АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАНОСТИ

Раздел 1.

Цель

Получить знания и навыки в области оценки и управления рисками:

- Понимать термины и важность менеджмента рисков
- Понимать место информационной безопасности в теме управления рисками организации
- Понимать общий подход к менеджменту рисков
- Знать общий подход к оценке рисков информационной безопасности
- Ориентироваться в методиках оценки

Неприятности подстерегают нас повсюду

Неприятности (опасности, угрозы) связаны со всем, что у нас есть !

«Если у Вас нет собаки, –
Ее не отравит сосед.
И с другом не будет драки,
Если у Вас друга нет…»

Чем больше мы имеем, тем в большей опасности находимся!

«Думайте сами,
Решайте сами,
Иметь или не иметь…»

ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ

Автомобильная аналогия

Какую машину покупать (какая безопасней) ?

Ставить противоугонное устройство или нет ?

Платить или нет за охраняемую стоянку ?

Страховать или нет ? (если да, - то от чего?)

Ставить ли новую зимнюю резину ?

…

А может вообще не покупать машину ?

ЗАЩИТА – ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ

Суть защиты ресурсов корпоративных сетей –

есть управление рисками, связанными с использованием этих сетей

Риск - вероятностно-стоимостная оценка возможных потерь

Связан с определенной угрозой безопасности и характеризуется:

- вероятностью реализации угрозы
- стоимостью потерь в случае реализации угрозы

Риск - вероятность причинения вреда … с учетом тяжести этого вреда

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»

Что такое риск?

Риск – возможная опасность чего либо (Д.Н. Ушаков Большой толковый словарь современного русского языка)

Риск – ситуация, когда результат какого либо действия неочевиден и неоднозначен и может быть несколько исходов результатов. (*Райзберг Б.А. Современный экономический словарь. – 1999)*

Риск есть всегда…

Некоторые классификации видов риска

- Время возникновения:
  - Ретроспективные
  - Текущие
  - Перспективные
- Основные факторы возникновения:
  - Политические
  - Экономические
  - Природные
  - Антропогенные
- Источники риска:
  - Внешние
  - Внутренние
- Характер последствий:
  - Чистые риски
  - Спекулятивные

Классификация рисков по сфере возникновения (деятельности)

- Промышленные
- Экологические
- Инвестиционные
- **Банковские**
- Кредитные
- Технические
- Финансовые
- Налоговые
- Организационные
- Политические
- Страховые
- …

ОБОБЩЕННАЯ ОЦЕНКА ИЗДЕРЖЕК

$$R = \sum_{i=1}^{n} (P_i \cdot B_i + C_i) < R_{\max}$$

n – количество рисков (угроз)

P – вероятностная оценка риска (0-1)

B – стоимостная оценка риска ($)

C – стоимость реализации мер защиты ($)

R – суммарные издержки ($)

R_{max} – допустимые издержки ($)

