

АНАЛИЗ РИСКОВ.
СУЩНОСТЬ И
ОСНОВНЫЕ ПОНЯТИЯ.
ОСНОВНЫЕ ФАКТОРЫ
РИСКА И ШКАЛЫ ДЛЯ
ИХ ИЗМЕРЕНИЯ. ДВУХ
И ТРЕХФАКТОРНЫЙ
АНАЛИЗ РИСКОВ

Выполнила
студентка 5
курса группы
20501.10
Родионова Е.

ОСНОВНЫЕ ПОНЯТИЯ

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 нарушения ИБ – возможность реализации угрозы;

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;



Управление рисками – процесс определения контрмер в соответствии с оценкой рисков;
Класс рисков – множество угроз ИБ, выделенных по определенному признаку.

ПРОЦЕСС ОЦЕНИВАНИЯ РИСКОВ

- 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.



ОСНОВНЫЕ ФАКТОРЫ РИСКА

Фактором риска называется состояние процесса или объекта, которое способствует реализации риска, т.е. обстоятельства, способствующие реализации рисков.



Степень риска зависит от следующих факторов:

- показателей ценности ресурсов, т.е. является ли привлекательным для сторонних лиц и можно ли использовать ресурс для получения дохода;
- 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.



ШКАЛЫ ИЗМЕРЕНИЯ ФАКТОРОВ РИСКА

- прямые (естественные)
- косвенными (производные).

Примерами прямых шкал являются шкалы для измерения физических величин, например шкалы для измерения объемов жидкости в литрах, шкалы для измерения длины в метрах.

В ряде случаев прямых шкал не существует, приходится использовать либо прямые шкалы других свойств, связанных с интересующими нас, либо определять новые шкалы. Шкала для измерения субъективного свойства «ценность информационного ресурса». Эта ценность может измеряться в единицах измерения производных шкал, таких как стоимость восстановления ресурса, время восстановления ресурса и др.



Определим шкалу для получения экспертной оценки, например объединим в ней три значения:

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.



Факторы выбора шкал из множества:

- Конкретные ресурсы конкретного предприятия.
- Шкала должна однозначно пониматься экспертами.

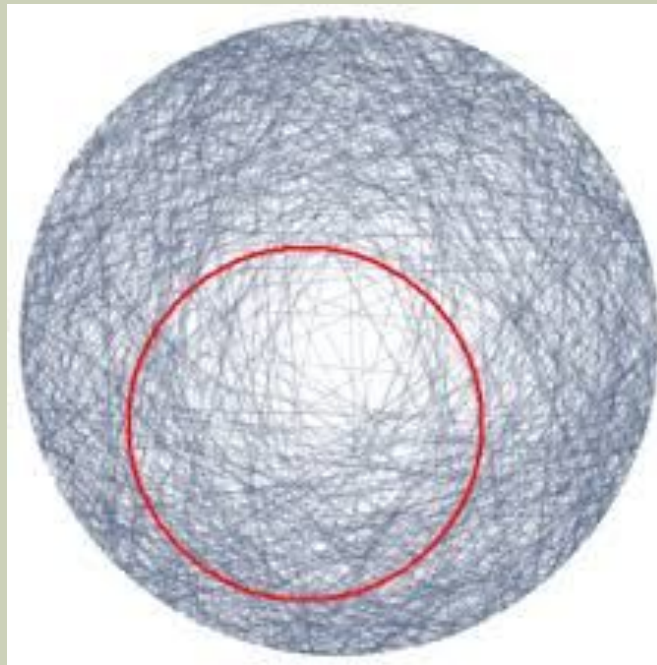
После выбора шкалы необходимо провести ее обкатку.

Риски можно оценивать по объективным либо субъективным критериям. Примером объективного критерия является вероятность выхода из строя какого-либо оборудования, например ПК, за определенный промежуток времени. Пример субъективного критерия - оценка владельцем информационного ресурса риска выхода из строя ПК.

