УДК 336.645.1

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

РАСЧЕТ ЭФФЕКТИВНОСТИ ИНВЕСТИРОВАНИЯ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ НА ОСНОВЕ НЕЧЕТКИХ МНОЖЕСТВ

Приведен расчет оценки эффективности инвестирования в информационную безопасность. Неопределенность, связанная с подобным инвестированием, моделируется с помощью нечетких множеств.

Ключевые слова: информационная безопасность, нечеткие множества, инвестиции.

В статье произведен расчет с помощью модели, предложенной в [1], использованы данные из «Глобальных исследований утечек» компании InfoWatch [2] и данные исследований CSI [3]. К сожалению, ни один из перечисленных выше источников не может считаться статистически репрезентативным, поэтому мы будем иметь дело с квазистатистикой [4]. Тем не менее каждая компания, производящая оценку собственных инвестиций в информационную безопасность, должна вести свою статистику для получения достоверной количественной оценки. Однако экспертные оценки неизбежны. Предложенная модель поможет не только в количественной оценке риска, но и позволит выбрать стратегию инвестирования в средства защиты, то есть в каком-то смысле формализовать экспертные ожидания.

Дадим общую характеристику гипотетической компании. Основываясь на данных CSI [2], наша компания должна быть большой коммерческой организацией с персоналом, насчитывающим более 1500 человек. Ежегодная выручка компании составляет более 100 млн долларов. Компания осуществляет контроль информационной безопасности самостоятельно. Внутренняя сеть защищена межсетевым экраном (файрволом), в компании используется антивирус и виртуальная частная сеть (VPN).

Определим угрозы, а далее дадим им количественную оценку:

- кража информации – несанкционированное копирование или кража физических носителей с конфиденциальной информацией;
- модификация информации – несанкционированное изменение конфиденциальной информации;
- уничтожение информации – несанкционированной уничтожение конфиденциальной информации;
- простой системы – бездействие информационной системы;
- снижение производительности – общее снижение производительности информационной системы.

В табл. 1 дан список возможных средств защиты, призванных снизить частоту реализации описанных выше угроз, а также нечеткая оценка стоимости внедрения в треугольных нечетких числах в долларах.

Таблица 1. **Выбор политики безопасности**

Средство защиты	Оценка стоимости внедрения		
Политика информационной безопасности	20000	40000	60000
Обновление программных и аппаратных средств	10000	35000	60000
Тонкая настройка существующих средств защиты	5000	10000	50000
Отдел информационной безопасности	50000	60000	120000
Регулярное резервное копирование	8000	10000	20000
Шифрование	25000	40000	100000
Централизованная система доступов	100000	120000	1200000
Межсетевые экраны	28000	35000	42000
Блокировка экрана	0	500	1500
Система обнаружения вторжений	50000	100000	200000

Мы примем ликвидационную стоимость приобретенных средств защиты равной нулю. Таблица 2 отражает наш выбор политики безопасности P_k, то есть тот набор средств, который мы решаем внедрять, принимая решение.

Необходима также количественная оценка результатов внедрения данных средств защиты. Если по компании ведется статистика инцидентов безопасности, то необходимо использовать эти данные, в другом случае необходимо применять экспертные оценки. Следующие таблицы созданы с помощью таких экспертных оценок. Таблица 3 отражает снижения в частоте реализации угроз, табл. 4 – снижения в последствиях реализации угроз (в треугольных нечетких числах).

Получено 07.04.11

Таблица 2. **Выбор политики безопасности**

Средство защиты	Статус-кво	Мин. улучшения	Средние улучшения	Макс. улучшения
Политика информационной безопасности	0	1	1	1
Обновление программных и аппаратных средств	0	0	1	1
Тонкая настройка существующих средств защиты	0	0	1	1
Отдел информационной безопасности	0	0	0	1
Регулярное резервное копирование	0	0	1	1
Шифрование	0	1	1	1
Централизованная система доступов	0	0	0	1
Межсетевые экраны	0	0	0	1
Блокировка экрана	0	1	1	1
Система обнаружения вторжений	0	0	0	1

