передачи информации ($n=\overline{1,N}$; $q=\overline{1,Q}$).

Для успешной передачи кадра в n-той пакетной радиосети ($n=\overline{1,N}$) при ее функционировании на q-той частоте (полосе частот) ($q=\overline{1,Q}$), использовании случайного многостанционного доступа корреспондентов к общей среде передачи и воздействии комплексов радиоподавления необходимо одновременное выполнение следующих событий:

A_1 – наличие пригодного состояния радиоканала при воздействии непреднамеренных помех в момент начала передачи кадра;

A_2 – отсутствие прерываний пригодного состояния радиоканала при воздействии непреднамеренных помех в течение длительности передачи кадра $\Delta T_{\text{кдр}}$ при условии, что в момент начала передачи радиоканал находился в пригодном состоянии;

A_3 – отсутствие конфликтов в течение длительности передачи кадра $\Delta T_{\text{кдр}}$, обусловленных использованием случайного многостанционного доступа корреспондентов к общей среде передачи;

A_4 – отсутствие воздействия комплекса радиоподавления противника на рабочей частоте ПРС в течение длительности передачи кадра.

С учетом независимости событий A_1, A_2, A_3 и A_4 вероятность успешной передачи кадра в n-той ПРС при ее функционировании на q–той частоте (полосе частот), использовании случайного многостанционного доступа корреспондентов к общей среде передачи и воздействии комплекса радиоподавления определим следующим образом:

$$p_{\text{пер}(nq)} = p_1(n,q)\times p_2(n,q)\times p_3(n,q)\times p_4(n,q),\quad (n=\overline{1,N}; q=\overline{1,Q}), \qquad (1)$$

где $p_1(n,q)$, $p_2(n,q)$, $p_3(n,q)$, $p_4(n,q)$ вероятности событий A_1, A_2, A_3, A_4 соответственно.

Вероятности указанных в (1) событий определим с использованием следующих выражений [1,2,3]:

$$p_1(n,q) = p_{nq}(D \ge D_{\text{доп}}),\ (n=\overline{1,N}; q=\overline{1,Q}), \qquad (2)$$

$$p_2(n,q) = \exp\left[-\frac{\Delta T_{кдр}}{\tau_{пр(nq)}(D \ge D_{доп})}\right],\quad (n=\overline{1,N}; q=\overline{1,Q}), \qquad (3)$$

$$p_3(n,q) = \exp\left[-\Delta T_{\text{кдр}}(\lambda_n + \lambda_{\text{пвт}(nq)})\right],\quad (n=\overline{1,N}; q=\overline{1,Q}), \qquad (4)$$

$$p_4(n,q) = 1-\frac{Q_{\text{рп}}}{Q},\ (n=\overline{1,N}; q=\overline{1,Q}). \qquad (5)$$

Обозначим

$$x_{nq} = \begin{cases} 1 - \text{при назначении } n\text{-той ПРС} \\ q\text{-той частоты (полосы частот)}, \\ 0 - \text{в противном случае}, \\ (n=\overline{1,N}; q=\overline{1,Q}). \end{cases}$$

Тогда задача оптимального распределения Q частот (частотных полос) между N пакетными радиосетями заключается в определении оптимального значения элементов матрицы $\left\|x^*_{nq}\right\|_{N\times Q}$, максимизирующих функционал Ф(X) вида

$$\Phi(X) = \sum_{n=1}^{N}\sum_{q=1}^{Q} p_{\text{пер}(nq)}\times x_{nq} \to \max_{x_{nq}} \qquad (6)$$

при ограничениях

$$\sum_{q=1}^{Q} x_{nq} = q_n,\ (n=\overline{1,N}), \qquad (7)$$

$$\sum_{n=1}^{N}\sum_{q=1}^{Q} x_{nq} \le Q, \qquad (8)$$

$$\sum_{n=1}^{N} x_{nq} \le 1,\ (q=\overline{1,Q}). \qquad (9)$$

Представленная задача является задачей линейного программирования с булевыми переменными и решена методами, приведенными в [3].

Заключение

При централизованной системе управления сетью пакетной радиосвязи предложенный подход к распределению частотного ресурса СПР позволяет назначить частоты, на которых обеспечивается максимально возможная в конкретных условиях обстановки вероятность успешной передачи кадров.

СПИСОК ЛИТЕРАТУРЫ

1. Шаров А. Н., Степанец В. А., Комашинский В. И. Сети радиосвязи с пакетной передачей информации.– СПб.: ВАС, 1994.– 216 с.

2. Шаров А. Н. Автоматизированные сети радиосвязи.– Л: ВАС, 1988.– 178 с.

3. Семисошенко М. А. Управление автоматизированными сетями декаметровой связи в условиях сложной радиоэлектронной обстановки. – СПб.: ВАС, 1997.– 364 с.

А. Д. Синюк
кандидат технических наук, доцент
Военная академия связи

МЕТОД ОТКРЫТОГО ФОРМИРОВАНИЯ КЛЮЧА СЕТИ СВЯЗИ

Предлагается описание метода формирования сетевого ключа по открытым каналам связи. Произведена постановка задачи и определены условия открытого сетевого ключевого согласования корреспондентов сетей связи. Прикладные вопросы реализации способа отражены с учетом решения ряда сложных задач управления процессом формирования сетевого ключа.

Введение

В статье [1] предложен протокол формирования сетевого ключа по открытым каналам связи с ошибками, который обладает преимуществами: ориентирован на использование первичных каналов; стойкость сетевого ключа (СК) обеспечивается возможностью формирования СК без центра распределения ключей и случайностью ошибок каналов связи. Однако он не лишен и недостатков связанных со сложностью управления процессом формирования СК. Данная работа продолжает исследования в [1] с учетом процедур управления.

Основная часть

Предлагается следующая постановка задачи. Все корреспонденты (Кор) сети имеют возможность связаться между собой по открытой сети и используют единый алгоритм шифрования. Функции управления формированием СК возлагаются на главную станцию сети (ГС), а остальные - подчиненные станции (ПС). Предварительно между Кор распределены открытые исходные данные. Предполагается, что факт компрометации СК нарушителем у одного из Кор или у нескольких Кор известен на ГС сети связи (СС). Необходимо сформировать СК между нескомпрометированными Кор (НКор).

Порядок формирования СК. Оператор ГС отмечает номера скомпрометированных Кор. Затем с ГС передается информация для оповещения Кор сети о компрометации, запрете обмена информацией по закрытой сети, перехода на открытую сеть связи и запуска процедуры формирования нового СК с НКор. Данная процедура основана на методе формирования СК по открытым каналам связи. Алгоритмическое описание метода для радиосети связи показано на рисунке. После формирования ключа по сигналу с ГС все НКор СС сети переводятся в закрытый режим работы на новом СК.

Предполагается, что групповые ключи (ГК) первой и второй фаз предлагаемого метода формирования СК по открытым каналам связи с ошибками реализуются посредством предложенного в [1] протокола формирования ГК для сети с минимальным числом Кор (ПМЧК).

Предварительно распределенные открытые исходные данные метода формирования сетевого СК: номера всех Кор сети, общее число Кор – $\tilde{N}$; номера запасных частот (ЗПЧ) соответствующие выбранным номиналам частот в том числе общей частоты и частот для выполнения ПМЧК первой и второй фаз метода формирования сетевого СК (СФСК);

– $\tilde{N}$ открытых ключей электронной цифровой подписи каждого Кор СС;

– алгоритмы обработки информации.

Примечание: известны номера скомпрометированных Кор (СКор) сети.

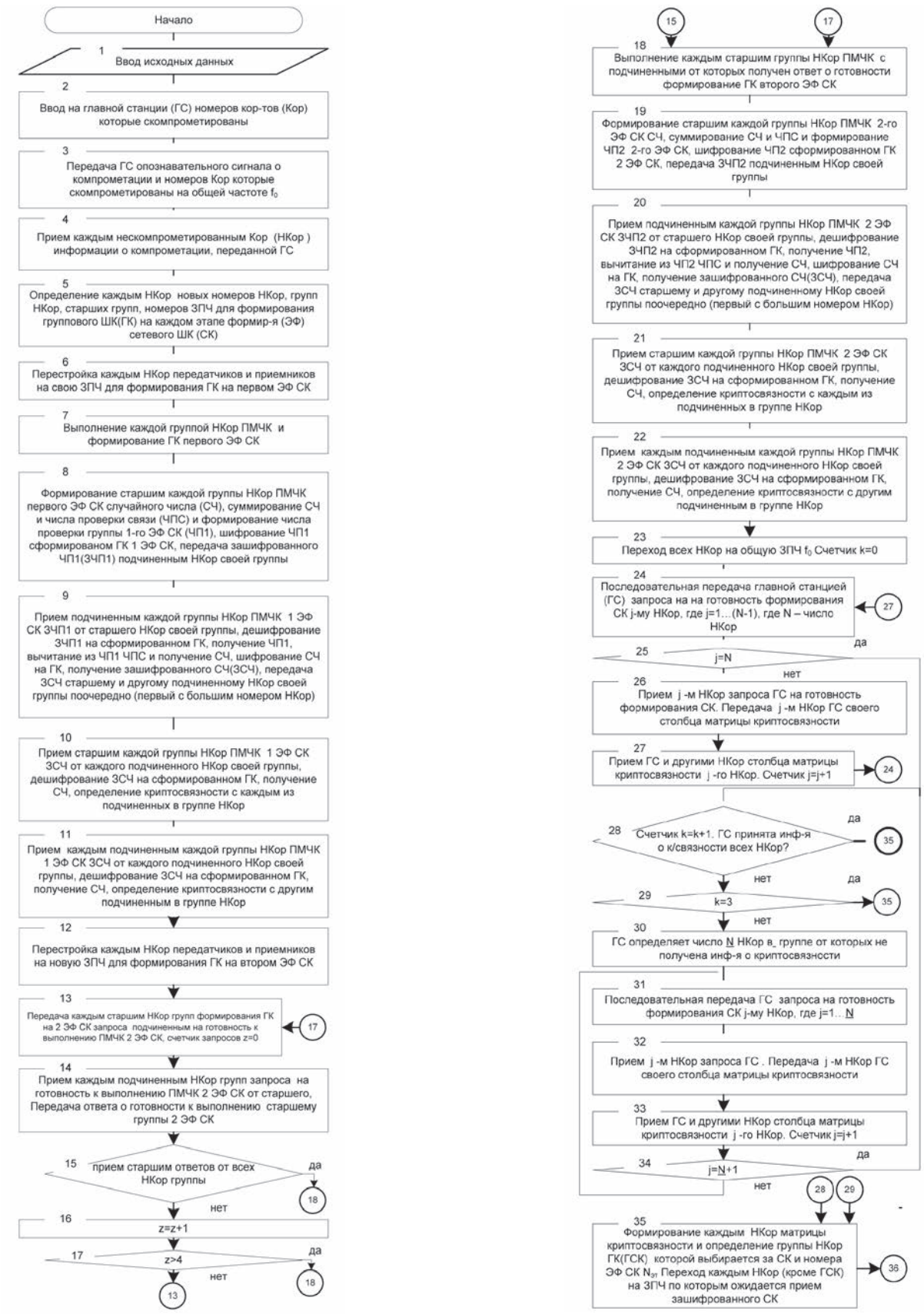


Рис. Метод формирования СК (начало)

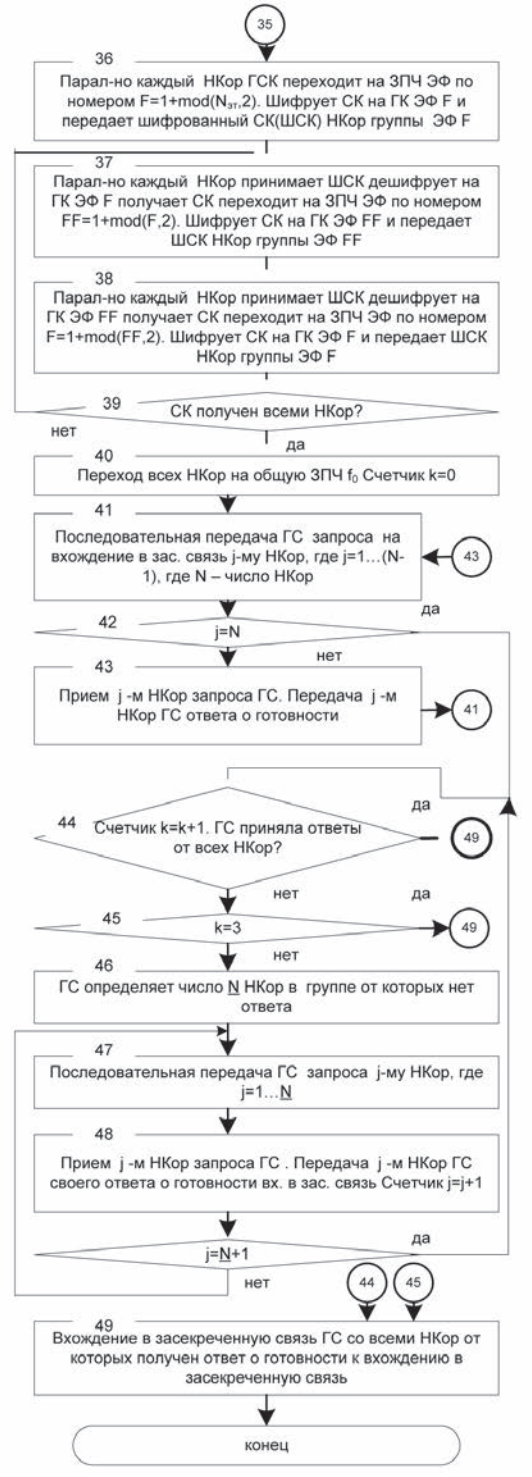


Рис. Метод формирования СК (окончание)

Алгоритмы обработки информации включают: выбора резервной ГС в случае компрометации основной ГС сети; переприсваивания (обновления) номеров НКор исходя из числа Кор после компрометации; формирования групповой связности на каждой фазе СФСК в зависимости от результатов переприсваивания номеров НКор; выбора каждым НКор номиналов ЗПЧ из общего числа ЗПЧ в зависимости от его номера и фазы СФСК; определения старшей станции группы НКор формирующих ГК на 1 и 2 фазах формирования СК СФСК; выбора параметров ПМЧК (протоколов формирования СК двух Кор); передачи команд в группе НКор при формировании ГК фазы СФСК для проверки полученной криптосвязности в группе НКор; формирования матрицы криптосвязности НКор; возвращения на общую ЗПЧ после выполнения фаз СФСК и формирования матрицы криптосвязности всех НКор; выбора СК из полученной матрицы криптосвязности всех НКор; последовательной передачи СК для всех НКор; вхождения в закрытую связь после формирования СК.

Заключение

Разработанный метод формирования СК по открытым каналам связи развивает результаты ранних исследований с учетом прикладных аспектов формирования СК Кор СС. Полученная совокупность результатов позволит эффективно внедрять метод в системы защиты информации, использующие криптографические преобразования.

СПИСОК ЛИТЕРАТУРЫ

1. Синюк А.Д., Саенко И.Б. Протокол формирования сетевого ключа по открытым каналам связи с ошибками // Труды СПИИРАН, Выпуск 3(14), 2010. СПб.: Издательство «Анатолия», 2010 г. С. 29—49.

А. Д. Синюк
кандидат технических наук, доцент
Военная академия связи

ОТКРЫТОЕ ФОРМИРОВАНИЕ ГРУППОВОГО КЛЮЧА

Обсуждаются пути построения протокола формирования ключа трех объектов связи для чего разработана модель процесса формирования группового ключа включающая модель канальной связности, принципы формирования ключа, процедуры реализации. Предложено использовать ошибки имеющие место в каналах связи в процессе формирования группового ключа.

Введение

Необходимо исследовать пути реализации протокола формирования ключа (ПФК) трех объектов связи *A, C* и *B*, осуществляя обмен данными конечной длины между ними по каналам, доступным нарушителю *E*. При этом требуется обеспечить формирование ключа (*K*) с высокой достоверностью для объектов связи (ОС) и обеспечить малую вероятностью совпадения с ключом *E*. Нарушитель пассивен [1].

Основная часть

Нарушителя и ОС, связанных каналами связи, можно представить моделью канальной связности (МКС) ОС *A, C* и *B* и нарушителя *E* (см. рис.).

Предположим, что каналы ОС МКС описываются моделью двоичного широковещательного канала без памяти (ШК) [2], причем составляющий канал 1 (КС-1) описывается моделью двоичного симметричного канала связи без памяти (ДСК) с вероятностью ошибки p_y, а канал 2 (КС-2) – ДСК с p_m. Каналы определяются алфавитами входным *X,* выходными Y и M.

На вход ШК ОС *A* подается последовательность $\overline{x} \in X^N$, где X^N - декартова *N*-я степень множества X. ОС *B* принимает на выходе КС-1 последовательность $\overline{y} \in Y^N$. ОС *C* принимает на

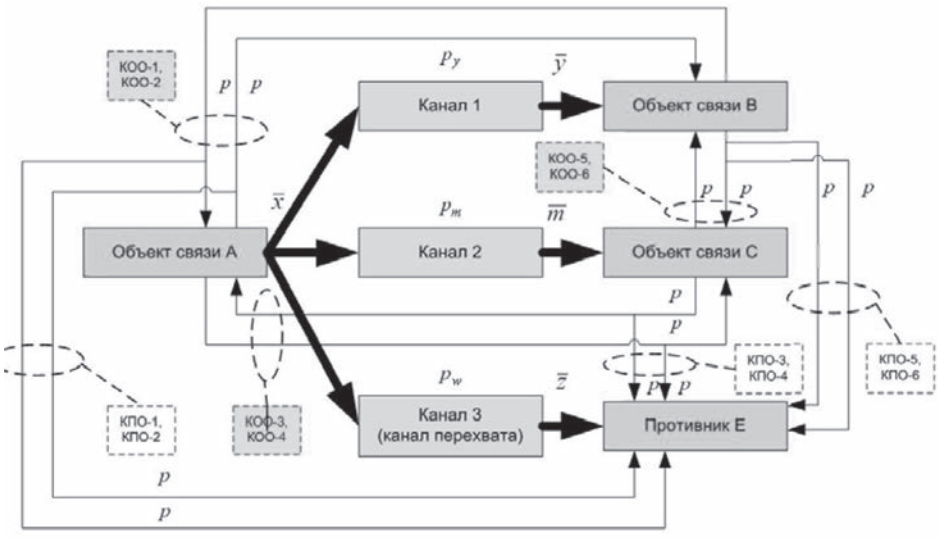


Рис. Модель канальной связности

выходе КС-2 последовательность $\bar{m} \in M^N$. Канал связи с ошибками от ОС *A* к *E* называется каналом перехвата (КП), описывается моделью ДСК с вероятностью ошибки p_w и алфавитами входным *X* и выходным Z. Нарушитель *E* принимает последовательность $\bar{z} \in Z^N$. В МКС также имеются каналы открытого обсуждения (КОО), направление и нумерация которых показаны на рисунке. Нарушитель контролирует каждый из КОО соответствующим каналом перехвата обсуждения (КПО). КОО и КПО – идеальные и независимые каналы.

Формирование *K* в МКС разделим на три последовательных этапа. Первый этап – генерирование начальных данных (НД) ОС *A* последовательности $\bar{x}$ и получение НД ОС *B* и *C* в виде последовательностей $\bar{y}$ и $\bar{m}$ на выходах КС-1 и КС-2. Нарушитель получает по КП начальные данные нарушителя (НДН) $\bar{z}$. Второй этап обеспечения формирования *K* с высокой достоверностью, что достигается исправлением ошибок составляющих каналов, которое производится при использовании передачи дополнительной информации по КОО. Предполагается, что нарушитель перехватывает ее по КПО и использует для устранения ошибок в НДН. В результате ОС формируют ключевые последовательности (КлП). Третий этап обеспечения формирования группового *K* с малой вероятностью совпадения с ключом нарушителя *E*, путем сжатия тождественных КлП ОС. Предполагается, что *E* знает точное описание действий, выполняемых ОС и для получения *K* и производит оптимальную обработку доступной информации известными методами обработки.

Для решения задач первого этапа разработан простейший протокол реализуемый следующим образом: **1.** ОС *A* выбирает двоичный информационный символ (ИС) x с равномерным законом распределения вероятностей. **2.** ОС *A* с использованием кода с повторениями $(n, 1)$ формирует из x кодовое слово (КдС) и запоминает его в качестве x_n. **3.** ОС *A* передает x_n по ШК. **4.** ОС *B* принимает принятое слово (ПС) y_n. ОС *C* получает ПС m_n. *E* получает ПС z_n. **5.** Если все его символы «1» или «0», тогда ОС *B* предварительно принимает y_n. В противном случае ОС *B* стирает y_n. Решение передается по КОО к другим ОС. Аналогично действует ОС *C* получая ПС m_n. **6.** ОС *A* сохраняет ИС x, если получены предварительные решения о приеме y_n и m_n. В противном случае ОС *A* стирает x. ОС *B* выносит решение об ИС y, соответствующем ПС y_n путем выделения первого символа из y_n и сохраняет y, если ОС *B* принял y_n и получено предварительное решение о приеме m_n. В противном случае ОС *B* стирает y_n. ОС *C* действует аналогично относительно ИС m КдС m_n.

Проведем анализ протокола на примере одного составляющего канала ШК, т.к. для другого он идентичен.

Код с повторениями содержит 2 КдС. Шаг 1 Примитива определяет, что КдС равновероятны. ОС *B* принимает y_n с вероятностью P_B

$$P_B = p_y^n + \left(1 - p_y\right)^n. \qquad (1)$$

ОС *C* принимает m_n с вероятностью P_C.

Совместная вероятность P_{ac} сохранения ОС ИС равна

$$\begin{aligned} P_{ac} = p_y^n p_m^n + p_y^n \left(1 - p_m\right)^n + \\ + \left(1 - p_y\right)^n p_m^n + \left(1 - p_y\right)^n \left(1 - p_m\right)^n. \end{aligned} \qquad (2)$$

Вероятность несовпадения сохраненных x и y при условии, что они сохранены

$$\tilde{p}_y = \frac{p_y^n}{p_y^n + \left(1 - p_y\right)^n}. \qquad (3)$$

Аналогично найдем $\tilde{p}_m$ условную вероятность события несовпадения x с m.

Опишем ситуацию у нарушителя *E*. На 4 шаге Примитива *E* принимает на выходе КП z_n. Решения ОС *B* и *C* передаваемые по КОО перехватываются по КПО на 5 шаге. *E* также может удалять символы, которые были стерты ОС. Однако соответствующие символы, сохраняемые *E*, не достаточно надежны, потому, что составляющие каналы ШК и КП независимы. Тогда $\tilde{p}_w$ равна

$$\tilde{p}_w = \sum_{i=\left\lfloor \frac{n}{2} \right\rfloor}^{n} C_n^i \beta(i,n)\, p_w{}^i (1 - p_w)^{n-i}, \qquad (4)$$

где $\lfloor \bullet \rfloor$ - символ округления до наибольшего целого числа,

$$\beta(i,n)=\begin{cases}0.5 \ \text{ если } i=\dfrac{n}{2},\\ 1 \ \text{ если } i\neq\dfrac{n}{2}.\end{cases} \qquad (5)$$

Процедура второго этапа может быть реализована с использованием метода *помехоустойчивого кодирования* [3]. Для этого ОС *A,* с помощью некоторого конструктивного линейного кода, находит проверочные символы к НД $\bar{x}'$ длиной N', полученным после реализации задач первого этапа. ОС *A* посылает проверочные символы к ОС *B* и *C* по КОО-1 и КОО-3, соответственно. ОС *B* и *C* исправляют ошибки в НД $\bar{y}'$ и $\bar{m}'$, соответственно, используя проверочные символы и конструктивный алгоритм декодирования выбранного кода.

