ЗАЩИТА ИНФОРМАЦИИ В ВЫДЕЛЕННЫХ ПОМЕЩЕНИЯХ

Сабынин В.Н., независимый эксперт, кандидат технических наук, доцент

В предыдущих номерах (№№ 15, 16, 17) нами были рассмотрены вопросы, касающиеся защиты информации на объектах - организация пропускного режима, организация конфиденциального делопроизводства, которые имеют большое значение в деле обеспечения безопасности конфиденциальной информации на фирме (в организации).

Сегодня особенно актуальна проблема защиты конфиденциальной информации в так называемых выделенных помещениях фирмы.

При этом под выделенным помещением (ВП) понимается служебное помещение, в котором ведутся разговоры (переговоры) конфиденциального характера.

Здесь речь идет о служебных помещениях, в которых отсутствуют какие-либо технические средства обработки (передачи) конфиденциальной информации. К таким помещениям относятся, прежде всего, комнаты для переговоров на фирмах, где ведутся деловые переговоры, содержащие конфиденциальную информацию.

Следует отметить, что переговорные комнаты используются все чаще и на сегодня они являются практически неотъемлемым атрибутом фирмы. Поэтому будет небезынтересно рассмотреть вопросы обеспечения безопасности информации в выделенных помещениях, имея в виду, прежде всего, комнаты для ведения переговоров.

Во-первых, необходимо понять основную цель и задачи защиты, ибо правильное уяснение цели и задач защиты определит в дальнейшем состав комплекса проводимых мероприятий, их стоимость и эффективность защиты в целом.

Основная цель обеспечения безопасности конфиденциальной информации в переговорных комнатах - исключить доступ к ее содержанию при проведении переговоров (разговоров).

Первостепенными задачами обеспечения безопасности информации (рис. 1) являются:

1. Защита информации от утечки по акустическому каналу (АК).
2. Защита информации от утечки по виброакустическому каналу (ВАК).
3. Защита информации от утечки за счет электроакустического преобразования (ЭАП).
4. Защита информации от утечки за счет ВЧ-навязывания (ВЧН).
5. Защита информации от утечки по оптическому каналу (ОК).

Уяснив основную цель и задачу защиты информации, можно перейти к разработке модели угроз для конфиденциальной информации, имеющих место при ведении переговоров (разговоров).

Модели угроз целесообразно разрабатывать, сообразуясь с задачами защиты.

Модель угроз для информации через акустический канал утечки

Несанкционированный доступ к конфиденциальной информации по акустическому каналу утечки (рис. 2) может осуществляться:

- путем непосредственного прослушивания;
- при помощи технических средств.

Непосредственное прослушивание переговоров (разговоров) злоумышленником может быть осуществлено:

- через дверь;
- через открытое окно (форточку);
- через стены, перегородки;
- через вентиляционные каналы.

Несанкционированный доступ к содержанию переговоров (разговоров) злоумышленник может осуществить и при помо-

Рис. 1. Задачи обеспечения безопасности конфиденциальной информации в комнате для переговоров.

щи технических средств - таких, как:

- направленные микрофоны;
- проводные микрофоны;
- радиомикрофоны;
- устройство "Электронное ухо".

Прослушивание переговоров (разговоров) через дверь возможно при условии, если вход в комнату для переговоров выполнен с нарушением требований по звукоизоляции. Не следует также вести переговоры при открытых окнах либо форточках, ибо в этом случае открыт непосредственный доступ к содержанию информации (переговоров или разговоров).

Стены, перегородки, потолки (и даже пол) комнат для ведения переговоров не являются гарантированной защитой от прослушивания, если они не проверены на предмет звукоизоляции или не отвечают этим требованиям.

Весьма опасными с точки зрения несанкционированного доступа к содержанию переговоров (разговоров) являются вентиляционные каналы. Они позволяют прослушивать разговор в комнате на значительном удалении. Поэтому к оборудованию вентиляционных каналов предъявляются особые требования.

В настоящее время для прослушивания разговоров широко распространено использование направленных микрофонов. При этом дистанция прослушивания в зависимости от реальной помехозащитной обстановки может достигать сотен метров.

В качестве направленных микрофонов злоумышленники могут использовать:

- микрофоны с параболическим отражателем;
- резонансные микрофоны;
- щелевые микрофоны;
- лазерные микрофоны.

