Криптографические алгоритмы, используемые для Java Secure Socket Extension

Криптографический алгоритм	Длина ключа(Bits)
RSA	2048 (authentication), 2048 (key exchange), 512(key exchange)
RC4	128, 128 (40 effective)
DES	64 (56 effective), 64 (40 effective)
Triple DES	192, (112 effective)
AES	256, 128
Diffie-Hellman	1024, 512
DSA	1024

Вышеприведенный алгоритм позволяет построить систему, лишенную подавляющего большинства недостатков, свойственных современным технологиям. Она исключает подделку и изменение как со стороны пользователя, так и со стороны проверяющего технического персонала. Подобная технология отлично масштабируется и позволяет построить централизованную систему в рамках предприятия. В то же время система открыта для доработки и может быть дополнена другими возможностями, например, статистическим анализом, распечаткой отчетов, сведений и др.

Выводы

Выполненное исследование позволяет сделать следующие выводы:

1.Проведен анализ основных аспектов работы с использованием технологии SmartCard.

2.Изучено использование аппаратного и программного обеспечения для работы с описанной технологией.

3.Предложен алгоритм, реализующий описанную технологию и позволяющий избавиться от недостатков, имеющихся в современных системах.

Поступила 07.03.2006

УДК 621.396.6

Шокало В.М., Цопа А.И.

КОНЦЕПЦИЯ СОЗДАНИЯ ОТЕЧЕСТВЕННЫХ СПЕЦИАЛЬНЫХ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

Рост числа техногенных и природных катастроф, усиление терроризма и кибертерроризма предполагает наличие у независимого государства собственных разработок защищенных специальных цифровых систем передачи информации (СЦСПИ), предназначенных для технического оснащения структур, обеспечивающих безопасность всех сторон жизнедеятельности государства.

Под защищенной СЦСПИ, как и в [1], в статье понимается та система, которая решает поставленные задачи как при наличии мешающих воздействий естественного происхождения (шумов, помех и пр.), так и при целенаправленных действиях противника.

Отсутствие в Украине собственных разработок и производства СЦСПИ, которые являются одним из основных признаков защищенности специальных систем, указывает на актуальность исследований в этом направлении.

При создании СЦСПИ целесообразно ориентироваться на имеющиеся решения по системам общего применения, что позволит существенно сократить сроки разработки и снизить стоимость технических средств.

Принятая в НАТО концепция построения СЦСПИ базируется на использовании коммерческой аппаратуры связи, модернизированной в части повышения помехоустойчивости и безопасности обмена информацией [2]. Проводная связь при этом интегрируется с беспроводной для полноты использования существующих информационных ресурсов государства.

Эту концепцию рационально дополнить системой взглядов на построение специальных командных радиосистем (СКРС), как разновидности СЦСПИ [3]. Современные командные радиосистемы обеспечивают дистанционное управление наземными, надводными и воздушными носителями с аппаратурой, выполняющей функции: видеоконтроля; поиска взрывных устройств и загазованных территорий; активной мобильной ретрансляции сигналов и т.д.

Постоянно растущие требования к оперативности и точности реагирования в экстремальных ситуациях выдвигают новые концептуальные задачи по техническому оснащению служб общественной безопасности. Появляется необходимость передачи больших объемов цифровой информации с места чрезвычайной ситуации, обеспечения оперативного доступа к базам данных, идентификации личности по отпечаткам пальцев, фото- и видеоматериалам и т.д. Узкополосные ведомственные системы передачи цифровой информации не могут полностью справиться с передачей больших объемов информации, что часто необходимо в экстремальных ситуациях.

Идеология проведения отечественных разработок СЦСПИ частично может быть построена на основе существующего опыта наших разработчиков и опыта авторов по исследованию проводных, беспроводных и командных систем [4-7].

Цель статьи состоит в разработке концепции создания СЦСПИ, выбора направлений исследований и определения круга задач, требующих решения. Предлагаемый вариант структуры СЦСПИ при разворачивании в зоне кризисной или чрезвычайной ситуации (ЧС) приведен на рис. 1.