Таблица 3. **Снижение частоты реализации угроз**

Средство защиты	Кража инф.	Модиф. инф.	Уничт. инф.	Простой сист.	Снижение произв.
Политика информационной безоп.	(0,1;0,3;0,4)	(0,01;0,25;0,3)	(0,1;0,25;0,35)	(0;0,1;0,2)	(0;0,1;0,15)
Обновление ПС и АС	(0,25;0,4;0,5)	(0,3;0,4;0,5)	(0,3;0,4;0,5)	(0,3;0,4;0,5)	(0,3;0,4;0,5)
Тонкая настройка существ. средств	(0,35;0,5;0,55)	(0,1;0,3;0,4)	(0,1;0,25, 0,3)	(0;0,1;0,15)	(0,2;0,4;0,45)
Отдел информационной безоп.	(0,2;0,4;0,5)	(0,2;0,4;0,5)	(0,2;0,4;0,5)	(0,2;0,4;0,5)	(0,2;0,4;0,5)
Регулярное резервное копирование	0	0	0	0	0
Шифрование	0	0	0	0	0
Централизованная система доступов	(0,15;0,25;0,3)	(0,3;0,4;0,45)	(0,2;0,4;0,5)	(0;0,1;0,15)	0
Межсетевые экраны	(0,2;0,4;0,6)	(0,2;0,4;0,6)	(0,1;0,4;0,5)	(0,1;0,4;0,6)	(0;0,1;0,2)
Блокировка экрана	(0,05;0,1;0,3)	(0,1;0,25,0,4)	(0,1;0,2;0,3)	0	0
Система обнаружения вторжений	(0,3;0,4;0,5)	(0,3;0,4;0,5)	(0,3;0,4;0,5)	(0,3;0,4;0,5)	(0,3;0,4;0,5)

Таблица 4. **Снижение последствий реализации угроз**

Средство защиты	Кража инф.	Модиф. инф.	Уничт. инф.	Простой сист.	Снижение произв.
Политика информационной безоп.	0	0	0	0	0
Обновление ПС и АС	0	0	0	0	0
Тонкая настройка существ. средств	0	0	0	0	0
Отдел информационной безоп.	(0,05;0,1;0,2)	(0,1;0,25;0,3)	(0,05;0,1;0,2)	0	(0,1;0,3;0,4)
Регулярное резервное копирование	0	(0,4;0,55;0,6)	(0,4;0,9;0,95)	0	0
Шифрование	(0,5;0,7;0,8)	(0,5;0,7;0,8)	0	0	0
Централизованная система доступов	0	0	0	0	0
Межсетевые экраны	0	0	0	0	0
Блокировка экрана	0	0	0	0	0
Система обнаружения вторжений	0	0	0	0	0

Также необходимы количественные оценки вероятности реализации угрозы (табл. 5) и последствий (табл. 6) ее реализации.

Таблица 5. **Вероятность реализации угрозы без внедренных средств защиты**

Угроза	Оценка вероятности
Кража информации	(0,16;0,18;0,21)
Модификация информации	(0,29;0,32;0,38)
Уничтожение информации	(0,25;0,29;0,35)
Простой системы	(0,21;0,28;0,39)
Снижение производительности	(0,42;0,64;0,80)

Таблица 6. **Последствия реализации угроз, тыс. дол**

Угроза	Оценка вероятности
Кража информации	(1;254;4800)
Модификация информации	(1;103;500)
Уничтожение информации	(1;163;1000)
Простой системы	(1;116;1000)
Снижение производительности	(1;345;1000)

Следующие оценки были даны на основании данных CSI с 2004 по 2008 г. [2]. Принято, что:

- кража информации коррелирует с кражей/утерей конфиденциальной информации, проникновением в систему, кражей/утерей данных о клиентах и несанкционированным доступом;
- модификация информации коррелирует с проникновением в систему, несанкционированным доступом и злоупотреблением персонала;
- уничтожение информации коррелирует со злоупотреблением персонала, проникновением в систему, кражей/утерей конфиденциальной информации, кражей/утерей данных о клиентах и несанкционированным доступом;
- простой системы коррелирует с отказом в доступе и DNS-атакой;
- снижение производительности коррелирует с вирусами и ботами.

