УДК 004.492.2

АНАЛИЗ МЕТОДОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Супонина А.О., студент; Штанько Е.И., студент; Губенко Н.Е., к.т.н., доц.
(Донецкий национальный технический университет, г. Донецк, Украина)

Учет информационных рисков является основополагающим этапом при построении системы защиты любой организации, что делает тему данной статьи актуальной сегодня и в будущем. К примеру, в результате недоработки функционирования системы безопасности банка, риск возможного возникновения финансовых потерь увеличивается во много раз.

Чтобы раскрыть тему данной статьи необходимо решить задачи связанные с определением существующих рисков, проведением сравнительного анализа качественных и количественных методов управления информационными рисками, определением их преимуществ и недостатков.

Под риском реализации угрозы информационной безопасности предприятия понимается вероятность свершения события, ведущего к нарушению режима его функционирования и экономическому ущербу. С оценкой степени риска связывается получение вероятностной оценки экономического ущерба, который может понести защищаемое предприятие в случае реализации информационной угрозы его безопасности.

Для определения способа оценки рисков следует выявить, какие риски существуют на данный момент времени. Это поможет в дальнейшем избежать неблагоприятных действий злоумышленников и сократить вероятность этого события.

В зависимости от сферы возникновения источников угроз в банке существуют следующие типы рисков: внутренние, внешние и комбинированные источники угроз информационным активам банка.

1. К внутренним рискам относят технологический риск, включая бухгалтерский риск, риск неэффективности системы контроля внутренних процессов и процедур; а также риск, связанный с использованием информационных технологий, нежелательным состоянием автоматизированных систем банка (риск ошибок программ обеспечения); риск персонала, связанный с некомпетентностью, недостаточной квалификацией, превышением полномочий.
2. Внешний риск связан с противоправными действиями извне (несанкционированное проникновение в электронные системы банка).
3. Из-за несоответствия законодательным актам внутренних нормативных документов банка возникает правовой риск или комбинированный риск[1].

Существует два основных способа оценки информационных рисков: качественные и количественные. Качественная оценка рисков - процесс представления качественного анализа идентификации рисков и определения рисков, требующих быстрого реагирования. То есть это оценка условий возникновения рисков, таких как угрозы (субъект атаки на систему), уязвимости (обстоятельства, которые ослабляют систему перед атаками) и защитные мероприятия (системы, люди). Чаще всего используется основанные на субъективной оценке ожидаемых параметров деятельности. Его основная задача состоит в определении факторов

риска, выявлении направлений деятельности и этапов, на которых может возникнуть риск. Качественный анализ является наиболее сложным этапом в проведении общего анализа степени риска. Таким образом, на протяжении качественного анализа устанавливаются потенциальные области риска и после этого определяются все возможные риски. А так же, качественный анализ предполагает описание возможного ущерба, его стоимостной оценки и мер по снижению или предотвращению риска

Но качественный метод расчета рисков является более субъективным, то есть он позволяет рассмотреть все возможные рисковые ситуации и описать все многообразие рисков, но получаемые при этом результаты оценки часто обладают не очень высокой объективностью и точностью.

Качественный подход, не позволяющий определить численную величину риска инвестиционного проекта, является основой для проведения дальнейших исследований с помощью количественных методов, широко использующих математический аппарат теории вероятностей, математической статистики, теории исследования операций.

Формула, которая используется при расчете рисков, представлена в виде произведения трех параметров: стоимость ресурса, мера устойчивости ресурса к угрозе, оценка вероятности реализации угроз.

$$ALE = AV * EF * ARO \quad (1)$$

Величина AV- стоимость ресурса, характеризующая его стоимость, часто ранжируется в диапазоне от 1 до 3, где 1 – это минимальная стоимость ресурса, 2 – средняя стоимость ресурса, 3 – максимальная стоимость ресурса. По отношению к банку, его автоматизированная система, к примеру, имеет AV=3, а отдельный информационный киоск, предназначенный для обслуживания клиента – AV=1.

Параметр EF- мера устойчивости ресурса к угроз. На сколько вероятна реализация определенной угрозы за определенный период времени показывает оценка угрозы ARO. Эти два параметра так же как и первый ранжируются от 1 до 3, от низкой до высокой соответственно[2]. Для расчета итоговых ожидаемых потерь от угрозы ALE используем формулу (1).

Рассмотрим количественный метод, который позволит нам посчитать меру риска. С помощью этого метода можно с заданной точностью сказать о необходимых средствах и мерах защиты, а также о степени экономии денежных средств при их внедрении. Количественный учет угроз, исходящих из различных источников, производят применительно к потенциальным каналам несанкционированного распространения конфиденциальной информации, каждый из которых понимается как вариант несанкционированного доступа к ней. Поэтому целесообразность организации защиты конфиденциальной информации будет определяется размерами потенциального ущерба, причиняемому предприятию утечкой (разглашением, утратой) конфиденциальной информации по каналам несанкционированного доступа.

$$I = k * L \quad (2)$$

где k – коэффициент, учитывающий допустимую величину затрат на организацию защиты конфиденциальной информации в долях от величины потенциального ущерба или упущенной выгоды (от 0,05 до 0,2).

I это затраты на организацию защиты конфиденциальной информации

Потенциального ущерб, упущенная выгода предприятия от использования конфиденциальной информацией L. Но если невозможно определить параметр L, его заменяют на пропорциональную величину прибыли.

Цель анализа риска состоит в выборе такой политики предприятия, которая позволит ему построить и реализовать оптимальный вариант собственной службы безопасности[3].

Сравнение подходов, их плюсов и минусов многократно приводилось ранее, но при этом, как правило, упускался тот факт, что при сравнении подходов наглядность, простота использования, удобство - это важные, но второстепенные критерии. Учитывая, что назначением анализа рисков является обоснование выделения финансовых средств на меры по обработке рисков, основным критерием должна быть степень полезности результатов для обоснования таких вложений.

Таким образом, с одной стороны, качественные методы просты для понимания и использования, с другой - качественные методы не позволяют дать конкретную оценку, насколько выгодно применение комплекса контрмер и выгодно ли вообще. Действительно, разница в ущербе, например, между высоким и средним уровнем риска не очевидна. Если существует ряд внешних угроз с высоким уровнем возможного ущерба, то качественный анализ не дает обоснованного ответа на вопрос. Несмотря на распространенность качественных методов и построенных на них систем, таких как OCTAVE, RiskPAC , RA2, PRo Audit Advisor и им подобных, они фактически не дают ответа на вопрос как и насколько можно снизить затраты.

Перечень ссылок

1.«Народ» Электронный ресурс. Режим доступа к статье: http://sedok.narod.ru/inv_risk_calc.html - Оценка информационного риска проекта. Бессонов Д.А.

2.«Амулет» Электронный ресурс. Режим доступа к статье: http:www/amulet-group.ru/page.html?id=30 –Страхование информационных рисков как метод защиты информации. Д.Дьяконов.

3.«Сит форум» Электронный ресурс. Режим доступа к статье: http:www/citforum.u/security/articles/risk – Методики и технологии управления информационными рисками. С. Петренко, С. Симонов.