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

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

**Ход работы**

**Информационные активы организации:**

* Нелегальное проникновение злоумышленников под видом санкционированных пользователей
* Незаконный импорт/экспорт программного обеспечения
* Доступ несанкционированных пользователей к сети

**Уязвимости системы защиты информационных активов:**

* Неправильное присвоение прав доступа (возможна, например, угроза использования программного обеспечения несанкционированным способом).
* Неконтролируемая загрузка и использование программного обеспечения (возможна, например, угроза столкновения с вредоносным программным обеспечением)
* Незащищенные линии связи (возможна, например, угроза перехвата информации)

**Угрозы, реализация которых возможна пока в системе не устранены названные в прошлом пункте уязвимости:**

* Программные сбои
* Ошибка при обслуживании
* Доступ несанкционированных пользователей к сети

**Оценка рисков информационной безопасности:**



**Контрольные вопросы:**

1. **Уязвимости системы защиты информации** - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данным.

2. **Угрозы ИБ** - совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Под угрозой понимается потенциально возможное событие, действие, процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам

3. **Оценка рисков** - выявление опасностей, существующих на производстве, определение масштабов этих опасностей и их возможных последствий; один из способов предупреждения несчастных случаев на производстве и повышения безопасности труда.