Киркоров С.И.
Герман Е.Н.
Степанян А.Б.

ПОДХОД К ОРГАНИЗАЦИИ ЗАЩИТЫ ФАКСИМИЛЬНОЙ ИНФОРМАЦИИ

Факсимильная связь получила широкое распространение в повседневной жизни большинства государственных учреждений. Однако факсимильные коммуникации внутри общей коммутируемой телефонной сети довольно легко перехватить. Перехват и анализ факсимильной коммуникации реализуем на современном техническом уровне без значительных капитальных вложений. Создание безопасной факсимильной сети, которая даст возможность избежать нежелательного раскрытия секрета каждого пользователя, сегодня является актуальной задачей.

В настоящее время некоторые зарубежные фирмы выпускают факс-аппараты с встроенными устройствами шифрования и автономные факсимильные шифраторы. Среди зарубежных аналогов обладающих возможностью защиты информации можно отметить следующие продукты: Opex – 4130, CRYPTOFAX hc 4220 (CRYPTO PRODUCTS), SecLine Fax (INTRACOM), JFX SAFE Vault Models 300 & 400 (JONES FUTUREX).

Основной недостаток зарубежных аналогов – использование в качестве криптографического преобразования данных стандарт DES или другие стандарты, которые не приняты в действие на территории РБ (обычно такие продукты имеют высокую стоимость).

Имея ввиду, что при построении отечественных защищенных изделий разработчики вынуждены соблюдать баланс между необходимостью поддержания безопасности информационных систем с помощью отечественных средств защиты информации и использования зарубежных прогрессивных информационных технологий и зарубежных аппаратных компонентов [1].

С другой стороны, создание защищенных систем "с нуля" от ОС до приложений – наиболее радикальный способ, но неприемлем с экономической точки зрения, поэтому защищенные системы создают из компонент, имеющихся в наличии, преодолевая присущие им недостатки с помощью построения особой архитектуры таких систем и специально разработанных отечественных средств защиты [2].

Поэтому, имея ввиду, что в нашей стране факс-аппараты не производятся, было принято решение разработать устройство, выполненное в виде приставки к факс-аппарату, подключаемой в разрыв между телефонной линией и самим факс-аппаратом.

Разработанная нами аппаратура криптографической защиты (АКЗ) предназначена для защиты факсимильной информации передаваемых факс-аппаратом по открытым каналам связи и обеспечивающая целостность, конфиденциальность и доступность данных.

Предпосылки и стратегия, использованные в разработке АКЗ

При разработке АКЗ учитывались следующие предпосылки:

- АКЗ предназначен для передачи/приема информации ограниченного распространения;
- оборудование, подключаемое к телефонной сети общего пользования, должно быть сертифицировано;
- пользователь АКЗ должен иметь возможность работы в открытом и закрытом режиме;
- реализовывать алгоритм криптографического преобразования в соответствии с ГОСТ 28147-89;
- позволять использовать порт RS-232 для записи зашифрованной информации в персональный компьютер (для альтернативного способа передачи);
- совместно работать с факс-аппаратами группы 3 (G3) согласно стандартам МККТТ Т.4, МККТТ V.27ter, МККТТ V.29.

В разработке АКЗ реализована следующая стратегия:

1) АКЗ выполнено в виде приставки к факс-аппарату, подключаемой в разрыв между телефонной линией и самим факс-аппаратом;
2) использование в АКЗ промышленно выпускаемого микроконтроллера и факс-модема;
3) генерация сеансовых ключей с помощью физического датчика случайных чисел;
4) логически АКЗ представлен как посредник (прокси-сервер) в узлах виртуальной факсимильной сети;
5) взаимодействие АКЗ с факс-аппаратом выполняется согласно стандартам МККТТ Т.4, МККТТ V.27ter, МККТТ V.29 и МККТТ V.17;
6) взаимодействие АКЗ с АКЗ выполняется согласно стандартам МККТТ V.90 или МККТТ V.34bis/V34;
7) целостность и конфиденциальность сменных программных компонентов и передаваемых данных обеспечивается в соответствии с ГОСТ 28147-89;

8) используется программный протокол Zmodem для считывания или записи зашифрованной информации в персональный компьютер;
9) для обеспечения доступности данных размер входных и выходных буферов определяется аналогично как [3];
10) специализированное встроенное программное обеспечение имеет следующие свойства:
    - компактность;
    - модульность;
    - расширяемость и настройку системы команд диспетчера.