ЗАЩИТА – ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ

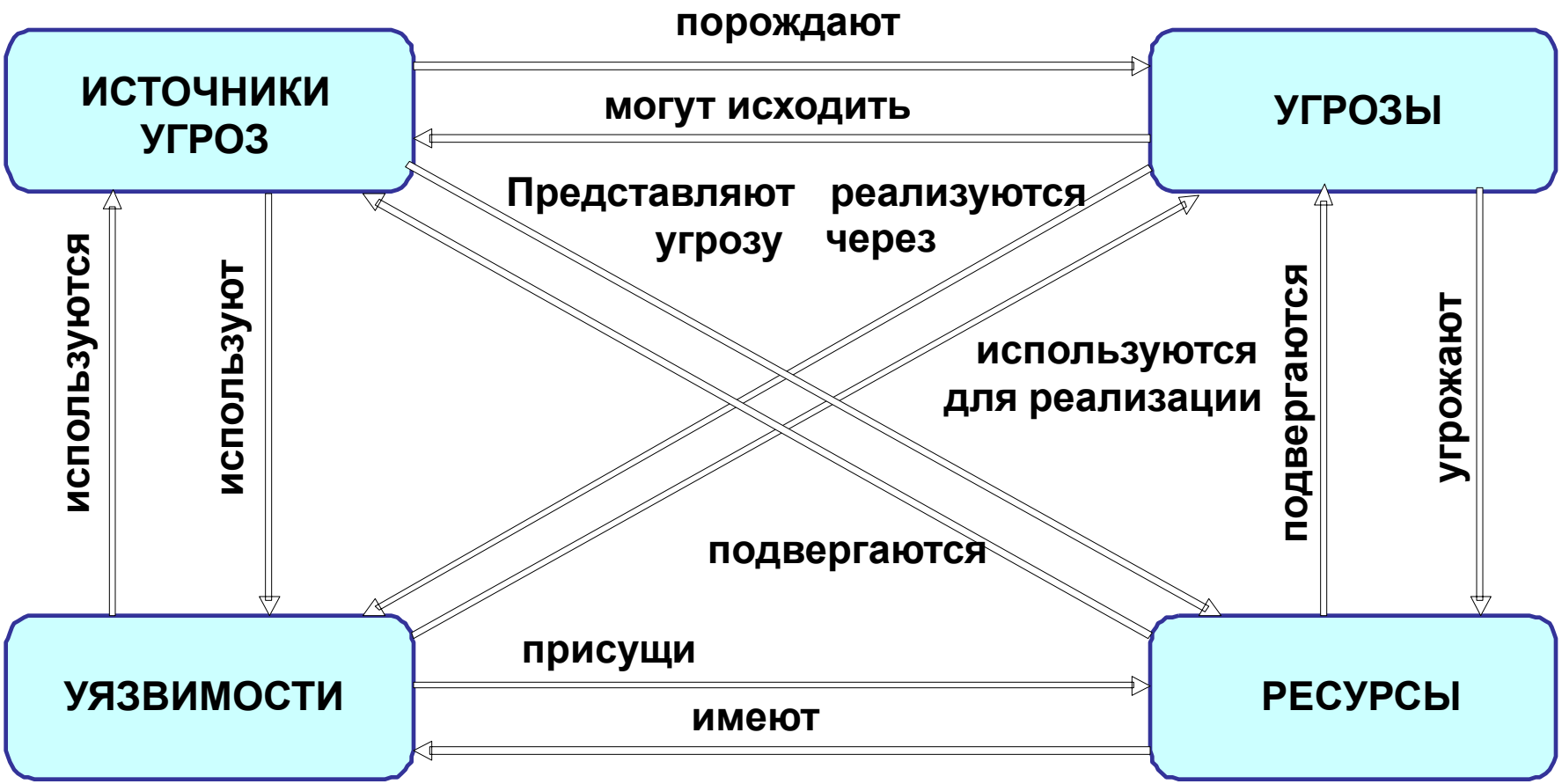
Оценка рисков предполагает выявление всех значимых угроз, то есть угроз с большой частотой (вероятностью) реализации и/или приводящих к существенным (ощутимым) потерям

Управление рисками предполагает принятие мер защиты (контрмер), направленных на снижение частоты (вероятности) реализации угроз и/или на снижение размера ущерба в случае их реализации (одна из 4х форм управления).

Защитные меры выбираются на основе принципа разумной достаточности (экономической целесообразности), исходя из минимизации общих издержек – затрат на защиту плюс возможных остаточных потерь от реализации угроз

ДВА СПОСОБА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Взаимосвязь понятий анализа рисков



Основные понятия

На этапе анализа рисков **определяется:**

- ✓потенциальная возможность Организации понести убытки из-за нарушения режима ИБ;
- ✓детализируются характеристики (или составляющие) рисков для используемых (планируемых к использованию) информационных ресурсов и технологий.

Результаты проведенного анализа **используются при:**

- ✓выборе средств защиты;
- ✓оценке эффективности существующих и проектируемых подсистем ИБ.

