РОССИЙСКОЕ НАУЧНО-ТЕХНИЧЕСКОЕ ОБЩЕСТВО
РАДИОТЕХНИКИ, ЭЛЕКТРОНИКИ И СВЯЗИ ИМ. А.С. ПОПОВА

LVII
НАУЧНАЯ СЕССИЯ, ПОСВЯЩЕННАЯ ДНЮ РАДИО

Т Р У Д Ы

Т О М 1

МОСКВА - 2002

ЗАКРЫТИЕ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ С ПОМОЩЬЮ ВНЕШНИХ УСТРОЙСТВ НА УРОВНЕ СТЫКА ТЕРМИНАЛЬНОГО И КОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

Ашурбейли И.Р., Рухадзе К.В., Спокойный М.Ю., Федотов А.Г.

ОАО ЦКБ «Алмаз», Москва

При организации закрытой связи, закрытие информации при помощи внешних устройств позволяет практически не быть связанным с платформой компьютеров используемых в системе обмена информацией, кроме того, это гарантирует систему защиты информации в канале связи от компрометации при помощи различного рода закладок в системное или иное программное обеспечение.

Наиболее универсальным является применение устройств закрытия информации на уровне стыка между компьютером (DTE сторона) и коммуникационным оборудованием (DCE сторона), например модемом, как показано на рис. 1.

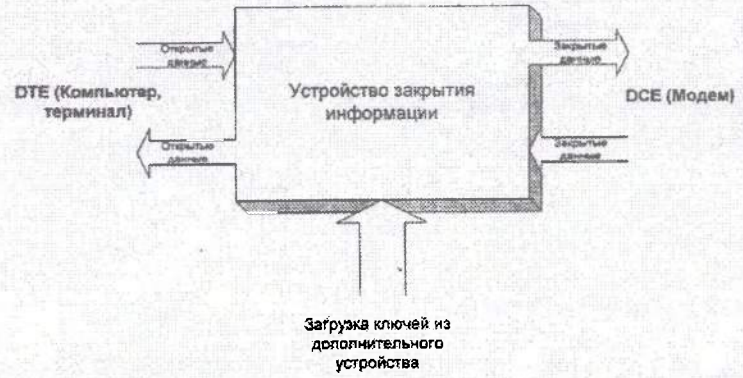


Рис. 1

Ключи загружаются из дополнительного устройства и хранятся только в самом устройстве, не попадая в компьютер и в коммуникационное оборудование. (Распределение и доставка ключей являются отдельной задачей, не рассматривается в рамках настоящего документа и решается не столько техническими, сколько организационными средствами.)

При организации закрытого канала связи общая схема соединений может выглядеть как показано на рис. 2.

