6. *Винокуров А.* «ГОСТ не прост, а очень прост». -М.: «Монитор », 1995, -№1, с. 60-73.

7. *Абель Питер.* Язык ассемблера для IBM PC и программирования. -М.: Высшая школа, 1992. - 192 с.

8. *Мешков А.В., Тихомиров Ю.В.* Visual C++ и MFC. -СПб.: БХВ-Петербург, 2003. –1040 с.

9. *RSA* Laboratories' Frequently Asked Questions About Today's Cryptography, v4.0

10. http://www.ancud.ru/catalog/crypton.htm (Устройства криптографической защиты данных (УКЗД) серии КРИПТОН.)

Поступила 19.04.2006

УДК 004.31 **Журавель Т.Н.**

ИСПОЛЬЗОВАНИЕ АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ ВОССТАНОВЛЕНИЯ ПРОТОКОЛОВ СВЯЗИ ЦИФРОВЫХ ТЕЛЕФОННЫХ АППАРАТОВ ДЛЯ ЗАЩИТЫ ТЕЛЕФОННЫХ ЛИНИЙ

Защита информации в телефонных линиях связи является неотъемлемой частью комплексной защиты объекта информационной деятельности.

Актуальность проблемы съема информации с использованием телефонных линий (ТЛ) ни у кого в наше время не вызывает сомнений. Как правило, ни один объект информационной деятельности (ОИД), в том числе тот, на котором циркулирует информация с ограниченным доступом (ИсОД), не обходится без ТЛ. В настоящее время широкое распространение получили цифровые автоматические телефонные станции (ЦАТС) импортного производства, которые полностью удовлетворяют потребность в комфортности и качестве связи как крупных учреждений и ведомств, так и более мелких организаций.

Проведя сравнительный анализ существующих методов и средств съема информации с ТЛ, можно считать цифровую телефонную связь более надежной, но ввиду некоторых особенностей и реализуемых функций существуют и недостатки.

Основным недостатком можно считать возможность дистанционного контроля акустической обстановки в помещении с использованием цифрового телефонного аппарата (ЦТА). Данная функция ЦТА может быть как заявленной производителем, так и принудительной (в случае несанкционированного прослушивания). Штатные режимы ЦАТС, реализующие удаленное прослушивание, сопровождаются звуковыми либо визуальными (на дисплее ЦТА) сигналами, каких-либо реальных гарантий относительно нештатных (или необъявленных) режимов ЦАТС импортного производства не существует.

Таким образом, четко прослеживается необходимость применения средств технической защиты информации. В данном случае к таким средствам выдвигаются следующие требования:

- блокирование возможности дистанционного контроля акустической обстановки в помещении, то есть гарантированная передача речевой информации от ЦТА к ЦАТС только в штатном режиме разговора;
- исключение возможности утечки преобразованной речевой информации через вспомогательные цифровые каналы ЦТА во всех режимах работы ЦТА;
- сохранение комфортности и качества выполнения основных заявленных производителем функций.

Проанализировав возможные пути реализации таких тренований, можно прийти к выводу, что существует необходимость вмешательства со стороны средств технической защиты в цифровые сигналы обмена между ЦАТС и ЦТА. Необходимо в то же время

заметить, что это невозможно без достоверных сведений о структуре сигналов обмена, в том числе о конкретных протоколах команд канала D. Эти данные производителями ЦАТС, как правило, не предоставляются либо предоставляются в очень ограниченном объеме.

Предварительное изучение ЦАТС импортного производства, наиболее часто эксплуатирующихся в качестве учрежденческих телефонных станций, позволяет сделать следующие выводы:

- так как линии связи ЦАТС не являются элементами сети общего доступа, то они, как правило, не полностью соответствуют либо вообще не соответствуют стандартам (речь идет о рекомендациях CCITT G.703 и CCITT I.430);
- как правило, используются ЦТА с двунаправленным 2-проводным интерфейсом (U-стык);
- основным форматом организации пакетов является 2B+D, но конкретная реализация пакетов каналов B и D различается у разных производителей;
- в интерфейсах обмена данными между ЦАТС и ЦТА определены три уровня:
  - уровень физический, определяющий физические параметры сигнала (напряжение, основная тактовая частота и т. д.);
  - уровень канала данных, определяющий расстановку бит в информационном потоке, преобразования для повышения надежности связи и т.д.;
  - уровень управления, определяющий коды команд для управления.

