Лабораторная работа 1

*1. Виды угроз*

*2. Характер происхождения угроз*

*3. Классы каналов несанкционированного получения информации*

*4. Источники появления угроз*

*5. Причины нарушения целостности информации*

*6. Потенциально возможные злоумышленные действия*

*7. Описание неформальной модели нарушителей*

**Наименование объекта защиты информации:**

«Серверы МФЦ»

**2. Характер происхождения угроз.**

1) Умышленные факторы:

- подключение к каналам связи

- несанкционированный доступ

- копирование данных

- размещение информации

2) Естественные факторы:

- стихийные бедствия

- несчастные случаи

- техногенные катастрофы

**3. Классы каналов несанкционированного получения информации:**

- копирование информации с носителей

- подключение к локальным линиям связи

- подключение к ПК по локальным сетям

- хищение носителей информации

**4. Источники появления угроз:**

- люди

- внешняя среда

- модели, программы, алгоритмы

**5. Причины нарушения целостности информации:**

1) Субъективно непреднамеренные:

- человеческий фактор

2) Субъективно преднамеренные:

- действия, произведенные с носителем информации

- программное воздействие (вирусы)

- диверсия

3) Объективно непреднамеренные:

- стихийные бедствия

- техногенные катастрофы

- несчастные случаи

**6. Потенциально возможные злоумышленные действия:**

1) Пассивные:

- получение несанкционированного доступа

- копирование информации

- кража электронных носителей

- сбои в работе электронного носителя

- сбои в работе ПО

2) Активные:

- несанкционированное подключение к локальной сети

- копирование информации с электронных носителей

- уничтожение/порча информации, находящейся в локальной сети

**7. Описание неформальной модели нарушителей:**

1) Внутренние:

Уборщик:

1. Побуждения:

- личная неприязнь к коллегам-сотрудникам

- корыстные побуждения

2. Доступ:

- в часы уборки (7:30-8:00, до работы; 14:00-15:00, в обеденные часы)

- также доступ в случае непредвиденных обстоятельств (разлили жидкость, принесли грязь с обувью и т.д.)

3. Время атаки:

- предпочтительное время для атаки – часы уборки, когда никого нет в бухгалтерии, утром – до прихода бухгалтеров, на обеденном перерыве, когда бухгалтера ушли на обед.

4. Вероятности определенных действий:

(Будем использовать балльную систему, где 1- крайне маловероятно, 10- крайне вероятно)

Кража электронных устройств 2

Порча информации, посредством изменения данных 4

Внедрение вирусов 3

Съем информации 7

Системный администратор:

1. Побуждения:

- личная неприязнь к коллегам-сотрудникам

- корыстные побуждения

2. Доступ:

- в сервисные часы (4 часа раз в 2 месяца)

- также доступ в случае непредвиденных обстоятельств (различные неполадки с техникой, поломки и т.д.)

3. Время атаки:

- предпочтительное время для атаки – сервисные часы, когда никого нет в бухгалтерии.

4. Вероятности определенных действий:

(Будем использовать балльную систему, где 1- крайне маловероятно, 10- крайне вероятно)

Кража электронных устройств 4

Порча информации, посредством изменения данных 5

Внедрение вирусов 6

Съем информации 8