Тактико-технические характеристики данных средств в литературе приведены достаточно подробно.

Для прослушивания злоумышленники применяют и т.н. проводные микрофоны. Чаще всего используются микрофоны со специально проложенными проводами для передачи информации, а также микрофоны с передачей информации по линии сети в 220 В.

Не исключено использование для передачи прослушиваемой информации и других видов коммуникаций (проводов сигнализации, радиотрансляции, часификации и т.д.). Поэтому при проведении всевозможных ремонтов и реконструкций этому необходимо уделять особое внимание, ибо в противном случае не исключена возможность внедрения таких подслушивающих устройств.

Широко применяются злоумышленниками для прослушивания переговоров и радиомикрофоны. В настоящее время их насчитывается более 200 типов. Обобщенные характеристики радиомикрофонов следующие:

- диапазон частот: 27 - 1500 МГц;
- вес: единицы граммов - сотни граммов;
- дальность действия: 10 - 1600м;
- время непрерывной работы: от нескольких часов до нескольких лет (в зависимости от способа питания).

Данные устройства представляют собой большую угрозу для безопасности ведения переговоров (разговоров), поэтому необходимо исключить их из переговорных комнат.

В последнее десятилетие злоумышленники стали применять устройства с использованием телефонных линий, позволяющие прослушивать разговоры в помещениях на значительном удалении (из других районов, городов и т.д.).

Такие устройства в литературе можно встретить под названием "Электронное ухо". Они также представляют большую угрозу для безопасности переговоров.

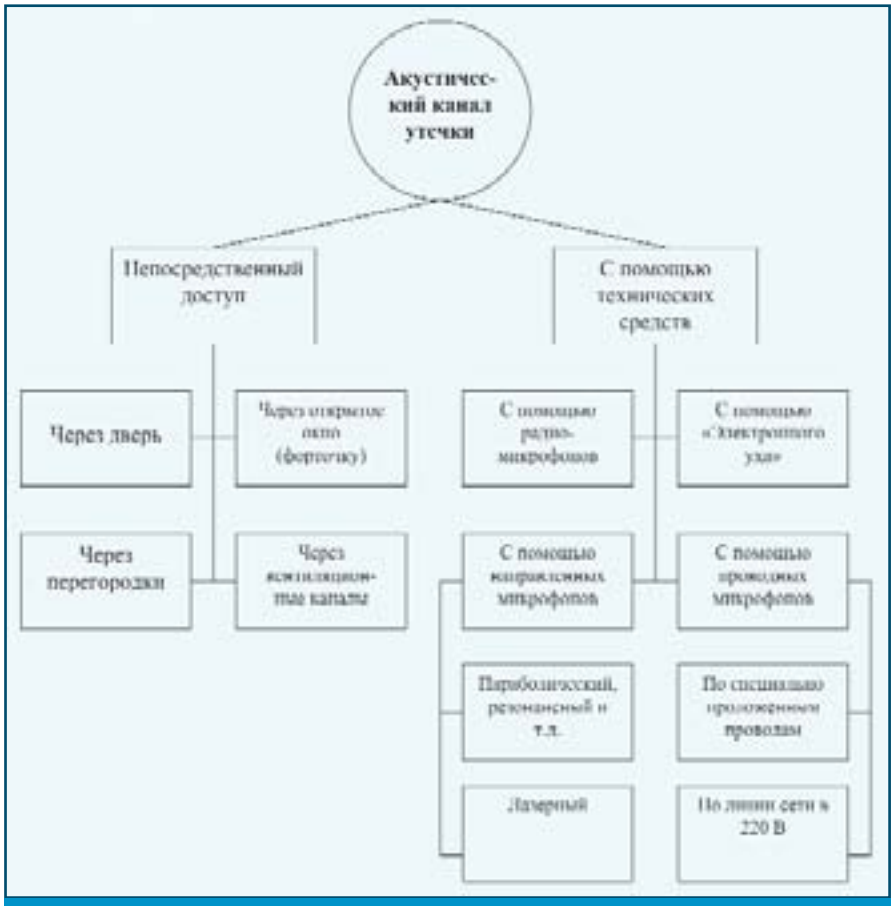

Рис. 2. Модель угроз через акустический канал утечки.

Модель угроз для информации через виброакустический канал утечки

Несанкционированный доступ к содержанию переговоров (разговоров) злоумышленниками может быть также осуществлен (рис. 3) с помощью стетоскопов и гидроакустических датчиков.

