ПРИОРИТЕТНЫЙ НАЦИОНАЛЬНЫЙ ПРОЕКТ «ОБРАЗОВАНИЕ»
РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Ю.Н. ЖИГУЛЕВЦЕВ

МЕТОДЫ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Учебное пособие

Москва
2008

Предисловие

Подготовку специалистов в области защиты информации ведут многие вузы, а также достаточно многочисленные центры повышения квалификации. Направ-ленность большинства программ подготовки состоит в освоении имеющегося арсенала средств защиты и методов их применения. Проблемы разработки новых методов и средств, а также повышения эффективности имеющихся с учётом со-временных возможностей их реализации представлены в существенно меньших объёмах.

Предлагаемое учебное пособие направлено на подготовку специалистов, способных решать названные проблемы. Его особенностью является расширенное знакомство с методами обработки речевых сигналов, а также современными возможностями их реализации. При этом не исключается изучение традиционных для подобных курсов разделов.

Подразумевается, что изучающие дисциплину обладают знаниями в объёме университетского курса высшей математики, а также в области аналоговой и циф-ровой схемотехники, микропроцессорной техники и цифровой обработки сигналов.

Ограниченность объёма учебного пособия не позволяет полностью рас-крыть все детали рассматриваемых проблем, поэтому рекомендуется пользоваться приведёнными ссылками на основную и дополнительную литературу. Большинство указанных источников могут быть получены в электронном виде.

Рекомендуется также пользоваться ресурсами Интернета, соответствующие ссылки приводятся в тексте, их также можно получить по запросу "Защита рече-вой информации" в поисковых системах. Подробные описания технических средств, названия которых упоминаются в пособии, легко найти в Интернете, подставив соответствующее название в поле запроса поисковой системы.

Жигулёвцев Юрий Николаевич - кандидат технических наук, доцент кафедры «Системы автоматического управления» МГТУ им. Н.Э. Баумана.

Введение

Информация играет важную роль во всех сферах функционирования современного общества, в этом её ценность, а ценности приходится защищать от недоброжелателей.

Слово информация происходит от латинского **informatio** - разъяснение, научение, изложение, оповещение. Понятие информации имеет много граней,

определение этого понятия можно давать в философском, математическом, социокультурном, техническом и прочих аспектах. В XX веке

слово "информация" стало термином во множестве научных областей, получив особые для них определения и толкования.

В общенаучном плане с понятием **информация** связаны прежде всего **сведения, факты, явления,** отражающиеся в состояниях либо параметрах любых природных объектов либо процессов,

выступающих в качестве материальных **носителей информации.** Существование информации связано также с **передачей** сведений от одного субъекта (произвольной природы) к другому.

Информационная безопасность может рассматриваться в широком смысле как часть процесса информатизации общества и становления информационной цивилизации.

В прикладном плане информационную безопасность можно рассматривать как совокупность свойств информации, связанных с обеспечением запрещения неавторизованного доступа

(получения, ознакомления с содержанием, передачи, хранения и обработки), модификации или уничтожения, а также любых других несанкционированных действий с личной,

конфиденциальной или секретной информацией, представленной в любом физическом виде [14]. Проблема обеспечения информационной безопасности - другими словами,

защиты информации - является комплексной задачей, включающей правовые, организационные и технические аспекты. Эффективная безопасность может быть реализована лишь в комплексе мер,

учитывающих все эти аспекты [11].

Речевая информация как реализация речевой коммуникативной функции человека является одним из наиболее употребительных средств оперативного обмена информацией.

Речевое общение реализуется как непосредственно при личных встречах между людьми, так и с использованием различных каналов связи - радио,

телефонных (проводных, мобильных), компьютерных (IP-телефония) и пр. Защита речевой информации наряду с другими видами информации является составной частью комплексной безопасности

организации.

При анализе проблемы комплексной безопасности важно учитывать все факторы, угрожающие безопасности, поэтому необходимо иметь по возможности полную и в то же время

обозримую классификацию возможных угроз. Такая клас-сификация основана на нескольких критериях:

- характер угрозы (разглашение, утечка, несанкционированный доступ);
- вид носителя информации (акустическая среда, каналы связи, машинные носители и т.д.);
- способ физического доступа (непосредственный, за счёт побочных излуче-ний, путём физических воздействий).

Исходя из анализа угроз и степени ценности информации разрабатывается комплекс мер по защите информации, включающий организационные и технические мероприятия.

К этим мерам относятся разграничение доступа, контроль и наблюдение, различные способы пассивной и активной защиты.

Для защиты речевой информации помимо мер противодействия несанкцио-нированному доступу эффективно применение шифрования при передаче кодированной речевой информации

по цифровым каналам связи. В связи с этим повышается роль речевых технологий - методов и средств обработки речевых сигналов, предназначенных для реализации речевого взаимодействия

человека с другими людьми, а также техническими системами. Применение современных речевых технологий для защиты речевой информации позволяет существенно повысить эффективность

этой защиты.

1. Правовые вопросы защиты речевой информации

Правовая защита информации - это комплекс международных и национальных государственных и ведомственных законодательных актов, правил, процедур и мероприятий, обеспечивающих защиту информации на правовой основе. Государственными актами являются Конституция Российской Федерации, законы Российской Федерации, гражданское, административное, уголовное право, изложенные в соответствующих кодексах. Ведомственные нормативные акты издаются в форме приказов, руководств, положений и инструкций, издаваемых ведомствами, организациями и предприятиями, действующими в рамках соответствующих структур.

К числу основных государственных нормативных актов в области информационной безопасности относятся следующие:

- Доктрина информационной безопасности Российской Федерации [27];
- Закон Российской Федерации "О безопасности" [28];
- Федеральный закон "Об информации, информационных технологиях и о защите информации" [29];
- Закон Российской Федерации "О государственной тайне" с дополнениями и изменениями [30].

Вопросы правового режима информации с ограниченным доступом реализуются в двух самостоятельных законах о государственной и коммерческой тайнах. Кроме того, этот аспект раскрывается и в Гражданском кодексе РФ статьей 139 "Служебная и коммерческая тайна". Указ Президента РФ "Об утверждении перечня сведений конфиденциального характера" от 6 марта 1997 г. № 188 [31] определяет понятие и содержание конфиденциальной информации.

Таким образом, правовая защита информации обеспечивается нормативно-законодательными актами, представляющими собой иерархическую систему от Конституции РФ до функциональных обязанностей и контракта отдельного конкретного исполнителя, определяющих перечень сведений, подлежащих охране, и меры ответственности за их разглашение.

Реализация мер по защите информации на государственном уровне возложена на следующие структуры:

- межведомственную комиссию по защите государственной тайны;
- федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности;
- федеральный орган исполнительной власти, уполномоченный в области обороны;
- федеральный орган исполнительной власти, уполномоченный в области внешней разведки;
- федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации;
- соответствующие территориальные органы

В настоящее время эти органы представлены следующими структурами:

- Службой специальной связи и информации Федеральной службы охраны Российской Федерации (Спецсвязь ФСО России);
- Федеральной службой безопасности;
- Министерством обороны РФ;
- Службой внешней разведки;
- Федеральной службой по техническому и экспортному контролю.

Распределение обязанностей этих структур связано с организацией системы мер по лицензированию деятельности в области информационной безопасности, сертификации

защищённых технических средств и аттестации защищаемых объектов. Любая организация для ведения деятельности в области защиты информации обязана иметь соответствующую лицензию, исполнители работ обязаны пользоваться только сертифицированными техническими средствами.

Лицензирование - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением действия лицензий в случае административного приостановления деятельности лицензиатов за нарушение лицензионных требований и условий, возобновлением или прекращением действия лицензий, аннулированием лицензий, контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий, ведением реестров лицензий, а также с предоставлением в установленном порядке заинтересованным лицам сведений из реестров лицензий и иной информации о лицензировании

Сертификация - это деятельность по подтверждению соответствия продукции установленным требованиям. Постановлением Правительства РФ "О сертификации средств защиты информации" [32] определены системы сертификации, которые создаются ФСТЭК, Спецсвязью, ФСБ, СВР и Минобороны РФ. Положение устанавливает основные принципы, организационную структуру системы обязательной сертификации средств защиты информации, порядок проведения сертификации этих средств по требованиям безопасности информации, а также государственного контроля и надзора за сертификацией и сертифицированными средствами защиты информации. Действие этого Положения распространяется на технические, программные и другие средства защиты информации, предназначен-ные для защиты информации, содержащей сведения, составляющие государственную тайну, от утечки, несанкционированных и непреднамеренных воздействий, несанкционированного доступа и от технической разведки, а также средства контроля эффективности защиты информации.

Система сертификации средств защиты информации по требованиям безопасности информации включает в себя **аттестацию** объектов информатизации по требованиям безопасности информации. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации, правила проведения, а также другие вопросы аттестации определяются "Положением по аттестации объектов информатизации по требованиям безопасности информации", утвержденным председателем Государственной технической комиссии при Президенте РФ (ныне ФСТЭК) 25 ноября 1994г. Деятельность системы сертификации средств защиты информации по требованиям безопасности информации организует ФСТЭК.

2. Организационные вопросы защиты речевой информации

Организационная защита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативноправовой основе,

исключающая или ослабляющая нанесение какого либо ущерба исполнителям [15]. Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации,

так как возможности несанкционированного использования секретных и конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами,

а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Полностью влияния этих аспектов невозможно избежать с помощью технических средств.

Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий,

которые исключали бы (или по крайней мере сводили бы к минимуму) возможность возникновения опасности информации. К основным организационным мероприятиям можно отнести:

- организацию режима и охраны с целью исключения возможности тайного проникновения на территорию и в помещения посторонних лиц;
- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками,

обучение правилам работы с закрытой информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

- организацию работ по анализу внутренних и внешних угроз информации и выработке мер по обеспечению ее защиты.

Защитные действия, ориентированные на обеспечение информационной безопасности, могут быть охарактеризованы целым рядом параметров, отражаю-щих, помимо направлений, ориентацию на объекты защиты, характер угроз, спо-собы действий, их распространенность, охват и масштабность [15].

Так, по характеру угроз защитные действия ориентированы на защиту информации от разглашения, утечки и несанкционированного доступа.

По способам действий их можно подразделить на предупреждение, выявление, обнаружение, пресечение.

По охвату защитные действия могут быть ориентированы на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры.

Масштабность защитных мероприятий характеризуется как объектовая, групповая или индивидуальная защита.

Уровень организационных мероприятий зависит от категории секретности защищаемой информации. К государственной тайне относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Эти сведения характеризуются по возрастанию степени важности как сек-ретные, совершенно секретные и особой важности. Кроме государственных сек-ретов, существуют другие виды защищаемой информации: различают служебную, коммерческую, личную тайну, которые можно отнести к разряду конфиденциаль-ной информации. Обоснованный выбор требуемого уровня защиты информации является важной задачей, поскольку как занижение, так и завышение уровня неиз-бежно ведет к потерям.

Организационные мероприятия должны четко планироваться, направляться и осуществляться организационной структурой, укомплектованной соответствующими специалистами по безопасности производственной деятельности и за-щите информации. Таким структурным подразделением обычно является служба безопасности организации, предприятия.

3. Методы и средства защиты речевой информации

3.1. Акустические характеристики среды

Анализ защищённости помещений от утечки речевой информации требует учитывать характер распространения

акустических волн в воздухе и твердых телах, процессы на границе двух сред с различными плотностями.

Распространение звуковых волн связано с отражением, поглощением, интерференцией и дифракцией. Свойства преград на пути звуковых волн характеризуются коэффициентами отражения и поглощения, зависящими от частоты звука. Интерференция и отражение приводят к возникновению стоячих волн с узлами и пучностями. Вследствие многократного отражения интенсивность звука падает, этот процесс называет-ся реверберацией. Реверберация зависит от характеристик помещений - формы, объёмов, коэффициентов поглощения, наличия связей с соседними помещениями и т.д. [4, 7, 8].

Звуковые волны могут проникать через препятствия вследствие дифракции; через сквозные поры, щели; через материал перегородок в виде продольных колебаний его частиц; через поперечные колебания перегородок. Знание акустики защищаемых помещений позволяет выявить возможные каналы утечки речевой информации.

3.2. Каналы утечки речевой информации

В рамках курса основное внимание уделяется техническим каналам утечки речевой информации. Их классификация основывается на характере среды распространения и физических эффектах, сопровождающих передачу речевой информации, а также способах съёма и передачи перехватываемой информации.

Акустический канал образуется за счёт непосредственного преобразования акустических речевых сигналов, например, в электрические сигналы с помощью закладных устройств и передачи их по специально организованным каналам связи за пределы выделенных помещений либо записи на диктофон с последующей выемкой закладки.

Виброакустический канал возникает при передаче речевых колебаний через конструкции сооружений. В этом случае для съёма информации применяются воспринимающие вибрации виброакустические преобразователи, также передающие вырабатываемые сигналы по каналам связи. Съём вибраций может осуществляться как контактным способом (стетоскопы, вибропреобразователи-акселерометры), так и бесконтактным, за счёт облучения колеблющихся конструкций, например, лазерным излучением и последующим приёмом и обработкой отражённых сигналов.

Электроакустические каналы утечки речевой информации возникают за счёт преобразования акустических сигналов в электрические в элементах, предназначенных для выполнения совершенно других функций. Микрофонный эффект является одним из проявлений прямых акустоэлектрических преобразований, возникающие при этом сигналы могут быть считаны соответствующими усилительными устройствами. Другой путь получения подобной информации - модуляционные акустоэлектрические преобразования, возникающие вследствие облучения потенциально обладающих акустоэлектрическим эффектом элементов высокочас-

тотным электромагнитным излучением с последующим съёмом модулированных наводимых сигналов бесконтактным способом с помощью приёмников высокочастотных излучений.

При передаче речевой информации по **проводным коммуникациям** съём информации может осуществляться как путём непосредственного последовательного либо параллельного электрического подключения к линии связи, так и с помощью индукционных преобразователей.

Радиоканалы, используемые для передачи речевой информации, могут прослушиваться на частотах передачи.

Наибольшее разнообразие методов передачи и перехвата информации возникает в **цифровых** и **компьютерных каналах связи.**

3.3. Методы и средства обнаружения утечек речевой информации

Обнаружение утечек речевой информации обеспечивается комплексом организационных и технических мероприятий, включающих регулярное визуальное обследование, а также поиск утечек с применением пассивных и активных технических средств. Методы обнаружения утечки информации можно классифицировать по тем же признакам, что и каналы утечки по характеру среды распространения, типу физических полей и т.п.

3.3.1. Средства обнаружения радиозакладок

Для обнаружения радиозакладок в выделенных помещениях могут использоваться индикаторы электромагнитного поля, интерсепторы, радиочастотомеры, сканерные приемники, программно-аппаратные комплексы контроля и другие технические средства [6,7,8]

Индикаторы электромагнитного поля (индикаторы поля) позволяют обнаруживать излучающие закладные устройства, использующие для передачи ин-формации практически все виды сигналов, включая широкополосные шумопо-добные и сигналы с псевдослучайной скачкообразной перестройкой несущей частоты.

Принцип действия приборов основан на интегральном методе измерения уровня электромагнитного поля в точке их расположения. Наведенный в антенне и продектированный сигнал усиливается и в случае превышения им установленного порога срабатывает звуковая или световая сигнализация.

Интерсепторы. В результате дальнейшего развития индикаторов поля созданы широкополосные радиоприемные устройства - интерсепторы. Приборы ав-томатически настраиваются на частоту наиболее мощного радиосигнала (как пра-вило, уровень этого сигнала на 15 ... 20 дБ превышает все остальные) и осуществ-ляют его детектирование.

Например, интерсептор "R11" позволяет осуществлять прием и детектирование сигналов с частотной модуляцией (девиация частоты < 100 кГц) в диапазоне частот от 30 до 2000 МГц. Система преобразования частоты позволяет "просмат-ривать" весь диапазон менее чем за 1 сек. Чувствительность интерсептора выше чувствительности детекторных индикаторов поля и составляет порядка 100 мкВ (на частоте 500 МГц). Приемник имеет память LOCKOUT на 1000 частот, которые нужно исключить из рабочего диапазона (это, как правило, частоты сигналов ра-диовещательных и телевизионных станций). При приеме сигнала оператор может либо оставить его в рабочем диапазоне, либо удалить из процесса дальнейшего контроля. Хотя интерсептор не позволяет точно измерить частоту принимаемого сигнала, с помощью светодиодных индикаторов можно приблизительно устано-вить поддиапазон частот, в который он попадает.

Радиочастотомеры. Принцип "захвата" частоты радиосигнала с максимальным уровнем и последующим анализом его характеристик микропроцессо-ром положен в основу работы современных портативных радиочастотомеров. Микропроцессор производит запись сигнала во внутреннюю память, цифровую фильтрацию, проверку на стабильность и когерентность сигнала и измерение его частоты с точностью от единиц Гц до 10 кГц. Значение частоты в цифровой форме отображается на жидкокристаллическом экране. Кроме частоты сигнала многие радиочастотомеры позволяют определить его относительный уровень.

Наиболее совершенным из данного типа приборов является специальный приемник "Xplorer". Он позволяет производить автоматический или ручной за-хват радиосигнала в диапазоне частот от 30 до 2000 МГц и осуществлять его де-тектирование и прослушивание через динамик. Дисплей показывает частоту обна-руженного сигнала, его относительный уровень и вид модуляции, а также широту и долготу места расположения прибора в системе GPS. Приемник имеет функции блокировки (пропуска) до 1000 частот и записи в память до 500 частот с дополнительной информацией о дате и времени записи. Чувствительность приемника ми-нус 59 ... 25 дБ. Приемник имеет размеры 140 ? 70 ? 40 мм и вес - 250 г.

Существенно лучшую чувствительность имеют специальные (профессиональные) радиоприемники с автоматизированным сканированием радиодиапазона (**сканерные приемники** или **сканеры**). Они обеспечивают поиск в диапазоне час-тот, перекрывающем частоты почти всех применяемых радиозакладок - от десятков кГц до единиц ГГц. Лучшими возможностями по поиску радиозакладок обладают **анализаторы спектра.** Кроме перехвата излучений закладных устройств они позволяют анализировать и их характеристики, что немаловажно при обнару-жении радиозакладок, использующих для передачи информации сложные виды сигналов.

Возможность сопряжения сканирующих приемников с переносными компьютерами послужило основой для создания автоматизированных комплексов для поиска радиозакладок (так называемых **программно-аппаратных комплексов контроля**). Кроме программно-аппаратных комплексов, построенных на базе сканирующих приемников и переносных компьютеров, для поиска закладных уст-ройств используются и специально разработанные многофункциональные ком-плексы, например, "OSCOR-5000".

Специальные комплексы и аппаратура для контроля проводных линий позволяют проводить измерение параметров (напряжений, токов, сопротивлений и т.п.) телефонных, слаботочных линий и линий электропитания, а также выявлять в них сигналы закладных устройств.

3.3.2. Определители диктофонов.

Для обнаружения работающих в режиме записи диктофонов применяются так называемые **детекторы диктофонов.** Принцип действия приборов основан на обнаружении слабого магнитного поля, создаваемого генератором подмагничи-вания или работающим двигателем диктофона в режиме записи. Электродвижу-щая сила (ЭДС), наводимая этим полем в датчике сигналов (магнитной антенне), усиливается и выделяется из шума специальным блоком обработки сигналов. При превышении уровня принятого сигнала некоторого установленного порогового значения срабатывает световая или звуковая сигнализация. Во избежание ложных срабатываний порог обнаружения необходимо корректировать практически перед каждым сеансом работы, что является недостатком подобных приборов.

Детекторы диктофонов выпускаются в переносном и стационарном вариантах. К переносным относятся детекторы "Сова", RM-100, TRD-800, а к стационарным - PTRD-14, PTRD-16, PTRD-18 и т.д.

Из-за слабого уровня магнитного поля, создаваемого работающими диктофонами (особенно в экранированных корпусах), дальность их обнаружения детекторами незначительна. Например, дальность обнаружения диктофона L-400 в ре-жиме записи в условиях офиса даже при использовании стационарного детектора PTRD-018 не превышает 45 ... 65 см. Дальность обнаружения диктофонов в неэк-ранированных корпусах может составлять 1 ... 1,5 м.

Наряду со средствами обнаружения портативных диктофонов на практике эффективно используются и средства их подавления. Для этих целей используются устройства электромагнитного подавления типа "Рубеж", "Шумотрон", "Бу-ран", "УПД" и др. и устройства ультразвукового подавления типа "Завеса".

Принцип действия устройств электромагнитного подавления основан на генерации в дециметровом диапазоне частот (обычно в районе 900 МГц) мощных шумовых сигналов. В основном для подавления используются импульсные сигна-лы. Излучаемые направленными антеннами помеховые сигналы, воздействуя на элементы электронной схемы диктофона (в частности, усилитель низкой частоты и усилитель записи), вызывают в них наводки шумовых сигналов. Вследствие этого одновременно с информационным сигналом (речью) осуществляется запись и детектированного шумового сигнала, что приводит к значительному искажению первого.

Зона подавления диктофонов зависит от мощности излучения, его вида, а также от типа используемой антенны. Обычно зона подавления представляет собой сектор с углом от 30 до 80 град. и радиусом до 1,5 м (для диктофонов в экра-нированном корпусе).

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно около 20 кГц), воздействующие непосредственно на микрофоны диктофонов или акустических закладок, что яв-ляется их преимуществом. Данное ультразвуковое воздействие приводит к пере-грузке усилителя низкой частоты диктофона или акустической закладки (усили-тель начинает работать в нелинейном режиме) и тем самым - к значительным искажениям записываемых (передаваемых) сигналов.

В отличие от систем электромагнитного подавления подобные системы обеспечивают подавление в гораздо большем секторе. Например, комплекс "Завеса" при использовании двух ультразвуковых излучателей способен обеспечить по-давление диктофонов и акустических закладок в помещении объемом 27 м3. Од-нако системы ультразвукового подавления имеют один важный недостаток: эф-фективность их резко снижается, если микрофон диктофона или закладки прикрыть фильтром из специального материала или в усилителе низкой частоты уста-новить фильтр низких частот с граничной частотой 3,4 ... 4 кГц.

3.3.3. Комплексы и аппаратура для контроля проводных линий

Средства контроля проводных линий предназначены для выявления, идентификации и определения местоположения закладных устройств, подключаемых к проводным линиям, включая электросеть, телефонные кабели, линии селекторной связи, пожарной сигнализации и т.п. Они позволяют проводить измерение пара-метров (напряжений, токов, сопротивлений и т.п.) телефонных, слаботочных линий и линий электропитания, а также выявлять в них сигналы закладных устройств.

Работа таких средств контроля основана на следующих принципах:

- на измерении электрических параметров линии (амплитуд напряжения и тока в линии, а также значений емкости и индуктивности линии, активного и реактивного сопротивления);
- обнаружении в линии низкочастотного информационного (тестового) сигнала;
- обнаружении в линии сигнала высокочастотного навязывания;
- обнаружении в линии высокочастотного сигнала, модулированного низкочастотный информационным (тестовым) сигналом;
- обнаружении мест подключения средств съёма информации методом локации (в том числе и нелинейной) проводной линии.

Для измерения параметров линий могут использоваться как обычные, так и специально разработанные для этих целей измерительные устройства, имеющие в своем составе специальные адаптеры для подключения к линиям различного типа.

Для обнаружения в линии низкочастотных информационных (тестовых) сигналов используются специальные низкочастотные усилители, а для обнаружения высокочастотных сигналов - специальные приемники или детекторы.

Специально разработанные средства контроля проводных линий, как правило, совмещают в себе почти все функции этих устройств. Исключение составляют специальные средства контроля телефонных линий связи.

В качестве средств контроля проводных линий используются приборы: ТСМ-03, СРМ-700, ПСЧ-5, РТ-030 ("Scanner"), D-008, КТЛ-3, КТЛ-400, ПТУ-5В, "Багер-01" и др.

Для обнаружения подключений к линии средств съема информации и определения мест подключения используются локаторы проводных линий, принцип работы которых аналогичен принципам работы обычных радиолокаторов. Отли-чие состоит только в том, что зондирующий сигнал не излучается, а подается в линию. По измененным параметрам отраженного сигнала можно судить о характере гальванически подключаемого к линии закладного устройства. При исполь-зовании нелинейного локатора проводных линий отраженный сигнал принимается на частоте второй гармоники зондирующего сигнала, что позволяет минимизировать ложные обнаружения.

Наиболее широко применяются локаторы проводных линий "Визир" (нелинейный), "НЛПК", "Бор-1" и др.

3.3.4. Локаторы нелинейностей.

Большую группу образуют средства обнаружения или локализации закладных устройств по физическим свойствам элементов электрической схемы или конструкции. Такими элементами являются: полупроводниковые приборы, кото-рые применяются в любых закладных устройств, электропроводящие металличе-ские детали конструкции и т.д. Из этих средств наиболее достоверные результаты обеспечивают средства для обнаружения полупроводниковых элементов по их не-линейным свойствам - **нелинейные радиолокаторы.**

Принципы работы нелинейных радиолокаторов близки к принципам работы радиолокационных станций, широко применяемых для радиолокационной разведки объектов. Существенное отличие заключается в том, что если приемник радио-локационной станции принимает отраженный от объекта зондирующий сигнал (эхо-сигнал) на частоте излучаемого сигнала, то приемник нелинейного локатора принимает 2-ю и 3-ю гармоники отраженного

сигнала. Появление в отраженном сигнале этих гармоник обусловлено нелинейностью характеристик полупроводников.

Обнаружители пустот позволяют обнаруживать возможные места уста-новки закладных устройств в пустотах стен или других деревянных или кирпичных конструкциях.

Металлоискатели (металлодетекторы) реагируют на наличие в зоне по-иска электропроводных материалов, прежде всего металлов, и позволяют обнаруживать корпуса или другие металлические элементы закладки.

Переносные **рентгеновские установки** применяются для просвечивания предметов, назначения которых не удается выявить без их разборки, прежде всего тогда, когда разборка невозможна без разрушения найденного предмета.

3.4. Методы предотвращения утечки речевой информации

Организационные мероприятия, помимо обнаружения утечек, должны быть направлены на их предотвращение. Одним из эффективных методов здесь является контроль и ограничение доступа к защищаемой информации. Применительно к защите речевой информации это ограничение доступа посторонних лиц в защи-щаемые и смежные с ними помещения для предотвращения установки закладок, случайного либо несанкционированного прослушивания ведущихся переговоров.

Для защиты акустической (речевой) информации используются пассивные и активные методы и средства [8].

Пассивные методы защиты акустической (речевой) информации направлены:

- на ослабление акустических (речевых) сигналов на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- ослабление информационных электрических сигналов в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразова-тели (обладающие микрофонным эффектом), до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- исключение (ослабление) прохождения сигналов высокочастотного навязы-вания во вспомогательные технические средства, имеющие в своем составе электроакустические преобразователи (обладающие микрофонным эффектом);
- обнаружение излучений акустических закладок и побочных электромагнит-ных излучений диктофонов в режиме записи;
- обнаружение несанкционированных подключений к телефонным линиям связи.

Активные методы защиты акустической (речевой) информации направле-ны:

- на создание маскирующих акустических и вибрационных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного акустического сигнала средством разведки;
- создание маскирующих электромагнитных помех в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (об-ладающие микрофонным эффектом), с целью уменьшения отношения сиг-нал/шум до величин, обеспечивающих невозможность выделения информа-ционного сигнала средством разведки;
- электромагнитное подавление диктофонов в режиме записи;
- ультразвуковое подавление диктофонов в режиме записи;
- создание маскирующих электромагнитных помех в линиях электропитания ВТСС, обладающих микрофонным эффектом, с целью уменьшения отноше-ния сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;

 создание прицельных радиопомех акустическим и телефонным радиоза-кладкам с целью уменьшения отношения сигнал/шум до величин, обеспечи-вающих невозможность выделения информационного сигнала средством разведки;
 подавление (нарушение функционирования) средств несанкционированного подключения к телефонным линиям;
 уничтожение (вывод из строя) средств несанкционированного подключения к телефонным линиям.

Ослабление акустических (речевых) сигналов осуществляется путем звуко-изоляции помещений.

Ослабление информационных электрических сигналов в соединительных линиях ВТСС и исключение (ослабление) прохождения сигналов высокочастотно-го навязывания во вспомогательные технические средства осуществляется мето-дами фильтрации сигналов.

В основе активных методов защиты акустической информации лежит ис-пользование различного типа генераторов помех, а также применение других спе-циальных технических средств. Для локализации побочных излучений осуществ-ляется звукоизоляция, экранирование, заземление устанавливаемой в выделенных помещениях аппаратуры. Должна быть предусмотрена установка развязок, фильт-ров, диэлектрических вставок в трактах, имеющих выход за пределы зоны контроля.

С целью создания помех прослушиванию вплоть до полной неразборчивости перехватываемых сигналов осуществляется пространственное и линейное за-шумление, подавление диктофонов и сотовых телефонов, уничтожение (выжига-ние) закладных устройств.

Для предотвращения перехвата речевой информации, передаваемой по каналам связи, наиболее эффективным методом является шифрование кодированных сообщений.

3.4.1. Звукоизоляция помещений

Звукоизоляция помещений направлена на локализацию источников акустических сигналов внутри них и проводится с целью исключения перехвата акусти-ческой (речевой) информации по прямому акустическому (через щели, окна, две-ри, технологические проемы, вентиляционные каналы и т.д.) и вибрационному (через ограждающие конструкции, трубы водо-, тепло- и газоснабжения, канали-зации и т.д.) каналам [8].

Основное требование к звукоизоляции помещения заключается в том, чтобы за его пределами отношение акустический сигнал/шум не превышало некоторого допустимого значения, исключающего выделение речевого сигнала на фоне есте-ственных шумов средством разведки. Поэтому к помещениям, в которых прово-дятся закрытые мероприятия, предъявляются определенные требования по звуко-изоляции.

Звукоизоляция помещений обеспечивается с помощью архитектурных и инженерных решений, а также применением специальных строительных и отделоч-ных материалов.

При падении акустической волны на границу поверхностей с различными удельными плотностями большая часть падающей волны отражается. Меньшая часть волны проникает в материал звукоизолирующей конструкции и распростра-няется в нем, теряя свою энергию в зависимости от длины пути и его акустиче-ских свойств. Под действием акустической волны звукоизолирующая поверхность совершает сложные колебания, также поглощающие энергию падающей волны. Характер этого поглощения определяется соотношением частот падающей аку-стической волны и спектральных характеристик поверхности средства звукоизоляции [9].

Одним из наиболее слабых звукоизолирующих элементов ограждающих конструкций выделенных помещений являются двери и окна.

Двери имеют существенно меньшие по сравнению со стенами и межэтажными перекрытиями поверхностные плотности и трудноуплотняемые зазоры и щели. Стандартные двери не удовлетворяют требованиям по защите информации.

Увеличение звукоизолирующей способности дверей достигается плотной пригонкой полотна двери к коробке, устранением щелей между дверью и полом, применением уплотняющих прокладок, обивкой или облицовкой полотен дверей специальными материалами и т.д. Применение уплотняющих прокладок повыша-ет звукоизоляцию дверей, однако при этом необходимо учитывать, что в процессе эксплуатации в результате обжатия, износа, затвердевая резиновых прокладок зву-коизоляция существенно снижается. Для защиты информации в особо важных помещениях используются двери с тамбуром, а также специальные двери с повы-шенной звукоизоляцией. Для повышения звукоизоляции проводится облицовка внутренних поверхностей тамбура звукопоглощающими покрытиями, а двери обиваются материалами со слоями ваты или войлока, и используются дополни-тельные уплотнительные прокладки.

Звукопоглощающая способность окон, так же как и дверей, зависит главным образом от поверхностной плотности стекла и степени прижатия притворов. Зву-коизоляция окон с одинарным остеклением соизмерима со звукоизоляцией оди-нарных дверей и недостаточна для надежной защиты информации в помещении. Существенно большую звукоизоляцию имеют окна с остеклением в раздельных переплетах с шириной воздушного промежутка более 200 мм или тройное комби-нированное остекление. Обычные окна с двойными переплетами обладают более высокой (на 4 ... 5 дБ) звукоизолирующей способностью по сравнению с окнами со спаренными переплетами. Применение упругих прокладок значительно улуч-шает звукоизоляционные качества окон. В случаях когда необходимо обеспечить повышенную звукоизоляцию, применяют окна специальной конструкции (напри-мер, двойное окно с заполнением оконного проема органическим стеклом толщи-ной 20 ... 40 мм и с воздушным зазором между стеклами не менее 100 мм). Разра-ботаны конструкции окон с повышенным звукопоглощением на основе стеклопа-кетов с герметизацией воздушного промежутка между стеклами и с заполнением его различными газовыми смесями или создание в нем вакуума. Повышение зву-коизоляции до 5 дБ наблюдается при облицовке межстекольного пространства по периметру звукопоглощающим покрытием.

Необходимо отметить, что увеличение числа стекол не всегда приводит к увеличению звукоизоляции в диапазоне частот речевого сигнала вследствие резо-нансных явлений в воздушных промежутках и эффекта волнового совпадения.

Для повышения звукоизоляции в помещениях применяют акустические экраны, устанавливаемые на пути распространения звука на наиболее опасных (с точки зрения разведки) направлениях. Действие акустических экранов основано на отражении звуковых волн и образовании за экраном звуковых теней. С учетом дифракции эффективность экрана повышается с увеличением соотношения раз-меров экрана и длины акустической волны. Размеры эффективных экранов пре-вышают длину волны более чем в 2 … 3 раза. Реально достигаемая эффективность акустического экранирования составляет 8 … 10 дБ.

