

МЕТОДЫ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

В.А. Садовский,

Д.С. Рябенко, канд. техн. наук, доц.

Институт пограничной службы Республики Беларусь,

Минск, Беларусь

Защита акустической речевой информации от утечки по техническим каналам – это ключ к обеспечению конфиденциальности при ведении переговоров. Оценка эффективности защиты речевой информации – первостепенная задача при создании системы защиты информации. Акустические сигналы распространения по воздуху, поэтому защита информации по акустическому каналу требует пристального внимания. В работе рассмотрены проблемы утечки речевой информации через технические каналы утечки и анализируются методы ее защиты. Описываются различные подходы к защите, такие как использование активных и пассивных методов защиты, мероприятий по поиску, обнаружению и подавлению технических средств разведки. Следует учесть, что защита речевой информации от утечки по техническим каналам – это часть комплексной системы защиты конфиденциальной информации, которая включает в себя алгоритмически упорядоченные и вспомогательные функции самостоятельных организационных и технических подсистем.

Ключевые слова: *речевая информация, каналы утечки информации, методы пассивной защиты информации, методы активной защиты информации.*

Существенной угрозой безопасности конфиденциальной информации является ее утечка по техническим каналам. Утечка информации по техническому каналу относится к неконтролируемому распространению информации от ее источника через физическую среду к несанкционированным техническим средствам, которые фиксируют эту информацию. Перехват информации происходит, когда злоумышленник получает информацию с помощью технологии, предназначенной для обнаружения, перехвата и обработки этих сигналов. В результате возникает риск несанкционированного доступа к конфиденциальной информации или ее записи.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды их распространения. Так, для технических каналов утечки речевой (акустической) информации информационный сигнал первоначально представляется акустическими колебаниями воздуха, образованными органами речи человека или техническими средствами, организующими схожие акустические колебания. Изменяющаяся среда распространения таких колебаний позволяют классифицировать каналы утечки речевой информации и соответствующие им технические средства перехвата информации.

1. В прямых акустических каналах утечки в качестве среды распространения используется воздушная среда. В таких каналах утечки для перехвата речевой информации применяются закладные радиоустройства, диктофоны, специализированные высокочувствительные направленные микрофоны и др. Речь, перехваченная встроенными устройствами, может передаваться по радиоканалам, оптическим каналам, сетям переменного тока, соединительным линиям вспомогательного оборудования и другим металлическим конструкциям, например, водопроводные и канализационные трубы. Для сбора речевой информации могут также использоваться мобильные устройства операторов сотовой подвижной электросвязи или диктофоны.

2. Виброакустические каналы утечки используют твердые среды распространения, такие как ограждающие конструкции помещений, окна, двери и предметы декора и мебели. В этих условиях контактные микрофоны, часто называемые стетоскопами, используются для улавливания колебаний с твердых поверхностей. Информация в основном передается по радиоканалам. Кроме того, может проходить по оптическим каналам или ультразвуковым каналам через металлические конструкции.

3. Акустооптические (лазерные) каналы утечки используют твердые среды распространения, состоящие из отражающих вибрирующих поверхностей. Для перехвата речевой информации через этот канал используются «лазерные микрофоны», которые работают в ближнем инфракрасном диапазоне длин волн (0,75 – 1,4 мкм).

4. Акустоэлектрические каналы утечки в качестве среды распространения используют проводящие структуры, подвергаемые преобразованию акустических сигналов в электрические. Для съема речевой информации применяются электронные встраиваемые устройства, подключаемые к линиям связи, сети переменного тока и соединительным линиям вспомогательных технических устройств, а также звукозаписывающие устройства (диктофоны). Передача информации может осуществляться через закладные устройства в радио- и оптическом диапазонах длин волн.

5. Акустоэлектромагнитные каналы утечки используют воздух в качестве среды распространения после преобразования акустических сигналов в электромагнитные волны.

