# Анализ рисков


Выполнил: Урюмцев Илья
Группа: 20501

# введение

**Анализ рисков** – процедуры выявления факторов рисков и оценки их значимости, по сути, анализ вероятности того, что произойдут определенные нежелательные события и отрицательно повлияют на достижение целей проекта.

Анализ рисков включает оценку рисков и методы снижения рисков или уменьшения связанных с ним неблагоприятных последствий. На первом этапе производится выявление соответствующих факторов и оценка их значимости. Назначение анализа рисков — дать потенциальным партнерам необходимые данные для принятия решений о целесообразности участия в проекте и выработки мер по защите от возможных финансовых потерь.

# Основные определения

**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.

# Этапы оценивания рисков

В настоящее время используются два подхода к анализу рисков. Их выбор зависит от оценки собственниками ценности своих информационных ресурсов и возможных последствий нарушения режима ИБ.

**В простейшей случае** собственники информационных ресурсов могут не оценивать эти параметры. В этом случае анализ рисков производится по упрощенной схеме: рассматривается стандартный набор наиболее распространенных угроз безопасности без оценки их вероятности и обеспечивается минимальный или базовый уровень ИБ.

**Полный вариант** анализа рисков применяется в случае повышенных требований в области ИБ. В отличие от базового варианта в том или ином виде производится оценка ценности ресурсов, характеристик рисков и уязвимостей ресурсов.

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.

# Определение требований

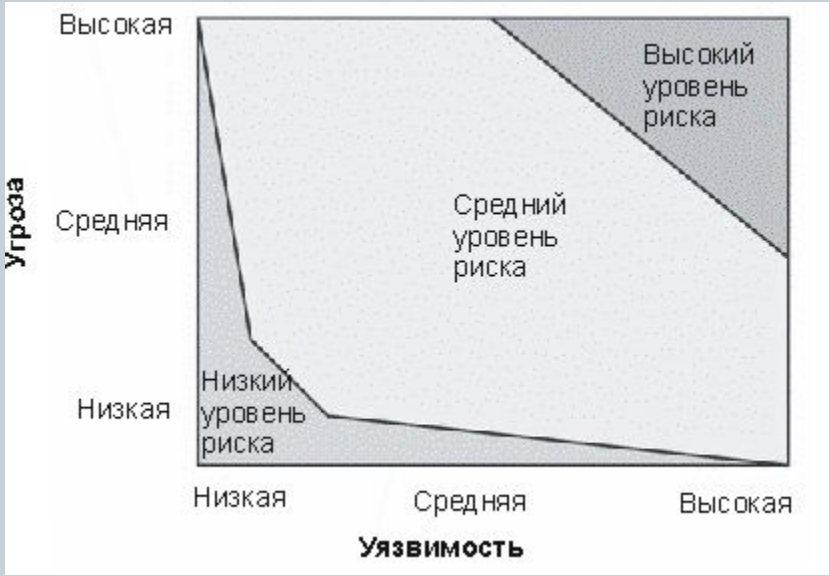
# Выявление риска для организации

Выявление риска не является проблемой. Все, что нужно - это определить уязвимости и угрозы - и дело сделано. Возникает вопрос: как этот установленный риск соотносится с реальным риском организации? Если ответить коротко - не совсем точно. Определение риска в организации должно выполняться по ее заказу.

# Определение риска

При исследовании риска вы должны понимать уязвимости и угрозы для организации.

Если нет угрозы или уязвимости, то нет и риска.



# ОЦЕНКА РИСКА

Для оценки риска следует определить ущерб, нанесенный организации при успешном выполнении атаки. Издержки организации в случае реализации риска - это определяющий фактор для любого решения по управлению риском. Помните, что риск нельзя полностью устранить - им можно только управлять.

# ФАКТОРЫ РИСКОВ

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

Следовательно степень риска зависит от следующих факторов:

1. показателей ценности ресурсов, т.е. является ли привлекательным для сторонних лиц и можно ли использовать ресурс для получения дохода;
2. вероятности реализации угроз;
3. простоты использования уязвимости при возникновении угроз;
4. существующих или планируемых к внедрению средств обеспечения ИБ, которые уменьшают уязвимости, сокращают вероятность возникновения угроз и негативных воздействий.

# Угроза + Уязвимость = Риск

**Риск** - это сочетание угрозы и уязвимости. Угрозы без уязвимости не являются риском так же, как и уязвимости без угроз. В реальном мире ни одно из этих условий не существует. Следовательно, оценка риска - это определение вероятности того, что непредвиденное событие произойдет. Риск качественно определяется тремя уровнями.