Для решения задачи объективного восстановления структуры сигналов обмена между ЦТА и ЦАТС (в том числе команд сигнализации), независимо от типа ЦАТС и производителя аппаратуры, был реализован аппаратно-программный комплекс, функциональная схема которого представлена на рис.1.

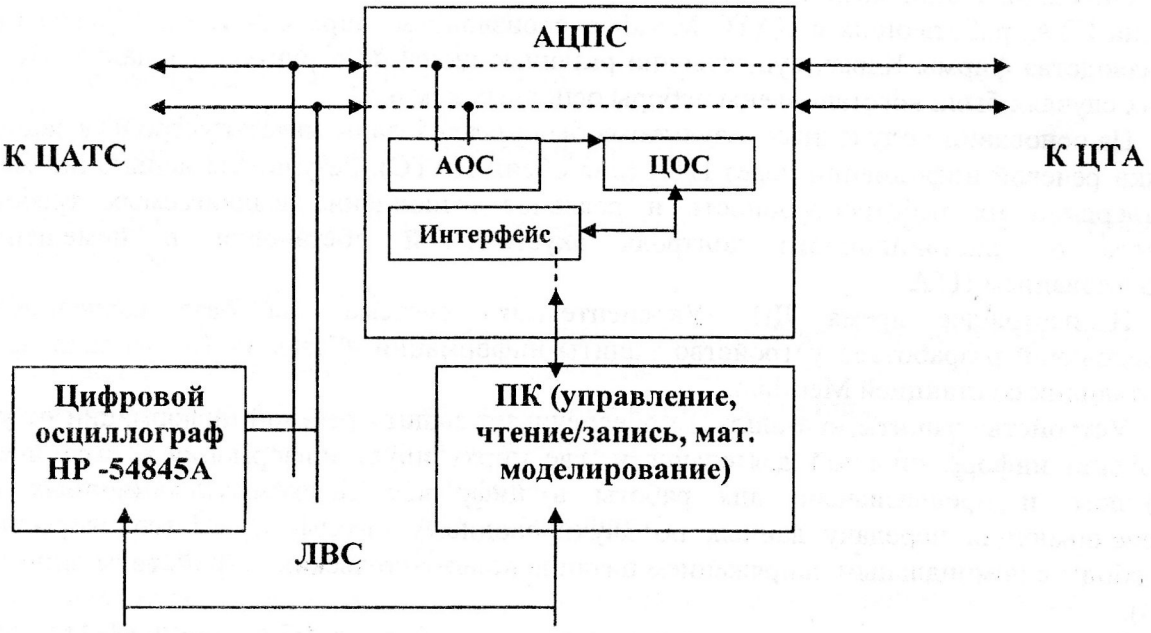

Рис. 1

В состав комплекса входит специализированный блок аналого-цифрового процессора сигналов (АЦПС), управляемый от персонального компьютера (ПК) и включенный в разрыв анализируемой телефонной линии; цифровой запоминающий осциллограф, объединенный локальной вычислительной сетью (ЛВС) с ПК; программное обеспечение для математического моделирования.

АЦПС включает в себя:

- узел аналоговой обработки сигналов (АОС) ЦАЛ, обеспечивающий преобразование сигналов ЦАЛ в цифровые сигналы для узла цифровой обработки сигналов (ЦОС);
- узел ЦОС, обеспечивающий выделение каналов B1, B2 и D для обоих направлений в соответствии с управляющими сигналами ПК;

- интерфейс RS-232, обеспечивающий сопряжение АЦПС с ПК, в том числе прием управляющих сигналов от ПК и запись цифровых потоков каналов B и D в ПК.

Цифровой запоминающий осциллограф обеспечивает формирование первичных выборок аналогового сигнала на ЦАЛ, их запоминание и передачу в ПК для анализа.

ПК предназначен для анализа сигналов от осциллографа и АЦПС, формирования управляющих сигналов для АЦПС и документирования результатов исследований.

