СПИСОК ЛИТЕРАТУРЫ

1. Калайда В.Т., Соловьев Б.А. Базовое программное обеспечение интегрированных распределенных систем безопасности // Информационные технологии. – 2006. – № 1. – С. 43–59.
2. Соловьев Б.А., Калайда В.Т. Программный комплекс построения распределенных систем обработки информации «Базис». Отраслевой фонд алгоритмов и программ Минобрнауки РФ 10.10.2006 № 7027. № гос. регистрации 50200601793 // Инновации в науке и образовании: Телеграф отраслевого фонда алгоритмов и программ. – 2006. – С. 8.
3. Калайда В.Т., Губанов Н.Ю. Идентификация лица человека методом опорной гиперплоскости // Вычислительные технологии – 2007. – № 1. – С. 96–101.
4. Елизаров А.И., Калайда В.Т., Соловьев Б.А. Программный комплекс идентификации человека по изображению лица «Observer». Отраслевой фонд алгоритмов и программ Минобрнауки РФ 10.10.2006 № 7026. № гос. регистрации 50200601792 // Инновации в науке и образовании: Телеграф отраслевого фонда алгоритмов и программ. – 2006. – С. 9.

Поступила 23.10.2008 г.

УДК 681.3.06

НЕКОТОРЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ КРИПТОГРАФИЧЕСКОГО ПРОЦЕССОРА ДЛЯ СИСТЕМ СВЯЗИ НА БАЗЕ ПАКЕТНОГО КОНТРОЛЛЕРА «ВИП-М»

В.В. Гринемаер, А.А. Шамин

Томский научный центр СО РАН
Томский политехнический университет
E-mail: salex@cc.tpu.edu.ru

Предложены способы обеспечения безопасности при обмене зашифрованной и исходной информации в системе связи с пакетной передачей данных на базе «ВИП-М». Разработан новый протокол обмена данными между криптографическим процессором и управляющим устройством.

Ключевые слова:
Информационно-телекоммуникационная система, пакетная передача данных, криптография.

Использование средств криптографической защиты данных в составе распределённых информационно-телекоммуникационных систем с пакетной передачей данных для труднодоступных объектов имеет свои особенности. Такого типа средства используют для построения систем оповещения и связи, автоматизированных систем сбора оперативной информации (авиабазы охраны лесов, государственные лесные службы, силовые структуры) [1]. Актуальность исследования и создания подобных систем обусловлена необходимостью в совершенствовании существующей технологии сбора первичной информации в труднодоступных районах, оперативного формирования данных в нужных форматах и своевременной их передаче в контрольные сроки заинтересованным службам и ведомствам.

Очевидно, что полноценный защищённый обмен может быть реализован с помощью криптографических процессоров – специализированных устройств для шифрования-дешифрования сообщений. Криптографический процессор в системах передачи данных отделяет функцию криптографических преобразований от функций приёма/передачи информации по каналам связи.

Широко известные информационно-телекоммуникационные системы с пакетной передачей данных для труднодоступных объектов часто используют в качестве абонентов пакетные контроллеры «ВИП-М», позволяющие передавать информацию по КВ и УКВ радиоканалам, телефонным и телеграфным линиям, через абонентские терминалы спутниковых систем связи [2].

В настоящем исполнении у пакетного контроллера «ВИП-М» недостаточно ресурсов для реализации криптографических алгоритмов согласно ГОСТ 28147-89.

Анализ существующих криптографических процессоров – «Криптон», «Верба», «Континент» и других показал, что они не могут быть использованы совместно с пакетным контроллером «ВИП-М» по причине особенностей его интерфейсов и конструкции. Поэтому актуальным является создание криптографического процессора, обеспечивающего режим защищённого обмена конфиденциальной информацией между абонентами в системах связи на базе пакетных контроллеров «ВИП-М» [3].

Разработан криптографический процессор «Актиния», позволяющий работать совместно с управляющими устройствами, имеющими интерфейс RS232, в том числе – совместно с «ВИП-М».

Отличительной особенностью данного криптографического процессора является возможность использования нескольких вариантов ввода ключа шифрования:

- Ключ (носитель типа iButton) считывается непосредственно криптопроцессором.
- Ключ вводится управляющим устройством. Данный вариант ввода ключа позволяет хранить их в управляющем устройстве, а также использовать для хранения ключей любой носитель, который управляющее устройство может прочитать – например FLASH-диск, SD/MMC-карту и т. п.