С помощью стетоскопов возможно прослушивание переговоров через стены толщиной до 1 м 20 см (в зависимости от материала).

В зависимости от вида канала передачи информации от самого вибродатчика стетоскопы подразделяются на:

- проводные (проводной канал передачи);
- радио- (канал передачи по радио);
- инфракрасные (инфракрасный канал передачи).

Не исключена возможность использования и гидроакустических датчиков, позволяющих прослушивать разговоры в помещениях, используя трубы водообеспечения и отопления. Правда, случаи применения таких устройств на практике очень редки.

Модель угроз для информации за счет электроакустического преобразования и гетеродинного оборудования

Утечка конфиденциальной информации при ведении переговоров (разговоров) возможна из-за воздействия звуковых колебаний на элементы электрической схемы некоторых технических средств обработки информации, получивших в литературе название "Вспомогательные средства".

К вспомогательным средствам относятся те, которые непосредственного участия в обработке конфиденциальной информации не принимают, но могут быть причиной ее утечки. Доступ к содержанию переговоров (разговоров) может быть осуществлен на значительном удалении от помещения, составляющем в некоторых случаях сотни метров, в зависимости от вида канала утечки (рис. 4).

Подобные каналы утечки существуют при наличии в помещениях телефонных аппаратов с дисковым номеронабирателем, телевизоров, электрических часов, подключенных к системе часификации, приемников и т.д.

Причем в случае с телефонными аппаратами и электрическими часами утечка информации осуществляется за счет преобразования звуковых колебаний в электрический сигнал, который затем распространяется по проводным линиям (телефонным либо по проводам системы часификации). Доступ к конфиденциальной информации может осуществляться путем подключения к этим линиям.

Что касается телевизоров и приемников, то утечка конфиденциальной информации происходит здесь за счет имеющихся в них гетеродинов (генераторов частоты).

Причина утечки - модуляция звуковым колебанием при ведении разговора несущей частоты гетеродина, просачивание ее в систему с последующим излучением в виде электромагнитного поля.

Модель угроз для информации по оптическому каналу и за счет высокочастотного навязывания

Если переговоры ведутся в комнате, окна которой не оборудованы шторами или жалюзи, то в этом случае у злоумышленника есть возможность с помощью оптических приборов с большим усилением (биноклей, подзорных труб) просматривать помещение.

Сущность прослушивания переговоров с помощью высокочастотного навязывания состоит в подключении к телефонной линии генератора частоты и последующего приема "отраженного" от телефонного аппарата промоделированного ведущимся в комнате разговором сигнала.

Таким образом, анализ угроз для конфиденциальной информации, которые имеют место при ведении переговоров (разговоров) показывает, что если не принять мер защиты, то возможен доступ злоумышленников к ее содержанию.

Рекомендации по защите

Прежде чем перейти к мерам защиты, можно обрисовать в общих чертах модель злоумышленника.