Применение акустического экранирования целесообразно при временном использовании помещения для защиты акустической информации. Наиболее часто применяются складные акустические экраны, используемые для дополнительной звукоизоляции дверей, окон,

технологических проемов, систем кондиционирова-ния, проточной вентиляции и других элементов ограждающих конструкций, имеющих звукоизоляцию, не удовлетворяющую действующим нормам.

Для повышения звукоизоляции помещений также применяют звукопоглощающие материалы. Звукопоглощение обеспечивается путем преобразования ки-нетической энергии акустической волны в тепловую энергию в звукопоглощаю-щем материале. Звукопоглощающие свойства материалов оцениваются коэффици-ентом звукопоглощения, определяемым отношением энергии звуковых волн, по-глощенной в материале, к энергии, падающей на поверхность материала и проникающей (неотраженной) в звукопоглощающий материал.

Применение звукопоглощающих материалов при защите акустической информации имеет некоторые особенности по сравнению с звукоизоляцией. Одной из особенностей является необходимость создания непосредственно в помещении акустических условий для обеспечения разборчивости речи в различных его зо-нах. Таким условием является прежде всего обеспечение оптимального соотноше-ния прямого и отраженного от ограждений акустических сигналов. Чрезмерное звукопоглощение приводит к ухудшению уровня сигнала в различных точках по-мещения, а большое время реверберации - к ухудшению разборчивости в результате наложения различных звуков.

Звукопоглощающие материалы могут быть сплошными и пористыми. Обычно пористые материалы используют в сочетании со сплошными. Один из распространенных видов пористых материалов - облицовочные звукопоглощаю-щие материалы. Их изготавливают в виде плоских плит (плиты минераловатные "Акмигран", "Акмант", "Силаклор", "Винипор", ПА/С, ПА/О, ПП-80, ППМ, ПММ) или рельефных конструкций (пирамид, клиньев и т.д.), располагаемых вплотную или на небольшом расстоянии от сплошной строительной конструкции (стены, перегородки, ограждения и т.п.). Используются также звукопоглощающие облицовки из слоя пористо-волокнистого материала (стеклянного или базальтово-го волокна, минеральной ваты) в защитной оболочке из ткани или пленки с пер-форированным покрытием (металлическим, гипсовым и др.).

Отдельную группу звукопоглощающих материалов составляют резонансные поглотители. Они подразделяются на мембранные и резонаторные. Мембранные поглотители представляют собой натянутый холст (ткань), тонкий фанерный (кар-тонный) лист, под которым располагают хорошо демпфирующий материал (мате-риал с большой вязкостью, например, поролон, губчатую резину, строительный войлок и т д.). В такого рода поглотителях максимум поглощения достигается на резонансных частотах.

Перфорированные резонаторные поглотители представляют собой систему воздушных резонаторов (например, резонаторов Гельмгольца), в устье которых расположен демпфирующий материал.

Между помещениями зданий и сооружений проходит много технологических коммуникаций (трубы тепло-, газо-, водоснабжения и канализации, кабель-ная сеть энергоснабжения, вентиляционные короба и т. д.). Для них в стенах и пе-рекрытиях сооружений делают соответствующие отверстия и проемы. Их надеж-ная звукоизоляция обеспечивается применением специальных гильз, коробов, прокладок, глушителей, вязкоупругих заполнителей и т. д. Обеспечение требуемой звукоизоляции в вентиляционных каналах достигается за счёт использования сложных акустических фильтров и глушителей.

Следует иметь в виду, что в общем случае звукоизоляция ограждающих конструкций, содержащих несколько элементов, должна оцениваться звукоизоляцией наиболее слабого из них.

Для защиты конфиденциальных разговоров разработаны специальные звукоизолирующие кабины. В конструктивном отношении они делятся на каркасные и бескаркасные. В первом случае на металлический каркас крепятся звукопогло-щающие панели. Примером таких кабин являются кабины междугородней теле-фонной связи. Кабины с двухслойными звукопоглощающими плитами обеспечивают ослабление звука до 35...40 дБ.

Более высокой акустической эффективностью (большим коэффициентом ослабления) обладают кабины бескаркасного типа. Они собираются из готовых многослойных щитов, соединенных между собой звукоизолирующими упругими прокладками. Такие кабины дороги в изготовлении, но снижение уровня звука в них может достигать 50 ... 55 дБ. Для повышения звукоизоляции кабины миними-зируют возможное число стыковочных соединений отдельных панелей между со-бой и с каркасом кабины. Тщательно герметизируют и уплотняют стыковочные соединения, применяют звукопоглощающие облицовки стен и потолка. В систе-мах вентиляции и кондиционирования воздуха устанавливают специальные глушители звука.

3.4.2. Виброакустическая маскировка

В случае если используемые пассивные средства защиты помещений не обеспечивают требуемых норм по звукоизоляции, необходимо использовать активные меры защиты [6,7].

Активные меры защиты заключаются в создании маскирующих акустических помех средствам разведки, то есть использованием виброакустической маскировки информационных сигналов. В отличие от звукоизоляции помещений, обеспечивающей требуемое ослабление интенсивности звуковой волны за их пре-делами, использование активной акустической маскировки снижает отношение сигнал/шум на входе технического средства разведки за счет увеличения уровня шума (помехи).

Виброакустическая маскировка эффективно используется для защиты речевой информации от утечки по прямому акустическому, виброакустическому и оптико-электронному каналам утечки информации.

Для формирования акустических помех применяются специальные генераторы, к выходам которых подключены звуковые колонки (громкоговорители) или вибрационные излучатели (вибродатчики).

На практике наиболее широкое применение нашли генераторы шумовых колебаний. Именно поэтому активную акустическую маскировку часто называют акустическим зашумлением. Большую группу генераторов шума составляют устройства, принцип действия которых основан на усилении колебаний первичных источников шумов. В качестве источников шумовых колебаний используются электровакуумные, газоразрядные, полупроводниковые и другие электронные приборы и элементы.

Временной случайный процесс, близкий по своим свойствам к шумовым колебаниям, может быть получен и с помощью цифровых генераторов шума, формирующих последовательности двоичных символов, называемые псевдослучайными.

Наряду с шумовыми помехами в целях активной акустической маскировки используют и другие помехи, например, "одновременный разговор нескольких человек", хаотические последовательности импульсов и т.д.

Роль оконечных устройств, осуществляющих преобразование электрических колебаний в акустические колебания речевого диапазона длин волн, обычно выполняют малогабаритные широкополосные громкоговорители, а осуществляющих преобразование электрических колебаний в вибрационные - вибрационные излучатели (вибродатчики).

Громкоговорители систем зашумления устанавливаются в помещении в местах наиболее вероятного размещения средств акустической разведки, а вибродатчики крепятся на рамах, стеклах, коробах, трубопроводах, стенах, потолках и т.д.

Создаваемые вибродатчиками шумовые колебания в ограждающих конструкциях, трубах, оконном стекле и т.д. приводят к значительному повышению в них уровня вибрационных шумов и тем самым - к существенному ухудшению ус-ловий приема и восстановления речевых сообщений средствами разведки.

В настоящее время создано большое количество различных систем активной виброакустической маскировки, успешно используемых для подавления средств перехвата речевой информации. К ним относятся системы "Заслон", "Кабинет", "Барон", "Фон-В", VNG-006, ANG-2000, NG-101 и др.

В состав типовой системы виброакустической маскировки входят шумогенератор и от 6 до 12 ... 25 вибродатчиков (пьезокерамических или электромагнитных). Дополнительно в состав системы могут включаться звуковые колонки.

Наиболее эффективным методом выявления радиозакладок в выделенных помещениях является **постоянный радиоконтроль** с использованием программно-аппаратных комплексов контроля. Для его организации в специально оборудо-ванном помещении на объекте разворачивается стационарный пункт радиоконтроля, в состав которого, как правило, входит один или несколько программно-аппаратных комплексов, позволяющих контролировать все выделенные помеще-ния. На пункте радиоконтроля устанавливается опорная антенна, а в выделенных (контролируемых) помещениях - малогабаритные широкополосные антенны и звуковые колонки или выносные микрофоны, которые при установке камуфлиру-ются. Антенны и звуковые колонки (или микрофоны) специально проложенными кабелями соединяются соответственно с блоками высокочастотного (антенного) или низкочастотного коммутаторов, установленных в помещении стационарного пункта контроля.

Если при проведении радиоконтроля обнаружена передача информации радиозакладкой, то до ее выявления может быть организована **постановка прицельных помех** на частоте передачи закладки. Для этих целей может использо-ваться, например, устройство постановки помех АРК-СП.

3.4.3. Методы и средства защиты телефонных линий

При защите телефонных аппаратов и телефонных линий необходимо учиты-вать следующее [6,7,8]:

- телефонные аппараты (даже при положенной трубке) могут быть использо-ваны для перехвата акустической речевой информации из помещений, в ко-торых они установлены, то есть для подслушивания разговоров в этих по-мещениях;
- телефонные линии, проходящие через помещения, могут использоваться в качестве источников питания акустических закладок, установленных в этих помещениях, а также для передачи перехваченной информации;

 возможен перехват (подслушивание) телефонных разговоров путем гальва-нического (или через индукционный датчик) подключения к телефонной линии закладок (телефонных ретрансляторов), диктофонов и других средств несанкционированного съема информации.

Телефонный аппарат имеет несколько элементов, имеющих способность преобразовывать акустические колебания в электрические, то есть обладающих "микрофонным эффектом". К ним относятся: звонковая цепь, телефонный и мик-рофонный капсюли. За счет электроакустических преобразований в этих элемен-тах возникают информационные (опасные) сигналы.

При положенной трубке телефонный и микрофонный капсюли гальваниче-ски отключены от телефонной линии, и при подключении к ней специальных вы-сокочувствительных низкочастотных усилителей возможен перехват опасных сиг-налов, возникающих в элементах только звонковой цепи. Амплитуда этих опасных сигналов, как правило, не превышает долей мВ.

При использовании для съема информации метода "высокочастотного навя-зывания", несмотря на гальваническое отключение микрофона от телефонной ли-нии, сигнал навязывания благодаря высокой частоте проходит в микрофонную цепь и модулируется по амплитуде информационным сигналом.

Следовательно, в телефонном аппарате необходимо защищать как звонко-вую цепь, так и цепь микрофона.

Для защиты телефонного аппарата от утечки акустической (речевой) ин-формации по электроакустическому каналу используются как пассивные, так и ак-тивные методы и средства.

К наиболее широко применяемым пассивным методам защиты относятся:

 ограничение опасных сигналов;
 фильтрация опасных сигналов;
 отключение преобразователей (источников) опасных сигналов.

Возможность ограничения опасных сигналов основывается на нелинейных свойствах полупроводниковых элементов, главным образом диодов. В схеме огра-ничителя малых амплитуд используются два встречно включенных диода. Такие диоды имеют большое сопротивление (сотни кОм) для токов малой амплитуды и единицы Ом и менее - для токов большой амплитуды (полезных сигналов), что исключает прохождение опасных сигналов малой амплитуды в телефонную ли-нию и практически не оказывает влияние на прохождение через диоды полезных сигналов. Диодные ограничители включаются последовательно в линию звонка или непосредственно в каждую из телефонных линий.

Фильтрация опасных сигналов используется главным образом для защиты телефонных аппаратов от "высокочастотного навязывания".

Простейшим фильтром является конденсатор, устанавливаемый в звонковую цепь телефонных аппаратов с электромеханическим звонком и в микрофонную цепь всех аппаратов. Емкость конденсаторов выбирается такой величины, чтобы зашунтировать зондирующие сигналы высокочастотного навязывания и не оказы-вать существенного влияния на полезные сигналы. Обычно для установки в звон-ковую цепь используются конденсаторы емкостью 1 мкФ, а для установки в мик-рофонную цепь - емкостью 0,01 мкФ. Более сложное фильтрующее устройство представляет собой многозвенный фильтр низкой частоты на LC-элементах.

Для защиты телефонных аппаратов, как правило, используются устройства, сочетающие фильтр и ограничитель. К ним относятся: устройства типа "Экран", "Гранит-8", "Корунд", "Грань-300" и др.

Отключение телефонных аппаратов от линии при ведении в помещении конфиденциальных разговоров является наиболее эффективным методом защиты речевой информации.

Самый простой способ реализации этого метода защиты заключается в ус-тановке в корпусе телефонного аппарата или телефонной линии специального вы-ключателя, включаемого и выключаемого вручную. Более удобным в эксплуата-ции является установка в телефонной линии специального устройства защиты, автоматически (без участия оператора) отключающего телефонный аппарат от линии при положенной телефонной трубке.

К типовым устройствам, реализующим данный метод защиты, относится изделие "Барьер-Ml". В эго состав входят электронный коммутатор, схема анализа состояния телефонного аппарата, наличия вызывных сигналов и управления ком-мутатором и схема защиты телефонного аппарата от воздействия высоковольтных импульсов.

Устройство работает в следующих режимах: дежурном, передачи сигналов вызова и рабочем. В дежурном режиме (при положенной телефонной трубке) те-лефонный аппарат отключен от линии, и устройство находится в режиме анализа поднятия телефонной трубки и наличия сигналов вызова. При получении сигналов вызова устройство переходит в режим передачи сигналов вызова, при котором через электронный коммутатор телефонный аппарат подключается к линии. Под-ключение осуществляется только на время действия сигналов вызова. При подня-тии телефонной трубки устройство переходит в рабочий режим и телефонный ап-парат подключается к линии.

Изделие устанавливается в разрыв телефонной линии, как правило, при вы-ходе ее из выделенного (защищаемого) помещения или в распределительном щит-ке (кроссе), находящемся в пределах контролируемой зоны.

Электропитание устройства осуществляется от телефонной линии при токе потребления в дежурном режиме не более 0,3 мА.

Устройство "Барьер - Ml" обеспечивает защиту телефонного аппарата не только от утечки информации по электроакустическому каналу, но также и его за-щиту от воздействия высоковольтных импульсов (напряжением до 1000 В и дли-тельностью до 100 мкс).

Активные методы защиты от утечки информации по электроакустическому каналу предусматривают линейное зашумление телефонных линий. Шумовой сигнал подается в линию в режиме, когда телефонный аппарат не используется (трубка положена). При снятии трубки телефонного аппарата подача в линию шу-мового сигнала прекращается.

К сертифицированным средствам линейного зашумления относятся устрой-ства МП-1А (защита аналоговых телефонных аппаратов) и МП-1Ц П-1А (защита цифровых телефонных аппаратов) и др.

Для защиты акустической (речевой) информации в выделенных помещениях наряду с защитой телефонных аппаратов необходимо принимать меры и для за-щиты непосредственно телефонных линий, так как они могут использоваться в качестве источников питания

акустических закладок, установленных в помещениях, а также для передачи информации, получаемой этими закладками.

При этом используются как пассивные, так и активные методы и средства защиты. Пассивные методы защиты основаны на блокировании акуститических закладок, питающихся от телефонной линии в режиме положенной трубки, а ак-тивные - на линейном зашумлении и уничтожении (электрическом "выжигании") закладных устройств или их блоков питания путем подачи в линию высоковольтных импульсов.

Защита телефонных разговоров от перехвата осуществляется главным обра-зом активными методами. К основным из них относятся:

- подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочас-тотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи);
- подача во время разговора в телефонную линию маскирующего высокочас-тотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи);
- поднятие напряжения в телефонной линии во время разговора (метод повы-шения напряжения);
- подача во время разговора в линию напряжения, компенсирующего посто-янную составляющую телефонного сигнала (метод "обнуления");
- подача в линию при положенной телефонной трубке маскирующего низко-частотного сигнала (метод низкочастотной маскирующей помехи);
- подача в линию при приеме сообщений маскирующего низкочастотного (ре-чевого диапазона) с известным спектром (компенсационный метод);
- подача в телефонную линию высоковольтных импульсов (метод "выжигания").

Суть метода синфазной маскирующей низкочастотной (НЧ) помехи заключается в подаче в каждый провод телефонной линии с использованием единой системы заземления аппаратуры АТС и нулевого провода электросети 220 В (ну-левой провод электросети заземлен) согласованных по амплитуде и фазе маски-рующих сигналов речевого диапазона частот (как правило, основная мощность помехи сосредоточена в диапазоне частот стандартного телефонного канала - 300…3400 Гц). В телефонном аппарате эти помеховые сигналы компенсируют друг друга и не оказывают мешающего воздействия на полезный сигнал (теле-фонный разговор). Если же информация снимается с одного провода телефонной линии, то помеховый сигнал не компенсируется. А так как его уровень значитель-но превосходит полезный сигнал, перехват информации (выделение полезного сигнала) становится невозможным. В качестве маскирующего помехового сигна-ла, как правило, используются дискретные сигналы (псевдослучайные последова-тельности импульсов).

Метод синфазного маскирующего низкочастотного сигнала используется для подавления телефонных радиозакладок с параметрической и кварцевой стаби-лизацией частоты, с последовательным (в разрыв одного из проводов) включени-ем, а также телефонных радиозакладок и диктофонов с подключением к линии (к одному из проводов) с помощью индукционных датчиков различного типа.

Метод высокочастотной маскирующей помехи заключается в подаче во время разговора в телефонную линию широкополосного маскирующего сигнала в диапазоне высших частот звукового диапазона.

Данный метод используется для подавления практически всех типов подслушивающих устройств как контактного (параллельного и последовательного) подключения к линии, так и подключения с использованием индукционных дат-чиков. Однако эффективность подавления средств съема информации с подключе-нием к линии при помощи с индукционных датчиков (особенно не имеющих пре-дусилителей) значительно ниже, чем средств с гальваническим подключением к линии.

В качестве маскирующего сигнала используются широкополосные аналоговые сигналы типа "белого шума" или дискретные сигналы типа псевдослучайной последовательности импульсов.

Частоты маскирующих сигналов подбираются таким образом, чтобы после прохождения селективных цепей модулятора закладки или микрофонного усили-теля диктофона их уровень оказался достаточным для подавления полезного сиг-нала (речевого сигнала в телефонной линии во время разговоров абонентов), но в то же время эти сигналы не ухудшали качество телефонных разговоров. Чем ниже частота помехового сигнала, тем выше его эффективность и тем большее мешаю-щее воздействие он оказывает на полезный сигнал. Обычно используются частоты в диапазоне от 6 ... 8 кГц до 16 ... 20 кГц. Например, в устройстве Sel SP-17/T по-меха создается в диапазоне 8 ... 10 кГц.

Такие маскирующие помехи вызывают значительные уменьшение отношения сигнал/шум и искажения полезных сигналов (ухудшение разборчивости речи) при перехвате их всеми типами подслушивающих устройств. Кроме того, у радио-закладок с параметрической стабилизацией частоты ("мягким" каналом) как по-следовательного, так и параллельного включения наблюдается "уход" несущей частоты, что может привести к потере канала приема.

Для исключения воздействия маскирующего помехового сигнала на телефонный разговор в устройстве защиты устанавливается специальный низкочас-тотный фильтр с граничной частотой 3,4 кГц, подавляющий (шунтирующий) по-меховые сигналы и не оказывающий существенного влияния на прохождение по-лезных сигналов. Аналогичную роль выполняют полосовые фильтры, установ-ленные на городских АТС, пропускающие сигналы, частоты которых соответст-вуют стандартному телефонному каналу (300 Гц ... 3,4 кГц), и подавляющие помеховый сигнал.

Метод ультразвуковой маскирующей помехи в основном аналогичен рассмотренному выше. Отличие состоит в том, что используются помеховые сигналы ультразвукового диапазона с частотами от 20 ... 25 кГц до 50 ... 100 кГц.

Метод повышения напряжения заключается в поднятии напряжения в телефонной линии во время разговора и используется для ухудшения качества функционирования телефонных радиозакладок. Поднятие напряжения в линии до 18 ... 24 В вызывает у радиозакладок с последовательным подключением и пара-метрической стабилизацией частоты "уход" несущей частоты и ухудшение раз-борчивости речи вследствие размытия спектра сигнала. У радиозакладок с после-довательным подключением и кварцевой стабилизацией частоты наблюдается уменьшение отношения сигнал/шум на 3 ... 10 дБ. Телефонные радиозакладки с параллельным подключением при таких напряжениях в ряде случаев просто отключаются.

Метод "обнуления" предусматривает подачу во время разговора в линию постоянного напряжения, соответствующего напряжению в линии при поднятой телефонной трубке, но обратной полярности.

Этот метод используется для нарушения функционирования подслушивающих устройств с контактным параллельным подключением к линии и использую-щих ее в качестве источника питания. К таким устройствам относятся: параллель-ные телефонные аппараты, проводные микрофонные системы с электретными микрофонами, использующие телефонную линию для передачи информации, аку-стические и телефонные закладки с питанием от телефонной линии и т.д.

Метод низкочастотной маскирующей помехи заключается в подаче в линию при положенной телефонной трубке маскирующего сигнала (наиболее часто типа "белого шума") речевого диапазона частот. Как правило, основная мощность помехи сосредоточена в диапазоне частот телефонного канала - 300 ... 3400 Гц. Метод применяется для подавления проводных микрофонных систем, исполь-зующих телефонную линию для передачи информации на низкой частоте, а также для активизации (включения на запись) диктофонов, подключаемых к телефонной линии с помощью адаптеров или индукционных датчиков, что приводит к сматы-ванию пленки в режиме записи шума (то есть при отсутствии полезного сигнала).

Компенсационный метод используется для односторонней маскировки (скрытия) речевых сообщений, передаваемых абоненту по телефонной линии.

Суть метода заключается в следующем. При передаче скрываемого сообщения на приемной стороне в телефонную линию при помощи специального генератора подается маскирующая помеха (цифровой или аналоговый маскирующий сигнал речевого диапазона с известным спектром). Одновременно этот же маски-рующий сигнал ("чистый" шум) подается на один из входов двухканального адап-тивного фильтра, на другой вход которого поступает аддитивная смесь принимае-мого полезного сигнала речевого сигнала (передаваемого сообщения) и этого же помехового сигнала. Аддитивный фильтр компенсирует (подавляет) шумовую со-ставляющую и выделяет полезный сигнал, который подается на телефонный ап-парат или устройство звукозаписи.

Недостатком данного метода является то, что маскировка речевых сообщений односторонняя и не позволяет вести двухсторонние телефонные разговоры.

Метод "выжигания" реализуется путем подачи в линию высоковольтных (напряжением более 1500 В) импульсов, приводящих к электрическому "выжига-нию" входных каскадов электронных устройств перехвата информации и блоков их питания, гальванически подключенных к телефонной линии.

При использовании данного метода телефонный аппарат от линии отключается. Подача импульсов в линию осуществляется два раза. Первый - для "выжи-гания" параллельно подключенных устройств - при разомкнутой телефонной ли-нии. Второй - для "выжигания" последовательно подключенных устройств - при закороченной (как правило, в центральном распределительном щитке здания) те-лефонной линии.

Для защиты телефонных линий используются как простые устройства, реализующие один метод защиты, так и сложные, обеспечивающие комплексную за-щиту линий различными методами, включая защиту от утечки информации по электроакустическому каналу.

На отечественном рынке имеется большое разнообразие средств защиты. Среди них можно выделить следующие: "SP 17/T", "S1-2001", "КТЛ-3", "КТЛ-400", "Ком-3", "Кзот-06", "Цикада-М", "Прокруст" (ПТЗ-003), "Прокруст-2000", "Консул", "Гром-ЗИ-6", "Протон" и др.

В активных устройствах защиты телефонных линий наиболее часто реализованы метод высокочастотной маскирующей помехи ("SP 17/T", ", "КТЛ-3", "КТЛ-400", "Ком-3", "Прокруст" (ПТЗ-003), "Прокруст-2000","Гром-ЗИ-6", "Протон" и др.) и метод ультразвуковой маскирующей помехи ("Прокруст" (ПТЗ-003), "Гром-ЗИ-6").

Метод синфазной низкочастотной маскирующей помехи используется в устройстве "Цикада-М", а метод низкочастотной маскирующей помехи - в устройст-вах "Прокруст", "Протон", "Кзот-06" и др.

Метод "обнуления" применяется, например, в устройстве "Цикада-М", а метод повышения напряжения в линии - в устройстве "Прокруст".

Компенсационный метод маскировки речевых сообщений, передаваемых абоненту по телефонной линии, реализован в изделии "Туман".

Большинство устройств защиты производят автоматическое измерение напряжения в линии и отображают его значение на цифровом индикаторе. В приборе "Гром-ЗИ-6" на цифровом индикаторе отображается уровень уменьшения напряжения в линии.

Для вывода из строя ("выжигания" входных каскадов) средств несанкционированного съема информации с гальваническим подключением к телефонной линии используются устройства типа "ПТЛ-1500", "КС-1300", "КС-1303", "Кобра".

Приборы используют высоковольтные импульсы напряжением не менее 1500 ... 1600 В. Мощность "выжигающих" импульсов составляет 15 ... 50 ВА. Так как в схемах закладок применяются миниатюрные низковольтные детали, то высоковольтные импульсы их пробивают и схема закладки выводится из строя.

"Выжигатели" телефонных закладок могут работать как в ручном, так и автоматическом режимах. Время непрерывной работы в автоматическом режиме со-ставляет от 20 сек до 24 ч.

Наряду со средствами активной защиты на практике широко используются различные устройства, позволяющие контролировать некоторые параметры теле-фонных линий и устанавливать факт несанкционированного подключения к ним.

Методы контроля телефонных линий в основном основаны на том, что любое подключение к ним вызывает изменение электрических параметров линий: амплитуд напряжения и тока в линии, а также значений емкости, индуктивности, активного и реактивного сопротивления линии.

Измерение параметров линии с целью выявления средств несанкционированного съема информации проводится, как правило, при проведении периодиче-ских специальных проверок.

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения. При настройке оператор фиксирует значение напряже-ние, соответствующее нормальному состоянию линии (когда к линии не подклю-чены посторонние устройства), и порог тревоги. При уменьшении напряжения в линии более установленного порога устройством подается световой или звуковой сигнал тревоги.

На принципах измерения напряжения в линии построены и устройства, сигнализирующие о размыкании телефонной линии, которое возникает при последо-вательном подключении закладного устройства.

Как правило, подобные устройства содержат также фильтры для защиты от прослушивания за счет "микрофонного эффекта" в элементах телефонного аппа-рата и высокочастотного "навязывания".

Устройства контроля телефонных линий, построенные на рассмотренном принципе, реагируют на изменения напряжения, вызванные не только подключе-нием к линии средств съема информации, но и колебаниями напряжения на АТС (что для отечественных линий довольно частое явление), что приводит к частым ложным срабатываниям сигнализирующих устройств. Кроме того, эти устройства не позволяют выявить параллельное подключение к линии высокоомных (с сопро-тивлением в несколько МОм) подслушивающих устройств. Поэтому подобные устройства не находят широкого применения на практике.

Принцип работы более сложных устройств основан на периодическом измерении и анализе нескольких параметров линии (наиболее часто: напряжения, тока, а также комплексного (активного и реактивного) сопротивления линии). Такие устройства позволяют определить не только факт подключения к линии средств съема информации, но и способ подключения (последовательное или параллель-ное). Например, контроллеры телефонных линий "КТЛ-2", "КТЛ-3" и "КТЛ-400" за 4 мин позволяют обнаружить закладки с питанием от телефонной линии неза-висимо от способа, места и времени их подключения, а также параметров линии и напряжения АТС. Приборы также выдают световой сигнал тревоги при кратко-временном (не менее 2 сек) размыкании линии.

Современные контроллеры телефонных линий, как правило, наряду со средствами обнаружения подключения к линии устройств несанкционированного съе-ма информации, оборудованы и средствами их подавления. Для подавления в ос-новном используется метод высокочастотной маскирующей помехи. Режим по-давления включается автоматически или оператором при обнаружении факта не-санкционированного подключения к линии.

Для блокировки работы (набора номера) несанкционированно подключенных параллельных телефонных аппаратов используются специальные электронные блокираторы.

Принцип работы подобных устройств состоит в следующем. В дежурном режиме устройство защиты производит анализ состояния телефонной линии пу-тем сравнения напряжения в линии и на эталонной (опорной) нагрузке, подключенной к цепи телефонного аппарата. При поднятии трубки несанкционированно подключенного параллельного телефонного аппарата напряжение в линии умень-шается, что фиксируется устройством защиты. Если этот факт зафиксирован в момент ведения телефонного разговора (трубка на защищаемом телефонном аппа-рате снята), срабатывает звуковая и световая (загорается светодиод несанкциони-рованного подключения к линии) сигнализация. А если факт несанкционирован-ного подключения к линии зафиксирован в отсутствие телефонного разговора (трубка на защищаемом телефонном аппарате не снята), то срабатывает сигнали-зация и устройство защиты переходит в режим блокирования набора номера с па-раллельного телефонного аппарата. В этом режиме устройство защиты шунтирует телефонную линию сопротивлением 600 Ом (имитируя снятие трубки на защи-щаемом телефонном аппарате), что полностью исключает возможность набора номера с параллельного телефонного аппарата.

Кроме несанкционированного подключения к линии параллельного телефонного аппарата подобные устройства сигнализирует также о фактах обрыва (размыкания) и короткого замыкания телефонной линии.

3.5. Методы закрытия речевой информации

Аналоговые каналы традиционно защищаются методами скремблирования во временной и частотной области.

Скремблирование - это перемешивание, перестановка временных либо частотных фрагментов исходного речевого сигнала перед передачей и обратное преобразование нарушенного порядка на приёмном конце. Дополнительную информацию по скремблированию можно найти в Интернете [33, 34]. Скремблирование может применяться и при передаче речевой информации по цифровым каналам,
однако в этом случае могут применяться более изощрённые методы шифрования, основанные на методах криптографии.

3.5.1. Криптографическая защита

Основные понятия и терминология криптографии приведены ниже [25].

Криптография - наука о методах преобразования (шифрования) информации с целью ее защиты от злоумышленников.

Шифр - способ (метод), преобразования информации с целью ее защиты от незаконных пользователей.

Стеганография - набор средств и методов сокрытия факта передачи сообщения.

Вскрытие шифра - процесс получения защищаемой информации (открытого текста) из шифрованного сообщения (шифртекста) без знания примененного шифра.

Шифрование - процесс применения шифра и защищаемой информации, т.е. преобразование защищаемой информации в шифрованное сообщение с помощью определенных правил, содержащихся в шифре.

Дешифрирование - процесс, обратный шифрованию, и заключающийся в преобразовании шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Под **ключом** в криптографии понимают сменный элемент шифра, который применяют для шифрования конкретных сообщений.

Криптология - наука, состоящая из двух направлений: криптографии и криптоанализа. **Криптоанализ** - это наука (и практика ее применения) о методах и способах вскрытия шифров.

Соотношение криптографии и криптоанализа очевидно: криптография - это защита, т.е.
разработка шифров, а криптоанализ - нападение, т.е. вскрытие шифров.
Однако это две науки связаны друг с другом, и не бывает хороших криптографов, не владеющих методами криптоанализа.

Чтобы криптографические методы преобразования обеспечили эффективную защиту информации, они должны удовлетворять ряду требований. В сжатом виде их можно сформулировать следующим образом:

 сложность и стойкость криптографического закрытия должны выбираться в зависимости от объема и степени секретности данных;

 надежность закрытия должна быть такой, чтобы секретность не нарушалась в том случае, когда злоумышленнику становится известен метод закрытия;
 метод закрытия, набор используемых ключей и механизм их распределения не могут быть слишком сложными;
 выполнение процедур прямого и обратного преобразований должно быть формализованным. Эти процедуры не должны зависеть от длины сообщений;
 ошибки, возникающие в процессе выполнения преобразования, не должны распространяться на текст в полной мере и по системе;
 вносимая процедурами защиты избыточность должна быть минимальной.

Классификация криптографических методов. В настоящее время не существует законченной и общепринятой классификации криптографических методов, так как многие из них находятся в стадии

развития и становления. Наиболее целесообразной представляется классификация, представленная на рис. 3.1.

Под шифрованием в данном случае понимается такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения.

Все известные способы шифрования разбиты на пять групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование.
Каждый из этих способов может иметь несколько разновидностей.

Под кодированием понимается такой вид криптографического закрытия, когда некоторые элементы защищаемых данных (не обязательно отдельные символы) заменяются заранее выбранными кодами

(цифровыми, буквенными, буквенно-цифровыми сочетаниями и т.д.). Этот метод имеет две разновидности: смысловое и символьное кодирование. При смысловом кодировании кодируемые элементы имеют
вполне определенный смысл (слова, предложения, группы предложений). При символьном кодировании кодируется каждый символ защищаемого текста. Символьное кодирование по существу совпадает
с подстановочным шифрованием.