Представленная СЦСПИ не является простым объединением результатов известных и опубликованных работ по проводным и беспроводным системам передачи информации. При синтезе этой структуры были использованы передовые идеи в области:

– технологий передачи информации;
– информационной и физической защиты каналов связи;
– топологии построения надежных сетей передачи информации;
– протоколов передачи данных;
– производительных программно-аппаратных платформ.

СЦСПИ включает в себя нескольких подсистем и сетей: сеть проводного доступа (СПД), сеть абонентского радиодоступа (САРД), сенсорную радиосеть (СРС) и командную радиосистему (КРС). Базовые станции (БС) системы радиодоступа подключаются по проводной сети к мультиплексору доступа (МД), который обеспечивает концентрацию информационных потоков и подключение к серверу данных оперативного штаба. Для передачи информации на дальние расстояния в центр принятия решений используются проводные многоканальные цифровые системы передачи (ЦСП). Система имеет сквозную систему удаленного управления и мониторинга состоянием элементов коммуникационной структуры. Для интеграции СЦСПИ с телекоммуникационными и информационными

системами общего назначения используется специальный шлюз, который обеспечивает защиту информации в зоне развертывания системы от несанкционированного доступа.

При выборе технологий передачи информации для построения проводных, беспроводных и командных сетей СЦСПИ были приняты во внимание лидирующие позиции, которые занимают в настоящий момент xDSL-технологии, основанные на эффективных методах модуляции и помехоустойчивого кодирования, позволяющих существенно увеличить пропускную способность линий связи (ЛС) и длину регенерационных участков. Если рассматривать 7-уровневую модель построения открытых сетей (OSI), то xDSL – это цифровая технология передачи физического уровня, предоставляющая удобную высокоскоростную среду для протоколов более высоких уровней, дающих возможность обеспечивать передачу голоса, данных и мультимедиа, включая доступ к сети Интернет [3].