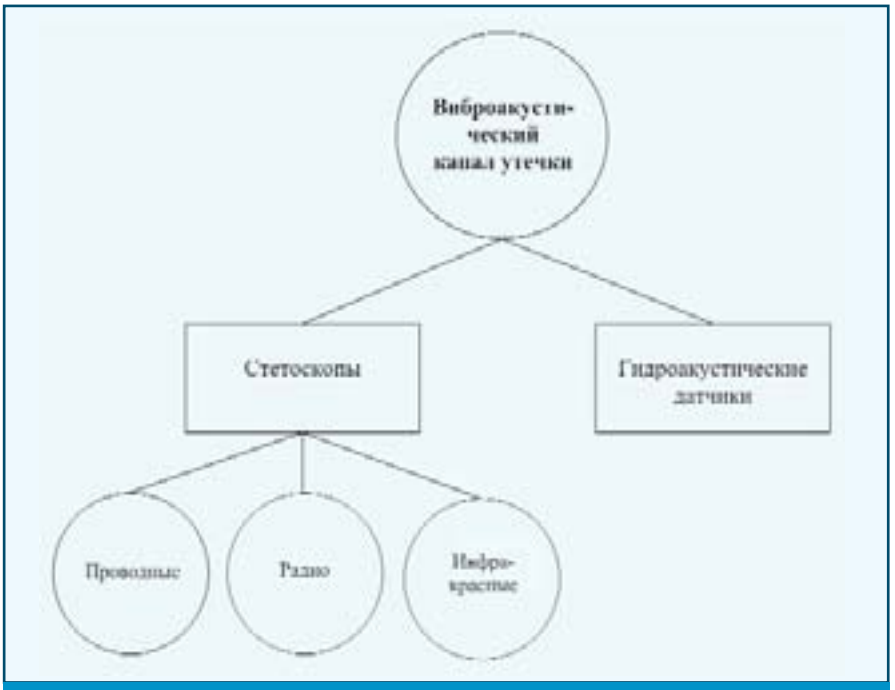

Рис. 3. Модель угроз через виброакустический канал утечки.

Рис. 4. Модель угроз за счет электроакустического преобразования и гетеродинного оборудования.

Предполагаемый злоумышленник - это человек хорошо подготовленный, знающий все каналы утечки информации в комнатах для ведения переговоров, профессионально владеющий способами и средствами добывания сведений, содержащих конфиденциальную информацию. Поэтому необходимо разработать и реализовать комплекс мероприятий, обеспечивающих надежную защиту во время ведения переговоров (разговоров).

1. Особо важен выбор места для переговорной комнаты. Ее целесообразно разместить по возможности на верхних этажах. Желательно, чтобы комната для переговоров не имела окон или же они выходили во двор.
2. В комнате для переговоров не должно быть телевизоров, приемников, ксероксов, электрических часов, системы часификации, телефонных аппаратов.
3. Вход в переговорную комнату должен быть оборудован тамбуром, а внутренняя сторона тамбура обита звукоизоляционным материалом. Необходимо помнить, что незначительная щель (единицы миллиметров) многократно снижает звукоизоляцию.
4. При наличии в комнате для переговоров вентиляционных каналов нужно позаботиться, чтобы они были оборудованы специальными решетками, позволяющими закрывать отверстие вентиляционного канала при ведении переговоров и открывать его, когда переговоры не ведутся.
5. Если в переговорной есть окна, то должны быть приняты следующие меры предосторожности:
   а). Проводить переговоры при закрытых форточках.
   б). На окнах должны иметься шторы либо жалюзи.
   в). Оконные стекла должны быть оборудованы вибродатчиками.
6. При наличии в переговорной телефонного аппарата должны быть приняты следующие меры защиты. В телефонных аппаратах с дисковым номеронабирателем требует защиты звонковая цепь. Поэтому целесообразно использовать фильтр **"Корунд-М"**, обеспечивающий затухание сигнала утечки порядка 80 дБ. Для защиты от высокочастотного навязывания рекомендуется подключить параллельно микрофону (для любых телефонных аппаратов) конденсатор емкостью **С = 0,01 - 0,05 мкФ**. На практике могут встречаться и более сложные схемы защиты звонковой и микрофонной цепи телефонных аппаратов.
7. Для защиты от проводных микрофонов, использующих для передачи информации сеть электропитания в 220 В, рекомендуется использовать генератор типа **"Соната-С1"**, который имеет хорошие тактико-технические характеристики и эффективно выполняет функции защиты.
8. Для защиты переговорных от специальных технических средств хорошо воспользоваться генератором виброакустического шума **"Соната-АВ"** и генератором радиопомех **"Баррикада-1"**. Генератор виброакустического шума **"Соната-АВ"** защищает от:
   - непосредственного подслушивания в условиях плохой звукоизоляции;
   - применения радио- и проводных микрофонов, установленных в полостях стен, надпотолочном пространстве, в вентиляционных проходах и т.д.;
   - использования стетоскопов, установленных на стенах, потолках, полах, трубах водо- и теплоснабжения и т.д.;
   - применения лазерных и других типов направленных микрофонов.

Генератор радиошума **"Баррикада-1"** обеспечивает защиту переговоров от всех радиозакладок, создавая в точке приема злоумышленником превышающего уровня помехи над уровнем излучаемого радиозакладкой сигнала.

Важен также контроль над состоянием безопасности конфиденциальной информации в переговорных комнатах, который осуществляется при периодическом проведении спецобследований и аттестаций. По окончании составляется акт спецобследования и аттестат соответствия.

Таким образом, предложенные нами рекомендации позволят обеспечить безопасность переговоров, проводимых в специально выделенных для этой цели помещениях.