УДК 621.396.93

С.В. Трушин, Г.Ю. Пучков, И.Е. Яковлев

КОМПЛЕКС СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ МНОГОЧАСТОТНОГО РАДИОМОДЕМА С ОРТОГОНАЛЬНЫМ ЧАСТОТНЫМ РАЗДЕЛЕНИЕМ ПОДНЕСУЩИХ

Представлены проблемы защиты информации в радиосетях, предназначенных для обеспечения конфиденциального радиообмена. Приводятся сведения о разработанном комплексе средств криптозащиты информации, передаваемой по каналам сетей подвижной радиосвязи. Описываются структура комплекса, возможности и технические характеристики его составных частей. Новизна разработки заключается в том, что впервые в России при создании СКЗИ для защищенных сетей подвижной радиосвязи реализована защита конфиденциальной информации по классу КВ 2 с возможностью замены ключей по радиоканалу.

Радиомодем; средство криптографической защиты информации; ключ; ретранслятор; радиостанция; маскиратор; скремблер; радиосеть; полоса частот; класс защиты информации; специализированный универсальный модуль.

S.V. Trushin, G.J. Puchkov, I.E. Jakovlev

SYSTEM OF CRYPTOGRAPHIC DATA PROTECTION (SCDP), BASED ON A MULTI-FREQUENCY MODEM WITH ORTHOGONAL SUB CARRIER DIVISION

The article deals with problems of data protection in radio networks, intended for secure radio communication. It describes the developed system of cryptographic data protection that is transmitted via mobile wireless networks. The article outlines the system's structure, features and performance specifications of its components. The novelty of the development consists in the fact that it is the first instance of implemented protection of confidential data, meeting class KB 2 specifications with possibility of wireless key substitution, developed in Russia for secured mobile wireless networks.

Radio modem; cryptographic data protection unit; key, repeater; radio station; maskirator; scrambler; radio network; frequency band; class of data protection; specialized versatile module.

Введение. При проведении оперативных мероприятий в чрезвычайных условиях важной задачей является обеспечение скрытности радиосвязи.

Обеспечение скрытности радиосвязи может быть достигнуто двумя путями – маскированием передаваемой информации и криптографической защитой передаваемой информации.

В настоящее время в ряде ведомств, задействованных при проведении работ в чрезвычайных ситуациях широко применяется метод маскирования передаваемой информации. Для этого используются два типа устройств преобразования речи: маскираторы и скремблеры.

Маскираторы обеспечивают самый простой способ маскирования информации – многополосную инверсию спектра (на первых этапах применялась двухполосная инверсия). Маскираторы применялись, в основном, до 2002 года.

Дальнейшее совершенствование методов преобразования частотного спектра привело к разработке устройств преобразования речи типа «скремблер», которые позволили обеспечить более эффективное маскирование передаваемой информации.

Главным преимуществом средств маскирования является простота их эксплуатации, основным недостатком – невозможность обеспечить защиту канала радиосвязи соответствующего уровня при проведении мероприятий в условиях чрезвычайной обстановки, а также при решении задач по передаче персональных данных граждан и другой конфиденциальной информации.

Это задача может быть решена путем применения специальных средств криптографической защиты информации (далее – СКЗИ).

В настоящей статье мы рассмотрим возможности комплекса СКЗИ, «Радиозанавес», разработанного в 2010 г. для обеспечения защиты конфиденциальной информации в сетях подвижной радиосвязи.

Комплекс предназначен для работы в радиосетях одно и двухчастотного симплекса, функционирующих в условном частотном диапазоне П45.

Комплекс обеспечивает защищенный речевой радиообмен, передачу по радиоканалу речевых сообщений, данных, служебной и управляющей информации.

Разработанные СКЗИ удовлетворяют «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну», предъявляемым к СКЗИ по уровню защищенности до класса КВ2 включительно при типе нарушителя до Н5 включительно.

