УДК 330.322.4

МЕТОДИЧЕСКИЕ ПОДХОДЫ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ ИНВЕСТИЦИЙ В ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПАНИИ

А.А. Обухов
соискатель ФГНУ «Институт экономики и организации промышленного производства» СО РАН (Новосибирск)
Е.А. Обухова
аспирант ФГНУ «Институт экономики и организации промышленного производства» СО РАН

Рассмотрены существующие подходы к оценке эффективности инвестирования в обеспечение безопасности компании, предложен кластерный подход к определению степени угроз безопасности.

Ключевые слова: безопасность компании, эффективность инвестиций, бизнес-безопасность.

Основными факторами производства и ключевыми преимуществами в современном бизнесе являются не столько труд и капитал, сколько технологии и информация. Особенно если речь идет об инновационном подходе в предпринимательстве. С учетом принятого в России курса на построение инновационной экономики, развитие наукоемких производств и государственную поддержку создания инновационной инфраструктуры можно полагать, что в ближайшие 10–15 лет высокотехнологичные компании станут ключевыми элементами и своеобразными «точками роста» национальной экономики. В этой связи доступ к уникальным информационным ресурсам, технологиям, базирующимся на передовых научных разработках, видится важнейшим условием коммерческого успеха. Соответственно, актуализируется вопрос защиты информации и обеспечения режима сохранения коммерческой тайны в отношении ключевой бизнес-информации. Таким образом, актуальность проблемы экономической безопасности, в том числе в информационном ее аспекте, можно рассматривать в качестве одной из особенностей современной экономической парадигмы [1, с. 130].

Подходы к обеспечению безопасности на микроуровне и макроуровне существенно разнятся. Основную роль в обеспечении экономической безопасности на государственном уровне играют в первую очередь федеральные органы исполнительной власти (правоохранительные, регулирующие, надзорные и др.), а также общественные организации. Экономическую безопасность на макроуровне обеспечивают благоприятная институциональная среда и отлаженные механизмы функционирования государственных структур.

На микроуровне, то есть для отдельно взятого субъекта хозяйствования, наиболее важным фактором обеспечения экономической безопасности служит система защиты жизненно важных интересов, построенная руководством компании. Функции государства ограничиваются созданием правового поля и обеспечением его эффективного функционирования, так что рассмотрение данного аспекта входит скорее в компетенцию специалистов в области юриспруденции, нежели экономики.

Как и любой вид деятельности компании, обеспечение экономической безопасности в целом и защиты информации в частности предполагает необходимость финансовых вложений. Заработная плата персонала, отвечающего за защиту коммерческой тайны, проведение тренингов с сотрудниками, приобретение технических средств защиты информации и соответствующего программного обеспечения, проведение периодического аудита системы безопасности – таковы основные статьи расходов на обеспечение защиты информации. При этом требуются как стартовые инвестиции (можно считать их вложениями в основные средства), так и постоянные вложения в поддержание функционирования системы безопасности (их можно считать оборотными средствами).

Эффективность инвестиций в соответствии с маржинальным подходом обычно характеризуется положительной отдачей на единицу вложенных средств. Предполагается, что инвестиции влекут некие положительные изменения в деятельности компании (рост спроса, снижение затрат на что-либо, увеличение скорости выпуска продукции и т.д.), которые могут быть выражены в денежных единицах, что позволит оценить степень целесообразности инвестирования с учетом инфляции и иных внешних факторов [2, с. 74].

К сожалению, данная модель не может быть применена к инвестициям в безопасность, поскольку главный их результат – не положительные изменения, а отсутствие отрицательных или предотвращение потерь. То есть позитивным результатом является отсутствие видимых негативных последствий, а наиболее естественным способом оценки результатов инвестиций в обеспечение безопасности может служить количественная оценка предотвращенных потерь и сопоставление их с понесенными затратами. Но реальную оценку таких потерь, обладающую свойством достоверности, произвести затруднительно ввиду отсутствия для этого необходимых данных, поэтому прибегают к вычислению их ожидаемой величины с учетом заданных экспертным путем вероятностей того или иного события.