Вероятность ошибочного декодирования НД ОС *B* P_{AB} найдем из формулы

$$P_{AB}=\sum_{i=\left\lfloor\frac{d-1}{2}\right\rfloor+1}^{N'} C_{N'}^{i}\tilde{p}_y^{i}(1-\tilde{p}_y)^{N'-i}. \qquad (6)$$

Аналогично найдем вероятность ошибочного декодирования НД ОС *C* P_{AC}.

Предполагается, что вероятность битовой ошибки равномерно распределяется по КлП. Тогда $\bar{p}_y$ - вероятность ошибки на бит в КлП ОС *B* может быть определена из выражения

$$\bar{p}_y=1-\left(1-P_{AB}\right)^{\frac{1}{N'}}. \qquad (7)$$

Подобным образом определяется $\bar{p}_m$ вероятность ошибки в КлП ОС *C*.

E также как и ОС *B* и *C* использует конструктивный алгоритм декодирования $\left(N'+r,N'\right)$ - кода. Вероятность ошибочного декодирования НДН P_W равна

$$P_W=\sum_{i=\left\lfloor\frac{d-1}{2}\right\rfloor+1}^{N'} C_{N'}^{i}\tilde{p}_w^{i}(1-\tilde{p}_w)^{N'-i}. \qquad (8)$$

Вероятность ошибки на бит $\bar{p}_m$ в КлП нарушителя *E* (в декодированной последовательности НДН) может быть определена из выражения

$$\bar{p}_w=1-\left(1-P_W\right)^{\frac{1}{N}}. \qquad (9)$$

Выполнение задачи третьего этапа - обеспечения формирования *K* малой вероятности совпадения группового *K* с ключом *E* достигается путем сжатия КлП ОС *A, C* и *B*, которые были получены после процедуры исправления ошибок «виртуального» ШК. Необходимость сжатия КлП, с целью уменьшения вероятности совпадения с *K* нарушителя подробно рассматривалось в [1]. Предлагается использовать простой алгоритм сжатия символов. Алгоритм может применяться для достижения цели размножения ошибок в версии *K* нарушителя *E*. Пусть длины КлП равны N' и параметр длины блока битов КлП v предварительно открыто распределен. Алгоритм состоит в следующем. ОС *A, C* и *B* выделяют из своих КлП l соответствующих блоков бит длины v, причем

$$l=N'/v. \qquad (10)$$

Блоки с нечетным числом символов «1» сжимаются (символы блока суммируются по модулю 2) в символ «1», а с четным числом «1» сжимаются в «0». Поученные символы объединяются в ключ.

Вероятность несовпадения бит в сформированных ключах ОС *A* и *B* описывается соотношением [4]

$$p_{AB}^{l}=\frac{1-(1-2\bar{p}_y)^{v}}{2}. \qquad (11)$$

Аналогично, вероятность несовпадения бит в ключах ОС *A* и *C* будет равна:

$$p_{AC}^{l}=\frac{1-(1-2\bar{p}_m)^{v}}{2}. \qquad (12)$$

Вероятность несовпадения сформированных *K* группы ОС P_E^l может быть определена из выражения

$$P_E^l=1-\left(1-p_{AB}^{l}\right)^{l}\left(1-p_{AC}^{l}\right)^{l}. \qquad (13)$$

Нарушитель *E* использует алгоритм для формирования своей версии *K*. Вероятность несовпадения бит в ключах ОС *A* и *E* описывается соотношением

$$p_{AE}^{l}=\frac{1-(1-2\bar{p}_w)^{v}}{2}. \qquad (14)$$

Вероятность совпадения *K* нарушителя *E* с групповым *K* P_S может быть определена из выражения

$$P_S=\left(1-p_{AE}^{l}\right)^{l}. \qquad (15)$$

Заключение

Подводя итог, отметим, что разработана модель формирования группового *K* включающая: модель канальной связности; принципы и процедуры формирования *K*. МКС позволяет в полной мере охарактеризовать объекты, участвующие в процессе формирования *K*. Последовательная реализация трех принципов формирования группового ключа на основе предложенных процедур позволят синтезировать конструктивный протокол формирования группового ключа по открытым каналам связи с ошибками.

СПИСОК ЛИТЕРАТУРЫ

1. Симмонс Г.Дж. Обзор методов аутентификации информации. -ТИИЭР, т.76, №5, 1988, с.105-125.

2. Чисар И., Кернер Я. Теория информации: теоремы кодирования для дискретных систем без памяти: Пер. с англ. —М.: Мир, 1985. - 400 с.

3. Мак-Вильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки. М., Связь, 1979, 744 с.

4. Галлагер Р. Коды с малой плотностью проверок на четность. М.: Мир, 1966, 320 с.

Скорик Ф.А.
Соискатель
Военная академия связи им. С.М. Буденного
Саенко И.Б.
Доктор технических наук, профессор
Военная академия связи им. С.М. Буденного

МЕТОД НЕПРЕРЫВНОГО ОБУЧЕНИЯ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ В ЗАДАЧЕ ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВОЕННОГО НАЗНАЧЕНИЯ

Рассматривается метод динамической подстройки весов искусственной нейронной сети на основе модели взаимодействия сущностей «учитель» – «ученик» в применении к распределенной информационной системе военного назначения. Приведены сравнительные результаты прогноза, данного системой с модулем динамической подстройки весов, относительно результатов, данных системой без этого модуля.

В настоящее время, использование информационных систем (ИС), как инструмента управления, является обязательным для любой организации, даже если она не связана напрямую с информационными технологиями.

В идеале в рамках организации должна функционировать единая распределенная информационная система, удовлетворяющая все существующие информационные потребности всех сотрудников, служб и подразделений.

Однако на практике создание такой всеобъемлющей ИС слишком затруднено или даже невозможно, вследствие чего в подразделениях Вооруженных силах Российской Федерации (ВС РФ) обычно функционируют несколько различных ИС, решающих отдельные группы задач, связанных с нормативным функционированием подразделений, в интересах которых они были развернуты.

Несмотря на то, что военных системах управления пункты хранения и обработки информации, а также линии связи, как правило, дублируются, это не исключает возникновения ситуации отказа в обслуживании одному или нескольким конечным пользователям.

В большинстве случаев это происходит из-за того, что часть задач бывает «покрыта» одновременно несколькими распределенными ИС (РИС), часть задач – вовсе не автоматизирована.

Чем больше РИС, тем сложнее осуществлять контроль над ее функционированием, и тем больше времени требуется на восстановление в случае отдельных элементов или подсистем ИС.

Время, требуемое для восстановления работоспособности, тем меньше, чем более эффективной является система определения состояния и прогнозирования нештатных ситуаций, возникающих в РИС.

В настоящей работе рассматривается модель системы прогнозирования, имеющей в своей основе искусственную нейронную сеть, обладающую динамической подстройкой весов уже в ходе функционирования, что позволяет существенно повысить точность прогноза.

Применение искусственных нейронных сетей для решения задач прогнозирования рассматривалось многими авторами, и по этой теме было написано большое количество статей и работ.

Однако даже при построении искусственных нейронных сетей большой размерности, и, как следствие, имеющих высокую точность аппроксимации, как правило, не учитывается тот факт, что при прогнозировании величина входных характеристик может выйти за пределы допустимого для правильного прогнозирования диапазона значений, что в свою очередь, может привести к негативному результату [1–2].

При решении задач прогнозирования, как правило, необходимо осуществлять непрерывный мониторинг прогнозируемых характеристик изучаемой системы.

Следовательно, для таких систем необходимо разработать дополнительный модуль, использующий нейронную сеть для определения текущего состояния системы на основе временного ряда за определенный предыдущий период $[t_{-N} ... t_0]$. Подобная система предусматривает определение сущностей «учитель» и «ученик».

При этом сущность «учитель» будет реализацией интерфейса слушателя данных. Следовательно, «учитель», будет являться модулем динамической подстройки, который на основании текущих и ранее полученных данных, производит их анализ. Ученик, в свою очередь, будет слушателем учителя.

На примере описанной выше модели, рассмотрим временное взаимодействие сущностей «учитель» и «ученик». При получении данных от источников данных «учитель», используя алгоритм кластеризации входных данных, (как правило, для этих целей используются самоорганизующиеся карты Кохонена), разбивает их на обучающие выборки. Одновременно с этим производится запрос к внутреннему хранилищу данных, содержащему уже обработанную ранее информацию. В том случае, если новая обучающая выборка выходит за пределы допустимого диапазона, «учитель» передает ее «ученику» для обучения в параллельном потоке. Одновременно с этим обучаемые компоненты должны произвести анализ полученных данных.

Схема взаимодействия сущностей «учитель» и «ученик» в рассматриваемой модели отображена на рис. 1. Эксперимент проводился на искусственной нейронной сети, содержащей 8 слоев и имеющей 15 входных нейронов.

В ходе эксперимента сеть обучалась распознаванию каждого входного вектора до получения отклонения в 1% от ожидаемого результата.

Обучение проводились следующим образом. Сеть проходила обучение полным набором

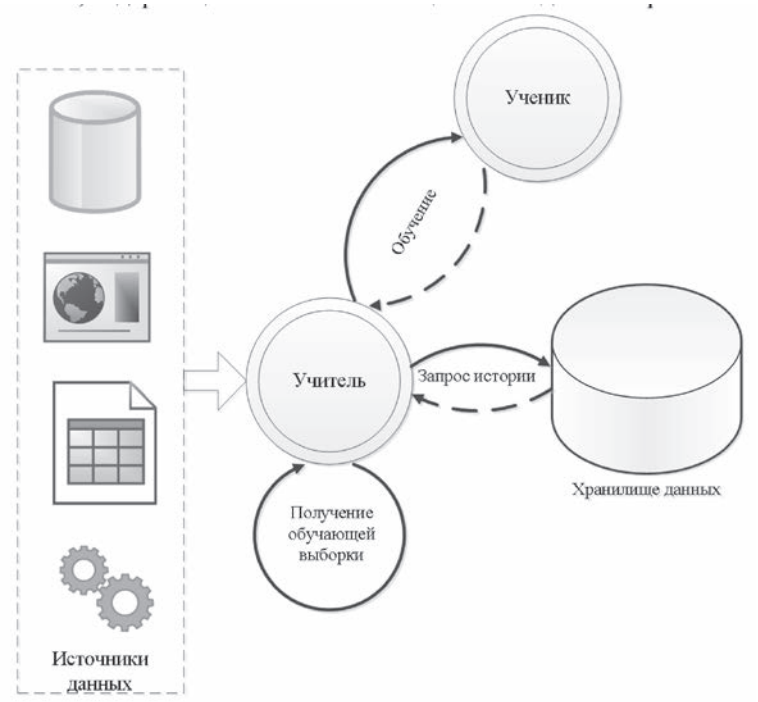


Рис. 1. Схема взаимодействия сущностей «учитель» и «ученик»

цТаблица 1

Результаты обучения многослойного персептрона

	Без модуля взаимодействия сущностей			С модулем взаимодействия сущностей		
Вносимая погрешность (%)	10	20	30	10	20	30
Максимальная ошибка обучения (%)	14.6	38.1	36.4	13.1	35.6	36.3
Средняя ошибка обучения (%)	6.1	16.2	12.8	4.6	12.4	12.1
Максимальная ошибка прогноза (%)	3.9	11.9	14.3	2.8	8.4	9.3
Средняя ошибка прогноза (%)	2.4	3.6	7.2	1.3	2.6	4.1

тестовых данных, потом проводилось тестирование модуля подстроки на той же выборке. Результаты исследования представлены в таблице №1.

Из данной таблицы видно, то искусственная нейронная сеть с модулем взаимодействия по принципу «учитель»-«ученик», осуществляющая динамическую подстройку весов нейронной сети на основании текущих и сохранных ранее данных, имеет меньшую погрешность прогноза по сравнению с обычной искусственной нейронной сетью.

Заключение

Поведение РИС невозможно описать с помощью линейных моделей традиционного технического анализа, так как имеют место быть элементы нелинейности и хаотичности, проявляющиеся при совместной работе большого количества обособленных элементов системы.

Модель, основанная на нейронной сети, позволяет учитывать эту нелинейность, что в свою очередь позволяет добиваться прогнозов с приемлемым уровнем погрешности.

Цель подобных систем – находить скрытые закономерности и зависимости между множеством показателей, моделировать поведение, сегментировать объекты анализа, строить долгосрочный прогноз на перспективу.

В работе приведена базовая модель взаимодействия сущностей, позволяющая осуществить динамическую подстройку весов искусственной нейронной сети при прогнозировании изменений характеристик динамической системы.

Испытания наглядно показали, что рассмотренный подход позволяет существенно уменьшить среднюю ошибку прогноза по сравнению с теми нейросетевыми методами прогнозирования, которые не осуществляют динамическую подстройку весов.

СПИСОК ЛИТЕРАТУРЫ

1. Минаев Ю.Н., Филимонова О.Ю., Бенамеур Лисс. Методы и алгоритмы решения задам идентификации и прогнозирования в условиях неопределенности в нейросетевом логическом базисе. – М.: Горячая линия Телеком, 2003.

2. Саймон Хайкин Нейронные сети. – 2-е изд. – М.: Вильямс, 2006.

В.И. Сучков
кандидат технических наук, доцент
В.А. Чикуров
кандидат технических наук, доцент
ФКГВОУ ВПО «Военно-космическая академия имени А.Ф. Можайского», г. *Санкт-Петербург*
О.Г. Лазутин
Главный испытательный космический центр имени Г.С. Титова, г. *Краснознаменск*

ТЕНДЕНЦИИ РАЗВИТИЯ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОБРАБОТКИ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ

Рассматриваются принципы построения специального программного обеспечения автоматизированных комплексов обработки телеметрической информации, наиболее полно воплощающие основные закономерности и тенденции построения и развития специального программного обеспечения существующих и перспективных автоматизированных комплексов обработки.

Введение

Специальное программное обеспечение (СПО) автоматизированных комплексов обработки (АКОИ) телеметрической информации (ТМИ) – СПО АКОИ определяется как совокупность программ, описаний, инструкций для решения задач преобразования ТМИ, контроля и диагностирования средств АКОИ как элементов вычислительной системы.

Отличительным свойством наиболее распространенных видов АКОИ является их универсальность как вычислительной системы. Она выражающаяся в способности в достаточно широком диапазоне варьировать перечнем решаемых задач обработки измерительной информации, порождаемой источниками с различными структурными и функциональными характеристиками.

Рассмотренные обстоятельства приводят к определению СПО АКОИ как порождающему программному комплексу. Он включает в себя систему описания исходных данных источника ТМИ, базу модулей процесса обработки, систему определения характеристик и структуры процесса обработки. Он предназначен для автоматического формирования программной продукции, реализация которой и обуславливает применение АКОИ для обработки ТМИ конкретных технических объектов (ТО). Именно средствами данного комплекса осуществляется отражение в программных инструкциях по обработке ТМИ специфики предметной области в виде учета априорных сведений о характеристиках ТО, требований к содержанию, форме и организации процесса обработки ТМИ.

Анализ характеристик специального программного обеспечения автоматизированных комплексов обработки информации

Программный комплекс выступает как СПО программирования процессов обработки (ППО). Программная продукция, порождаемая им в процессе подготовки к обработке информации конкретных источников (в процессе постановки объектов на автоматизированное обслуживание), в этом случае представляет собой СПО конкретного технического объекта (ТО). Характер взаимодействия СПО ППО и СПО ТО иллюстрирует рисунок 1.

Соотнесение структур, представляющих субъект порождения программной продукции (ПП) и субъект обработки измерительной информации, с перечнем функциональных характеристик, предъявляемых разработчиками

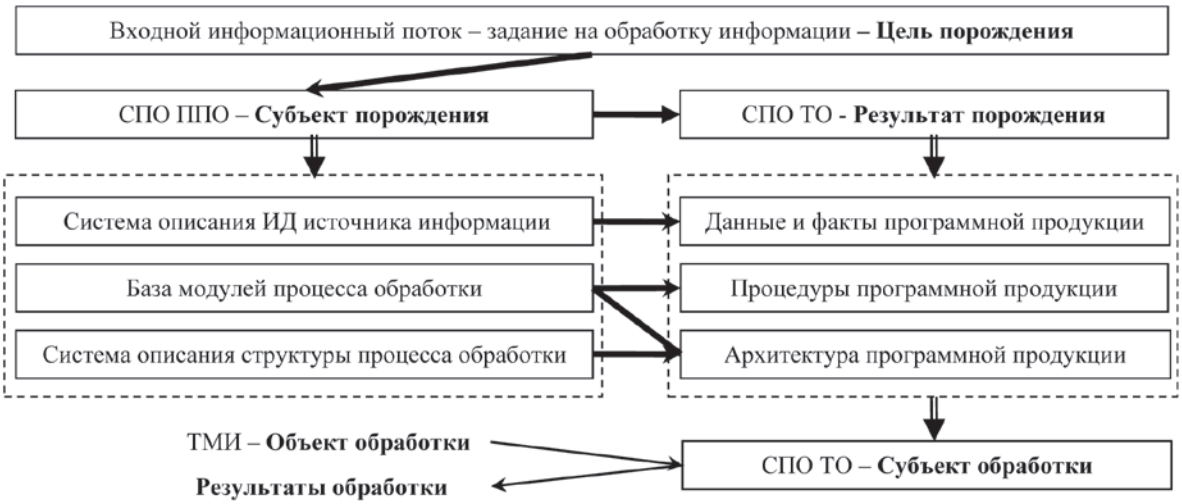


Рис. 1. Характер взаимодействия СПО ППО и СПО ТО

СПО обработки ТМИ и подвергаемых исследованию в процессе испытаний СПО АКОИ, показывает, что практически все они имеют отношение к субъекту обработки ТМИ и в весьма ограниченных пределах, косвенно позволяют выносить суждения о свойствах и характеристиках субъекта порождения. Поскольку именно к эксплуатационным свойствам субъекта обработки предъявляются наиболее жесткие, конкретные требования пользователя, вытекающие из оперативно-тактических и технологических условий проведения обработки информации, как по привлекаемым ресурсам вычислительной системы, так и по качеству получаемых результатов.

Свойства и характеристики СПО ТО являются производными, порождаемыми конструкционными возможностями и свойствами принятой в конкретном СПО АКОИ системе или технологии компиляции программ обработки. В свою очередь, возможности конкретного компилятора программ обработки являются отражением принятых в конкретном СПО АКОИ технологий и подходов к описанию и концентрации атомарных знаний, фактов и правил их композирования.

Таким образом, сложившаяся система анализа характеристик СПО АКОИ и определения перспектив его развития ориентирована преимущественно на исследование свойств субъекта обработки, оставляя практически без внимания свойства и характеристики СПО ППО, являющимся основным источником свойств СПО ТО.

В связи с этим в качестве основного предмета задачи оценивания и анализа характеристик СПО АКОИ должно выступать СПО ППО. Оценки его свойств и показателей качества помимо аттестации собственно СПО АКОИ, как элемента программного обеспечения АСУ ТО, являются наиболее весомыми и существенными в определении порождающей способности СПО ППО.

В соответствии со сформулированной концепцией рассмотрения СПО АКОИ в таблице 1 приведены имеющие место в настоящее время формы и способы исходного представления в среде порождения выделенных выше (рис.1) компонентов синтезируемой ПП. Отметим, что представленные в таблице 1 шкалы выразительных возможностей имеют качественный, отражающий тенденцию, характер. Количество градаций и их определения может быть иным. Диаграмма на рисунке 2 отражает уровень реализации представленных в таблице 1 выразительных возможностей среды СПО ППО в конкретных, хронологически упорядоченных, образцах СПО АКОИ.

Объективным результатом проведенного рассмотрения существа СПО АКОИ является вывод о том, что СПО ТО, реализуемое в вычислительной системе АКОИ, представляет собой композированные в соответствии с определенной логической схемой процедуральные знания, аргументы которых определяются совокупностью фактов (исходных и

входных данных), подлежащих преобразованию или используемых при преобразовании в рамках конкретного СПО ТО.

Таким образом, система автоматизированной подготовки программ обработки измерительной информации обеспечивает эффективную организацию работы АКОИ на следующих этапах:

– подготовки исходных данных по контролируемому объекту и по условиям обработки полученной от него информации;

– формализации знаний по методам обработки измерительной информации;

– подготовки заданий на обработку измерительной информации;

– формирования и исполнения рабочих программ сеанса как СПО ТО;

– управления сеансом обработки.

Для решения перечисленных задач СПО ППО располагает совокупностью компонентов – системой подготовки и хранения данных (СПХД), базой модулей обработки (БМО), компилятором рабочих программ (КРП), языком заданий на обработку (ЯЗО). Отметим, что все эти компоненты теснейшим образом взаимосвязаны. Так, например, логика работы КРП в значительной степени определяется синтаксисом и семантикой ЯЗО, а так же методами, используемыми при построении модулей БМО. Структура записей СПХД определяется принятым методом их использования в КРП.

Представленные результаты показывают, что объективной тенденцией развития и совершенствования АКОИ и его СПО является повышение уровня их универсальности, рассматриваемой как способность подготавливать и осуществлять в рамках единой вычислительной среды процесс обработки измерительной информации с произвольной исходной структурой в необходимом диапазоне задач и методов преобразования

Таблица 1

Формы и способы представления в среде порождения компонентов синтезируемой программной продукции

№ п/п	Средства представления в среде порождения компонента синтезируемой ПП		
	Логическая архитектура	Примитивы преобразования информации	Факты и исходные данные
1	Фиксированная средствами машин-но-ориентированного языка (МОЯ)	Подпрограммы на МОЯ	Стандартные информационные структуры МОЯ
2	Формируемая на этапе подготовки СПО ТО средствами МОЯ	Процедуры алгоритмического языка (АЯ)	Программируемые средствами МОЯ информационные структуры
3	Формируемая на этапе подготовки СПО ТО средствами АЯ	Программные модули на МОЯ или АЯ	Стандартные информационные структуры АЯ
4	Фиксированная средствами МОЯ, дополняемая средствами табличного языка	Библиотеки модулей на МОЯ или АЯ	Сложные информационные структуры программируемые средствами АЯ
5	Фиксированная средствами МОЯ, дополняемая средствами АЯ	Библиотеки программных модулей и эвристик	Файлы и библиотеки исходных данных
6	Формируемая при подготовке СПО ТО средствами специализирован-ного процедурного языка (СПЯ)	Библиотеки модулей, эвристик и продукции-онных правил	Базы данных с фиксированной концептуальной моделью
7	Формируемая при выполнении СПО ТО применительно к текущему запросу средствами механизма логического вывода	Базы вычислительных модулей, эвристик и продукционных правил	Базы структурированных и не структурированных данных с настраиваемой концептуальной моделью

ТМИ применительно, как к результатам измерений отдельных параметров, так и к их совокупностям.

