



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

К.Т.Н.

Струков Владимир Ильич

Вопросы к разделу 5.1

1. **Каким законом регулируются вопросы создания и деятельности частных СБ?**
2. **Кем выдаются лицензии на осуществление частной детективной и охранной деятельности?**
3. **Какое оружие и специальные средства могут применяться при осуществлении частной охраной деятельности?**
4. **Могут ли частные охранники использовать специальные технические средства, предназначенные для негласного получения информации?**
5. **Правовая ответственность за превышение полномочий служащими частных охранных или детективных служб.**

5.2. Правовые основы использования технических средств сбора и защиты информации

К техническим средствам сбора информации относятся:

1. Основные технические средства:

- телефоны городской, внутренней и сотовой связи;**
- селекторная связь;**
- ПК и сети ПЭВМ;**
- копировальная техника.**

Способы сбора информации с использованием телефона и линий связи

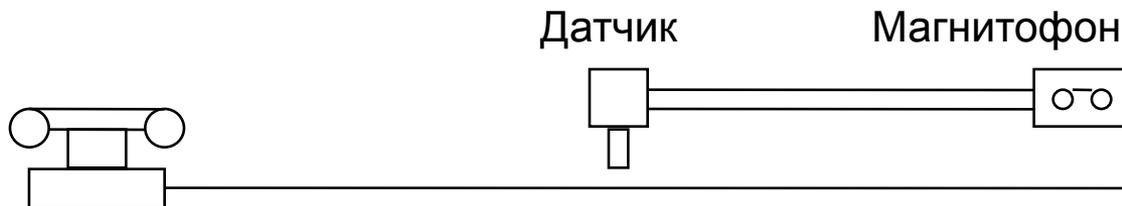
Переизлучение самой конструкции аппарата.

Старые кнопочные аппараты переизлучали информацию в СВ, КВ и УКВ на десятках частот на R до 200 м.

Утечка по звонковой цепи ТЛФ при электроакустическом преобразовании при неснятой трубке (микрофонный эффект).

Подача ВЧ колебаний (от 150 кГц) на один провод, а с другого снимаются модулированные речью колебания (трубка не снята). Дальность съема информации этими способами - несколько десятков метров.

За счет наводки в проводе, параллельном телефонному. Датчик может быть на расстоянии до 20 см от самого провода. Способ трудно обнаружить.

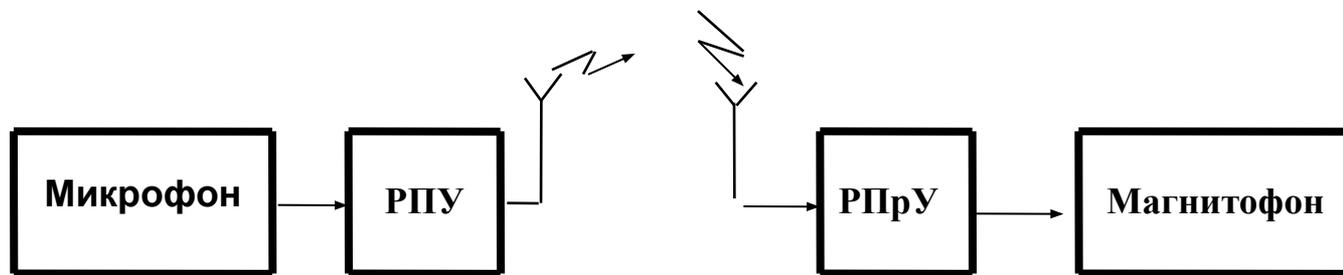


2. Вспомогательные технические средства и системы

- телевизор, магнитофон и др. виды бытовой радиоэлектроники;
- датчики охраны и пожарной сигнализации;
- кондиционер;
- штатное электрооборудование и сети газификации помещения.

3. Специальные технические средства сбора информации

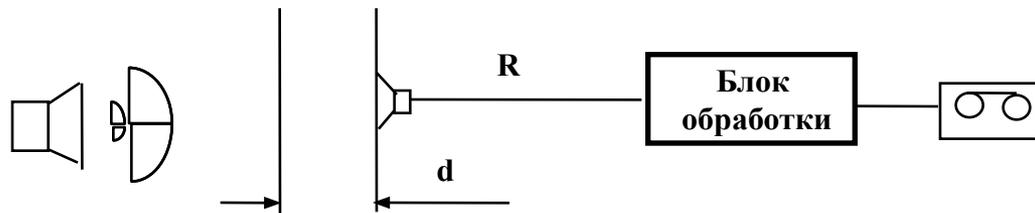
Радиомикрофон (жучок)



Структурная схема подслушивающего устройства

Стетоскоп

Прослушивание через резонирующие перегородки - стены, стекла, батареи отопления.

