**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.

1) Среди сотрудников могут оказаться “инсайдеры”, которые будут причиной утечки информации.

2) Так как, в данном учреждении, посетители могут свободно передвигаться, не исключено, что возможно хищение информации.

3) Утеря сотрудником электронного хранителя информации с важными данными.

4) Нередки потери и кражи мобильных устройств, из-за чего происходят утечки важной конфиденциальной информации. Имеют место и потери данных через установленные на мобильных устройствах мессенджеры, почтовые клиенты и другое ПО.

5) Передача физических документов.

6)  использование вредоносного программного обеспечения

7) Электронная почта. Чаще всего по этому каналу происходят инсайдерские утечки

8) Немалое количество утечек по техническим каналам происходит через всевозможные мессенджеры. Через них также возможна передача вредоносного ПО, фишинговых ссылок и т.д. Для защиты информации от утечек по этим каналам используются организационные меры (например, запрет использования личных аккаунтов в рабочих целях и наоборот), IM-антивирусы и другие программные средства.

9) Вследствие неосторожности сотрудников, инсайдерской деятельности или вторжения извне могут происходить утечки из корпоративных сетей.

Защитные меры:

проводить качественный отбор сотрудников

ужесточение контроля за посетителями.

Применять маскировку объектов и носителей информации.

Использование антивирусного программного обеспечения, шифрование данных.

Ограничивать доступ сотрудников к визуальной информации. В этом помогут специально разработанные политики безопасности.

Оборудовать помещения, в которых работают с визуальными данными, средствами преграждения или ослабления отраженного света: темными стеклами, шторами, роллетами, ставнями.

Располагать экраны и другие защищаемые объекты так, чтобы исключить отражение света в сторону посторонних лиц.

создание системы резервирования информации;

фильтры для запрета отправки почты на определённые домены, системы анализа содержимого писем и прикрепляемых вложений, проверка адресов отправителя и получателя.

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