Использовался следующий алгоритм исследований сигналов ЦАЛ:

- производилась запись первичных выборок аналоговых сигналов ЦАЛ с помощью запоминающего цифрового осциллографа (использовались режимы внесения разных затуханий от ЦТА и ЦАТС для надежного разделения направлений передачи сигналов по амплитуде);
- проводился анализ первичных выборок аналоговых сигналов на ПК. При этом определялись параметры линейного кодирования, определялись структура пакетирования и количественные параметры пакетирования для каналов B1, B2 и D обоих направлений, определялось наличие скремблирования в каналах B. Анализ с использованием методов и программ математического моделирования (на основании доступных данных об элементной базе микросхем контроллеров U-интерфейса ЦАТС и ЦТА);
- результаты анализа (структура пакетов передачи данных) передавались в АЦПС и использовались для восстановления потоков цифровых данных в каналах B1, B2 и D обоих направлений;
- восстановленные потоки цифровых данных для различных режимов работы ЦАТС и ЦТА записывались в ПК и анализировались с использованием методов и программ математического моделирования.

Описанный аппаратно-программный комплекс был применен для анализа сигналов обмена ЦТА, работающих с ЦАТС Meridian производства фирмы Nortel и Midistar Flash 8 производства фирмы Kapsh, существенно различающихся по структуре сигналов обмена. В обоих случаях были восстановлены наборы основных команд.

На основании полученных результатов были реализованы макеты устройств защиты от утечки речевой информации через ЦТА (для обеих ЦАТС). Результаты испытаний макетов подтвердили их работоспособность и реальное выполнение выдвигаемых требований защиты от дистанционного контроля акустической обстановки в помещении с использованием ЦТА.

В настоящее время ДП «Укрспецтехника система» на базе вышеописанных исследований разработало устройство защиты информации «Базальт-31» для защиты ЦТА, работающих со станцией Meridian.

Устройство защиты «Базальт-31» обеспечивает защиту речевой информации от утечки с объекта информационной деятельности, где циркулирует информация с ограниченным доступом, и предназначено для работы в цифровых телекоммуникационных сетях, обеспечивающих передачу данных по двухпроводному интерфейсу U (со скоростью до 512 кбод/с с номинальным напряжением питания пользовательских устройств от линии связи 24 В).

Разработанное устройство предназначено для работы с ЦТА серий M31**, M38**, M39** и других, совместимых с ЦАТС типа «Меридиан».

Реализованная структура изделия «Базальт-31» позволяет применять его для защиты ЦТА разных ЦАТС без аппаратных изменений, путем наращивания программной составляющей изделия и использования предусмотренного многопозиционного переключателя.

Функциональная схема устройства представляет собой совокупность блока питания, блоков цифровой и аналоговой обработки сигналов, формирователей входных и выходных сигналов и блока автоматического управления порогами.

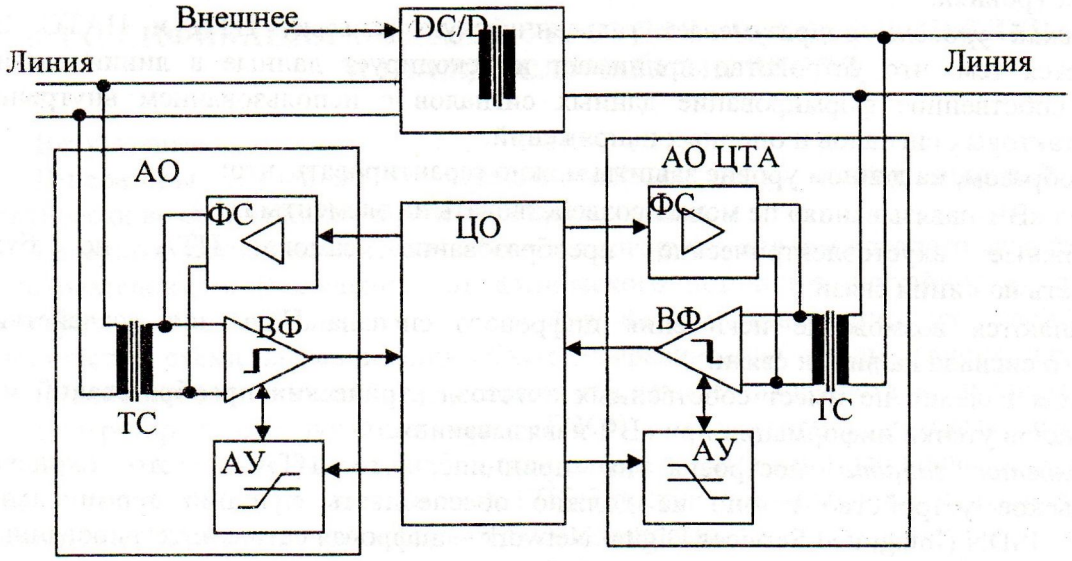

Рис. 2

Условные обозначения:
DC/DC – блок питания с гальванической развязкой;
ЦОС – блок цифровой обработки сигналов;
АО ЦАТС – блок аналоговой обработки сигналов ЦАТС;
АО ЦТА – блок аналоговой обработки сигналов ЦТА;
ТС – сигнальный трансформатор;
ФС – формирователь выходных сигналов;
ВФ – входной формирователь сигналов;
АУП – блок автоматического управления порогами.