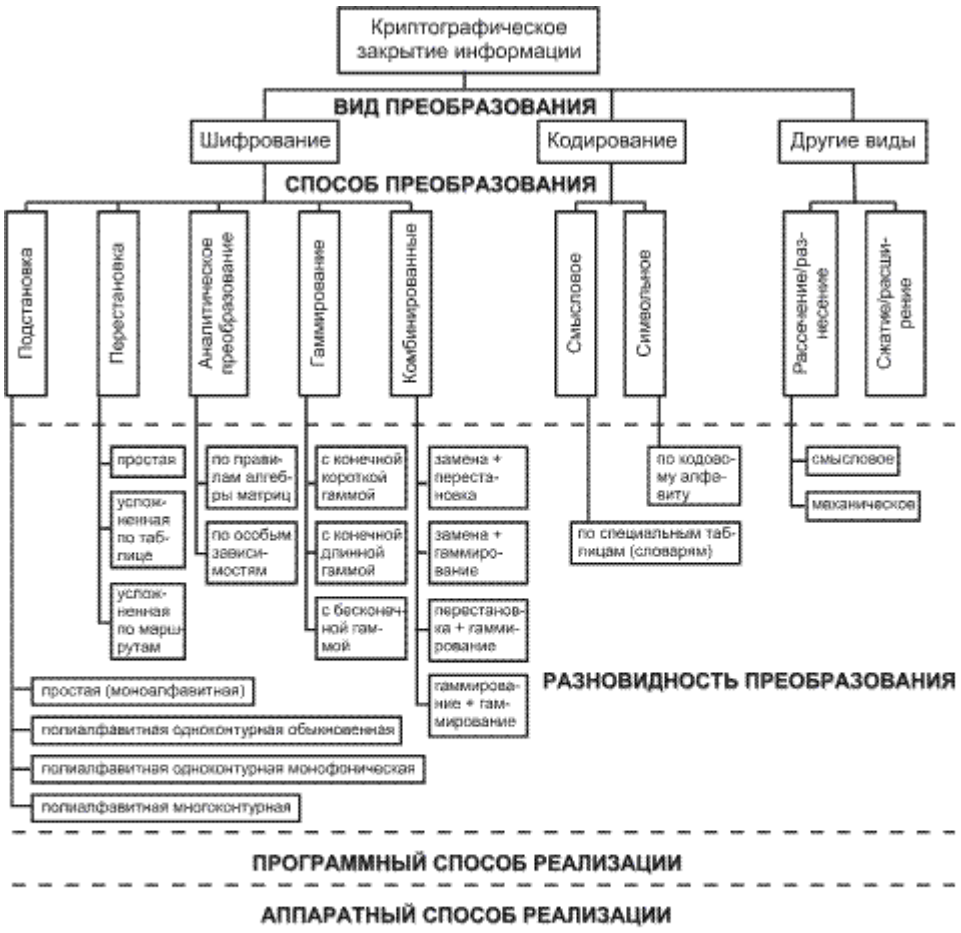

Рис. 3.1. Классификация криптографических методов [25]

К отдельным видам криптографии относятся методы рассечения/разнесения и сжатия данных. Рассечение/разнесение заключается в том, что массив защищаемых данных делится (рассекается) на такие

элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделенные таким образом элементы данных разносятся по разным зонам памяти или располагаются на разных носителях. Сжатие данных представляет собой замену часто встречающихся одинаковых строк данных или последовательностей одина-ковых символов некоторыми заранее выбранными символами.

Требования к криптографическим методам защиты информации. Раскрытие зашифрованных текстов (в первую очередь нахождение ключа) осуществляется при помощи методов криптоанализа. Основными методами криптоанализа являются:

 статистические, при которых зная статистические свойства открытого текста пытаются исследовать статистические закономерности шифротекста и на основании обнаруженных закономерностей раскрыть текст;
 метод вероятных слов, в котором при сопоставлении некоторой небольшой части шифротекста с известным фрагментом открытого текста пытаются найти ключ и с его помощью расшифровать весь текст. Требуемый фрагмент открытого текста можно найти с помощью статистических методов или про-сто угадать, исходя из предполагаемого содержания или структуры открытого текста.

Анализ основных криптографических методов защиты информации. Иногда криптографические методы защиты информации разделяют на три группы: методы подстановки, методы перестановки и аддитивные методы. Методы пе-рестановки и подстановки характеризуются хорошими ключами, а их надежность связана со сложным алгоритмом преобразования. При аддитивных методах поль-зуются простыми алгоритмами преобразования, обеспечивая надежность с помо-щью ключей большого объема.

Иногда говорят о блочных методах, имея в виду первые две группы, в которых алгоритм работает сразу над большим блоком информации, и о потоковых методах, где шифрование происходит знак за знаком. Однако при использовании ад-дитивных методов преобразование может осуществляться сразу над целым ма-шинным словом и метод приобретает признаки блочного.

Шифрование методом подстановки (замены). В этом, наиболее простом, методе символы шифруемого текста заменяются другими символами, взятыми из одного (моноалфавитная подстановка) или нескольких (полиалфавитная подста-новка) алфавитов. Самой простой разновидностей является прямая замена, когда буквы шифруемого текста заменяются другими буквами того же самого или неко-торого другого алфавита.

Шифрование методом перестановки. Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов.

Шифрование методом гаммирования. Суть этого метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он по-лучил название "гаммирование".

Комбинированные методы шифрования. Как уже отмечалось, одним из важнейших требований, предъявляемых к системе шифрования, является ее стойкость. Однако повышение стойкости любого метода шифрования приводит, как правило, к существенному усложнению самого процесса шифрования и увеличе-нию затрат ресурсов (времени, аппаратных средств, уменьшению пропускной способности и т.п.).

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов.

Комбинировать можно любые методы шифрования и в любом количестве, однако на практике наибольшее распространение получили следующие комбинации:

- подстановка + гаммирование;
- перестановка + гаммирование;
- гаммирование + гаммирование;
- подстановка + перестановка.

Типичным примером комбинированного шифра является национальный стандарт США криптографического закрытия данных (DES).

Кодирование. Одним из средств криптографического закрытия информа-ции, также имеющим длительную историю практического использования, является кодирование, под которым понимается замена элементов закрываемых данных некоторыми цифровыми, буквенными или комбинированными сочетаниями - ко-дами. Нетрудно заметить, что между

кодированием информации и ее шифрова-ни-ем подстановкой существует значительная аналогия. Однако между этими мето-дами можно найти различия.

При шифровании подстановкой заменяемыми единицами информации яв-ляются символы алфавита, и, следовательно, шифрованию могут подвергаться любые данные, для фиксирования которых используется выбранный алфавит. При кодировании замене подвергаются смысловые элементы информации, поэтому для каждого специального сообщения в общем случае необходимо использовать свою систему кодирования. Правда, в последнее время разработаны специальные коды, имеющие целью сократить объем информации при ее записи. Специфика этих ко-дов заключается в том, что для записи часто встречающихся символов использу-ются короткие двоичные коды, а для записи редко встречающихся - длинные. Примером такого кода может служить код Хоффмана.

К другим видам криптографического закрытия отнесены рассече-ние/разнесение и сжатие данных. Рассечение/разнесение данных состоит в том, что массив защищаемых данных рассекается на такие элементы, каждый из кото-рых не позволяет раскрыть содержание защищаемой информации, и выделенные таким образом элементы размещаются в различных зонах памяти. Обратная про-цедура называется сборкой данных. Совершенно очевидно, что алгоритм разнесе-ния и сборки данных должен сохраняться в тайне.

Шифрование с открытым ключом. Одно из главных ограничений исполь-зования обычных криптографических систем связано с трудностью распространения ключей. Диффи и Хеллман, а также, независимо от них, Меркль, показали, что можно исключить защищенный канал передачи ключей и при этом обеспечить защиту при передаче сообщений по незащищенному каналу без осуществления каких-либо предварительных мероприятий. Как видно из рис. 3.2, между отправи-телем и получателем допускается двухсторонний обмен, но перехватчик здесь пассивный и только слушает [25].

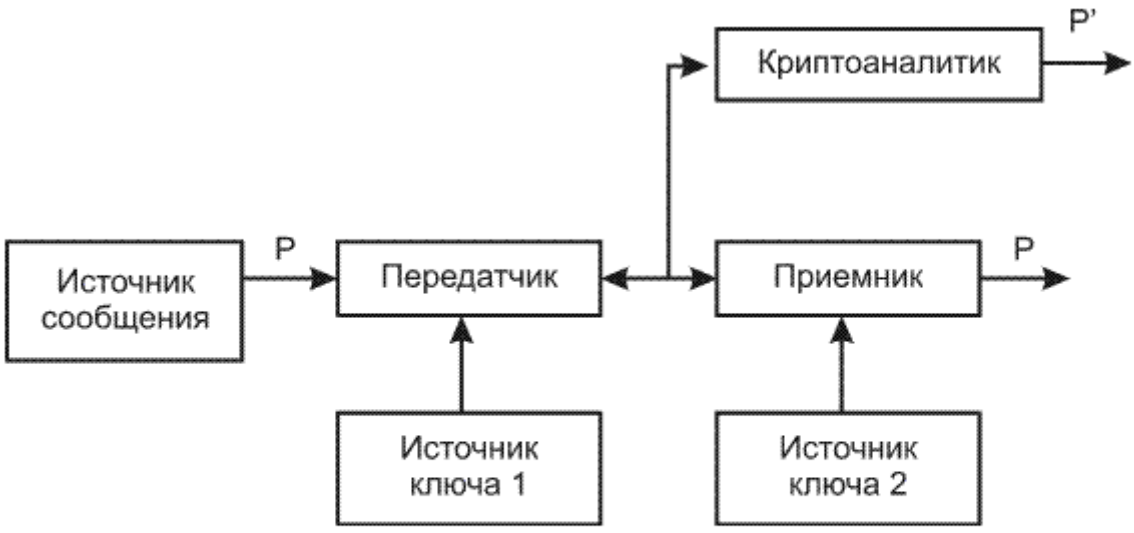

Рис. 3.2. Поток информации в криптографической системе с открытым ключом

В отличие от обычных систем, в которых ключ должен сохраняться в секре-те, системы, допускающие такую работу, называются системами с открытым ключом. Для решения

этой проблемы предлагаются два подхода. Первый подход за-ключается в том, что при открытом распространении ключей отправитель и полу-чатель могут договориться о ключе, используемом в обычной криптографической системе. Несмотря на то, что противник слушает все переговоры, он не в состоя-нии вычислить ключ и не может понять последующего обмена сообщениями. Второй подход реализует криптографические системы с открытыми ключами, в которых для шифрования используются разные ключи.

Цифровая подпись. Идея цифровой подписи (ее еще называют электронной подписью) была предложена Диффи и Хеллманом. Суть ее заключается в использовании односторонней функции с секретом FK. В настоящее время эта идея реа-лизована в большом количестве систем передачи данных. Сообщение, подписан-ное цифровой подписью, можно представить в виде пары (x, y), где x - сообще-ние, FK: x y -односторонняя функция, известная всем взаимодействующим абонентам, y - решение уравнения FK(y) = x.

Криптографическая система RSA. Как бы ни были сложны и надежны классические криптографические системы, их слабым местом при практической реализации является проблема распределения ключей. Для того чтобы был возмо-жен обмен конфиденциальной информацией между двумя абонентами, ключ дол-жен быть сгенерирован одним из них, а затем каким-либо образом передан друго-му в конфиденциальном порядке. В общем случае для передачи ключа по каналам связи требуется использование еще одной криптосистемы, для которой вновь воз-никает проблема распределения ключей и т.д.

Для решения этой и ряда других проблем были предложены криптосистемы с открытым ключом, называемые также асимметричными криптосистемами.

Перед отправкой сообщения адресату исходный текст шифруется открытым (общедоступным) ключом адресата. Алгоритм шифрования построен таким образом, что расшифровывание сообщения возможно только с использованием личного (секретного) ключа адресата.

Впервые модель системы секретной связи с открытым ключом была пред-ложена Диффи и Хеллманом в 1976 г.

Суть этой модели состоит в том, что ключ известен полностью только полу-чателю сообщения и представляет собой тройку чисел k = (e, d, n), где подключ e служит ключом шифрования, а ключ d - ключом расшифровывания. При этом только d является секретным (личным) ключом. Стойкость системы обеспечивает-ся за счет особых свойств шифрпреобразования, которое представляет собой так называемую одностороннюю функцию с лазейкой. Вычисление значения такой функции (от открытого текста и параметра e) должно быть несложным, в то же время ее обращение должно быть вычислительно нереализуемым без знания сек-ретной информации, "лазейки", связанной с секретным ключом d.

В криптосистеме с открытым ключом сообщение, предназначенное абонен-ту, зашифровывается отправителем с помощью ключа e и расшифровывается получателем с помощью ключа d. Если шифрпреобразование действительно являет-ся односторонней функцией, то сам отправитель не в состоянии расшифровать сформированную им криптограмму.

Широко известным примером криптосистемы с открытым ключом является криптосистема RSA, разработанная в 1977 г. и получившая название в честь её создателей: Ривеста, Шамира и Эйдельмана. Стойкость этой системы основывает-ся на сложности

обратимости степенной функции в кольце вычетов целых чисел по составному модулю n (при надлежащем выборе модуля).

Стандарт шифрования данных DES. Стандарт шифрования данных

DES (Data Encryption Standard) принят в США в 1977 г. в качестве федерального. В стандарт входит описание блочного шифра типа шифра Файстеля, а также раз-личных режимов его работы, как составной части нескольких процедур крипто-графического преобразования данных. Обычно под аббревиатурой DES понимает-ся именно блочный шифр, который в стандарте соответствует процедуре шифро-вания в режиме электронной кодовой книги (ECB - E1ectronic Codebook Mode). Название вызвано тем, что любой блочный шифр является простым подстановочным шифром и в этом отношении подобен кодовой книге.

3.5.2. Скремблирование

В речевых системах связи известно два основных метода закрытия речевых сигналов, различающихся по способу передачи по каналам связи: аналоговое скремблирование и дискретизация речи с последующим шифрованием. Под скремблированием понимается изменение характеристик речевого сигнала, таким образом, что полученный модулированный сигнал, обладая свойствами неразбор-чивости и неузнаваемости, занимает ту же полосу частот, что и исходный сигнал.

Каждый из этих методов имеет свои достоинства и недостатки. Так, для аналоговых скремблеров характерно присутствие при передаче в канале связи фрагментов исходного открытого речевого сообщения, преобразованного в час-тотной и (или) временной области. Это означает, что злоумышленники могут по-пытаться перехватить и проанализировать передаваемую информацию на уровне звуковых сигналов. Поэтому ранее считалось, что, несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры могут обеспе-чивать лишь низкую или среднюю, по сравнению с цифровыми системами, сте-пень закрытия. Однако новейшие алгоритмы аналогового скремблирования спо-собны обеспечить не только средний, но очень высокий уровень закрытия.

Цифровые системы не передают какой-либо части исходного речевого сигнала. Речевые компоненты кодируются в цифровой поток данных, который смешивается с псевдослучайной последовательностью, вырабатываемой ключевым генератором по одному из криптографических алгоритмов. Подготовленное таким образом сообщение передается с помощью модема в канал связи, на приемном конце которого проводятся обратные преобразования с целью получения открыто-го речевого сигнала.

Технология создания широкополосных систем, предназначенных для закрытия речи, хорошо известна, а ее реализация не представляет особых трудностей. При этом используются такие методы кодирования речи, как АДИКМ (адаптивная дифференциальная и импульсно-кодовая модуляция), ДМ (дельта-модуляция)

и т.п. Но представленная таким образом дискретизированная речь может передаваться лишь по специально выделенным широкополосным каналам связи с полосой пропускания 4,8…19,2 кГц. Это означает, что она не пригодна для передачи по линиям телефонной сети общего пользования, полоса пропускания которых 3400 Гц. В таких случаях используются узкополосные системы, главной трудностью при реализации которых является высокая сложность алгоритмов сжатия речевых сигналов, осуществляемого в вокодерных устройствах (см. разд. 4.4).

Посредством дискретного кодирования речи с последующим шифрованием всегда достигалась высокая степень закрытия. Ранее этот метод имел ограниченное применение в имеющихся узкополосных каналах из-за низкого качества вос-становления передаваемой речи. Достижения в развитии технологий низкоскоро-стных дискретных кодеров позволили значительно улучшить качество речи без снижения надежности закрытия.

Аналоговые скремблеры. Аналоговые скремблеры подразделяются [25]:

" на речевые скремблеры простейших типов на базе временных и (или) частотных перестановок речевого сигнала (рис. 3.3);

" комбинированные речевые скремблеры на основе частотно-временных перестановок отрезков речи, представленных дискретными отсчетами, с применением цифровой обработки сигналов (рис. 3.4).

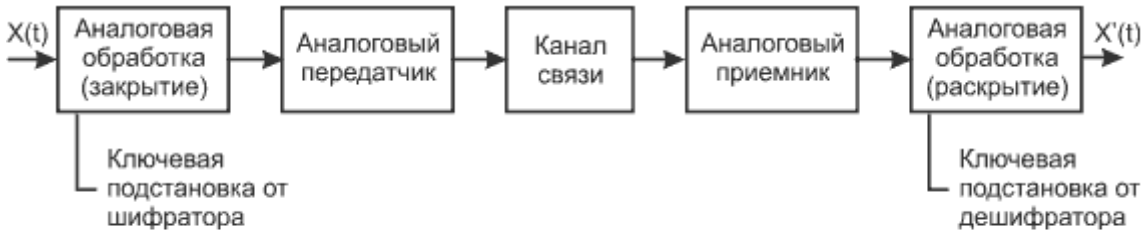

Рис. 3.3. Схема простейшего речевого скремблера

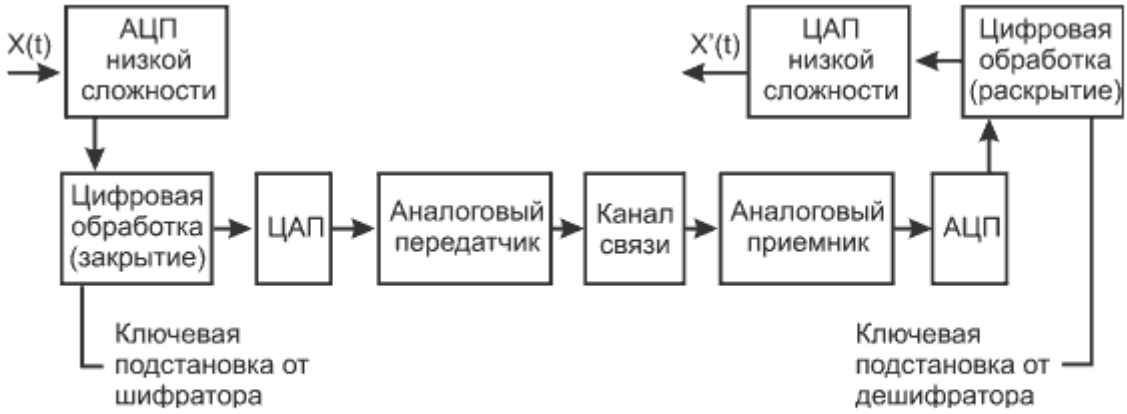

Рис. 3.4. Схема комбинированного речевого скремблера

Цифровые системы закрытия речи подразделяются на широкополосные (рис. 3.5) и узкополосные (рис. 3.6).

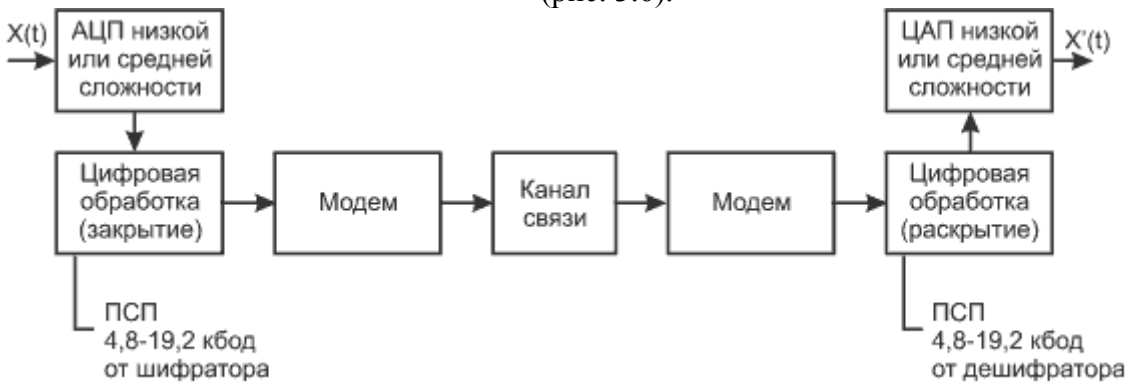

Рис. 3.5. Схема широкополосной системы закрытия речи

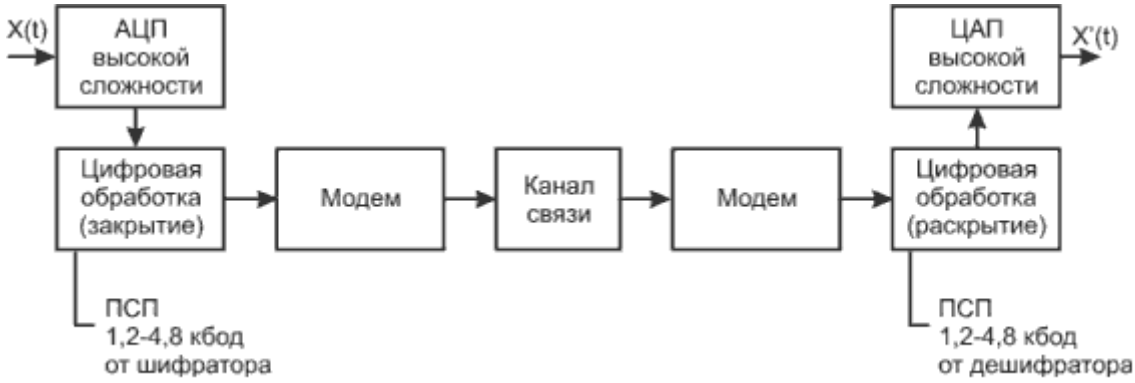

Рис. 3.6. Схема узкополосной системы закрытия речи

Тактический, или низкий, уровень используется для защиты информации от прослушивания посторонними лицами на период, измеряемый от минут до дней. Существует много простых методов и способов обеспечения такого уровня защиты с приемлемой стойкостью.

Стратегический, или высокий, уровень защиты информации от перехвата используется в ситуациях, подразумевающих, что высококвалифицированному, технически хорошо оснащенному специалисту потребуется для дешифрования перехваченного сообщения период времени от нескольких месяцев до нескольких лет.

По результатам проведенных исследований можно составить диаграммы (рис 3.7), показывающие взаимосвязь между различными методами закрытия речевых сигналов, степенью секретности и качеством восстановленной речи [25].

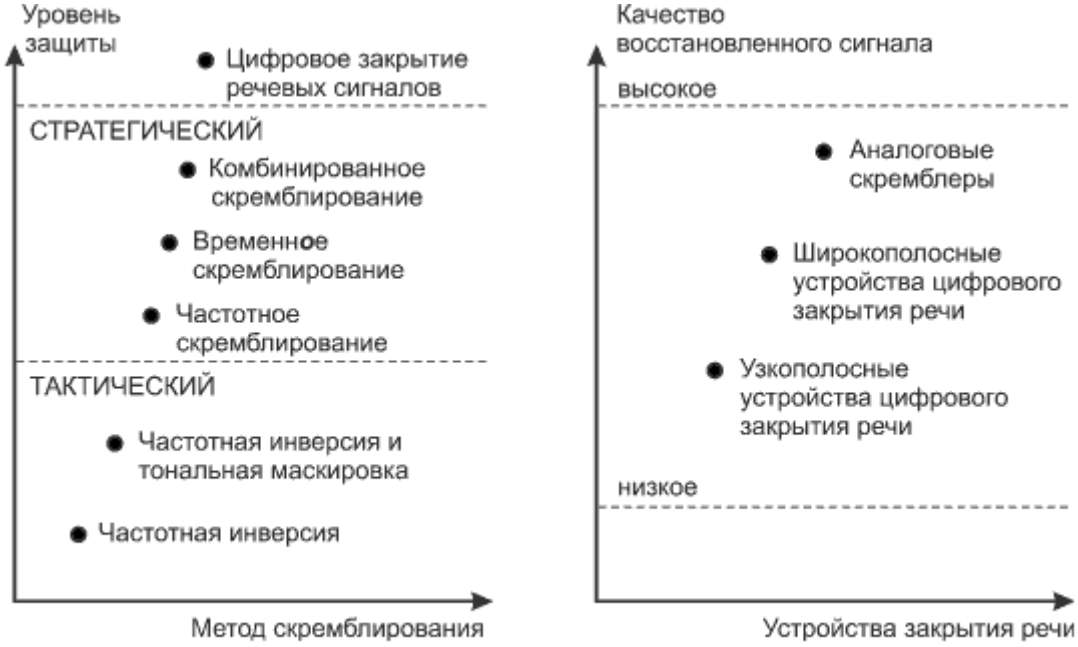

Рис. 3.7. Сравнительные диаграммы разных методов закрытия речевых сигналов

Цифровое скремблирование. Альтернативным аналоговому скремблированию речи является шифрование речевых сигналов, преобразованных в цифровую форму, перед их передачей (см. рис. 3.5). Этот метод обеспечивает более высокий уровень закрытия по сравнению с описанными выше аналоговыми методами. В основе устройств, работающих по такому принципу,

лежит представление речево-го сигнала в виде цифровой последовательности, закрываемой по одному из крип-тографических алгоритмов [25]. Передача данных, представляющих дискретизи-рованные отсчеты речевого сигнала или его параметров, по телефонным сетям, как и в случае устройств шифрования алфавитно-цифровой и графической информации, осуществляется через устройства, называемые модемами.

Основной целью при разработке устройств цифрового закрытия речи является сохранение тех ее характеристик, которые наиболее важны для восприятия слушателем. Одним из путей является сохранение формы речевого сигнала. Это направление применяется в широкополосных цифровых системах закрытия речи. Однако более эффективно использовать свойства избыточности информации, со-держащейся в человеческой речи. Это направление разрабатывается в узкополос-ных цифровых системах закрытия речи.

Наиболее распространенными типами вокодеров являются полосные и с линейным предсказанием. Целью любого вокодера является передача параметров, характеризующих речь и имеющих низкую информационную скорость. Полосный вокодер достигает эту цель путем передачи амплитуды нескольких частотных по-лосных речевого спектра. Каждый полосовой фильтр такого вокодера возбуждает-ся при попадании энергии речевого сигнала в его полосу пропускания. Так как спектр речевого сигнала изменяется относительно медленно, набор амплитуд вы-ходных сигналов фильтров образует пригодную для вокодера основу. В синтезато-ре параметры амплитуды каждого канала управляют коэффициентами усиления фильтра, характеристики которого подобны характеристикам фильтра анализато-ра. Таким образом, структура полосового вокодера базируется на двух блоках фильтров - для анализа и для синтеза. Увеличение количества каналов улучшает разборчивость, но при этом требуется большая скорость передачи. Компромисс-ным решением обычно становится выбор 16…20 каналов при скорости передачи данных около 2400 бит/с.

Наибольшее распространение среди систем цифрового кодирования речи с последующим шифрованием получили системы, основным узлом которых являются вокодеры с линейным предсказанием речи (см. раздел 4.4).

Защите информации может способствовать скрытие самого факта её переда-чи, одним из возможных путей для этого служат системы связи на широкополосных и сверхширокополосных сигналах.

Одно из перспективных направлений защиты информации сформировали современные методы стеганографии [15,25]. Слово **стеганография** в переводе с греческого буквально означает тайнопись (steganos - тайна, секрет; graphy - за-пись). Стеганография представляет собой совокупность методов, основывающих-ся на различных принципах, которые обеспечивают сокрытие самого факта суще-ствования секретной информации в той или иной среде, а также средств реализа-ции этих методов. К ней можно отнести огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные (скрытые) каналы, средства связи с плавающими частотами, голо-графия и т.д.

4. Свойства и характеристики речевых сигналов

Речевой сигнал относится к акустическим сигналам, то есть механическим колебаниям среды распространения - газов, жидкостей и твердых тел. Различают первичные и вторичные

акустические сигналы [4]. К первичным относятся аку-стические сигналы, порождаемыми процессами в природе - речь, музыка, разно-образные шумы. Вторичные акустические сигналы воспроизводятся электроаку-стическими устройствами после прохождения первичных сигналов по трактам связи и вещания. Акустические сигналы характеризуются динамическим диапазо-ном, средним уровнем, частотным диапазоном и спектром. Временных характери-стики акустических сигналов характеризуют изменение уровней и частотных параметров во времени.

Речевые сигналы являются переносчиками речевой информации, являющей-ся акустической формой языка (наряду с текстовой его формой). Кроме смыслового (языкового) содержания речевой сигнал несёт и другую информацию - об ин-дивидуальности говорящего, его эмоциональном и физическом состоянии и т.п. Речевые технологии объединяют в себе методы и средства использования речевых сигналов для реализации разнообразных задач речевого взаимодействия между людьми, а также человека с техническими средствами. Помимо передачи речи по каналам связи сюда относятся задачи распознавания и синтеза речи, идентифика-ции и верификации диктора, оценки психофизиологического состояния говорящего, диагностики некоторых заболеваний и т.д. В сфере речевых технологий накоп-лен большой арсенал методов обработки речевых сигналов, который с успехом может быть использован для защиты речевой информации.

4.1. Модели речеобразования и восприятия речи.

Для эффективного применения речевых технологий необходимо представ-лять специфику порождения и восприятия речевых сигналов.

Акустический речевой сигнал возникает в результате сложных координиро-ванных движений, происходящих в ряде органов, вся совокупность которых называется речевым аппаратом (рис. 4.1, А). Легкие со всей дыхательной мускулатурой обеспечивают развитие давлений и возникновение воздушных потоков в речевом тракте. Речевой тракт включает в себя артикуляторные органы - гортань с голосо-выми связками, ротовую и носовую полости язык, нёбную занавеску, зубы и губы. Источниками возбуждения голосовых колебаний являются колебания голосовых связок (голосовой источник), а также турбулентные шумы, возникающие при про-хождении потока воздуха через сужения речевого тракта (шумовой источник).

На рисунке 4.1 [23] представлены три различные интерпретации схемы ре-чевого тракта человека.

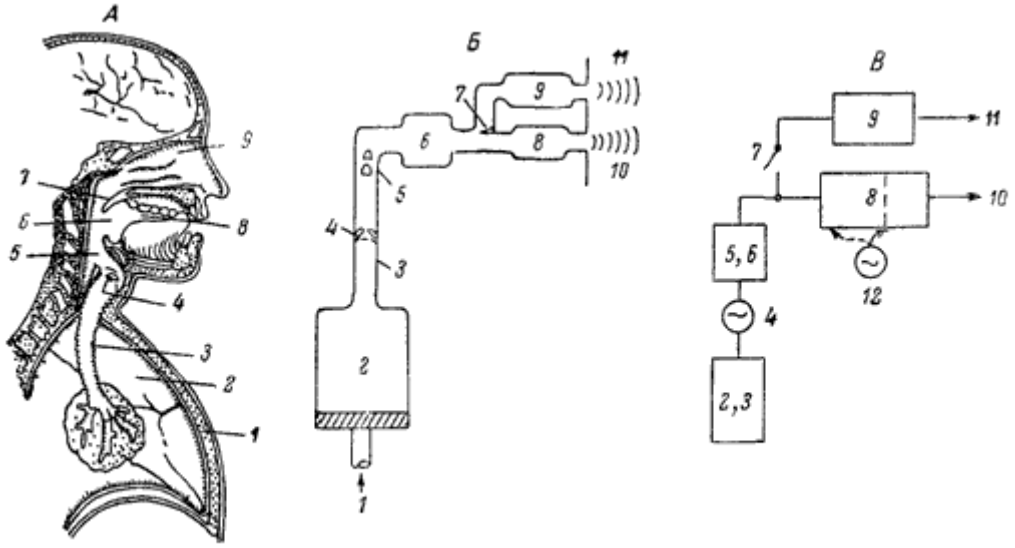

Рис. 4.1. Схемы речеобразующего аппарата.

А - анатомическое изображение: 1 - грудная клетка, 2 - легкие, 3 - тра-хея, 4 - голосовые связки, 5 - гортанная трубка, 6 - полость глотки, 7 - нёбная занавеска, 8 - полость рта, 9 - полость носа.

Б - функциональные элементы; 1 - сила дыхательных мышц, 2 - объем лёгких, 3 - трахея, 4 - голосовые связки, 5 - гортанная трубка, 6 - полость глотки, 7 - небная занавеска, 8 - полость рта, 9 - полость носа, 10 - излучение из ротового отверстия, 11 - излучение из носовых отверстий.

В -эквивалентная блок-схема: 2, 3 - емкость легких и трахеи, 4 - голосо-вой источник колебаний, 5, 6 - емкость гортани и глотки, 7 - механизм небной занавески, 8 - ёмкость полости рта, 9 - ёмкость полостей носа, 10 - выходной сигнал ротового тракта, 11 - выходной сигнал носового тракта, 12 - шумовой источник.

В зависимости от положения и движения артикуляторных органов в процес-се речеобразования, а также источника возбуждения речевых колебаний возникают различные звуки речи, акустическое представление которых представляет со-бой звучащие абстрактные аналоги букв алфавита - фонемы. Основное отличие фонем от символов алфавита состоит в их существенно большей изменчивости: вариантов произношения фонем значительно больше вариантов написания букв вследствие существенно большего числа факторов, влияющих на параметры фор-мируемого звука. Кроме того, процесс формирования звуков является динамиче-ским, протяжённым во времени, при этом инерционность артикуляторных движе-ний приводит к взаимовлиянию соседних звуков, в результате фонем в идеальном их выражении просто не существует - они реализуются в виде позиционных вари-антов - аллофонов, изменчивость которых ещё выше. В экспериментальной фоне-тике существует классификация звуков речи по способу и месту образования, учи-тывающая, например, степень подъёма языка и продвинутости его вперёд или на-зад, положение и степень раскрытия губ и т.п. Учитывается также характер источ-ника возбуждения и место его образования (для шумных звуков). Эти признаки часто имеют противопоставительный характер (высокий-низкий, передний-задний и т.п.). Это дало основание построить систему так называемых дифференциаль-ных признаков, являющихся перспективной

системой установления связи между фонетическими и акустическими характеристиками речевых сигналов, необходимого для решения многих задач речевых технологий.