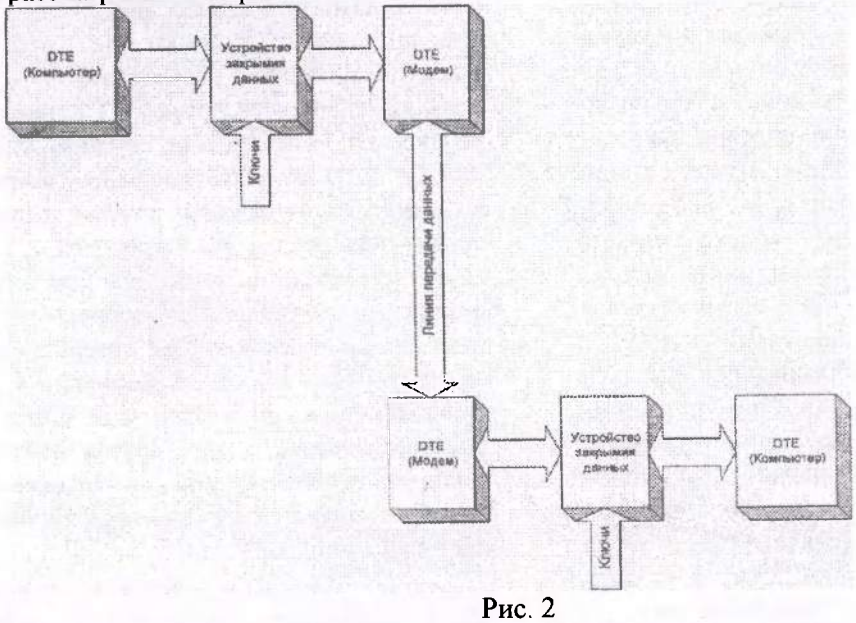
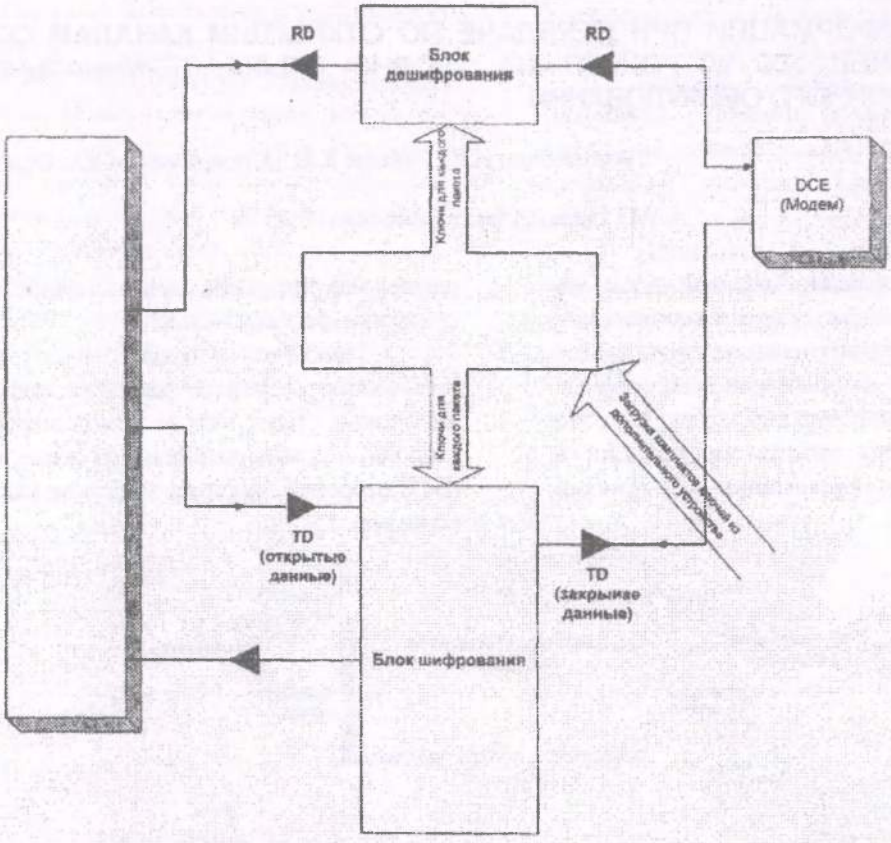


Рис. 2

Структура самого устройства закрытия данных показана на рисунке 3.



Блок хранения комплектов ключей
DTE
(Терминал, компьютер)
CTS Управление потоком

Рис. 3

Возможны три варианта организации закрытого канала передачи данных.

1.Вопросы гарантированной доставки информации берет на себя PTE сторона. Например при использовании пакетного режима передачи информации (это могут быть пакеты стандартных протоколов передачи информации или любые иные). В этом случае устройство закрытия данных, в которое предварительно загружены ключи, получив пакет из компьютера закрывает его и снабдив минимумом служебной информации (синхропосылка и номер ключа из комплекта) отправляет в модем. И наоборот, получив из модема закрытый пакет, раскрывает его и отдает в компьютер.

2.Вопросы гарантированной доставки информации берет на себя коммуникационное оборудование. С точки зрения устройства закрытия данных этот вариант аналогичен первому, устройство делит поступающую информацию на блоки (это могут быть те же пакеты или просто поток разделяется на кванты по времени) и шифрует каждый из них.

3.Вопросы гарантированной доставки и синхронизации устройств закрытия данных берет на себя дополнительный блок в самом устройстве. В этом случае компьютер и коммуникационное оборудование максимально разгружены от этих вопросов, но само устройство значительно усложняется.

В первом и во втором случае в устройстве закрытия данных необходимо наличие прозрачного режима для управления коммуникационным оборудованием со стороны компьютера (например AT команды для управления модемом или команды управления X25 PAD для установления соединения) и возможность управления потоком данных из компьютера со стороны устройства.

В третьем варианте для компьютеров организуется «труба» и все вопросы управления коммуникационным оборудованием, синхронизации ключей и обеспечения гарантированной доставки берет на себя само устройство, которое в этом случае становится сложнее, появляется дополнительный блок, который решает вопросы гарантированной доставки и синхронизации.