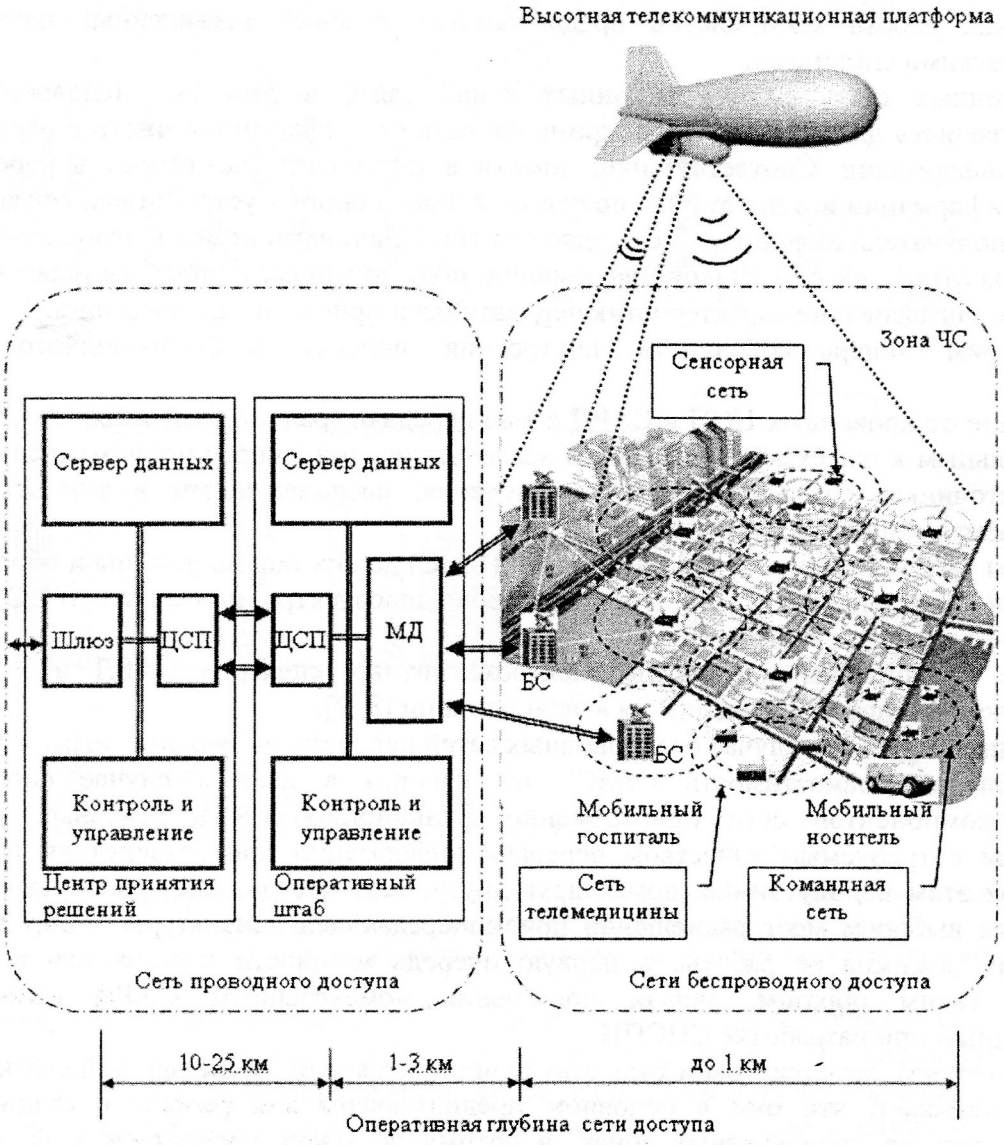

Рис. 1. Схема развертывания цифровой системы передачи информации специального назначения (СЦСПИ) в зоне кризисной или чрезвычайной ситуации

В работе [6] показано, что на отечественных кабельных линиях связи при использовании многоуровневого линейного сигнала с кодированием TC-PAM-16 и технологии SHDSL можно достичь скорости передачи информации более 2 Мбит/с при вероятности битовой ошибки не хуже 10^{-7}. Предельная рабочая дальность работы SDSL системы составила от 4,5 км до 15,3 км в зависимости от типа кабеля и условий эксплуатации.

Главными факторами, влияющими на качество работы xDSL-оборудования линейного тракта цифровых систем передачи (ЦСП), являются:

– ослабление сигнала в линии связи;
– нелинейность АЧХ линии связи;
– перекрестные наводки на ближнем и дальнем концах линии связи;
– групповое время задержки сигнала в кабеле;
– радиочастотная интерференция.

Большое влияние на передачу многоуровневых линейных сигналов оказывает радиочастотная интерференция. Радиопередачи в диапазонах длинных и средних волн, работа мощных радиорелейных станций и других радиотехнических систем вызывают наводки на кабельную линию при передаче линейных сигналов, если они имеют совпадающие участки спектров. Этот фактор необходимо исследовать и учитывать при разработке защищенных ЦСП, так как работа xDSL-систем предполагается в зонах, насыщенных различными радиотехническими системами.

В проводных сетях передачи данных канал связи в рабочем (неповрежденном) состоянии «закрыт» для всех сигналов, кроме «полезного», сформированного в передатчике источника информации. Соответственно, помехи в таких сетях возникают в передатчике источника информации и в приемнике получателя информации – устройствах, согласующих источник и получатель информации с каналом связи. Причинами помех в этом случае могут быть сигналы от других источников информации, подключенных к этому же передатчику, а также плохое согласование характеристик передатчика и приемника информации.

Рассмотрим теперь особенности построения подсистемы беспроводного доступа СЦСПИ.

В отличие от проводных ЦСП в САРД канал передачи (радиоканал) является открытым и чувствительным к помехам и мешающим воздействиям различного происхождения, в том числе к источникам электромагнитного излучения, расположенным в том же, что и рассматриваемая радиосеть, регионе.

Вопросы электромагнитной совместимости (ЭМС) до сих пор не решены и обостряются в связи с конфликтами электромагнитных спектров радиоэлектронных систем (РЭС), систем связи и систем передачи информации.

На рис. 2 показаны конфликты электромагнитных спектров САРД и некоторых радиотехнических систем, находящихся в эксплуатации [8, 9].