Концепции управления рисками

- Семейство СУИБ ISO 27x
- ГОСТ Р ИСО/МЭК 13335-3-2000 – рекомендации по выбору методики управления рисками.
- «Рекомендации в области стандартизации Банка России» РС БР ИББС - 2.2. «Методика оценки рисков нарушения ИБ»
- BSI (Германия).
- NIST 800-30 (США).
- Решение Microsoft Operations Framework (MOF).
- Решение Microsoft Solutions Framework (MSF).
- Группа CERT (Computer Emergency Response Team): методика самостоятельной оценки рисков и планирования OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM).
- Стандарт COBIT (контрольные показатели для информационных и связанных с ними технологий).
- Группа IETF: глоссарий Request for Comments (RFC) 2828.

Уровни анализа рисков

БАЗОВЫЙ:

- ✓ рассчитан на наиболее распространенные риски и соответствующие контрмеры

ПОЛНЫЙ:

- ✓ включает изучение бизнес-процессов компании;
- ✓ принятие во внимание как реальных, так и потенциальных угроз и уязвимостей;
- ✓ предполагает использование количественных методик ранжирования рисков.

дель анализа рисков

ГОСТ Р ИСО/МЭК 15408-1-2008

Постановка задачи анализа рисков

Анализ информационных рисков позволяет эффективно управлять ИБ предприятия.

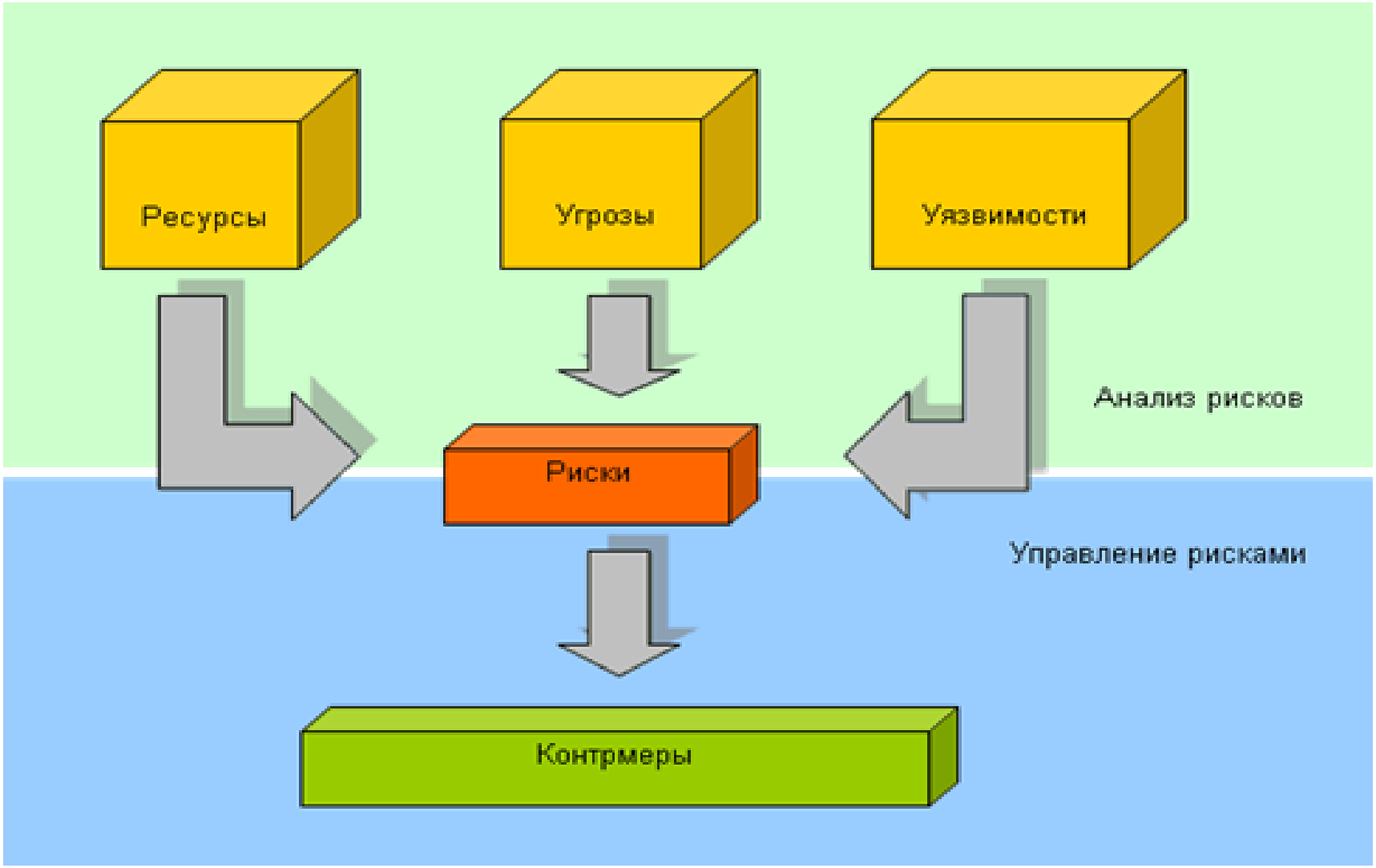
При анализе рисков необходимо:

1. Что именно подлежит защите на предприятии (категорирование и инвентаризация ресурсов/определение ценности ресурсов).
2. Воздействию каких угроз это подвержено (оценка факторов риска).
3. Математические расчёты величины рисков (с использованием ПО).

==========

4. Выработать рекомендации по практике защиты.

Этапы анализа рисков



Управление рисками (подходы)

Первый - уменьшение риска путем использования комплексной системы контрмер, включающей программно-технические и организационные меры защиты (т.е. действия по уменьшению вероятности и/или влияния риска)

Второй - уклонение от риска (например, прекращение деятельности, ведущей к риску).

Управление рисками (подходы)

Третий - в некоторых случаях допустимо принятие риска.

Четвёртый – передача (перераспределение) риска – например: страхование.

Дилемма: что для предприятия выгоднее – бороться с рисками или же с их последствиями (оптимизационная задача).

После определения стратегии управления рисками, производится окончательная оценка мероприятий по обеспечению ИБ с подготовкой экспертного заключения о защищенности ИР.

В экспертное заключение включаются все материалы анализа рисков и рекомендации по их снижению.

ТЕХНОЛОГИИ АНАЛИЗА РИСКОВ

Методология измерения рисков

Сравнение двух подходов

Как количественный, так и качественный подход к управлению рисками ИБ имеет свои преимущества и недостатки.

В некоторых случаях организациям выгоднее использовать количественный подход, а качественный подход может лучше подойти организациям небольшого размера или обладающим ограниченными ресурсами.

Оценка рисков по двум факторам

Используется оценка двух факторов: ***вероятность происшествия*** и ***тяжесть возможных последствий***.

Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий.

Общая идея может быть выражена формулой:

РИСК = Р происшествия * ЦЕНА ПОТЕРИ

Если переменные являются количественными величинами, риск - это оценка математического ожидания потерь.

Если переменные являются качественными величинами, то метрическая операция умножения не определена.

Таким образом, в явном виде эта формула использоваться не должна.

Использование качественных величин

1. Определение шкалы.

Определятся субъективная шкала **вероятностей событий**, пример такой шкалы:

A - Событие практически никогда не происходит
B - Событие случается редко
C - Вероятность события за рассматриваемый промежуток времени – около 0.5
D - Скорее всего, событие произойдет
E - Событие почти обязательно произойдет.

Использование качественных величин

2. Определение субъективной шкалы *серьезности происшествий,* например:

N - Воздействием можно пренебречь

Mi - Незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на ИТ – незначительно.