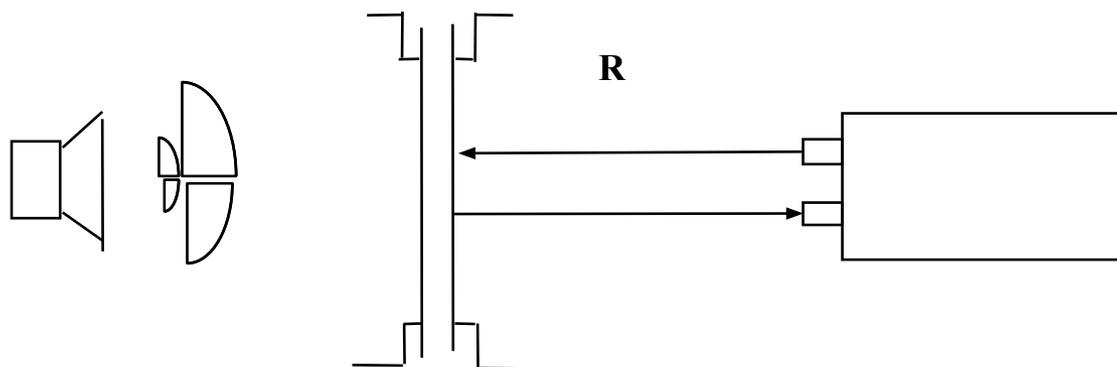


Структурная схема использования стетоскопа.

При d до 1 м и R до 25 м.

d - толщина стены или балки

Лазерный локатор



**Структурная схема использования лазерного локатора.
При R до 600 м.**

Направленный микрофон

Информация по звуковому каналу считывается на расстоянии до 150 м.

Миниатюрные видео- и фотокамеры

Миниатюрные телекамеры размещенные в корпусе наручных часов, замаскированные под винт, авторучку и т.п.

Оборудование для приема побочного ЭМ излучение элементов ПК

Излучение исходит от: монитора, центрального процессора, клавиатуры, принтера, цепи питания.

Диапазон излучения от десятков кГц до сотен мГц и R до 1000 м от ПК.

Оборудование для прослушивания каналов мобильной СВЯЗИ

Технические средства защиты и противодействия

Средства для «контршпионажа» помогают «очистить» помещения и телефоны от всевозможных закладок или их нейтрализовать.

К таким средствам относятся.

1. Устройства поиска и обнаружения активных технических устройств и ПЭМИН (детекторы, сканеры-приемники, детекторы магнитофонов, анализаторы спектра).

Детекторы «жучков» и видеокамер изготавливаются в виде авторучки, пачки сигарет со светодиодным индикатором. Радиус действия - несколько метров.

Карманный детектор подслушивающих "жучков" и скрытых видеокамер определяет точное местонахождение средств нелегального съема аудио и видео информации с передачей данных по радиоканалу.

Индикаторы радиоизлучения

в виде широкополосных приемников или сканирующих детекторов (0,5-3000 МГц).

Нелинейные локаторы - находят пассивные и активные устройства, содержащие полупроводниковые и др. нелинейные элементы.

2. Средства обеспечения скрытности обмена информации

Скремблер - шифровальное средство, предназначенное для защиты информации от непосредственного прослушивания за счет: преобразование аналоговых параметров речи (временная или частотная перестановка сигнала) или цифрового шифрования.

3. Устройства нейтрализации средств съема информации

- Передатчики активных помех (в т.ч. прицельных)**
- Генераторы шумов**
- Устройства защиты от подслушивания через телефонную сеть**
- Индикаторы субъектов и системы ограничения доступа с использованием паролей, ключей, биометрических систем (по отпечаткам пальцев, по голосу, по сетчатки глаз)**

4. Программные и криптографические средства защиты

Программные средства защиты реализуются путем применения специальных программ, включенных в состав программного обеспечения АС и реализующих защиту баз данных и программ обработки конфиденциальной информации.

Используются: пароли, антивирусные программы, электронная подпись, защищенные документы.

Криптографические средства основаны на преобразовании математическими методами какого - либо сообщения.