Для предотвращения утечки речевой информации по техническим каналам применяются различные методы и средства. Эти методы разделяют на активные и пассивные, которые направлены на снижение риска перехвата речевой информации.

Пассивные методы защиты акустической (речевой) информации направлены на:

- снижение уровня акустических (речевых) сигналов на периметре контролируемой территории, где возможно размещение технических средств разведки, до уровней, исключающих их выделение на фоне естественных шумов;
- минимизация электрических информационных сигналов в соединительных линиях вспомогательных технических средств, включающих электроакустические преобразователи с микрофонным эффектом, до уровней, гарантирующих невозможность их выделения от естественного шума;
- предотвращение передачи высокочастотных сигналов во вспомогательные технические средства, использующие электроакустические преобразователи с микрофонным эффектом;

- обнаружение побочных электромагнитных и других видов излучений от закладных устройств;
- выявление несанкционированных подключений к телефонным линиям.

Пассивные методы ориентированы на оптимизацию отношения сигнал/шум путем создания (усиления) физических барьеров в среде распространения для улучшения звукоизоляции, тем самым снижая вероятность несанкционированного подслушивания.

Звукоизоляция помещений направлена на ограничение распространения речевой информации от источников акустических сигналов, что ограничивает возможность ее перехвата по акустическому виброакустическому каналам утечки информации. За счет звукоизоляции помещения достигается ослабление акустических (речевых) сигналов.

Применяя методы фильтрации сигналов, обеспечивается уменьшение электрических информационных сигналов в соединительных линиях вспомогательных технических средств и предотвращение попадания в эти устройства сигналов высокочастотных помех.

При этом критерием эффективности защиты речевой информации пассивными методами является то, чтобы отношение сигнал/шум за пределами помещения не превышало заданного допустимого уровня, что гарантирует невозможность отличить речевые сигналы от естественного фоновых шума техническими средствами разведки.

Активные методы акустической защиты информации направлены на:

- формирование дополнительных маскирующих акустических и вибрационных колебаний, снижающих отношение сигнал/шум по периметру контролируемой территории, что затрудняет выделение акустического информационного сигнала техническими средствами разведки на фоне помех;
- создание в соединительных линиях вспомогательных технических средств маскирующих электромагнитных помех для снижения отношения сигнал/шум до уровней, исключающих выделение информационного сигнала техническими средствами разведки;
- электромагнитное и/или ультразвуковое подавление скрытно размещаемых диктофонов во время записи;
- создание маскирующих электромагнитных помех в линиях электропитания технических средств, размещаемых в помещении, для снижения отношения сигнал/шум до уровней, исключающих выделение информационного сигнала техническими средствами разведки;
- создание направленных радиопомех акустическим и телефонным радиозакладным устройствам с целью снижения отношения сигнал/шум;
- подавление, отключение или вывод из строя технических средств несанкционированного подключения к телефонным линиям;

Методы активной защиты речевой информации основаны на использовании различных типов генераторов шума, создающих акустические и виброакустические помехи на границе ограждающих конструкций, с подключаемыми к ним звуковыми динамиками (громкоговорителями) или виброизлучателями (вибродатчиками), а также других специализированных технических средств.

Эти методы применяются для активного снижения отношения сигнал/шум до более управляемого уровня. Такие методы, как введение контролируемого шума или противодействие звуковым волнам, могут эффективно маскировать информацию, передаваемую посредством речи или других акустических средств.

К сожалению, применение активных и пассивных методов защиты информации не формируют исчерпывающий перечень организационных и технических мероприятий по гарантированной защите речевой информации от утечки по техническим каналам. С целью обеспечения защиты речевой информации от скрытно размещаемых (встраиваемых) технических средств разведки дополнительно проводится:

- поиск и обнаружение технических средств разведки, содержащих электронные устройства;
- обнаружение и подавление диктофонов и акустических закладок.