СКЗИ обеспечивают:

- работу с речевым сигналом в полосе частот от 0,3 до 3,0 кГц для шага сетки рабочих частот 25 и от 0,3 до 2,55 кГц для шага сетки рабочих частот 12,5 КГц;
- преобразование речи (кодирование речи) в цифровую форму методом линейного предсказания на скорости 4800 бит/с в режиме работы СКЗИ с шагом сетки рабочих частот 25 кГц на основе алгоритма ACELP и 2400 бит/с в режиме работы СКЗИ с шагом сетки рабочих частот 12,5 кГц на основе алгоритма MELP.

Комплекс обеспечивает построение защищенных радиосетей на базе СКЗИ различного типа (носимых, мобильных, стационарных), в которых используются принципы унификации в части криптографических преобразований, обработки речи, данных и ключевых структур. Все СКЗИ имеют возможность получения ключевой информации, команд управления и мониторинга по каналу радиосвязи от единого пункта управления безопасностью.

Особенности разработанного комплекса СКЗИ:

1. Разработка всех типов СКЗИ осуществлена на базе комплекса радиостанций типа «Гранит» (ЗАО «САНТЭЛ, г. Москва), освоенных промышленностью и принятых на снабжение ОВД России.

2. Создание всех типов СКЗИ велось с применением унифицированных аппаратно-программных решений по защите информации, реализованных в рамках специального универсального модуля (СУМ), встраиваемого во все типы радиосредств. Специальное программное обеспечение СУМ обеспечивает возможность выполнения функций криптографической защиты информации, управления приемопередатчиком и функционирования СКЗИ в радиосети согласно единому протоколу.

3. Разработка СКЗИ проводилась на принципах унификации для всех составных частей подсистем как в части криптографической обработки речи, данных и ключевых структур, так и в системе криптографических протоколов внутреннего и внешнего управления сигнализацией.

4. СКЗИ комплекса совместимы по алгоритмам цифрового преобразования речи, канального протокола передачи данных, шифрования, управлению и сигнализации.

5. Алгоритмы шифрования обеспечивают быстрое вхождение в синхронизм СКЗИ. Время вхождения в синхронизм двух аппаратов шифрования, в режиме прямой связи, не более 500 мс.

6. Все типы СКЗИ работают под управлением диспетчерского пункта управления безопасностью.

В состав комплекса СКЗИ входят следующие технические средства:

- СКЗИ носимое абонентское;
- СКЗИ возимое абонентское;
- СКЗИ стационарное абонентское;
- ретранслятор с функциями СКЗИ;
- диспетчерский пункт оперативного дежурного (ДПОД);
- диспетчерский пункт управления безопасностью (ДПУБ);
- устройство ввода ключевой информации и программирования (УВКиП).

СКЗИ абонентские. Абонентские СКЗИ представляют собой абонентские РС типа «Гранит», выполненные по требованиям, предъявляемым к РС, предназначенным для передачи конфиденциальной информации, защищаемой по классу КВ 2, со встроенным СУМ, осуществляющим функции криптографической защиты информации и удаленного управления функциями безопасности.

СКЗИ носимое абонентское разработано на базе радиостанции «Гранит-303-35».

СКЗИ абонентское возимое и абонентское стационарное разработаны на базе мобильной радиостанции «Гранит-203-25».

СУМ реализуется в виде самостоятельного модуля на базе многослойной печатной платы и обеспечивает:

- необходимые габариты, достаточные для встраивания его в носимые, возимые и стационарные радиостанции;
- работу по единому протоколу радиосвязи, что позволяет обеспечить организацию конвенциальных сетей защищенной радиосвязи;
- ввод/вывод речевой информации, данных, ключевой информации и сигналов управления;
- преобразование речевого сигнала (сжатие) в цифровую форму и обратно;
- пакетную передачу данных с использованием методов помехоустойчивого кодирования и решающей обратной связи;
- криптографическую защиту речевой информации и данных, имитозащиту передаваемых данных;
- полный контроль аппаратных и программных средств после включения питания и каждого нажатия тангенты;
- преобразование цифровых сигналов в аналоговый вид и обратно для помехоустойчивой передачи/приема по радиоканалу (функцию радиомодема);
- симплексный режим работы;
- возможность функционирования СКЗИ в режимах:
  а) незащищённой аналоговой связи;
  б) незащищённой цифроаналоговой связи;
  в) защищённой цифроаналоговой связи;
  г) ввода ключевой информации;
  д) управления ключами по каналу связи;
  е) мониторинга безопасности и состояния готовности по каналам связи.
- дистанционное включение СКЗИ на передачу;
- отключение (блокировку) или включение (разблокировку) приёмопередающих трактов СКЗИ (в произвольной комбинации);
- ответ СКЗИ на запрос ДПУБ о его состоянии;
- передачу и приём вызовов «циркулярный», «групповой» и «индивидуальный»;
- передачу и прием служебной информации для ДПУБ;
- блокировку работы СКЗИ в радиоканале при вводе ключевой информации с устройства ввода ключей и программирования (УВКиП).

Ретранслятор с функциями СКЗИ. Ретранслятор с функциями СКЗИ создан на базе ретранслятора «Гранит-Р102-15» и обеспечивает следующие возможности:

- расшифровку управляющей информации;
- канал связи для шифрованных речевых сигналов и данных абонентов, идентификационные номера которых фигурируют в базе данных ретранслятора (разграничение доступа для абонентов);
- регенерацию информационного сигнала на уровне модемов СКЗИ;
- обмен ключевой и управляющей информацией с ДПУБ по каналу связи;
- дистанционное считывание и запись информации из/в базу данных ретранслятора по каналу связи от ДПУБ;
- дистанционное управление основными режимами работы от ДПУБ по рабочему радиоканалу;
- принудительное отключение приёмопередатчика со стиранием открытой ключевой информации;
- программирование радиоданных и ввод ключевой информации с использованием устройства ввода ключей и программирования;
- блокировку работы приемопередатчиков в радиоканале при вводе ключевой информации с устройства УВКиП в блок контроллера управления;
- защиту от несанкционированного доступа.

Диспетчерский пункт оперативного дежурного. Диспетчерский пункт оперативного дежурного (ДПОД) обеспечивает контроль за соблюдением корреспондентами радиосети регламента связи, запись (документирование) радиопереговоров и данных о параметрах сеансов связи, а также возможность просмотра и анализа документированной информации о фактах выхода СКЗИ в эфир.

В состав ДПОД входят следующие технические средства:

- СКЗИ стационарное диспетчерское;
- автоматизированное рабочее место оперативного дежурного (АРМОД).
- СКЗИ стационарное диспетчерское предназначено для сбора и выдачи в АРМОД необходимой для работы оперативного дежурного служебной информации.
- СКЗИ стационарное диспетчерское обеспечивает также выдачу дешифрованного речевого сигнала в ПЭВМ АРМОД для осуществления записи (документирования) радиопереговоров.

АРМОД обеспечивает обработку служебной информации, полученной от стационарного СКЗИ, и вывод на монитор следующих данных о работе сети:

- идентификационных данных абонентов, с отображением информации кто и кого вызывал;
- типов режима вызова (циркулярный, групповой или индивидуальный);
- номера рабочего ключа, на котором осуществлялся сеанс связи;
- времени начала и конца сеанса связи, а также длительности сеанса;
- сведения о фактах дистанционного управления СКЗИ сети защищенной радиосвязи со стороны ДПУБ.

АРМОД обеспечивает также возможность оперативного прослушивания записанных переговоров.

Устройство ввода ключевой информации и программирования. Устройство ввода ключевой информации и программирования (УВКиП) предназначено для ввода ключей, обеспечивающих криптографическую защиту конфиденциальной информации, а также для программирования радиоданных.