Как видно из рис. 2, в случае беспроводных сетей первостепенную роль играет проблема электромагнитной совместимости (ЭМС), означающая в данном случае способность различных компонентов сети одновременно функционировать в реальных условиях эксплуатации с требуемым качеством передачи информации при воздействии помех, не создавая при этом недопустимых помех друг другу. Решение данной проблемы связано с оптимальным выбором мест размещения приемопередающей аппаратуры и определением оптимальных режимов ее работы, в первую очередь мощности передатчика и частоты излучения. Таким образом, задачи повышения помехозащиты САРД относятся к первоочередным при разработке СЦСПИ.

Анализ сетевой архитектуры и существующих протоколов беспроводной связи Wi-Fi и WiMAX показывает, что они в основном предназначены для работы в стационарных условиях и заранее определенных зонах, а потому не могут предоставить возможность широкополосной передачи там, где она наиболее важна для служб общественной безопасности: в движении, на месте происшествия или в зоне ЧС.

Этим требованиям удовлетворяют технология и система беспроводной ячеистой самоорганизующейся сети (БСС - Wireless Mesh Networks). В такой сетевой структуре физическое взаимодействие узлов формирует полносвязную (mesh) топологию. Любое устройство в такой системе работает как маршрутизатор/ретранслятор для остальных элементов сети. Это означает, что каждое устройство имеет возможность связи с точкой доступа как напрямую, так и через «соседние» устройства. Такая распределенная структура

значительно повышает устойчивость системы к отказам, а также общую пропускную способность, поскольку пакеты данных автоматически направляются по менее загруженным «путям» передачи информации. Более того, увеличение количества одновременно работающих абонентов системы (как обычно происходит в зоне экстремальной ситуации) только улучшает радиопокрытие и устойчивость системы БСС, в то время как традиционные ведомственные, а тем более коммерческие сотовые системы связи испытывают перегрузку. Кроме того, при полносвязной топологии построения САРД узлы обладают определенной независимостью, что обеспечивает дополнительную информационную безопасность и облегчает процедуру определения мест повреждений на участках связи средствами сетевого управления.