**Низкий.** Существует маленькая вероятность проявления угрозы. По возможности нужно предпринять действия по устранению уязвимого места, но их стоимость должна быть сопоставлена с малым ущербом от риска.

**Средний.** Уязвимость является значительным уровнем риска для конфиденциальности, целостности, доступности и/или идентифицируемости информации, систем или помещений организации. Существует реальная возможность осуществления такого события. Действия по устранению уязвимости целесообразны.

**Высокий.** Уязвимость представляет собой реальную угрозу для конфиденциальности, целостности, доступности и/или идентифицируемости информации, систем или помещений организации. Действия по устранению этой уязвимости должны быть предприняты незамедлительно.

# ДВУХФАКТОРНЫЙ АНАЛИЗ РИСКОВ

Оценка рисков по двум факторам. В простейшем случае используется оценка двух факторов: вероятность происшествия и тяжесть возможных последствий.

Риск = Р происшествия * 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.

# ТРЕХФАКТОРНЫЙ АНАЛИЗ РИСКОВ

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 происшествия = P угрозы * P уязвимости

Соответственно риск определяется следующим образом:

Риск = P угрозы * P 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.

# методы проведения анализа риска. Метод CRAMM

CRAMM (the UK Government Risk Analysis and Management Method) — метод, разработанный Службой Безопасности Великобритании и является государственным стандартом Великобритании. Получивший широкое распространение в мире, данный стандарт используется как в коммерческих, так и государственными организациями Великобритании с 1985 года. Метод CRAMM был изобретён фирмой Insight Consulting Limited.

Базируясь на комплексном подходе к оценке рисков, метод CRAMM сочетает количественные и качественные методы анализа рисков и может быть применён как в крупных, так и небольших организациях. Имеются различные версии CRAMM для разных типов организаций, они отличаются базами знаний (профилями): существует коммерческий профиль и правительственный профиль(с помощью которого имеется возможность проводить аудит в соответствие с требованиями американского стандарта ITSEC — так называемой «оранжевой книгой»).

# Метод RiskWatch


Разработанный американской компанией RiskWatch Inc., одноимённый программный продукт служит мощным инструментом анализа и управления рисками. Данное семейство продуктов используется для различных видов аудитов безопасности и содержит следующие средства:

- RiscWatch for Physical Security — инструмент для физических методов защиты информационных систем;
- RiscWatch for Physical Security — инструмент, применяемый к информационным рискам;
- HIPPAA-WATCH for Healthcare Industry — инструмент для оценки соответствия стандарта HIPAA;
- RiskWatch RW17799 for ISO17799 — для оценки требованиям стандарта ISO17799.

Критериями для оценки и управления рисками в методе RiskWatch служит «предсказание годовых потерь» (ALE — Annual Loss Expectancy) и оценка подсчёта ROI(Return on Investment) — «возврата от инвестиций».

# Метод ГРИФ


В отличие от западных систем анализа рисков, достаточно громоздких и не предполагающих самостоятельное применение IT-менеджерами и системными администраторами, система ГРИФ располагает интуитивно-понятным интерфейсом. Но при всей простоте, в системе ГРИФ реализованы огромное количество алгоритмов анализа рисков, учитывающие более ста параметров, и система способна предоставить максимально точную оценку рисков, которые имеют место в информационной системе. Важная особенность ГРИФ — в предоставлении возможности самостоятельной, без привлечения экспертов, оценки рисков в информационной системе, оценка текущего состояния, и расчёта инвестиций в целях обеспечения защищённости информации.

Порядковая шкала. Существуют случаи, когда не имеется необходимости или возможности установки соответствия ценности информации в денежных единицах (например, информация личного характера, военная или политическая информация, оценка которой в денежном эквиваленте может быть неразумной), но при этом может иметь смысл сравнительная оценка отдельных информационных компонент одной компоненты относительно другой.

В качестве примера можно рассмотреть ситуацию в государственных структурах, где информация разбивается по грифам секретности. В свою очередь, грифы секретности представляют собой порядковые шкалы ценностей, например: несекретно, для служебного пользования, секретно, совершенно секретно, особой важности (НС, ДСП, С, СС, ОВ); по американской системе: unclassified, confidential, secret, top secret (U, Conf, S, TS). Чем выше класс грифа, тем большую ценность имеет защищаемая информация, в связи с чем по отношению к ней применяются более высокие требования по её защите от несанкционированного доступа.

# Контрольные вопросы

- Что такое риск?
- Что такое уязвимость?
- Что такое угроза?
- Какими методами оценки рисков можно воспользоваться на практике?