Определяющую роль в обеспечении данной тенденции играет СПО ППО как аппарат формализации имеющихся априорных сведений о ТО и формального представления аксиоматики построения процесса обработки, реализуемой в дальнейшем в архитектуре СПО ТО.

При этом универсализация СПО АКОИ не является самоцелью, а выступает как средство обеспечения адекватности инструментальных средств организации и проведения обработки текущим требованиям к форме и содержанию этого процесса.

В связи с этим наилучшими адаптационными качествами, а следовательно и более высоким уровнем универсальности, будет обладать СПО АКОИ, порождающая компонента которого обеспечивает независимое, наиболее корректное и компактное исходное представление компонентов СПО ТО. Порождающая компонента такого СПО АКОИ характеризуется последней строкой табл.1.

Однако этими же свойствами характеризуются такие системы обработки информации как оболочечные экспертные системы и относимые к совокупности программных систем искусственного интеллекта (СИИ). Таким образом, тенденция универсализации СПО АКОИ средствами СПО ППО обеспечивается, по сути теми же средствами, что и интеллектуализация ПП обработки ТМИ. Настоящий уровень достижений в этом направлении и представлен на рис.2.

Заключение

Рассмотренные обстоятельства определяют стратегию организации объективной оценки свойств и характеристик СПО АКОИ, предусматривающую:

– выделение в СПО АКОИ компонентов описания и порождения в интересах оценки свойств и характеристик функционально эквивалентной программной продукции;

– оценка эффективности построения СПО АКОИ, определение случайностей и закономерных тенденций его развития возможны только на основе выделения и анализа аксиоматики реализуемого СПО ППО как основы сопоставления типов и версий СПО АКОИ;

– целенаправленная функционально эквивалентная модернизация СПО АКОИ осуществляется как модернизация СПО ППО по крайней мере не снижающая уровень его выразительной способности;

– уровень и интеллектуальная сложность средств порождения должны быть не ниже уровня и сложности представляющего интерес процесса обработки измерительной информации конкретных ТО.

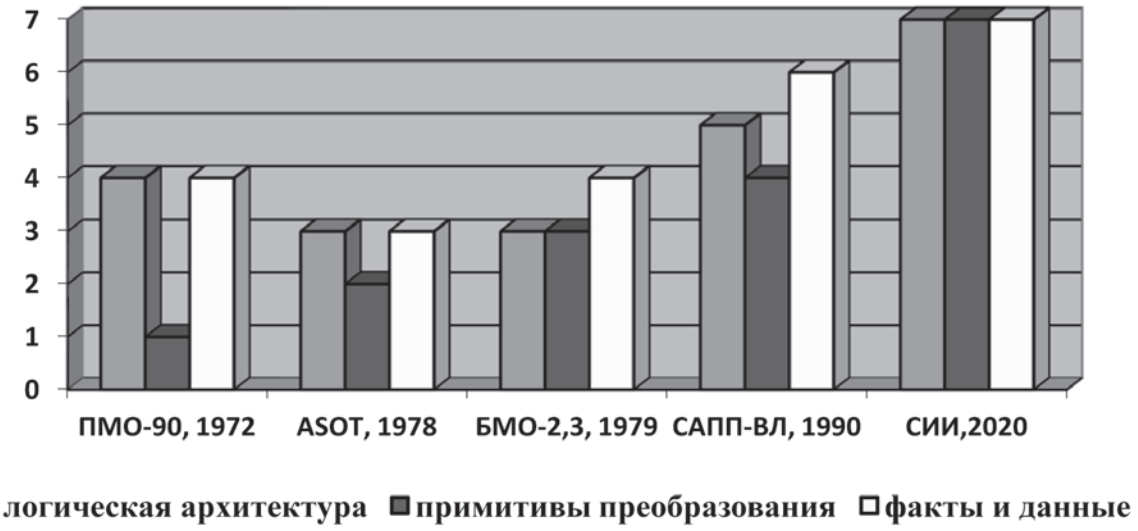


Рис. 2. Уровень достижений в направлении универсализации и интеллектуализация ПП обработки информации

П. Ю. Хахамов
кандидат военных наук, доцент,
ОАО «Научно-исследовательский институт «Рубин»

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ОРГАНОВ ИНФОТЕЛЕКОММУНИКАЦИОННОГО ОБЕСПЕЧЕНИЯ К ВЫПОЛНЕНИЮ ФУНКЦИОНАЛЬНЫХ ЗАДАЧ В УСЛОВИЯХ КРИЗИСНЫХ СИТУАЦИЙ

В работе рассматриваются концептуальные подходы, позволяющие разработать модель подготовки специалистов в ходе подготовки специалистов органов инфотелекоммуникационного обеспечения (ОИТКО). Данная модель предназначена для повышения качества процесса планирования их профессиональной подготовки путем использования средств автоматизации

Введение

Современное состояние подготовки специалистов ОИТКО к выполнению функциональных задач в условиях кризисных ситуаций, характеризуется тем, что в настоящее время не существует единого подхода к ее проведению. При этом не учитывается данные, характеризующие условия и факторы развития кризисных ситуаций, качество укомплектованности специалистами различного профиля, уровень их обученности и профессионально важных качеств. Процесс подбора и расстановки по штатным должностям специалистов в структурные подразделения ОИТКО осуществляется традиционными методами без применения средств автоматизации. Кроме того, структурные подразделения ОИТКО могут быть представлены группами профильных специалистов комплексов инфотелекоммуникационного обеспечения, что также необходимо учитывать при организации их подготовки к выполнению функциональных задач.

Таким образом, на основании вышеизложенного возникает необходимость в разработке соответствующей модели, позволяющей спрогнозировать результаты подготовки специалистов без практического развертывания и эксплуатации сил и средств ОИТКО и теоретического обоснования сроков, содержания и порядка ее организации для конкретных условий обстановки.

Концептуальные основы моделирования подготовки специалистов ОИТКО к выполнению функциональных задач в условиях кризисных ситуаций

Предлагаемая в настоящей работе модель предназначена для определения времени подготовки специалистов и оценки уровня готовности ОИТКО к функционированию в условиях кризисных ситуаций, на определенный момент времени после планируемого начала процесса подготовки.

Структурно модель состоит из следующих модулей: модуль формирования и корректировки исходных данных; модуль определения уровня обученности специалистов при подготовке к выполнению функциональных задач в условиях кризисных ситуаций; модуль определения уровня ППП специалистов; модуль автоматизированной расстановки специалистов на штатные должности; модуль формирования выходных данных (Рис. 1)

В состав исходных данных (ИД) включены: данные, характеризующие возможное развитие кризисной ситуации; требования нормативных документов, регламентирующих организацию и сроки подготовки ОИТКО к функционированию в условиях кризисных ситуациях; требования нормативных документов по комплектованию специалистами ОИТКО; учетные данные специалистов; организационно штатные структуры ОИТКО.

Рис. 1. Общая структура модели подготовки специалистов ОИТКО к выполнению функциональных задач в условиях кризисных ситуаций

Модуль формирования и корректировки исходных данных позволяет задавать векторы параметров (концепты), характеризующие кризисные ситуации, при которых обеспечивается предоставление услуг специального инфокоммуникационного обеспечения, а также структурировать информацию о специалистах ОИТКО. Кроме того в данном модуле предусматривается возможность вносить изменения об уровне обученности и профессионально-психологической пригодности (ППП) специалистов, определяемых по результатам последующего моделирования.

В первом модуле определяется начальный уровень обученности базирующийся на методологии итеративного научения и теории статистического обучения [1,2], а полученные в ходе расчета результаты учитываются при автоматизированной расстановке специалистов на штатные должности в соответствующем модуле предлагаемой модели.

В модуле определения уровня профессиональной психологической пригодности специалистов вычисляется показатель прогнозируемой успешности профессиональной деятельности специалистов, определяемый с помощью известных тестовых конструкций. В результате выносится итоговое заключение о профессиональной пригодности к выполнению функциональных обязанностей в условиях кризисных ситуаций, а полученные в ходе расчета данные учитываются при автоматизированной их расстановке на штатные должности в следующем модуле предлагаемой модели.

В модуле автоматизированной расстановки специалистов на штатные должности с учетом оценки уровня обученности и профессиональной психологической пригодности осуществляется рациональное распределения имеющегося ресурса личного состава, вследствие чего повышается начальный уровень слаженности подразделений. По результатам моделирования с использованием данного модуля становится возможным выявить из большого числа факторов те, которые в наибольшей степени влияют на обученность специалистов.

Так как основной целью при расстановке специалистов является получение максимального уровня готовности ОИТКО к функционированию в условиях кризисных ситуаций на основе оценки их уровня обученности, поэтому необходимо учитывать принцип равномерного и наиболее целесообразного распределения квалифицированных специалистов по экипажам комплексов и структурным подразделениям ОИТКО. Это не противоречит вышеуказанной цели, так как в результате равномерного распределения в каждом из подразделений будет находиться некоторое число наиболее подготовленных специалистов, которые способны обучать остальных. Кроме того, процесс расстановки специалистов должен учитывать помимо их

уровней обученности и профпригодности данные, связанные с восстановлением знаний, навыков и умений менее подготовленных специалистов, т. е. предполагаемой интенсивностью обучения. Интенсивность научения (организация педагогических воздействий) зависит от сложности усваиваемого материала, применяемой при обучении методики, мотивации, уровня памяти и ППП обучаемого [1,2].

Применение данного подхода позволяет определить уровень обученности специалистов к началу процесса подготовки к выполнению функциональных задач в условиях кризисных ситуаций путем последовательного расчета периодов обучения и забывания.

В качестве инструмента, осуществляющего оценку влияния значений педагогических воздействий на обученность специалиста, а также прогнозируемое изменение их значений за некоторое время, может использоваться аппарат искусственных нейронных сетей [5].

Исходя из вышеизложенного, алгоритм рациональной расстановки в рассматриваемом модуле реализован следующим образом. Во время всего периода мониторинга состояния обученности специалистов осуществляется контроль значений педагогических воздействий в процессе их подготовки. Одновременно с этим происходит оценка значений уровней слаженности экипажей (комплексов). Затем, масштабируются значения уровня обученности на максимальный допустимый его показатель для заданного подразделения, а значения педагогического воздействия на максимальное значение уровня обученности, при котором интенсивность обучения самого готового структурного подразделения в составе ОИТКО принимает нулевое значение. Далее по масштабируемым значениям осуществляют обучение искусственных нейронных сетей с радиальными базисными элементами, для аппроксимации зависимостей интенсивности обучения специалистов от значений педагогических воздействий. После чего, матрицы синаптических весов обученных нейронных сетей сохраняются, в соответствии с характеристиками конкретного специалиста. ЛПР о назначении на должность осуществляет инсталляцию нейронных сетей с радиальными базисными элементами по количеству входящих в подразделение ОИТКО специалистов и выполняет контроль значений педагогических воздействий. Масштабируя данные значения, при помощи фокусированной сети прямого распространения с задержкой по времени, ЛПР принимается решение о назначении специалиста на должности, прогнозируется значения педагогических воздействий и подаются данные значения на инсталлированные нейронные сети с радиальными базисными элементами, на выходах которых получают прогнозные значения уровней обученности для каждого специалиста, структурного подразделения и ОИТКО в целом.

В модуле формирования выходных данных аккумулируется информация об уровне слаженности экипажей комплексов ОИТКО, обученности их специалистов, рассчитанных в первом и втором модулях соответственно. Затем с учетом заданного максимального уровня обученности и критериальных значений определяется количество готовых экипажей комплексов к функционированию в условиях кризисных ситуаций и готовность ОИТКО в целом.

Заключение

Полученные таким образом результаты, позволяют провести научно-методическое обоснование адаптации содержания и формы организации подготовки специалистов ОИТКО к выполнению функциональных задач в условиях кризисных ситуаций путем обоснованного назначения их на должности, предложений по совершенствованию системы подготовки специалистов для конкретных условий обстановки.

СПИСОК ЛИТЕРАТУРЫ

1. Новиков, Д.А. Закономерности итеративного научения. – М.: Институт проблем управления РАН, 1998. – 77 с.

2. Свиридов, А.П. **Статистическая теория обучения: монография.** – М.: Издательство РГСУ, 2009. – 570 с.

3. Хахамов, П.Ю. Модель подготовки специалистов органов инфокоммуникационного обеспечения специального назначения к выполнению функциональных задач в условиях кризисных ситуаций. [Текст] / П. Ю. Хахамов, Д. В. Жердев // Информационные технологии в инновациях, медико-биологических и технических науках: сборник научных трудов Пятого международного научного конгресса «Нейробиотелеком-2012» : (Санкт-Петербург, 6–7 декаб. 2012 г.) / СПб Гос. университет им. проф. М. А. Бонч-Бруевича. – СПб. : СПбГУТ им. проф. М.А. Бонч-Бруевича. – 2013. – С. 259–264.

П. Ю. Хахамов
кандидат военных наук, доцент,
ОАО «Научно-исследовательский институт «Рубин»

МОДЕЛИРОВАНИЕ МЕХАНИЗМА ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ НА ФУНКЦИОНИРОВАНИЕ ОРГАНОВ ИНФОТЕЛЕКОММУНИКАЦИОННОГО ОБЕСПЕЧЕНИЯ В УСЛОВИЯХ КРИЗИСНЫХ СИТУАЦИЙ

В работе рассматриваются основные подходы моделирования деструктивного воздействия на функционирование органов инфотелекоммуникационного обеспечения с использованием метода анализа иерархий и когнитивных карт.

Введение

В последние десятилетия на территории Российской Федерации наблюдается тенденция к росту количества и масштабов кризисных ситуаций (КС). При ликвидации их последствий становится насущной проблема инфокоммуникационного обеспечения деятельности органов государственной власти (ОГВ), что определяет перечень задач для органов инфотелекоммуникационного обеспечения (ОИТКО), представляющих инфотелекоммуникационные услуги (ИТКУ) ОГВ из неподготовленных районов.

Сложность и многогранность их функционирования требуют выбора наиболее рационального варианта действий из множества возможных, который должен опираться на строгие математические расчеты и модели.

Моделирование механизма деструктивного воздействия на функционирование ОССИ в условиях кризисных ситуаций

Моделирование механизма деструктивного воздействия на функционирование ОИТКО в условиях кризисных ситуаций осуществляется поэтапно. На первом этапе подготавливаются исходные данные и задаются векторы параметров (концепты), характеризующие кризисные ситуации при которых обеспечивается предоставление ИТКУ. На втором этапе осуществляется моделирование развития кризисной ситуации с помощью когнитивной карты (КК) рассматриваемого процесса для выявления существенных фаз, факторов и продолжительности кризисной ситуации в целом. Результаты моделирования используются для оценки деструктивных воздействий и определения количества пунктов управления ОГВ, перечня ИТКУ и количества информационных направлений между соответствующими пунктами управления, которые систематизируются и формируются на завершающем этапе с целью использования в качестве исходных данных для прогнозирования функционирования ОИТКО.

Подготовка исходных данных (ИД) должна учитывать: факторы, оказывающие влияние на развитие КС; продолжительность и логические взаимосвязи ее фаз; состав и порядок функционирования системы государственного управления; перечень предоставляемых ИТКУ; физико-географические (особые природно-климатические), экономические и социально-политические условия в районах КС; состав, состояние и возможности ОИТКО в регионе КС.

На основании работ [1,2] становится возможным предположить, что подготовка исходных должна учитывать ряд слабоструктурированных факторов и проблем. Реализация этого подхода осуществляется путем применения метода анализа иерархий (МАИ), в котором рассматриваемый процесс представляется в виде иерархии (рис.1) и используется стандартная итерационная схема, когда на каждом уровне,

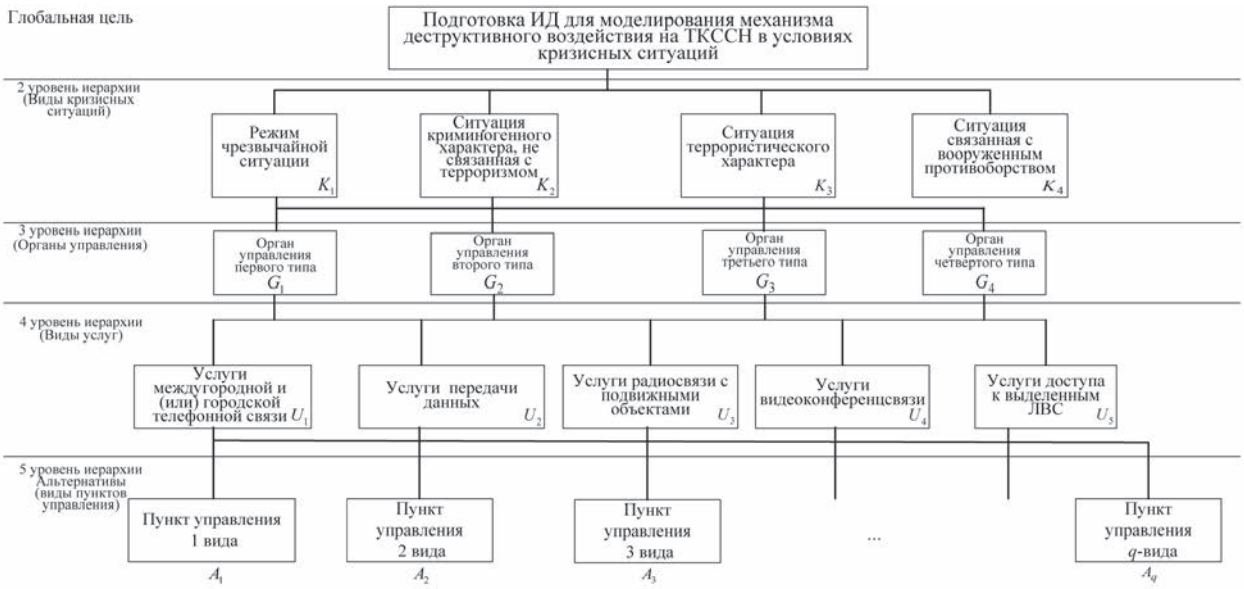


Рис. 1. Иерархическое представление процесса подготовки исходных данных для моделирования механизма деструктивного воздействия на ОИТКО в условиях кризисных ситуаций (вариант)

начиная со второго, составляются матрицы парных сравнений для определения вектора локальных приоритетов параметров (концептов), его характеризующих.

В зависимости от цели моделирования, становится возможным за счет структурирования исходных данных обеспечить формирование вектора параметров в виде совокупности векторов локальных приоритетов концептов каждого уровня рассматриваемой иерархии, характеризующих КС при которых обеспечивается предоставление ИТКУ на пунктах управления ОГВ $P^{\text{КС}} = \{K_n, G_m, U_p, A_q\}$, где – n – количество рассматриваемых видов КС; m – число групп рассматриваемых типов ОГВ; p – количество ИКУ; q – количество пунктов управления ОГВ обеспечиваемых соответствующими ИТКУ в различных условиях кризисных ситуаций. Концепты, характеризующие условия КС, представлены в таблице 1.

Для выявления и анализа типовых событий, продолжительности фаз кризисной ситуации предлагается обобщенная модель в виде когнитивной карты, разработанная с использованием методологии когнитивного моделирования, общий вид которой представлен на рис. 2.

Общая схема *(алгоритм)* моделирования *заключается в следующем [2]:* задается начальное состояние возможной ситуации, определяемое начальными значениями переменных состояния; имитируется воздействие некоторой угрозы путем изменения значений концептов деструктивных воздействий; производится расчет изменения переменных состояния для всех концептов.

Далее находятся установившиеся значения переменных состояния концептов, а также отклонения этих значений по отношению к переменным состояния тех концептов, на которые не оказывается деструктивное воздействие. Если указанные отклонения переменных недопустимы, то полученные значения характеризуют степень влияния деструктивных воздействий. Предотвращение, смягчение или уменьшение влияния деструктивных воздействий осуществляется за счет целенаправленного изменения переменных состояния путем влияния на концепты возможных действий. Для этого можно использовать алгоритм работы искусственных нейронных сетей. При изменении концепта в каком-то направлении, он увеличивает его положительные веса связей когнитивной карты. Если значения концептов меняются в противоположном направлении, то алгоритм увеличивает его отрицательные веса связей.