Важную роль как при исследовании процессов речеобразования, так и тех-нической реализации каналов речевой коммуникации играют физические и математические модели речевого тракта. Выбор адекватной физической модели и её математическая формализация позволяют строить системы синтеза речи, то есть машинного генерирования речевого сигнала. Модели речевого тракта играют важ-ную роль также при построении систем связи на основе передачи сжатых кодиро-ванных речевых сообщений. Одной из наиболее простых и распространённых яв-ляется модель на основе отрезков цилиндрических труб различного диаметра и длины, аппроксимирующих форму речевого тракта. На этой модели базируется акустическая теория речеобразования в её классическом виде, а также большое число методов кодирования и восстановления речевых сигналов.

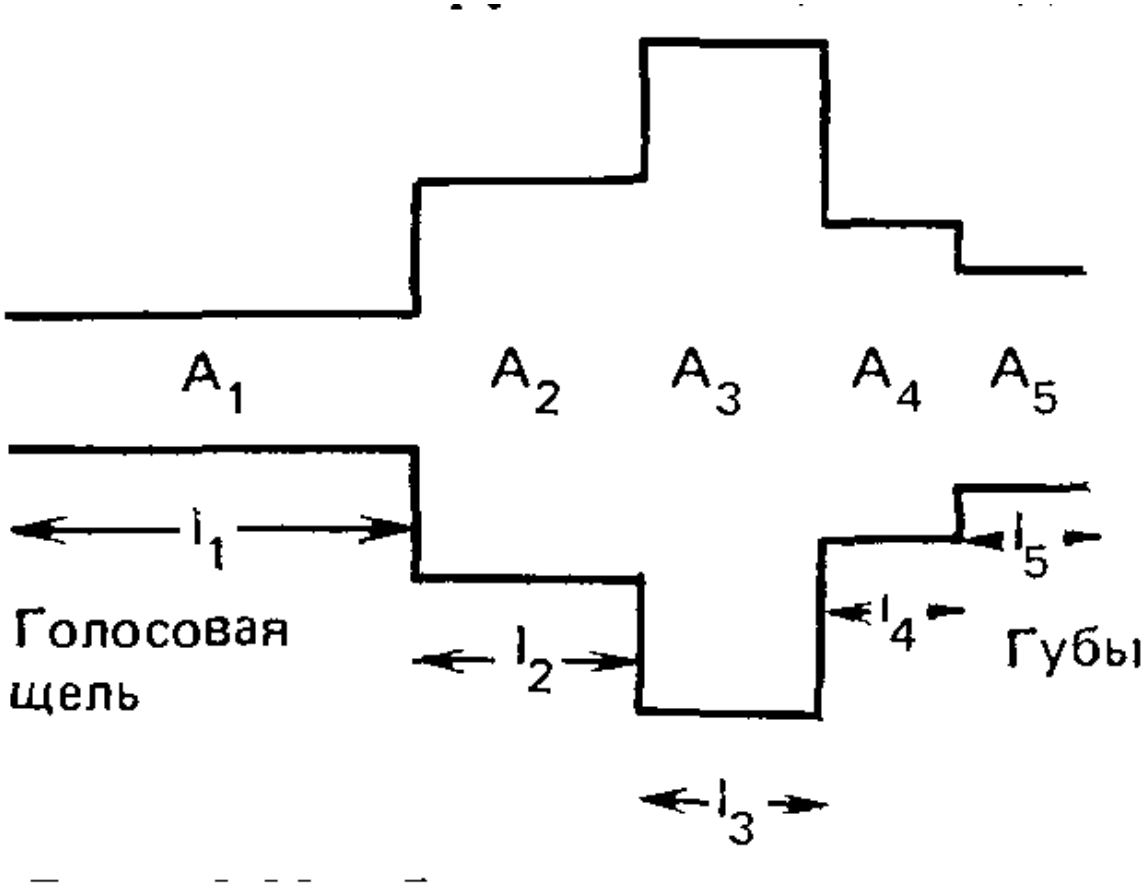

Рис. 4.2. Соединение пяти труб без потерь [3]

Площади поперечного сечения труб выбираются так, чтобы результирую-щая оказалась равной функции площади поперечного сечения голосового тракта A(x). Если количество труб велико, а их длина достаточно мала, то можно ожи-дать, что резонансные частоты такого соединения будут близки к резонансным частотам трубы с непрерывной функцией площади сечения. Поскольку при таком приближении пренебрегают потерями на трение, теплопроводность и вибрацию стенок, можно ожидать, что ширина резонансных областей будет отличаться от ширины таких областей в сложной модели, учитывающей и потери. Потери в го-лосовой щели и около губ могут быть учтены, и это позволяет достаточно точно описать резонансные свойства речевого сигнала.

Более полные модели речевого тракта должны учитывать непрерывный и гладкий характер изменения поперечного сечения речевого тракта и его формы, упругость и податливость стенок тракта, динамику движений артикуляторных ор-ганов и т.п. Это приводит к существенно более сложным математическим моде-лям, реализованным в настоящее время лишь в экспериментах [18]. Потенциально именно артикуляторный синтез может обеспечить наилучшую натуральность и разборчивость синтезированной речи.

Знание механизмов и особенностей слухового восприятия обеспечивает возможности как улучшения качества систем связи, так и искажения речевых сообщений, необходимого для защиты речевой информации. Этапы обработки рече-вого сигнала в слуховой системе человека включают:

- приём и первичный анализ акустического сигнала;
- выделение акустических событий и признаков;
- лингвистическая интерпретация речевого сообщения.

Первый из этих этапов осуществляется периферической слуховой системой, состоящей из наружного, среднего и внутреннего уха (рис. 4.3, 4.4) [23].

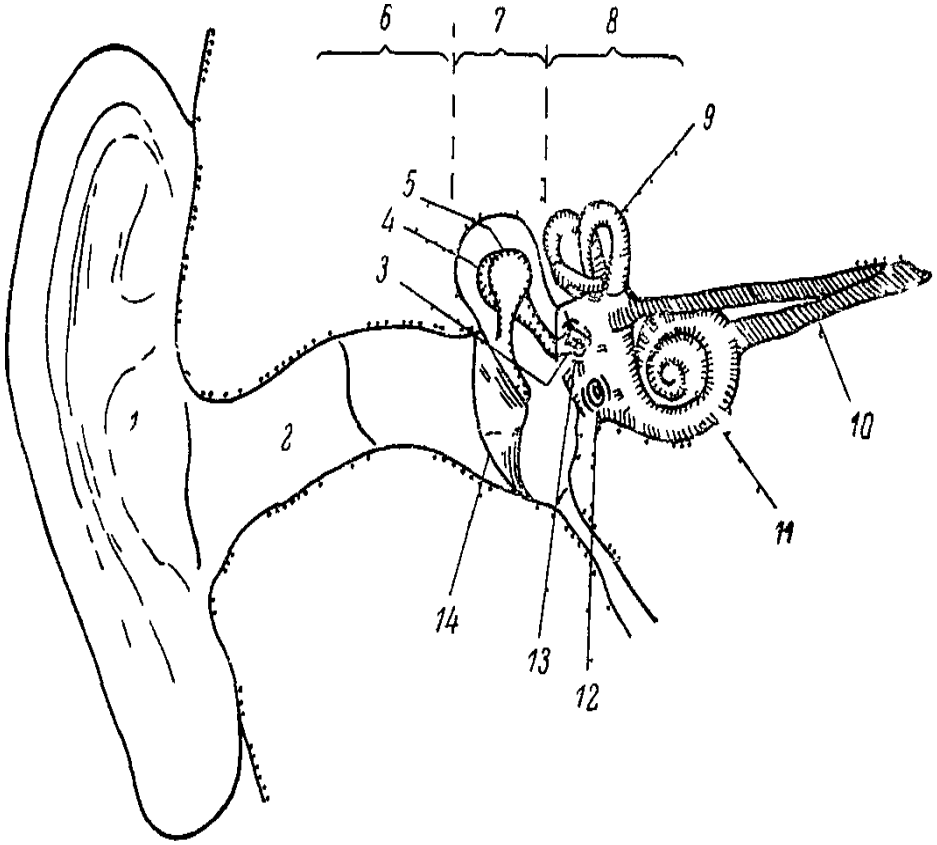

Рис. 4.3. Схематическое изображение уха человека

1 - ушная раковина; 2 - наружный слуховой проход; 3, 4, 5 - слуховые косточки: соответственно стремечко, наковаленка и молоточек; 6 - наружное ухо; 7 - сред-нее ухо; 8 - внутреннее ухо; 9 - вестибулярный аппарат; 10 - слуховой нерв;

11 - улитка; 12 - круглое окно; 13 - овальное окно; 14 - барабанная перепонка

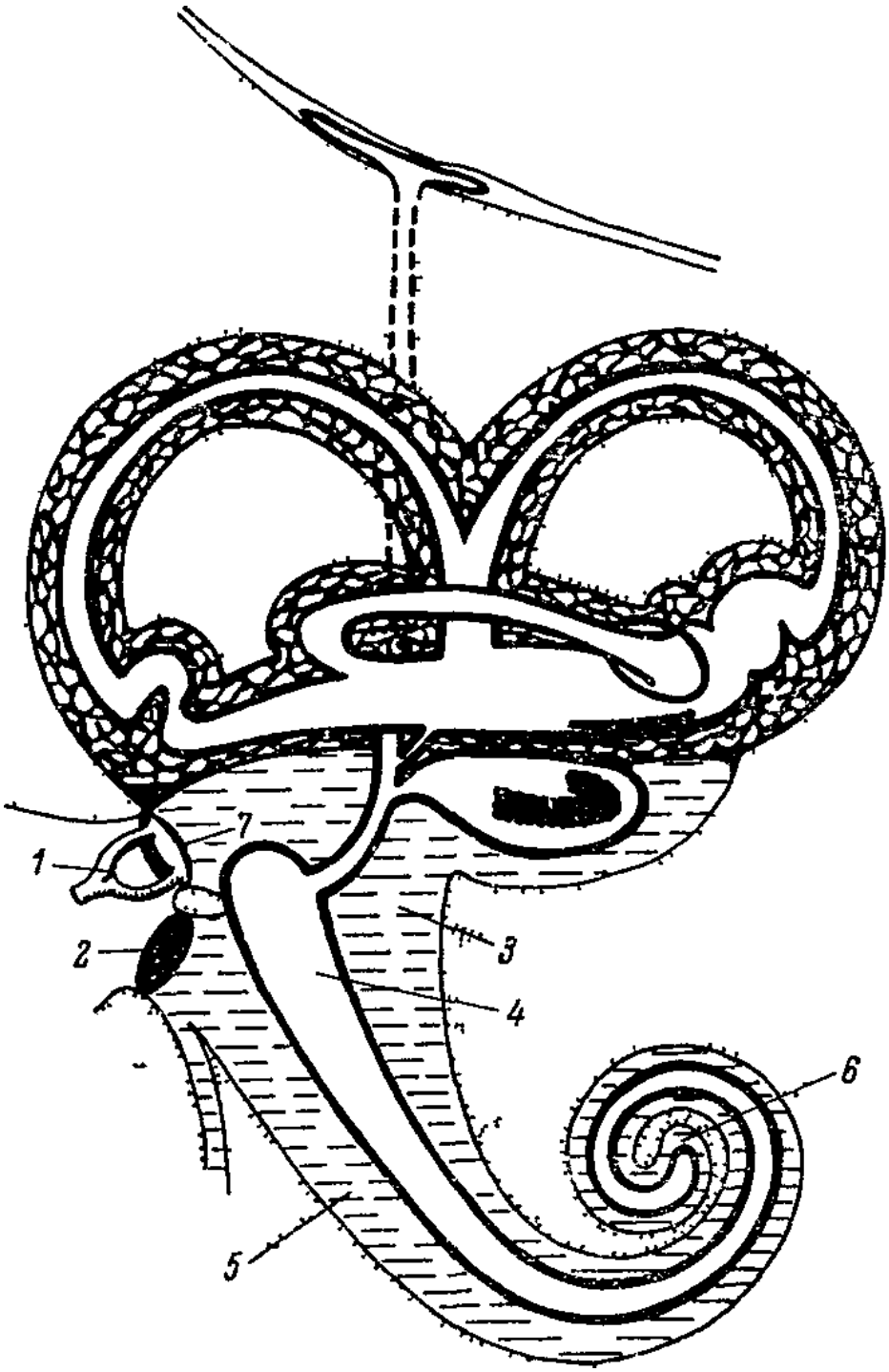

Рис. 4.4. Схематическое изображение строения внутреннего уха млекопитающих

1 - стремечко; 2 - круглое окно; 3 - вестибулярный канал;

4 - средний, или кохлеарный, канал;

5 - тимпанальный ка-нал; 6 - геликотрема;

7 - овальное окно

Ушная раковина и наружный слуховой проход обеспечивают направленный приём звуковых колебаний и коррекцию частотной характеристики. Среднее ухо передаёт звуковые колебания барабанной перепонки во внутреннее ухо, усиливая уровень звукового давления примерно на 30 дБ. Во внутреннем ухе происходит амплитудный и частотный анализ звуковых

колебаний (базилярная мембрана), ре-зультаты которого преобразуются в нервные импульсы кортиевым органом и передаются в слуховой нерв.

Характеристики слухового восприятия в значительной степени определяются свойствами слухового нерва. Чувствительность слуха к восприятию и разделению звуковых колебаний различной частоты и интенсивности описывается доста-точно сложными зависимостями, учёт которых при построении технических уст-ройств обработки звуковых сигналов позволяет существенно улучшить их харак-теристики.

Основными свойствами слуха, которые необходимо учитывать, являются зависимости субъективного восприятия высоты и громкости звука от объективно измеренных частоты и уровня звукового давления. Фундаментальные результаты исследования особенностей слухового восприятия получены в работе [26]. На рис. 4.5 и 4.6 показаны названные зависимости.

Например, при частотном анализе целесообразно деформировать равномерную частотную шкалу (герц) в шкалу мелов, вводя таким образом психоакустическую коррекцию получаемых описаний речевых сигналов. Наиболее часто этот приём используется при распознавании речи.

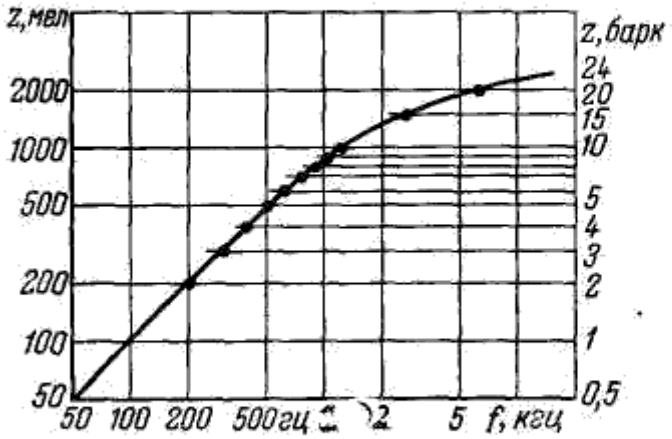

Рис 4.5. Высота тона и шкала частотных групп в зависимости от частоты

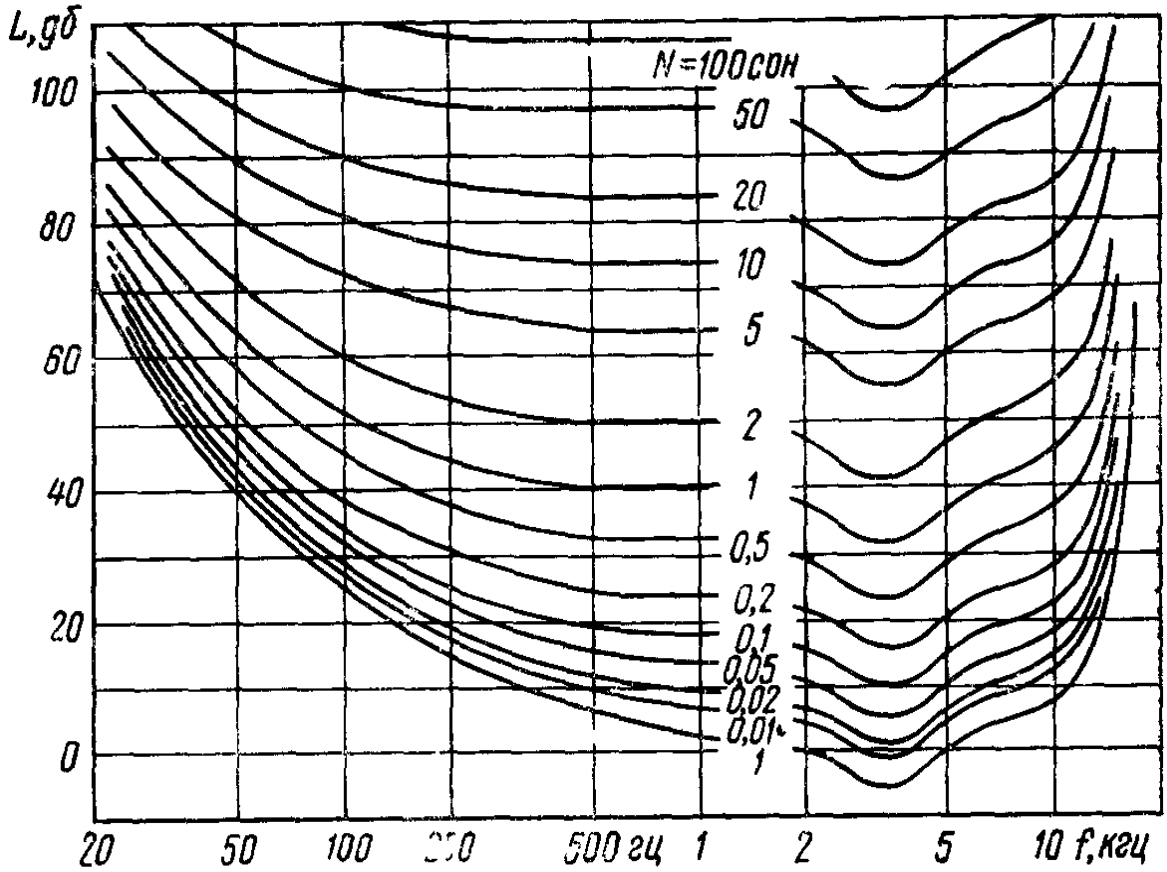

Рис. 4.6. Кривые равной громкости на плоскости слышимости в плоском звуковом поле

Модели обработки речи в центральной нервной системе наиболее сложны и наименее изучены, однако общие представления о слуховом восприятии можно сформулировать следующим образом. По перцептивной картине, сформированной на нижних уровнях слухового анализа, выделяются акустические события и при-знаки, несущие информацию о фонетической структуре речевого сообщения. Да-лее происходит обобщение этой информации, и формируются картины верхних уровней восприятия, соответствующих лексическому, синтаксическому, семанти-ческому и прагматическому уровню языковых знаний, соотносимых со всем мно-жеством ассоциаций, сформированных в процессе жизнедеятельности человека. Таким образом, решение частной проблемы искусственного интеллекта - моделирования восприятия речи человеком - возможно в рамках построения полной модели интеллекта. Соответственно частные (промежуточные) решения этой проблемы должны учитывать максимум априорной информации о речи и предметной области, о которой идёт речь в текущем диалоге.

4.2. Методы обработки речевых сигналов

С точки зрения теории обработки сигналов речевой сигнал представляет собой непрерывный нестационарный случайный процесс, что накладывает ограничения на набор методов и алгоритмов его обработки. Речевые сигналы характери-зуются параметрами, которые могут быть оценены на конечных интервалах вре-мени, в течение которых сигнал можно считать стационарным. Эти параметры от-ражают вероятностные свойства, временные, спектральные, корреляционные характеристики речевых сигналов.

4.2.1. Алгоритмы анализа речевых сигналов

Наиболее распространённым и физически интерпретируемым считается спектрально-временное представление речевых сигналов, т.е. совокупность "спектральных срезов", полученных на следующих друг за другом (или частично пере-крывающихся) интервалах времени. Основой такого анализа является дискретное преобразование Фурье. Методы его аппаратной и программной реализации (в том числе быстрые и рекуррентные алгоритмы), свойства и специфические для речи параметры алгоритмов подробно изложены в литературе по цифровой обработке сигналов [3, 5]. Для реализации спектрального анализа возможно применение раз-личных ортогональных базисов. Для сокращения объёма информации применяется аппроксимации огибающих речевых спектров, в том числе спектрально-полосный анализ, ранее широко применявшийся в аналоговых анализаторах спектра. Предельным случаем спектрально-временного представления является динамический спектральный анализ [19], когда оценка текущего спектра обновляется для каждого дискретного отсчёта речевого сигнала.

Ограничением спектрального представления по Фурье является противоречие между "разрешением" анализа по частоте и времени. Увеличение интервала оценивания спектра обеспечивает повышение разделения спектральных состав-ляющих, но приводит к "размыванию", то есть сглаживанию динамики изменения спектра по времени, и наоборот. При этом точность Фурье-анализа одинакова для любой частоты, в то время как спектральная чувствительность слухового анализа-тора имеет более сложный, нелинейный характер. Считается, что преодоление этих противоречий возможно с использованием **вейвлет-анализа,** базирующегося в изначальном варианте на свёртке анализируемого сигнала с семейством масштабируемых по времени однотипных весовых функций, что эквивалентно динамическому анализу с помощью гребёнки цифровых фильтров с конечно-импульсными характеристиками. В настоящее время этот подход интенсивно развивается.

Речевой сигнал может быть представлен в виде свёртки сигнала возбуждения с переходной (фильтровой) функцией речевого тракта. На свойствах систем, гомоморфных относительно свёртки, основан гомоморфный анализ [3]. Идея его применения для анализа речи состоит в возможности выделить из речевого сигна-ла отдельно как параметры возбуждения, так и речевого тракта. Отсюда вытекают методы оценивания основного тона, а также параметров для распознавания и ко-дирования речи, называемых кепстральными коэффициентами. Известны вариан-ты гомоморфного анализа, позволяющие учитывать психоакустические свойства слуха.

Линейное предсказание, математически относящееся к авторегрессионным методам спектрального оценивания, применительно к речевым сигналам получило специфическую интерпретацию и применение [3]. Коэффициенты, оценивае-мые в процедуре линейного предсказания, могут быть интерпретированы как па-раметры модели речевого тракта в виде отрезков труб. Спектр, оцениваемый на основе линейного предсказания, хорошо аппроксимирует передаточную функцию речевого тракта, правда, содержащую лишь нули, что ограничивает его

возможно-сти (либо вынуждает увеличивать число оцениваемых коэффициентов) при опи-сании некоторых согласных звуков. Кроме этого, коэффициенты линейного предсказания имеют значительный разброс по величине, что затрудняет их использо-вание при распознавании и кодировании. Более удобными являются вычисляемые на основе параметров линейного предсказания линейные спектральные пары, более устойчивые к шумам.

Кроме спектральных параметров, для анализа, кодирования-декодирования речи необходимо оценивать и другие характеристики, в частности, **основной тон** (ОТ) - частоту колебаний речевых складок, а также признаки характера и наличия голосовой активности "тон - шум - пауза".

Периодичность речевых сигналов выявляется с помощью временных, спектральных и корреляционных характеристик. Существуют локальные и усреднённые оценки ОТ.

Первые предназначены для обнаружения каждого периода колебаний связок, в том числе интервалы их смыкания и размыкания. В простейшем случае импульсы ОТ возможно выделять, анализируя амплитуду речевой волны, сглаженной фильтром нижних частот с полосой пропускания, равной полосе частот ОТ (до 200 Гц для мужчин и до 350 Гц для женщин). Импульсам ОТ при этом будут соот-ветствовать локальные максимумы амплитуды. Однако такой простой метод не даёт хороших результатов, особенно для высоких голосов, когда частота ОТ соиз-мерима с частотой первой форманты (впрочем, эта проблема относится и ко всем другим методам оценивания ОТ). Работоспособные процедуры локального выде-ления ОТ представляют собой достаточно изощрённые комбинации нескольких оценок, дополняющих и уточняющих друг друга.

Один из наиболее распространённых методов интегрального оцениваня частоты ОТ основан на свойстве периодичности автокорреляционной функции (АКФ) для периодических сигналов. Основному тону и его гармоникам на корреляцин-ной картине соответствуют равноотстоящие локальные максимумы, амплитуда ко-торых постепенно убывает с ростом номера гармоники. Решение о наличии и час-тоте ОТ принимается с учётом значимости первого макимума АКФ и, возможно, наличии, периодичности и скорости убывания дополнительных максимумов. Су-ществуют также методы выделения периодичности на основе спектральых и го-моморфных представлений речевых сигналов, причём в последнем случае разные компоненты кепстра дают возможность оценивания как ОТ, так и формантных частот.

Следует отметить, что современные подходы к оцениванию параметров речевого сигнала отличаются довольно изощрённым, комплексным подходом к решению задач оценивания, использующим параллельно и/или последовательно не-сколько разнотипных процедур оценивания с целью взимного дополнения и уточ-нения оценок и получения в результате полного и точного описания.

4.2.2. Методы цифрового кодирования речевой информации

Исторически аналоговые методы передачи и кодирования речи развились раньше цифровых, и, хотя роль цифровых методов постоянно возрастает, аналоговые устройства как относительно простые и отработанные, продолжают приме-няться достаточно широко. Однако новые разработки, особенно для качественных и ответственных приложений, базируются на применении цифровых методов.

Идея кодирования речевых сообщений изначально была связана с двумя основными предпосылками: сокращением полосы частот, занимаемой в канале связи, а также засекречиванием содержимого сообщений. С развитием цифровых ме-тодов кодирование стало необходимым элементом процесса передачи речевой ин-формации (по крайней мере, аналого-цифровое и цифро-аналоговое преобразование) при сохранении первоначальных предпосылок. Системы кодирования речи условно могут быть разделены на две группы: с кодированием формы и с кодиро-ванием параметров сигнала. К первой группе относятся методы представления сигнала в виде последовательности его отсчётов с возможным сокращением объё-ма информации, необходимой для передачи одного отсчёта. Это импульсно-кодовая модуляция (ИКМ), адаптивная ИКМ (АИКМ), адаптивная дифференци-альная ИКМ (АДИКМ), а также дельта-модуляция (ДМ) и её модификации - адап-тивная ДМ и дельта-сигма модуляция. Все эти виды модуляции обеспечивают пе-редачу формы сигнала, и при сокращении объёма передаваемых данных качество речи снижается. Скорости потоков данных при этом могут быть уменьшены отно-сительно исходной всего в 2…4 раза.

Вокодеры (от Voice Coder) - устройства кодирования-декодирования речи, преобразующие речевой сигнал в набор изменяющихся во времени параметров, передаваемых по линии связи, и восстанавливаемых на приёмном конце с приме-нением методов синтеза речи. В зависимости от применяемых параметров и мето-дов синтеза различают полосные, формантные, гомоморфные, с линейным пред-сказанием, ортогональные и другие вокодеры. Современные вокодеры обеспечи-вают передачу речи со скоростями от 2,4 Кбит/с при сохранении хорошей разбор-чивости и даже узнаваемости диктора. Предельного сокращения скорости переда-чи (60 бит/с) позволят достичь фонемные вокодеры, однако для их реализации не-обходимо решить проблемы распознавания речи и идентификации индивидуаль-ных особенностей диктора. В качестве примера приведём краткое описание одно-го из современных телекоммуникационные стандартов для передачи речи по циф-ровым каналам связи, сетям мобильной связи и компьютерным сетям.

Рекомендация ITU-T G.723.1 - это двухскоростной вокодер для мультимедийных коммуникаций, являющийся частью семейства стандартов H.324. Вокодер работает на скоростях 5,3 и 6,3 кбит/с. Большая скорость передачи обеспечивает лучшее качество. Меньшая скорость дает хорошее качество речи и предоставляет разработчикам дополнительные возможности при построении систем. В любой момент на границе кадра допустимо переключение скорости передачи.

Входной речевой сигнал с частотой дискретизации 8 КГц разбивается на кадры длиной 30мс, что соответствует 240 16-битным отсчетам в линейном законе. Дополнительно существует задержка (look ahead), которая составляет 7,5 мс, что определяет суммарную алгоритмическую задержку равной 37,5 мс. Дополни-тельные задержки в практическом приложении этого алгоритма возникают по сле-дующим причинам:

- процессы кодирования и декодирования требуют некоторого времени;
- время передачи по каналу;
- задержка мультиплексирования при комбинировании аудиоданных с другими видами данных.

Кодер основывается на принципе линейного предсказания с анализом через синтез и минимизирует взвешенный сигнал ошибки. Он оперирует кадрами речевого сигнала длиной 240 отсчетов. Сначала каждый кадр пропускается через фильтр верхних частот для удаления

постоянной составляющей, а затем делится на 4 подкадра длиной по 60 отсчетов. Для каждого подкадра вычисляются пара-метры фильтра линейного предсказания (Linear Prediction Coder Filter) 10-го по-рядка, а для последнего подкадра эти параметры квантуются с использованием предсказывающего векторного квантователя (Predictive Split Vector Quantizer - PSVQ). Для передачи декодеру осуществляются преобразование LPC-коэффициентов в вектор линейных спектральных пар (LSP) и его последующее квантование. Неквантованные LPC-коэффициенты используются для построения кратковременного взвешивающего фильтра, через который пропускается кадр сигнала для получения взвешенного речевого сигнала. Для каждых двух подкад-ров по схеме с разомкнутой петлей вычисляется период основного тона (open-loop pitch period), лежащий в диапазоне от 18 до 142 отсчетов.

Дальнейшая обработка происходит по подкадрам. С учётом ранее вычисленной оценки периода основного тона строится гармонический шумопонижающий фильтр (harmonic noise shaping filter). Для получения импульсного отклика используется комбинированный фильтр, состоящий из синтезирующего LPC-фильтра, формантного взвешивающего фильтра и harmonic noise shaping filter. На основании оценки периода основного тона и импульсного отклика вычисляется предсказатель основного тона 5-го порядка в схеме с замкнутой петлей. Диффе-ренциал вычисляется в небольшой окрестности полученной ранее оценки периода основного тона. Вклад предсказателя периода основного тона вычитается из пер-воначального целевого вектора. И оценка основного тона, и дифференциал пере-даются от кодера к декодеру.

Наконец, аппроксимируется непериодическая компонента возбуждения. Для большей скорости используется возбуждение, полученное по схеме MP-MLQ, а для меньшей скорости - по схеме ACELP.

Работа декодера также построена на покадровом принципе. Сначала декодируются индексы квантованных LPC-коэффициентов, затем строится синтезирующий LPC-фильтр. Для каждого подкадра декодируется возбуждение и адаптивной, и фиксированной кодовых книг и подается на синтезирующий фильтр. Адаптив-ный постфильтр состоит из формантного постфильтра и реверсивного (forward-backward) постфильтра основного тона. Сигнал возбуждения передается на пост-фильтр основного тона, затем на синтезирующий фильтр, а выход синтезирующе-го фильтра подается на вход формантного постфильтра. Блок масштабирования усиления сохраняет уровень энергии на входе формантного постфильтра. В деко-дере также существует механизм восстановления потерянных кадров, который включается в случае несовпадения контрольного бита. Восстановление основыва-ется на типе последнего полученного кадра и сохраненном контексте декодера.

Помимо "чистой" рекомендации G.723.1, существуют "приложение A" (annex A). Приложение A добавляет в кодер часть классификации входного речевого сигнала. Это так называемый VAD - voice activity detector (буквально - де-тектор голосовой активности). Классификатор входного сигнала определяет, что в данный момент присутствует на входе - речь или пауза. В моменты пауз битовый поток понижается с 6,3 (или 5,3) кбит/с до 1 кбит/с и менее. В моменты пауз в би-товом потоке передается информация о структуре фонового шума, чтобы на сто-роне декодера у слушателя не возникало дискомфорта от "чистых" пауз между фразами - то есть присутствует генератор комфортного шума. Более того, инфор-мация о паузном кадре передается декодеру только в случае изменения характери-стик шума. В противном случае на выходе кодера устанавливается признак такого типа кадра, а на декодер никакой информации не

поступает. Полное описание ре-комендации можно найти в документе: ITU-T Recommendation G.723.1 Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s (доступен на сайте http://www.itu.int).

4.3. Методы моделирования и экспериментального исследования алгоритмов защиты речевой информации

Для эффективной реализации алгоритмов обработки сигналов необходимо до начала проектирования аппаратно-программного обеспечения убедиться в работоспособности выбранных методов, оценить необходимые для реализации ресурсы и допустимые ограничения, провести исследование функционирования алгоритмов на моделях и реальных сигналах и, наконец, подготовить тестовые дан-ных для отладки и верификации аппаратно-программных средств. Это является необходимым условием в особенности при реализации алгоритмов обработки ре-чевых сигналов, для которых (речевых сигналов) не существует адекватных моде-лей. Экспериментального подтверждения требуют и современные алгоритмы обработки речи в приложении к задаче повышения эффективности средств ЗРИ.

Существующие инструментальные средства работы со звуковыми сигналами не в полной мере удовлетворяют требованиям речевых технологий. Сигнальные редакторы в большинстве своём ориентированы скорее на работу с музыкой и аудиозаписью и не включают достаточно полный набор специфических методов обработки речевых сигналов (формирование описаний, распознавание и синтез речи, идентификация и верификация дикторов и т.д.). Относительно небольшой набор редакторов, позиционирующихся как речевые, например, SpeechLab, Colea, Praat, являются (за исключением, может быть, Colea) закрытыми для модификации и дополнения, и также не охватывают всех известных методов обработки речевых сигналов.

