**Практическая работа № 16**

**Моделирование технической разведки по исходным данным для объекта информатизации**

**Цель работы:** Приобрести практические навыки в определении степени защищенности объекта *информатизации* путем моделирования возможных действий технических разведок. Научиться определять потенциальные и реальные каналы утечки информации.

**Ход работы:**

1)Выявить оставшиеся, потенциально возможные каналы утечки информации (с учетом исходных данных, используя, при необходимости оговорки): визуальные, позволяющие перехватывать или копировать сведения, отражающиеся в визуальной форме, это документы, информация, выведенная на экран монитора компьютера; акустические, позволяющие перехватывать ведущиеся в помещении переговоры или разговоры по телефонам; электромагнитные, позволяющие получать данные, выраженные в виде излучения электромагнитных волн, их дешифровка может также дать необходимые сведения; материальные, связанные с анализом предметов, документов и отходов, возникших в результате деятельности компании.

2)Смоделировать возможные действия технических разведок, определить реальные каналы утечки информации: реальный канал утечки информации – материальный. Возможные действия технических разведок: радиотехнические методы (радиоразведка, радиотехническая разведка, радиолокационная разведка), электронно-оптические методы (фотографическая разведка, телевизионная разведка, инфракрасная разведка, фотометрическая разведка, лазерная разведка), электронно-акустические методы (акустическая и гидроакустическая разведки) и т.д.

3)Доказать целесообразность и предложить проведение тех или иных защитных мероприятий: для защиты абонентской линии можно: подать в линию во время разговора маскирующие низкочастотные сигналы звукового диапазона, поднимать напряжение в линии во время разговора, подача в линию импульсов высокого напряжения для выжигания электронных устройств и блоков их питания.

Для защиты сети электропитания от акустических закладок используется фильтрование и маскирование с помощью трансформаторов и фильтров.

Для защиты речевой информации можно производить звукоизоляцию помещений а также использовать виброакустическое маскирование.

**Вывод:** я приобрел практические навыки в определении степени защищенности объекта информатизации путем моделирования возможных действий технических разведок. Научился определять потенциальные и реальные каналы утечки информации.