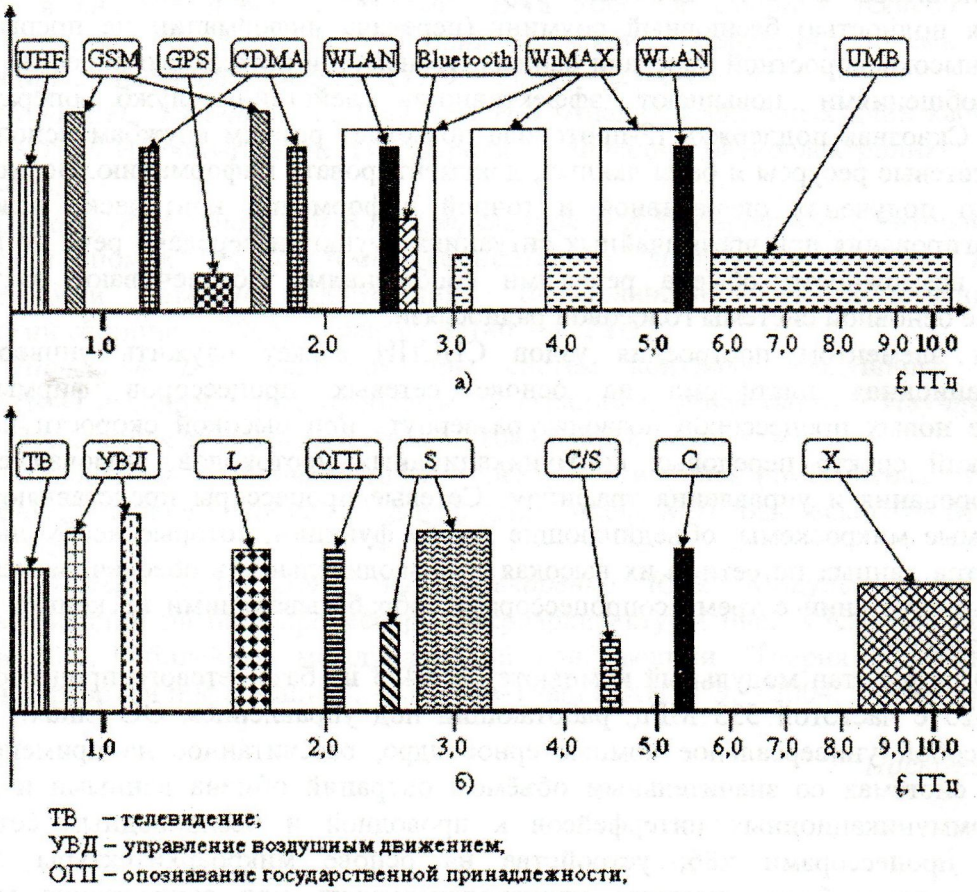

Рис. 2. Диапазоны частот, занимаемые различными радиоэлектронными системами:
***а* – системами мобильной связи и беспроводными системами передачи данных;**
***б* – радиолокационными системами управления воздушным движением и телевидением**

Самоорганизующаяся архитектура беспроводной сети может обеспечить необходимую совместную работу нескольких смежных сетей: сенсорной сети, командной сети, сети телемедицины и других беспроводных сетей, развернутых в зоне чрезвычайной ситуации.

Для повышения безопасности персонала оперативних служб и снижения численности людских потерь возможности САРД могут быть дополнены беспроводными сенсорными сетями, которые используются в целях мониторинга состояния организма человека на основе таких показателей, как частота пульса и характер дыхания. Можно также установить детекторы дыма, температурные, газовые и другие датчики и в режиме беспроводной связи передавать данные в оперативный штаб для раннего оповещения об опасности.

Для контроля ситуации и хода проводимых мероприятий могут быть использованы видеокамеры. Видеоинформация с места ЧС может транслироваться с подвижных носителей и подвесных дирижаблей и передаваться в оперативный штаб, что позволяет дать полную картину ситуации для эффективного управления ресурсами и их распределения. При этом

высотная телекоммуникационная платформа обеспечивает активную ретрансляцию сигналов и расширенную зону радиопокрытия.

Все устройства инфраструктуры, входящие в состав БСС, поддерживают IP-протокол, что позволяет использовать в системе любое периферийное оборудование, такое, как мобильные терминалы передачи данных, карманные и портативные компьютеры, IP-видеокамеры, микрофоны и пр. Технология систем БСС позволяет абонентским устройствам работать через оборудование (базовые станции) инфраструктуры и организовывать местные локальные сети, состоящие только из абонентских устройств. Связь с ретрансляторами, базовыми станциями и точками доступа во внешние сети осуществляется одновременно со связью в локальных сетях, причем при переходе абонентского устройства из зоны действия одного ретранслятора в зону действия другого ретранслятора или точки доступа обеспечивается полностью бесшовный роуминг (передача информации не прерывается). Возможности высокоскоростной передачи данных, трансляции потокового видео и обмена речевыми сообщениями повышают эффективность действий служб оперативного реагирования. Сквозная поддержка IP-протокола позволяет разным службам использовать одни и те же сетевые ресурсы и базы данных, документировать информацию. Возможность своевременного получения оперативной и точной информации критически важна для успешного реагирования при чрезвычайных ситуациях. Функции передачи речи по каналам IP (VoIP) и возможности обмена речевыми сообщениями обеспечивают экстренное резервирование основной системы голосовой радиосвязи.

Основным элементом построения узлов СЦСПИ может служить универсальная телекоммуникационная платформа на основе сетевых процессоров фирмы Intel. Использование новых процессоров позволит развернуть при высокой скорости передачи данных широкий спектр передовых коммуникационных протоколов, включая средства защиты, шифрования и управления трафиком. Сетевые процессоры представляют собой программируемые микросхемы, объединяющие в себе функции, которые необходимы для передачи пакетов данных по сети, а их высокая производительность обеспечивается ядром Intel XScale® в сочетании с тремя сопроцессорами, обрабатывающими несколько пакетов данных одновременно.

В ХНУРЭ разработан модульный компьютер МК425 на базе сетевого процессора Intel XScale® IXP425 с частотой 533 МГц, работающий под управлением ОС Linux. МК425 представляет собой универсальное компьютерное ядро, рассчитанное на применение во встраиваемых системах со значительным объёмом операций обмена данными и которое имеет ряд коммуникационных интерфейсов к проводной и беспроводным сетям. По сравнению с процессорами x86, устройства на основе микроархитектуры XScale® обеспечивают гораздо более высокую производительность при существенно меньшем потреблении энергии [10].