Таблица 1

Перечень концептов, используемых при моделировании деструктивного воздействия на ОИТКО

Концепт	Наименование	Переменная состояния, X_i
Базовые концепты $C=\{C_1,C_2,...C_n\}$		
C_1	Кризисная ситуация, K_1	Длительность, сутки
C_2	Кризисная ситуация, K_1	Длительность, сутки
C_3	Кризисная ситуация, K_1	Длительность, сутки
C_4	Кризисная ситуация, K_1	Длительность, сутки
C_5	Фаза кризисной ситуации, F_1	Длительность, сутки
C_6	Фаза кризисной ситуации, F_1	Длительность, сутки
C_7	Фаза кризисной ситуации, F_1	Длительность, сутки
C_8	Фаза кризисной ситуации, F_1	Длительность, сутки
C_9	Фаза кризисной ситуации, F_1	Длительность, сутки
C_{10}	Территория региона кризисной ситуации, S	Площадь. Га
C_{11}	Органы управления государственной власти (ОГВ), G_m	Количество, единиц

Перечень концептов, используемых при моделировании деструктивного воздействия на ОИТКО

C_{12}	Пункты управления ОГВ, A_q	Количество, единиц
C_{13}	Должностные лица ОГВ, $N_m^{\text{ДЛ}}$	Численность, человек
C_{14}	Информационные направления между ПУ, $I_q^{\text{ПУ}}$	Количество, единиц
C_{15}	Виды ИТКУ, U_p	Количество, единиц
Концепты управляющих воздействий (принимаемых решений) $C_i^R \in C$,		
C_{16}	Мобильные многофункциональные инфотелекоммуникационные комплексы ОИТКО (МИТКК), $N_q^{\text{мобил.}}$ на ПУ	Количество, единиц
C_{17}	Функциональные подразделения (ФП) ОИТКО. $N_q^{\text{ФП}}$	Количество, единиц
C_{18}	Персонал ФП ОИТКО $N_q^{\text{лс ФП}}$	Численность, человек
C_{19}	Резерв мобильных МИТКК, $N_q^{\text{мобил рез.}}$ на ПУ	Количество, единиц
C_{20}	Резерв специалистов (персонала) ФП ОИТКО, $N_q^{\text{лс ФП рез.}}$	Численность, человек
Концепты деструктивных воздействий (угроз) $C_i^u \in C$		
C_{21}	Интенсивность деструктивных воздействий, $\lambda^{\text{пор}}$	Количество в сутки
C_{22}	Интенсивность деструктивных информационных (программных) воздействий, $\lambda^{\text{ДИПВ}}$	Количество в сутки
C_{23}	Количество пораженных МИТКК ОИТКО, $N_q^{\text{мобил пор.}}$	Количество, единиц
C_{24}	Количество пораженного персонала ФП ОИТКО, $N_q^{\text{лс ФП пор.}}$	Численность, человек
C_{25}	Количество пораженных ФП ОИТКО. $N_q^{\text{ФП}}$	Количество, единиц

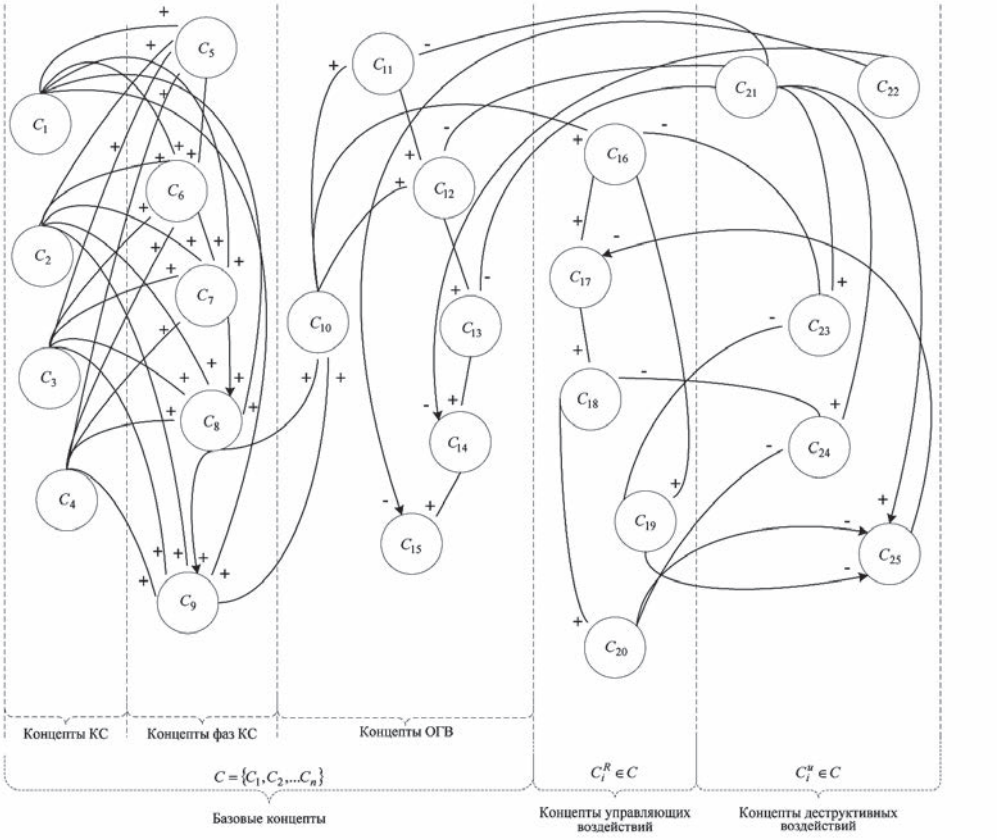


Рис.*2* Нечеткая когнитивная карта моделирования механизма деструктивного воздействия на ОИТКО в условиях кризисных ситуаций

Заключение

В зависимости от характера моделирования деструктивных воздействий на ОИТКО становится возможным получить множество сценариев их деятельности по выполнению функциональных задач в условиях различных кризисных ситуаций, а использование КК для моделирования рассматриваемых процессов придает определенную степень актуальности дальнейшим исследованиям данного направления.

СПИСОК ЛИТЕРАТУРЫ

1. Андрейчиков, А.В., Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике. – М.: Финансы и статистика, 2002. – 368 с.

2. Ямалов, **И.У.** Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций / И. У. Ямалов. – М. : Лаборатория Базовых Знаний, 2010. – 288 с. : ил.

П. Ю. Хахамов
кандидат военных наук, доцент
ОАО «Научно-исследовательский институт «Рубин»

МОДЕЛЬ ПРОЦЕССА КОМПЛЕКТОВАНИЯ ОРГАНОВ ИНФОТЕЛЕКОММУНИКАЦИОННОГО ОБЕСПЕЧЕНИЯ СПЕЦИАЛИСТАМИ ДЛЯ ВЫПОЛНЕНИЯ ФУНКЦИОНАЛЬНЫХ ЗАДАЧ В УСЛОВИЯХ КРИЗИСНЫХ СИТУАЦИЙ

Описываются назначение, структура модели процесса комплектования органов инфотелекоммуникационного обеспечения (ОИТКО) специалистами для выполнения функциональных задач в условиях кризисных ситуаций

Введение

Сложность и многогранность процесса комплектования специалистами ОИТКО для обеспечения их функционирования в условиях кризисных ситуаций значительно осложняет прогнозирование его развития и определения временных показателей. Такое прогнозирование уже не может быть интуитивным, а должно опираться на строгие математические методы расчета и соответствующие процедуры моделирования.

Описание модели процесса комплектования ОИТКО специалистами для выполнения функциональных задач в условиях кризисных ситуаций

Предлагаемая модель предназначена для определения времени комплектования органов инфотелекоммуникационного обеспечения специалистами для выполнения функциональных задач в условиях кризисных ситуаций.

Для формулировки математической модели процесса комплектования следует иметь в виду следующее [1–3]:

– под потоком заявок следует понимать поток специалистов находящихся в резерве (СНР);

– под событием понимается поступление очередной партии специалистов;

– заявка – это отдельно взятый специалист;

– поступление двух единиц ресурса за бесконечно малый промежуток времени одновременно невозможно, поэтому можно считать данный процесс ординарным;

– будем считать, что вероятность поступления очередного специалиста в определенном интервале времени не зависит от выбора начала его измерения, соответственно такой поток является стационарным;

– вероятность поступления заявки (специалиста) в интервале времени t_1, t_2 не зависит от событий, происшедших до момента t_1, таким образом, данный поток без последействия;

– поступившая заявка в систему обслуживается до конца (под системой массового обслуживания следует понимать пункт комплектования специалистами);

– система обслуживания с ожиданием, так как СНР до момента обслуживания находится в районе ожидания;

– обслуживание заявки осуществляется без прерывания;

– очередная заявка не поступает в систему обслуживания (пункт приема мобресурса), пока не обслужится предыдущая;

– принцип обслуживания заявок FIFO (первый пришел первый обслужился);

– рассматриваемая система многоканальная, так как пункты приема специалистов могут имеют

в своем составе структурные подразделения по направлениям деятельности;

Таким образом, на вход системы массового обслуживания – пункта комплектования специалистами (ПКС) – поступает поток специалистов стационарный, ординарный, без последействия. А система массового обслуживания представляет собой многоканальную систему, так как ПКС может имеет в своем составе несколько отделений.

Для определения времени приема специалистов необходимо определить время обслуживания заявки (в нашем случае время приема одного специалиста) и далее, зная число СНР в команде, определяется время обслуживания команды. Общее время комплектования можно определить по формуле:

$$t_{\text{прм}} = N_{\text{ком}}^{\text{СПР}} \cdot \left(N_{\text{СНР}} \cdot t_{\text{обс}}^{\text{СНР}} \right), \qquad (1)$$

где $N_{\text{ком}}^{\text{СНР}}$ – число команд СНР; $N_{\text{СНР}}$ – количество СНР в команде; $t_{\text{обс}}^{\text{СНР}}$ – время прохождения ПКС.

Для разработки модели также необходимо определиться с ограничениями. В нашем случае, время обслуживания заявки в системе есть величина случайная, так как длительность обслуживания СНР на элементах ПКС зависит от уровня подготовки должностных лиц этих пунктов, от исполнительности СНР, наличия у них требуемых документов, а также соответствия тем требованиям, которые предъявляются к процессу комплектования специалистами.

В случае невыполнения требований по комплектованию заявки на обслуживание не принимаются и удаляются из системы, поэтому поток отказов не рассматривается. В работе предлагается моделировать процесс поставки и приема СНР с целью расчета его длительности посредством имитационного моделирования [4].

Функциональная схема имитационной модели процесса комплектования ОИТКО специалистами представлена на рис.1.

Основу функционирования имитационной модели составляют три генератора случайных чисел. Первый формирует время прибытия СНР, второй количество СНР, а третий генерирует случайное время обслуживания одного специалиста. Время прибытия СНР генерируется на основании вводимых исходных данных, которые выбираются при планировании комплектования специалистами, таких как срок поставки $t_{\text{нач}}$, количество ГПЗ $N_{\text{СНР}}$, и предельного времени $t_{\text{кон}}$, в течение которого планируется осуществлять их поставку.

Работа имитационной модели представлена в виде алгоритма на рис 2.

После ввода исходных данных последовательно генерируются значения времени поставки СНР, количества специалистов в команде, значение времени обслуживания одного человека. На следующем этапе производится упорядочение по времени

Рис. 1. Функциональная схема модели процесса комплектования ОИТКО специалистами

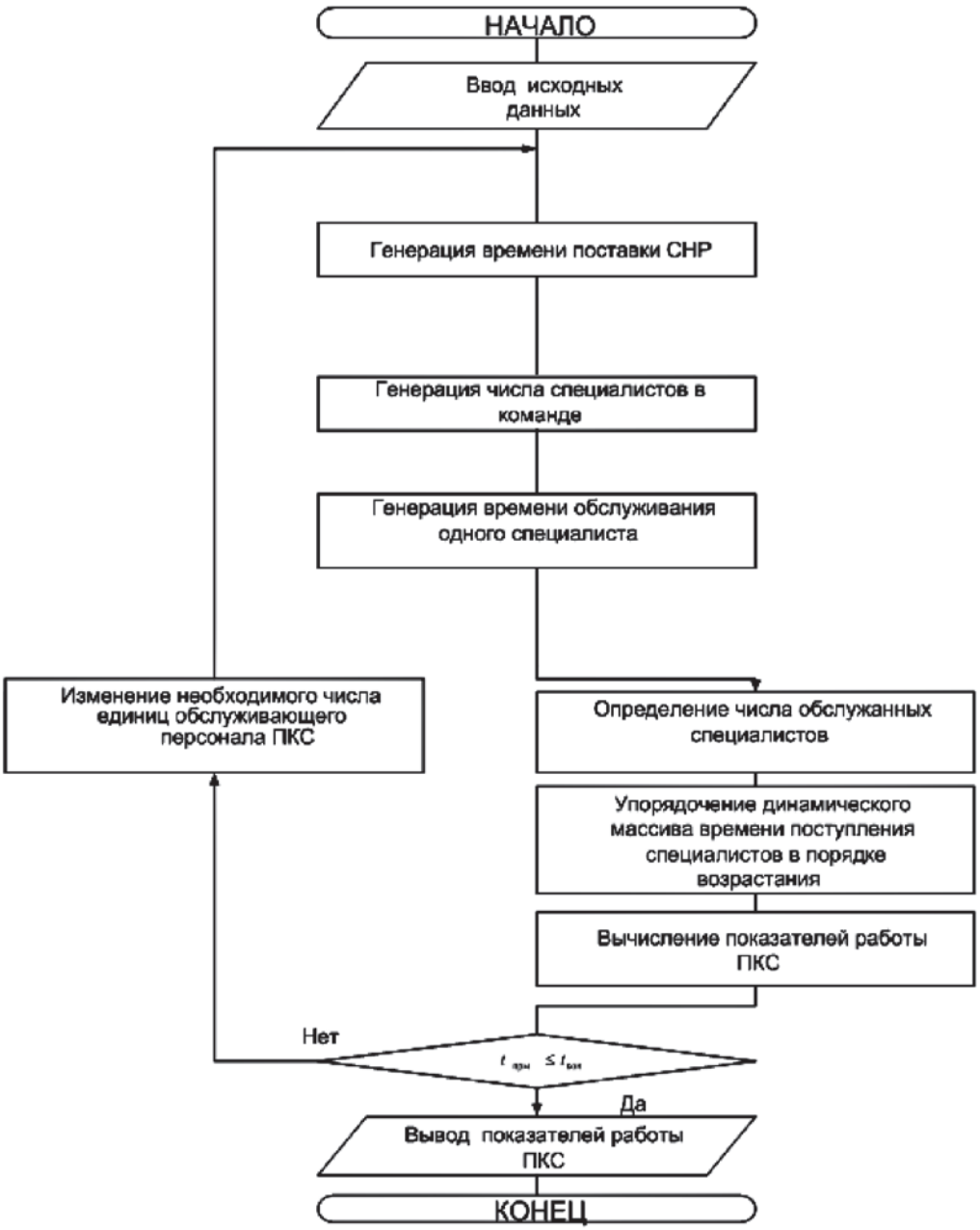


Рис. 2. Алгоритм работы имитационной модели процесса комплектования ОИТКО специалистами

поступления партий (групп) специалистов в порядке возрастания, после чего определяются (1) показатели работы ПКС. Если общее время приема СНР $t_{\text{прм}}$ не превышает предельное значение срока его поставки, тогда выводятся результаты моделирования в виде графиков. В противном случае предлагается увеличить число элементов ПКС (количество обслуживающего персонала ПКС).

Таким образом, используя имитационную модель можно определить время комплектования специалистами ОИТКО для выполнения функциональных задач в условиях кризисных ситуаций.

Заключение

Предлагаемая в настоящей работе модель позволяет оценить процесс комплектования СНР по

критерию времени окончания основных мероприятий при заданном варианте распределения сил и средств. Эти результаты могут использоваться в качестве исходных данных в процессе планирования организации выполнения задач по предназначению ОИТКО в условиях кризисных ситуаций.

СПИСОК ЛИТЕРАТУРЫ

1. Максимей**, И.В.,** Имитационное моделирование на ЭВМ. – М.: Радио и связь, 1998. – 232 с.

2. Шеннон, Р Имитационное моделирование систем: Искусство и наука. – М.: Мир, 1978. – 420 с.

3. Крылов, В.В., Самохвалова С.С. Теория телетрафика и ее приложения. – СПб.: БХВ-Петербург, 2005. – 288 с.: ил.

4. Хахамов**, П.Ю.** и др. Моделирование процессов обслуживания заявок в организационно-технических системах иерархического типа. [Текст] / П.Ю. Хахамов, О.Б. Кривенцов // Известия Орловского государственного технического университета. Серия «Информационные системы и технологии». Вып. № 2. Материалы 3 Всероссийской научно-практической Интернет конференции «Методы прикладной математики и компьютерной обработки данных».– Орел: ГТУ, 2006. – С.155–160

П. Ю. Хахамов
кандидат военных наук, доцент
ОАО «Научно-исследовательский институт «Рубин»

ОСНОВЫ ПРОЕКТИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ ОЦЕНКИ ОБСТАНОВКИ В РЕГИОНЕ

В статье рассматриваются структура и алгоритм функционирования автоматизированной информационно-аналитической системы оценки обстановки в регионе, обеспечивающей реализацию интеллектуальной деятельности должностных лиц органов управления, с целью повышения качества анализа и формирования выводов о складывающейся ситуации с требуемой достоверностью и приемлемым уровнем ошибок

Введение

Информационные системы, обеспечивающие деятельность должностных лиц (ДЛ) органов управления (ОУ) регионов Российской Федерации автоматизированной поддержкой процессов сбора, обработки и анализа данных о состоянии объектов наблюдения, формирования моделей функционирования объекта и наблюдения его состояния, объединяются в класс информационно-аналитических систем (ИАС).

В самом общем виде ИАС можно определить как совокупность ресурсов системы автоматизации (технических, математических, алгоритмических, программных, информационных, лингвистических, организационных и др.), обеспечивающих и реализующих процессы интеллектуальной (творческой) деятельности должностных лиц органов управления при осуществлении ими своих функций [1, 2, 3].

Главной целью создания АИАС является повышение эффективности анализа разнородных данных при оценке обстановки в регионе, оперативности анализа и формирования выводов о складывающейся ситуации, допуская при этом приемлемый уровень ошибок и достоверности анализа не ниже требуемого, а также снижение трудоемкости деятельности ДЛ ОУ.

Описание автоматизированной информационно-аналитической системы оценки обстановки в регионе

Элементы функциональной структуры АИАС в совокупности с организованными ими информационными связями представлены на рис 1.

Основными функциями предлагаемой автоматизированной системы являются предварительная обработка данных, обеспечение ДЛ информацией, необходимой и достаточной для принятия ими решения о состоянии обстановки, и выдача рекомендаций.

Предъявление требований по оперативности вскрытия изменений в обстановке обусловило необходимость разработки АИАС с соблюдением принципов многоконтурности, системности, стандартизации и унификации, открытости, информационной полноты и функциональности [3, 5].

Блок-схема обобщенного алгоритма работы АИАС представлена на рис. 2.

Результаты текущего контроля параметров объектов поступают из основной системы хранения данных через входной интерфейс, реализующий функции согласования исходных данных с внутренним форматом представления информации.

Далее разнородные данные поступают в подсистему обработки, где производится

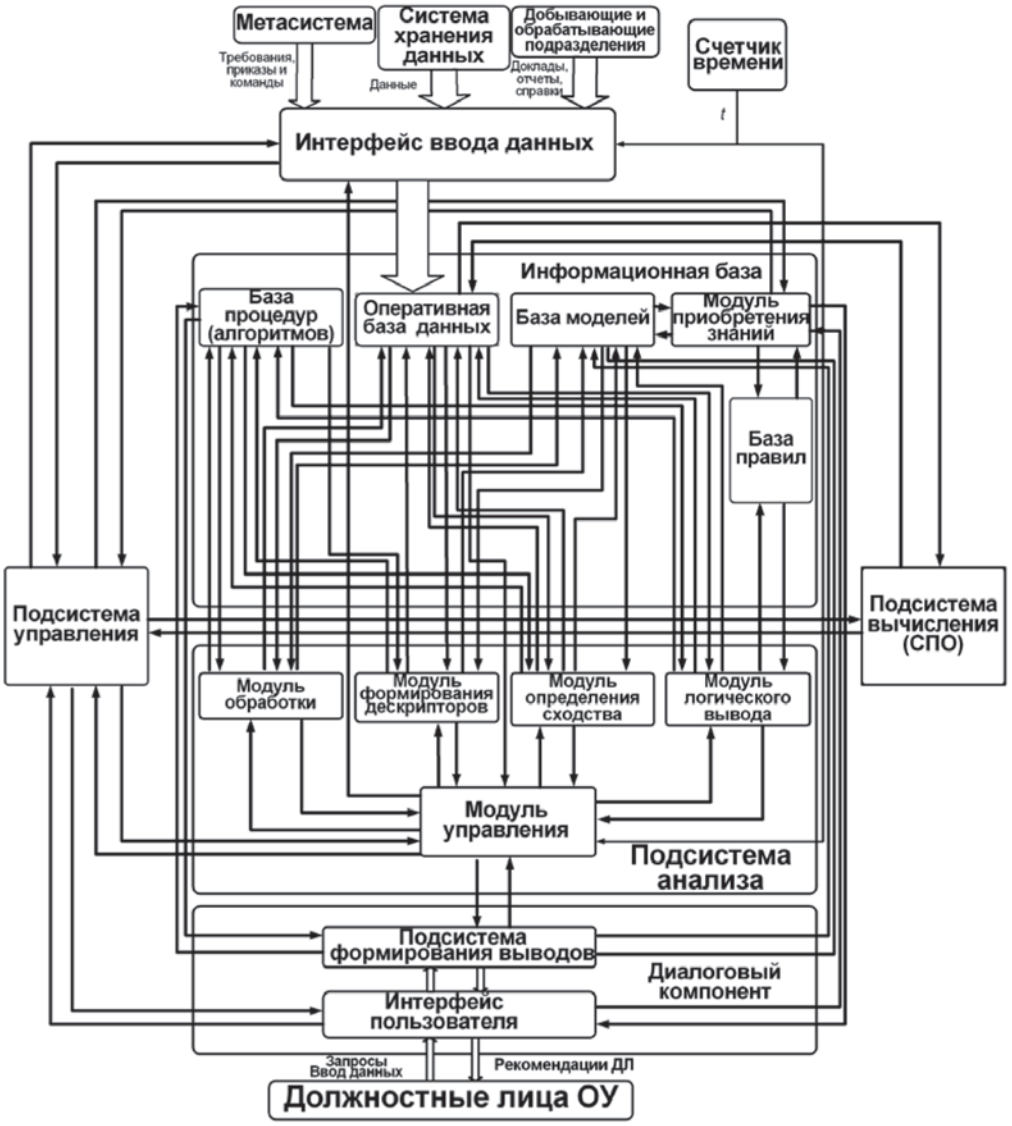


Рис. 1. Элементы функциональной структуры АИАС

нормировка пространства измерения величин в диапазон [0,1].

Расчет величин производится в подсистеме вычисления по запросу от подсистемы обработки. Результаты вычислений заносятся в оперативную базу данных. После обработки входного массива данных, соответствующего текущему значению *t*, при выполнении условия $\tau = \tau_{i_{\text{треб}}}$ подсистема обработки передает в подсистему управления сообщение о готовности массива данных для определения факта изменения значений элементов информационного поля.

Далее полученные данные поступают в подсистему анализа, задачей которой является формирование формализованного описания текущего состояния обстановки в виде кортежа $s = \langle \{X\}, \{T\}, \{V\} \rangle$. Вычисление значений, занесенных в указанные массивы, производится в подсистеме вычисления на основе запроса от подсистемы анализа. По результатам формирования кортежа подсистема анализа передает в подсистему управления сообщение о готовности данных для распознавания ситуации.

Формализованное описание текущей ситуации записывается в оперативную базу данных и значения из массивов передаются в подсистему анализа для формирования операторов расчета коэффициентов сходства для

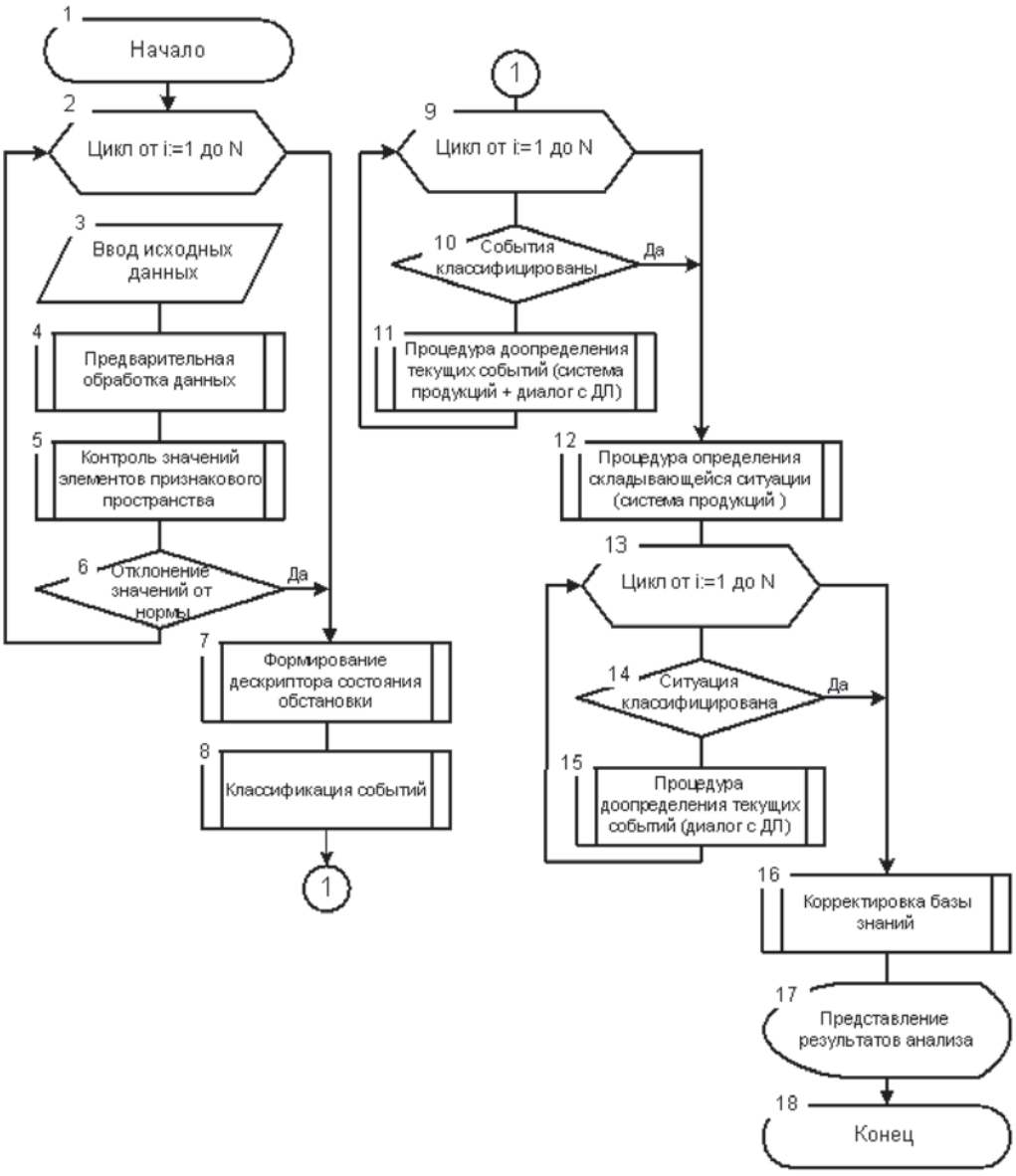


Рис. 2. Блок схема алгоритма функционирования АИАС

определения принадлежности текущего состояния к тому или иному классу.

