ПРОБЛЕМА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Белова Т.А.
Оренбургский государственный университет

В условиях развития информационных технологий одним из важнейших приоритетов предприятия является информационная безопасность, поскольку последствия и возможный ущерб из-за нарушения безопасности информационной системы могут привести к высоким убыткам организации.

На сегодняшний день не существует единой количественной методики расчета величин рисков, измеряемой в стоимостной оценке. В первую очередь это связано с отсутствием необходимого объема статистических данных о вероятности возникновения угрозы. Вторая причина заключается в том, что современные методики основаны на опыте иностранных компаний и поэтому в российских реалиях их применение сопряжено с определенными трудностями. Поэтому более часто используются качественные или смешанные методики оценки рисков.

Еще одной проблемой является децентрализация процесса оценки рисков. В следствие этого исключается возможность реализации единого подхода к управлению рисками в организации.

При рассмотрении оценки рисков информационной безопасности в общем виде следует выделить основные функциональные блоки системы экономической безопасности предприятия, обеспечивающие максимальное соответствие менеджмента предприятия и его ресурсного потенциала:

– имущество (активы) предприятия;
– финансы предприятия;
– кадры предприятия;
– технологии и инновации;
– информационная система предприятия;
– организационная структура предприятия.

Данная структура функциональных составляющих соответствует структуре механизма обеспечения экономической безопасности предприятия и затрагивает все функциональные области деятельности предприятия.

Информационная система предприятия, как правило, охватывает все сферы его деятельности: административную, производственную, финансовую, выступает как связующее звено при выработке стратегии бизнеса и качества управления предприятием и персоналом. Однако, из-за сложности оценки зачастую не рассматриваются такие типы объектов защиты как сервисы, нематериальные ресурсы, люди, их квалификация, навыки и опыт.

Рассматривая информационную систему в ее исходном состоянии, мы оцениваем размер ожидаемых потерь от инцидентов, связанных с информационной безопасностью. После этого, делается оценка того, как предлагаемые

средства и меры обеспечения безопасности влияют на снижение рисков, и сколько они стоят. Если представить некоторую идеальную ситуацию, то идею подхода отображает приведенный ниже график (рисунок 1).

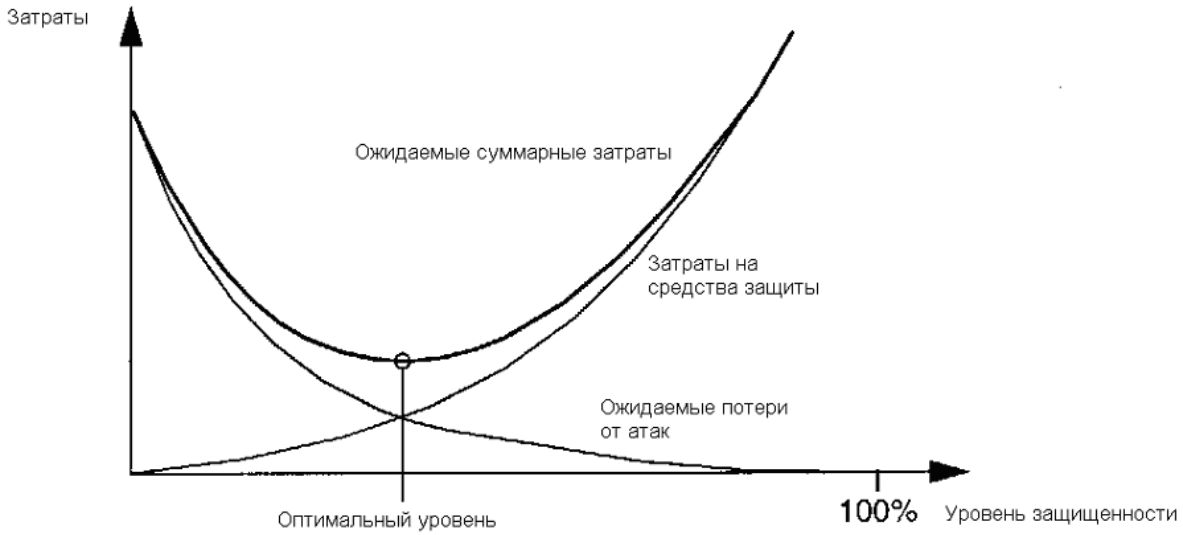

Рисунок 1 – Идеализированный график соотношения
«затраты на защиту/ожидаемые потери»

По мере того, как затраты на защиту растут, размер ожидаемых потерь падает. Если обе функции имеют вид, представленный на рисунке, то можно определить минимум функции «Ожидаемые суммарные результаты», который нам и требуется.

К сожалению, на практике точные зависимости между затратами и уровнем защищенности определить не представляется возможным, поэтому аналитический метод определения минимальных затрат в представленном виде неприменим.