Библиотеки звуковых и сигнальных приложений пакетов Matlab и LabView являются неплохими средствами, позволяющими развить набор средств исследования алгоритмов обработки сигналов в требуемом направлении. Развитие этих двух пакетов в последнее время происходит в направлении сближения и взаимо-проникновения с целью расширения возможностей Matlab по вводу-выводу и ви-зуализации сигналов и пополнению арсенала математических алгоритмов в Lab-View на основе взаимодействия фирм-разработчиков. Возможность включения ал-горитмов пользователя в программы LabView на уровне динамически связывае-мых библиотечных модулей (dll) обеспечивает так необходимую гибкость и рас-ширяемость средств исследования. Дополнительным аргументом в пользу приме-нения названных инструментальных средств является достаточно широкое рас-пространение их в отечественных университетах благодаря программам академической поддержки.

Следует подчеркнуть важность эффективной визуализации речевых сигналов и результатов их обработки. Основанием для такого утверждения является сложность речевых сигналов, разнообразие и многоэтапность методов анализа и преобразования сигналов, требующие контроля не только конечных, но и проме-жуточных результатов. Известно, что данные в текстовой, табличной форме труд-нее анализировать и интерпретировать, чем в случае удачного графического, "об-разного" представления. Для визуализации речевых сигналов применяются различные способы, основными из них являются:

- осциллографический: представление сигнала в виде графика в функции времени, при этом детальность масштаба времени желательно изменять таким образом, чтобы можно было

наблюдать как мгновенные изменения сиг-нала (форму волны), так и изменение амплитуды на более длительных отрезках времени (форму огибающей);

 спектральный, или частотный: отображение распределения интенсивности сигнала по частоте в интервалах времени, соответствующих квазистацио-нарным участкам сигнала (для речевых сигналов интервал стационарности оценивается в 10...40 мс);

 динамические спектрограммы (сонаграммы), отображающие квазитрёхмерное представление речи в координатах "время-частота-интенсивность", при этом последний параметр отображается оттенками цвета, либо яркости мо-нохромного изображения. Такое представление является одним из наиболее информативных, позволяя экспертам даже "читать" сонаграмы, т.е. визуально распознавать произносимый текст;

 комбинированное отображение, представляющее три вышеперечисленные формы в виде "проекций" параметров на оси частоты и времени, а также плоскость "время-частота".

Пример комбинированного представления результатов анализа слитно произнесённой фразы представлен на рис. 5.9.

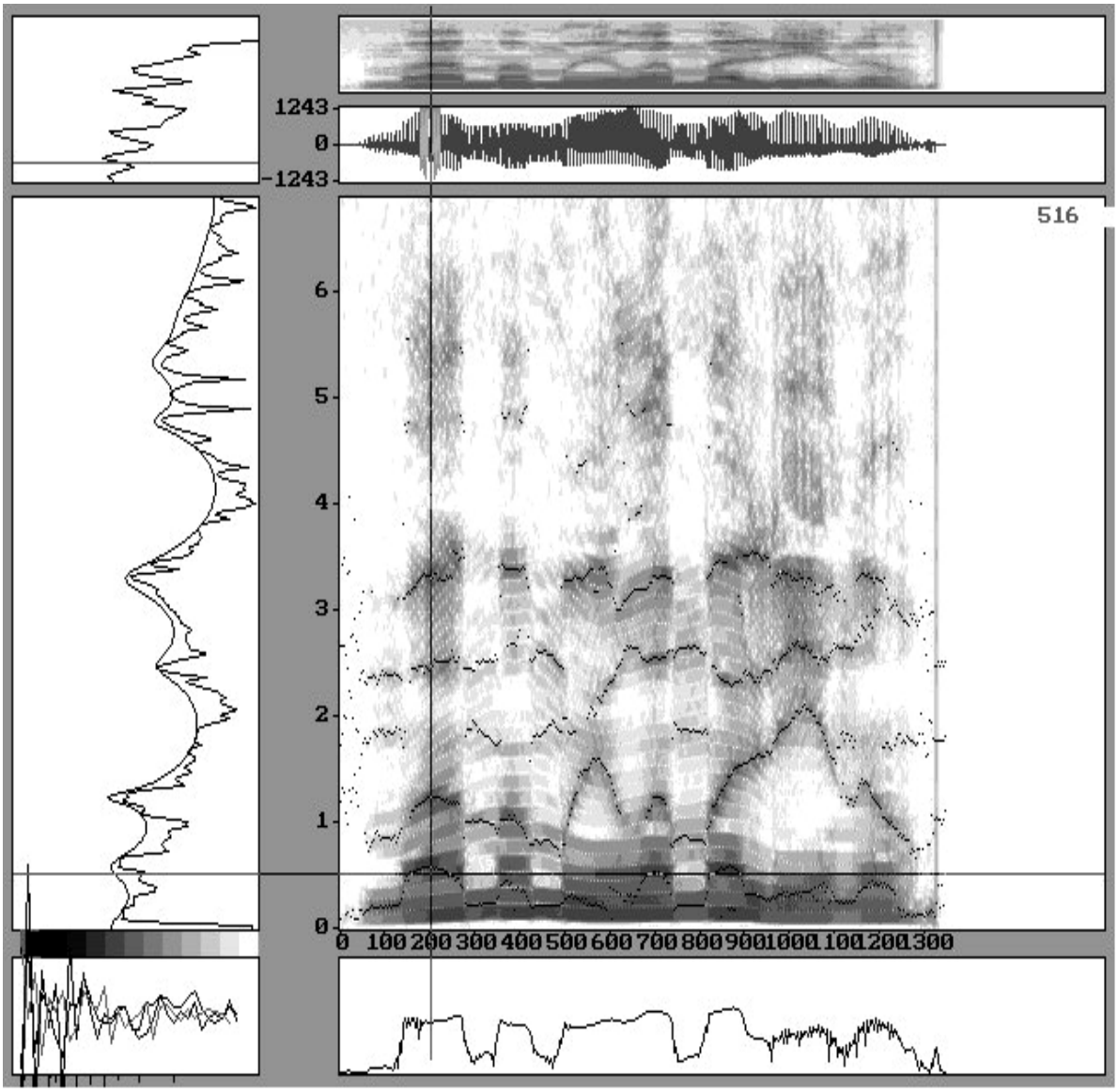

Рис.5.9. Пример визуализации результатов анализа речевого сигнала

В правой части экрана отображаются развёртки по времени (горизонтальная ось) следующих параметров (сверху вниз):

 динамическая спектрограмма нелинейно преобразованного по частоте спектра (психоакустическое сглаживание);
 огибающая амплитуды речевого сигнала;
 динамическая спектрограмма, построенная на основе преобразования Фурье (вертикальная ось - частота);
 график изменения во времени коэффициента Фурье, соответствующего положению горизонтальной линии курсора (частота около 500 Гц).

В левой части отображены частотные срезы соответственно аппроксимированного и исходного спектров (два верхних прямоугольника), при этом на спектр Фурье (более неравномерный) наложен спектр, полученный из модели линейного предсказания. Нижний прямоугольник отображает значения коэффициентов пред-сказания и корреляции в функции номера коэффициента (по горизонтали).

Программа курса предполагает знакомство обучаемых с имеющимися инструментальными средствами и исследование примеров моделирования алгоритмов обработки сигналов с применением упомянутых пакетов на практических заняти-ях. Предусмотрено изучение интерфейсов программных средств, а также ряда конкретных алгоритмов обработки сигналов.

5. Аппаратно-программная реализация средств защиты речевой информации

Цепочка передачи речевой информации в общем виде может быть представлена следующими звеньями: субъект произнесения - акустическая среда - электроакустический преобразователь (микрофон) - предварительный усилитель - тракт обработки и/или передачи - выходной усилитель - выходной электроаку-стический преобразователь (динамик) - субъект восприятия. Современные сред-ства обработки сигналов преимущественно реализуются на основе цифровых ме-тодов, поэтому обязательным элементом построения средств речевых коммуника-ций являются аналого-цифровые (АЦП) и цифро-аналоговые (ЦАП) преобразователи.

5.1. Аналого-цифровые и цифро-аналоговые преобразователи

Существует несколько основных типов АЦП. На рис. 5.1. [http://www.efo.ru/doc/Silabs/Silabs.pl?2089] показаны возможности основных архитектур АЦП в зависимости от разрешения и частоты дискретизации.

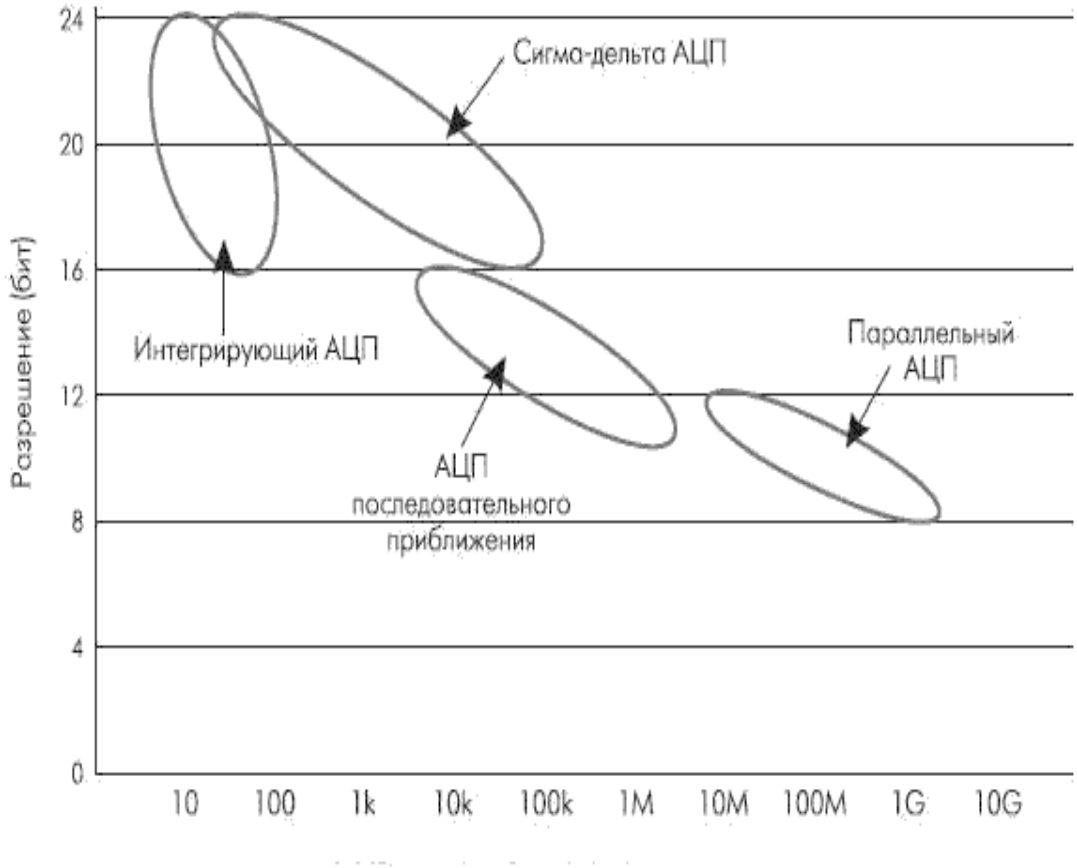

Рис. 5.1. Типы АЦП - разрешение в зависимости от частоты дискретизации

По указанным параметрам для обработки речевых сигналов подходят АЦП последовательного приближения и сигмадельта АЦП. Однако существует ещё целый ряд параметров, по которым оценивается применимость преобразователей для конкретных типов сигналов, это характеристики статических и динамических погрешностей.

Статические погрешности определяются как отклонения статической характеристики преобразования от идеальной и характеризуются следующими параметрами:

 аддитивная погрешность (Offset Error) определяется смещением начала статической характеристики от начала координат в единицах значения веса младшего значащего разряда (LSB);

 мультипликативная погрешность (Full-Scale Error) (погрешность полной шкалы) представляет собой разность между идеальной и реальной переда-точными характеристиками в точке максимального выходного значения при условии нулевой аддитивной погрешности (смещение отсутствует), что про-является как изменение наклона передаточной функции;

 дифференциальная нелинейность (DNL) измеряется как неравномерность значений разностей между соседними уровнями квантования по всей шкале относительно величины LSB;

 интегральная нелинейность измеряется как отклонение уровней напряжения, при которых происходит кодовый переход, от соответствующих идеальных значений, точно кратных LSB;
 погрешность квантования - это погрешность отклонения шага квантования от идеального значения LSB.

При сопоставимой разрядности преобразователей требуемые статические погрешности легче обеспечить для преобразователей последовательного приближения.

Динамические характеристики АЦП обычно определяют с помощью спектрального анализа, по результатам выполнения быстрого преобразования Фурье (БПФ) над массивом выходных значений АЦП, соответствующих некоторому тестовому входному сигналу, (рис. 5.2).

Рис.5.2. Спектр синусоидального сигнала 1000 Гц после аналого-цифрового преобразования

Нулевая гармоника соответствует основной частоте входного сигнала. Все остальное представляет собой шум, который содержит гармонические искажения, тепловой шум и шум квантования. Некоторые составляющие шума генерируются самим АЦП, некоторые могут поступать на вход АЦП из внешних цепей. Гармо-нические искажения, например, могут

содержаться в измеряемом сигнале и одновременно генерироваться АЦП в процессе преобразования.

Отношение "сигнал/шум" (SNR) - это отношение среднеквадратического значения величины входного сигнала к среднеквадратическому значению величины шума (за исключением гармонических искажений), выраженное в децибелах:

$$\mathrm{SNR(dB)} = 20\log\left[V_{signal}(\mathrm{rms}) / V_{noise}(\mathrm{rms}) \right]$$

Нелинейность в результатах преобразования данных приводит к появлению гармонических искажений. Такие искажения наблюдаются как "выбросы" в спектре частот на четных и нечетных гармониках измеряемого сигнала. Эти искажения определяют как общие гармонические искажения (THD). Они определяются как:

$$THD = 20\log\left[\frac{\sqrt{V_2^2 + V_3^2 + \ldots + V_n^2}}{V_1} \right]$$

Отношение "сигнал/шум и искажения" (SiNAD) более полно описывает шумовые характеристики АЦП. SiNAD учитывает величину как шума, так и гармонических искажений по отношению к полезному сигналу. SiNAD рассчитывается по следующей формуле

$$SiNAD = \mathbf{20\log}\left[\frac{V_1}{\sqrt{V_2^2 + \ldots + V_n^2 + V_{noise}^2}} \right]$$

В наибольшей степени на качество передачи сигналов влияет величина максимальной побочной гармоники. Динамический диапазон, свободный от гармоник, представляет собой разницу между величиной измеряемого сигнала и наибольшим пиком искажений и обозначается как SFDR.

При передаче и воспроизведении звука наиболее заметными являются именно динамические искажения, в первую очередь необходимо обеспечить наибольший динамический диапазон и наименьшие нелинейные искажения. По этим параметрам наилучшие свойства показывают сигма-дельта преобразователи, по-этому для звуковых приложений предпочтительно применение преобразователей именно этого типа.

Обратное преобразование из цифровой формы представления в аналоговую реализуется цифро-аналоговыми преобразователями (ЦАП), при этом для оценки их качества применяются те же характеристики, что и для АЦП. Поэтому в трак-тах обработки звука и речи также наиболее распространены сигма-дельта ЦАП.

5.2. Современная элементная база цифровой обработки сигналов

Интенсивное развитие микроэлектронных технологий обеспечивает удвоение степени интеграции микросхем каждые два года. Это позволяет, с одной стороны, повышать структурную и функциональную сложность микросхем и за счёт этого реализовывать более сложные методы обработки информации, а с другой стороны, при неизменной сложности снижать энергопотребление и массогабарит-ные характеристики аппаратуры. Можно даже предположить, что развитие техно-логий обработки сигналов идёт в основном по экстенсивному варианту, поскольку рост вычислительных возможностей заметно опережает темпы создания принци-пиально новых методов и алгоритмов. Однако реальное практическое применение многих

известных эффективных методов до сих пор сдерживалось именно огра-ничениями по возможностям их реализации с требуемыми ограничениями по экс-плуатационным характеристикам. Поэтому освоение достижений современной микроэлектроники позволит существенно повысить научно-технический уровень, эффективность и доступность современных средств защиты информации.

Технические средства защиты речевой информации представляют собой, по сути, устройства обработки сигналов. Поэтому для реализации методов защиты речевой информации целесообразно применение вычислительных средств, про-блемно-ориентированных на класс алгоритмов цифровой обработки сигналов (ЦОС) - цифровые сигнальные процессоры (ЦСП). Применение таких процессо-ров для ЦОС существенно эффективнее применения сравнимых по сложности процессоров общего назначения по критерию цена - производительность.

Особенностями архитектуры ЦСП, обеспечивающими их преимущества при реализации алгоритмов ЦОС, являются:

- повышенная степень параллелизма, предусматривающая совмещение во времени нескольких действий;
- аппаратная поддержка специфических для ЦОС и массово выполняемых операций - умножение со сложением, циклические вычисления и т.д.;
- аппаратная поддержка типичных для ЦОС структур данных, в частности, кольцевых буферов.

Цифровые сигнальные процессоры производит целый ряд фирм, среди которых наиболее известны Texas Instruments, Motorola, Analog Devices, NEC, AT&T, Zilog и др. На отечественном рынке электронных компонентов (как и во всём мире) значительную долю представляют ЦСП Texas Instruments; фирма Motorola не предпринимает серьёзных усилий по продвижению своей линейки ЦСП на рынок России в отличие от Analog Devices, имеющей своё представительство и дист-рибьюторов, поставляющих продукцию этой фирмы в Россию. ЦСП Analog Devices создавались несколько позже, чем аналогичные устройства других фирм, но архитектура этих процессоров оказалась весьма удачной, что обеспечивает их преимущества по производительности при сопоставимой тактовой частоте. Это, а также доступность на отечественном рынке делает ЦСП призводства Analog Devices достаточно привлекательными для разработок на их основе аппаратуры обработки сигналов.

Производители предлагают несколько семейств ЦСП, различающихся по основным классификационным параметрам - разрядности, форме представления данных, объёму и типам памяти, набору периферийных узлов на кристалле.

Например, Analog Devices выпускает в настоящее время четыре основные семейства ЦСП:

- ADSP-21xx - 16-разрядные с фиксированной запятой;
- ADSP-BF5xx - 16/32-разрядные с фиксированной запятой;
- SHARC: ADSP-21xxx - 32/40-разрядные с плавающей и фиксированной запятой;
- TigerSHARC: ADSP-TSxxx - 32/40-разрядные с плавающей и фиксированной запятой и аппаратной поддержкой многопроцессорных вычислений.

Символы "x" в обозначениях семейств означают цифры, отражающие конкретную модель ЦСП в семействе. Подробную информацию о назначении, составе и характеристиках семейств ЦСП можно получить на сайте http://www.analog.com.ru/.

5.3. Цифровые сигнальные процессоры ADSP-219x

Поскольку все семейства ADSP имеют сходную архитектуру, здесь ограничимся знакомством с представителем последнего на настоящее время поколения 16-разрядных ЦСП с фиксированной точкой ADSP-2191 [10].

Цифровые сигнальные процессоры семейства ADSP-219x - это высокопроизводительные 16-разрядные процессоры, предназначенные для использования в системах связи, измерительных приборах, системах управления промышленным производством, в системах обработки речи, в медицинских и военных приложени-ях, а также в других областях.

5.3.1. Структура процессора

ЦСП состоят из процессорного ядра (на блок-схеме рис. 5.3 показано слева) и интегрированных на кристалле периферийных устройств (в правой части схемы) и, таким образом, представляют собой однокристальную микро-ЭВМ.

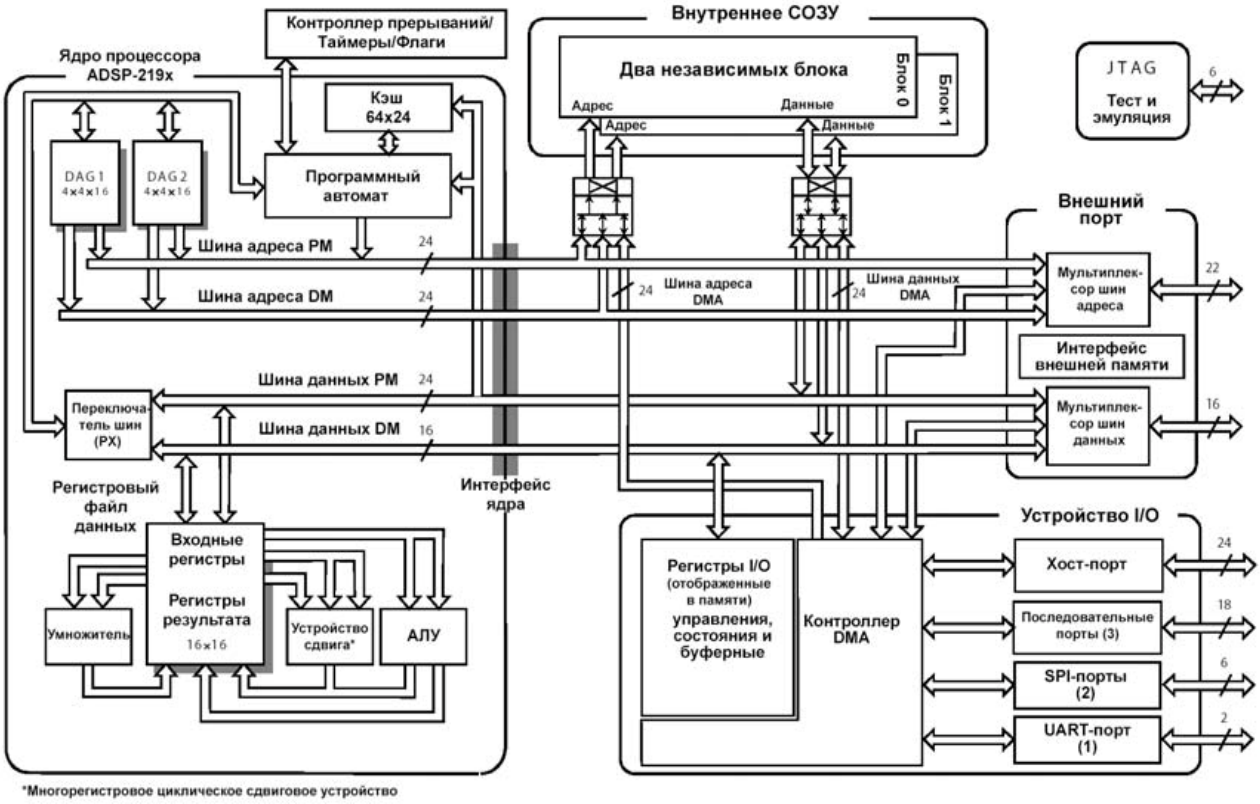

Рис. 5.3. Блок-схема процессора ADSP-2191

Здесь явно проявляются упомянутые выше особенности архитектуры ЦСП. Расширенная Гарвардская архитектура предусматривает наличие двух логически и схемно разделённых адресных пространств - программ и данных. Повышенная степень параллелизма выражена следующими решениями:

- наличие трёх магистралей с шинами адреса и данных для доступа к двум адресным пространствам - внутренней памяти программ и данных, а также прямого доступа к внутренней памяти со стороны подсистемы ввода-вывода (Input/Output - I/O) обеспечивает совмещение во времени операций выборки команд из памяти программ, операндов из памяти данных и программ, а также операций ввода-вывода;
- наличие трёх независимых вычислительных узлов - арифметико-логического устройства (ALU), умножителя-аккумулятора (MAC) и сдвигателя (SHIFTER), каждый из которых связан с регистровым файлом, реализо-ванным как многопортовое СОЗУ, позволяет эффективно

манипулировать входными и выходными данными, используя результат выполнения опера-ции на любом из узлов в качестве входных данных для других узлов.

Аппаратурная поддержка типичных для ЦОС операций реализуется наличием следующих возможностей:

- умножитель-аккумулятор за один цикл выполняет перемножение двух 16-разрядных операндов и сложение произведения с накопленной в регистре результата суммой предыдущих операций, что при разрядности этого регистра и сумматора 40 разрядов обеспечивает выполнение 256 таких операций без необходимости проверки признаков переполнения результата;
- программный автомат обеспечивает эффективную аппаратную (без необходимости включения в программу дополнительных команд) поддержку циклических вычислений, ветвлений программы и условного выполнения большинства команд;
- программный автомат в сочетании с двумя генераторами адресов обеспечивает аппаратную поддержку типичных для ЦОС структур данных, таких, как одномерные и многомерные массивы и, в особенности, кольцевые буферы.

В каждом цикле DSP может:

- прочитать два операнда из памяти или записать один в память;
- завершить выполнение одной вычислительной операции;
- записать в регистровый файл до трех операндов.

Процессоры семейства ADSP-219x выполняют все вычислительные команды за один цикл, при этом любая команда может быть условной - то есть выполняться при удовлетворении заданного условия (режима либо результата предыду-щих вычислений). Они поддерживают высокую тактовую частоту и полноценный набор арифметических операций.

Процессор обрабатывает данные в форматах 16-разрядное целое и дробное (в дополнительном коде и беззнаковые). Процессор перемещает данные повышенной точности между своими вычислительными устройствами, ограничивая ошиб-ку округления промежуточных данных.

Процессор имеет два генератора адреса данных (DAG), которые обеспечивают прямую или косвенную адресацию с пред- и пост-модификацией адреса с произвольным шагом - вплоть до размеров адресного пространства. Поддержива-ется адресация по модулю и с перестановкой бит (применяется для реализации быстрого преобразования Фурье).

Кроме циклов с аппаратной проверкой условия окончания (без дополнительной команды проверки окончания цикла) процессор поддерживает быструю инициализацию циклов и выход из них. Циклы могут быть вложенными (восемь аппаратных уровней) и прерываемыми. Процессор поддерживает задержанный и незадержанный переходы.

Гибкая архитектура и полноценный набор команд процессоров семейства ADSP-219x обеспечивают параллельное выполнение нескольких операций. Например, за один такт ADSP-2191 может:

- сгенерировать адрес для следующей выборки команд;
- выбрать следующую команду;
- переместить одно или два значения;
- обновить один или два адресных указателя;
- выполнить вычислительную операцию.

Все это происходит в то время, как процессор продолжает:

- принимать и передавать данные через два последовательных порта;
- выполнять обмен данными с хост-машиной;

- принимать и передавать данные через UART-порт;
- принимать и передавать данные через два SPI-порта;
- обращаться к внешней памяти через интерфейс с внешней памятью;
- уменьшать значение таймера.

5.3.2. Архитектура ядра DSP

Кроме стандартного набора арифметических и логических операций ALU также обеспечивает примитивы деления. В умножителе операции умножения, умножения/сложения, умножения/вычитания выполняются за один такт. Он имеет два 40-разрядных аккумулятора, помогающих сохранить данные при переполне-нии результата. В устройстве сдвига выполняются операции логического и ариф-метического сдвигов, нормализации и денормализации, а также операция опреде-ления порядка. Устройство сдвига может эффективно обрабатывать различные чи-словые форматы, включая многословные представления чисел и представления блоков чисел с плавающей точкой.

Правила использования регистров в вычислительных устройствах определяют, где может быть размещен входной операнд или результат вычислений. При выполнении большинства операций регистры данных в вычислительных устрой-ствах функционируют как регистровый файл данных, что позволяет любому реги-стру входных данных или регистру результата передавать входное значение лю-бому вычислительному устройству. Что касается циклических операций, то выход (результат) любого вычислительного устройства может быть входом для любого вычислительного устройства на следующий такт. При выполнении условных или многофункциональных команд существуют некоторые ограничения на то, какие регистры могут обеспечить входные данные или принять результат от каждого вычислительного устройства.

Эффективный программный автомат управляет потоком исполняемых команд. Программный автомат поддерживает условные переходы, вызовы подпрограмм и низкоприоритетные прерывания при переполнении. Наличие внутренних счетчиков цикла и стеков цикла в ADSP-2191 позволяет выполнять циклические алгоритмы с нулевыми непроизводительными затратами; для реализации циклов не требуются команды явного перехода.

Два генератора адреса данных обеспечивают адресацию для одновременной выборки двух операндов (из памяти данных и памяти программы). Каждый DAG хранит и обновляет четыре 16-разрядных адресных указателя. Какой бы из указа-телей не использовался для доступа к данным (косвенная адресация), он может использовать пред- и постмодификацию значением, хранящимся в одном из четы-рех регистров модификации. Значения, хранящиеся в регистрах длины и базового адреса, могут быть связаны с произвольным указателем, что создает условия для выполнения автоматической адресации по модулю, необходимой для реализации циклического буфера. Регистры страницы памяти генераторов допускают цикли-ческую адресацию в любой из 256 страниц памяти, занимающих 64 Кслова, хотя циклические буферы не могут выходить за пределы указанных 64 Кслов. В DAG существуют основные регистры, которые дублируются дополнительными, кото-рые используются при необходимости быстрого контекстного переключения.

Эффективная передача данных в процессоре достигается путем использования внутренних шин:

- Шины адреса памяти программы (шина адреса PM или шина PMA);
- Шины данных памяти программы (шина данных PM или шина PMD);

- Шины адреса памяти данных (шина адреса DM или шина DMA);
- Шины данных памяти данных (шина данных DM или шина DMD);
- Шины адреса DMA (прямого доступа в память);
- Шины данных DMA.

В памяти программы могут храниться и команды, и данные, что позволяет ADSP-219x выбирать два операнда за один цикл: один из памяти программы, а второй - из памяти данных. Наличие двух шин памяти в процессоре позволяет яд-ру за один такт выбирать операнд из памяти данных и следующую команду из памяти программ.

Внутренние шины адреса соединяются с одной внешней шиной адреса (та-ким образом позволяя наращивать память за пределами кристалла), а шины дан-ных - с одной внешней шиной данных. Эти внешние шины используются для дос-тупа к памяти начальной загрузки и к памяти внешних устройств I/O.

5.3.3. Организация памяти

Адресное пространство ADSP-219x (рис. 5.4) представляет собой единое пространство памяти программ и данных, и занимает 16 миллионов ячеек, доступ к которым обеспечивается с помощью 24-разрядных шин адреса: шин адреса PM и DM. На кристалле ADSP-2191 размещается 64 Кслова памяти, которая сконфи-гурирована как 32 Кслова (24-разрядных) памяти программы и 32 Кслова (16-разрядных) памяти данных, которые размещаются в нулевой странице памяти карты памяти процессора. Вся карта памяти процессора занимает 256 страниц (стра-ницы от 0 до 255), и каждая страница имеет размер, равный 64 Ксловам. Про-странство внешней памяти состоит из четырех банков памяти (банки 3-0). Банки выбираются с помощью вывода (сигнала) выбора банка памяти ( ) и конфи-гурируются по таким параметрам, как граница страницы, состояние ожидания, режим состояния ожидания. 1 Кслово расположенного на кристалле постоянного запоминающего устройства (ПЗУ) начальной загрузки занимает младшие адреса 255-й страницы. Оставшиеся 254 страницы (все страницы, кроме страниц 0 и 255) - это адресное пространство внешней памяти.

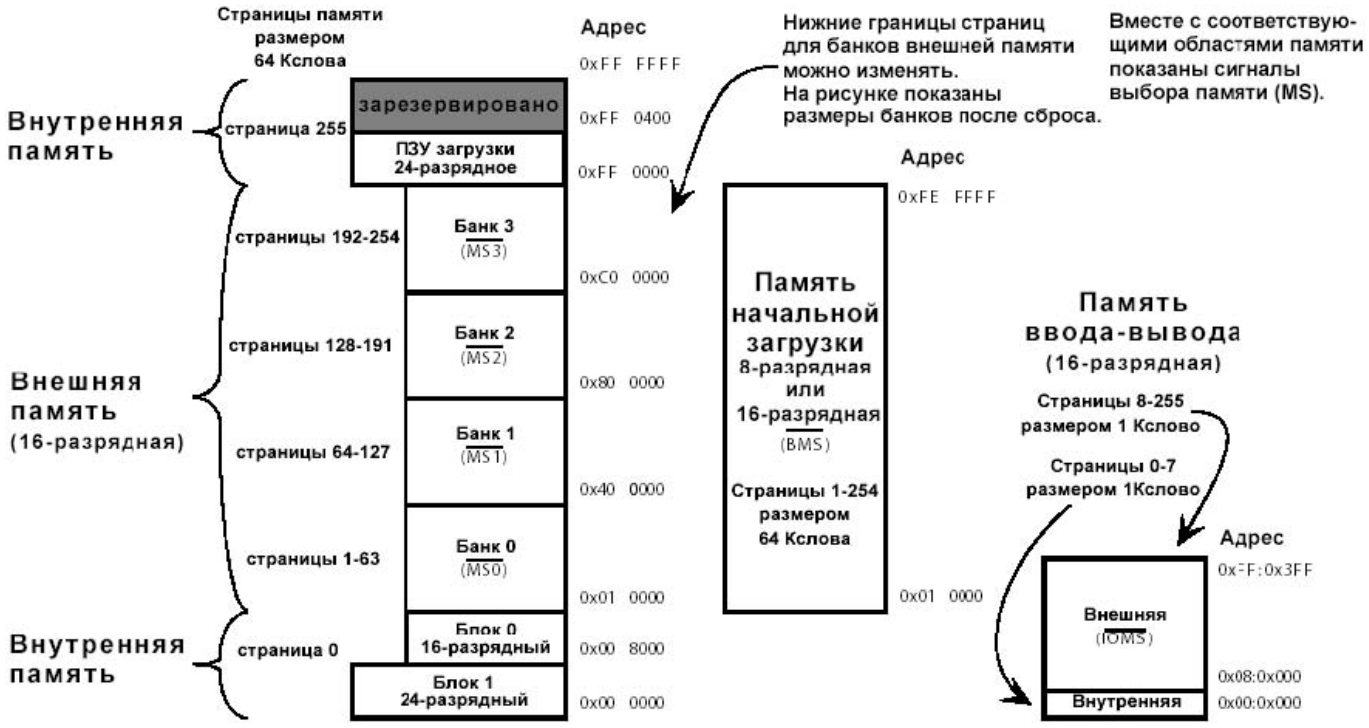

Рис. 5.4. Карты внутренней и внешней памяти ADSP-2191, памяти начальной загрузки и памяти ввода-вывода

Помимо внутреннего и внешнего пространств памяти ADSP-2191 может ис-пользовать два дополнительных и раздельных пространства: пространство памяти I/O и пространство памяти начальной загрузки. Страницы памяти I/O отличаются от страниц внешней памяти тем, что они имеют размер, равный 1Кслову, и стра-ницы внешней памяти I/O имеют свой собственный сигнал выбора страницы ( ). Страницы с 0 по 7 пространства памяти I/O размещаются на кристалле и содержат регистры конфигурации периферийных устройств.

