При защите телефонных аппаратов и телефонных линий необходимо учитывать несколько аспектов:

- телефонные аппараты (даже при положенной трубке) могут быть использованы для перехвата акустической речевой информации из помещений, в которых они установлены, то есть для подслушивания разговоров в этих помещениях;
- 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 гальванического 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, конечно, микрофонный капсюли. За счет электроакустических преобразований в этих элементах возникают информационные (опасные) сигналы.

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

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

Следовательно, в телефонном аппарате необходимо защищать как звонковую цепь, так и цепь микрофона.

Для защиты телефонного аппарата от утечки акустической (речевой) информации по электроакустическому каналу используются как пассивные, так и активные методы и средства.

К наиболее широко применяемым пассивным методам защиты относятся:

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

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

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 информации.

Самый простой способ реализации этого метода защиты заключается в установке в корпусе телефонного аппарата или телефонной линии специального выключателя, включаемого и выключаемого вручную. Более удобным в эксплуатации 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- М1".

В эго состав входят:

- электронный коммутатор;
- схема анализа состояния телефонного аппарата, наличия вызывных сигналов и управления коммутатором;
- схема защиты телефонного аппарата от воздействия высоковольтных импульсов.

Устройство имеет следующие режимы работы: дежурный режим, режим передачи сигналов вызова и рабочий режим.

В дежурном режиме (при положенной телефонной трубке) телефонный 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. Подключение осуществляется только на время действия сигналов вызова.

При поднятии телефонной трубки устройство переходит в рабочий режим и телефонный аппарат подключается к линии.

Изделие устанавливается в разрыв телефонной линии, как правило, при выходе ее из выделенного помещения или в распределительном щитке, находящемся в пределах контролируемой зоны.

Устройство "Барьер - М1" обеспечивает защиту телефонного аппарата не только от утечки информации по электроакустическому каналу, но также и его защиту от воздействия высоковольтных импульсов.

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 шумового сигнала прекращается.

К сертифицированным средствам линейного зашумления относятся устройства МП-1А (защита аналоговых телефонных аппаратов) и МП-1Ц П-1А (защита цифровых телефонных аппаратов) и др. [9].

Для защиты акустической (речевой) информации в выделенных помещениях наряду с защитой телефонных аппаратов необходимо принимать меры и для защиты 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 акустических закладок, питающихся от телефонной линии в режиме положенной трубки, а активные - на линейном зашумлении линий и уничтожении (электрическом "выжигании")

закладных устройств или их блоков питания путем подачи в линию высоковольтных импульсов.

Защита информации, передаваемая по каналам связи, может осуществляться на семантическом и энергетическом уровнях. На семантическом ровне защита информации достигается применением криптографических методов и средств защиты и направлена на исключение ее получения (выделения), даже при перехвате противником (злоумышленником) информационных сигналов. Методы защиты информации на энергетическом уровне направлены на исключение (затруднение) приема противником (злоумышленником) непосредственно информационных сигналов. То есть эти методы направлены на уменьшение отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки (средством несанкционированного съема информации).

В данной статье рассмотрим только методы защиты информации на энергетическом уровне. Защита телефонных разговоров осуществляется как активными, так и пассивными методами.

В качестве маскирующего помехового сигнала, как правило, используются дискретные сигналы речевого диапазона частот.

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 датчиков. Однако эффективность подавления средств съема информации с подключением к линии при помощи с индукционных датчиков (особенно, не имеющих предусилителей) 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.

Для исключения воздействия маскирующего помехового сигнала на телефонный разговор в устройстве защиты устанавливается специальный низкочастотный

фильтр с граничной частотой 3,4 кГц, подавляющий (шунтирующий) помеховые сигналы и не оказывающий существенного влияния на прохождение полезных сигналов.

Компенсационный метод используется для односторонней маскировки (скрытия) речевых сообщений, передаваемых абоненту по телефонной линии, и обладает высокой эффективностью подавления всех известных средств несанкционированного съема информации.

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 маскирующий сигнал ("чистый" шум) подается на один из входов двухканального адаптивного фильтра, на другой вход которого поступает аддитивная смесь принимаемого полезного сигнала речевого сигнала (передаваемого сообщения) и этого же помехового сигнала. Аддитивный фильтр компенсирует (подавляет) шумовую составляющую и выделяет полезный сигнал, который подается на телефонный аппарат или устройство звукозаписи.