Используя основные принципы, предложенные в работах [4], [5], [6], [7] можно АКЗ обеспечить возможностью, при необходимости менять архитектуру и отдельные аппаратные компоненты.

Для АКЗ разработана и внедрена специальная система управления ключами, которая дает возможность обеспечить защищенное соединение между N пользователями (каждый с каждым). В обычном (не активном) режиме АКЗ передает нормальную (без шифрования) факсимильную информацию. В активном режиме вся факсимильная информация передается и принимается в зашифрованном виде. Вся секретная факсимильная информация (исходящая и входящая) хранится в памяти АКЗ (можно хранить до 60 страниц и более, в зависимости от комплектации) в шифрованном виде. Эти документы расшифруются только тогда, когда некий авторизованный пользователь посчитает нужным, чтобы эти документы передавались в локальный факс-аппарат. Все коммуникации в секретной сети подтверждаются и обе стороны проводят аутентификацию, т.е. отправитель отправляет документ только уполномоченному получателю, и наоборот, получатель принимает документ только от уполномоченного отправителя.

Аутентификация пользователя осуществляется с помощью электронной пластиковой карточки, где хранится ключевая информация, дополнительно для обеспечения безопасности, при каждом новом сеансе связи из пульта управления АКЗ вводится PIN-код данного пользователя.

Структура аппаратуры криптографической защиты информации, передаваемой факс-аппаратом

Блок преобразования информации и интерфейсов с блоком электропитания и комплектом соединительных кабелей представляет собой аппаратно-программную платформу (АПП) АКЗ, которая является универсальной частью и позволяет построить на ее основе специализированную аппаратуру криптографической защиты данных при передаче факсимильной информации. Структурная схема АКЗ представлена на рисунке 1.