Таким образом, предлагается следующая концепция построения отечественных защищенных СЦСПИ (рис. 1), которая базируется на передовых технологиях в области передачи информации и микроэлектронной техники:

– проводные и беспроводные сети, входящие в состав СЦСПИ, должны быть интегрированными и построенными по принципу ячеистых сетей;

– как отдельные составляющие в СЦСПИ должны входить командные радиотехнические системы;

– СЦСПИ, включая командные, должны быть построены на базе xDSL-технологий, обладающих высокой степенью защищенности;

– для повышения защищенности по радиоканалу в СЦСПИ должны быть предложены решения конфликтов электромагнитных спектров САРД и действующих РЭС.

Список литературы

1. *Сердюков П.Н., Бельчиков А.В., Дронов А.Е. и др.* Защищенные радиосистемы цифровой передачи информации. – М.: АСТ, 2006. – 403 с.

2. *Баушев С. В., Передрий А. В.* Разработка перспективных систем связи вооруженных сил США и объединенных вооруженных сил НАТО // Зарубежная электроника. – 2002. – №4.

3. *Антонов В.М., Пермяков О.Ю.* Комп'ютерні мережі військового призначення. – К.: МК-ПРЕС, 2005. – 320 с.

4. *Паневин О.М., Цопа А.И.* Аппаратура высокоскоростного доступа в Интернет "Антарес-115" с одновременным использованием каналов передачи данных и голоса // Сборник научных трудов II Международной конференции "Информационные технологии и безопасность-2002". – Киев-Партенит: ИПРИ НАН Украины. –2002. – С.103-106.

5. *Цопа А.И., Овчаренко Ю.Б., Власенко В.А.* Использование новой технологии G.SHDSL в системе передачи данных "Вега 2000" // Сборник тезисов докладов 9-й Международной конференции "Теория и техника передачи, приема и обработки информации". – Харьков-Туапсе: ХНУРЭ. – 2003. – С. 44-45.

6. *Цопа А.И., Тихонов В.А., Савченко И.В.* Анализ предельных длин кабельных линий системы SDSL// Научно-технический журнал "Прикладная радиоэлектроника". –2005. – № 2. – С. 400-404.

7. *Шокало В.М., Лихограй В.Г., Стрельницкий А.Е.* Вероятность битовой ошибки при воздействии помех на системы абонентского доступа с учетом характеристик направленности антенн// Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2005. – Выпуск №140. – С.28-31.

8. *Литвинов В.В.* Радиолокаторы систем контроля воздушного пространства: ретроспектива и современные проблемы интеграции и унификации // Научно-технический журнал "Прикладная радиоэлектроника". –2004. – № 4. – С. 61-74.

9. *Управление* радиочастотным спектром и электромагнитная совместимость радиосистем. Учебное пособие / Под ред. д.т.н., проф. М.А. Быковского. – М.: Эко-Трендз, 2006. – 376 с.

10. *Шокало В.М., Цопа А.И., Овчаренко Ю.Б.* Модульный компьютер для телекоммуникаций на базе процессора микроархитектуры Intel XScale // Сборник тезисов докладов 10-й Юбилейной международной конференции "Теория и техника передачи, приема и обработки информации". –Харьков-Туапсе: ХНУРЭ. – 2004, г. Харьков. – С. 69-70.

Поступила 10.04.2006

УДК 681.3.06

Хорошко В.А., Терейковский И.А.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ РАСПОЗНАВАНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

Введение

В последнее время в самых разных отраслях науки и техники отмечается возросший интерес к применению искусственных нейронных сетей. Во многом популярность нейронных сетей объясняется возможностью их эффективного использования в задачах, плохо решаемых «аналитическими» методами. В теоретических работах [1-4], посвященных нейронным сетям, отмечается, что их использование целесообразно в задачах:

– классификации образцов. Задача состоит в указании принадлежности входного образца, представленного вектором признаков, одному или нескольким предварительно определенным классам;

– кластеризации/категоризации. Задача отличается от классификации образцов только тем, что классы заранее не определены, хотя во многих случаях количество классов все-таки предварительно указывается;