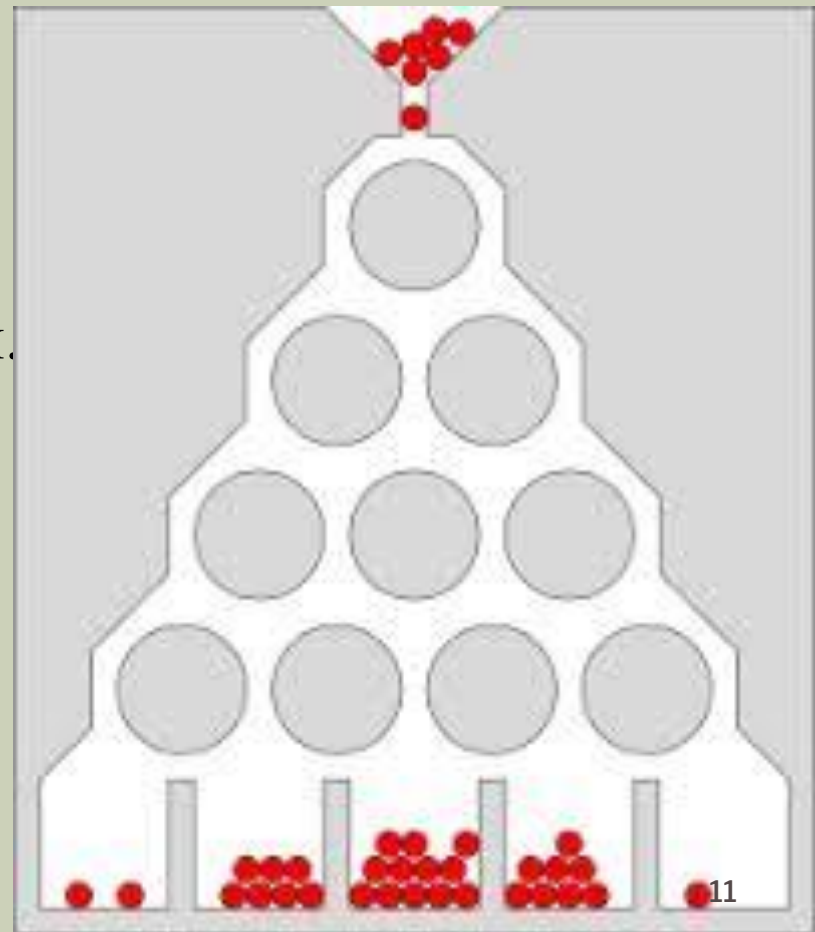


ОБЪЕКТИВНЫЕ И СУБЪЕКТИВНЫЕ ВЕРОЯТНОСТИ

- Под субъективной вероятностью имеется в виду мера уверенности некоторого человека или группы людей в том, что данное событие в действительности будет иметь место (меры, полученные экспертным путем).



Под объективной (иногда называемой физической) вероятностью понимается относительная частота появления какого-либо события в общем объеме наблюдений или отношение числа благоприятных исходов к общему количеству наблюдений. Это понятие применяется при анализе результатов большого числа наблюдений, имевших место в прошлом, а также полученных как следствия из моделей, описывающих некоторые процессы.



ОЦЕНКА РИСКОВ ПО ДВУМ ФАКТОРАМ

В простейшем случае используется оценка из двух факторов.

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

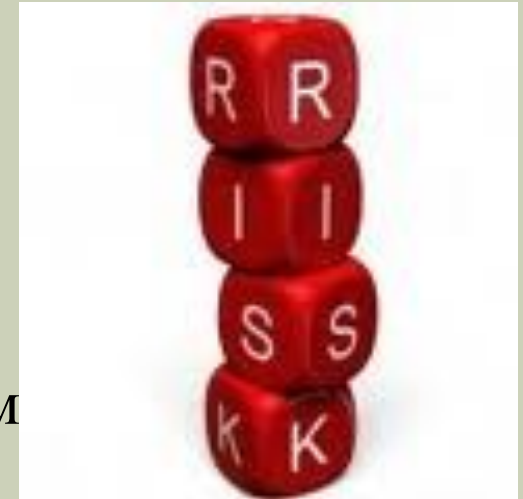
Если переменные являются количественными величинами, то риск – это оценка математического ожидания потерь. Если переменные являются качественными величинами, то метрическая операция умножения не определена. Т.о. в явном виде эта формула использоваться не должна.



ОЦЕНКА РИСКОВ ПО ТРЕМ ФАКТОРАМ

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

Вероятность происшествия, которая в данном подходе может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей.



$$P_{\text{происшествия}} = P_{\text{угрозы}} * P_{\text{уязвимости}}$$

Соответственно риск определяется следующим образом:

$$\text{Риск} = P_{\text{угрозы}} * P_{\text{уязвимости}} * \text{Цена потери}$$

Данное выражение можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал качественная.



КОНТРОЛЬНЫЕ ВОПРОСЫ

- Что такое угроза?
- Чем отличается угроза от уязвимости?
- Как происходит процесс оценивания рисков?
- Какие шкалы измерения факторов риска Вы знаете?
- Какие факторы учитываются при двухфазном анализе риска?
- Какие факторы учитываются при трехфазном анализе риска?