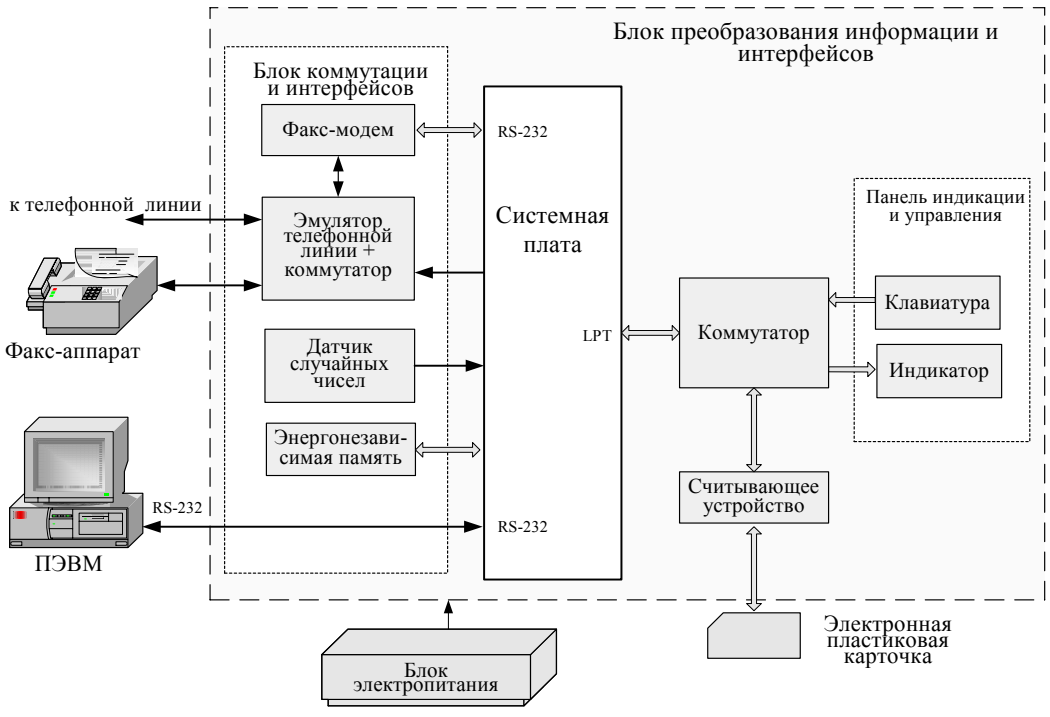

Рисунок 1 – Структурная схема АКЗ

Вид исполнения конструкции АКЗ – настольный. АКЗ представляет собой двухблочную конструкцию (блок преобразования информации и интерфейсов и блок электропитания). Блок преобразования информации и

интерфейсов выполняет все функции по назначению, блок электропитания обеспечивает электропитание аппаратуры.

Блок преобразования информации и интерфейсов состоит из следующих компонентов:

– блок коммутации и интерфейсов, предназначенный для коммутации факс-модема с телефонной линией, факс-аппаратом и ПЭВМ, считывающим устройством для ЭПК. Кроме этого, в состав блока коммутации и интерфейсов входят датчик случайной последовательности (ДСП) и энергонезависимая память. ДСП генерирует сеансовые ключи шифрования. Энергонезависимая память используется для хранения шифрованной факсимильной информации;

– системная плата. В качестве системной платы используется плата ICOP6015 (фирма "ICOP Technology Inc.", Тайвань), на которой установлен микроконтроллер M6117D, энергонезависимое оперативное запоминающее устройство (ОЗУ) – 4 Мбайт, ОЗУ – 4 Мбайт, два последовательных порта RS-232;

– панель индикации и управления, предназначенная для интерфейса с пользователем и отображения информации о состоянии АКЗ. Панель индикации и управления имеет удобный интерфейс и надписи на русском языке;

– считывающее устройство для ЭПК. Считывающее устройство предназначено для совместной работы с ЭПК КБ5004ВЕ1 (завод "Ангстрем", г. Зеленоград, Россия) по протоколу Т0.

При разработке специализированного встроенного микропрограммного обеспечения (ВМО) используется принцип разработки программного обеспечения для мультимикропроцессорной системы, приведенного в работе [4] с использованием алгоритмического языка Modula-2.

Основные задачи, выполняемые ВМО АКЗ:

- реализация алгоритмов криптографического преобразования в соответствии с ГОСТ 28147-89;
- реализация имитозащиты открытых данных;
- управление считыванием информации, поступающей с факс-аппарата;
- управление записью информации, принимаемой из телефонной сети в факс-аппарат;
- управление передачей/приемом информации по телефонной линии связи через модем;
- генерация сеансовых ключей с помощью физического датчика случайных чисел (ДСЧ);
- считывание ключа шифрования с электронной пластиковой карточки (ЭПК) КБ 5004 ВЕ1.

ВМО является составной частью АКЗ и не может быть использовано для самостоятельной работы.

В состав ВМО входят следующие модули:

- модуль начальной загрузки и управления;
- модуль закрытого режима;
- модуль коммуникации;
- модуль специального режима;
- модуль шифрования;
- модуль тестирования.

Структура ВМО АКЗ приведена на рисунке 2.