УВКиП используется для ввода ключевой информации и радиоданных при начальном запуске (инициализации) СКЗИ и вводе очередных рабочих ключей в процессе эксплуатации при невозможности их доведения дистанционно по каналам радиосвязи от ДПУБ до СКЗИ.

Устройство УВКиП обеспечивает:

- ввод в СКЗИ частот приема/передачи не более чем для 99 каналов радиосвязи;
- прием ключей из малогабаритных электронных носителей ключевой информации из состава аппаратуры САУБ через COM-порт;
- хранение ключей;
- ввод ключей в СКЗИ комплекса;
- индикацию на жидкокристаллический индикатор состояния процесса загрузки и состояния устройства;
- автономную работу от штатных аккумуляторов;
- электропитание от сети 220 В с одновременной подзарядкой аккумуляторов с помощью сетевого адаптера 220В/9В;
- защиту от несанкционированного доступа.

Диспетчерский пункт управления безопасностью. Диспетчерский пункт управления безопасностью (ДПУБ) предназначен для централизованного управления процессами организации защищенной радиосвязи и контроля ее корректной работы со стороны диспетчера системы безопасности.

В состав ДПУБ входят следующие технические средства:

- СКЗИ стационарное диспетчерское;
- автоматизированное рабочее место диспетчера (АРМД);
- средство автоматизированного управления безопасностью (САУБ);

Технические средства ДПУБ территориально могут находиться в разных местах, при этом их взаимодействие осуществляется через локальную вычислительную сеть.

СКЗИ стационарное диспетчерское предназначено для обеспечения обмена по радиоканалу ключевой и служебной информацией между ДПУБ и удаленными СКЗИ, входящими в состав радиосети.

АРМД обеспечивает диспетчеру системы возможность визуального анализа информации о работе системы безопасности и радиосети в целом, формирование и посылку команд об изменении режимов ее работы.

САУБ является основным элементом ДПУБ. Он предназначен для генерации ключей, их хранения, распределения и доведения до абонентских СКЗИ по каналу радиосвязи.

В части реализации криптографических алгоритмов САУБ удовлетворяет «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну», предъявляемым к СКЗИ по уровню защищенности до класса КА 1 включительно при типе нарушителя до Н6 включительно.

САУБ обеспечивает следующие функциональные процессы:

- управление ключевой и служебной информацией;
- управление безопасностью;
- работа с базами данных (БД) и регистрационным журналом;
- обмен служебной информацией.

Управление ключевой информацией. САУБ обеспечивает следующие процессы управления ключевой и служебной информацией:

а) децентрализованное формирование ключей из исходной двоичной случайной последовательности, хранящейся на электронных дисках;

б) распределение и доведение ключей до СКЗИ по каналам связи согласно заданной схеме распределения и криптографической связанности (передача ключевых документов по каналу связи производится в режиме служебной связи в зашифрованном и имитозащищенном виде);

в) запись ключевых документов в электронные носители информации (криптофлэш) для дальнейшей перезаписи в УВКиП;

д) хранение собственной ключевой информации (осуществляется в зашифрованном и имитозащищенном виде под ключом хранения. Ключ хранения является уникальным и с его помощью зашифровывается вся ключевая информация, изготовленная децентрализовано в САУБ);

е) гарантированное выборочное и полное стирание ключевой и специальной служебной информации.

ж) программно-аппаратное резервирование технических средств, ответственных за хранение ключевой и служебной информации.

Управление безопасностью. Для управления безопасностью радиосети в САУБ реализованы следующие функции:

а) Функция отслеживания криптографической связанности СКЗИ.

Сведения о криптографической связанности СКЗИ хранятся в виде электронного справочника абонентов. Электронный справочник содержит служебную информацию о каждом СКЗИ.

Электронный справочник является, по своей сути, динамической базой данных, в которую заносится вся служебная информация о каждом СКЗИ. Данный справочник формируется на АРМД.