Назначение основных узлов функциональной схемы можно охарактеризовать следующим образом:

блок питания обеспечивает:

- выработку гальванически изолированных от линий внешнего источника питания и ЦАТС питающих напряжений для ЦТА и устройства защиты;
- автоматическое переключение на внешний источник питания;
- контроль нагрузочной способности линии ЦАТС;
- индикацию режимов электропитания;

блок цифровой обработки сигналов обеспечивает:

- анализ данных от ЦАТС и ЦТА;
- принятие решений о необходимости внесения изменений в данные и о недопустимых режимах передачи данных;
- внесение необходимых изменений в принятые данные;
- индикацию режимов обмена данными.

Функционально идентичные блоки АО ЦАТС и АО ЦТА обеспечивают согласование ЦОС с линиями связи с ЦАТС и ЦТА. Сигнальные трансформаторы обеспечивают гальваническую развязку устройства от линий связи. Входные формирователи совместно с блоком автоматического управления порогами обеспечивают усиление входных сигналов и преобразование их в логические уровни для ЦОС. Формирователи выходных сигналов обеспечивают необходимое усиление сигналов для передачи в линию связи.

Метод подключения и конструктивные особенности данного устройства не требуют внесения изменений в ЦАТС и ЦТА.

Функции защиты, выполняемые устройством, можно разделить на физическом и программном уровнях.

Физический уровень подразумевает гальваническую развязку ЦТА и ЦАТС. Это сопровождается тем, что устройство принимает и декодирует данные в линии связи и производит собственное формирование данных сигналов с использованием внутренних источников тактовых сигналов и опорных напряжений.

Таким образом, на данном уровне защиты можно гарантировать, что:

- сигнал «ВЧ-навязывания» не может воздействовать на элементы ЦТА;
- возможные акустоэлектрические преобразования самого ЦТА не будут присутствовать на линии связи;
- устраняются возможные искажения цифрового сигнала ЦТА под воздействием акустического сигнала на линии связи.

При этом изделие не имеет собственных акустоэлектрических преобразований и не образует каналов утечки информации при «ВЧ-навязывании».

Программная защита построена на принципе, что ЦТА – это оконечное пользовательское устройство и оно не должно обеспечивать функций терминального адаптера сети ISDN (Integrated Services Digital Network – цифровая сеть с интегрированными услугами) во избежание подключения к линии S/T сети несанкционированных устройств.

Это обеспечивается следующим образом:

- устройство защиты во всех режимах работы заменяет данные в канале B2 при передаче от ЦТА к ЦАТС на данные, которые генерируются в самом устройстве;
- устройство защиты контролирует объем передаваемых данных в канале сигнализации D от ЦТА к ЦАТС и, при превышении объема 100 бит за секунду, блокирует на 10 с обмен всеми данными между ЦТА и ЦАТС с индикацией возникновения нештатной ситуации.

Анализ канала сигнализации D от ЦТА к ЦАТС устройством производится независимо от режима работы. При появлении признака поднятия микротелефонной трубки на ЦТА подмена канала B1 прекращается (с индикацией незащищенности канала B1) и данные от ЦТА проходят на ЦАТС, обеспечивая возможность разговора абонентов. При появлении в канале D признака опускания микротелефонной трубки на ЦТА подмена канала B1 возобновляется. Изделие не реагирует на команды управления от ЦАТС и, следовательно, нейтрализует попытки удаленного воздействия на ЦТА, которые могут привести к утечке информации из защищаемого помещения (например, включение ЦТА в режиме «контроль помещения»).

В перспективе, благодаря гибкой программной архитектуре устройства защиты, возможно расширение функций для работы с ЦАТС и ЦТА других производителей.

Поступила 02.02.2006
После доработки 14.06.2006