# СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Ст-т БГУИР*
*Мицкевич П.Н.*

*Руководитель:*
*ст. преп. Дворникова Т.Н.*

Технический канал утечки информации представляет собой совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация. Техническая защита конфиденциальной информации – защита информации не криптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования.

Под техническими средствами приема, обработки, хранения и передачи информации (ТСПИ) понимают технические средства, непосредственно обрабатывающие конфиденциальную информацию. К таким средствам относятся: электронно-вычислительная техника, режимные АТС, системы оперативно-командной и громко-говорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д.

При выявлении технических каналов утечки информации ТСПИ необходимо рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления.

Отдельные технические средства или группа технических средств, предназначенных для обработки конфиденциальной информации, вместе с помещениями, в которых они размещаются, составляют объект ТСПИ. Под объектами ТСПИ понимают также выделенные помещения, предназначенные для проведения закрытых мероприятий.

Наряду с ТСПИ в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ТСПИ и находящиеся в зоне электромагнитного поля, создаваемого ими. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и т.д.

В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ), т.е. зоны, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков.

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками.

К мероприятиям защиты с использованием активных средств относятся:

Пространственное зашумление:

– пространственное электромагнитное зашумление с использованием генераторов шума или создание прицельных помех (при обнаружении и определении частоты излучения закладного устройства или побочных электромагнитных излучений ТСПИ) с использованием средств создания прицельных помех;

– создание акустических и вибрационных помех с использованием генераторов акустического шума;

– подавление диктофонов в режиме записи с использованием подавителей диктофонов.

Линейное зашумление:

– линейное зашумление линий электропитания;

– линейное зашумление посторонних проводников и соединительных линий ВТСС, имеющих выход за пределы контролируемой зоны.

Уничтожение закладных устройств:

– уничтожение закладных устройств, подключенных к линии, с использованием специальных генераторов импульсов.

Одним из основных способов несанкционированного доступа к информации частного и коммерческого характера является прослушивание телефонных переговоров. Наиболее широко применяемы приборы и устройства защиты телефонных переговоров это – скремблер и криптофон.

Скремблер — это устройство, которое осуществляет шифрование передаваемой по каналам связи речи. При скремблировании возможно преобразование речевого сигнала по следующим параметрам: амплитуде, частоте и времени. В системах подвижной радиосвязи практическое применение нашли в основном частотные, временные преобразования сигнала или их комбинация. Помехи в радиоканале существенно затрудняют точное восстановление амплитуды речевого сигнала, поэтому амплитудные преобразования при скремблировании практически не применяются. Достоинство скремблеров: защита осуществляется на всем протяжении линии связи, то есть в открытом виде информация передается только от

скремблера к телефону, это расстояние ограничено длинной провода или радиусом действия Bluetooth. Недостатки скремблера: необходимость использования совместимого оборудования всеми абонентами, с которыми предполагается вести защищенные переговоры и потеря времени необходимая для синхронизации аппаратуры при установке безопасного соединения.

При частотных преобразованиях сигнала в средствах подвижной радиосвязи чаще всего используются следующие виды скремблирования:

• частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и фильтра);

• разбиение полосы частот речевого сигнала на несколько поддиапазонов и частотная инверсия спектра в каждом относительно средней частоты поддиапазона;

• разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки.

При временных преобразованиях производится разбиение сигнала на речевые сегменты и их перестановки во времени:

• инверсия по времени сегментов речи;

• временные перестановки сегментов речевого сигнала.

Комбинированные методы преобразования сигнала используют одновременно частотные и временные преобразования.

Скремблер присоединяется к телефону (по проводу или Bluetooth) и в выключенном состоянии никак себя не проявляет. Как только владелец аппарата включает его, как он тут же начинает принимать все сигналы, идущие с микрофона, шифровать их и только после этого отсылать на выход. Декодирование речи происходит в обратном порядке. Сигналы с антенны подаются в скремблер, а уже оттуда — на динамик. Таким образом, скремблер шифрует передаваемую речь и дешифрует принятый сигнал.

Криптофон — сравнительно новое устройство защиты телефонных разговоров. Криптофон представляет собой тот же смартфон, но на нем установлено специальное программное обеспечение. Принцип работы криптофона схож со скремблером: сигнал с микрофона оцифровывается, затем кодируется и передается абоненту. Отличие состоит в способе шифрования. Для этого используют способы криптографической защиты.Современные криптофоны используют следующие алгоритмы шифрования: AES, Twofish и др. Основным достоинством криптофонов является их высокая безопасность благодаря устойчивым к взлому алгоритмам шифрования. Недостатки криптофонов:

• Необходимость у обоих абонентов таких устройств;

• Неприятности, связанные с задержкой голоса (могут достигать нескольких секунд);

• Наличие эха во время разговора.

Выводы: таким образом, защита информации представляет собой комплекс целенаправленных мероприятий ее собственников по предотвращению утечки, искажения, уничтожения и модификации защищаемых сведений с применением современных достижений науки и техники. Услуги по технической защите информации высоко востребованы во всех сферах современной деятельности многочисленных компаний и корпораций, политиков, государственных и военных организаций.

.

Список использованных источников:

1. Хорев А.А. Защита информации от утечки по техническим каналам // Учебное пособие – Москва, 1998. - 320 с.
2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; Технические средства и методы защиты информации // Учебник для вузов под ред. А.П. Зайцева и А.А. Шелупанова. – Москва, ООО «Издательство Машиностроение», 2009 – 508 с.

.