Данный подход имеет ряд существенных недостатков, главный из которых – его низкая объективность, связанная с оценками вероятности наступления тех или иных негативных последствий. Кроме того, сложно оценить скрытые потери от утраты информации, связанные,

например, с переходом клиентов к конкурентам или иными слабо поддающимися точному прогнозированию факторами. Следовательно, описанный метод оценки эффективности инвестиций, по-видимому, не отвечает критерию объективности, что ограничивает его применимость для принятия управленческих решений.

В качестве возможной альтернативы в специальной литературе предлагается метод оценки свойств системы безопасности (Security Attribute Evaluation Method, SAEM), разработанный в Carnegie Melon University. Основой указанного метода служит подход, связанный с сопоставлением архитектур различных систем безопасности, последующей оценкой потенциальной финансовой выгоды и ожидаемых рисков, возникающих после их внедрения [3, с. 235]. Данная методика широко применяется в IT-сфере при проектировании систем информационной безопасности. Однако в отсутствие четких критериев, позволяющих подсчитать экономический эффект от внедрения той или иной системы, данный подход содержит в себе высокую долю субъективности. При проведении исследований данным методом оценки бывают, как правило, весьма умозрительны и базируются на интуитивных прогнозах экспертов, что не обеспечивает достаточной точности.

Относительно новый и нетрадиционный метод анализа дерева ошибок (Fault Tree Analysis) позволяет выявить внутренние причины нарушений политики безопасности. Содержательную часть методики составляет разработка сглаживающих контрмер, применимых в той или иной ситуации [4, с. 277]. Дерево ошибок – это графическое средство, которое дает возможность представить полную систему возможных нарушений в виде логических отношений «и/или» между компонентами системы. При доступности статистической информации о частоте сбоев в критических компонентах системы дерево ошибок позволяет определить ожидаемую вероятность отказа всей системы. Эффект от внедрения мер обеспечения безопасности может быть определен на основании сравнения структуры «двух деревьев»: с использованием защитных мер и в их отсутствие [4, с. 281].

Эта методика отличается наглядностью, относительной простотой в использовании и комплексностью. Вместе с тем, полученные с ее помощью разрозненные данные плохо поддаются обобщению, а вопрос о вероятности отказа каждого конкретного узла системы также остается открытым.

Таким образом, подходы, применяемые при анализе методов оценки уровня безопасности компании и эффективности инвестиций, имеют серьезные недостатки, например:

– широкое применение экспертных оценок вероятностей, коэффициентов и ряда других используемых в расчетах показателей снижает достоверность производимых вычислений;

– наличие в применяемых моделях большого количества скрытых, неучтенных факторов ухудшает качество проводимого анализа;

– отсутствие системного теоретически обоснованного подхода, относительно универсального и пригодного для применения в условиях дефицита информации.

Альтернативным подходом по сравнению с применением описанных выше моделей, оценивающих эффективность инвестирования в обеспечение безопасности post factum либо прогностически, может служить оценка потребности компании в инвестициях, рассматриваемая в динамике.

Для оценки потребности компании в инвестициях в обеспечение безопасности можно принять в качестве основополагающего критерия оптимальный уровень сложности (и, как следствие, стоимости) системы безопасности в зависимости от оценки уровня угрозы, создаваемой элементами внутренней и внешней среды. Вместе с тем, попытка произвести точную количественную оценку степени угрозы и применять полученное значение для конкретных вычислений представляется нецелесообразной. Высокая зависимость экспертных оценок от субъективных факторов ведет к значительному искажению результатов вычислений объема требуемых инвестиций, что существенно снижает достоверность получаемых оценок.

В качестве возможного решения может быть предложена кластеризация степени угрозы безопасности, то есть выделение нескольких ее уровней. Для большего удобства и наглядности вслед за моделью структуризации степени террористической угрозы, принятой во многих странах, в том числе в Российской Федерации [5], возможно применение для обозначения уровня угрозы различных цветов.