Поиск и обнаружение закладных устройств может осуществляться визуально или с использованием специализированного оборудования, включающего: обнаружители диктофонов и видеокамер, индикаторы поля, измерители радиочастот, интерцепторы, сканирующие приемники, анализаторы спектра, программно-аппаратные комплексы поиска и обнаружения закладных устройств, нелинейные локаторы, рентгеновские системы, а также специализированное оборудование для обследования проводных линий.

К наиболее простым и экономичным детекторам радиоизлучений от закладных устройств можно отнести индикаторы электромагнитного поля, которые фиксируют и сигнализируют о присутствии электромагнитного поля, превышающего фоновый уровень в месте расположения антенны. Более продвинутые приборы, такие как индикаторы-частотомеры, также могут измерять несущую частоту самого сильного сигнала в точке приема, позволяя при этом идентифицировать тип применяемого закладного устройства. Интерцепторы – это специализированные устройства, используемые для обнаружения излучения от встроенных устройств в непосредственной близости. Они автоматически настраиваются на частоту самого сильного сигнала для обнаружения.

Для улучшения чувствительности применяются специализированные радиостанции с возможностями автоматического сканирования (сканеры), которые охватывают диапазон частот от десятков кГц до нескольких ГГц. Анализаторы спектра обеспечивают наилучшие возможности обнаружения радиометок, позволяя не только перехватывать излучение от встроенных устройств, но и анализировать их характеристики, что имеет решающее значение для идентификации радиозакладок, использующих сложные методы передачи сигнала.

Значительная категория средств обнаружения фокусируется на физических свойствах элементов или структур электрических цепей, таких как полупроводниковые приборы и электропроводящие металлические компоненты. Среди этих средств нелинейные радары, которые улавливают отраженный сигнал из-за нелинейности характеристик полупроводников, входящих в состав элементной базы технических средств разведки.

Устройства, известные как детекторы диктофонов, используются для идентификации диктофонов в режиме записи. Диапазон обнаружения диктофонов в неэкранированных корпусах обычно составляет от 1 до 1,5 метров. Кроме того, достаточно

эффективно применяются средства подавления диктофонов, в результате действия которых на носитель информации фиксируется лишь акустический шумовой сигнал. На дальность подавления диктофонов влияют мощность и тип излучения, а также используемая антенна.

Ультразвуковые системы подавления генерируют мощные ультразвуковые колебания, неслышимые человеческим ухом (обычно около 20 кГц). Эти колебания воздействуют на микрофоны диктофонов или акустических закладок, что является существенным преимуществом. Ультразвуковое воздействие может перегрузить низкочастотный усилитель диктофона или акустической закладки, заставив его работать в нелинейном режиме и вызвав существенные искажения записываемых или передаваемых сигналов.

В линиях электропитания технических средств при выходе их из выделенных помещений устанавливаются фильтры помехоподавления. Учитывая, что проводные закладные устройства передают информацию на частотах выше 40–50 кГц, для защиты информации необходимо применять фильтры нижних частот с частотой среза не более 40 кГц, исключаящую основную полосу частот речевого сигнала.

Технические основы защиты речевой информации включают в себя комплексное исследование технических каналов утечки речевой информации, таких как акустические, виброакустические, акустоэлектрические, акустооптические и акустоэлектромагнитные. Эффективные защитные стратегии руководствуются нормативными базами, включая соответствующие указы и установленные руководящие политики, которые диктуют, каким образом заинтересованные лица должны осуществлять управление речевой конфиденциальной информацией.

ЛИТЕРАТУРА

1. Хорев А.А. Техническая защита информации : учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.
2. Бузов, Г.А. Защита от утечки информации по техническим каналам : учеб. пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М.: Горячая линия–Телеком, 2005. – 416 с.
3. Железняк В.К. Защита информации от утечки по техническим каналам / В.К. Железняк. – СПб.: ГУАП, 2006. – 188 с.
4. Трилисский, В.О. Технические каналы утечки речевой информации / В. О. Трилисский, С. Б. Ревин // Инжиниринг и технологии. – 2019. – Vol. 4(1). – С. 1–3.