

**ПРОЕКТ**

По дисциплине **«Введение в проектную деятельность»**

Группа: 191-331

Студент: Травкин А. И.

Руководителей образовательной программы:

Гневшев Александр Юрьевич

МОСКВА 2020

**Методика оценки рисков ИБ**

Обычно для определения рисков информационной безопасности используются 2 метода: **количественный и качественный**.

Теперь давайте разберёмся в разнице этих двух методов.

**Количественный метод** - применяется в тех ситуациях, когда исследуемые угрозы и связанные с ними риски можно сопоставить с конечными количественными значениями, выраженными в деньгах, процентах, времени. Данный метод позволяет получить конкретные значения объектов оценки риска при реализации угроз информационной безопасности.

При количественном подходе всем элементам оценки рисков присваивают конкретные и реальные количественные значения. Алгоритм получения данных значений должен быть нагляден и понятен. Объектом оценки может являться ценность актива в денежном выражении, вероятность реализации угрозы, ущерб от реализации угрозы, стоимость защитных мер и прочее.

**Как провести количественную оценку рисков?**

1.  Определить ценность информационных активов в денежном плане.

2. Оценить потенциальный ущерб от реализации каждой угрозы в отношении каждого информационного актива.

Следует получить ответы на вопросы «Какова стоимость ущерба в денежном выражении от единичного инцидента при реализации данной угрозы к данному активу?».

3. Определить вероятность реализации каждой из угроз ИБ.

Для этого можно использовать статистические данные, опросы сотрудников и заинтересованных лиц. В процессе определения вероятности рассчитать частоту возникновения инцидентов, связанных с реализацией рассматриваемой угрозы ИБ за контрольный период (например, за один год).

4. Определить общий потенциальный ущерб от каждой угрозы в отношении каждого актива за контрольный период (за один год).

Значение рассчитывается путем умножения разового ущерба от реализации угрозы на частоту реализации угрозы.

5. Провести анализ полученных данных по ущербу для каждой угрозы.

По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск.

Принять риск — значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения.

Снизить риск — значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы.

Перенести риск — значит переложить последствия от реализации риска на третье лицо, например, с помощью страхования.

В результате количественной оценки рисков должны быть определены:

* ценность активов в денежном выражении;
* полный список всех угроз ИБ с ущербом от разового инцидента по каждой угрозе;
* частота реализации каждой угрозы;
* потенциальный ущерб от каждой угрозы;
* рекомендуемые меры безопасности, контрмеры и действия по каждой угрозе.

## **Количественный анализ рисков информационной безопасности (пример)**

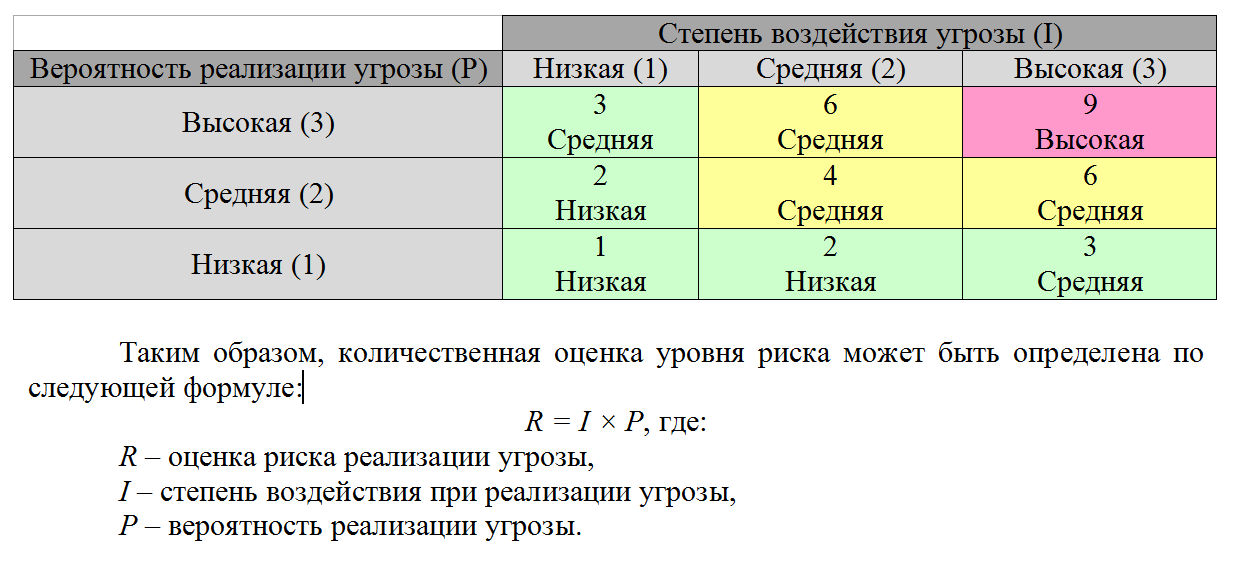
Рассмотрим методику на примере веб-сервера организации, который используется для продажи определенного товара. Количественный **разовый** ущерб от выхода сервера из строя можно оценить как произведение среднего чека покупки на среднее число обращений за определенный временной интервал, равное времени простоя сервера. Допустим, стоимость разового ущерба от прямого выхода сервера из строя составит 100 тысяч рублей.