Теперь необходима оценка затрат в случае каждой из политик P_k (см. табл. 1). Для расчета по методике *ALE* воспользуемся формулой [5]

$$ALE_k = \sum_{i=1}^{n}\left\{F_0\left(B_i\right)D_0\left(B_i\right)\ \times\right.$$

$$\left.\times\prod_{j=1}^{m}\left[\left(1-E_f\left(B_i,S_j\right)I_k\left(S_j\right)\right)\left(1-E_d\left(B_i,S_j\right)I_k\left(S_j\right)\right)\right]\right\}.$$

Получаем:

$$ALE_0 = (1{,}33;\ 379{,}23;\ 2738);$$
$$ALE_1 = (1{,}03;\ 270{,}51;\ 1251{,}89);$$
$$ALE_2 = (0{,}54;\ 92{,}24;\ 343{,}35);$$
$$ALE_3 = (0{,}25;\ 19{,}92;\ 34{,}99).$$

Как и следовало ожидать, с внедрением все большего набора средств защиты уменьшаются регулярные издержки на компенсацию реализованных. Но не следует забывать, что эти цифры не отражают первоначальные инвестиции. Теперь произведем расчет *NPV* по следующей формуле:

$$NPV_{mk} = I_k + \sum_{i=1}^{N}\frac{ALE_i}{\left(1+r_i\right)^i} - \frac{C}{\left(1+r_{N+1}\right)^{N+1}}.$$

Как отмечалось выше, ликвидационная стоимость принята равной нулю. Ставку дисконтирования примем равной уровню инфляции в России в 2009 г.: 8,1 %. Хотя в этом случае расчет был произведен по одному периоду, в некоторых случаях необходим расчет по нескольким периодам, например – в случае рассрочки платежа за средства защиты.

I_k для каждой *k*-й политики будет равен:

$$I_0 = 0;$$
$$I_1 = (45000,\ 81500,\ 160000);$$
$$I_2 = (68000,\ 136500,\ 290000);$$
$$I_3 = (296000,\ 451500,\ 1852000).$$

Рассчитаем *NPV* для каждого *k*:

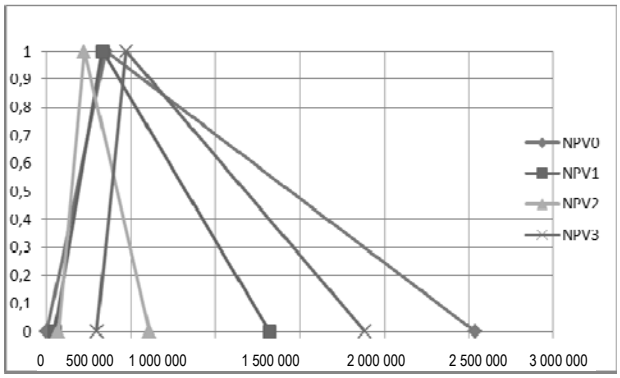
$$NPV_0 = (1231{,}48;\ 351138{,}9;\ 2535185);$$
$$NPV_1 = (45953{,}79;\ 331978{,}8;\ 1319150);$$
$$NPV_2 = (68500{,}86;\ 221911{,}4;\ 607919{,}7);$$
$$NPV_3 = (296229{,}4;\ 469947;\ 1884399).$$

В данном случае можно предположить исходя из графика, что вложения будут оптимальны в случае P_2. Осталось вычислить непосредственно риск инвестиций.

Рассмотрим подробные вычисления для NPV_0 и NPV_1, для сравнения остальных нечетких чисел приведем только результаты. Запишем функции принадлежности:

$$\mu_{NPV_0}(x) = \begin{cases} 0, & x \le 1231{,}48, \\ \dfrac{x-1231{,}48}{349907{,}42}, & 1231{,}48 < x \le 351138{,}9, \\ \dfrac{2535185-x}{2184046{,}1}, & 351138{,}9 < x \le 2535185, \\ 0, & 2535185 < x; \end{cases}$$

$$\mu_{NPV_1}(x) = \begin{cases} 0, & x \le 45953{,}79, \\ \dfrac{x-45953{,}79}{286025{,}01}, & 45953{,}79 < x \le 331978{,}8, \\ \dfrac{1319150-x}{987171{,}2}, & 331978{,}8 < x \le 1319150, \\ 0, & 1319150 < x. \end{cases}$$