Совокупность полученных вариантов событий должна быть ранжирована, преобразована в варианты рекомендаций должностным лицам ОУ в качестве реакций на текущую ситуацию. Эта задача решается в подсистеме формирования выводов. В случае, если не сформирован ни один вариант или получены равновероятные оценки нескольких событий, осуществляется переход ко второму этапу распознавания, связанному с применением правил нечеткого вывода. Данный этап реализуется подсистемой анализа.

Работа подсистемы представляет собой последовательность шагов, на каждом из которых из базы выбирается некоторое правило, которое применяется к текущему содержимому дескриптора, описывающего текущее состояние обстановки. Цикл заканчивается, когда осуществляется выбор наиболее вероятной ситуации. Цикл работы иначе называется логическим выводом, который осуществляется с помощью прямого порядка вывода.

Прямой порядок вывода – от состояния объектов наблюдения в регионе, которое описывается дескриптором текущего состояние, к заключению, т. е. состоянию обстановки.

На основе полученных рекомендаций подсистема формирования выводов представляет данные по обстановке в регионе для ДЛ.

Сформированные рекомендации поступают в интерфейс пользователя, решающий задачи согласования форматов представления информации в АИАС и формирования выводов и рекомендаций для должностных лиц ОУ, а также отчетных документов, передаваемых в вышестоящий орган управления.

Заключение

Таким образом, предлагаемая АИАС, построенная на основе комплексного использования составляющих ее подсистем, может значительно повысить качество оценки обстановки в регионе должностными лицами ОУ.

СПИСОК ЛИТЕРАТУРЫ

1. Тараскин, **М. М.** Теоретические проблемы поддержки выработки решения при распознавании ситуации в автоматизированных информационных системах : монография. – СПб.: ВУС, 2002. – 332 с.

2. Бушуев, С.Н., Осадчий, А. С., Фролов, В. М. Теоретические основы создания информационно-технических систем. СПб.: ВАС, 1998. – 404 с.

3. Бушуев, С.Н., Организация распределенного преобразования информации в информационно-технических системах. – СПб.: ВАС, 1994. – 226 с.

4. Гаврилова, Т. А., Хорошевский, В. Ф. Базы знаний интеллектуальных систем. СПб.: Питер, 2001. – 384 с.: ил.

5. Гайдамакин, **Н.А.** Автоматизированные информационные системы, базы и банки данных. Вводный курс: учебное пособие. – М.: Гелиос АРВ, 2002. – 368 с., ил.

П. Ю. Хахамов
Р. *Г.* П*антелеев***

ФОРМИРОВАНИЕ РАЦИОНАЛЬНОЙ СТРУКТУРЫ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ

Анализ основных функций, процедур и операций, реализуемых сотрудниками и подразделениями организационно-технических, дает возможность сформулировать основные подходы по формированию их рациональной структуры.

организационно-техническая система, метод анализа иерархий, линейное программирование, рациональное распределение, численность сотрудников.

Масштабность и важность решений, принимаемых людьми в организационно-технических системах (далее – ОТС), зависит от цели их деятельности, функций и задач, выполнение которых может обеспечить ее достижение. Функции, являясь составляющими инструмента решения задач, одновременно выражают связи, существующие между компонентами ОТС. Поэтому в процессе формирования рациональной структуры ОТС необходимо учитывать общую цель ее функционирования, какие функции должны выполнять структурные подразделения при реализации конкретных классов задач, что в свою очередь позволит произвести декомпозицию функций на процедуры и операции, осуществляемые группами людей (отделами или отделениями) и конкретными должностными лицами (сотрудниками) (рис. 1).

Учитывая вышесказанное, представляется возможным представить процесс формирования ОТС в виде иерархии с использованием метода анализа иерархий (МАИ), с целью определении рационального количества сотрудников в структурных подразделениях (отделах или отделениях), задействованного в выполнении конкретных функций или реализации процедур (операций).

Иерархия строится с вершины – это общая цель или фокус проблемы. В общем случае целей может быть несколько. За фокусом следует уровень наиболее важных критериев. Каждый из критериев может разделяться на субкритерии, за которыми следует уровень альтернатив. Формирование множества альтернатив и критериев осуществляется с учетом рекомендаций, указанных в работах [1–4].

Далее, составляется матрица парных сравнений, в которой с помощью шкалы предпочтений появляется возможность ставить в соответствие степеням предпочтения одного сравниваемого объекта перед другим некоторые числа. Результат сравнения отражает не только факт, но и степень (силу, интенсивность и т. п.) превосходства.

На последнем этапе МАИ проверяется однородность суждений с использованием отклонения величины максимального собственного значения матрицы парных сравнений от ее порядка.

Таким образом, процесс формирования рациональной ОТС в виде иерархической структуры совокупности основных функций (процедур или операций), изображен на рис. 2.

Фокусом иерархии принимается структура ОТС. На первом уровне иерархии находятся основные функции, выполняемые ее отделами, составляющими второй уровень.

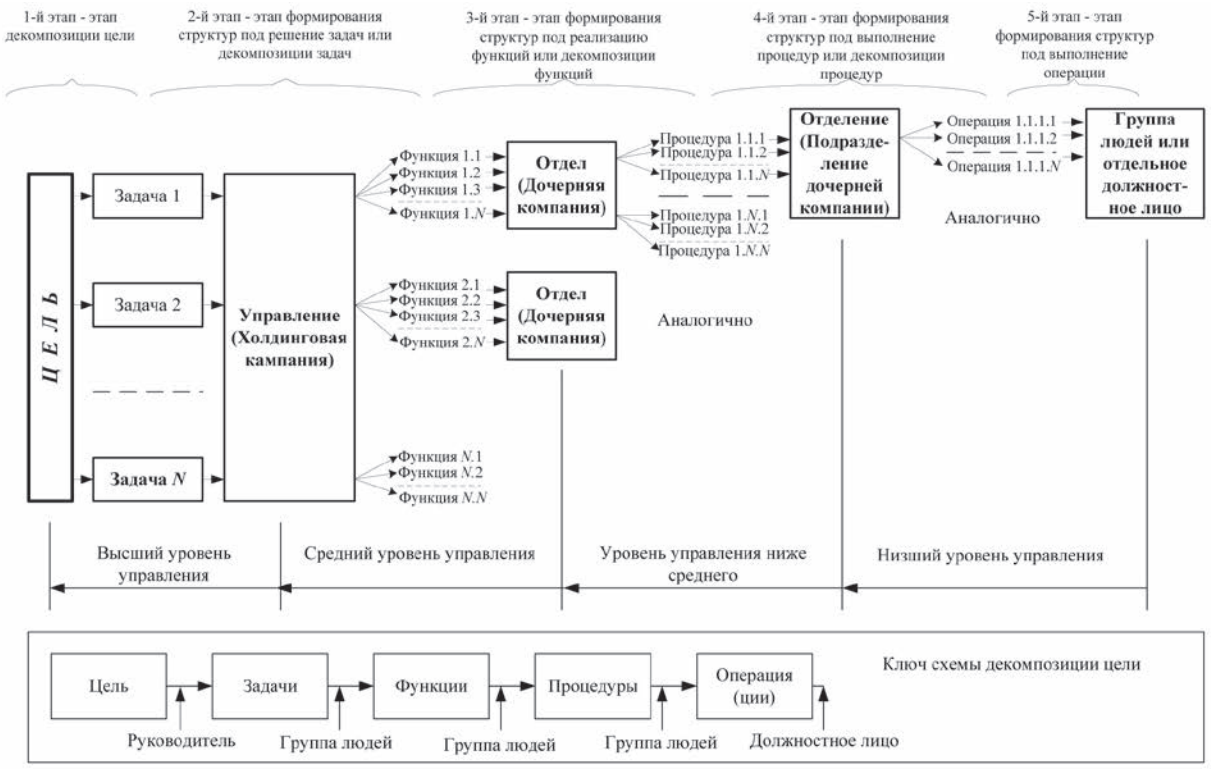


Рис. 1. Схема декомпозиции целей ОТС

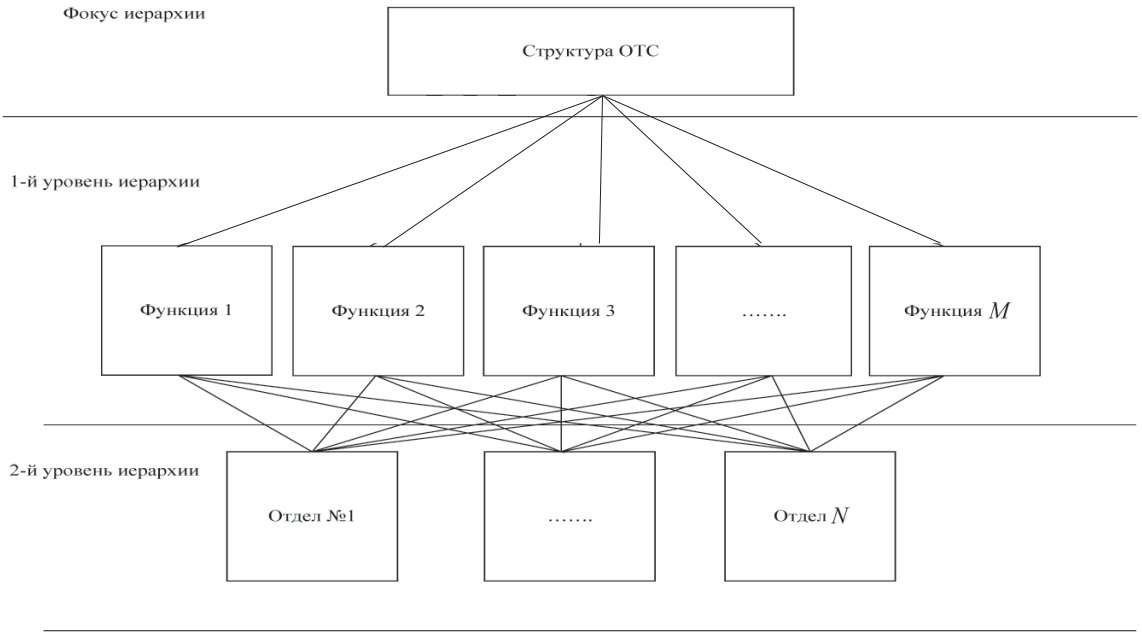


Рис. 2. Иерархическое представление процесса формирования рациональной структуры ОТС

Таким образом, составив матрицы парных сравнений отделов, входящих в ОТС, можно определить их веса векторов приоритетов v_1, v_2, v_n, а на основании матрицы парных сравнений основных функций выполняемых ОТС вычисляются их веса векторов приоритетов p_1, p_2, p_n.

Далее определяются коэффициенты важности отделов ОТС по выражению

$$V_i = \sum_{i=1}^{n} P_i \cdot V_i \qquad (1)$$

где P_i – веса векторов основных функций ОТС; V_i – веса векторов приоритетов отделов, реализующих n функции.

Следующий этап представляет собой процедуру распределения сотрудников ОТС по отделам, реализующим конкретные функции на основе решения транспортной задачи, путем нахождения целевой функции (2) и решения систем уравнений (3) [1,5].

$$F(x) = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} \cdot x_{ij} \qquad (2)$$

$$\begin{cases} x_{11} + x_{12} + x_{1j} = A_1 \\ x_{21} + x_{22} + x_{2j} = A_2 \\ x_{31} + x_{32} + x_{3j} = A_3 \\ x_{i1} + x_{i2} + x_{ij} = A_i \end{cases} \qquad (3)$$

$$\begin{cases} x_{11} + x_{21} + x_{i1} = B_1 \\ x_{12} + x_{22} + x_{i2} = B_2 \\ x_{13} + x_{23} + x_{i3} = B_3 \\ x_{1j} + x_{2j} + x_{ij} = B_j \end{cases}$$

где $A_i = \sum_{j=1}^{m} x_{ij}$ – общее количество сотрудников по отделам, составляющим штатную численность ОТС; x_{ij} – искомая численность сотрудников ОТС; m – количество функций выполняемых ОТС; $B_j = \sum_{i=1}^{n} x_{ij}$ – потребность в сотрудниках для выполнения конкретных функций (таблица 1); n – количество отделов ОТС.

В качестве c_{ij}, предлагается использовать отношение весов векторов приоритетов основных функций ОТС к весам векторов приоритетов отделов, реализующих их (таблица 2), так как это отношение характеризует большую, по сравнению с другими, важность (приоритет) рассматриваемой функции и отдела, следовательно большее количество сотрудников данного отдела необходимо выделить именно для ее реализации.

Таблица 1

Потребность в сотрудниках для выполнения конкретных функций

Количество отделов в ОТС	Потребность в сотрудниках для выполнения основных функций ОТС				
	B_1	B_2	B_3	B_4	B_m
Отдел 1 A_1	$c_{11} \cdot x_{11}$	$c_{12} \cdot x_{12}$	…	…	$c_{1m} \cdot x_{1m}$
Отдел 2 A_2	$c_{21} \cdot x_{21}$	$c_{22} \cdot x_{22}$	…	…	$c_{2m} \cdot x_{2m}$
Отдел N A_n	$c_{n1} \cdot x_{n1}$	$c_{n2} \cdot x_{n2}$	…	…	$c_{nm} \cdot x_{nm}$

Таблица 2

Отношение весов векторов приоритетов основных функций ОТС к весам векторов приоритетов отделов

c_{ij}	Вес векторов приоритетов основных функций ОТС				
Вес векторов приоритетов отделов ОТС	Функция 1 P_1	Функция 2 P_2	Функция 3 P_3	.....	Функция M P_m
Отдел 1 A_1	P_1 / V_1	P_2 / V_1	P_3 / V_1		P_m / V_1
Отдел 2 A_2	…	…	…	…	…
Отдел N A_n	P_1 / V_3	P_2 / V_3	P_3 / V_3		P_m / V_n

В результате расчетов получается матрица начального плана распределения сотрудников для выполнения основных функций ОТС, представленных в таблице 3, в которой на пересечении строк и столбцов указано количество сотрудников $N_{\text{лс}_{ij}}$, которое необходимо выделить для выполнения основных функций ОТС. Далее в зависимости от исходных данных план распределения сотрудников можно пересматривать.

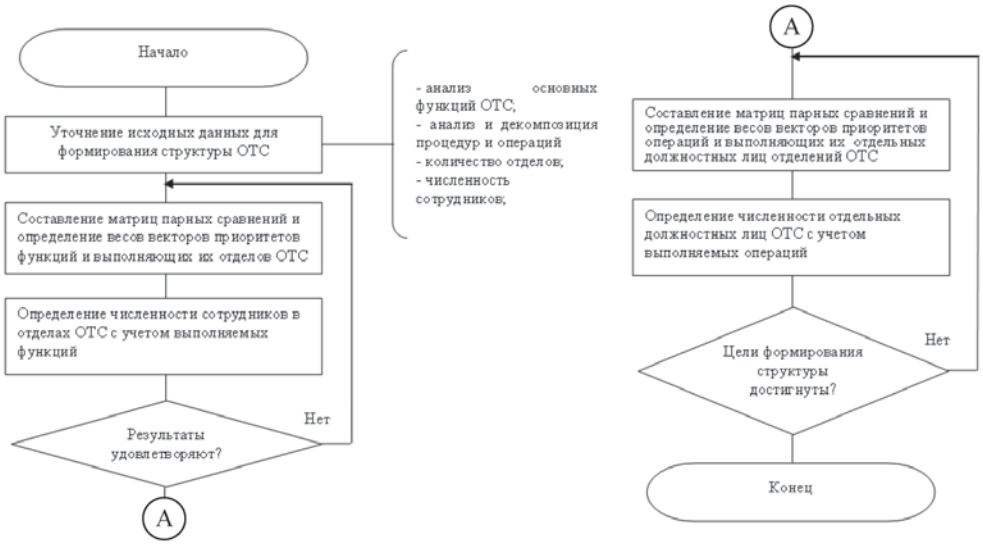


Рис. 3. Формализованная последовательность формирования рациональной структуры ОТС

Таблица 3

Матрица начального плана распределения сотрудников для выполнения основных функций ОТС

Отелы ОТС	Функция 1 P_1	Функция 2 P_2	Функция 3 P_3	.....	Функция M P_m
Отдел 1 A_1	$N_{лс_{11}}$	$N_{лс_{12}}$	$N_{лс_{13}}$	.....	$N_{лс_{1m}}$
Отдел 2 A_2	$N_{лс_{21}}$	$N_{лс_{22}}$	$N_{лс_{23}}$	.....	$N_{лс_{2m}}$
Отдел N A_n	$N_{лс_{31}}$	$N_{лс_{32}}$	$N_{лс_{33}}$	.....	$N_{лс_{nm}}$

Представленный подход можно применять и при обосновании численности отделений, только при этом требуется учитывать численность сотрудников реализующих конкретные процедуры, а не функции. В целом процесс формирования рациональной структуры носит итеративный характер, и общая его последовательность представлена на рис. 3.

Таким образом, рассматриваемый вариант формирования рациональной структуры ОТС позволит снизить долю субъективизма за счет применения метода анализа иерархий и определить количество структурных подразделений и численность их сотрудников с учетом выполняемых функций, процедур и операций.

СПИСОК ЛИТЕРАТУРЫ

1. Формирование рациональной структуры организационно-технических систем / Курносов В.И., Хахамов П. Ю. // Вопросы радиоэлектроники. Сер. СОИУ. 2012. Вып. 2. С. 157–166.

2. Анализ, синтез, планирование решений в экономике. / Андрейчиков А.В., Андрейчикова О.Н. – М.: Финансы и статистика, 2002. – 368 с.

3. Принятие решений. Метод анализа иерархий: пер. с англ. / Саати Т. – М.: Радио и связь,1993. – 278 с.

4. Использование метода анализа иерархий в процессе планирования деятельности органов военного управления. Сборник научных трудов межвузовской научно-теоретической конференции. «Организация и методика информационно-коммуникативного обеспечения военно-образовательного процесса 29-30 ноября 2005 г.»/ Хахамов, П.Ю. и др. – СПб: ВМИ, 2006. – С.128–132

5. Руководство по методам вычислений и применения MathCad. / Ракитин В.И. – М.: ФИЗМАТЛИТ, 2005. – 264 с.

К.Ю.Цветков,
доктор технических наук, профессор
К.В.Ушанев
Военно-космическая академия имени А.Ф.Можайского

ОЦЕНКА ВЛИЯНИЯ ФАКТОРА СТРУКТУРНЫХ СВОЙСТВ ИНФОРМАЦИОННЫХ ПОТОКОВ НА РЕШЕНИЕ ЗАДАЧИ ПАРАМЕТРИЧЕСКОГО СИНТЕЗА ТЕЛЕКОММУНИКАЦИОННЫХ ТРАНСПОРТНЫХ СИСТЕМ

Рассматриваются вопросы обработки нестационарного трафика с применением новых механизмов «Traffic shaping» и «Traffic Policing» для достижения необходимого качества передачи информации в телекоммуникационных транспортных системах.

В современном мире широкое развитие и применение получили высокоскоростные сети связи. Активность развития таких сетей является стремительной во многом благодаря востребованности на массовом уровне услуг сети Интернет, появлению новых приложений (IP-телефония, IPTV), работающих в режиме реального времени, мультимедийных приложений, а также развитию сотовых сетей связи. Все это привело к необходимости передачи по сети различных видов трафика, в том числе, чувствительного к задержкам. Однако, даже значительно возросшие в последнее время пропускные способности каналов и серверов могут оказаться недостаточными из-за продолжающегося роста интенсивности трафика, повышения его структурной сложности, а также повышения требований к качеству обслуживания абонентов. В связи с этим всё большую роль играют методы проектирования, адекватность математических моделей, используемых при этом, в том числе с учетом характера трафика.

Используемые в настоящее время методы параметрического синтеза базируются на применении классических математических моделей потоков, которые хорошо себя зарекомендовали при проектировании сетей с коммутацией каналов, таких как телефонные сети. Современные исследования трафика, передаваемого в транспортных сетях (ТС), показывают, что его статистические характеристики отличаются от тех, которые приняты в классической теории телетрафика. Использование представления о том, что объединение большого числа потоков от независимых источников информации приводит к получению процесса, описываемого пуассоновским потоком, не соответствует истине. Это приводит к тому, что использование традиционных методов расчета параметров ТС и их вероятностно-временных характеристик (ВВХ) приводит к неверным результатам, что вызывает недооценку нагрузки.

Последние исследования свойств информационных потоков в мультисервисных ТС показали, что использование моделей самоподобных (фрактальных) процессов позволяет более точно описывать трафик, передаваемый в данных системах. С практической точки зрения это можно объяснить высокой изменчивостью интенсивности трафика и, как следствие, высокой пачечностью поступления пакетов в узел сети при высокой скорости передачи данных, что приводит, из-за ограниченности буфера, к потерям пакетов.

В отличие от пуассоновских процессов, самоподобные характеризуются наличием последействия: вероятность поступления следующего события зависит не только от времени, но и от предыдущих событий. Это означает, что число текущих событий может зависеть от числа пре-

дыдущих событий в отдаленные промежутки времени.