На современном этапе существуют специальные методики и системы анализа рисков, но они не позволяют провести комплексный анализ, решая лишь частные задачи. Среди распространенных методик принята классификация:

– методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»). К таким методикам, в частности, относится FRAP;

– количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;

– методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.).

Проведем сравнительный анализ некоторых методик.

Среди преимуществ методики FRAP можно выделить более подробное раскрытие путей получения данных о системе и ее уязвимостях. Однако, при проведении анализа, как правило, принимают, что изначально в системе отсутствуют средства и механизмы защиты. Таким образом оценивается уровень риска для незащищенной ИС.

Оценка RiskWatch имеет сравнительно небольшую трудоемкость работ по анализу рисков с использованием этого метода. Существенным достоинством RiskWatch является интуитивно понятный интерфейс и большая гибкость метода, обеспечиваемая возможностью введения новых категорий, описаний, вопросов и т. д. Он подходит, если требуется провести анализ рисков на программно-техническом уровне защиты без учета организационных и административных факторов.

В отличие от других методик анализа рисков, ГРИФ предлагает все способы снижения рисков (обход, снижение и принятие). Данная методика учитывает сопроводительную документацию, такую как описание бизнес-процессов или отчетов по проведенным оценкам рисков ИБ.

Положительной стороной CORAS является то, что программный продукт, реализующий эту методику, распространяется бесплатно и не требует значительных ресурсов для установки и применения. Однако, CORAS не предусматривает такой эффективной меры по управлению рисками, как «Программа повышения информированности сотрудников в области информационной безопасности».

Ключевыми показателями при оценке MSAT являются: профиль риска для бизнеса (величина изменения риска в зависимости от бизнес-среды, действительно, важный параметр, который не всегда учитывается при оценки уровня защищенности системы в организациях разных сфер деятельности) и индекс эшелонированной защиты (сводная величина уровня защищенности). MSAT не дает количественной оценки уровня рисков, однако, качественные оценки могут быть привязаны к ранговой шкале. MSAT позволяет оценить эффективность инвестиций, вложенных во внедрение мер безопасности, но не дает возможности найти оптимальный баланс между мерами, направленными на предотвращение, выявление, исправление или восстановление информационных активов.

Методика COBRA позволяет выполнить в автоматизированном режиме простейший вариант оценивания информационных рисков любой компании. Представляет требования стандарта ISO 17799 в виде тематических вопросников, на которые следует ответить в ходе оценки рисков информационных активов и электронных бизнес-транзакций компании. Далее введенные ответы автоматически обрабатываются, и с помощью соответствующих правил логического вывода формируется итоговый отчет с текущими оценками информационных рисков компании и рекомендациями по их управлению. Данная методика является качественной и поэтому дать интерпретацию полученных результатов не всегда возможно.

Особенность методики OCTAVE заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная группа, включающая как технических специалистов, так и руководителей разного уровня, что позволяет всесторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры.

Компания MethodWare разработала свою собственную методику оценки и управления рисками и выпустила ряд соответствующих инструментальных средств. Risk Advisor, являющийся одним из ПО данной компании, позиционируется как инструментарий аналитика или менеджера в области информационной безопасности. Данная методика позволяет автоматизировать различные аспекты управления рисками компании. При этом оценки рисков даются в качественных шкалах. Подробный анализ факторов рисков не предусмотрен. Сильной стороной рассмотренной методики является возможность описания различных связей, адекватный учет многих факторов риска и существенно меньшая трудоемкость.

Таким образом, система оценки рисков информационной безопасности предприятия должна полно и всесторонне охватывать современные требования к осуществлению анализа рисков.

Методика, разрабатываемая нами, будет централизованно оценивать величину риска при изначально любом уровне защищенности информационной системы. Система будет давать количественную оценку уровня рисков и оптимальный баланс между затратами на защиту и ожидаемыми потерями. Кроме того, она всесторонне будет анализировать факторы рисков. Это особенно важно в тех случаях, когда к информационной системе компании предъявляются повышенные требования в области защиты информации и непрерывности бизнеса.

Список литературы

1 Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Е. К. Баранова, А. В. Бабаш – Москва: ИНФРА-М: РИОР – 2017. – 322 с.

2 Плетнев, П. В. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса / П. В. Плетнев, В. М. Белов // Доклады ТУСУРа – 2012. – №1 – С. 83-86.

3 Семкина, А. А. Оценка уровня информационной безопасности предприятия через остаточный риск / А. А. Семкина, А. М. Цыбулин // Вестник ВолГУ – 2012. – №6 – С. 156-158.

4 Кузнецова, О. Б. Оценка информационных рисков в обеспечении экономической безопасности предприятия / О. Б. Кузнецова // Труды ИСА РАН – 2007. – Т. 31 – С. 31-98.

5 Баранова, Е. Анализ рисков информационной безопасности для малого и среднего бизнеса / Е. Баранова, А. Мальцева // Директор по безопасности – 2015. – С. 58-63.