Таким образом, в методике при оценке уровня СОБ рассматриваются следующие группы: работники предприятия, органы государственной власти и местного самоуправления, потребители, бизнес-партнеры (поставщики и кредиторы) и общественность. Для каждой группы предложены соответствующие показатели, отражающие их социальные ожидания. Например, для работников организации анализируются социальная структура коллектива, условия труда и культурно-бытовые условия, оплата и дисциплина труда, социальная инфраструктура. Для органов государственной власти и местного самоуправления – выплата налогов, занятость работоспособного населения, охрана окружающей среды. Уровень СОБ определяется путем сравнения норматива или социального ориентира данного показателя с его фактическим значением. Чем ближе фактический показатель к нормативу, тем выше степень социальной ответственности в данной группе.

Результаты, полученные в ходе применения предлагаемой методики, позволяют оценить тенденцию изменения того или иного параметра, своевременно отреагировать на исправление ситуации, скорректировать стратегию развития компании, что в конечном итоге приведет к успешному развитию всего бизнеса в долгосрочной перспективе.

Список литературы

1. *Андреев А. А.* Методика комплексной оценки объемов социального инвестирования // Вестник Челябинского государственного университета. – 2009. – № 9(147). – С. 73–78.

2. *Кашин В.*, *Нещадин А.* Методика оценки эффективности корпоративной социальной политики (социальных инвестиций и социального партнерства) // Человек и труд. – 2009. – № 5.

2. *Захаров Н. Л.*, *Кузнецов А. Л.* Управление социальным развитием организации : учебник. – М. : ИНФРА-М, 2009. – 263 с.

3. *Полищук Л. И.* Корпоративная социальная ответственность или государственное регулирование: институциональный анализ с приложением к России. – М. : Изд. дом ГУ ВШЭ, 2009. – № 01. – 24 с.

4. *Гринберг Т. В.*, *Лещинская К. Л.* Экономическая политика России – XXI век. – URL: www.csrjournal.com

5. *Fridman M.*, *Fridman R.* Free to Choose: A Personal Statement. – 1980.

6. *Packard D.* The HP way: How Bill Hewlett and I built our company. – Collins, 1996. – 224 p.

G. A. Lobanova, Candidate of Economic Sciences, Associate Professor, Izhevsk State Technical University
A. A. Kolesnikova, Post-Graduate Student, Izhevsk State Technical University

Development of Complex Estimation of Business Social Responsibility Level

The concept of business social responsibility, the basic interested groups and their social expectations are considered. The technique of estimation of business social responsibility taking into account the given approach is offered.

Key words: social responsibility of business, complex estimation of social responsibility level, interested groups.

УДК 336.645.1

В. П. Первадчук, доктор технических наук, профессор, Пермский государственный технический университет
В. А. Белецкий, аспирант, Пермский государственный технический университет

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНВЕСТИРОВАНИЯ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ НА ОСНОВЕ НЕЧЕТКИХ МНОЖЕСТВ

Рассмотрен количественный подход оценки эффективности инвестирования в информационную безопасность. Неопределенность, связанная с подобным инвестированием, моделируется с помощью нечетких множеств.

Ключевые слова: информационная безопасность, нечеткие множества, инвестиции.

Защита информации – это сложная и затратная задача. Помимо высоких инвестиций, необходимо решить противоречие между доступностью информационных ресурсов, то есть их удобством – одним из основных преимуществ информатизации – и необходимой степенью защиты. Так как защитные меры приводят к снижению удобства использования информационных ресурсов и несут неявную и зачастую плохо вычисленную выгоду, решения в пользу безопасности принимаются лишь в том случае, если сторонник защиты информации пользуется личным уважением у руководства. Такие отношения восходят к прошлому, когда оракул предсказывал будущее, основываясь на собственной мудрости. Сегодня требуется количественная оценка рисков и преимуществ, основанная на рациональных математических моделях.