Теперь следует оценить экспертным путем, как часто может возникать такая ситуация (с учетом интенсивности эксплуатации, качества электропитания и т д.). Например, с учетом мнения экспертов и статистической информации, мы понимаем, что сервер может выходить из строя до 2 раз в год.

Умножаем две эти величины, получаем, что **среднегодовой** ущерб от реализации угрозы прямого выхода сервера из строя составляет 200 тысяч рублей в год.

Эти расчеты можно использовать при обосновании выбора защитных мер. Например, внедрение системы бесперебойного питания и системы резервного копирования общей стоимостью 100 тысяч рублей в год позволит минимизировать риск выхода сервера из строя и будет вполне эффективным решением.

Мы можем определить степень риска по формуле ниже:



## **Качественный метод**



К сожалению, не всегда удается получить конкретное выражение объекта оценки из-за большой неопределенности. Как точно оценить ущерб репутации компании при появлении информации о произошедшем у нее инциденте ИБ? В таком случае применяется качественный метод.

При качественном подходе не используются количественные или денежные выражения для объекта оценки. Вместо этого объекту оценки присваивается показатель, проранжированный по трехбалльной (низкий, средний, высокий), пятибалльной или десятибалльной шкале (0… 10). Для сбора данных при качественной оценке рисков применяются опросы целевых групп, интервьюирование, анкетирование, личные встречи.

Анализ рисков информационной безопасности качественным методом должен проводиться с привлечением сотрудников, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

### Как провести качественную оценку рисков:

1. Определить ценность информационных активов.

Ценность актива можно определить по уровню критичности (последствиям) при нарушении характеристик безопасности (конфиденциальность, целостность, доступность) информационного актива.

2. Определить вероятность реализации угрозы по отношению к информационному активу.

Для оценки вероятности реализации угрозы может использоваться трехуровневая качественная шкала (низкая, средняя, высокая).

3. Определить уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты.

Для оценки уровня возможности реализации угрозы также может использоваться трехуровневая качественная шкала (низкая, средняя, высокая). Значение возможности реализации угрозы показывает, насколько выполнимо успешное осуществление угрозы.

4. Сделать вывод об уровне риска на основании ценности информационного актива, вероятности реализации угрозы, возможности реализации угрозы.

Для определения уровня риска можно использовать пятибалльную или десятибалльную шкалу. При определении уровня риска можно использовать эталонные таблицы, дающие понимание, какие комбинации показателей (ценность, вероятность, возможность) к какому уровню риска приводят.

5. Провести анализ полученных данных по каждой угрозе и полученному для нее уровню риска.

Часто группа анализа рисков оперирует понятием «приемлемый уровень риска». Это уровень риска, который компания готова принять (если угроза обладает уровнем риска меньшим или равным приемлемому, то она не считается актуальной). Глобальная задача при качественной оценке — снизить риски до приемлемого уровня.

6. Разработать меры безопасности, контрмеры и действия по каждой актуальной угрозе для снижения уровня риска.

## **ИТОГ: Какой метод выбрать?**

Целью обоих методов является понимание реальных рисков ИБ компании, определение перечня актуальных угроз, а также выбор эффективных контрмер и средств защиты. Каждый метод оценки рисков имеет свои преимущества и недостатки.

Количественный метод дает наглядное представление в деньгах по объектам оценки (ущербу, затратам), однако он более трудоемок и в некоторых случаях неприменим.

Качественный метод позволяет выполнить оценку рисков быстрее, однако оценки и результаты носят более субъективный характер и не дают наглядного понимания ущерба, затрат и выгод от внедрения СЗИ.

Выбор метода следует делать исходя из специфики конкретной компании и задач, поставленных перед специалистом.