Исследование влияния самоподобных свойств информационного трафика на качество обслуживания абонентов представляется важным, поскольку при наличии свойства самоподобия, качество обслуживания (QoS – Quality of Service), как правило, ухудшается по сравнению с тем, что наблюдалось бы, в случае пуассоновского трафика. Учет самоподобных (фрактальных) свойств трафика позволит более точно описать и воспроизвести информационный трафик, что, в свою очередь, обеспечит возможность получения показателей QoS, соответствующих реально наблюдаемым. Поэтому актуальными представляются исследования свойств самоподобия трафика информации, их влияния на характеристики QoS в ТС и оптимизация входных параметров ТС с целью обеспечения заданного QoS.

В этом случае необходимо установить взаимосвязь в виде аналитических выражений между параметрами передаваемых потоков и параметрами качества обслуживания. Полученные в результате зависимости необходимо использовать в составе ограничений и целевой функции при решении задач параметрического синтеза. Актуальными при решении данных задач в настоящее время являются методы управления интенсивностью сетевого трафика. Выделяют два основных направления.

1. Аппроксимация поведения трафика на длительных временных интервалах. Используя прогнозируемые данные, возможно создавать эффективные алгоритмы управления трафиком. С практической точки предсказание величины возможной пиковой нагрузки и времени ее появления является очень важным атрибутом для принятия соответствующих мер по обеспечению качества обслуживания QoS.

2. Использование механизмов Traffic shaping (TS) и Traffic Policing (TP), суть которых заключается в следующем:

– с помощью TS сглаживается трафик и пересылается с постоянной интенсивностью путем постановки в очередь (буферизации) пакетов, интенсивность передачи которых превысила среднее значение;

– механизмом TP отбрасываются пакеты, интенсивность которых выше согласованной скорости передачи. С одной стороны, так как в TS не допускается отбрасывания пакетов, является положительным для управления передачей информации реального времени (речь, видео). С другой стороны - вносятся задержки, связанные с буферизацией, что отрицательно сказывается на характеристиках передаваемого трафика.

Предлагаемые методы параметрического синтеза могут быть использованы в процессе проектирования и являются обоснованием для выбора значений параметров конфигурации телекоммуникационного оборудования в узлах сети при планировании и эксплуатации мультисервисных ТС, а также составлении спецификаций устанавливаемого оборудования, при развертывании новых и модернизации существующих мультисервисных ТС.

В.В. Шмелев
кандидат технических наук
ФКГВОУ ВПО «Военно-космическая академия имени А.Ф. Можайского», г. Санкт-Петербург
Е.Б. Самойлов
кандидат технических наук
ФКГВОУ ВПО «Военно-космическая академия имени А.Ф. Можайского», г. Санкт-Петербург

МОДЕЛИ ОПЕРАЦИЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА И КОНТРОЛЯ ПРАВИЛЬНОСТИ ОПЕРАЦИЙ

Рассматривается недостатки существующего способа представления и контроля технологических графиков выполнения операций технологического процесса испытаний и применения объектов ракетно-космической техники. Предлагается способ формализации технологических графиков и процесса их контроля на основе сетей Петри и формальных грамматик.

Введение

Испытания и применение объектов ракетно-космической техники (РКТ) можно представить как совокупность технологических процессов, т.е. совокупности операций, выполнение которых в установленной последовательности преследует определенную цель. При ведении технологической документации на объектах РКТ, а также их проектировании и разработке, технологические процессы обычно отображают с помощью технологических графиков (карт). Технологический график можно определить как графическое отображение технологического процесса, содержащее необходимые сведения для его выполнения [1]. Зачастую под технологическим графиком понимается циклограмма соответствующего процесса, которая обычно изображается с помощью блок-схем.

В качестве примера на рис. 1 приведена блок-схема фрагмента циклограммы одного из режимов функционирования объекта РКТ.

Записи «Операция 1», «Операция 2» и т.д. обозначают соответствующие операции, «Условие 1» и «Условие 2» – проверку соответствующих условий. В практике испытаний и применения объектов РКТ проверка условий заключается в сравнении значений измеряемых и вычисляемых параметров с заранее заданными допусками [2]. Положительный результат проверки обозначен символом «+», отрицательный символом «–». Циклограмма состоит из 5 операций. Операции 1, 2 и 5 безусловно выполняются, операция 3 выполняется только при положительном результате проверки условия 1, операция 4 – условия 2.

Контроль выполнения операций технологического графика

При испытаниях и применении РКТ решается задача контроля правильности выполнения операций. Это осуществляется в автоматизированном режиме, когда оператору выводятся на экран ожидаемые и фактические значения времен контрольных меток циклограммы. При этом автоматизация заключается в выводе результата сравнения ожидаемого и фактического значений времени контрольных меток. Для визуализации процесса отслеживания (контроля) используется инструмент диаграмм Ганта [3]. Такой способ отслеживания циклограммы обладает следующими недостатками:

– отсутствует методическое обеспечение автоматической генерации диаграмм Ганта по существующим технологическим графикам;

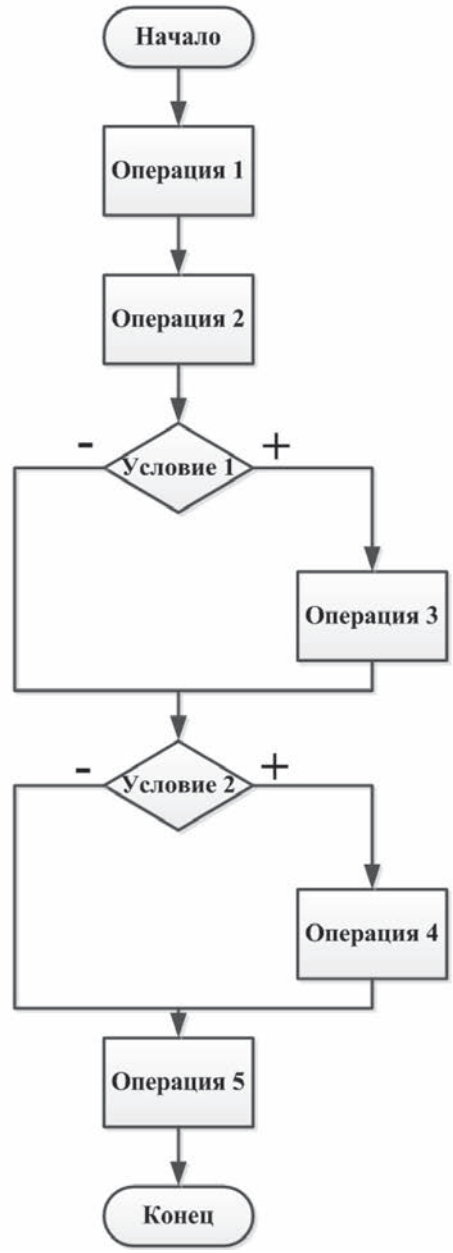


Рис. 1. Блок-схема фрагмента циплограммы

– затруднительно отобразить возможные ветвления в циклограмме (которые наглядно представляются в блок-схемном виде);

– затруднительно отслеживать в потоковом виде несколько режимов;

– невозможно перестроить операции (этапы) циклограммы без участия человека.

Для устранения этих недостатков и создания информационной системы, решающей задачи полностью автоматического контроля циклограмм функционирования объекта РКТ с возможность их перестройки, необходимо разработать формальную модель как самой циклограммы, так и процесса ее контроля.

Общие модели циклограммы и процесса ее контроля

Рассмотрим возможность применения аппарата сетей Петри [4], модернизировав его под особенности рассматриваемой предметной области.

Модель циклограммы в виде сети Петри содержит позиции и переходы. Позиции здесь выступают индикаторами стационарных состояний процесса функционирования, а переходы – индикаторами процессов, проходящих на борту объекта.

В модели контроля циклограммы позиции являются ячейками памяти, в которые записываются переменные. Срабатывание переходов является флагом для изменения состояния процессов в работе программы отслеживания. При этом структура сетей Петри, моделирующих и циклограмму, и процесс ее отслеживания, будет идентичной.

На рис. 2 представлена модернизированная сеть Петри, моделирующая процесс отслеживания циклограммы, изображённой на рис. 1.

Для начала работы необходимо наличие входного сигнала «Запуск». Данная позиция имеет вид полукруга (подробнее см. [5]). При получении данного сигнала запускается переход «Н1» (начало операции 1), что является флагом для начала визуального отслеживания операции 1. Отслеживание операции 1 фиксируется активацией позиции «Вып1» (выполняется операция 1).

Совокупность переходов «Н1» и «К1» (конец операции 1) является индикаторами начала и окончания отслеживания операции 1. Здесь переходы «Н1» и «К1» по сути являются единым переходом, имеющим длительность срабатывания Т1. Разделение единого перехода является необходимым, так как следует адаптировать разрабатываемый инструмент к возможности наличия условий окончания отслеживаемой операции, а также возможности извлечения информации, получаемой в процессе её выполнения.

Завершение отслеживания операции 1 фиксируется срабатыванием перехода К1, после чего флаг-фишка помещается в позицию «Зак1» (операция 1 закончена), которая является

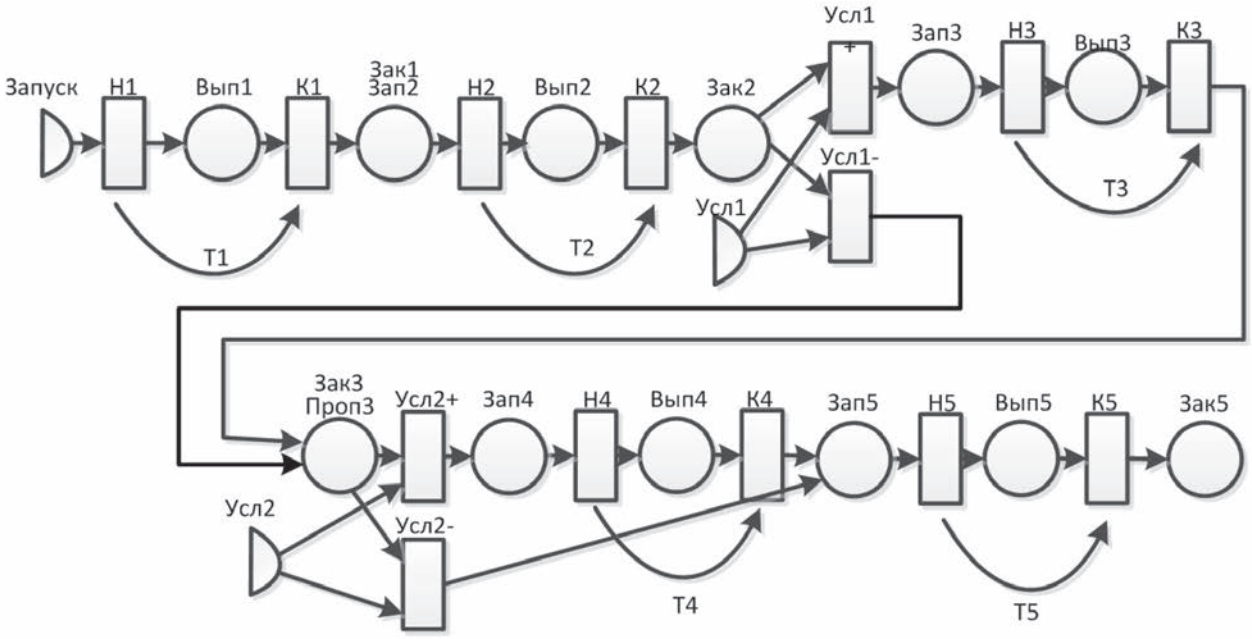


Рис. 2. Общая модель циклограммы в виде модернизированной сети Петри

индикатором выполнения операции 1. Тем самым оканчивается визуальное отслеживание операции 1 – она считается выполненной. Данная позиция является также позицией «Зап2», запускающей выполнение – отслеживание операции 2. Процесс отслеживания данной операции не отличается от процесса отслеживания операции 1. Операция 2 будет считаться выполненной по формированию фишки в позиции «Зак2».

Для выполнения операции 3 необходима проверка условия 1. На данном этапе требуются входные данные в виде значений измеряемых и вычислительных параметров. В зависимости от результата проверки указанных входных данных должен сработать соответствующий переход «Усл1+» или «Усл1–». При срабатывании перехода «Усл1+» формируется фишка в позиции «Зап3» для запуска операции 3, а при срабатывание перехода «Усл1–» – фишка в позиции «Проп3», что будет являться индикатором пропуска операции 3, а также флагом для проверки условия 2. Дальнейшее функционирование модели аналогично рассмотренному.

По срабатыванию перехода «К5», обозначающего окончание отслеживания операции 5, формируется флаг в позиции «Зак5», являющийся индикатором выполнения операций 1-5.

Формальные модели циклограммы и процесса контроля операций циклограммы

Формальная модель циклограммы может быть представлена формальным описанием расширенной модели сетей Петри. Такая модель представляет собой совокупностью позиций, переходов, а также их входных и выходных функций. Она строится на основе графической модели циклограммы (см. рис. 2). Расширение классической модели заключается в доопределении переходов временной характеристикой «перетекания» фишки от момента ее поступления на вход перехода до момента ее передачи в выходную позицию. Эта временная характеристика аналогична длительности операции, а входная и выходная функции аналогичны соответствующим функциям, определяемым при описании классических сетей Петри.

Процесс отслеживания может быть представлен с помощью формальной грамматики [6], построенной на формальной модели циклограммы и состоящей из 5 элементов.

1. Конечное непустое множество терминальных символов. Данное множество содержит возможные в рамках отслеживаемой циклограммы варианты состояний позиций: наличие (отсутствие) фишки, возможные значения или интервалы значений характеризующей переменной. Для

рассматриваемого примера данное множество содержит 30 элементов, образованных из двух вариантов состояния 15 позиций.

2. Конечное непустое множество нетерминальных символов, являющимися словами в грамматике. Каждый нетерминальный символ содержит совокупность терминальных символов, каждое слово имеет одинаковую мощность, равную количеству позиций.

3. Правила формирования нетерминальных символов, выводимые из модели циклограммы. Этот элемент модели отслеживания циклограммы содержит множество пар. Первым элементом каждой пары является нетерминальный символ, вторым – нетерминальный элемент, полученный путем реализации входных и выходных функций позиций и переходов в исходном нетерминальном символе. Именно функции определяют способы перехода из одного нетерминального символа в другой. Мощность данного множества правил равна мощности множества нетерминальных символов.

4. Начальный и конечный нетерминальные символы, которые для начального не имеют предшествующего нетерминального символа, а для конечного не имеют последующего символа.

5. Правила работы программы отслеживания – совокупность пар. В каждой паре имеется первая часть – нетерминальный символ, вторая – соответствующее действие на экране или другом средстве индикации процесса отслеживания циклограммы. Например, для начального нетерминального символа программа отслеживания должна отобразить все операции как невыполнявшиеся, для второго символа – отметить приход сигнала, разрешающего выполнение операции 1, для третьего символа – начать отсчитывать долю выполнения операции 1.

Заключение

Дальнейшие исследования этой проблематике целесообразно сосредоточить на проработке особенностей формальной грамматики, в соответствии с которой формируется модель отслеживания операций циклограммы, а также на разработке методики непосредственного отслеживания операций.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 3.1109-82. Единая система технологической документации. Термины и определения основных понятий.

2. Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов. М.: Наука, 2006. – 410 с.

3. Друкер Питер Ф. Менеджмент / Пер. с англ. — М.: ООО «И.Д. Вильямс», 2010. – 704 с.

4. Питерсон Дж. Теория сетей Петри и моделирование систем / Пер. с англ. М.В. Горбатовой и др.; Под ред. В.А.Горбатова. – М.: Мир, 1984. – 264 с.

5. Охтилев М.Ю. Диссертация на соискание ученой степени доктора технических наук. МО РФ.

6. Актуальные вопросы автоматизированной обработки и анализа информационных процессов. Учебное пособие. МО РФ, 1992. – 140 с.

В.С. Шумилин
Академия ФСО России, г. Орел

ЗАЩИТА ЭЛЕМЕНТОВ СЕТЕЙ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО МОНИТОРИНГА

В докладе рассматривается процесс ведения нарушителем несанкционированного мониторинга элементов сети связи посредством анализа демаскирующих признаков, а также предлагается способ управления демаскирующими признаками сети связи, как один из вариантов обеспечения защиты её элементов.

Введение

С развитием информационных и телекоммуникационных технологий, становится актуальным процесс развития сетей связи, путем цифровизации и интеграции их в общемировое телекоммуникационное пространство, что в свою очередь, существенно увеличивает возможности нарушителей по идентификации, вскрытию и воздействию на их элементы.

Порядок проведения несанкционированного мониторинга элементов сети связи

Анализ элементов сети связи осуществляется нарушителем посредством ведения несанкционированного мониторинга (рисунок 1).

Из рисунка 1 видно, что процесс ведения несанкционированного мониторинга элементов сети связи осуществляется поэтапно. Сначала определяются цели мониторинга (необходимость определения состава сети связи, вскрытие структуры сети связи либо выявление алгоритмов функционирования сети связи). Далее анализируются (исследуются) демаскирующие признаки (ДМП) элементов сети связи и процессов их функционирования.

Процесс анализа демаскирующих признаков элементов сети связи реализуется двумя подсистемами: активной и пассивной [1].

Пассивное исследование осуществляет сбор типовых демаскирующих признаков элементов сети связи. К типовым демаскирующим признакам элементов сети связи относятся: форма огибающей сигнала; спектр сигналов; вид излучения, вид модулирующего сигнала; значения параметров сигнала; мощность излучения; количество излучаемых фиксированных частот, взаимные удаления элементов, площадь размещения элементов и др. [2].

Активное исследование предполагает использование комплексных программных воздействий, наиболее часто реализуемыми из которых являются: анализ сетевого трафика, сканирование сети, отказ в обслуживании и др. После анализа демаскирующих признаков переходят к формированию множества вариантов сетей связи, которое включает в себя отображение параметров по демаскирующим признакам, их обобщение и интеллектуальный анализ, что позволяет сформировать «типовые образы» сети связи, отражающие ее функциональные особенности [3].

Предложения по защите элементов сети связи от несанкционированного мониторинга

Анализ существующих средств и методов защиты позволил определить, что демаскирующие признаки элементов сети связи, выявляемые активным исследованием, могут быть скрыты методами разграничения доступа и криптографического закрытия семантической составляющей информационного обмена [4, 5]. Однако существующие методы защиты не всегда эффективны.

В связи с этим возникает необходимость разработки научно-технических предложений, позволяющих осуществлять формирование защищенной сети связи, путем управления

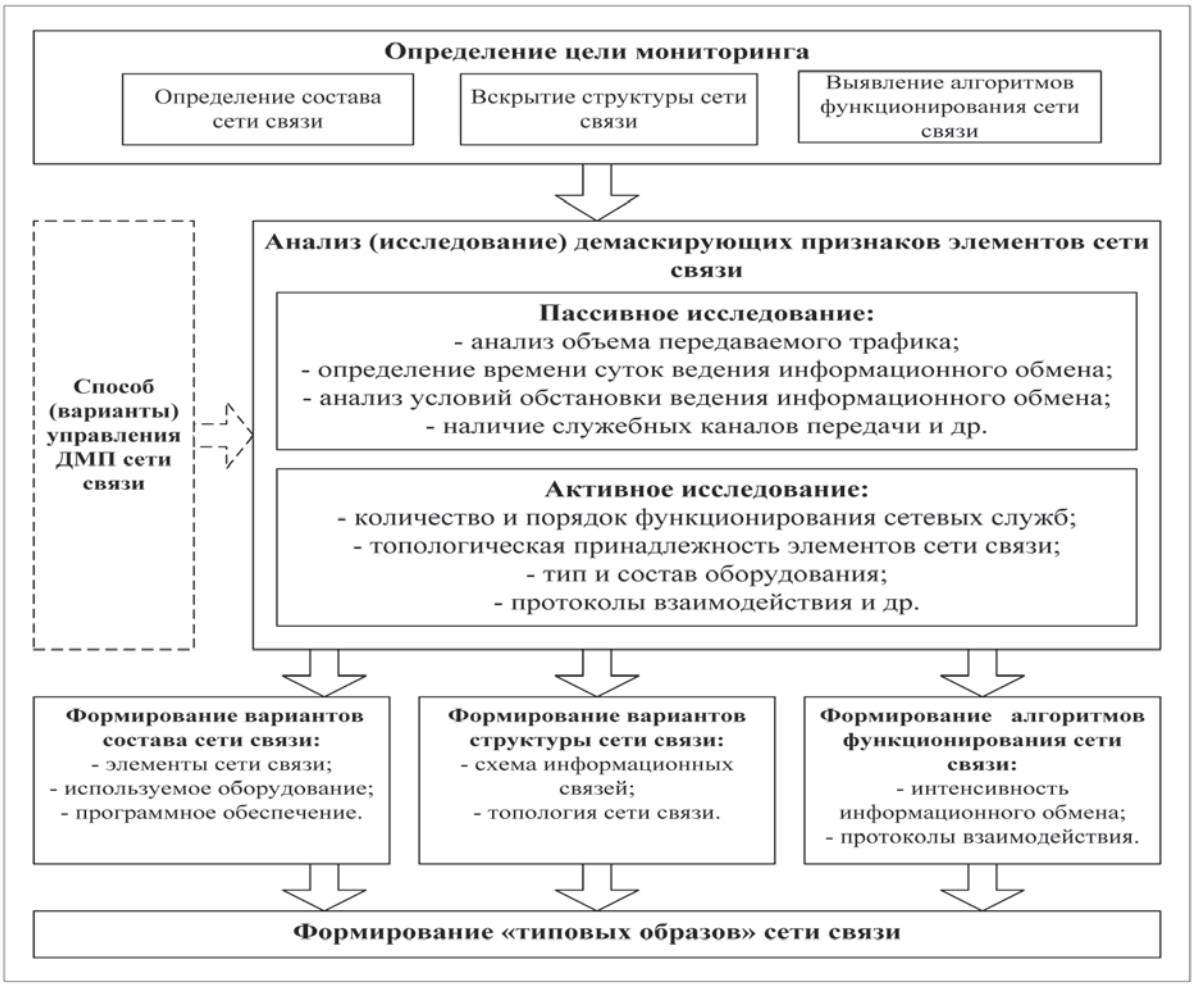


Рис. 1. Обобщенный порядок проведения несанкционированного мониторинга элементов сети связи (вариант)

(ослабления, устранения) ее демаскирующими признаками. В качестве предложения по защите разработан способ управления демаскирующими признаками сети связи [6]. Обобщенная схема, поясняющая способ управления демаскирующими признаками сети связи представлена на рисунке 2.

Суть способа заключается в варьировании значениями управляемых демаскирующих признаков по соответствующим правилам и в заданных пределах, в результате чего, злоумышленник вводится в заблуждение относительно структуры сети связи и параметров её функционирования,что приводит к повышению устойчивости сети связи в условиях деструктивных программных воздействий. В качестве исходных данных задают множество контролируемых параметров демаскирующих признаков сети связи. В результате измерения значений данных контролируемых параметров, в ходе выполнения цикла анализа, формируют группы контролируемых параметров демаскирующих признаков и задают коэффициенты важности для каждой группы. Дополнительно определяется количество управляемых и неуправляемых демаскирующих признаков. Перед развертыванием, разрабатываются варианты ложного функционирования сети связи. После этого осуществляют развертывание сети связи, настраивают основные параметры и применяют ее по назначению. На функционирующей сети связи производят измерение значений контролируемых параметров демаскирующих признаков и запоминают их с целью дальнейшего использования.