Получено 16.08.10

Если организация взвешивает целесообразность реализации того или иного проекта, то в простейшем случае она может рассчитать чистую приведенную стоимость *NPV* прибыли и затрат, которые принесет проект, и сравнить их [1]. Другими словами, прибыль от инвестиций должна превосходить затраты, а уровень доходности компания устанавливает самостоятельно.

$$ROI = NPV_i - NPV_c.$$

Точно такой же базовый подход может быть применен и для расчета целесообразности инвестиций в информационную безопасность. Основное отличие при оценке инвестиций в средства безопасности заключается в том, что они никогда не приносят прибыль (возможно, косвенно), а лишь предотвращают гипотетические затраты. Таким образом, любые средства защиты должны предотвратить затраты на бóльшую сумму, чем средства, затраченные на их внедрение, что и будет говорить о рентабельности инвестиций в средства защиты (*ROSI*).

$$ROSI = NPV_u - NPV_m, \qquad (1)$$

где NPV_u – затраты на устранение компрометации безопасности без внедренных средств защиты; NPV_m – затраты на устранение компрометации безопасности с внедренными средствами защиты.

При этом чистая приведенная стоимость (*NPV*) будет рассчитываться следующим образом:

$$NPV_u = \sum_{i=1}^{N} \frac{ALE_i}{(1+r_i)^i}; \quad NPV_m = I_0 + \sum_{i=1}^{N} \frac{ALE_i}{(1+r_i)^i},$$

где N – число интервалов инвестирования; ALE_i – ожидаемые потери в *i*-м периоде; r_i – ставка дисконтирования, выбранная для *i*-го периода; I_0 – стоимость средств защиты.

Также можно учитывать ликвидационную стоимость средств защиты (*C*), приобретенных в процессе инвестирования.

$$NPV_m = I_0 + \sum_{i=1}^{N} \frac{ALE_i}{(1+r_i)^i} - \frac{C}{(1+r_{N+1})^{N+1}}.$$

Так как затраты при расчете гипотетические, то мы применяем методику расчета *Annual loss expectancy – ALE*, то есть ожидаемые потери в каждый период оценки [2]. Также эта методика позволяет преодолеть такой недостаток *NPV*, как отсутствие учета рисков – в дальнейшем мы их учтем и смоделируем неопределенность с помощью нечетких множеств.

В этой методике риски вычисляются оценкой вероятности реализации предполагаемого события и взвешиванием последствий такого хода событий. Таким образом, риск определяется как множество упорядоченных пар последствий (*O*) и вероятностей их реализации (*L*).

$$Risk \equiv \{(L_1, O_1), \ldots, (L_i, O_i), \ldots, (L_n, O_n)\}.$$

К сожалению, эта модель не позволяет различить часто реализующиеся события с последствием малой стоимости и редкие события с последствиями высокой стоимости.

$$ALE = \sum_{i=1}^{n} I(O_i) F_i,$$

где $\{O\}$ – множество угроз; $I(O)$ – стоимостные последствия реализации угрозы; F – частота реализации угрозы; ALE – ожидаемый урон от реализации

Изначально эта модель была не лишена недостатков. Во-первых, предполагалась генерация всевозможных событийных сценариев, для каждого из которых производился расчет *ALE*, а это задача невероятной величины. Модели на основе *ALE* фокусировались на максимально возможной детализации, а не на эффективности описания моделируемого объекта. Второй изъян лежит в бинарном взгляде на безопасность. Полагалось, что все количественные значения могут быть вычислены исключительно точно. Последний существенный недостаток – это зависимость модели от информации, которой явно недостаточно. Модель хороша лишь тогда, когда хорошая информация лежит в ее основе.

Мы предлагаем преодолеть вышеобозначенные недостатки следующим образом: отход от перебора сценариев предлагается осуществить с помощью построения лишь нескольких комплексных решений и последующего их сравнения методом, предложенным в [3, с. 15–23]. Неопределенность мы предлагаем смоделировать с помощью нечетких множеств, как показано у А. О. Недосекина [4].

Отметим, что неопределенность также можно смоделировать с помощью случайных множеств, минимаксного и интервального методов. Предпочтение в данном случае отдается нечетким множествам из-за ограниченности статистики по информационной безопасности и невозможности предвидеть, как отмечалось выше, все сценарии развития событий.

Из (1) видно, что перед нами стоит задача сравнения NPV_u и NPV_m. В случае, если $NPV_u > NPV_m$ – инвестиции эффективны.

В [4] показано, что если *NPV* задана треугольным числом, то эффективность инвестиций

$$V \,\&\, M = \int_0^1 \varphi(\alpha)\, d\alpha = \int_0^{\alpha_1} \varphi(\alpha)\, d\alpha + \int_{\alpha_1}^1 \varphi(\alpha)\, d\alpha, \qquad (2)$$

где

$$\phi(\alpha) = \frac{S_\alpha}{(NPV_{u2} - NPV_{u1}) \times (NPVm_2 - NPVm_1)}.$$

Здесь S_α – площадь фигуры, образованная на пересечении нечетких чисел NPV_u и NPV_m.