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

Для защиты телефонных линий используются как простые устройства, реализующие один метод защиты, так и сложные, обеспечивающие комплексную защиту 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", "SI-2001", "КТЛ-3","КТЛ-400", "Ком-3", "Кзот-06", "Цикада-М", "Прокруст" (ПТЗ-003), "Прокруст-2000", "Консул", "Гром-ЗИ-6", "Протон" и др. Основные характеристики некоторых из них приведены в табл. 1, эффективность - в табл. 2, а внешний вид - на рис. 5 [4, 6, 8, 10, 11, 14].

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 устройствах "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.

Устройства защиты телефонных линий имеют сравнительно небольшие размеры и вес (например, изделие "Прокруст" при размерах 62• 155• 195 мм весит 1 кг). Питание их, как правило, осуществляется от сети переменного тока 220 В. Однако некоторые устройства (например, "Кзот-06") питаются от автономных источников питания.

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.

Устройство "КС-1300" оборудовано специальным таймером, позволяющим при работе в автоматическом режиме устанавливать временной интервал подачи импульсов в линию в пределах от 10 минут до 2 суток.

Наряду со средствами активной защиты на практике широко используются различные устройства, позволяющие контролировать некоторые параметры телефонных 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. В зависимости от способа подключения закладного устройства к телефонной линии (последовательного, в

разрыв одного из проводов телефонного кабеля, или параллельного), степень его влияния на изменение параметров линии будет различной.

За исключением особо важных объектов линии связи построены по стандартному образцу. Ввод линии в здание осуществляется магистральным многопарным (многожильным) телефонным кабелем до внутреннего распределительного щита. Далее от щита до каждого абонента производится разводка двухпроводным телефонным проводом марки ТРП или ТРВ. Данная схема характерна для жилых и небольших административных зданий размеров.

Подключение средств съема информации к магистральному кабелю (как наружному, так и внутреннему) маловероятно. Наиболее уязвимыми местами подключения являются: входной распределительный щит, внутренние распределительные колодки и открытые участки из провода ТРП, а также телефонные розетки и аппараты. Наличие современных внутренних мини-АТС не влияет на указанную ситуацию.

Телефонные адаптеры с внешним источником питания, гальванически подключаемые к линии, имеют большое входное сопротивление до нескольких МОм (в некоторых случаях и более 100 МОм) и достаточно малую входную емкость.

Важное значение имеют энергетические характеристики средств съема информации, а именно потребляемый ток и падение напряжения в линии.

Однако падение напряжения в линии (при положенной и поднятой трубке) не дает однозначного ответа - установлена в линии закладка, или нет, так как колебания напряжения в телефонной линии могут происходить из-за ее плохого качества (как результат изменения состояния атмосферы, времени года или выпадения осадков и т.п.). Поэтому для определения факта подключения к линии закладного устройства необходим постоянный контроль ее параметров.

Простейшее устройство контроля телефонных линий представляет собой измеритель напряжения. При настройке оператор фиксирует значение напряжение, соответствующее нормальному состоянию линии (когда к линии не подключены 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

последовательном подключении закладного устройства.

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

Устройства контроля телефонных линий, построенные на рассмотренном принципе, реагируют на изменения напряжения, вызванные не только подключением 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 сопротивлением 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 параллельное).

Современные контроллеры телефонных линий, как правило, наряду со средствами обнаружения подключения к линии устройств несанкционированного съема информации, оборудованы и средствами их подавления. Для подавления в основном используется метод высокочастотной маскирующей помехи. Режим подавления включается автоматически или оператором при обнаружении факта несанкционированного подключения к линии.

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

Принцип работы подобных устройств поясним на примере изделия "Рубин". В дежурном режиме устройство производит анализ состояния телефонной линии путем сравнения напряжения в линии и на эталонной (опорной) нагрузке, подключенной к цепи телефонного аппарата. При поднятии трубки несанкционированного подключенного параллельного телефонного аппарата напряжение в линии уменьшается, что фиксируется устройством защиты. Если этот факт зафиксирован в момент ведения телефонного разговора (трубка на защищаемом телефонном аппарате снята), срабатывает звуковая и световая

(загорается светодиод несанкционированного подключения к линии) сигнализация.

Кроме несанкционированного подключения к линии параллельного телефонного аппарата устройство защиты "Рубин" сигнализирует также о фактах обрыва (размыкания) и короткого замыкания телефонной линии.