4.

1) Незащищенные линии связи

2) Отсутствие идентификации и аутентификации отправителя и получателя

3) Пересылка паролей открытым текстом

5.

1) Неисправности в системе электроснабжения

2) Аппаратные отказы

3) Ошибка обслуживающего персонала

6.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Актив | Ценность актива | Уровень угрозы | | | | | | | | |
| низкий | | | средний | | | высокий | | |
| Уровень уязвимости | | | Уровень уязвимости | | | Уровень уязвимости | | |
| Н | С | В | Н | С | В | Н | С | В |
| Незащищенные линии связи | 3 | 2 | 3 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| Отсутствие идентификации и аутентификации отправителя и получателя | 4 | 4 | 3 | 5 | 3 | 2 | 6 | 4 | 5 | 6 |
| Пересылка паролей открытым текстом | 6 | 4 | 5 | 6 | 7 | 6 | 7 | 5 | 7 | 8 |

Контрольные вопросы:

1. Уязвимость системы защиты данных - недостаток или слабое место в системном или прикладном программном обеспечении информационной системы, которые могут быть использованы для реализации угрозы безопасности персональных данных.
2. Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.
3. Оценка рисков – это анализ, который позволяет определить необходимую и достаточную совокупность средств защиты информации, а также организационных мер, направленных на снижение рисков информационной безопасности.

**Вывод: мы ознакомились с алгоритмами оценки уязвимости информационной безопасности и научились проводить оценку уязвимости системы.**