Целью данной работы является представление протокола взаимодействия криптографического процессора с управляющим устройством, например, с пакетным контроллером «ВИП-М».

На рис. 1 показана система передачи данных с защитой части абонентов от несанкционированного доступа (средства сопряжения абонентов – ВИП-М и ПЭВМ – с каналами связи не приведены). Все абоненты могут передавать и принимать открытую информацию, не защищённую криптопроцессором.

Конфиденциальную информацию могут принимать и передавать лишь абоненты, имеющие криптопроцессор и соответствующий ключ.

К устройствам криптографической защиты информации предъявляется ряд требований, которые описаны в государственных стандартах. В частности – алгоритмы, применяемые для шифрования, также регламентированы государственными стандартами и не могут быть выбраны произвольно.

С учётом требований эксплуатации систем, в состав разрабатываемых средств защиты криптографической информации (СКЗИ) должны входить:

1. Криптопроцессор в виде дополнительного встраиваемого электронного устройства к пакетному контроллеру «ВИП-М».
2. Программное обеспечение, выполняющее функции шифрования и контроля целостности.
3. Программа тестирования программно-аппаратного обеспечения.
4. Документация на разработанное программное обеспечение и аппаратные средства.

На основании изучения требований к разрабатываемой СКЗИ и требований государственных стандартов выработан перечень характеристик, которым должно соответствовать разрабатываемое устройство «ВИП-крипто», а именно устройство должно:

- хранить ключевую информацию на отчуждаемых носителях;
- выполнять хеширование данных в соответствии с ГОСТ Р34.11-94 («Информационная технология. Криптографическая защита информации. Функция хеширования»);
- производить шифрование данных во всех режимах, определённых ГОСТ 28147-89 («Системы обработки информации. Защита криптографическая»);

Целостность программной части продукта должна обеспечиваться при помощи электронно-цифровой подписи (ЭЦП).

Разработанная система криптографической защиты для пакетных контроллеров «ВИП-М», основанная на сертифицированных аппаратно-программных средствах, обладает следующими основными характеристиками:

- ключевая информация хранится в стандартных носителях типа iButton фирмы Dallas;
- передача информации по различным каналам связи (радиоканал, проводной канал, спутниковые каналы – Гонец и ГлобалСтар) осуществляется одним устройством;

Криптопроцессор «Актиния» выполнен в виде отдельного модуля.

Работа интерфейса RS232 организована таким образом, что информация циркулирует в виде пакетов в режиме полудуплекса, т. е. в каждый момент времени движение информации может происходить только в одном направлении. Обмен осуществляется всегда под управлением ведущего (управляющего) устройства, посылающего пакет с данными или команду и получающего от «Актинии» ответный пакет. Целостность информационных пакетов проверяется методом контрольной суммы (CRC16).

Обмен между устройствами удовлетворяет следующим правилам (протоколу):

- Управление обменом осуществляет ведущее устройство «ВИП-М».
- Режим полного дуплекса запрещён: два устройства не могут передавать информацию одновременно.