В этом случае в наибольшей степени будет происходить «разжимание» информации, поскольку вместе с полезной информацией должна передаваться служебная (в первом и втором случае этой информации передается

минимум), плюс, когда необходимо, повторная передача блоков полученных с ошибками, передача проверочных сумм, кодов восстановления, подтверждений и т.п.). Соотношение скорости передачи полезной информации и скорости передачи в линии в большой степени зависит от качества линии. В случае использования коммутируемых телефонных линий (для Москвы в среднем) это соотношение для гарантированного канала находится в пределах 1 к 1,6 - 2,5 (вместе с затратами на закрытие и открытие).

Блок хранения комплектов ключей должен сохранять данные при отключении питания и иметь емкость достаточную для хранения не одного, а многих ключей (с точки зрения надежности закрытия необходимо минимизировать количество информации закрытой на одном ключе), кроме того там же долен храниться резервный комплект ключей. Поскольку комплекты ключей должны меняться с некоторой периодичностью удобнее в нужный момент одновременно перейти на резервный комплект, а уже затем загрузить новый комплект.

С точки зрения использования алгоритмов закрытия информации наиболее правильным является использование ГОСТированного алгоритма закрытия информации. Этот алгоритм хорошо реализуется на подобном оборудовании, достаточно быстро работает и устойчивость его не подвергается сомнению.

Настоящий документ является в известной степени ознакомительным и не преследует цель рассмотреть все аспекты поднятой темы.

ПРОГРАММНАЯ РЕАЛИЗАЦИИ ЗАКРЫТОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ С ГАРАНТИРОВАННОЙ ДОСТАВКОЙ

Ашурбейли И.Р., Рухадзе К.В., Спокойный М.Ю., Федотов А.Г.

ОАО ЦКБ «Алмаз»

Под программной реализацией имеется в виду то, что все операции по:

- подготовке данных к передаче - компрессия;
- закрытию (шифрование) данных перед передачей их в линию;
- открытию (расшифровка) данных по получении их из линии;
- синхронизацию шифрования и защиту от несанкционированного доступа;
- введению необходимой избыточности для обеспечения контроля целостности переданных данных;
- исправлению искаженных в линии данных за счет добавляемых помехозащищающих кодов и обеспечение повторной передачи блоков данных в случаях, когда это невозможно;
- управлению оборудованием передачи данных;

берет на себя телекоммуникационное программное обеспечение, загружаемое в компьютер.

Таким образом, для прикладного ПО интерфейс к телекоммуникационному программному обеспечению является "бронированной трубой" к прикладному ПО на другой стороне.

Примером реализации такого телекоммуникационного ПО является система КаСот.

При использовании схемы передачи данных, показанной на рис.1.

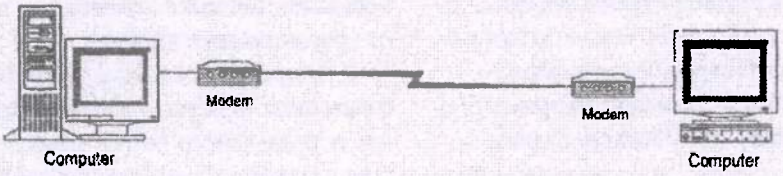


Рис. 1

Система проектировалась как банковская телекоммуникационная среда ориентированная на обеспечение работы подсистем Банк - Клиент и Банк - Филиал. Реальная эксплуатация системы рядом банков началась в апреле 1994 года. Сегодня около 60 банков и других организаций используют систему КаСот в своем технологическом процессе.

В ряде случаев, особенно на периферии, система КаСот оказалась единственным надежно работающим средством передачи данных по коммутируемым линиям. Система

работает в среде MS-DOS или Windows 95. Реальная эксплуатация показала, что для одновременного обслуживания четырех каналов на скорости до 38400 бит/сек достаточно компьютера уровня 386SX-25. (Четыре канала возникли из-за платформы реализации.)

Система построена по принципу Центр - Абоненты (рис. 2). Центр -компьютер, к которому подключено от одного до четырех телефонных линий через модемы, при этом Центр держит модемы в Автоответе и отвечает на "звонки" Абонентов. Возможна настройка всей системы или одного из каналов на поддержание постоянного соединения.