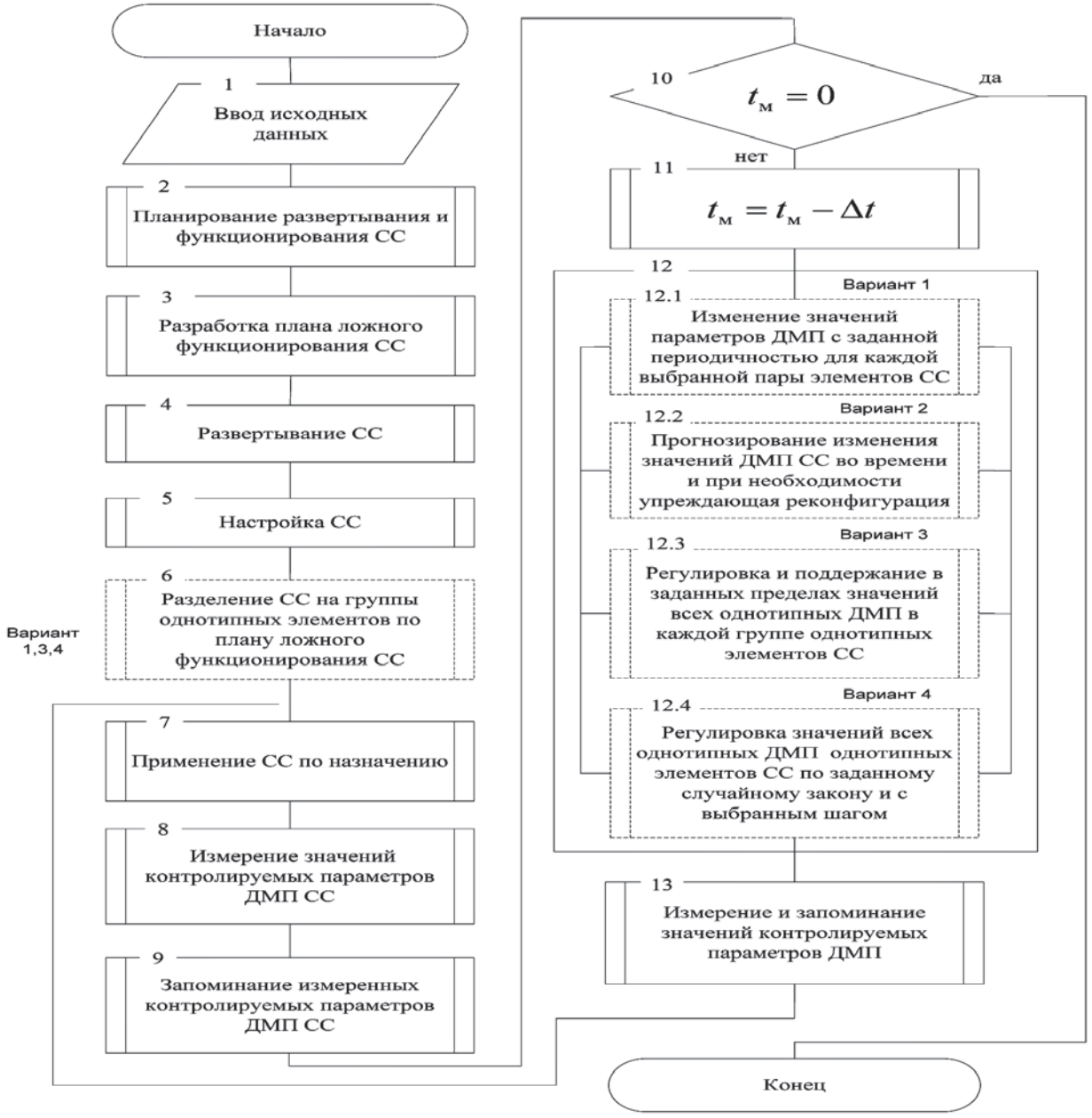


Рис. 2. Обобщенная схема способа управления демаскирующими признаками сети связи

Способ предполагает управление защищенностью сетей связи по нескольким направлениям.

В первом варианте злоумышленник вводится в заблуждение относительно структуры сети связи и ее параметров за счет периодического (по необходимости корректируемого) взаимного изменения демаскирующих признаков на выбранных парах элементов сети связи.

Во втором варианте злоумышленник вводится в заблуждение относительно структуры сети связи и ее параметров на основе прогнозирования значений показателей демаскирующих признаков и, при необходимости, упреждающей реконфигурации сети связи.

В третьем варианте заявленного способа злоумышленник вводится в заблуждение относительно структуры сети связи и ее параметров за счет принудительной регулировки (с заданной периодичностью) и поддержания в установленных пределах на однотипных элементах сети связи значений всех однотипных признаков.

В четвертом варианте злоумышленник вводится в заблуждение относительно структуры сети связи и ее параметров за счет одновременного изменения всех однотипных параметров демаскирующих признаков в каждой группе всех однотипных элементов сети связи по заданному случайному закону и шагу с заданным периодом так, чтобы параметры демаскирующих признаков элементов сети связи попали в заданный интервал значений.

Заключение

Таким образом, в настоящее время становится актуальным вопрос по разработке практических рекомендаций, а также средств, методов(способов) и систем защиты, соответствующих современным условиям безопасного функционирования сетей связи и их элементов в условиях ведения злоумышленником несанкционированного мониторинга. В качестве предложения по защите предлагается использование способа управления демаскирующими признаками сети связи, в котором реализована возможность корректировки значений управляемых демаскирующих признаков ее элементов в заданных значениях и упреждающей реконфигурации, позволяющая снизить эффективность ведения несанкционированного мониторинга элементов сети связи. Кроме того, полученные результаты могут использоваться при проведении исследований по разработке методов и способов защиты сетей связи в условиях внешних деструктивных программных воздействий, а также при проэктировании систем защиты сетей связи в рамках определения защитного ресурса.

СПИСОК ЛИТЕРАТУРЫ

1. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. СПб.: БХВ - Петербург, 2003. – 368 с: ил.

2. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки. – М. : Российск. гос. гуманит. ун-т, 2002. – 399 с.

3. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия. – Труды ИСА РАН, том 41, 2009., 104-146 с.

4. Пат. 2419153 Российская федерация, МПК G06N 5/00. Способ контроля демаскирующих признаков системы связи / Е. В. Гречишников [и др.] ; заявитель и патентообладатель Академия ФСО России. – № 2009125131/08 ; заявл. 30.06.09 ; опубл. 20.05.11, Бюл. № 1. – 22 с. : ил.

5. Пат. 2422892 Российская федерация, МПК G06F 21/20. Способ защиты вычислительной сети / Е. В. Гречишников [и др.] ; заявитель и патентообладатель Академия ФСО России. – № 2010114785/08 ; заявл. 13.04.10; опубл. 27.06.11, Бюл № 18 – 9 с. : ил.

6. Пат. 2450337 Российская федерация, МПК G06F 15/00. Способ (варианты) управления демаскирующими признаками системы связи / Е. В. Гречишников [и др.] ; заявитель и патентообладатель Академия ФСО России. – № 2011117814/08 ; заявл. 03.05.11 ; опубл. 10.05.12, Бюл. № 13. – 19 с. : ил.

В.Н. Шунто
кандидат технических наук, *профессор*
М.О. Татаров
кандидат технических наук
В.С. Догадов
Военно-космическая академия имени А.Ф.Можайского (филиал г.Ярославль).

АВТОМАТИЗИРОВАННАЯ СИСТЕМА МОНИТОРИНГА СОСТОЯНИЯ ВВСТ ЧАСТЕЙ И ПОДРАЗДЕЛЕНИЙ ВКО

Для решения одной из проблем, возникших при переходе к сервисному обслуживанию вооружения, военной и специальной техники ВКО, рассмотрена возможность создания автоматизированной системы мониторинга технического состояния вооружения, военной и специальной техники ВКО. Определены основные задачи предложенной системы и входящих в нее основных подсистем, и основные концепции их создания.

Реформирование системы технического обеспечения войск на современном этапе заключается, прежде всего, в переходе к сервисному обслуживанию вооружения, военной и специальной техники (ВВСТ) ВКО[1]. В настоящее время функционирование системы сервисного обслуживания ВВСТ осложнено рядом серьезных проблем, одна из которых заключается в отсутствии на всех уровнях иерархии системы технического обеспечения своевременной и достоверной (точной) информации о состоянии ВВСТ подразделений и частей ВКО. Это обусловливает актуальность создания автоматизированной системы мониторинга состояния ВВСТ частей и подразделений ВКО. Под автоматизированной системой мониторинга состояния ВВСТ в данном случае понимается система, предназначенная для систематического сбора, накопления и обработки данных о техническом состоянии образцов ВВСТ.

Создание системы мониторинга состояния ВВСТ воинских частей и подразделений, входящих в состав ВКО, позволит:

осуществлять непрерывный контроль состояния ВВСТ воинских частей и подразделений;

прогнозировать состояние образцов ВВСТ на заданный период времени;

оптимизировать состав запасных частей, инструментов и принадлежностей;

осуществлять оптимальное распределение усилий между предприятиями промышленности, ремонтными организациями и сервисными центрами по поддержанию работоспособного состояния образцов ВВСТ.

Для создания системы мониторинга состояния ВВСТ необходимо решить ряд задач, основными из которых являются:

разработка моделей функционирования подсистем сбора и обработки данных о состоянии ВВСТ ВКО;

разработка модели функционирования подсистемы управления;

разработка методов и алгоритмов сбора и систематизации данных о состоянии ВВСТ в подразделениях и частях;

разработка методов и алгоритмов обработки полученных данных на всех уровнях иерархии.

Очевидно, что система мониторинга должна включать в свой состав три подсистемы:

подсистему сбора данных о состоянии ВВСТ;

подсистему обработки данных;

подсистему управления.

Задачами подсистемы сбора данных о состоянии ВВСТ должны быть:

непосредственный сбор данных о состоянии ВВСТ подразделений (частей);

накопление и хранение в базе данных статистических сведений, необходимых для эффективного функционирования подсистем обработки данных и управления;

систематизация (обобщение) данных о состоянии ВВСТ;

передача данных между различными уровнями иерархии.

Для создания подсистемы сбора данных о состоянии ВВСТ подразделений и частей вначале необходимо решить ряд задач, связанных с определением необходимого и достаточного количества параметров, характеризующих состояние ВВСТ, определением области допустимых значений этих параметров, разработкой алгоритмов сбора, систематизации и передачи данных о состоянии ВВСТ.

Необходимое и достаточное количество параметров, характеризующих состояние ВВСТ подразделения (части), определяется типом и техническими характеристиками конкретного образца ВВСТ. Для их определения могут применяться такие методы как дерево отказов, анализ характера и последствий потенциальных отказов. Применение данных методов позволит не только выявить параметры, характеризующие техническое состояние конкретного типа ВВСТ подразделения (части), но и существенно сократить номенклатуру этих параметров.

Областями допустимых значений параметров характеризующих техническое состояние образца ВВСТ в данном случае являются предельно допустимые значения параметров, при которых обеспечивается работоспособное состояние образца ВВСТ. Под работоспособным состоянием образца ВВСТ подразумевается состояние, при котором он способен выполнить требуемую функцию при условии, что предоставлены необходимые внешние ресурсы[3].

Реализация подсистемы сбора данных возможна с использованием современных телекоммуникационных средств и технологий и (или) при помощи электронных носителей информации, с помощью которых может быть организована доставка данных о состоянии образцов ВВСТ в пределах системы мониторинга нарочными. В первом случае реализация подсистемы сбора возможна без введения дополнительной аппаратуры, при условии наличия в составе контролируемого образца ВВСТ вычислительной сети на базе современных сетевых технологий. Передача данных мониторинга в этом случае будет осуществляться в соответствии с установленным в данной сети стандартом. В случае, когда вычислительная сеть в составе образца ВВСТ отсутствует, появляется необходимость либо в развертывании вычислительной сети, либо в организации своевременной доставки данных о текущем техническом состоянии контролируемого образца ВВСТ нарочным.

Подсистема обработки данных должна обеспечивать выполнение различных функций, основными из которых являются:

прогнозирование технического состояния образцов ВВСТ частей и подразделений ВКО на заданный интервал времени;

выработка рекомендаций по продолжению эксплуатации образцов ВВСТ частей и подразделений ВКО, или снятии их с эксплуатации для технического обслуживания (ремонта, восстановления);

выработка рекомендаций по оптимальному распределению усилий между воинскими частями (подразделениями), предприятиями промышленности, ремонтными организациями и сервисными центрами по поддержанию работоспособного состояния ВВСТ при ограниченных ресурсах.

Для создания подсистемы обработки данных о техническом состоянии образцов ВВСТ подразделений и частей необходимо решить ряд задач, связанных с разработкой алгоритмов прогнозирования состояния образцов ВВСТ на заданный интервал времени, разработкой алгоритмов выработки рекомендаций о продолжении эксплуатации образцов ВВСТ или снятии его с эксплуатации для обслуживания, разработкой алгоритмов выработки рекомендаций по оптимальному распределению усилий между воинскими частями (подразделениями), предприятиями промышленности, ремонтными организациями и сервисными центрами по поддержанию работоспособного состояния ВВСТ при ограниченных ресурсах.

Прогнозирование технического состояния образцов ВВСТ является одним из эффективных методов поддержания их эксплуатационной надежности путем своевременного проведения мероприятий по ТО и ремонту. Сущность прогнозирования заключается в определении наиболее вероятного момента появления отказа на основании имеющейся информации о параметрах, определяющих техническое состояние образца ВВСТ или его элементов и принятии мер по его предупреждению, определении сроков и объемов проведения технического обслуживания. При этом различают статистические и аппаратурные (инструментальные) методы прогноза [4].

Сущность статистических методов прогнозирования состоит в том, что на основании известных статистических данных об интенсивности отказа элементов в процессе эксплуатации конкретной аппаратуры производят расчет ее надежности и определение момента для выполнения

профилактических работ (замены, ремонта, регулировки). Располагая статистическими данными о результатах эксплуатации или специальных испытаний различных элементов можно производить статистическое прогнозирование отказов.

Для использования инструментальных методов прогнозирования отказа необходимо располагать результатами периодического контроля параметров ВВСТ при его функционировании в специальном или нормальном режиме, на основе которых можно получить статистические данные о характере изменения того или иного параметра. Недостатком инструментального метода прогнозирования является невысокая достоверность прогноза (из-за малого количества статистических данных).

Выработка рекомендаций о продолжении эксплуатации образца ВВСТ или снятии его с эксплуатации для обслуживания осуществляется на основании проведенных ранее вычислений, в соответствии с текущим техническим состоянием образца ВВСТ и прогнозом его состояния на заданный интервал времени. Исходя из требуемого уровня надежности, определяется время, при достижении которого производится профилактическая замена элементов.

Выработка рекомендаций по оптимальному распределению усилий между воинскими частями (подразделениями), предприятиями промышленности, ремонтными организациями и сервисными центрами по поддержанию исправного, либо работоспособного состояния ВВСТ при ограниченных ресурсах является оптимизационной задачей и может быть успешно решена, например, методами исследования операций[7,8].

Основными задачами подсистемы управления очевидно являются:

автоматизированное формирование заявок на проведение ТО на основании результатов работы подсистем сбора и обработки данных о техническом состоянии образцов ВВСТ;

автоматизированное формирование заявок на пополнение ЗИП;

автоматизированный контроль своевременности оказания услуг по сервисному обслуживанию ВВСТ.

Рассмотренные выше принципы построения системы мониторинга технического состояния ВВСТ, могут быть применены при создании программного обеспечения центра автоматизированного ситуационного управления сервисным обслуживанием ВВСТ[1] и системы территориальных сервисных центров (пунктов, представительств) исполнителя работ по сервисному обслуживанию. Создание указанных сервисных центров (пунктов, представительств) в рамках системы сервисного обслуживания ВВСТ, считается одним из приоритетных направлений для устранения проблем, имеющихся в функционировании системы сервисного обслуживания[1].

На основе результатов работы системы мониторинга ВВСТ, могут быть получены данные об элементах и узлах, значения показателей надежности которых ниже заданных, и чаще всего требуют замены в процессе восстановления ВВСТ, а также элементах, интенсивность отказов которых наиболее высока. Используя полученные данные, возможно, например, оптимизировать состав комплекта запасных частей, инструментов и принадлежностей, под которым понимается запасные части, инструменты, принадлежности и материалы, необходимые для технического обслуживания и ремонта изделий и скомплектованные в зависимости от назначения и особенностей использования[9].

СПИСОК ЛИТЕРАТУРЫ

1. Купреев Д.В., Мирук К.В. Стратегия сервисного обслуживания. //Воздушно-космическая оборона.2013. №2 (69).

2. ГОСТ Р ИСО МЭК ТО 10032-2007: Эталонная модель управления данными.

3. ГОСТ Р 53480-2009 Надежность в технике. Термины и определения.

4. Байхельт Ф., Франкен П. Надежность и техническое обслуживание. Математический подход: Пер. с нем. – М.: Радио и связь,1988.

5. Барлоу Р., Прошан Ф. Математическая теория надежности. Пер. с англ.- М.: Сов. радио, 1969.

6. Кузьмин Ф.И. Задачи и методы оптимизации показателей надежности. – М.: Сов. радио, 1972.

7. Вентцель Е.С. Исследование операций: задачи, принципы, методология. М: Дрофа, 2006.

8. Моудер Дж., Элмаграби С. Исследование операций. Методические основы и математические методы. Пер. с англ. Под редакцией Макарова И.М., Бескровного И.М. – М.: Мир, 1981.

9. ГОСТ 18322–78 Система технического обслуживания **и ремонта техники. Термины и определения.**

А.А. Густов
доктор военных наук
ОАО «Информационные телекоммуникационные технологии» г. Санкт-Петербург

ОБЩИЙ ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ПУНКТОВ УПРАВЛЕНИЯ

Система пунктов управления представляет собой сложную иерархическую организационно-техническую систему, в которой органично соединены оперативный состав и средства управления, составляющие её техническую основу (ТО СПУ). Предлагаемый методический подход позволяет исследовать приспособленность ТО СПУ к решению возлагаемых на неё задач в процессе управления группировкой войск.

Методологические вопросы оценки эффективности функционирования системы пунктов управления (СПУ) являются важнейшим инструментом, обеспечивающим её количественную оценку. Научно-методическую основу оценки эффективности функционирования СПУ составляет решение комплекса научных вопросов, включающих:

а) синтез структуры системы показателей и критериев качества функционирования СПУ в операциях;

б) конструктивную формализацию показателей, то есть их представление в вычисляемой форме;

в) разработку целесообразных способов вычисления значений показателей качества СПУ;

г) установление на множествах значений построенных показателей правил выбора предпочтительных вариантов построения и функционирования СПУ.

Оценка эффективности функционирования СПУ неотделима от понятия качества. Качество присуще СПУ в той же мере, как и любому объекту материального мира. Качество СПУ (равно как и всех элементов, её составляющих) выделяет её существенную определённость, благодаря которой она является именно СПУ общевойскового объединения и отражает устойчивое отношение составляющих её элементов (пунктов управления). Качество СПУ обнаруживается в совокупности её свойств, обусловливающих способность обеспечивать реализацию функций управления в процессе управления войсками в операциях. Количественно качество СПУ может быть оценено по характеристикам её свойств.

Формирование понятия «эффективность», прежде всего, связано с установлением класса систем, в отношении которых оно имеет смысл. Такой класс составляют только целенаправленные материальные системы. В этом смысле категория «качество» имеет более общее значение, поскольку качественной определенностью обладают системы любой природы. «Эффективность» характеризует целенаправленные материальные системы только в отношении их функционирования, т.е. «эффективность» - это характеристика целенаправленного действия системы. Эффективность характеризует систему не непосредственно, а опосредованно, через действие, причём только в отношении соответствия результатов этого действия поставленным целям и имеющимся ресурсам, т.е. отражает способность системы получать необходимый результат с учётом затрат на его достижение. При этом вполне естественно стремление к построению такой системы, которая обеспечит минимум затрат на достижение результата.

Функционирование СПУ в операции, как и любой целенаправленной системы, характеризуется диалектической взаимообусловленностью:

а) целей, которые должны быть достигнуты;

б) используемых для достижения поставленных целей ресурсов;

в) способов применения имеющихся сил и средств;

г) получаемых при этом результатов.

Структурная схема такой взаимообусловленности может быть представлена в виде ориентированного графа (рисунок 1).

При такой структуризации функционирование СПУ в операции можно охарактеризовать с помощью показателей, отражающих получаемый результат и затраты на его достижение, положенные в основу построения СПУ технологии, способность обрабатывать информацию и передавать (принимать) сообщения, способы использования имеющегося ресурса.

В основу методологии оценки эффективности функционирования СПУ положен подход, в соответствии с которым понятие эффективности относят к действию, направленному на выполнение определённой задачи (т.е. к операции). Применительно к СПУ под операцией в общем случае будем понимать согласованную совокупность действий, объединенных общим замыслом с целью реализации функций управления войсками в ходе боевых действий.

А поскольку система ПУ выступает в качестве средства достижения цели, понятие «эффективности операции» отождествляется с понятием эффективности функционирования самой СПУ. Чем в большей степени система приспособлена к решению задач в тех условиях,

Рис. 1. Взаимообусловленность способов организации СПУ и средств на её функционирование для достижения цели

которые для неё определены, тем лучше будет результат её функционирования. Поэтому результат функционирования зависит от качества системы, а также условий и способов её применения по целевому назначению, что и определяет возможность оценки эффективности функционирования по характеристикам качества СПУ.

Оценка целенаправленного функционирования системы ПУ и её элементов производится на основе оценки характеристик её свойств – показателей эффективности. Способность сохранять своё качество в различных условиях обстановки определяет пригодность СПУ к рассматриваемым условиям. В качестве критериев эффективности принимается принадлежность значений выбранных показателей эффективности некоторой заданной области, позволяющей судить об успешности функционирования СПУ.

Количественное определение показателей эффективности функционирования СПУ позволяет при наличии специального методического аппарата выбрать наиболее приемлемый для заданных условий вариант. В научной сфере решение проблемы организации СПУ сводится к разработке научно-методического аппарата, позволяющего провести оценку эффективности функционирования СПУ и на её основе подтвердить или опровергнуть гипотезы, определяющие пути и способы построения СПУ, её применения в операциях и дальнейшего развития.

В соответствии с общей схематизацией процесса противоборства (рисунок 2) для проведения корректной оценки выделено несколько уровней, отличающихся степенью общности, последовательное рассмотрение которых обеспечивает в целом решение задачи оценки эффективности функционирования СПУ (рисунок 3).

На первом уровне обеспечивается оценка эффективности технической основы ПУ, на втором – ПУ, а на третьем – системы ПУ в целом. Четвёртый и пятый относятся к оценке пригодности СПУ с точки зрения систем более высокого уровня: системы управления и группировки войск.

Методология оценки эффективности функционирования технической основы ПУ опира-

Рис. 2. Структура сил, средств и объектов, участвующих в операции

ется на достаточно хорошо проработанный методический аппарат оценки эффективности функционирования узлов связи ПУ. В то же время изменение требований со стороны старшей системы, вызванные, прежде всего, изменением характера оперативных действий войск, необходимостью перехода к автоматизированной системе управления войсками, обусловили разработку ряда методик, обеспечивающих учёт важных в современных условиях свойств: манёвренности технической основы ПУ; обоснования технического облика технической основы ПУ.