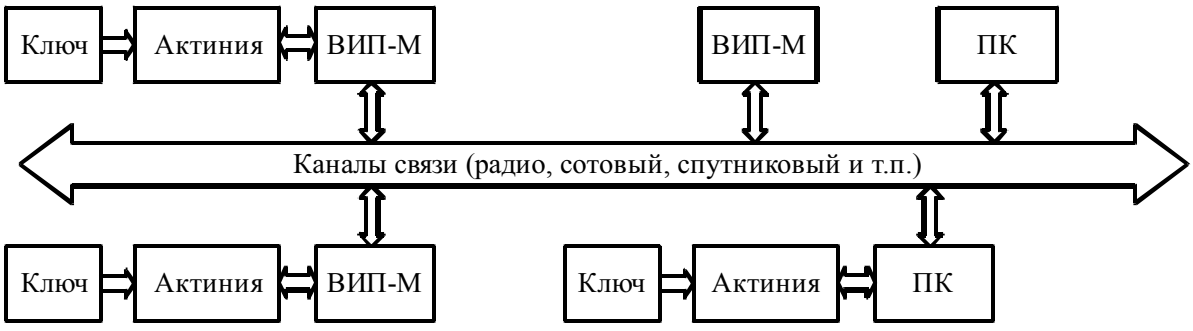

Рис. 1. *Система передачи данных, включающая СКЗИ. ПК – персональный компьютер*

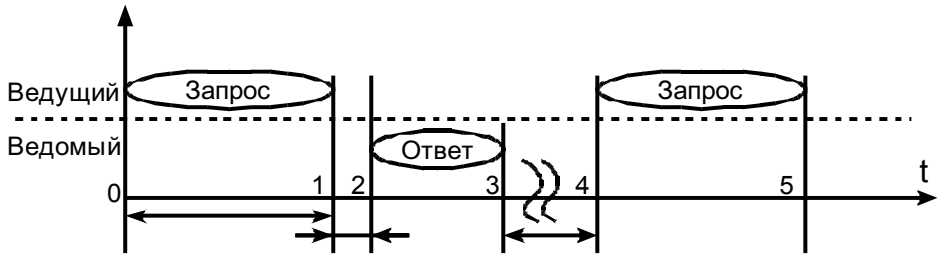

Рис. 2. *Временные диаграммы обмена данными*

- Максимальный размер пакета данных, передаваемый в одном сеансе обмена – 8 Кбайт.
- Разрешение коллизий:
  а) «Актиния» всегда находится в режиме приёма и отслеживает в канале адресованные только ему пакеты, каждый принятый адресный пакет подтверждается квитанцией.
  б) По приёму пакета запускается таймер обратного отсчёта времени задержки до активной посылки.
  в) При искажении пакета на стороне приёмника отсутствует квитанция, передатчик повторяет запрос.
  г) Каждый пакет имеет номер, квитанция имеет такой же номер, как и активный пакет.
  д) «Актиния» всегда отвечает на корректно принятый адресный пакет, квитанция может отсутствовать только если принятый пакет искажён или выставленная в пакете команда не входит в список поддерживаемых ведомым.

Временная диаграмма обмена данными представлена на рис. 2.

Пояснения диаграмме:

- Временной интервал 0–1 – передача пакета от ведущего к ведомому (зависит от скорости интерфейса и длины блока данных).
- Интервал 1–2 – время реакции ведомого, от момента получения пакета ведомым до начала посылки первого байта квитанции. В случае, если время превышает 300 мс, пакет от ведущего к ведомому считается не доставленным и его передача может повторяться до 3-х раз.
- Временной интервал 2–3 – передача квитанции от ведомого к ведущему (зависит от скорости интерфейса и длины блока данных).
- Временной интервал 3–4 – пауза между сеансами связи. Может составлять от 200 мс до нескольких секунд, определяется алгоритмом работы ведущего устройства.
- Временной интервал 4–5 – начало следующего сеанса связи (то же, что и интервал 0–1).

Для обеспечения безопасности при обмене зашифрованной и исходной информации в системе связи на базе пакетного контроллера «ВИП-М» приняты следующие алгоритмические меры:

- Блоки данных с зашифрованной информацией хранятся в отдельных фиксированных участках памяти (ведущего устройства и «Актинии») и очищаются сразу же после использования.
- Блоки данных с исходной информацией так же располагаются в отдельных участках памяти, очищаемых после использования.
- Время хранения исходных данных на «ВИП-М» и в криптографическом процессоре «Актиния» минимально, хранение их в любом виде в энергонезависимой памяти исключено.

Разработан протокол обмена данными между криптографическим процессором и управляющим устройством. Предложенный протокол обмена информацией позволяет использовать модуль криптографической защиты информации «Актиния» как совместно с «ВИП-М», так и в составе других устройств передачи данных.

Наличие нескольких способов ввода ключа позволяет адаптировать систему под различные условия работы.

СПИСОК ЛИТЕРАТУРЫ

1. Сонькин М.А., Слядников Е.Е. Архитектура и общая технология функционирования территориально распределенных аппаратно-программных комплексов с пакетной передачей данных // Известия Томского политехнического университета. – 2006. – Т. 309. – № 5. – С. 131–139.
2. Мирошенников А.И., Сергейчик С.А., Харламов С.А. Интегрированная система документированной связи и передачи данных. (Опыт внедрения и перспективы развития во внутренних войсках МВД России) // Связь и автоматизация МВД России. – 2005. – № 2. – С. 28–33.
3. Мещеряков Р.В., Росошек С.К., Шелупанов А.А., Сонькин М.А. Криптографические протоколы в системах с ограниченными ресурсами // Вычислительные технологии. – 2007. – Т. 12. – Спец. вып. 1. – С. 51–61.

Поступила 01.11.2008 г.