Mo - Происшествие с умеренными результатами: ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию не велико и не затрагивает критически важные задачи.

S - Происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами, воздействие на ИТ ощутимо, воздействует на выполнение критически важных задач.

C - Происшествие приводит к невозможности решения критически важных задач.

Использование качественных величин

3. Для оценки рисков определяется шкала из трех значений:

Показатель риска:

Низкий риск

Средний риск

Высокий риск

Определение риска в зависимости от двух факторов

	N	Mi	Mo	S	C
A	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
B	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
C	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
D	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
E	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

Определение риска в зависимости от двух факторов

Шкалы факторов риска и сама таблица могут быть определены иначе, иметь другое число градаций.

При разработке (использовании) методик оценивания рисков необходимо учитывать следующие особенности:

- Значения шкал должны быть четко определены (словесное описание) и пониматься одинаково всеми участниками процедуры экспертной оценки.

- Требуются обоснования выбранной таблицы: необходимо убедиться, что разные инциденты, характеризующиеся одинаковыми сочетаниями факторов риска, имеют с точки зрения экспертов одинаковый уровень рисков (для этого существуют специальные процедуры проверки).

Оценка рисков по трем факторам

Модель оценки риска с тремя факторами: ***угроза, уязвимость, цена потери.***

Угроза - совокупность условий и факторов, которые могут стать причиной нарушения КЦД информации.

Уязвимость - слабость (свойство) в системе защиты, которая делает возможным реализацию угрозы.

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

P происшествия = P угрозы * P уязвимости

Оценка рисков по трем факторам

Риск определяется следующим образом:

РИСК = Р угрозы * Р уязвимости * 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. В последнем случае используются различного рода табличные методы для определения риска в зависимости от трех факторов.

Например, ***показатель риска*** измеряется в шкале от 0 до 8 со следующими определениями уровней риска:

- 0 - риск практически отсутствует. Теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик.
- 1 - риск очень мал. События подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики.
- .....
- 8 - риск очень велик. Событие, скорее всего наступит, и последствия будут чрезвычайно тяжелыми.

Определение риска в зависимости от трех факторов

Степень серьезности происшествия (цена потери)	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
N	0	1	2	1	2	3	2	3	4
Mi	1	2	3	2	3	4	3	4	5
Mo	2	3	4	3	4	5	4	5	6
S	3	4	5	4	5	6	5	6	7
C	4	5	6	5	6	7	6	7	8

Выбор допустимого уровня риска

Два подхода к выбору допустимого уровня рисков

Первый подход (*базовый уровень* безопасности):

- Уровень остаточных рисков не принимается во внимание.
- Затраты на программно-технические средства защиты и организационные мероприятия, необходимые для соответствия ИС спецификациям базового уровня (антивирусное ПО, МСЭ, системы резервного копирования и контроля доступа) являются обязательными, их целесообразность не обсуждается.

Дополнительные затраты (если такой вопрос будет поставлен по результатам проведения аудита ИБ, либо по инициативе службы безопасности) должны находиться в разумных пределах и не превышать 5-15% средств, которые тратятся на поддержание работы ИС.

Второй подход применяется при обеспечении ***повышенного уровня*** безопасности. Собственник ИР должен сам выбирать допустимый уровень остаточных рисков и нести ответственность за свой выбор.

Обоснование выбора допустимого уровня риска

Наиболее распространенным способом является анализ стоимость/эффективность различных вариантов защиты.

Примеры постановок задач:

- Стоимость подсистемы безопасности должна составлять не более 20% от стоимости ИС. Найти вариант контрмер, максимально снижающих уровень интегральный рисков.

- Уровень рисков по всем классам должен не превышать «очень низкий уровень». Найти вариант контрмер с минимальной стоимостью.

- В случае постановок оптимизационных задач важно правильно выбрать комплекс контрмер (перечислить возможные варианты) и оценить его эффективность.