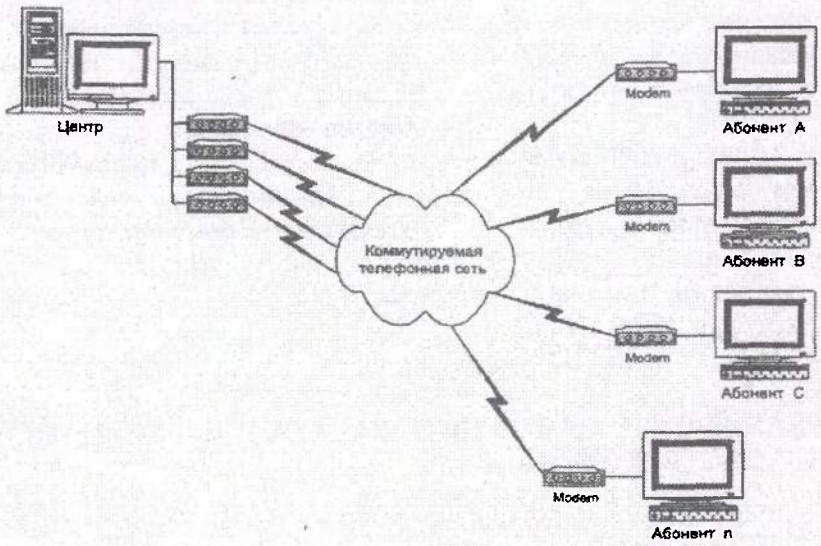


Рис. 2

Передача данных в рамках системы базируется на специально разработанном протоколе передачи данных, обладающем высокой помехоустойчивостью. Алгоритм протокола построен с учетом характера и уровня помех на отечественных телефонных линиях.

Система КаСom версии 3.6 обеспечивает упаковку и закрытие информации во время передачи ее по каналам связи. При этом упаковка и шифрование передаваемых данных происходит в памяти непосредственно перед передачей, а дешифрование и распаковка -сразу после приема информации перед записью ее на диск. Таким образом снижается время передачи информации и обеспечивается защита от несанкционированного доступа во время передачи информации по каналам связи. Время затрачиваемое на шифрование и паковку информации пренебрежимо мало по сравнению с временем передачи элементарного блока информации.

В виду того, что система КаСom использует собственный протокол передачи, данных и коррекции ошибок, использование модемов или другого каналообразующего оборудования без встроенной коррекции ошибок на зашумленных линиях не ухудшает и не замедляет передачи данных.

Для каждого Абонента на Центре заводится "Почтовый ящик" (группа каталогов) и ему присваивается ключ доступа к Центру, корректность которого проверяется в момент установления соединения. Таким образом соединиться и передать (и/или принять) данные может только зарегистрированный Абонент (заведенный в конфигурации Центра). В случае утраты или компрометации ключей доступа и шифрования, в Центре может быть сгенерирован новый ключ.

Подробнее о протоколе передачи данных:

1. Протокол является адаптивным - максимальная длина передаваемого элементарного блока динамически изменяется в зависимости от уровня помех в линии.

2. Встроенная система коррекции ошибок в сочетании с перераспределением данных в рамках передаваемого блока помогает в большинстве случаев избавиться от необходимости повторной передачи поврежденного блока. Алгоритм коррекции ошибок выбранный с учетом характера помех в линиях подключается только при высокой частоте искажений и изменяет избыточность в зависимости от зашумленности линии.

3. Специальные меры по увеличению надежности распознавания заголовка передаваe-

мого блока позволяют избавиться от рассинхронизации алгоритма на разных концах линии, что является наиболее неприятным при использовании известных протоколов передачи данных на зашумленных линиях.

4. Используемые в рамках протокола меры по отслеживанию состояния линии позволяют не разрывать связь при кратковременном исчезновении несущей.

5. Динамическая компрессия данных непосредственно перед передачей снижает время передачи. Кроме того после компрессии данные шифруются перед передачей в линию, что является надежной защитой от несанкционированного доступа и съема информации непосредственно с линии.

6. Протокол реализован так, что все настроечные параметры. оптимальные значения которых зависят от характера и уровня помех в линии, могут изменяться. В настоящий момент они подобраны для оптимальной передачи по коммутируемым линиям, на основе опыта эксплуатации в различных регионах России. Часть параметров вынесена в настроечные файлы.

На современных модемах система поддерживает скорость передачи данных до 38400 бит/сек (ограничение искусственное, больше никогда не требовалось), а с учетом предварительной упаковки информации реальная скорость передачи может быть значительно выше.

Существует версия протокола, реализованного в системе (правда несколько устаревшая), перенесенная в среду UNIX на компьютерах "Беста". А также версия системы, в которой "абонент" перенесен на карточный POS терминал Bull-Ю (чиповые депозитные карточки).

Основываясь на этом опыте, система целиком или некоторая ее часть может быть перенесена на другую платформу и адаптирована под нужды Заказчика и к его коммуникационному оборудованию.