Анализ Рисков

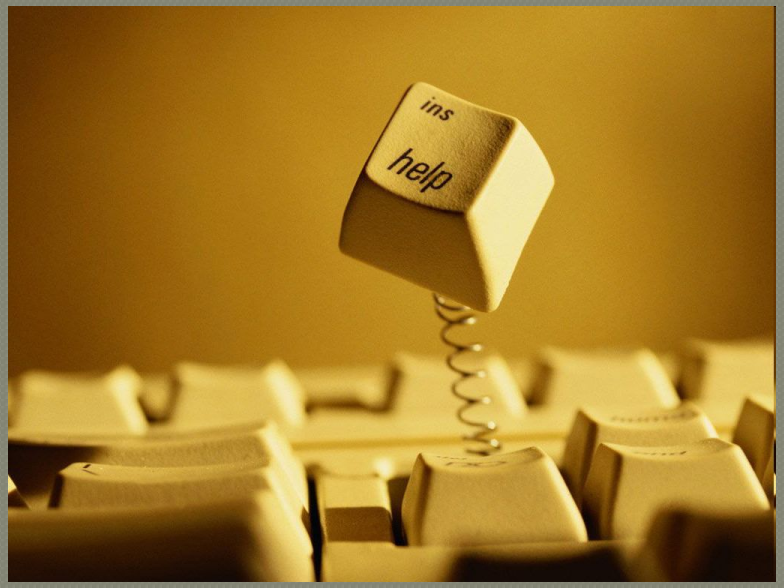
Выполнил
Яшин
Максим
20501

Основные понятия

Анализ рисков является важным разделом КСЗИ на предприятии и при проведение этого анализа используется ряд терминов.

Угроза

- Совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

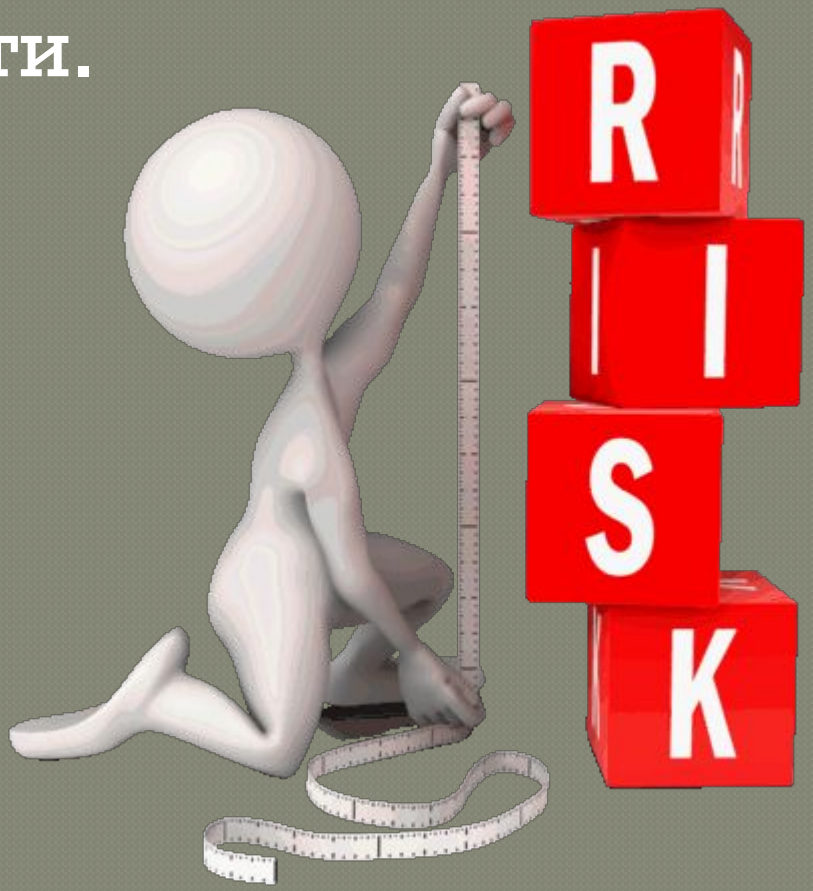


Уязвимость

- Слабость в системе защиты, которая делает возможным реализацию угрозы.

Риск

- Возможность реализации угрозы, нарушения информационной безопасности.



Анализ рисков

- Процесс определения угроз, уязвимостей, возможного ущерба, а также контрмер

Оценка рисков

- Идентификация рисков, выбор параметров для их описания и получения оценок по этим параметрам.

Процесс оценивания рисков содержит несколько этапов:

- Идентификация ресурса и оценивание его количественных показателей или определение потенциального негативного воздействия на бизнес;
- Оценивание угроз;
- Оценивание уязвимостей;
- Оценивание существующих и предполагаемых средств обеспечения информационной безопасности;
- Оценивание рисков;
- Выбор средств, обеспечивающих режим ИБ.

Фактором риска

- Состояние процесса или объекта, которое способствует реализации риска, т.е. обстоятельства, способствующие реализации рисков.

Степень риска зависит от следующих факторов

Показателей ценности ресурсов

Вероятности реализации угроз

Простоты использования уязвимости при возникновении угроз

Существующих или планируемых к внедрению средств обеспечения ИБ, которые уменьшают уязвимости, сокращают вероятность возникновения угроз и негативных воздействий

Шкала оценки ресурсов

- **малоценный информационный ресурс**: от него не зависят критически важные задачи и он может быть восстановлен с небольшими затратами времени и денег;
- **ресурс средней ценности:** от него зависит ряд важных задач, но в случае утраты он может быть восстановлен за время, не превышающее критически допустимое, но стоимость восстановления - высокая;
- **ценный ресурс:** от него зависят критически важные задачи, в случае утраты время восстановления превышает критически допустимое либо стоимость чрезвычайно высока.

Шкала угроз

- **низкий (Н)** - реализация данной угрозы маловероятна, за последние два года подобных случаев не зафиксировано;
- **средний (С)** - угроза может реализоваться в течение одного года с вероятностью около 0,3;
- **высокий (В)** - угроза, скорее всего, реализуется в течение года и, возможно, не один раз

Шкала уязвимостей:

низкий (Н) - защищенность системы очень высока, реализация угроз почти никогда не приводит к происшествию;
средний (С) - защищенность системы средняя, реализация около 30% угроз приводит к происшествию;
высокий (В) - защищенность системы низкая, реализация угрозы практически всегда приводит к происшествию.

Двухфакторный анализ рисков

Риск =$P_{\text{Происшествия}}$ * Цена потери

Трёхфакторный анализ рисков

В зарубежных методиках, рассчитанных на более высокие требования, чем базовый уровень, используется модель оценки риска с тремя факторами: угроза, уязвимость, цена потери;

$$Риск = P_{угрозы} * P_{уязвимости} * цена\ потери$$