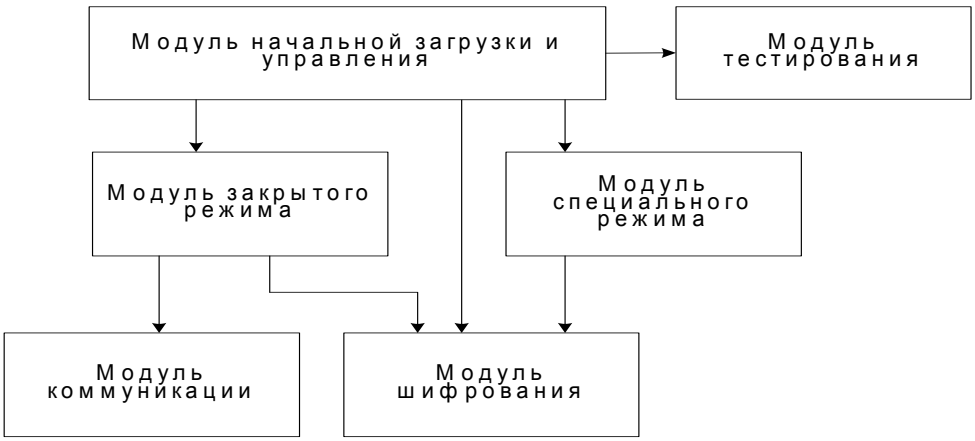

Рисунок 2 – Структура ВМО АКЗ

При разработке ВМО АКЗ применяются:

– алгоритм криптографического преобразования по ГОСТ 28147-89;
– протокол передачи данных, совместимый с Zmodem;
– алгоритм упаковки данных по методу LZH.

Функциональные возможности АКЗ

АКЗ предназначен для работы в следующих режимах:

а) открытый режим (без включения функций защиты информации), рисунок 3;

б) закрытый режим:

1) со стандартным факс-аппаратом по телефонным каналам связи, рисунок 3;
2) с ПЭВМ (Windows 2000, факс-модем) по телефонным каналам связи, рисунок 4;
3) со стандартным факс-аппаратом через почтовые сообщения с помощью ПЭВМ (Windows 2000, ПО Outlook, модем) по Интернет-каналам (с помощью услуг Интернет-провайдера), рисунок 5;
4) с ПЭВМ (Windows 2000, факс-модем) через почтовые сообщения с помощью ПЭВМ (Windows 2000, ПО Outlook, модем) по Интернет-каналам (с помощью услуг Интернет-провайдера) (см. рисунок 6);

в) тестовый.

АКЗ также обеспечивает специальный режим, который предназначен для смены мастер-ключа, паролей пользователя и администратора, обновления адресной книги, факсимильной программы, протокола передачи Zmodem, программы архиватора, программы тестового режима (см. рисунок 7).

АКЗ может функционировать при пяти различных схемах подключения, в зависимости от возможностей и желания потребителя. Структурные схемы подключения АКЗ приведены на рисунках 3-7.

