Имея современные технические средства, любая информационная система может оперативно и в полном объеме удовлетворять информационные потребности пользователей. Чем больше средств, тем успешнее работает система. Однако любые технические средства по своей природе потенциально обладают техническими каналами утечки информации. Это расширяет возможности не только в плане использования их конкурентами в криминальных интересах, но и предоставляет дополнительные возможности по несанкционированному доступу к источникам конфиденциальной информации через технические средства информационных систем.

Каждая электронная система, содержащая в себе совокупность элементов, узлов и проводников, обладает источниками информационного сигнала и, естественно, каналами утечки конфиденциальной информации. Утечка информации через технические средства может происходить

К системам акустического контроля относится широкая номенклатура различных радиомикрофонов, назначением которых является съем информации и передача ее по радиоканалу.

Радиомикрофоны — это специальные устройства съема информации, которые по своему исполнению бывают:

— простейшие — непрерывно излучающие;

— с включением на передачу при появлении в контролируемом помещении разговоров или шумов;

— дистанционно управляемые — включающиеся и выключающиеся дистанционно на время, необходимое для контроля помещения.

Специальные устройства съема информации и передачи ее по радиоканалу можно, классифицировать но следующим признакам:

— диапазону используемых частот (от 27 МГц до 1,5 ГГц и выше);

— продолжительности работы (от 5 часов до 1 года);

— радиусу действия (от 15 м до 10 км),

— виду модуляции (АМ, ЧМ, узкополосная ЧМ, однополосная АМ, широкополосная шумоподобная).

Следует отметить, что в последнее время появились специальные устройства съема информации, использующие для передачи акустической информации так называемые «нетрадиционные каналы». К этим каналам можно отнести следующие:

— Устройства съема информации, ведущие передачу в инфракрасном диапазоне (ИК передатчики). Характеризуются такие изделия крайней сложностью их обнаружения. Срок непрерывной работы — 1–3 суток. Используют эти устройства, как правило, для увеличения дальности передачи информации и размещаются у окон, вентиляционных отверстий и т. п., что может облегчит задачу их поиска. Для приема информации применяют специальный приемник ИК диапазона, который обеспечивает надежную связь на расстоянии 10–15 м.

— Устройства съема информации, использующие в качестве канала передачи данных силовую электрическую сеть 127/220/380 В. Такие устройства (рис. 5.1) встраиваются в электрические розетки, удлинители, тройники, бытовую аппаратуру и другие места, где проходит или подключается сеть.

В последнее время одним из основных способов несанкционированного доступа к информации частного и коммерческого характера стало прослушивание телефонных переговоров. Для прослушивания телефонных переговоров используются следующие способы подключения:

— параллельное подключение к телефонной линии. В этом случае телефонные радиоретрансляторы труднее обнаруживаются, но требуют внешнего источника питания.

— последовательное включение телефонных радиоретрансляторов в разрыв провода телефонной линии.

Для приема информации от телефонных радиотрансляторов используются такие же приемники, как в акустических устройствах съема информации по радиоканалу.

В настоящее время появились системы перехвата факсовой и модемной связи, которые при использовании персонального компьютера со специальным программным обеспечением позволяют получить расшифровку информации.

Однако такие системы очень дорогие и пока не нашли широкого применения в нашей стране.

Способы, которыми может вестись, прослушивание телефонных линий и какая при этом используется аппаратура наглядно представлены на рис. 5.6. Кратко рассмотрим эти способы.

Непосредственное подключение к телефонной линии — наиболее простой и надежный способ получения информации. В простейшем случае применяется трубка ремонтника — телефониста, подключаемая к линии в распределительной коробке, где производится разводка кабелей. Чаше всего это почерк «специалистов» нижнего звена уголовного мира (верхнее звено оснащено аппаратурой не хуже государственных секретных служб). Необходимо помнить, что АТС переключает линию на разговор при шунтировании ее сопротивлением около 1 кОм.

Применение аппаратуры подслушивания с низкоомным входным сопротивлением можно достаточно быстро обнаружить. Если вы услышите щелчки в линии или перепады громкости, — есть вероятность того, что вас пытаются прослушать не совсем профессиональным способом.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей логики их работы. Обычно слабости все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавиться от них невозможно. Кроме того, уязвимые места иногда обнаруживаются и в электронных цепях, особенно в системах связи и передачи данных.

Список литературы:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.