**Практическая работа №20. Оценка уязвимости информации**

**Цель работы:** Ознакомиться с алгоритмами оценки уязвимости информационной безопасности.

**Практическое задание**

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.»

2. Ознакомьтесь с **Приложениями C, D** и **Е** ГОСТа.

3. Выберите три различных информационных актива организации.

4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

5. Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов, предложенных в **Приложении Е** ГОСТа произведите оценку рисков информационной безопасности.

Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Ход работы:

3)

Бомбовая атака

Применение оружия

Пожар

4) 1- угроза использования программного обеспечения несанкционированным способом

2- угроза намеренного повреждения

3 - угроза использования сетевых средств несанкционированным способом

5) 1- Использование программного обеспечения несанкционированными пользователями

2 - Намеренное повреждение

3 - Использование сетевых средств несанкционированным способом

6) 

**Контрольные вопросы**

Дайте определение понятиям:

1. Уязвимости системы защиты информации

2. Угрозы ИБ

3. Оценка рисков

Ответы:

1) Уязвимости системы защиты информации - это недостаток средств защиты информационной системы, который может быть использован нарушителем (как внешним, так и внутренним) для реализации угроз информационной безопасности.

2) Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

3) Оценка риска является частью процесса менеджмента риска и представляет собой структурированный процесс, в рамках которого идентифицируют способы достижения поставленных целей, проводят анализ последствий и вероятности возникновения опасных событий для принятия решения о необходимости обработки риска.

**Вывод:** в результате практической работы мы ознакомились с алгоритмами оценки уязвимости информационной безопасности.