5. Новые средства:

- устройства, реагирующие на свет (подающие сигнал при открытии ящика стола), светочувствительные покрытия, наносимые на документы**
- маркеры - красители не смывающиеся в течение недели, защищающие от ксерокопирования, дурнопахнущие**
- вязкая пена**
- лазерные ослепители (фонари)**

Детекторы лжи для мобильных телефонов

Устройство может подключаться к сотовому телефону и оценивать правдивость собеседник отличает различные типы состояния и определяет, говорит ли человек правду, сильно возбужден, пытается слегка хитрить или просто врет. Разработчики заявляют, что точность мобильного полиграфа составляет почти 85%.

Услуга компании КТФ на базе технологии Nemesysco. Человеческая речь проходит через датчики, определяющие ее эмоциональную насыщенность. В конце разговора обладатель детектора лжи получает график, демонстрирующий сомнительные моменты беседы и делает соответствующие выводы.



Правовая защита информации, циркулирующей в телефонных и др. линиях связи

Конституция РФ (ст. 23, 24).

Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (ст. 23).

Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается (ст. 24).

УК РФ Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

- 1. Нарушения прав, указанных в 23 ст. Конституции РФ наказываются штрафом до 80 тыс. руб., либо исправительными работами до 1 года.**
- 2. Те же действия, совершенные лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации**

наказываются штрафом до 300 тыс. руб., либо лишением права занимать определенные должности на срок до 5 лет, либо арестом на срок до 4 месяцев, либо лишением свободы на срок от одного года до четырех лет.

3. **Незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, -**

наказываются штрафом в размере **до двухсот тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до **трех лет**, либо **лишением свободы на срок до трех лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на **срок до трех лет**.

Регулирование деятельности, связанной со специальными техническими средствами

Указ Президента РФ №21 от 9.01 96г. «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» постановляет возложить на ФСБ:

- выдачу разрешений на деятельность и контроль использования в области специальных технических средств, предназначенных для негласного получения информации**

- **лицензирование деятельности** не уполномоченных на осуществление оперативно-розыскной деятельности физических и юридических лиц, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввозом в РФ и вывозом за ее пределы специальных технических средств, предназначенных для негласного получения информации, **а также сертификацию**, регистрацию и учет таких специальных технических средств;
- **выявление и пресечение случаев** проведения оперативно-розыскных мероприятий и использования специальных и иных технических средств, разработанных, приспособленных, запрограммированных для негласного получения информации, неуполномоченными лицами.

Постановлением Правительства от 1.07.96г. №770 введено “Положение о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно- розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в РФ и вывоза за ее пределы СТС (специальных технических средств) ”.

В постановлении регламентируются деятельность, связанная с использованием СТС, предназначенных для негласного получения информации.

Лицензированию подлежат следующие виды деятельности:

- разработка и производство СТС;**
- реализация СТС;**
- приобретение СТС в целях продажи, ввоза и вывоза из РФ.**

Регламентируется также деятельность, связанная с применением радиоэлектронным средствам (РЭС).

Постановлением Правительства РФ от 5.06.94г. №643 утверждено “Положение о порядке изготовления, ввоза в РФ и использования на территории РФ радиоэлектронных средств”.

В данном постановлении к РЭС относятся:

- радиостанции**
- системы радионавигации**
- системы кабельного телевидения**
- другие устройства с рабочей частотой выше 9 кГц.**

Литература

1. Шпионские штучки. Под ред. Золоторева С.А. Справочное пособие. Лань, 1996.
2. Технические средства защиты. /Конфидент. Защита информации, №1. 1994.
3. Сугубо конфиденциально. /Коммерсант, №40 за октябрь 1994г.
4. Ярочкин В.И. Служба безопасности коммерческого предприятия. М.: Ось-89. 1995.
5. О.Панин. Служба безопасности и ее роль в обеспечении комплексной защиты предприятия // «Безопасность, достоверность, информация», №2 (53), 2004, с.24-27,

Контрольные вопросы

1. Назовите основные и вспомогательные технические средства утечки информации.
2. Какие технические средства используются для защиты от СТС негласного получения информации?
3. Ответственность за нарушения конституционного права на личную тайну (тайна переписки телефонных переговоров и др. сообщений).
4. Ответственность за незаконное использование СТС.
5. Кто занимается вопросами лицензирования и контроля в области СТС получения информации?
6. Какие виды деятельности подлежат лицензированию в области СТС?
7. Какими документами регулируется деятельность, связанная с использованием радиоэлектронных средств и СТС?