ALE будет рассчитано следующим образом [3]:

$$ALE_k = \sum_{i=1}^{n}\left\{F_0(B_i)D_0(B_i)\prod_{j=1}^{m}\left[\left(1-E_f(B_i,S_j)I_k(S_j)\right)\times\right.\right.$$
$$\left.\left.\times\left(1-E_d(B_i,S_j)I_k(S_j)\right)\right]\right\}, \quad (3)$$

где B_i – угрозы, i = 1, n (например, кража информации, уничтожение информации); S_j – средства защиты, j = 1, m; P_k – выбор политики безопасности, k = 0,l; $R(S_j)$ – прибыли, вызванные внедрением S_j; $I(S_j)$ – бинарная функция, отражающая наличие S_j в P_k; $F_0(B_i)$ – начальная оценка частоты реализации B_i; $D_0(B_i)$ – начальная оценка урона от реализации угрозы B_i; $E_f(B_i,S_j)$ – снижение частоты реализации B_i в случае внедрения S_j; $E_d(B_i,S_j)$ – снижение последствий от B_i в случае внедрения S_j; $C(S_j)$ – стоимость внедрения S_j.

Другими словами, мы рассмотрим лишь несколько наборов средств защиты. После этого мы рассчитаем эффективность внедрения каждого из таких наборов по формуле (1).

Итак, нами была построена модель оценки эффективности инвестирования в информационную безопасность. В основе ее лежит сравнение чистой приведенной стоимости затрат на устранение последствий реализации угроз (например, вирусной атаки) при внедренных средствах защиты и без них. Неопределенность моделируется с помощью нечетких множеств и методики *ALE*.

Список литературы

1. *Aubuchon K.* Applying NPV and ROI to Security Investment Decisions. – URL : http://defaultdenyjournal.com/blog/2009/10/30/extended-article-applying-npv-and-roi-to-security-investment-decisions (дата обращения 12.05.10).

2. National Bureau of Standards, Guideline for Automatic Data Processing Risk Analysis, FIPS PUB 65. – Washington, DC : U.S. General Printing Office, 1979.

3. *Hoo S.* How much is enough? A risk management approach to Computer Security. – 2000. – URL : http://www.eecs.harvard.edu/~stuart/papers/thesis.pdf (дата обращения 24.03.10).

3. *Недосекин А. О.* Нечетко-множественный анализ риска фондовых инвестиций. – СПб. : Тип. «Сезам», 2002.

V. P. Pervadchuk, Doctor of Technical Sciences, Professor, Perm State Technical University
V. A. Beletsky, Postgraduate Student, Perm State Technical University

Effectiveness Evaluation of Investment in Information Security Based on Fuzzy Sets

The quantitative approach to investments in information security is considered. The uncertainty is modeled with fuzzy sets.

Key words: information security, fuzzy sets, investments.

УДК 338.2 (045)

Г. А. Лобанова, кандидат экономических наук, доцент, Ижевский государственный технический университет
К. А. Гамбург, магистрант, Ижевский государственный технический университет

АНАЛИЗ УСЛОВИЙ ФОРМИРОВАНИЯ КЛАСТЕРОВ В РОССИИ

На основании анализа отечественной литературы, а также опроса предпринимателей в статье определены условия, необходимые для формирования кластеров в России.

Ключевые слова: кластер, внутренние и внешние условия формирования кластеров в России.

Кластерная политика является одним из главных направлений государственной политики по повышению национальной и региональной конкурентоспособности в экономически развитых странах на протяжении последних 10 лет. К настоящему времени Правительством России кластерная политика начинает рассматриваться как одна из 11 «ключевых инвестиционных инициатив» согласно концепции долгосрочного социально-экономического развития Российской Федерации, утвержденной в 2008 году [1].

Согласно данной концепции предусмотрено формирование кластеров в регионах России (кластер – это группа географически соседствующих взаимосвязанных компаний и связанных с ними организаций, действующих в определенной сфере и характеризующихся общностью деятельности и взаимодополняющих друг друга [2]). Однако следует понимать, что формирование кластеров невозможно без четкого определения условий, необходимых для его создания.

В. П. Третьяк полагает, что ключевым условием формирования кластера является *наличие доста-*

Получено 15.09.10