Электронный справочник позволяет вводить сведения о новых СКЗИ, редактировать эти сведения, удалять их. Все действия производятся диспетчером при наличии соответствующего полномочия и фиксируются в журнале регистрации событий.

б) Функция дистанционного мониторинга.

Функция дистанционного мониторинга со стороны САУБ реализуются в форме команд, передаваемых по радиоканалу в зашифрованном и имитозащищенном виде.

К процессам дистанционного мониторинга относятся:

а) Контроль и учет технического состояния готовности СКЗИ и ретранслятора с функциями СКЗИ.

При получении команды от ДПУБ СКЗИ и ретранслятор с функциями СКЗИ проводят контроль своих аппаратных средств. Полученный результат зашифровывается, затем по каналу радиосвязи передается в ДПУБ, со стороны которого получен запрос. При получении ответа СКЗИ из состава ДПУБ расшифровывает данные и проверяет имитозащитную вставку. При положительном результате контроля данные заносятся в журнал регистрации событий, включая дату, время, регистрационный номер и криптономер СКЗИ, проводившего контроль, результаты контроля. Эти же данные отображаются на пульте управления АРМД.

б) Установление факта отсутствия несанкционированного доступа.

После установления факта несанкционированного доступа к СКЗИ с помощью САУБ необходимо провести дополнительные проверки факта и установление причин организационно-техническими методами.

При подтверждении факта несанкционированного доступа САУБ рассылает всем нескомпрометированным СКЗИ команды о факте несанкционированного доступа с указанием криптономера скомпрометированного СКЗИ и регистрирует данное событие соответствующим способом в регистрационном журнале.

Результатом выполнения этих действий является исключение скомпрометированных абонентов из радиосвязи. Таким образом, СКЗИ, по отношению к которому установлен факт несанкционированного доступа, блокируется.

в) Функция разграничения полномочий и управления доступом к ресурсам САУБ.

Доступ операторов и администраторов управления к техническим средствам САУБ осуществляется только после подключения индивидуальных носителей аутентифицирующей информации, их аутентификации, и после ввода личного пароля.

Индивидуальный носитель аутентифицирующей информации формируется для каждого пользователя в процессе инициализации САУБ. В формат аутентифицирующей информации входит ФИО пользователя, должность, индивидуальный номер, назначаемые полномочия, время действия полномочий. Также в индивидуальный носитель аутентифицирующей информации записывается образ личного пароля. Личный пароль вырабатывается в специальном блоке САУБ из исходной случайной двоичной последовательности с применением криптоалгоритма.

Аутентифицирующая информация зашифровывается и нарабатывается соответствующая имитозащитная вставка. Затем зашифрованная и имитозащищенная аутентифицирующая информация, а также образ пароля записываются в носитель аутентифицирующей информации, а пароль доступа выдается пользователю.

При трехкратном вводе неправильного пароля доступ пользователя к центру генерации ключей блокируется.

Обмен служебной информацией. От ДПУБ к СКЗИ служебная информация передается по каналам радиосвязи.

Она передается в зашифрованном и имитозащищенном виде. К служебной информации относятся:

- команды дистанционного мониторинга;
- команды передачи по каналам связи ключевых документов и ключей;
- команды по удалению ключевых документов и ключей.

Результаты обработки всех служебных команд фиксируются в регистрационном журнале. Изменения в состоянии ключевых документов заносятся в базу данных по учету ключевых документов.

Радиомодемы для СКЗИ. При создании радиомодемов для СКЗИ важной задачей являлся выбор сигнально-кодовых конструкций, обеспечивающих помехоустойчивую передачу информации по УКВ радиоканалам с шагом сетки частот соответственно 12,5 и 25,0 кГц с шириной спектра 2,55 и 3,0 кГц.

Во всех типах СКЗИ комплекса «Радиозанавес» (абонентских носимых, возимых и стационарных СКЗИ, диспетчерских СКЗИ, ретрансляторе с функциями СКЗИ) применены радиомодемы, обеспечивающие передачу речи, преобразованной речепреобразующим устройством, и данных (ключевой информации, радиоданных, команд управления безопасностью, команд оперативного управления) с необходимым уровнем помехоустойчивости и достоверности.