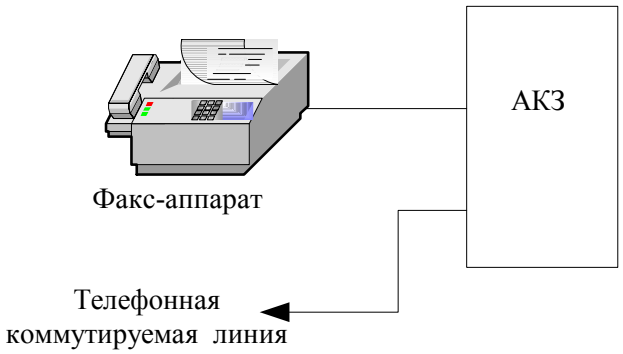

Рисунок 3 – Структурная схема подключения АКЗ
со стандартным факс-аппаратом

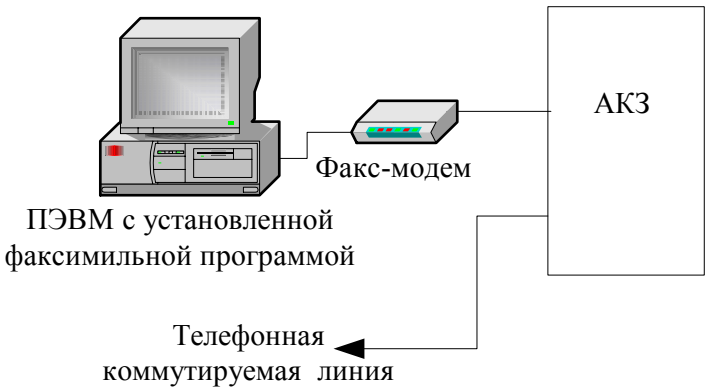

Рисунок 4 – Структурная схема подключения АКЗ
с факс-модемом под управлением ПЭВМ

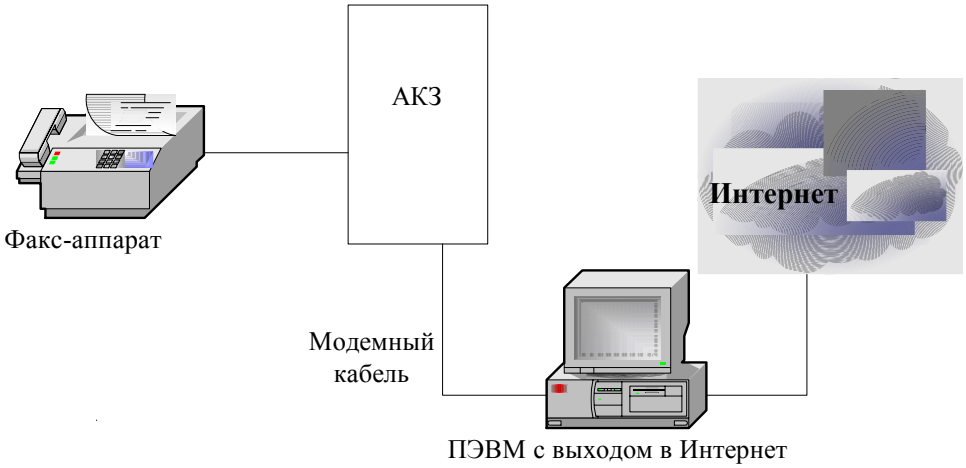

Рисунок 5 – Структурная схема подключения АКЗ со
стандартным факс-аппаратом и ПЭВМ