Внутренняя память (память на кристалле). Для каждой из шин исполь-зуются немного отличающиеся механизмы генерации 24-разрядных адресов. В процессоре имеются 3 способа, используя которые, можно получить доступ ко всей карте памяти:

 DAG генерирует 24-разрядные адреса для выборок данных во всем диапазо-не адресов памяти процессора. Так как регистры индекса (адреса) генерато-ров 16-разрядные и хранят только младшие 16 разрядов адреса, каждый из генераторов имеет свой собственный 8-разрядный регистр страницы (DMPGx), где хранятся старшие 8 разрядов значения адреса. Перед тем как DAG сгенерирует адрес, программа должна установить в регистре генератора номер соответствующей адресной страницы;
 программный автомат генерирует адреса для выборок команд. Для команд с относительной адресацией (не путать с косвенной!) программный автомат определяет адреса, основываясь на содержимом счетчика команд (Program Counter - PC). Команды с прямой адресацией (команды из двух слов) обес-печивают непосредственное 24-разрядное значение адреса. допускает ли-нейную адресацию во всем диапазоне адресов 24-разрядного адресного пространства;
 программный автомат использует 8-разрядный регистр страницы косвенно-го перехода ( ) как источник определения 8 старших бит адреса для кос-венных переходов и вызовов, использующих содержимое 16-разрядного ре-гистра адреса в DAG как часть адреса, по которому выполняется переход или вызов. До того, как выполнить переход или вызов с пересечением гра-ницы страницы, программа должна установить значение в регистре программного автомата, равное номеру соответствующей страницы.

ADSP-2191 имеет на кристалле ПЗУ размером 1 Кслово, в котором хранятся подпрограммы загрузки. Если выбрана загрузка с помощью периферийных уст-ройств, то процессор начинает выполнение содержащихся в этом устройстве ко-манд, которые, в свою очередь, запускают процесс загрузки через выбранное пе-риферийное устройство. ПЗУ начальной загрузки на кристалле размещается на странице 255 карты памяти процессора.

Внешняя память (память за пределами кристалла). Адресное простран-ство внешней памяти процессора ADSP-2191 разделяется на три части (простран-ства), каждая из которых имеет собственный регистр управления; таким образом, приложения могут определять отдельные наборы параметров для доступа к от-дельным пространствам памяти. Параметры доступа это: счетчик тактов ожида-ния при чтении и записи, режим выхода из состояния ожидания, коэффициент де-ления тактовой частоты при I/O, увеличение времени владения шиной при записи, полярность строба и разрядность шины. Коэффициенты деления тактовых частот ядра и периферийных устройств влияют на ширину стробов при доступе к внеш-ней памяти. К пространствам внешней памяти относятся:

 пространство внешней памяти (выводы выбора);
 пространство памяти I/O (вывод выбора);
пространство памяти начальной загрузки (вывод выбора).

Все эти внешние пространства памяти доступны через внешний порт, разрядность которого может изменяться между двумя значениями - 8 или 16 разрядов.

Пространство памяти I/O. Для ADSP-2191 поддерживается дополнитель-ная внешняя память, которая называется пространство памяти ввода-вывода. Это пространство предназначено для обеспечения простоты соединения с периферий-ными устройствами (такими, как преобразователи данных и внешние регистры) или для осуществления интерфейсного соединения через шину с регистрами дан-ных в интегральных схемах специального назначения. Общий размер пространст-ва I/O не превышает 256 Кслов. Первые 8 Кслов зарезервированы для располо-женных на кристалле периферийных устройств. Старшие 248 Кслов доступны для внешних периферийных устройств и выбираются с помощью сигнала . В процессоре имеются команды доступа к пространству памяти I/O. Эти команды используют 18-разрядное значение адреса, которое складывается из содержимого 8-разрядного регистра страницы памяти ввода-вывода ( ) и 10-разрядного числа, присутствующего непосредственно в команде. И ядро процессоров семей-ства ADSP-219x, и хост-процессор (используя хост-интерфейс) могут обращаться к пространству памяти I/O.

Пространство памяти начальной загрузки. Это пространство состоит из расположенного за пределами кристалла банка, включающего 253 страницы. Сиг-нал определяет выбор пространства памяти начальной загрузки. И ядро про-цессора, и периферийные устройства, поддерживающие DMA, могут обращаться к внешнему пространству памяти начальной загрузки. Если процессор сконфигу-рирован таким образом, что должен загружаться извне, то он начинает выполнять команды из расположенного на кристалле ПЗУ загрузки; команды, в свою очередь, инициируют загрузку процессора из памяти загрузки.

5.3.4. Архитектура периферийной части процессора

На рис. 5.3. (см.) показаны имеющиеся на кристалле компоненты процессора, предназначенные для связи с периферийными устройствами; к этим компонентам относятся: интерфейс с внешней памятью, хост-порт, последовательные пор-ты, SPI-совместимый порт, UART-порт, JTAG-порт для тестирования и эмуляции, флаги и контроллер прерываний. На рис. 5.5 показана типовая система соединения процессора ADSP-2191 с периферийными устройствами.

ADSP-2191 имеет 16-разрядный хост-порт, поддерживающий DMA; хост-порт обеспечивает доступ для внешней головной-машины (хост-процессора) к внутренней памяти. Этот параллельный порт с мультиплексной шиной данных и адреса обеспечивает передачу данных с низкоприоритетными прерываниями при возникновении переполнения. Разрядность шины порта изменяется (8 или 16 раз-рядов), что позволяет реализовывать не требующий дополнительных компонентов для соединения интерфейс с различными 8- и 16-разрядными микроконтроллера-ми. Два входа выбора кристалла обеспечивают доступ для хост-машины ко всей карте памяти процессора. Хост-порт может использоваться для начальной загруз-ки процессора. ADSP-2191 также содержит интерфейс с внешней памятью, кото-рый совместно используется ядром процессора, контроллером DMA, и поддержи-вающими DMA периферийными устройствами, к которым относятся UART-порт, последовательные порты, SPI-порты и хост-порт.

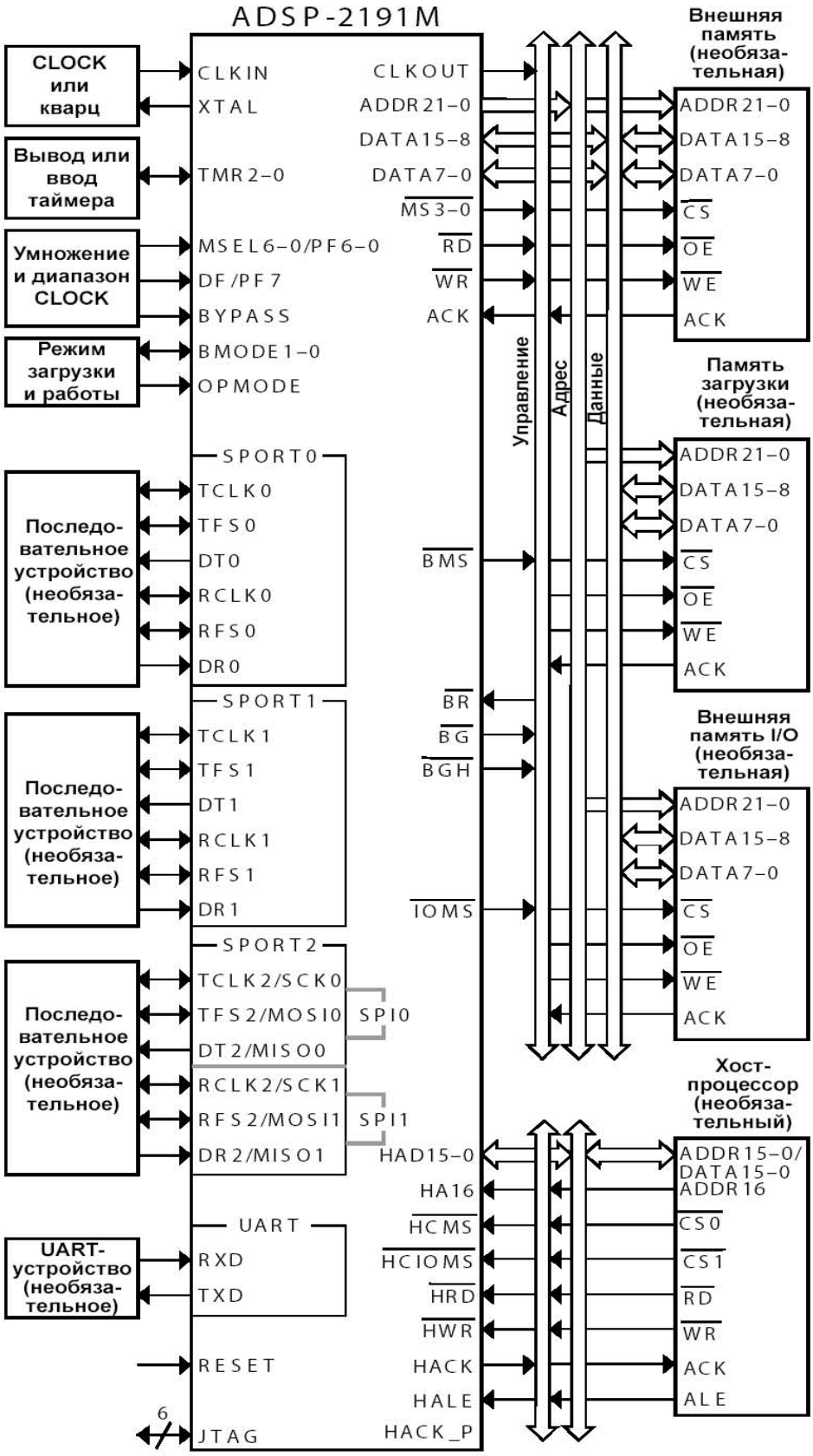

Рис. 5.5. Блок-схема вычислителя на базе процессоров ADSP-219x

Внешний порт состоит из 8- или 16-разрядной шины данных, 22-разрядной адресной шины и выводов сигналов управления. Шина данных может конфигури-роваться как 8- или 16-разрядная для обеспечения интерфейса с внешней памя-тью. Наличие возможности упаковки слов

позволяет процессору обращаться к 16- или 24-разрядной внешней памяти при любой разрядности внешней шины дан-ных. Когда шина данных сконфигурирована как 8-разрядная, оставшиеся 8 линий используются как программируемые, двунаправленные линии программируемых флагов общего назначения, 6 из них могут отображаться как программно управляемые условные сигналы.

Контроллер DMA позволяет процессору ADSP-2191 передавать данные во внешнюю и внутреннюю память и из внешней и внутренней памяти. Расположен-ные на кристалле периферийные устройства также могут использовать этот внеш-ний порт для передач с DMA в память и из памяти.

ADSP-2191 может обслуживать 17 источников прерываний в любой момент времени: три внутренних запроса на прерывание (стек, ядро эмулятора, выключе-ние), два внешних запроса (эмулятор и сброс) и 12 определяемых пользователем для периферийных устройств запросов. Программист назначает (распределяет) эти 12 запросов для периферийных устройств. Приоритет каждого устройства при обработке прерывания зависит от указанного распределения. Можно назна-чить нескольким периферийным устройствам одну и ту же линию запроса прерывания.

Три последовательных порта ADSP-2191 обеспечивают синхронный, полно-дуплексный последовательный интерфейс. Интерфейс поддерживает дополни-тельное аппаратное компандирование и большое количество режимов приема и передачи данных с синхронизацией и без нее. Каждый последовательный порт может передавать или принимать внутренние или внешние программируемые по-следовательные сигналы тактовой и кадровой синхронизации. Каждый последова-тельный порт поддерживает 128-канальное временное мультиплексирование.

ADSP-2191 обеспечивает до 16 выводов общего назначения для ввода-вывода, каждый из которых может программироваться и как вход, и как выход. Восемь из них - программируемые флаги общего назначения. Остальные 8 - мно-гофункциональные выводы, работающие как выводы общего назначения для опе-раций ввода-вывода при соединении процессора с 8-разрядной внешней шиной и как выводы, соответствующие старшим 8 разрядам слова данных, при соединении процессора с 16-разрядной внешней шиной. Выводы программируемых флагов могут быть использованы для формирования прерываний как по фронту, так и по уровню входного сигнала. Состояние этих выводов может также проверяться при выполнении условных команд.

Три программируемых таймера могут генерировать периодические преры-вания. Любой таймер может независимо устанавливаться для работы в одном из следующих режимов:

- режим генерации импульсного сигнала;
- режим оценки/фиксации длительности импульса;
- режим реагирования на внешний сигнал.

Каждый таймер имеет один двунаправленный вывод и четыре регистра, с помощью которых реализуются вышеперечисленные режимы; регистр конфигу-рации, регистр счетчика, регистр периода и регистр длительности импульса. Ра-бота всех трех таймеров поддерживается одним регистром состояния. Бит в реги-стре состояния может блокировать или разрешить работу всех трех таймеров, а бит регистра конфигурации каждого таймера блокирует или разрешает работу таймера независимо от состояния остальных.

Работа в режиме пониженного энергопотребления. ADSP-2191 имеет че-тыре режима работы с пониженным энергопотреблением, позволяющие значи-тельно уменьшить расход энергии, когда устройство работает в режиме ожидания. Переход в один из режимов ожидания осуществляется, когда процессор выполня-ет команду IDLE. ADSP-2191 изменяет биты

в регистре PLLCTL и таким образом выбирает один из вариантов (режимов) ожидания, в то время как процессор вы-полняет команду IDLE. В зависимости от выбранного режима IDLE выключает тактовую синхронизацию в различных частях процессора. Существуют следую-щие режимы работы с пониженным энергопотреблением:

- простое ожидание;
- ожидание с выключением ядра;
- ожидание с выключением ядра и периферийных устройств;
- выключение всех компонентов.

Сигналы тактовой синхронизации. Тактовая синхронизация ADSP-2191 может выполняться с помощью кварцевого резонатора или с помощью сигналов тактовой синхронизации от внешнего источника. Если используется кварцевый резонатор, то он должен быть соединен с выводами CLKIN и XTAL, к которым также подсоединяются конденсаторы. Емкость конденсаторов зависит от типа кварца и должна определяться производителем. В этой конфигурации должен ис-пользоваться резонансный кварцевый генератор опорных частот для микропроцессоров.

Если используются сигналы, сформированные внешним источником, то сигнал синхронизации подсоединяется к выводу CLKIN процессора. Во время выполнения обычной операции сигнал на выводе CLKIN не может быть зафикси-рован и изменен, а также иметь частоту ниже определенного значения. Это дол-жен быть TTL-сигнал. При работе от внешнего источника вывод XTAL должен ос-таваться отсоединенным.

Пользователь может программно переопределять коэффициент умножения частоты входного сигнала тактовой синхронизации от 1 до 31, включая некоторые дробные значения, что обеспечивает 128 вариантов отношения частот тактовой синхронизации внутренней части (ядра) процессора и его внешней периферии.

Режимы загрузки. В ADSP-2191 имеется семь вариантов автоматической загрузки внутренней памяти программы после сброса. Сигналы на выводах BMODE2-0, опрашиваемые во время аппаратного сброса, и три бита в регистре конфигурации при сбросе определяют следующие режимы:

- загрузка из внешней 16-разрядной памяти;
- загрузка из 8-разрядного СППЗУ;
- загрузка из хост-процессора;
- выполнение программы из 8-разрядной внешней памяти (Нет загрузки);
- загрузка из UART;
- загрузка через SPI с пропускной способностью 4 Кбита в секунду;
- загрузка через SPI с пропускной способностью 512 Кбит в секунду.

JTAG-порт. Этот порт поддерживает предложенный IEEE стандарт комплексной проверки функционирования системы 1149.1 (дословно - комплекс дей-ствий по тестированию соединений в системе JTAG). Этот стандарт определяет методику последовательной проверки результатов ввода-вывода во всех компо-нентах системы. Эмуляторы используют JTAG-порт для мониторинга и управле-ния процессором во время эмуляции. При этом обеспечивается эмуляция на пол-ной скорости с возможностями доступа к памяти, регистрам и стекам процессора для проверки и модификации. Основанная на JTAG эмуляция является неинтру-зивной (неагрессивной, т.е. не изменяет режима работы тестируемого устройства) и не влияет на загрузку целевой системы, а также не нарушает временную схему работы устройства.

5.3.5. Средства разработки

Программирование ADSP-219x выполняется с помощью VisualDSP® - удобной в использовании среды управления проектом, состоящей из интегрированной среды разработки (Integrated Development Environment - IDE) и отладчика. VisualDSP позволяет программисту управлять проектами от начала и до конца, используя один общий интерфейс. Поскольку среды разработки и отладки проекта объединены, программист может легко переходить между режимами редактирова-ния, компоновки и отладки. Язык Ассемблера процессоров ADSP-219x использует алгебраический синтаксис, что обеспечивает простоту кодирования и читаемость кода.

Гибкое управление проектом. Среда разработки (IDE) обеспечивает гибкость разработки проекта для реализации процессорных приложений. IDE дает возможность выполнять все действия, необходимые для создания и отладки про-ектов процессорных приложений. С помощью редактора (IDE Editor) вы можете изменять исходные файлы или просматривать список или карту файлов. Этот мощный редактор, являясь частью среды разработки, поддерживает синтаксиче-скую индикацию для множества языков, операцию графического интерфейса "пе-ретащить и оставить" (Drag and Drop) технологии OLE, создание закладок, а так-же стандартный набор операций редактирования: отменить/вернуть, най-ти/заменить, копировать/вставить/вырезать и перейти.

Кроме того, среда разработки позволяет использовать такие средства, как: компилятор языка С для реализации процессорных приложений, исполняемые библиотеки функций языка С, транслятор, компоновщик, загрузчик, симулятор и сплиттер. Опции этих инструментов задаются в диалоговых окнах (страницах свойств). Легкие в использовании диалоговые окна позволяют легко конфигури-ровать, изменять и управлять проектом. Указанные опции определяют, как инст-рументы среды обрабатывают входные данные и как формируют выходные, а так-же один к одному соответствуют определяемым в командой строке ключевым па-раметрам для данного средства. Вы можете задать эти опции, а затем изменять в соответствии с требованиями разрабатываемого приложения. Вы также можете, если хотите, вызвать любой из перечисленных инструментов из командной строки операционной системы.

Значительно уменьшенное время отладки. Отладчик имеет легкий в использовании, единый интерфейс для всех процессорных симуляторов и эмулято-ров, разрабатываемых компанией Analog Devices или третьей стороной. Отладчик обладает множеством черт, которые значительно уменьшают время отладки. Вы можете одновременно анализировать код на С и ассемблерный код. Вы можете определять временные характеристики выполнения последовательности команд в программе, устанавливать симулируемые точки останова по условию для аппа-ратных регистров и для программы в памяти программы и памяти данных, а так-же отслеживать выполнение команд и обращения к памяти. Эти возможности по-могают исправлять ошибки программирования, выявлять критические элементы программы и оценивать характеристики процессора. Вы можете использовать оп-цию "регистр пользователя" для определения любых комбинаций регистров, со-держимое которых будет отображаться в одном окне. Отладчик может генериро-вать входные и выходные сигналы, а также прерывания: все это позволяет симу-лировать реальные условия работы приложения.

Программные средства разработки. Программные средства разработки для процессоров семейства ADSP-219x позволяют разрабатывать приложения, ко-торые используют все достоинства архитектуры, включая совместно используе-мую память и оверлей. К этим

средствам относятся: компилятор языка С, испол-няемые библиотеки С, библиотеки DSP и Math, транслятор, компоновщик, загруз-чик, симулятор и сплиттер.

Компилятор языка С/С++ и транслятор. Компилятор языка С/С++ генерирует эффективный код, оптимальный и с точки зрения эффективности, и с точки зрения скорости выполнения программы. Компилятор позволяет включать в про-грамму выражения языка Ассемблер. Таким образом, вы можете программировать на С, но использовать Ассемблер для критичных к времени циклов. Вы также мо-жете использовать предварительно протестированные подпрограммы библиотек Math, DSP, а также исполняемой библиотеки, которые помогут сократить время написания программы. Ассемблер, используемый для реализации приложений на процессорах семейства ADSP-219x, основан на алгебраическом синтаксисе, кото-рый легок в изучении, программировании и отладке.

Компоновщик и загрузчик. Компоновщик обеспечивает гибкие системные определения с помощью файлов описания компоновки (Linker Description Files - LDF). Эти файлы имеют расширение .ldf. В одном файле можно определить раз-личные типы исполнения одно- или многопроцессорной системы. Компоновщик распределяет символы для различных исполнений, оптимизирует использование памяти и легко разделяет общий код между несколькими процессорами. Загрузчик поддерживает создание исполняемого кода для загрузки из постоянной памяти, из хост-машины, через SPI-порт и UART-порт. Загрузчик позволяет уменьшить объем кода, необходимый для конфигурирования мультипроцессорной системы, а также позволяет сократить время загрузки такой системы.

Возможности третьих лиц. Среда разработки VisualDSP позволяет третьим лицам, используя распространяемые компанией Analog Devices наборы программ-ных интерфейсов приложения (Application Programming Interface - API), расши-рять систему. Создаваемые такими компаниями продукты - операционные систе-мы реального времени, эмуляторы, компиляторы языков высокого уровня, муль-типроцессорная аппаратура - могут встраиваться в VisualDSP; таким образом, уп-рощается задача интегрирования этих средств. VisualDSP соответствует формату COM API (речь идет о стандартном механизме, включающем интерфейсы, с по-мощью которых одни объекты предоставляют свои сервисы другим). Два инстру-мента API - мастер целевой системы (Target Wizard) и тестер интерфейса (API Tester) - также используются в наборе интерфейсов. Мастер целевой системы строит программную оболочку, основываясь на характеристиках интерфейса. Тес-тер реализует индивидуальные характеристики независимо от VisualDSP. Третьи лица могут использовать такие комбинации этих интерфейсов, которые удовле-творяют их собственным нуждам. Интерфейсы полностью поддерживают друг друга, а также обратно совместимы.

5.4. Программируемая логика

Существуют алгоритмы, реализация которых более эффективна или даже возможна только в виде параллельных аппаратных структур. Создание заказных интегральных схем экономически оправдано только в случае массового производ-ства, средства защиты информации с предельными характеристиками вряд ли не-обходимы в больших количествах. В таком случае целесообразно использовать программируемые логические интегральные схемы (ПЛИС). Если программа ЭВМ (и ЦСП) определяет последовательность выполнения действий по реализа-ции алгоритма, то в ПЛИС программируются соединения между аппаратно реали-зованными логическими блоками, работающими параллельно. В частности, с по-мощью ПЛИС часто

реализуют интерфейсные узлы, обеспечивающие подключе-ние нестандартных устройств к ЦВМ. Таким образом, ЦСП и ПЛИС могут при-меняться совместно как взаимодополняющие универсальные программируемые средства реализации соответственно последовательных и параллельных устройств обработки информации. Разграничение функций ЦСП и ПЛИС при создании средств ЗРИ определяется характеристиками реализуемых алгоритмов, наличием или отсутствием необходимых интерфейсных и специализированных вычислительных узлов в ЦСП.

5.4.1. Классификация и номенклатура ПЛИС

Классификация ПЛИС по структурному признаку даёт наиболее полное представление о классе задач, пригодных для решения на той или иной ПЛИС [22]. Общепринятой оценкой логической ёмкости ПЛИС является число эквива-лентных вентилей, определяемое как среднее число вентилей "2И-НЕ", необхо-димых для реализации эквивалентного проекта на ПЛИС и базовом матричном кристалле (БМК). Основным критерием такой классификации является наличие, вид и способы коммутации элементов логических матриц. По этому признаку можно выделить несколько классов ПЛИС.

Программируемые логические матрицы - наиболее традиционный тип ПЛИС, имеющий программируемые матрицы "И" и "ИЛИ". В зарубежной лите-ратуре соответствующими этому классу аббревиатурами являются FPLA (Field Programmable Logic Array) и FPLS (Field Programmable Logic Sequensers). Приме-рами таких ПЛИС могут служить отечественные схемы К556РТ1, РТ2, РТ21. Не-достаток такой архитектуры - слабое использование ресурсов программируемой матрицы "ИЛИ", поэтому дальнейшее развитие получили микросхемы, построенные по архитектуре программируемой матричной логики (PAL - Programmable Array Logic) - это ПЛИС, имеющие программируемую матрицу "И" и фиксиро-ванную матрицу "ИЛИ". К этому классу относится большинство современных ПЛИС небольшой степени интеграции. В качестве примеров можно привести оте-чественные ИС КМ1556ХП4, ХП6, ХП8, ХЛ8, ранние разработки (середина-конец 1980-х годов) ПЛИС фирм INTEL, ALTERA, AMD, LATTICE и др. Разно-видностью этого класса являются ПЛИС, имеющие только одну (программируе-мую) матрицу "И", например, схема 85С508 фирмы INTEL. Следующий традици-онный тип ПЛИС - программируемая макрологика. Они содержат единственную программируемую матрицу "И-НЕ" или "ИЛИ-НЕ", но за счёт многочисленных инверсных обратных связей способны формировать сложные логические функ-ции. К этому классу относятся, например, ПЛИС PLHS501 и PLHS502 фирмы SIGNETICS, имеющие матрицу "И-НЕ", а также схема XL78C800 фирмы EXEL, основанная на матрице "ИЛИ-НЕ".

Перечисленные архитектуры ПЛИС, содержащие небольшое число ячеек, к настоящему времени морально устарели и применяются для реализации относи-тельно простых устройств, для которых не существует готовых ИС средней степе-ни интеграции. Естественно, для реализации алгоритмов ЦОС они непригодны.

ИС ПМЛ (PLD) имеют архитектуру, весьма удобную для реализации цифро-вых автоматов. Развитие этой архитектуры - программируемые коммутируемые матричные блоки (ПКМБ) - это ПЛИС, содержащие несколько матричных логи-ческих блоков (МЛБ), объединённых коммутационной матрицей. Каждый МЛБ представляет собой структуру типа ПМЛ, то есть программируемую матрицу "И", фиксированную матрицу "ИЛИ" и макроячейки. ПЛИС типа ПКМБ, как правило, имеют высокую степень интеграции (до 10000 эквивалентных вентилей, до 256 макроячеек). К этому классу относятся ПЛИС семейства MAX5000 и MAX7000

фирмы ALTERA, схемы XC7000 и XC9500 фирмы XILINX, а также большое чис-ло микросхем других производителей (Atmel, Vantis, Lucent и др.). В зарубежной литературе они получили название Complex Programmable Logic Devices (CPLD).

Другой тип архитектуры ПЛИС - программируемые вентильные матрицы (ПВМ), состоящие из логических блоков (ЛБ) и коммутирующих путей - про-граммируемых матриц соединений. Логические блоки таких ПЛИС состоят из од-ного или нескольких относительно простых логических элементов, в основе кото-рых лежит таблица перекодировки (ТП, Look-up table - LUT), программируемый мультиплексор, D-триггер, а также цепи управления. Таких простых элементов может быть достаточно много, например, у современных ПЛИС ёмкостью до

1 млн. вентилей число логических элементов достигает нескольких десятков ты-сяч. За счёт такого большого числа логических элементов они содержат значи-тельное число триггеров, а также некоторые семейства ПЛИС имеют встроенные реконфигурируемые модули памяти (РМП, embedded array block - EAB), что де-лает ПЛИС данной архитектуры весьма удобным средством реализации алгорит-мов цифровой обработки сигналов, основными операциями в которых являются перемножение, умножение на константу, суммирование и задержка сигнала. Вместе с тем возможности комбинационной части таких ПЛИС ограничены, поэтому совместно с ПВМ применяют ПКМБ (CPLD) для реализации управляющих и ин-терфейсных схем. В зарубежной литературе такие ПЛИС получили название Field Programmable Gate Array (FPGA). К FPGA (ПВМ) классу относятся ПЛИС XC2000, XC3000, XC4000, Spartan, Virtex фирмы XILINX; ACT1, ACT2 фирмы ACTEL, а также семейства FLEX8000 фирмы ALTERA, некоторые ПЛИС Atmel и Vantis. Множество конфигурируемых логических блоков (Configurable Logic

Blocks - CLBs) объединяются с помощью матрицы соединений. Характерными для FPGA-архитектур являются элементы ввода/вывода (input/output blocks - IOBs), позволяющие реализовать двунаправленный ввод/вывод, третье состояние и т. п.

Особенностью современных ПЛИС является возможность тестирования уз-лов с помощью порта JTAG (Boundary-Scan), а также наличие внутреннего генера-тора (Osc) и схем управления последовательной конфигурацией.

Фирма Altera пошла по пути развития FPGA-архитектур и предложила в се-мействе FLEX10K так называемую двухуровневую архитектуру матрицы соеди-нений. ЛЭ объединяются в группы - логические блоки (ЛБ). Внутри логических блоков ЛЭ соединяются посредством локальной программируемой матрицы со-единений, позволяющей соединять любой ЛЭ с любым. Логические блоки связа-ны между собой и с элементами ввода/вывода посредством глобальной програм-мируемой матрицы соединений (ГПМС). Локальная и глобальная матрицы соеди-нений имеют непрерывную структуру - для каждого соединения выделяется не-прерывный канал.

Дальнейшее развитие архитектур идёт по пути создания комбинированных архитектур, сочетающих удобство реализации алгоритмов ЦОС на базе таблиц перекодировок и реконфигурируемых модулей памяти, характерных для FPGA-структур и многоуровневых ПЛИС с удобством реализации цифровых автоматов на CPLD-архитектурах.

Как известно, при выборе элементной базы систем обработки сигналов обычно руководствуются следующими критериями отбора:

- быстродействие;
- логическая ёмкость, достаточная для реализации алгоритма;
- схемотехнические и конструктивные параметры ПЛИС, надёжность, рабочий диапазон температур, стойкость к ионизирующим излучениям и т. п.;

 стоимость владения средствами разработки, включающая как стоимость программного обеспечения, так наличие и стоимость аппаратных средств отладки;
 стоимость оборудования для программирования ПЛИС или конфигурацион-ных постоянных запоминающих устройств (ПЗУ);
 наличие методической и технической поддержки;
 наличие и надёжность российских поставщиков;
 стоимость микросхем.

Рассмотрим с этих позиций продукцию ведущих мировых производителей ПЛИС, доступную на российском рынке.

Фирма **Altera Corporation.** В настоящее время Altera выпускает семейство APEX20K, CPLD семейств MAX3000, MAX7000, MAX9000 и FPGA семейств FLEX10K, FLEX8000, FLEX6000.

Кроме того, ПЛИС фирмы Altera выпускаются с возможностью программи-рования в системе непосредственно на плате. Для программирования и загрузки конфигурации устройств опубликована схема загрузочного кабеля ByteBlaster и ByteBlasteMV. Следует отметить, что новые конфигурационные ПЗУ EPC2 позво-ляют программировать с помощью этого устройства, тем самым отпадает нужда в программаторе, что, естественно, снижает стоимость владения технологией.

Компания **Xilinx Inc.** производит ПЛИС семейства Virtex. Архитектура се-мейства Virtex характеризуется широким разнообразием высокоскоростных трас-сировочных ресурсов, наличием выделенного блочного ОЗУ, развитой логикой ус-коренного переноса. ПЛИС данной серии обеспечивают высокие скорости меж-кристального обмена - до 200 МГц (стандарт HSTL IV). Кристаллы серии Virtex за счёт развитой технологии производства и усовершенствованного процесса ве-рификации имеют до-статочно низкую стоимость (до 40% от эквивалентной стои-мости серии XC4000XL).

Помимо семейства Virtex, Xilinx выпускает FPGA семейств XC3000A, XC4000E, Spartan, XC5200, а также CPLD XC9500 и малопотребляющую серию CoolPLD.

Компания **Actel Corporation.** Особенностью ПЛИС Actel является примене-ние так называемой Antifuse-технологии, представляющей собой создание металлизированной перемычки при программировании. Данная технология обеспечива-ет высокую надёжность и гибкие ресурсы трассировки, а также не требуется кон-фигурационное ПЗУ. По этой технологии выпускаются семейства ACT1, ACT2, 1200XL, а также новые семейства 54SX, A40MX и A42MX (со встроенными мо-дулями памяти), имеющие хорошие показатели цена/логическая ёмкость (ПЛИС, заменяющая 300…350 корпусов ТТЛ, при частоте > 250 МГц стоит 10 долл. США).

Новое семейство ProASIC фирмы Actel обладает ёмкостью до 500 000 экви-валентных логических вентилей. Его отличительной особенностью является энер-гонезависимость, обеспечиваемая за счёт применения FLASH-технологии, и на-личия интегрированного на кристалле запоминающего устройства.

5.4.2. Система проектирования MAX+PLUS II ALTERA

В качестве примера рассмотрим свободно распространяемую через Internet версию MAX+PLUS II Baseline.

