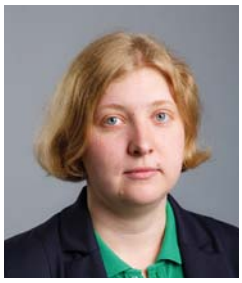
ЗАЩИТА ИНФОРМАЦИИ В ВЫДЕЛЕННЫХ ПОМЕЩЕНИЯХ НА ПРЕДПРИЯТИИ

Ланин Сергей Павлович
Студент 4 курса, направление: Информационная безопасность Автоматизированных систем, Московский Политехнический университет



Ковалёва Анастасия Александровна
старший преподаватель кафедры «Инфокогнитивные технологии», Московского политехнического университета

Аннотация: *в статье описаны технические каналы утечки информации и некоторые методы по избеганию утечки этой информации.*

Ключевые слова: *выделенные помещения, ОТСС, ВТСС, СЗИ, НСД.*

Abstract: *the article describes the technical channels of information leakage and some methods to avoid the leakage of this information.*

Keywords: *allocated premises, OTSS, VTSS, SPI, NSD.*

Введение: В наши дни в серьезных организациях особенно остро стоит проблема защищенности информации от посторонних лиц, в следствии чего появляется все больше компаний и специалистов, компетентных в этих вопросах.

Речь будет идти исключительно о выделенных помещениях. Под выделенным помещением (далее – ВП) понимается помещение, предназначенное для проведений переговоров, собраний и других мероприятий, на которых обсуждается секретная или конфиденциальная информация. В первую очередь, к таким помещениям относятся переговорные комнаты в организациях, в которых происходят мероприятия речевого характера по конфиденциальным вопросам.

Следует отметить, что на данный момент ВП является хорошим показателем серьезности организации, к вопросам защищенности информации. В следствии чего будет интересно и полезно рассмотреть вопросы защиты информации в таких ВП, прежде всего говоря о переговорных комнатах.

Цель исследования: изучить концепцию построения СЗИ в выделенных помещениях.

Задачи исследования:

1) Рассмотреть технические каналы утечки информации;

2) Проанализировать способы несанкционированного доступа к информации закрытого характера;

3) Разработать рекомендации по обеспечению защищенности ВП.

На рисунке 1 представлена схема главных задач в обеспечении безопасности информации является защита информации от:

Рисунок 1. Задачи обеспечения БИ

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

Построение модели угроз и нарушителей для конфиденциальной информации, которое имеет большое значение при проведении переговоров в выделенных помещениях и не только. Разрабатывать модели угроз и нарушителей целесообразно опираясь на поставленные задачи защиты.

На рисунке 2 описаны некоторые виды утечки в акустическом канале:

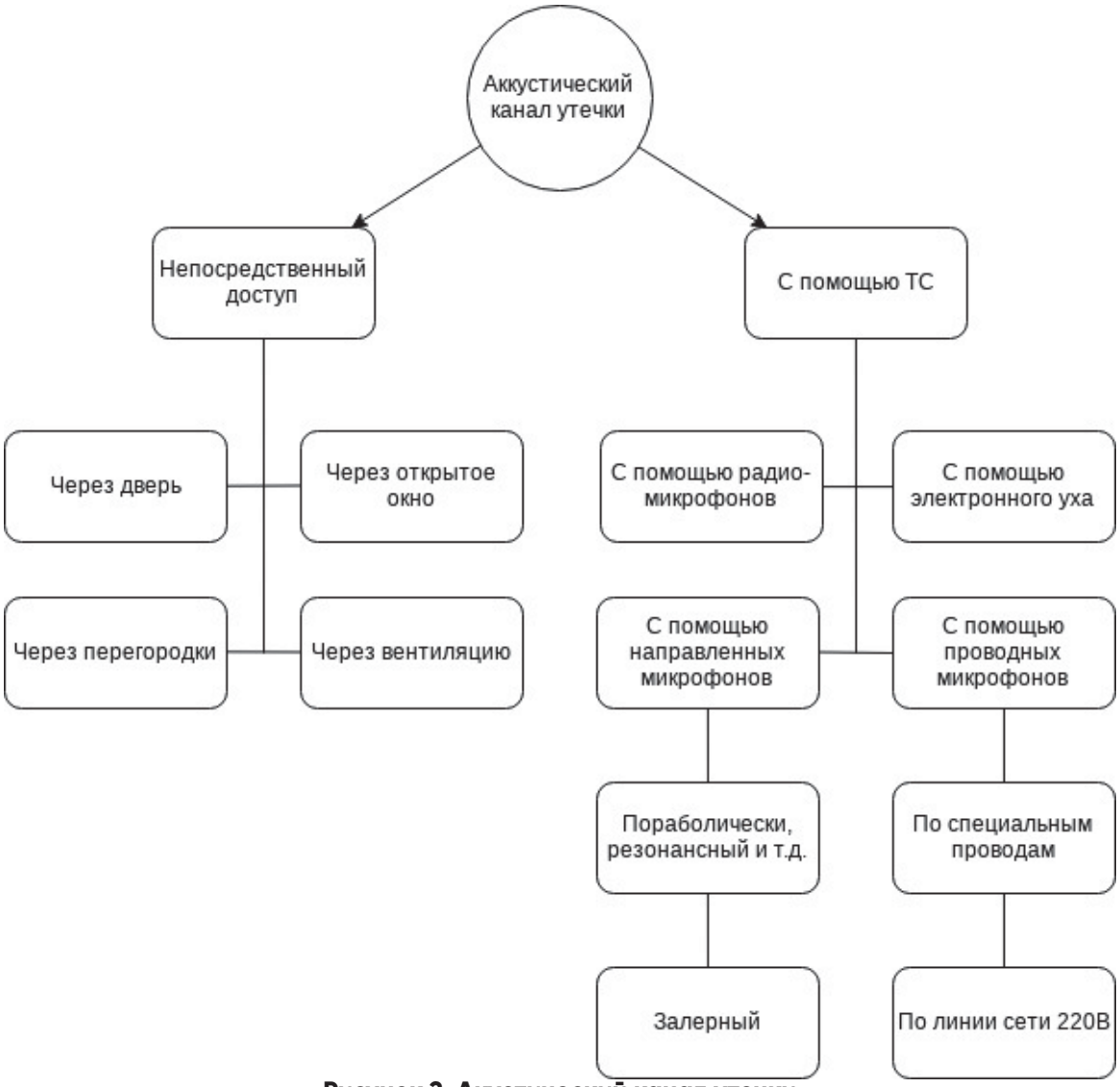


Рисунок 2. Акустический канал утечки

НСД к информации для служебного пользования может осуществляться путем:

- Непосредственного прослушивания;
- С помощью технических средств.

Переговоры можно «подслушать» если не закрыто окна или дверь, либо даже они закрыты, они могут не соответствовать звукоизоляционным нормам. Так же многие ошибочно считают, что потолок, стены и пол служат звукоизоляционными средствами, но ничто из перечисленного не является гарантированной защитой от утечки информации и тут стоит уточнить, если спецпроверки не проводились в принципе - никаких гарантий быть не может.

В настоящее же время злоумышленниками широко используются направленные микрофоны. При всем этом дистанция прослушивания вполне может достигать сотни метров.

В качестве направленных микрофонов злоумышленники часто используют:

- с параболическим отражателем
- резонансные
- щелевые
- лазерные

Более подробные технические характеристики перечисленных микрофонов достаточно полно представлены в интернете и необходимой литературе [2].

На рисунке 3 описано то, как несанкционированный доступ может быть осуществлен:

Рисунок 3. Виброакустический канал утечки

С помощью стетоскопов можно прослушивать стены толщиной до 20 сантиметров, в зависимости от

материала.

Утечка информации для служебного пользования возможно так же благодаря тому, что воздействие звуковых колебаний на элементы электрической схемы вспомогательных технических средств. В профессиональной среде такие технические средства (далее- ТС) принято обозначать как ВТСС.

К таким ТС относятся те, которые не принимают непосредственное участие в обработке информации, но могут быть причиной ее утечки.

На рисунке 4 представлены некоторые возможные каналы утечки за счет ВТСС:

Рисунок 4. Каналы утечки за счет ЭАП и ГО

Такие каналы возможно, если в комнате присутствуют телефонные аппараты, телевизор, электрические часы, приемники и так далее.

Рекомендации по защите:

Для начала необходимо сформулировать задачи и поставить цели. После этого необходимо выявить все каналы утечки информации, путем составления модели угроз и нарушителей.

Потенциальный нарушитель хорошо осведомленный человек, поэтому нужно сразу реализовывать комплекс средств защиты информации.

Очень важен контроль соответствия нормативным документам по ЗИ, и для этого необходима аттестационная комиссия, которая может указать на найденные недостатки и, по мере их полного устранения, - выдать аттестат соответствия.

Список литературы

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005, с. 416.

2. Положение по аттестации объектов информатизации по требованиям безопасности информации. (Утверждено Председателем Гостехкомиссии России 25.11.1994). – М.: Гостехкомиссия РФ, 1994, с. 22.