Предлагается в рамках пятиступенчатой модели следующее деление степеней угрозы экономической безопасности:

– зеленый уровень – низкая степень угрозы, то есть ниже среднестатистического, что характеризует обстановку как благоприятную;

– синий уровень – приемлемая степень угрозы, предполагает относительную благоприятность обстановки, ее обыденные рамки;

– желтый уровень – повышенная степень угрозы, наличие значимых угрозообразующих факторов, которые, тем не менее, не могут нанести непоправимого ущерба компании и вероятность их наступления относительно невелика;

– оранжевый уровень – высокая степень угрозы, подразумевает наличие большого количества факторов, способных нанести существенный ущерб деятельности компании;

– красный уровень – критическая степень угрозы, наличие очень большого количества факторов, реализация которых приведет к полному прекращению деятельности компании, ее банкротству, притом вероятность их наступления весьма значима.

Для каждого уровня угрозы можно разработать соответствующий комплекс мер, направленных на недопущение реализации угроз либо на снижение потерь, а также определить связанный с ним объем требуемого финансирования.

Модель позволяет гибко оценивать степень существующей угрозы компании, относительно устойчива к погрешностям первичных измерений, что особенно актуально в случае экспертных оценок, и достаточно наглядна, что облегчает ее практическое применение.

В целях более успешного применения предлагаемой модели требуется структурировать и угрозы безопасности компании. Это обусловлено их значительной неод-

нородностью и сложностью сопоставления разных по типу угроз. Например, достаточно затруднительно соотнести на одной унифицированной шкале угрозу от поданного в отношении компании судебного иска, от демпинга со стороны конкурентов или от проникновения в производственные помещения воров. Логичным представляется разделить угрозы безопасности компании по принципу сфер относимости на:

– экономические (включая, например, недобросовестную конкуренцию, риски резкого изменения макроэкономических показателей и т.д.);

– юридические (такие как угроза судебного иска со стороны контрагента; претензий со стороны антимонопольной службы, подразделений полиции, специализирующихся на раскрытии преступлений экономического характера, и т.д.);

– физические (угроза проникновения на территорию компании недоброжелателя с целью хищения материальных ценностей или повреждения ее имущества);

– информационные (угроза утраты или похищения документов, предметов, составляющих коммерческую тайну либо являющихся их носителями, риски нарушения информационных потоков в компании при несанкционированном доступе к компьютерной информации, повреждения информационных массивов и т.д.).

Безусловно, такая классификация является в значительной мере укрупненной, однако большая детализация типов угроз безопасности может привести к чрезмерному усложнению модели, непрозрачности критериев разделения, что, в свою очередь, приведет к путанице при отнесении той или иной угрозы к одному из выделенных типов.

Предложенный метод кластеризации степени угроз безопасности по уровню интенсивности рисков, предполагающий деление на зоны, которым для наглядности присвоена цветовая кодировка, позволяет значительно сократить количество факторов, необходимых для учета при оценке угрозы безопасности. Кроме того, кластеризация степени угрозы делает возможным сопоставление с ней комплекса противодействующих мероприятий, следовательно, позволяет оптимизировать объем инвестиций на эти цели.

Разумеется, для применения указанного подхода необходима его корректировка с учетом реальной экономической практики.

Литература

1. *Артёмова А.Н.* Формирование системы обеспечения экономической безопасности на корпоративном уровне // Микроэкономика. 2010. № 1. С. 129–136.

2. *Бендиков М.А., Хрусталев Е.Ю.* Наукоемкие производства и экономическая безопасность // ЭКО. 1999. № 8. С. 70–76.

3. *Shawn A.B.* Security attribute evaluation method: A cost-benefit approach // Proceedings of the 24th International Conference on Software Engineering. Pittsburgh, 2002. P. 232–240.

4. *Sanjay K.T., Pandey D., Reena T.* Fuzzy set theoretic approach to fault tree analysis // International Journal of Engineering, Science and Technology. 2010. Vol. 2, № 5. P. 276–283.

5. О Порядке установления уровней террористической опасности, предусматривающих принятие дополнительных мер по обеспечению безопасности личности, общества и государства: Указ Президента Рос. Федерации от 14 июня 2012 г. № 851.