При этом помехоустойчивость передачи данных обеспечивается с большим уровнем, так как требуется гарантированное доведение данных до получателя.

Выбор сигнально-кодовых конструкций радиомодема осуществлялся с учетом результатов сравнительного анализа характеристик различных радиомодемов отечественного и импортного производства [1–4].

Принципы реализации радиомодема для передачи речи. В радиомодеме в режиме передачи защищенной речи применен многочастотный модем с ортогональным частотным разделением поднесущих (OFDM) с двух и трехкратной относительной фазовой модуляцией.

Для режимов работы по радиоканалу с шагом сетки рабочих частот 25 и 12,5 кГц применены различные сигнально-кодовые конструкции, отличающиеся длиной модемной посылки (OFDM-символа), и обеспечивающие различную ширину спектра группового модемного сигнала. Параметры модемного сигнала приведены в табл. 1.

Таблица 1

Полоса спектра сигнал, кГц	Кол-во поднесущих	Длина посылки (OFDM-кадра), мс	Тип модуляции	Помехоустойчивое кодирование	Кол-во бит в одной посылке	Кол-во информационных бит в посылке	Информационная скорость передачи, бит/с
0,3–3,0	75	30	ОФМ-8	3,2	225	144	4800
0,3–2,55	36	20	ОФМ-4	3,2	72	48	2400

В пределах одной модемной посылки (OFDM-кадра) осуществляется перемежение.

Кодирование осуществляется сверточным кодом, с длиной кодового ограничения К=7 и кодовой скоростью 2/3. На приеме осуществляется декодирование по алгоритму Витерби.

Для режима работы по радиоканалу с шагом сетки рабочих частот 25 кГц применена сигнально-кодовая конструкция, обеспечивающая канальную скорость передачи информации 7200 бит/с, с учетом помехоустойчивого кодирования информационная скорость составляет 4800 бит/с.

Для режима работы по радиоканалу с шагом сетки рабочих частот 12,5 кГц применена сигнально-кодовая конструкция, обеспечивающая канальную скорость передачи информации 3600 бит/с, с учетом помехоустойчивого кодирования, информационная скорость составляет 2400 бит/с.

Кадры с речевой информацией начинают передаваться сразу после преамбулы.

Принципы реализации радиомодема для передачи данных. В радиомодеме в режиме передачи данных применен многочастотный модем с ортогональным частотным разделением поднесущих (OFDM) с двух и трехкратной относительной фазовой модуляцией.

Для режимов работы по радиоканалу с шагом сетки рабочих частот 25 и 12,5 кГц применены различные сигнально-кодовые конструкции, отличающиеся длиной модемной посылки (OFDM-символа), и обеспечивающие различную ширину спектра группового модемного сигнала. Параметры модемного сигнала приведены в табл. 2.

Таблица 2

Полоса спектра сигнала, кГц	Количество поднесущих	Длина посылки (OFDM-кадра), мс	Тип модуляции	Помехоустойчивое кодирование	Кол-во бит в одной посылке	Кол-во информационных бит в посылке	Информационная скорость передачи, бит/с
0,3–3,0	75	30	ОФМ-8	2,1	225	144	3600
0,3–2,55	36	20	ОФМ-4	2,1	72	48	1800

В пределах одной модемной посылки (OFDM-кадра) осуществляется перемежение.

Кодирование осуществляется сверточным кодом, с длиной кодового ограничения К=7 и кодовой скоростью 1/2. На приеме осуществляется декодирование по алгоритму Витерби.

Для режима работы по радиоканалу с шагом сетки рабочих частот 25 кГц применена сигнально-кодовая конструкция, обеспечивающая канальную скорость передачи информации 7200 бит/с, с учетом помехоустойчивого кодирования информационная скорость составляет 3600 бит/с.