Название системы MAX+PLUS II является аббревиатурой от Multiple Array MatriX Programmable Logic User System. Система MAX+PLUS II имеет средства удобного ввода проекта, компиляции и отладки, а также непосредственного программирования устройств.

Процедуру разработки нового проекта от концепции до завершения можно упрощённо представить следующим образом:

- создание нового файла проекта или иерархической структуры нескольких файлов проекта с помощью любого сочетания редакторов в системе MAX+PLUS II, то есть графического, текстового и сигнального редакторов;
- задание имени файла - проекта верхнего уровня в качестве имени проекта;
- назначение семейства ПЛИС для проекта;
- открытие окна компилятора Compiler и выбор кнопки Start для начала ком-пиляции проекта. По желанию пользователя можно подключить модуль из-влечения временных параметров проекта Timing SNF Extractor для создания файла, используемого при временном моделировании;

В случае успешной компиляции возможен временной анализ, для проведе-ния которого выполняется следующее:

- для анализа задержек открыть окно Timing Analyzer, выбрать режим анализа и нажать кнопку Start;
- для проведения симуляции нужно сначала создать векторной тестовый век-тор в файле канала тестирования (.scf), пользуясь сигнальным редактором, или в файле вектора (.vec), пользуясь текстовым редактором. Затем открыть окно отладчика Simulator и нажать кнопку Start;
- открытие окна программатора Programmer с последующим выбором одного из двух способов: использование программатора MPU (Master Programming Unit) или подключение загрузочных устройств BitBlaster, Byte-Blaster или FLEX Download Cable к устройству, программируемому в системе;
- выбор кнопки Program для программирования устройств с памятью типа EPROM или EEPROM либо выбор кнопки Configure для конфигурации уст-ройства с памятью типа SRAM.

На рис. 5.6 представлено окно пакета MAX+PLUS II с загруженной схемой.

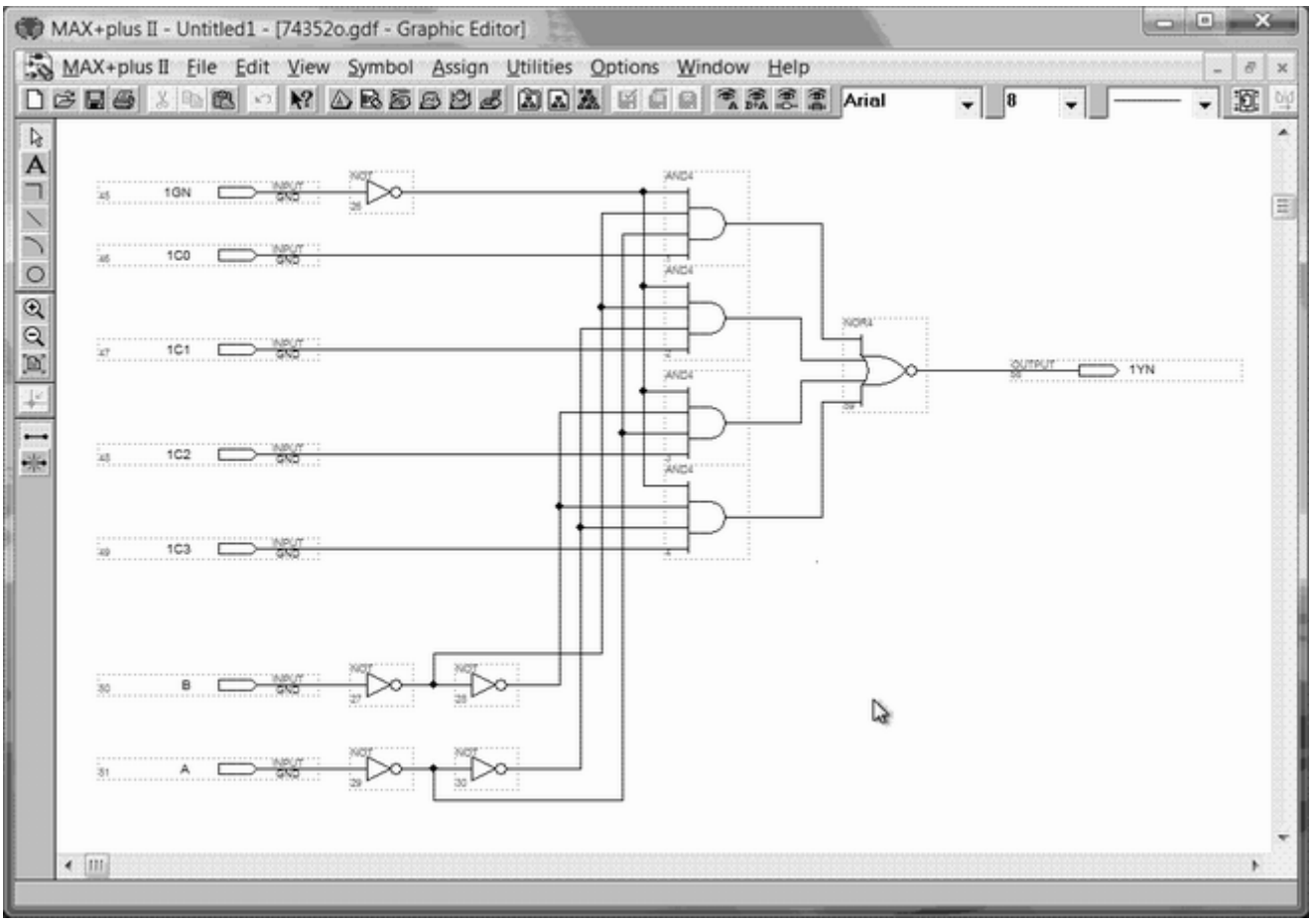

Рис. 5.6. Главное окно системы MAX+PLUS II

Программное обеспечение системы MAX+PLUS II содержит 11 приложений и главную управляющую программу. Различные приложения, обеспечивающие создание проекта, могут быть активизированы мгновенно, что позволяет пользо-вателю переключаться между ними щелчком мыши или с помощью команд меню. В это же время может работать одно из фоновых приложений, например, компиля-тор, симулятор, анализатор синхронизации и программатор. Одни и те же команды разных приложений работают одинаково, что облегчает задачу разработки логиче-ского дизайна. В табл. 5.1 приведено описание приложений.

Таблица 5.1

Приложение	Выполняемая функция
Hierarchy Display	Обзор иерархии – отображает текущую иерархическую структуру файлов в виде дерева с ветвями, представляющими собой подпроекты
Graphic Editor	Графический редактор – позволяет разрабатывать схемный логический проект в формате реального отображения на экране WYSIWYG
Symbol Editor	Символьный редактор – позволяет редактировать существующие символы и создавать новые
Text Editor	Текстовый редактор – позволяет создавать и редактировать текстовые файлы логического дизайна, написанные на языках AHDL, VHDL, Verilog HDL
Waveform Editor	Сигнальный редактор – выполняет двойную функцию: инструмент для рахработки дизайна и инструмент для ввода тестовых векторов и наблюдения результатов тестирования
Floorplan Editor	Поуровневый планировщик – позволяет графическими средствами делать назначения контактам устройства и ресурсов логических элементов
Compiler	Компилятор – обрабатывает графические проекты
Simulator	Симулятор – позволяет тестировать логические операции и внутреннюю синхронизацию проектируемой логической цепи
Timing Analyzer	Временной анализатор – анализирует работу проектируемой логической цепи после того, как она была синтезирована и оптимизирована компилятором
Programmer	Программатор – позволяет программировать, конфигурировать, проводить верификацию и тестировать ПЛИС фирмы ALTERA
Message Processor	Генератор сообщений – выдает на экран сообщения об ошибках, предупреждающие и информационные сообщения

Перед тем как начать работать в системе MAX+PLUS II, следует понять раз-ницу между файлами проекта, вспомогательными файлами и проектами.

Файл проекта - это графический, текстовый или сигнальный файл, создан-ный с помощью графического или сигнального редакторов системы MAX+PLUS II или в любом другом использующем промышленные стандарты схемном или текстовом редакторе либо при помощи программы netlist writer, имеющейся в пакетах, поддерживающих EDIF, VHDL и Verilog HDL. Этот файл содержит логику для проекта MAX+PLUS II и компилируется компилятором. Компилятор может автоматически обрабатывать следующие файлы проекта: гра-фические файлы проекта (.gdf); текстовые файлы проекта на языке AHDL (.tdf); сигнальные файлы проекта (.wdf); файлы проекта на языке VHDL (.vhd); файлы проекта на языке Verilog (.v); схемные файлы OrCAD (.sch); входные файлы EDIF (edf); файлы формата Xilinx Netlist (.xnf); файлы проекта Altera (.adf); файлы циф-рового автомата (.smf).

Вспомогательные файлы - это файлы, связанные с проектом MAX+PLUS II, но не являющиеся частью его иерархического дерева. Большинство таких фай-лов не содержит логики проекта. Некоторые из них создаются автоматически при-ложением системы MAX+PLUS II, другие - пользователем. Примерами вспомо-гательных файлов являются файлы назначений и конфигурации (.acf), символьные файлы (.sym), файлы отчета (.rpt) и файлы тестовых векторов (.vec).

Проект состоит из всех файлов иерархической структуры проекта, в том числе вспомогательных и выходных файлов. Именем проекта является имя файла проекта верхнего уровня без расширения. Система MAX+PLUS II выполняет ком-пиляцию, тестирование, анализ синхронизации и программирование сразу целого проекта, хотя пользователь может в это время редактировать файлы этого проекта в рамках другого проекта. Для каждого проекта желательно создавать отдельный подкаталог в рабочем каталоге системы MAX+PLUS II.

В системе MAX+PLUS II легко доступны все инструменты для создания проекта. Разработка проекта ускоряется за счёт имеющихся стандартных функций, в том числе примитивов, мегафункций, библиотеки параметризованных модулей (LPM) и макрофункций устаревшего типа микросхем 74 серии. В системе MAX+PLUS II есть три редактора для разработки проекта: графический, тексто-вый и сигнальный, а также два вспомогательных редактора: поуровневый плани-ровщик и символьный редактор.

В иерархической структуре проекта на любом уровне допускается смешан-ное использование файлов с расширениями ".gdf .tdf .vhd .v .edf .sch". Однако файлы с расширением ".wdf .xnf .adf .smf " должны быть либо на самом нижнем иерархическом уровне проекта, либо быть единственными.

Во всех приложениях MAX+PLUS II есть возможность с помощью команд из меню Assign вводить, редактировать и удалять типы назначений ресурсов, уст-ройств и параметров, которые управляют компиляцией проекта. Пользователь мо-жет делать назначения для текущего проекта независимо от того, открыт ли какой-нибудь файл проекта или окно приложений. Доступны следующие типы назначений.

Clique assignment (Назначение клики) задаёт, какие логические функции должны оставаться вместе в одном и том же блоке логической структуры LAB, блоке ячеек памяти EAB, в одном ряду или устройстве.

Chip assignment (Назначение кристалла) задаёт, какие логические функции должны быть реализованы в одном и том же устройстве в случае разделения про-екта на несколько устройств.

Pin assignment (Назначение контакта) назначает вход или выход одной логи-ческой функции конкретному контакту или нескольким контактам чипа.

Location assignment (Назначение ячейки) назначает единственную логиче-скую функцию конкретной ячейке чипа.

Probe assignment (Назначение зонда) присваивает уникальное имя входу или выходу логической функции.

Connected pin assignment (Назначение соединенных контактов) задаёт внеш-нее соединение двух или более контактов на схеме пользователя.

Local routing assignment (Назначение местной разводки) присваивает коэф-фициент разветвления по выходу узла логическому элементу, находящемуся в том же блоке LAB, что и узел, или в соседнем LAB, прилежащем к узлу, с использованием общих местных разводок.

Device assignment (Назначение устройства) назначает тип ПЛИС, на которой реализуется проект.

Logic option assignment (Назначение логической опции) управляет логиче-ским синтезом отдельных логических функций во время компиляции с применением стиля логического синтеза.

Timing assignment (Назначение временных параметров) управляет логиче-ским синтезом и подгонкой отдельных логических функций для получения требуемых характеристик для времени задержки tPD (вход - неподрегистренный вы-ход), tCO (синхросигнал - выход), tSU (синхросигнал - время установки), fMAX (частота синхросигнала).

Можно определить глобальные опции устройства для компилятора, чтобы он использовал их для всех устройств при обработке проекта. Для резервирования дополнительных возможностей на будущее можно задать процентное соотноше-ние контактов и логических элементов, которые должны оставаться неиспользованными во время текущей компиляции.

С использованием команды Global Project Parameters можно задать имена и глобальные установки, которые будут использованы компилятором для параметров всех параметризованных функций в проекте.

При помощи команды Global Project Timing Requirements можно ввести гло-бальные требования по синхронизации для проекта, задавая общие характеристики для времени задержки tPD (вход - нерегистрируемый выход), tCO (синхросиг-нал - выход), tSU (синхросигнал - время установки), fMAX (частота синхросигнала).

Команда Global Project Logic Synthesis позволяет сделать глобальные уста-новки для компилятора в части логического синтеза проекта.

Все пять редакторов MAX PLUS II и три редактора создания дизайна (гра-фический, текстовый и сигнальный) имеют общие функции, такие как, например, создание, сохранение и открытие файла. Кроме того, приложения редактора MAX PLUS II имеют следующие общие функции: создание файлов символов и файлов с прототипами функций (Include-файлы); поиск узлов; траверз иерархического де-рева; всплывающие окна меню, зависящего от контекста;

временной анализ; поиск и замена фрагментов текста; отмена последнего шага редактирования, его возвра-щения, вырезка, копирование, вставка и удаление выбранных фрагментов, обмен фрагментами между приложениями MAX PLUS II или приложениями Windows; печать.

Графический редактор (Graphic Editor) обеспечивает проектирование в ре-альном формате изображения (WYSIWIG). Графические файлы проекта (.gdf) или схемные файлы OrCAD (.sch), созданные в данном графическом редакторе, могут включать любую комбинацию символов примитивов, мегафункций и макрофункций. Символы могут представлять собой любой тип файла проекта (.gdf .sch .tdf .vhd .v .wdf .edf .xnf .adf .smf).

Инструмент выбора ("стрелка") облегчает разработку дизайна. Он позволя-ет двигать и копировать объекты, а также вводить новые символы. Когда вы помещаете его на контакт или конец линии, он автоматически преобразуется в инст-румент рисования ортогональных линий. Если им щелкнуть на тексте, он автоматически преобразуется в инструмент редактирования текста.

Графический редактор обеспечивает ряд других возможностей. Например, можно увеличивать или уменьшать масштаб отображения на экране, выбирать гарнитуру и размер шрифта, задавать стили линий, устанавливать и отображать направляющие, получать зеркальное отображение, поворачивать выделенные фрагменты на 90, 180 или 270 градусов; задавать размер и ориентацию текущего листа схемы.

Символьный редактор (Symbol Editor) позволяет просматривать, создавать и редактировать символ. Символьный файл имеет то же имя, что и проект, и расширение ".sym". Команда Creat Default Symbol меню File, которая есть в графиче-ском, текстовом и сигнальном редакторах, создает символ для любого файла проекта. Символьный редактор обладает следующими характеристиками: можно переопределить символ, представляющий файл проекта, создавать и редактировать выводы и их имена, используя входные, выходные и двунаправленные выводы, а также задавать варианты ввода символа в файл графического редактора, задать значения параметров и их значения по умолчанию; сетка и направляющие помо-гают выполнить точное выравнивание объектов, в символе можно вводить комментарии.

Текстовый редактор (Text Editor) является инструментом для создания тек-стовых файлов проекта на языках описания аппаратуры: AHDL (.tdf), VHDL (.vhd), Verilog HDL (.v). В этом текстовом редакторе можно работать также с про-извольным файлом формата ASCII. Все перечисленные файлы проекта можно создавать в любом текстовом редакторе, однако данный редактор имеет встроенные возможности ввода файлов проекта, их компиляции и отладки с выдачей сообще-ний об ошибках и их локализацией в исходном тексте или в тексте вспомогательных файлов; кроме того, существуют шаблоны языковых конструкций для AHDL, VHDL и Verilog HDL, выполнено окрашивание синтаксических конструкций. В данном редакторе можно вручную редактировать файлы назначений и конфигура-ции (.acf), а также делать установки конфигурации для компилятора, симулятора и временного анализатора.

Пользуясь данным текстовым редактором, можно создавать тестовые векто-ры (.vec), используемые для тестирования, отладки функций и при вводе сигнального проекта. Можно также создавать командные файлы (.cmd - для симулятора и .edc - для EDIF), а также макробиблиотеки (.lmf). В текстовом редакторе MAX PLUS II обеспечивается контекстная справка.

Сигнальный редактор (Waveform Editor) служит инструментом создания описания проекта, ввода тестовых векторов и просмотра результатов тестирования. Пользователь может создавать сигнальные файлы проекта (.wdf), которые со-держат временные диаграммы, описывающие логику работы проекта, а также файлы каналов тестирования (.scf), которые содержат входные вектора для тестирования и функциональной отладки. Разработка описания проекта в сигнальном редакторе является альтернативой его созданию в графическом или текстовом редакторах. Здесь можно графическим способом задавать комбинации входных ло-гических уровней и требуемых выходов. Созданный таким образом файл WDF может содержать как логические входы, так и входы цифрового автомата, а также выходы комбинаторной логики, счётчиков и цифровых автоматов. Способ разра-ботки дизайна в сигнальном редакторе лучше подходит для цепей с чётко опреде-лёнными последовательными входами и выходами, то есть для цифровых автоматов, счётчиков и регистров.

С помощью сигнального редактора можно легко преобразовывать времен-ные диаграммы сигналов целиком или частично, создавая и редактируя узлы и группы. Простыми командами можно создавать файл таблицы ASCII-символов (.tbl) или импортировать файл тестовых векторов в формате ASCII (.vec) для создания файлов тестируемых каналов SCF и сигнального дизайна WDF. Можно также сохранить файл WDF как SCF для проведения тестирования или преобразо-вать SCF в WDF для использования его в качестве файла проекта.

Сигнальный редактор имеет следующие отличительные черты: можно соз-дать или отредактировать узел, задав его тип; при разработке WDF можно задать тип логики узла, задать значения по умолчанию в логическом узле, а также имя состояния по умолчанию в узле типа цифрового автомата, для упрощения создания тестового вектора можно легко добавить в файл тестируемых каналов SCF несколько узлов или все из информационного файла симулятора (.snf), существую-щего для полностью откомпилированного проекта, можно объединять от 2 до 256 узлов для создания новой группы (шины) или разгруппировывать объединённые ранее в группу узлы. Можно также объединять группы с другими группами. Зна-чение группы может быть отображено в двоичной, десятичной, шестнадцатерич-ной или восьмеричной системе счисления с преобразованием или без в код Грэя, можно копировать, вставлять, перемещать или удалять выбранную часть ("интер-вал") сигнала, а также весь узел или группу. Можно также инвертировать, встав-лять, переписывать, повторять, расширять или сжимать интервал сигнала любой длины с любым логическим уровнем, тактовым сигналом, последовательностью счёта или именем состояния, задать сетку для выравнивания переходов между ло-гическими уровнями, в любом месте файла можно вводить комментарии между сигналами, менять масштаб отображения.

Для облегчения тестирования можно сделать наложение любых выходов в текущем файле или наложить второй файл сигнального редактора для сравнения сигналов его узлов и групп с соответствующими сигналами текущего файла.

Поуровневый планировщик (Floorplan Editor) предназначен для назначения ресурсов физических устройств и просмотра результатов разводки, сделанных компилятором. В окне поуровневого планировщика могут быть представлены два типа изображения:

- Device View (Вид устройства) показывает все контакты устройства и их функции;
- LAB View (Вид логического структурного блока) показывает внутреннюю часть устройства, в том числе все логические структурные блоки (LAB) и отдельные логические элементы.

После выполнения всех назначений и задания проекта приступают к его компиляции. Сначала компилятор извлекает информацию об иерархических связях между файлами проекта и проверяет проект на простые ошибки ввода описания проекта.

Компилятор применяет разнообразные способы увеличения эффективности проекта и минимизации использования ресурсов устройства. Если проект слишком большой, чтобы быть реализованным в одном устройстве, компилятор может автоматически разбить его на части для реализации в нескольких устройствах того же самого семейства, при этом число соединений между устройствами минимизи-руется. В файле отчёта (.rpt) затем будет отражено, как проект будет реализован в одном или нескольких устройствах.

Кроме того, компилятор создает программирующие файлы, используемые программатором для программирования одного или нескольких устройств. У разработчика также есть возможность настроить обработку проекта. Например, мож-но задать стиль логического синтеза проекта по умолчанию и другие параметры логического синтеза в рамках всего проекта, что позволит провести логический синтез в соответствии с вашими потребностями. Кроме того, вы можете ввести требования по синхронизации в рамках всего проекта, точно задать разбиение большого проекта на части для реализации в нескольких устройствах и выбрать варианты параметров устройств, которые будут применены для всего проекта в целом. Загрузку готового проекта в ПЛИС или конфигурационное ПЗУ выполня-ют с помощью программатора (Programmer).

В современных САПР поддерживаются как стандартизованные языки опи-сания аппаратуры, такие как VHDL и Verilog HDL, так и языки описания аппаратуры, разработанные компаниями-производителями ПЛИС специально для ис-пользования только в своих САПР и учитывающих архитектурные особенности конкретных семейств ПЛИС.

5.4.3. Язык описания аппаратуры VHDL

Языки описания аппаратуры (Hardware Description Language) являются формальной записью, которая может быть использована на всех этапах разработки цифровых электронных систем. Это возможно вследствие того, что язык легко воспринимается как машиной, так и человеком. Он может использоваться на этапах проектирования, верификации, синтеза и тестирования аппаратуры, а также для передачи данных о проекте, модификации и сопровождения. Существует не-сколько разновидностей этих языков: AHDL, VHDL, VerilogHDL, Abel и др. Известны также случаи использования стандартных языков программирования, например Си, для описания структуры БИС.

Ряд языков описания аппаратуры (AHDL, Abel) предназначены для описания систем на ПЛИС, другие появились изначально как средство моделирования цифровых систем, а затем стали инструментом их описания.

Одним из наиболее универсальных языков описания аппаратуры является VHDL, первый стандарт которого был разработан в 1983-1987 годах при спонсорстве Минобороны США. На этом языке возможно как поведенческое, так структурное и потоковое описание цифровых схем.

VHDL поддерживает три различных стиля для описания аппаратных архи-тектур.

1. Структурное описание (structural description), в котором архитектура представляется в виде иерархии связанных компонентов.

2. Потоковое описание (data-flow description), в котором архитектура представляется в виде множества параллельных регистровых операций, каждая из которых управляется вентильными сигналами. Потоковое описание соответствует стилю описания, используемому в языках регистровых передач.

3. Поведенческое описание (behavioral description), в котором преобразование описывается последовательными программными предложениями, которые похожи на имеющиеся в любом современном языке программирования высокого уровня.

Все три стиля могут совместно использоваться в одной архитектуре. Струк-турное и потоковое описание используется в основном для проектирования цифровых схем, поведенческое - только для моделирования, так как содержит конструкции, которые невозможно реализовать в виде схемы.

Наиболее важными в языке VHDL являются понятия параллелизма и иерархии.

Объект проекта (entity) представляет собой описание компоненты проекта, имеющей чётко заданные входы и выходы и выполняющей чётко определённую функцию. Объект проекта может представлять всю проектируемую систему, некоторую подсистему, устройство, узел, стойку, плату, кристалл, макроячейку, логический элемент и т. п. В описании объекта проекта можно использовать компо-ненты, которые, в свою очередь, могут быть описаны как самостоятельные объек-ты проекта более низкого уровня. Таким образом, каждый компонент объекта проекта может быть связан с объектом проекта более низкого уровня. В результате такой декомпозиции пользователь строит иерархию объектов проекта, представ-ляющих весь проект в целом и состоящую из нескольких уровней абстракций. Та-кая совокупность объектов проекта называется **иерархией проекта** (design hierarchy).

Каждый объект проекта состоит, как минимум, из двух различных типов описаний: описания интерфейса и одного или более архитектурных тел. Интерфейс описывается в **объявлении объекта проекта** (entity declaration) и определяет только входы и выходы объекта проекта.

Для описания поведения объекта или его структуры служит **архитектурное тело** (architecture body). Чтобы задать, какие объекты проекта использованы для создания полного проекта, используется **объявление конфигурации** (configuration declaration).

В языке VHDL предусмотрен механизм пакетов для часто используемых описаний, констант, типов, сигналов. Эти описания помещаются в **объявлении пакета** (package declaration). Если пользователь использует нестандартные операции или функции, их интерфейсы описываются в объявлении пакета, а тела содержатся в **теле пакета** (package body).

Таким образом, при описании цифровых схем на языке VHDL, возможно использование пяти различных типов описаний: объявление объекта проекта, архитектурное тело, объявление конфигурации, объявление пакета и тело пакета. Каждое из описаний является самостоятельной конструкцией языка VHDL, может быть независимо проанализирована анализатором и поэтому получило название **"модуль проекта"** (design unit). Модули проекта, в свою очередь, можно разбить на две категории: **первичные** и **вторичные.** К первичным модулям относятся различного типа объявления. К вторичным - отдельно анализируемые тела первичных модулей. Один или несколько модулей проекта могут быть помещены в один файл, называемый **файлом проекта** (design file). Каждый проанализированный модуль проекта помещается в

библиотеку проекта (design library) и становится **библиотечным модулем** (library unit). Данная реализация позволяет создать лю-бое число библиотек проекта. Каждая библиотека проекта в языке VHDL имеет логическое имя (идентификатор). Фактическое имя файла, содержащего эту биб-лиотеку, может совпадать или не совпадать с логическим именем библиотеки про-екта. Для ассоциирования логического имени библиотеки с соответствующим ей фактическим именем предусмотрен специальный механизм установки внешних ссылок.

Объекты данных (data object) являются хранилищами для значений определённого типа. Следует заметить, что все типы в VHDL конструируются из элементов, представляющих собой скалярные типы. Значения всех объектов в создавае-мой модели, взятые все вместе, отражают текущее состояние моделирования. Описание на VHDL содержит объявления, которые создают объекты данных че-тырёх классов: константы, переменные, сигналы и файлы.

Константы и переменные содержат одно значение данного типа. Значения переменных могут быть изменены назначением нового значения в предложении назначения переменной. Значение константы устанавливается до начала модели-рования и не может после этого изменяться.

Сигнал имеет текущее значение подобно переменной. Он также имеет прошлую историю значений, на которые разработчик может сослаться, а также множество будущих значений, которые будут получены от формирователей сигналов. Новые значения для сигналов создаются предложениями назначения сигналов. Каждый объект в описании должен ассоциироваться с одним и только одним ти-пом. Тип состоит из множества возможных значений и множества операций. Имеются операции двух видов. Некоторые операции являются предопределёнными, на пример, операторы "+", "-" для значений типа integer. Другие операции яв-но кодируются в VHDL; например, может быть написана функция подпрограмма Max, которая возвращает наибольший из двух целых аргументов. Тип объекта представляет информацию, которая окончательно определяется в момент записи модели. Эта информация способствует обнаружению несоответствий в тексте без обращения к моделированию. Например, легко обнаружить и отметить попытку назначения булевого значения (True или False) целой переменной. Новое значение, которое должно быть создано предложением назначения, определяется выражени-ем в правой части. Выражения используются также и в других контекстах, напри-мер, как условие в предложении if. В состав выражения могут входить константы, переменные, сигналы, операторы и указатели функций. Когда имя объекта используется в выражении, при расчёте значения выражения учитывается его текущее значение.

Рассмотрим некоторые примеры описания цифровых схем на VHDL.

Примером описания цифрового автомата является преобразователь параллельного кода в последовательный [22]. Преобразователь кода представляет собой устройство, на вход которого подается n-битное число в параллельном коде "d", сигнал загрузки "load" и синхроимпульсы "clk". По сигналу загрузки происходит запись входного слова во внутренний регистр и последовательная выдача в тече-нии n тактов этого входного слова в последовательном коде на выходе "o" син-хроимпульсами "oclk". После окончания преобразования на выходе "e" появляет-ся высокий уровень сигнала в течение одного такта. Такого рода преобразователи кода часто используются для управления синтезаторами частот 1104ПЛ1 и им подобными.

Описание этого устройства на языке VHDL приведено в таблице 5.2.

Таблица 5.2

```
library ieee;
use ieee.std_logic_1164.all;
entity Serial is
  port  (
 clk   : in STD_LOGIC;
                load  : in STD_LOGIC;
                reset : in STD_LOGIC;
                d : in STD_LOGIC_vector (3 downto 0);
                oclk  : out STD_LOGIC;
                o : out STD_LOGIC;
                e : out STD_LOGIC
                );
end;
architecture behavioral of Serial is
  type t1 is range 0 to 4;
  signal s : STD_LOGIC_vector (2 downto 0);
  signal i : t1;
begin
process (clk)
  begin
  if reset = «1» then
                i <=0;
  else
       if (clk'event and clk='1') then
                     if (i = 0 and load = «1») then
                                  s(2 downto 0) <= d(3 downto 1);
                                  o <= d(0);
                                  i <= 4;
```

```
end if;
                if (i > 1) then
                        o <= s(0);
                        s(1 downto 0) <= s(2 downto 1);
                 i <= i - 1;
                end if;
                if (i = 1) then
                        e <= «1»;
                        i <= 0;
                else
                        e <= «0»;
                end if;
                end if;
        end if;
        if i >0 then
        oclk <= not clk;
        else
        oclk <= «0»;
    end if;

end process;
 end behavioral;
```

По переднему фронту синхроимпульса "clk" при высоком уровне на входе загрузки происходит загрузка трёх старших бит входного слова d[3..1] во времен-ный регистр s[2..0]. Младший бит входного слова d[0] подаётся на выход "o". На выходе "oclk" появляются синхроимпульсы. На сигнале "i" собран внутренний счётчик, выдающий сигнал окончания

преобразования "e". При поступлении по-следующих синхроимпульсов происходит выдача на выход "o" остальных бит входного слова, хранящихся в регистре s[2..0].

Результаты моделирования представлены на рис. 5.7.

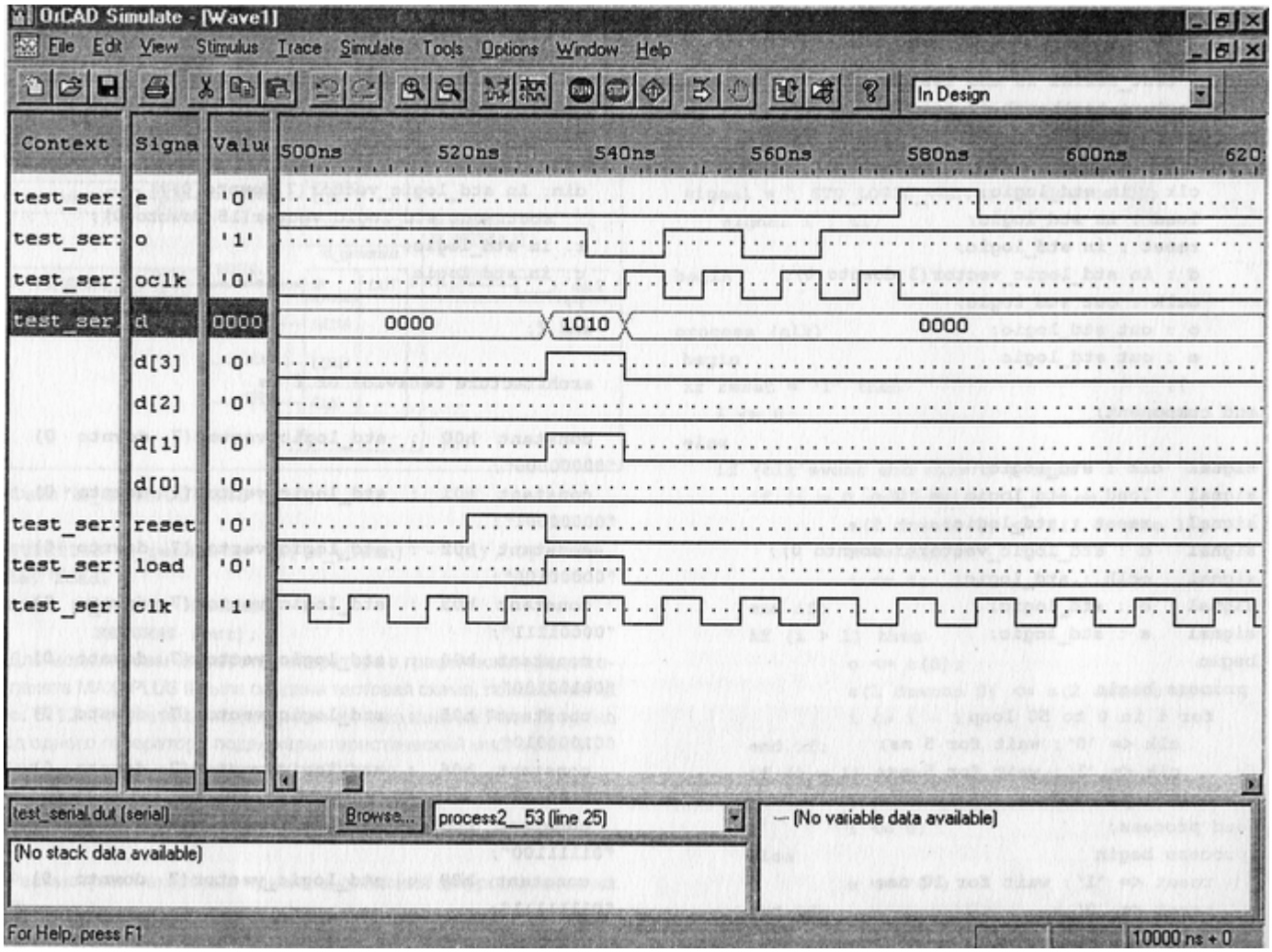

Рис. 5.7. Результаты моделирования

5.5. Системы на кристалле

Если для реализации сложных методов обработки информации необходимо применение достаточно мощных аппаратно-программных комплексов, то многие отработанные и массово применяемые методы преобразования и кодирования ин-формации могут быть реализованы с использованием относительно несложных вычислителей типа однокристальных микроконтроллеров. Однако здесь также желательна проблемная ориентация таких вычислителей, направленная на разме-щение всех необходимых для создания конкретного устройства узлов на одном кристалле (для снижения стоимости и массогабаритных характеристик). Создание подобных специализированных средств ЦОС возможно на основе концепции сис-тем на кристалле (SOC - System on a Crystal).