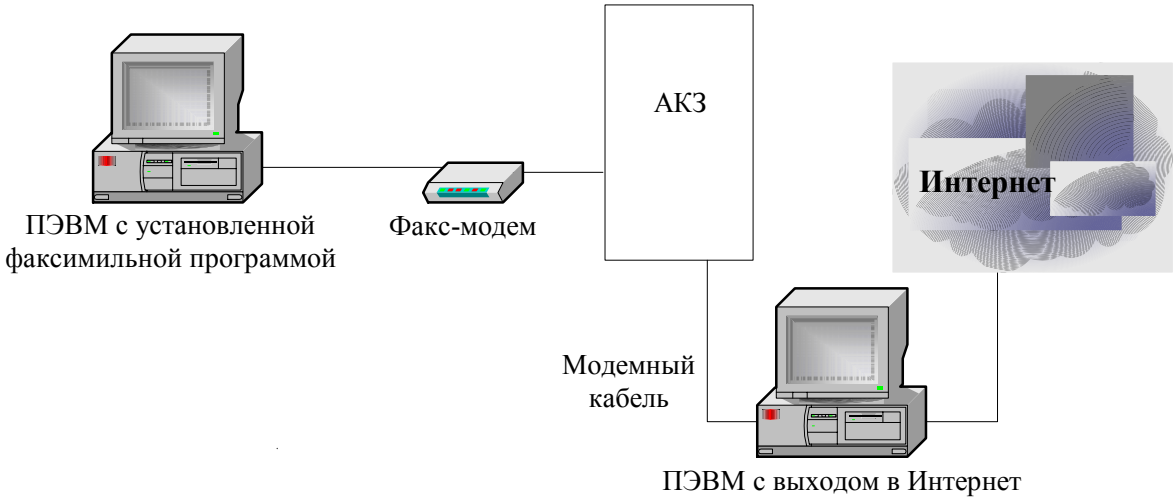

Рисунок 6 – Структурная схема подключения АКЗ с
факс-модемом под управлением ПЭВМ и ПЭВМ

Рисунок 7 – Структурная схема подключения АКЗ к ПЭВМ

Заключение

Принципиальным важным стратегическим решением является представление АКЗ как посредника (прокси-сервера) в узлах виртуальной факсимильной сети. Данный подход к организации защиты факсимильной информации позволил:

- разделить во времени прием/передачу защищаемой факсимильной копии документа с факс-аппарата, шифрование и собственно доставку в узел назначения виртуальной факсимильной сети, поэтому ключи, данные, программные модули размещаются в открытом виде в памяти АКЗ строго конкретное контролируемое время и гарантированно уничтожаются после использования или аппаратного сбоя;
- использовать для доставки зашифрованной факсимильной копии документа, как устройство модем (согласно стандарту МККТТ V.90), так и любое другое альтернативное устройство, что позволяет увеличить пропускную способность телефонной сети, а в случае отказа телефонной сети доставить зашифрованную факсимильную копию документа любым другим способом (например, через Internet или с помощью дискеты);
- обеспечить высокое качество факсимильной копии документа независимо от помех на телефонной линии (фактически максимально возможное качество для используемого факс-аппарата);
- обеспечить широкий набор сервисных функций и адаптацию коммуникационных модулей АКЗ под конкретные условия применения изделия.

Опытная эксплуатация АКЗ проводилась с тональным набором номера на внутренней офисной АТС предприятия, с импульсным набором номера на двух различных АТС одного населенного пункта и междугородней телефонной сети, показала устойчивость работы АКЗ в основных режимах. В настоящий момент проводятся работы по подготовке к серийному производству АКЗ.

Литература

1. Томина Г.Д., Киркоров С.И. Подход к организации активной защиты информационных систем. Ж-л Управление защитой информации, т. 5, № 2, Минск, 2001. С. 179.
2. Зегжда Д.П., Ивашко А.М. Технология создания безопасных систем обработки информации на основе защищенной ОС. Ж-л Проблемы информационной безопасности. Компьютерные системы, №2, 1999.
3. Вензель Е.Ф., Злотник Е.М., Киркоров С.И. Синтез адаптивного монитора графической подсистемы автоматизированного рабочего места проектировщика. Ж-л Весці Акадэміі Навук БССР, серыя фізіка-тэхнічных навук, №4, Мінск, 1987.
4. Киркоров С.И. Метод разработки программного обеспечения для мультимикропроцессорной системы. Препринт №34, Институт технической кибернетики АН БССР, Минск 1987.
5. Киркоров С.И. Монитор терминальной микропроцессорной системы. Научно-технический сборник. Программно-технические средства САПР. Минск, 1986. С. 75-81.
6. Анищенко В.В., Винокурова О.Ф., Киркоров С.И. Организация межпроцессорного взаимодействия в мультимикропроцессорной системе. Научно-технический сборник. Автоматизация проектирования микропроцессорных устройств. Минск, 1986. С. 47-53.
7. Семенков О.И., Анищенко В.В., Горобченко А.А., Злотник Е.М., Киркоров С.И., Винокурова О.Ф., Фатеева Н.Е., Рутковский Е.И. Микропроцессорная графическая станция ГТ-80. Ж-л Микропроцессорные средства и системы, №4, М. 1987. С. 54-56.