Для режима работы по радиоканалу с шагом сетки рабочих частот 12,5 кГц применена сигнально-кодовая конструкция, обеспечивающая канальную скорость передачи информации 3600 бит/с, с учетом помехоустойчивого кодирования, информационная скорость составляет 1800 бит/с.

В режиме передачи данных в модеме реализован протокол пакетной передачи. Передача выполняется в полудуплексном пакетном режиме с квитированием принятого пакета данных и автоматическим повтором непринятого пакета данных.

Кадры с данными начинают передаваться сразу после преамбулы.

Таблица 3

Информационная скорость передачи, бит/с	Преамбула, число посылок			Данные, число посылок			Признак конца пакета
	Ускоритель	Признак начала пакета	Блок служебных данных	Заголовок пакета (10 байт информации)	Полезные данные (N байт)	Контрольная сумма данных (4 байта)	
4800	5	1	6 (x6)	3 (x4)	k	1	1
2400	5	1	9 (x3)	6 (x2)	k	1	1

Ускоритель – специализированная сигнальная конструкция, используемая для ускоренной синхронизации модема.

Признак начала пакета, признак конца пакета – сигнальные конструкции, обнаруживаемые модемом, используются для целей пакетной синхронизации.

Блок служебных данных предназначен для передачи служебной информации, содержащей данные об идентификации, сетевой адресации и параметрах функционирования криптосистемы для данного сеанса связи.

Заголовок пакета содержит служебную информацию, необходимую для функционирования протокола передачи данных.

Контрольная сумма данных – контрольная сумма на поле полезных данных по алгоритму CRC 32

Формат заголовка пакета представлен в табл. 4.

Таблица 4

Тип пакета	Номер сеанса	Длина пакета	Резерв	Контрольная сумма
4 бита	8 бит	16 бит	20 бит	32 бита

Тип пакета:

0x1 – сообщение (команда, радиоданные, ключевая информация и др.).

0x4 – ответ на сообщение.

Номер сеанса инкрементируется при передаче следующего пакета данных. При повторной передаче не изменяется. Приемник по совпадению номера сеанса определяет повторный пакет и использует линейное накопление (код повторение-накопление).

Длина пакета – исходная длина блока пользовательских данных, байт.

Контрольная сумма – контрольная сумма на поле заголовока по алгоритму CRC32.

Результаты испытаний СКЗИ комплекса «Радиозанавес» на реальных каналах радиосвязи подтвердили правильность выбранных сигнально-кодовых конструкций радиомодема. Заложенные при реализации алгоритмы обработки сигналов позволяют модему обеспечивать передачу/прием информации при отношении сигнал/шум 2–4 дБ во всех режимах работы. При обеспечении приемником радиостанции отношения сигнал/шум не хуже 12 дБ на выходе демодулятора (что требует ГОСТ 12252-86) радиомодем гарантированно обеспечивает надежную и качественную передачу криптографически защищенных речи и данных.

Выводы. Анализ возможностей комплекса средств криптографической защиты информации, разработанного в рамках ОКР «Радиозанавес», позволяет сделать вывод о том, что создан эффективный инструмент для создания защищенных конвенциональных сетей подвижной радиосвязи. Новизна разработки заключается в том, что впервые в России при создании СКЗИ для защищенных сетей подвижной радиосвязи реализованы следующие возможности:

- защита конфиденциальной информации, циркулирующей в радиосети, техническими средствами криптографической защиты с уровнем защищенности по классу КВ 2;
- реализация процедуры управления ключевой информацией по УВЧ-радиоканалу, что позволило обеспечить хранение всей ключевой информации в контролируемой зоне, а в абонентских СКЗИ – только рабочих ключей. Это дало возможность существенно упростить процесс эксплуатации абонентских радиостанций. Теперь процедура замены рабочих ключей может осуществляться дистанционно по каналам радиосвязи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Немировский М.С., Шорин О.А., Бабин А.И., Сартаков А.Л.* Беспроводные технологии от последней мили до последнего дюйма / Под ред. М.С. Немировского, О.А. Шорина. – М.: Эко-Трендз, 2009. – 400 с.
2. Сайт группа компаний DataRadio [Электронный ресурс]. – Режим доступа: www. dataradio.ru/.
3. Javad. Group of companies [Электронный ресурс]. – Режим доступа: www. javad.com/.
4. TLP Holding [Электронный ресурс]. – Режим доступа: www.tl-group.de.