NPV

Для данного соотношения нечетких чисел NPV_0 и NPV_1 функция $\varphi(\alpha)$ существует только на трех интервалах: интервале $NPV_{01} < NPV_{11} < NPV_{12} < NPV_{02}$ при $\alpha \in [0;\alpha_0]$, интервале $NPV_{11} < NPV_{01} < NPV_{12} < NPV_{02}$ при $\alpha \in [\alpha_0;\alpha_1]$ и интервале $NPV_{12} < NPV_{01}$ при $\alpha \in [\alpha_1;1]$. Прежде чем применить формулы для расчета степени риска проекта, нам необходимо найти величины α_0 и α_1. Приравняв функции μ_{NPV_0} и μ_{NPV_1} на соответствующих интервалах, получим следующий результат:

$$\alpha_0 = 0{,}7 \text{ при } NPV_0 = NPV_1 = 246191{,}7;$$

$$\alpha_1 = 0{,}986 \text{ при } NPV_0 = NPV_1 = 346124{,}8.$$

На основании этих данных рассчитаем степень риска неэффективности проекта [2]:

$$V\,\&\,M = \int_0^{0{,}986}\varphi(\alpha)d\alpha = \int_0^{0{,}7}\varphi_2(\alpha)d\alpha + \int_{0{,}7}^{0{,}986}\varphi_1(\alpha)d\alpha;$$

$$\int_0^{0{,}7}\varphi_2(\alpha)d\alpha = 0{,}184;\quad \int_{0{,}7}^{0{,}986}\varphi_1(\alpha)d\alpha = 0{,}045;$$

$$V\,\&\,M_1 = 0{,}184 + 0{,}045 = 0{,}229;\quad V\,\&\,M_2 = 0{,}071;$$

$$V\,\&\,M_3 = 0{,}308.$$

Степень риска инвестиций по политике P_1 составит $V\,\&\,M = 0{,}229$. Риск заключается в том, что затраты без вложений будут меньше, чем затраты при инвестировании. Каждый инвестор сам принимает решение о верхней границе приемлемого риска. Теперь рассчитаем $V\,\&\,M$ для оставшихся P_k.

Итак, вложения будут оптимальны в случае P_2, риск неэффективных инвестиций составляет 7 %. Это значит, что после совершения инвестиций по данному сценарию затраты компании будут в 93 % случаях ниже, чем если бы организация осталась в состоянии «как есть».

На основании данных оценок легко принять решение. Если компания готова терпеть риск $V \,\&\, M = 0,229,$ то необходимо предпочесть политику P_1, так как исходные инвестиции в этом случае наименьшие. В том случае, если организация стремиться минимизировать свои риски, то необходимо принять решение в пользу P_2.

Следует отметить, что метод оценки риска неэффективности инвестиций на основе нечетких множеств дает возможность работать также с четко заданным условием эффективности. Для этого случая могут быть использованы все инструменты, которые были представлены на данном примере.

Итак, мы продемонстрировали возможность данного метода при оценке риска инвестирования в информационную безопасность. Как видно из примера, в процессе моделирования возникает большая степень неопределенности, которую компенсируют нечеткие множества. Тем не менее чем больше четких условий будет в постановке задачи, тем точнее будет оценка риска. К сожалению, в случае информационной безопасности четкая постановка задачи зачастую невозможна.

Библиографические ссылки

1. *Первадчук В. П.*, *Белецкий В. А.* Оценка эффективности инвестирования в информационную безопасность предприятия на основе нечетких множеств // Вестник ИжГТУ. – 2011. – № 1(49).

2. http://www.infowatch.ru/analytics.html

3. http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf

4. *Недосекин А. О.* Нечетко-множественный анализ риска фондовых инвестиций. – СПб. : Сезам, 2002.

5. *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).

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

Quantitative Evaluation of Investment Effectiveness in Information Security Based on Fuzzy Sets

Example of investments in information security is considered. The investment uncertainty is modeled with fuzzy sets.

Key words: information security, fuzzy sets, investments.