Следует заметить, что на современном уровне развития науки и техники потенциально имеются широкие возможности для выбора характеристик и оценки достижения полезного эффекта СПУ. Однако свобода выбора сужается наличием различного рода ограничений. Прежде всего, они касаются области потребления ресурса для достижения цели. Вполне объективно ресурс всегда ограничен. В связи с этим при оценке эффективности функционирования СПУ применяется следующая постановка задачи: осуществляется максимизация полезного эффекта ($U^{бу}$ – реализуемый уровень боевого управления) при ограничениях на уровень потребления ресурса R^o

$$U^{бу} \to \max, \quad R \le R^0.$$

На следующих уровнях производится оценка эффективности функционирования ПУ и системы ПУ в целом. Причём исследуемые объекты рассматриваются в двух аспектах: с точки зрения структуры и с точки зрения поведения.

Анализ исследований, проводимых в области оценки эффективности сложных систем показывает, что в качестве определяющего при разработке методологии для оценки эффективности применяется подход, основанный на определении роли и места системы в выполнении задач старшей системы, взаимодействующих систем, а также оценке подсистем, входящих в состав рассматриваемой системы.

Возможность оценки с позиции старшей системы определяется тем, что СПУ во многом может оказать влияние на боевые возможности группировки войск и достижение целей операции. Приспособленность СПУ к манёвренным боевым действиям с массированным применением высокоточного оружия, обеспечение своевременного получения и обработки информации состояния, а также выработки и доведения управляющих воздействий, создаёт условия для полной реализации боевого потенциала группировки и достижения задач, поставленных старшим штабом, с минимальными потерями. Поэтому с позиции старших систем эффективность функционирования СПУ может быть оценена

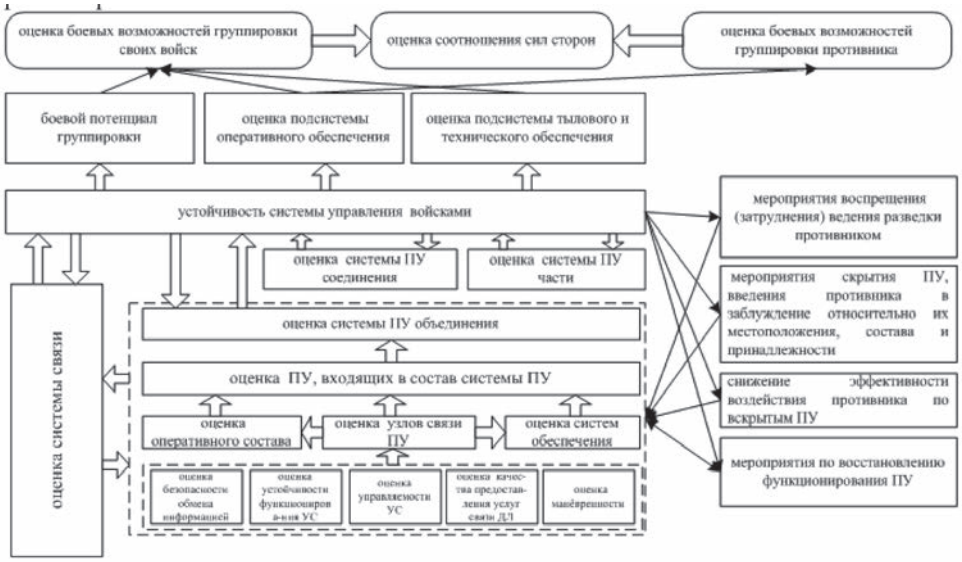


Рис. 3. Декомпозиция уровней оценки эффективности функционирования системы ПУ

на основе устойчивости функционирования системы управления и боевой эффективности группировки войск. Это определяет конечный целевой эффект, на выявление которого направлена оценка эффективности функционирования СПУ общевойскового объединения. При этом очевидно, что рассмотрение СПУ только одной инстанции может привести к получению локальных результатов, поэтому на уровне оценки эффективности функционирования с позиции старших систем следует учитывать влияние систем ПУ всех инстанций.

Показатели эффективности функционирования СПУ с позиции старших систем характеризуют её вклад в боевую эффективность действий войск, и для их определения, как правило, используют модели двухсторонних боевых действий. Поскольку эффективность боевых действий войск зависит от состава войск сторон, от способа (метода) управления ими, то для выделения вклада СПУ необходимо зафиксировать решение по управления войсками, состав и задачу действий войск, принять допущение об оптимальности управления и сравнить между собой показатели эффективности рассматриваемых боевых действий, отвечающих различным способам построения СПУ.

Таким образом, при проведении оценки СПУ не рассматривается качество управленческого решения. К тому же оно не входит в понятие система ПУ. Считается, что объём задач, который может быть выполнен на ПУ и доведён до исполнителей, пропорционален количеству оперативного состава и техники связи. В связи с этим осуществляется проведение оценки потенциальных возможностей по обоснованию и своевременному принятию решения, которые зависят от количества и подготовленности операторов, технической оснащённости ПУ и, следовательно, определяют способность системы управления воспользоваться имеющимся ресурсом. Если в СПУ имеются необходимые силы и средства, выработанное управленческое решение считается обоснованным.

Такой подход получил широкое применение, несмотря на то, что он указывает только на относительное влияние СПУ на управление войсками, т.е. на степень использования системой управления потенциальных возможностей войск при условии своевременного принятия, уточнения и доведения управленческих решений до исполнителей.

С точки зрения оценки эффективности внутреннего аспекта функционирования СПУ рассматривается внутреннее строение системы ПУ и обеспечивается целенаправленный поиск технического облика системы ПУ и её элементов, системообразующих взаимосвязей между элементами, порядка применения и объединения в войсковые формирования.

Показатели на этих уровнях характеризуют соответствие процессов, протекающих в СПУ и

её подсистемах, внутренним целям её функционирования. Целями в этом случае являются своевременное принятие, уточнение и доведение управленческих решений до исполнителей. Результатами функционирования являются управляющие воздействия в виде директив, планов, приказов, распоряжений и команд по управлению в интересах достижения целей, поставленных перед войсками.

При таком подходе методология оценки эффективности системы ПУ представляет собой иерархическую систему взаимосвязанных методик, согласованных по уровням и задачам и позволяющих оценить наиболее существенные аспекты её функционирования (рисунок 4).

Выбор показателей для оценки качества системы ПУ и её элементов осуществляется с учетом достижения необходимой полноты оценки. При этом, как правило, применяется векторный подход. Эта постановка обеспечивает наиболее разностороннюю и полную оценку рассматриваемого объекта и является наиболее приемлемой в отсутствии ясной до конца математической постановки цели его создания, что характерно для системы ПУ. Кроме того, она позволяет после проведения векторной оптимизации строить процедуры выбора на основе максимизации (минимизации) одного из показателей при выполнении ограничений на другие.

Следует особо подчеркнуть, что методический аппарат для расчёта параметров системы

Рис. 4. Комплекс моделей для оценки эффективности функционирования системы ПУ

ПУ не может обеспечить их измерение в строгом смысле этого слова. Рассматриваемым характеристикам присваиваются определённые числовые значения, которые рассчитываются по правилам, опирающимся на объективные методы, и в этом смысле являются необходимыми и достаточными для определения изучаемого свойства на шкале порядка и сравнения объектов между собой на основе рассчитанных величин. В некоторых случаях система ПУ, на чьё поведение сильное влияние оказывают суждения, действия или эмоции человека, не поддаётся точному количественному анализу. В таких случаях применяется, как единственно возможный, способ оценки характеристик поведения, основанный на использовании лингвистических переменных, т.е. переменных, значением которых являются не числа, а слова или предложения в естественном или формальном языке.

В критериальной части методологии под критерием понимается совокупность определенных правил, обеспечивающих в процессе принятия решений выбор из множества альтернативных вариантов некоторого их подмножества, которое удовлетворяет условиям пригодности, оптимальности или превосходства. Очевидно, что выбор того или иного условия оценки зависит от характера решаемой задачи, поставленной цели и содержания объекта исследования.

При решении проблемы организации системы ПУ имеется противоречие, которое носит системный характер.

В силу невозможности формализовать вопросы, связанные с поиском приемлемых организационных решений на начальном этапе обоснования, поскольку поиск новых идей и технических решений представляет собой сложную процедуру, творческую по своей природе, может возникнуть вопрос о корректности полученных результатов из-за ограниченности количества рассматриваемых вариантов на каждом уровне оценки эффективности, в то время как потенциально это количество ничем не ограничено. При этом очевидно, что подход к решению задачи организации системы ПУ на основе прямого перебора всех её возможных вариантов не реализуем из-за большой размерности задачи.

В рамках решения проблемы организации для этой цели могут быть применены только эвристические методы, основанные на накопленных знаниях в данной области, практическом опыте и здравом смысле лиц, разрабатывающих решение, определении цели, для которой создаётся система. Проблема сужения поиска возможных вариантов организации технической основы СПУ решается на этапе синтеза вариантов технического облика и правил применения в ходе боевых действий. В процессе синтеза с учётом имеющихся ограничений разрабатывается некоторое количество классов построения системы ПУ, а их обоснованность определяется накопленными знаниями, учётом мнения специалистов в таких областях, как оперативное искусство, организация ПУ, системы связи, узлов связи ПУ, защита элементов системы управления.

Кроме того, иерархическая структура методологии также является тем условием, которое обеспечивает чувствительность и конструктивность оценки по всем аспектам организации системы ПУ, повышает обоснованность принимаемых решений. Увязанные в единый комплекс методики позволяют не только проводить оптимизацию решений по организации системы ПУ, но и на любом из рассматриваемых уровней обнаруживать факт несоответствия цели, вскрывать причины низкой эффективности принимаемых решений.

Методология оценки эффективности системы ПУ нацелена на то, что необходимо не просто понять причины состояния системы ПУ в условиях, прогнозируемых на определённый период, и определить, что может произойти в конкретной ситуации в результате некоторых изменений обстановки, а как организовать систему ПУ, чтобы подобные изменения не могли бы сказаться на ней существенным образом. На основе оценке эффективности решается задача выработки линии поведения, рекомендации по внедрению организационных и технических решений, способных вывести систему на новый уровень, соответствующий задачам, которые предстоит решать в будущих вооружённых конфликтах.

Методология оценки эффективности, разработанная на основе рассмотренного подхода, является логичным продолжением исследований, проводимых в рассматриваемой предметной области. Она позволяет на единой методической основе решать задачи определения

количественных значений показателей эффективности СПУ на любом из обозначенных уровней и на их основе производить выбор предпочтительного варианта, обосновывать требования как к элементам СПУ, так и к системе в целом.

СПИСОК ЛИТЕРАТУРЫ

1 Проблемные вопросы теории управления войсками (силами). – М.: ВАГШ, 1996 – 442с.

2 Сосюра О.В. Расчёт обобщённых показателей боевых возможностей войск в операциях (боевых действиях) с учётом эффективности управления ими. Военная мысль №5. - М.: МО РФ, 1997 – 24-30с

3 Петухов Г.Б. Основы теории эффективности целенаправленных процессов. Часть 1. Методология, методы, модели. – М.: МО СССР, 1989- 660 с.

4 Петухов Г.Б, Якунин В.И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремлённых систем. – М.: АСТ, 2006-304с.

В.И. Талагаев
ОАО «Информационные телекоммуникационные технологии» г. Санкт-Петербург

ОБОБЩЕННАЯ МОДЕЛЬ ДЛЯ АНАЛИЗА ПОТЕНЦИАЛЬНЫХ ВОЗМОЖНОСТЕЙ РАДИОРАЗВЕДКИ

В статье предложена математическая модель для оценки вероятностно-временных характеристик систем обнаружения и классификации радиоизлучений.

Современные передающие радиосредства, особенно СНЧ, СДВ, ДВ, СВ и КВ диапазонов, входящие в состав радиоканалов, обладают большой мощностью и обеспечивают дальность связи до 20 тыс. км, что создает благоприятные условия для классификации (обнаружения и анализа параметров) их радиоизлучений разведывательными комплексами с панорамным обзором /1/.

При проектировании защищенных от радиоразведки (РР) и радиоэлектронного подавления (РЭП) каналов радиосвязи необходимо учитывать возможности средств РР по определению вероятностно-временных характеристик сигналов, и в первую очередь, таких, как вероятность правильной классификации и время обнаружения сигналов многоканальными разведывательными приемниками. Эти данные необходимы для рационального выбора частотно-временных параметров сложных сигналов, в частности при выборе полосы широкополосных сигналов (ШПС) и времени переключения для сигналов с псевдослучайной перестройкой частоты (ПСПЧ).

Ограниченные сведения о возможностях систем РР и РЭП, как правило, получают в результате анализа зарубежных источников научно-технической информации. Достоверность и полнота таких данных не гарантирована и не достаточна для надежного выбора параметров сигналов для проектирования развед- и помехозащищенных каналов радиосвязи.

При отсутствии достоверной информации о возможностях РР целесообразно ориентироваться на потенциально достижимые вероятностно-временные характеристики, которыми могли бы обладать средства РР при реализации в разведывательных приемниках оптимальных методов обработки и классификации многопозиционных (по частоте) сигналов.

Задача классификации многопозиционных сигналов, называемая иногда обнаружением с распознаванием или многоальтернативным обнаружением, формулируется следующим образом. На входе многоканального приемника может присутствовать один из m ненулевых сигналов или только шум. Требуется определить, присутствует ли на входе приемника в текущий момент времени какой-либо из m сигналов (с указанием какой именно) либо никакого сигнала нет, а есть только шум.

Необходимо отметить, что на станции РР точная информация о начале работы радиоканала (о появлении радиоизлучений) практически отсутствует, т.е. допускается возможность присутствия на входе приемника только шума, без сигнала, что обуславливает необходимость работы с порогом, установка которого необходима для фиксации на определенном уровне ложных срабатываний разведывательного приемника от естественных шумов.

Исходя из прогноза развития зарубежных средств РР для классификации излучений будут применяться панорамные приемники, имеющие

m (до 3000) каналов приема с обзором всего разведываемого диапазона, используемого для КВ, СВ, ДВ, СДВ и СНЧ связи.

Если для упрощения рассматривать проектируемые радиоканалы как каналы с δ – коррелированным нормальным шумом и неизвестной (при неизвестном местоположении излучателя) фазой, то решающая схема многоканального разведывательного приемника должна реализовывать критерий Неймана-Пирсона, т.е. работать в режиме с порогом.

Оценку вероятностно-временных характеристик приемника некогерентных многочастотных ШПС, сигналов с ПСПЧ и других сложных сигналов для радиоканалов с постоянными параметрами можно произвести по методике [2-4], содержащей выражения для расчета основных характеристик системы классификации по критерию Неймана-Пирсона:

– вероятности пропуска сигнала в системе

$$P_{проп} = (1 - P_{лт})^{1-\frac{1}{m}} \times \times\{1 - Q[\sqrt{-2\ln(1-(1-P_{лт})^{1/m})}, h]\}, \quad (1)$$

где $P_{лт}$ – вероятность ложной тревоги; m – число позиций сигнала (каналов приема); $Q\,(U,\ V)$ – интеграл Релея - Райса

$$Q(U,V) = \int_U^\infty \rho \exp\left[-\frac{1}{2}(U^2+\rho^2)\right] I_0(V_\rho) d\rho;$$

$h = \sqrt{\frac{2E}{N_0}}$ – отношение сигнал/помеха на входе приемника, E – напряженность поля сигнала, V_0 – спектральная плотность мощности флуктуационных помех (другие виды помех не учитываются);

– вероятность правильной классификации сигнала в системе

$$P_{прав} = \sum_{i=0}^{m-1} (-1)^i \frac{(m-1)!\exp[-ih^2/2(i+1)]}{(m-1-i)!(i+1)!} \times \times Q\left(\sqrt{-2(i+1)\ln[1-(1-P)^{1/m}]}, \frac{h}{\sqrt{i+1}}\right); \quad (2)$$

– вероятности трансформации сигнала

$$P_{тр} = 1 - P_{проп} - P_{прав} \quad (3)$$

Под вероятностью ложной тревоги $P_{лт}$ понимается вероятность ответа о наличии какого-либо сигнала, когда в действительности сигнал на входе отсутствует, под вероятностью правильной классификации $P_{прав}$ – вероятность правильного указания частотной позиции (одной из т) присутствующего на входе сигнала, а под вероятностью трансформации $P_{тр}$ – вероятность неправильного указания позиции присутствующего на входе сигнала.

Результаты расчета основных характеристик потенциальной системы классификации по формулам (1) – (3) для $m = 400$ ветвей приема и значений вероятности ложной тревоги $P_{лт} = 10^{-1}$, $5\cdot10^{-2}$, 10^{-2} в зависимости от отношения сигнал/помеха h на входе приемника представлены в таблице 1.

Анализ данных таблицы, в частности, показывает, что надежная ($P_{прав} > 0{,}9$) классификация сигнала обеспечивается разведывательным приемником при отношении сигнал/помеха более 6.

Таблица 1

h	Значения основных характеристик системы классификации сигналов								
	При $P_{лт} = 10^{-1}$			При $P_{лт} = 5\cdot10^{-2}$			При $P_{лт} = 10^{-2}$		
	$P_{проп}$	$P_{тр}$	$P_{прав}$	$P_{проп}$	$P_{тр}$	$P_{прав}$	$P_{проп}$	$P_{тр}$	$P_{прав}$
1	0,898	0,1	0,002	0,949	0,05	0,001	0,99	0,01	0
2	0,873	0,098	0,029	0,932	0,049	0,019	0,983	0,01	0,007
3	0,738	0,087	0,175	0,82	0,045	0,135	0,92	0,09	0,071
4	0,427	0,066	0,517	0,517	0,031	0,452	0,679	0,008	0,313
5	0,132	0,021	0,847	0,181	0,013	0,806	0,305	0,004	0,691
6	0,019	0,004	0,977	0,029	0,003	0,968	0,067	0,001	0,932
7	0,001	0	0,999	0,002	0	0,998	0,007	0	0,993

Превышение некоторого принятого в системе порогового значения этой величины $P_{прав.\ пор}$ (или $h_{пор}$) является основанием для принятия решения о надежном обнаружении сигнала. Время, необходимое РР для надежного обнаружения сигналов $t_{РР}$, зависит от отношения сигнал/помеха h на входе приемника в месте расположения разведывательной станции составляет

$$t_P = \frac{h_{пор} N_0}{P_C} \quad , \qquad (4)$$

где $h_{пор}$ – пороговое значение отношения сигнал/помеха, необходимое для обеспечения порогового значения $P_{прав} = P_{прав.\ пор}$; P_c – мощность сигнала на входе разведывательного приемника; N_0 – спектральная плотность мощности шума на входе приемника.

Для примера для радиоканала диапазона СДВ выполнен расчет по формуле (4) и методике /5/ значений отношения сигнал/помеха h для $P_{изл} = 530 кВт$, $\Delta F_c = 75 Гц$ и уровня атмосферных помех, наводимых на антенну типа «Рамка», 20 мкВ/м на частоте 10 кГц и 8 мкВ/м на частоте 60 кГц. Результаты расчета приведены в таблице 2.

Таблица 2

Отношение сигнал/помеха в пункте РР

d (км) *F* (кГц)	500	1000	1500	2000
10	925	310	122	61
60	6200	1550	310	124

Из таблицы 2 видно, что значение h на выходе приемника РР существенно превышает значение, требуемое для надежной классификации радиоизлучений СДВ передатчиков, т.е. РР с высокой надежностью установит факт и частоту передачи за 20 мс (при скорости 1/50 Бод). Если станция РР совмещена со станцией РЭП это время будет временем реакции средств РЭП, т.е. интервалом безопасным для передачи информации на одной частоте.

Аналогичные расчеты, выполненные по формулам (1) и (2) для СНЧ системы связи, характеризующейся еще большей стабильностью канала связи и слабым затуханием на воздушном участке трассы распространения сигналов, показывают, что для надежной классификации СНЧ радиоизлучений РР требуется 30 – 60 мс.

Таким образом, для обеспечения защиты СДВ и СНЧ систем связи от РЭП частоту передачи при использовании ПСПЧ, или частоту элементарных посылок при использовании многочастотных ШПС сигналов, следует изменять не менее чем через 20 мс в СДВ и через 30–60 мс в СНЧ системах, что обусловлено потенциальными возможностями РР противником их радиоизлучений.

Таким образом, для определения потенциально возможного (минимального) времени обнаружения радиоизлучение необходимо располагать сведениями о мощности передатчика сигналов и спектральной мощности шума на входе приемника вместе расположения станции радиоразведки, о пространственной структуре «место передачи – станция радиоразведки», а так же, трассы распространения сигналов для различных диапазонов «передатчик – приемник» и об уровне помех в месте расположения средств РР.

Пространственная структура зависит от расположения и ТТХ средств разведываемой и подавляемой систем связи и их элементов, а так же от оперативно-тактической ситуации, определяющей организацию использования средств системы.

Модель является обобщенной и может быть использована при анализе потенциальных возможностей обнаружения работы радиоканалов как с постоянными (УКВ, ДВ, СДВ, СНЧ), так и с переменными (СВ, КВ) параметрами. Для КВ радиоканалов оценка разведзащищенности по приведенной методике соответствует худшему случаю, т.е. отсутствию замираний и межсимвольной интерференции на трассе «передающее средство радиоканала – станция РР».

Модель программно реализована на платформе Android для многофункциональных мобильных устройств в среде программирования Java под операционной системой Microsoft Windows 7 /5/.

СПИСОК ЛИТЕРАТУРЫ

1. Система радио и радиотехнической разведки. ФАИРС, М., 1978.

2. Долуханов М.П. Распространение радиоволн. М.: Связь, 1972.

3. Пусь В.В. Инвариантный прием многопозиционных некогерентных сигналов. Известия вузов СССР. – Радиоэлектроника, 1983, т. 26, вып. 12.

4. Пусь В.В., Талагаев В.И. Указатель поступлений информационных материалов, в/ч 11520, серия А, вып. 7(10), 1987.

5. Талагаев В.И., Лебедев Д.В. Программа для анализа потенциальных возможностей радиоразведки v.1.0, ОАО «Интелтех», 2013.

ТЕХНИКА СРЕДСТВ СВЯЗИ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

№1 (141). 2018

Компьютерная верстка *С. В. Горячевой*
Дизайн обложки: Шаутин А.В.
Поддержка сетевой версии журнала: Лебедев Д.В.

Налоговая льгота — Общероссийский классификатор продукции
ОК 005-93, т. 2; 95 3004 — научная и производственная литература

Подписано в печать 19.02.2018. Формат 60×84/8. Печать цифровая.
Усл. печ. л. 36,5. Тираж 100. Заказ 11160b.

Санкт-Петербургский государственный политехнический университет.
Издательство Политехнического университета,
член Издательско-полиграфической ассоциации университетов России.
Адрес университета и издательства: 195251, Санкт-Петербург, Политехническая ул., 29.
Тел.: (812) 550-40-14.
Тел./факс: (812) 297-57-76.