Статью рекомендовал к опубликованию д.т.н. В.Х. Пшихопов.

Трушин Станислав Владимирович
МВД России.
E-mail: s-trushin@YANDEX.RU.
г. Москва, ул. Житная, 12.
Тел.: 84956678090.
Первый заместитель начальника департамента.

Пучков Геннадий Юрьевич
ГУ НПО «СТиС» МВД России.
E-mail: PGU7@YANDEX.RU.
г. Москва, ул. Пруд Ключики, 2.
Тел.: +79857652920.
Начальник научно-исследовательской лаборатории; к.т.н.

Яковлев Игорь Евгеньевич
ФГУП «ПНИЭИ».
E-mail: yakovlev.pniei@gmail.com.
г. Пенза, ул. Советская, 9.
Тел.: 88412593389
Заместитель научного директора.

Trushin Stanislav Vladimirovich
MIA of Russian Federation.
E-mail: s-trushin@YANDEX.RU.
12, Zhitnaja Street, Moscow, Russia.
Phone: +74956678090.
First Deputy of the Chief of Department.

Puchkov Gennady Jurievich
GU NPO «STiS» MIA of Russia.
E-mail: PGU7@YANDEX.RU.
2, Prud Kluchiki Street, Moscow, Russia.
Phone: +79857652920.
Chief of Research Laboratory; Cand. of Eng. Sc.

Yakovlev Igor Evgenyevich
FGUP «PNIEI».
E-mail: yakovlev.pniei@gmail.com.
9, Soviet Street, Penza, Russia.
Phone: +78412593389.
Deputy Scientific Director.

УДК 51-74, 519.178

В.В. Кульба, Д.С. Сомов, А.А. Кочкаров

ПРИМЕНЕНИЕ СТРУКТУРНО-ИНТЕГРИРОВАННЫХ ИНДИКАТОРОВ В МОНИТОРИНГЕ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

Предлагается индикаторный подход в мониторинге сложных технических систем, позволяющий снизить информационную нагрузку на оператора системы, не снижая точности и эффективности передаваемой оператору информации. Рассматривается теоретико-графовая модель распространения возмущений по системе. Сформулирована многокритериальная задача оптимального выбора индикаторов. Предложены алгоритмы построения решений задачи. Алгоритмы предлагают решения, оптимальные по одним критериям, и дают приближенные оценки по остальным.

Техническая система; мониторинг; датчики, индикаторы.

V.V. Kulba, D.S. Somov, A.A. Kochkarov

THE USE OF STRUCTURE-INTEGRATED INDICATORS IN COMPLEX TECHNICAL SYSTEMS MONITORING

The article proposes an indicator approach to the problem of monitoring complex technical systems, which allow to reduce the information load on the system operator, without loss in the accuracy and efficiency of information transmitted to the operator.

The graph-theoretical model of the disturbance distribution in the system is used in the article. The multicriterion problem of optimal choice of indicators is set. In the article we propose algorithms for constructing solutions of the problem. Algorithms offer a solution optimal for one criterion, and give approximate estimates for the remaining criteria.

Technical system; monitoring; sensors; indicators.

Введение. Одними из важнейших задач, решаемых при проектировании сложных технических систем, являются задачи обеспечения безопасности, надежности и устойчивости функционирования системы [1, 2, 3]. Одной из составляющих решения данных задач является использование систем мониторинга, позволяющих получать различные параметры состояния системы, ее функционирова-