Идея концепции состоит в размещении на кристалле полупроводникового материала как вычислительного ядра - микропроцессора со стандартными пери-ферийными узлами - так и специализированных интерфейсных и, возможно, вы-числительных и других узлов, необходимых для решения конкретного круга задач. При этом обеспечивается выбор готовых наработок подобных узлов - блоков ин-теллектуальной собственности (Intellectual Property) благодаря

развивающейся системе международного (на уровне компаний-разработчиков и производителей) сотрудничества в рамках ассоциаций заинтересованных организаций. Ведущую роль здесь играет организация Virtual Socket Interface Alliance (VSIA), объединив-шая ведущие электронные фирмы м сосредоточившая свою деятельность на раз-работке эффективных методов повторного использования IP-блоков и развитии стандартов по созданию, обмену и интеграции IP.

SOC можно определить [16] как сложную интегральную схему, объединяющую в одном чипе или чипсете все основные фнкциональные элементы полного конечного продукта. В перспективе могут быть решены проблемы интеграции как аналоговых, цифровых и радиочастотных (RF) структур, так и микроэлектромеха-нических (MEMS) систем, реализующих датчики, микроприводы, оптические, химические и биохимические элементы.

Проектирование SOC - сложный процесс, доступный компаниям, спициализирующимся на разработке электронных компонентов. Существует два основных подхода к проектированию - на основе IP-блоков и так называемое платформен-ное проектирование. Второй подход основан на использовании более крупных на-боров компонентов, составляющих платформу, ориентированную на конкретное приложение либо конкретный процессор (процессорное ядро).

Общий маршрут проектирования систем на кристалле [А. Бухтеев] состоит из следующих основных этапов:

- концептуальное проектирование системы; основной задачей данного этапа является исследование проектируемой системы и получение её исполняе-мых спецификаций на языке высокого уровня (стандартно на C/C++);
- проектирование, то есть трансформация исполняемой спецификации проекта на уровень регистровых передач (получение спецификаций на языках описания схем Verilog/VHDL) и далее на вентильный уровень;
- верификация проекта, то есть проверка проекта и проектных решений на соответствие исходной спецификации и другим требованиям в процессе проектирования и детализации;
- физическое проектирование, начиная от выбора технологического и библиотечного базиса и заканчивая получением финального описания проекта в формате GDSII.

Отечественные компании также начинают подключаться к этой деятельности, в качестве примера можно привести разработку однокристального звукового микроконтроллера UNC81SRV01 ООО "Юникор микросистемы", который с успе-хом может применяться для реализации устройств защиты речевой информации благодаря интегрированным на кристалле аналого-цифровым и цифро-аналоговым преобразователям и умножителям-аккумуляторам.

5.5.1. Звуковой микроконтроллер

Микроконтроллер UNC81SRV01 (рис. 5.8) реализован с использованием технологии с проектными нормами 0,18 мкм. На кристалле размещен высокоэф-фективный RISC процессор UNC80 с гарвардской архитектурой, память программ и данных, а также периферийные узлы, обеспечивающие аппаратную поддержку алгоритмов ввода-вывода и обработки звуковых сигналов. Каждая команда испол-няется за 1 такт. Имеется быстрый стек контекста, ускоряющий переключение контекста при прерываниях и вызовах подпрограмм. Три регистровых файла по 8 8-разрядных регистров отображаются на произвольные области внутренней памя-ти данных, а один из них - дополнительно на области регистров процессора и пе-риферийных устройств. Два индексных регистра обеспечивают косвенную адре-сацию с настраиваемой постмодификацией,

обеспечивая эффективные пересылки, в том числе из памяти в память, а также пересылки строк байтов. В составе про-цессора имеется аппаратный умножитель 8?8.

Двухпортовая память данных объёмом 8 Кбайг поддерживает команды типа "память-память". Энергонезависимая стираемая Flash-память программ объёмом 128 Кбайт (64К?16) может перепрограммироваться через аппаратный буфер 512 байт, размещённый в конце адресного пространства данных.

Набор периферийных устройств, размещённых на кристалле, обеспечивает минимизацию внешней "обвязки" микроконтроллера при построении прикладных систем, а также уменьшение времени обработки сигналов.

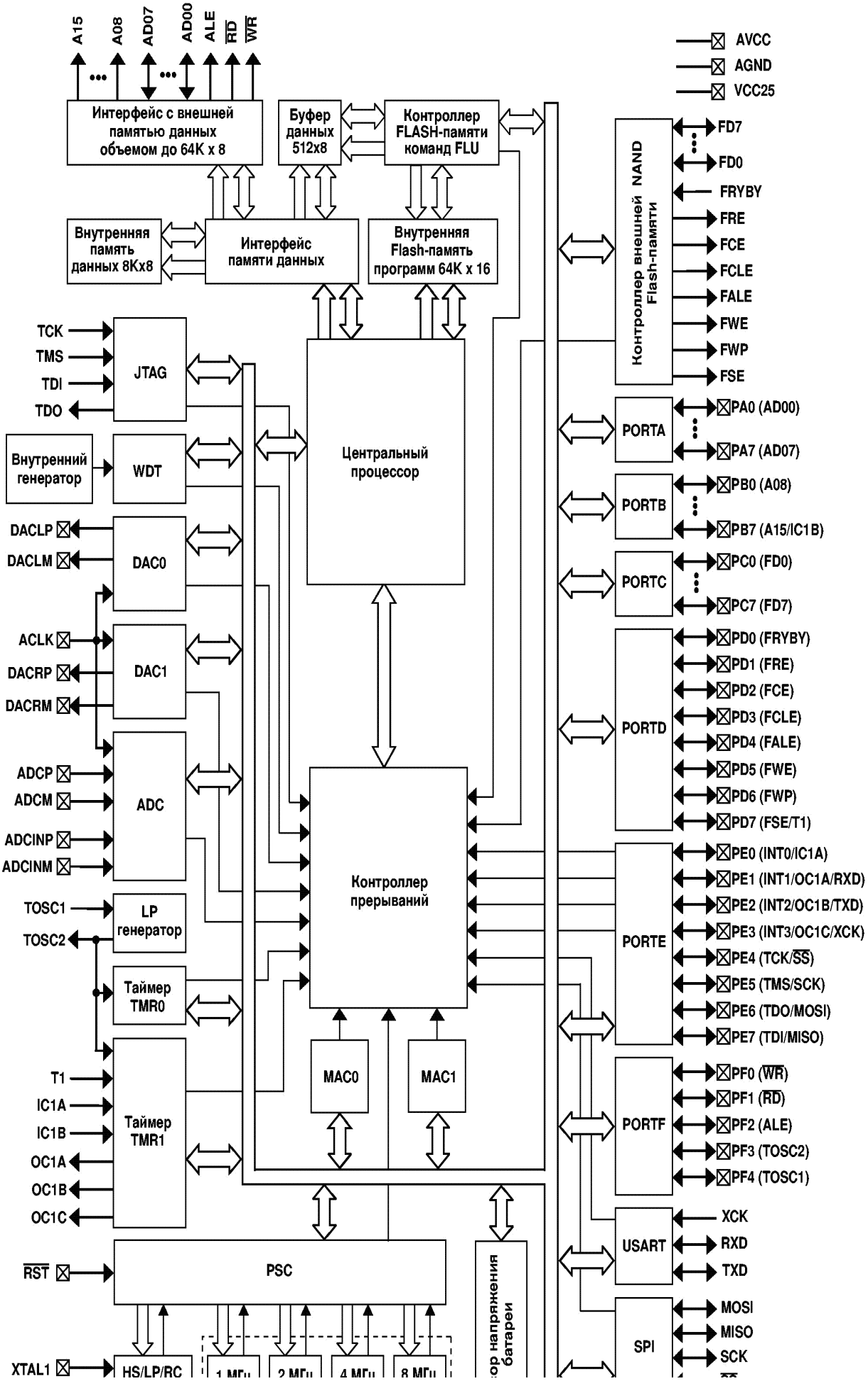
A15
A08
AD07
AD00
ALE
RD
WR
Интерфейс с внешней памятью данных объемом до 64K x 8
Буфер данных 512x8
Контроллер FLASH-памяти команд FLU
Внутренняя память данных 8Kx8
Интерфейс памяти данных
Внутренняя Flash-память программ 64K x 16
AVCC
AGND
VCC25
Контроллер внешней NAND Flash-памяти
FD7
FD0
FRYBY
FRE
FCE
FCLE
FALE
FWE
FWP
FSE
TCK
TMS
TDI
TDO
JTAG
Центральный процессор
Внутренний генератор
WDT
PORTA
PA0 (AD00)
PA7 (AD07)
PORTB
PB0 (A08)
PB7 (A15/IC1B)
DACLP
DACLM
DAC0
PORTC
PC0 (FD0)
PC7 (FD7)
ACLK
DACRP
DACRM
DAC1
PORTD
PD0 (FRYBY)
PD1 (FRE)
PD2 (FCE)
PD3 (FCLE)
PD4 (FALE)
PD5 (FWE)
PD6 (FWP)
PD7 (FSE/T1)
ADCP
ADCM
ADCINP
ADCINM
ADC
Контроллер прерываний
PORTE
PE0 (INT0/IC1A)
PE1 (INT1/OC1A/RXD)
PE2 (INT2/OC1B/TXD)
PE3 (INT3/OC1C/XCK)
PE4 (TCK/SS)
PE5 (TMS/SCK)
PE6 (TDO/MOSI)
PE7 (TDI/MISO)
TOSC1
TOSC2
LP генератор
Таймер TMR0
MAC0
MAC1
PORTF
PF0 (WR)
PF1 (RD)
PF2 (ALE)
PF3 (TOSC2)
PF4 (TOSC1)
T1
IC1A
IC1B
OC1A
OC1B
OC1C
Таймер TMR1
USART
XCK
RXD
TXD
RST
PSC
SPI
MOSI
MISO
SCK
XTAL1
HS/LP/RC
1 МГц
2 МГц
4 МГц
8 МГц
Монитор напряжения батареи

Рис. 5.8. Функциональная схема звукового микроконтроллера

В состав микроконтроллера, помимо процессорного ядра и памяти, входят два 16-разрядных таймера-счётчика T0 и T1, сторожевой таймер WDT, програм-мируемый контроллер синхронизации PSC, универсальный синхронно-асинхронный последовательный интерфейс USART, синхронный последователь-ный интерфейс SPI, интерфейс внешней NAND Flash-памяти 8 Мбайт и 5 про-граммируемых параллельных портов ввода-вывода. Эффективную внутрисистемную отладку и программирование обеспечивает JTAG-интерфейс.

Проблемную ориентацию микроконтроллера осуществляют 16-разрядные дельтасигма блоки аналого-цифрового и цифро-аналогового преобразования, а также два умножителя-аккумулятора (MAC0 и MAC1), реализующие покомпо-нентное перемножение двух массивов 16-разрядных данных с накоплением 40-разрядной суммы произведений и обеспечивающие эффективную реализацию ал-горитмов спектрального анализа и цифровой фильтрации сигналов. Блоки MAC имеют собственную память ёмкостью 2*512 16-разрядных слов, загружаемую в режиме DMA из памяти данных и программ, и работают независимо друг от друга и основного процессора.

Средства разработки обеспечивают полный цикл разработки и отладки приложений с использованием интегрированной среды разработки, объединяю-щей транслятор с языка Ассемблера, оптимизирующий компилятор C, компонов-щик, библиотекарь, набор стандартных библиотек и библиотек реального времени языка C, программный симулятор и внутрисхемный эмулятор на основе JTAG. SDK может поставляться в комплекте с отладочными модулями, предусматри-вающими различные конфигурации внешних устройств (индикаторов, элементов управления, предварительных и выходных усилителей и т.д.), необходимых для оценки возможностей построения конкретных прикладных систем.

Библиотека прикладных программ обработки звука предназначена для создания на основе речевой микросхемы прикладных устройств пользователей, использующих комплекс речевых технологий - алгоритмов распознавания, синте-за, кодирования и воспроизведения речевых, музыкальных и других сигналов.

Первая очередь библиотеки включает набор программных модулей обработки звука:

- модуль распознавания изолированно произносимых слов и слитных фраз ограниченного словаря с подстройкой под диктора - дикторозависимое рас-познавание (ДЗР);
- модуль распознавания изолированно произносимых слов и слитных фраз ограниченного словаря без подстройки под диктора - дикторонезависимое распознавание (ДНР);
- модуль компилятивного синтеза речи на уровне слов и слитных фраз (КСР);
- модуль записи и воспроизведения речи с различной степенью сжатия (ЗВР)

В последующем планируется дополнить библиотеку модулями синтеза речи по произвольному тексту (ТТС) и синтеза музыки (МС), а также распознавания слитной речи (на базе 32-разрядного микроконтроллера).

Алгоритмы распознавания речи, реализуемые в настоящее время, обеспечи-вают распознавание словарей объёмом до 64 слов и слитно произносимых слово-сочетаний с надёжностью 99% для ДЗР и 95% для ДНР в условиях шумов офис-ного помещения с использованием близкорасположенного микрофона (гарнитура) либо встроенного в аппаратуру (удалённого до 2 м) микрофона. Типы словарей - предопределённый (ДНР), пользовательский (ДЗР, ДНР). Для ДЗР применяются алгоритмы на основе субоптимальных модификаций

динамического программи-рования [19], ДНР реализуется на основе неявных Марковских моделей.

Группа алгоритмов синтеза, записи и воспроизведения речи использует ряд общих программных модулей, обеспечивающих кодирование - декодирование ре-чевых сигналов с различными сочетаниями качества и степени сжатия информа-ции - от 0,5 до 8 Кбайт/с. При этом объёмы словарей для КСР и ЗВР ограничены ёмкостью памяти и с учётом возможности применения внешней Flash памяти объ-ёмом до 8 Мбайт могут достигать 4 ч. Для предопределённых словарей преду-смотрены библиотечные функции озвучивания типовых фраз (например, числи-тельных для различных единиц измерения и входных форматов числовых данных).

Введение.

Лекции – 1 час. Самостоятельная работа – 2 час.

Основные понятия и определения. Информация. Безопасность. За-щита речевой информации как составная часть комплексной безопасности организации, предприятия. Классификация угроз и методов борьбы с ними. Речевые технологии, их роль и место в защите речевой информации.

Раздел 6. Правовые вопросы ЗРИ

Лекции – 1 час. Самостоятельная работа – 2 час.

Государственная система защиты информации Нормативные акты правового регулирования вопросов информатизации и защиты информации в России. Структура, задачи и основные функции Государственной систе-мы защиты информации. Лицензирование. Сертификация средств защиты. Аттестация объектов информатизации.

Раздел 7. Организационные вопросы ЗРИ

Лекции – 1 час. Самостоятельная работа – 2 час.

Организация защиты информации в государственных и коммерче-ских структурах. Категории секретности (конфиденциальности) информа-ции, их связь с уровнем организационных мероприятий по защите инфор-мации. Классификация и методы реализации организационных мер по защите речевой информации.

Раздел 8. Аппаратно-программная реализация средств ЗРИ

Лекции – 8 час. Практические занятия – 14 час. Самостоятельная ра-бота – 12 час.

Тема 8.1. Современная элементная база цифровой обработки сигналов (ЦОС)

Лекции 6 час.

Цифровые сигнальные процессоры (ЦСП) и программируемые логические интегральные схемы (ПЛИС) как взаимодополняющие универсальные программируемые средства реализации соответственно последовательных и параллельных устройств обработки информации. Разграничение функций ЦСП и ПЛИС при создании средств ЗРИ. Номенклатура и характеристики современных ЦСП и ПЛИС. Архитектура ЦСП (на примере сигнальных процессоров фирмы Analog Devices). Возможности создания многопроцессорных вычислителей. Виды ПЛИС. Особенности и возможности проектирования устройств обработки информации на основе ПЛИС. Возможности создания специализированных средств ЦОС на основе концепции систем на кристалле (SOC – System on Crystal). Отечественная элементная база ЦОС.

Практические занятия

☐ Архитектура и система команд ADSP-21xxx – 2 час.
☐ Структура и характеристики ПЛИС Altera – 2 час.

Тема 8.2. Инструментальные средства создания приложений ЦОС

Лекции 1 час.

Интегрированные среды разработки на примере Visual DSP фирмы Analog Devices и Max Plus фирмы Altera. Примеры реализации алгоритмов обработки речевых сигналов с применением языков Ассемблер, Си, VHDL.

Практические занятия

☐ Реализация фильтров на ADSP – 2 час.
☐ Генератор псевдослучайных последовательностей на ПЛИС – 2 час.

Тема 8.3. Методы моделирования и экспериментального иссле-дования алгоритмов ЗРИ

Лекции 1 час.

Обоснование необходимости создания приложений ЗРИ на основе современных алгоритмических и аппаратных средств. Сигнальные редак-торы. Библиотеки речевых приложений пакетов Matlab и LabView. Примеры моделирования алгоритмов обработки сигналов.

Практические занятия

☐ Изучение интерфейсов программных средств – 2 час.
☐ Исследование методов модуляции-демодуляции сигналов – 4 ч

Раздел 9. Свойства и характеристики речевых сигналов

Лекции – 20 час. Практические занятия – 22 час. Самостоятельная работа – 20 час.

Определения и классификация. Речевая информация. Речевой сигнал. Речевые технологии.

Тема 9.1. Модели речеобразования и восприятия речи.

Лекции 4 час.

Речевой тракт. Артикуляторные органы. Процесс речеобразования. Источники возбуждения голосовых колебаний. Классификация звуков речи по способу и месту образования. Дифференциальные признаки. Связь между фонетическими и акустическими характеристиками речевых сигналов. Физические и математические модели речевого тракта. Синтез речи.

Периферическая слуховая система. Устройство и функции наружно-го, среднего и внутреннего уха. Характеристики слухового восприятия. Кривые чувствительности. Критические полоски слуха. Эффект маскировки. Модели обработки речи в центральной нервной системе.

Практические занятия

☐ Моделирование формантного синтезатора речи – 4 час.

.Тема 9.2. Методы обработки речевых сигналов

Лекции 8 час.

Классификация методов обработки речевых сигналов. Временные, спектральные, корреляционные характеристики. Аналоговые и цифровые представления и преобразования. Вероятностные, корреляционные и спек-тральные характеристики речевых сигналов. Нестационарный характер ре-чевых сигналов. Спектральные базисы представления речи. Спектрально-полосный анализ. Динамический спектральный анализ. Вейвлет-анализ. Гомоморфный анализ. Линейное предсказание. Линейные спектральные пары. Выделение основного тона, признаков «тон-шум», голосовой активности

Практические занятия

☐ Методы спектрального представления речевых сигналов – 4 час.
☐ Исследование алгоритмов линейного предсказания– 4 час.
☐ Исследование методов выделения основного тона – 2 час.

Тема 9.3. Методы кодирования речевой информации

Лекции 8 час.

Роль и место цифровых и аналоговых методов кодирования речевых сигналов в системах передачи речи. Вокодеры: классификация, характери-стики. Полосные, формантные, фонемные вокодеры. Современные теле-коммуникационные стандарты в передаче речи. Цифровые каналы связи. Мобильная связь. IP-телефония.

Практические занятия

☐ Исследование речевых кодеков стандартов G.721, G.723.1, G.729– 8 час.

Раздел 10. Методы ЗРИ

Лекции – 20 час. Практические занятия – 15 час. Самостоятельная работа – 30 час.

Тема 10.1. Акустические характеристики среды

Лекция 2 час.

Распространение акустических волн в воздухе и твердых телах, процессы на границе двух сред с различными плотностями. Отражение и по-глощение акустических волн в среде распространения. Понятие о реверберации.

Тема 10.2. Каналы утечки речевой информации

Лекции 6 час.

Классификация технических каналов утечки информации. Их структурная схема. Технические каналы утечки речевой информации, образующиеся в выделенных помещениях (акустический, виброакустический, электроакустический, за счет навязывания и т.п.) Утечка речевой информации по проводным коммуникациям. Акустоэлектрические преобразования и высокочастотное "навязывание" (облучение). Побочные электромагнитные излучения и наводки (ПЭМИН). Утечка акустической информации за счет прямого и модуляционного акустоэлектрических преобразований. Электромагнитный, электродинамический, и др. эффекты. Утечки акустической информации за счет параметрического преобразования. Механизмы параметрической модуляции. Утечки акустической информации за счет оптико-электронного (лазерного) излучения. Технические каналы утечки информации, создаваемые за счет использования закладных устройств. Структура и демаскирующие признаки закладных устройств. Технические каналы перехвата информации, передаваемой по каналам связи. Электрические, электромагнитные и индукционные методы перехвата информации, их демаскирующие признаки.

Тема 10.3. Методы обнаружения утечек речевой информации

Лекции 4 час.

Визуальное обследование, поиск с применением пассивных и активных технических средств. Классификация методов обнаружения утечки информации по характеру среды распространения, типу физических полей. Номенклатура и характеристики технических средств выявления каналов утечки информации. Индикаторы поля. Сканирующие приемники. Локаторы нелинейностей. Определители диктофонов. Анализаторы телефонных и проводных линий.

Практические занятия

☐ Средства обнаружения утечек речевой информации – 4час.

Тема 10.4. Методы предотвращения утечки речевой информации

Лекции 4 час.

Организационно-технические мероприятия, направленные на предотвращение утечки речевой информации. Контроль и ограничение досту-па. Локализация излучений: звукоизоляция, экранирование, заземление. Установка развязок, фильтров, диэлектрических вставок в трактах, имею-щих выход за пределы зоны контроля. Пространственное и линейное за-шумление, подавление диктофонов и сотовых телефонов, уничтожение (выжигание) закладных устройств.

Практические занятия

☐ Исследование методов заземления и фильтрации – 3 час.

Тема 10.5. Методы закрытия речевой информации

Лекции 4 час.

Возможности закрытия речевой информации при передаче по каналам связи. Скремблирование во временной и частотной области. Шифро-вание при передаче кодированной речевой информации по цифровым кана-лам. Основные сведения о криптографических методах. Стеганографиче-ские методы. Системы связи на широкополосных и сверхширокополосных сигналах.

Практические занятия

☐ Исследование методов формирования и приёма широкополосных сигналов – 4 час.
☐ Реализация временного скремблирования на ПЛИС – 4 час.

Структура курса:

Лекции: 51 час

Практические занятия: 51 час

Курсовая работа: 34 часа

Самостоятельная работа: 68 часов

Тематический план

Наименование разделов и тем	Ауд.занятий,всего,час.	Лекций,час.	Практич.занятий,час	Самост.работа,час
Введение	1	1	-	2
Раздел 1. Правовые вопросы ЗРИ	1	1	-	2
Раздел 2. Организационные вопросы ЗРИ	1	1	-	2
Раздел 3. Аппаратно-программная реализация средств ЗРИ Тема 3.1. Современная элементная база цифровой обработки сигналов (ЦОС) Тема 3.2. Инструментальные средства создания приложений ЦОС Тема 3.3. Методы моделирования и экспериментального исследования алгоритмов ЗРИ	10 5 7	6 1 1	4 4 6	4 4 4
Раздел 4. Свойства и характеристики речевых сигналов Тема 4.1. Модели речеобразования и	8 18 16	4 8 8	4 10 8	4 8 8

восприятия речи. Тема 4.2. Методы обработки речевых сигналов Тема 4.3. Методы кодирования речевой информации				
Раздел 5. Методы защиты речевой информации Тема 5.1. Акустические характеристики среды. Тема 5.2. Каналы утечки речевой информации Тема 5.3. Методы обнаружения утечек речевой информации Тема 5.4. Методы предотвращения утечки речевой информации **Тема 5.5. Методы закрытия речевой информации**	2 6 8 7 12	2 6 4 4 4	4 3 8	4 8 6 4 8
	102	51	51	68

Курсовая работа

Цель выполнения курсовой работы – закрепление знаний и навыков решения задач защиты речевой информации. Обучаемые должны продемонстрировать умение провести анализ поставленной задачи, выбрать и реализовать с применением современной алгоритмической и элементной базы один из методов. Примерный объём курсовой работы: пояснительная записка на 40 листах формата А4 с приложением графических материалов по схемным и программным решениям также на листах формата А4 либо А3. Условием получения наивысшей оценки является экспериментальное подтверждение полученных результатов разработки на реальной аппаратуре либо имитационной модели (в случае отсутствия требуемой аппарату-ры). Для масштабных задач допускается совместная разработка проекта несколькими обучаемыми с обязательным распределением конкретных подзадач между ними.

Перечень возможных тем курсовых работ:

☐ Речевой кодек стандарта G.729 (либо другого) на основе ЦСП
☐ Разработка лабораторных стендов для исследования методов ЗРИ
☐ Исследование возможностей создания фонемного вокодера

От обучаемых требуется посещение лекций и практических занятий, выполнение курсовой работы

Бальная структура оценки

Форма контроля

Посещение занятий 20 баллов

Выполнение и защита лабораторных работ 20 баллов

Выполнение и защита курсовой работы 30 баллов

Итоговое испытание (экзамен) 30 баллов

Всего 100 баллов

Шкала оценок (академической учет активности студента)

Баллы за семестр	Автоматическая Оценка	Баллы за экзамен	Общая сумма баллов	Итоговая оценка
91-100	5	-	100	5
76-90	4	6-30	76-90 91-110	4 5
55-75	3	6-30	36-75 76-90 91-95	3 4 5
35-54	-	6-30	55-74	3
< 35	-	-	< 35	2

Студенты, набравшие на экзамене менее 5 баллов, получают оценку «неудовлетворительно» независимо от числа набранных в семестре баллов.

Разработка описания и программы учебно-методического комплекса (УМК)

Название курса «Методы защиты речевой информации»

Цель и задачи курса

Целью курса является изучение научно-технических основ анализа, разработки, применения и совершенствования методов и средств защиты речевой информации в процессе её сбора, обработки, передачи и распро-странения с целью технического, организационного и правового обеспечения информационной безопасности государства, общества и личности.

Задачами курса являются:

☐ изучение нормативно-правовой базы, определяющей порядок созда-ния и применения методов и средств защиты информации;
☐ знакомство с организационными принципами построения систем безопасности, включающих средства защиты речевой информации;
☐ изучение каналов утечки речевой информации, методов и средств их обнаружения и противодействия;
☐ изучение методов и алгоритмов закрытия речевой информации для передачи по каналам связи;
☐ освоение навыков математического моделирования и эксперимен-тального исследования алгоритмов защиты речевой информации;

Область знаний, к которой относятся изучаемые в курсе вопросы – обработка информации и информационная безопасность.

Данная дисциплина предназначена для дополнительной профессио-нальной подготовки по направлению "Информационно-телекоммуникационные системы".

Инновационность курса по:

– содержанию

Основу курса составляют достижения в области создания методов, алгоритмов и устройств цифровой обработки речевых сигналов, позволяющие создавать современные эффективные средства защиты речевой информации. Углублённое изучение этих методов отличает данный курс от традиционных, рассматривающих создававшихся ещё десятилетия назад методы скремблирования и т.п. Теоретические сведения подкрепляются экспериментами с реальными речевыми сигналами, а также знакомством с возможностями реализации алгоритмов на современных цифровых сигнальных процессорах.

– методике преподавания

Обучение ведется по кредитно-модульной системе. Организация учебного процесса с использованием системы кредитов осуществляется по так называемой «нелинейной» схеме, в отличие от «линейной», действую-щей в настоящее время в вузах РФ. Основные отличительные черты нелинейной схемы:

☐ большая свобода выбора учащимися дисциплин, перечисленных в учебном плане,
☐ личное участие каждого студента в формировании своего индивиду-ального учебного плана,
☐ вовлечение в учебный процесс академических консультантов, содей-ствующих студентам в выборе образовательной траектории, в частности, в выборе изучаемых дисциплин,
☐ введение системы зачетных единиц (з.е.) для оценки трудозатрат студентов и преподавателей по каждой дисциплине,
☐ широкие полномочия факультета в организации учебного процесса, в том числе, в определении и учете видов педагогической нагрузки преподавателей,
☐ обеспеченность учебного процесса всеми необходимыми методиче-скими материалами в печатной и электронной формах,
☐ обязательное использование балльно-рейтинговых систем для оцен-ки усвоения обучаемыми учебных дисциплин.

Кроме традиционных методов ведения лекционных и практических занятий, предусмотрено выполнение курсовой работы, включающей исследовательскую и прикладную части, и посвящённой исследованию и реализации одного из методов защиты речевой информации.

– литературе

Наряду с учебниками и учебными пособиями широко используются монографии и статьи в научных журналах, справочно-информационные материалы из Интернета.

– организации учебного процесса

Разделы курса подкрепляются практическими занятиями с примене-нием современных пакетов прикладных программ – MatLab, LabView, взаимодействующих со средствами ввода-вывода звуковых сигналов, слу-жащих для моделирования и экспериментального исследования алгоритмов обработки сигналов.

ЛИТЕРАТУРА

ОСНОВНАЯ:

1. Демин В.П., Куприянов А.И., Сахаров А.В. **Радиоэлектронная разведка и радиомаскировка. - М.: Изд-во МАИ, 1997.**

2. Каторин Ю.Ф. и др. **Большая энциклопедия промышленного шпионажа. - СПб.: Полигон, 2000.**

3. Рабинер Л.Р., Шафер Р.В. **Цифровая обработка речевых сигналов/Пер. с англ. - М.: Радио и связь, 1981.**

4. Сапожков М.А. Электроакустика: Учебник для вузов. - М.: Связь,1978.

5. Сергиенко А.Б. Цифровая обработка сигналов - СПб.: Питер, 2003.

6. Торокин А.А. **Основы инженерно-технической защиты информации. - М: Ось-89, 1998.**

7. Халяпин Д. Б. **Защита информации. Вас подслушивают? Защищайтесь! - М.: Баярд. 2004.**

8. Хорев А.А. **Способы и средства защиты информации. - М.: МО РФ, 2000.**

9. Ярочкин В.И. **Технические каналы утечки информации. - М.: ИПКИР, 1994.**

ДОПОЛНИТЕЛЬНАЯ:

10. Руководство пользователя по 16-ти разрядным цифровым сигнальным процессорам семейства ADSP219X. - **http://www.analog.com.ru/pub_dsp.htm**

11. Барсуков В.С. **Интегральная защита информации//Специальная Техника №5, 6. 2002.**

12. Кодзасов С.В., Кривнова О.Ф. **Общая фонетика: Учебник. - М.: РГГУ, 2001.**

13. Корнюшин П.Н. Костерин С. С. **Информационная безопасность. Владивосток: Дальневосточный государственный университет, 2003.**

14. Котухов М.М., Марков А.С. **Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем. 1998.**

15. Грибунин В.Г. **Цифровая стеганография. - М.:СОЛОН-Пресс,2002.**

16. Немудров В., Мартин Г. **Системы-на-кристалле. Проектирование и развитие. - М.: Техносфера, 2004.**

17. Петраков А.В. **Основы практической защиты информации. - М.: Радио и связь, 1999.**

18. Петраков А.В. **Утечка и защита информации в телефонных каналах. М.: Энергоатомиздат, 1996.**

19. Плотников В.Н., Суханов В.А., Жигулёвцев Ю.Н. **Речевой диалог в системах управления. - М.: Машиностроение, 1988.**

20. Сорокин В.Н. **Теория речеобразования. - М.: Радио и связь, 1985.**

21. Интернет-ссылки в поисковых системах **Google, Yandex по запросу "Защита речевой информации"**

22. Стешенко В.Б. **ПЛИС фирмы Altera: проектирование устройств обработки сигналов. - М.: ДОДЭКА, 2000.**

23. Физиология речи. Восприятие речи человеком/Л.А. Чистович и др. Сер. "Руководство по физиологии". - Л.: "Наука", 1976.

24. Хорев А.А. **Методы и средства поиска электронных устройств перехвата информации.- М.: МО РФ, 1998.**

25. В.А.Хорошко, А.А.Чекатков. **Методы и средства защиты информации/Под ред. Ю.С.Ковтанюка. - К.: Юниор, 2003.**

26. Цвикер Э., Фельдкеллер Р. **Ухо как приёмник информации. Перевод с немецкого под ред. Б.Г. Белкина. М.: "Связь", 1971.**

НОРМАТИВНЫЕ АКТЫ:

27. Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента РФ от 9 сентября 2000 г. № Пр-1895

28. Закон Российской Федерации от 5 марта 1992 г. № 2446-I "О безопасности"

29. Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

30. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 "О государственной тайне".

31. Указ Президента РФ от 6 марта 1997 г. № 188 "Об утверждении перечня сведений конфиденциального характера".

32. Постановление Правительства РФ от 26 июня 1995 г. № 608 "О сертифика-ции средств защиты информации"

ИНТЕРНЕТ-ССЫЛКИ

33. http://www.skrembler.ru

34. http://infobez.com