УДК 338:004.056
ББК 65.290.4-134
Л 96

И.И. Лютова
Доктор экономических наук, профессор кафедры финансов и кредита Национального института бизнеса, г. Москва. Тел.: (499) 374 68 01, e-mail: irina_lyutova@mail.ru

МОДЕЛИРОВАНИЕ УРОВНЯ ПРИЕМЛЕМОГО РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Рецензирована)

Аннотация. Ускоренная динамика развития информатизации общества сопровождается увеличением рисков вследствие уязвимости ресурсов. Рассматривая традиционные подходы к оценке величины риска, мы определили их недостаточность при несоответствующей защите и, как следствие, увеличение финансирования на обеспечение информационной безопасности коммерческого предприятия. Рекомендована итеративная модель процесса управления рисками информационных активов.
Ключевые слова: объем денежных средств; оптимальный уровень инвестиций; ущерб.

I.I. Lyutova
Doctor of Economics, Professor of Finance and Credit Department, National Business Institute, Moscow. Ph.: (499) 374 68 01, e-mail: irina_lyutova@mail.ru

ACCEPTABLE RISK LEVEL MODELING OF INFORMATION SECURITY

Abstract. Fast dynamics of information society development is accompanied by an increase in risk due to the vulnerability of resources. The paper considers the traditional approaches to the risk magnitude estimating. The author determines their deficiency in inadequate protection and, consequently, an increase in funding for the provision of business information security. The paper studies iterative process model of risk management of information assets.
Keywords: amount of money; optimal level of investment; damage.

Развитие информационной инфраструктуры предприятия неизменно влечет за собой неконтролируемый рост числа информационных угроз и уязвимостей информационных ресурсов. В этих условиях анализ и оценка рисков информационной безопасности, являясь на сегодняшний день актуальной задачей, позволяет определить необходимый уровень защиты информации, осуществлять его поддержку, а также выработать рекомендации по совершенствованию системы защиты и минимизации рисков.

Путь эволюции обеспечения информационной безопасности сводился к тому, что топ-менеджмент и руководство отделов ИБ персонально делали выбор в сторону предложенных стандартных наборов защитных мер. Недостатком указанного подхода послужила неизвестность при принятии риска, а именно отсутствие данных о его величине.

Вскоре эксперты пришли к заключению, что само обеспечение ИБ может порождать дополнительные риски. И последующая эволюция модели ИБ свелась к позиции, согласно которой все риски информационной безопасности должны быть согласованы с рисками организации в целом. Так появилась задача интеграции системы управления информационными рисками (СУИР) в систему корпоративного управления всей компанией.

При всех своих достоинствах прагматичные модели ИБ (расчет

совокупной стоимости владения СУИБ, «возврат» инвестиций и пр.) требуют большого объема статистической и прогностической информации и не получили широкого распространения в силу ожесточенной конкуренции в бизнес-среде.

Рассмотренные количественные подходы, будучи общепринятыми и хорошо зарекомендовавшими себя на практике, позволяют нам выяснить, являются ли затраты на информационную безопасность обоснованными с экономической точки зрения. Однако данные подходы не исключают проблему неточности исходных данных, не предоставляют достаточной информации для сравнительного анализа, расстановки приоритетов и для принятия решения в целом.

Остается открытым вопрос оптимальности размера инвестиций в информационную безопасность и определения тех участков системы, повышение затрат на защиту которых наиболее существенно повлияет на снижение риска для системы в целом.

Анализ позволил сформулировать вывод о необходимости формирования методического инструментария для анализа и оценки рисков информационной безопасности применительно к определенной информационной области или сфере деятельности с учетом динамики параметров риска.

У руководства компаний появляется необходимость количественного расчета для финансового обоснования инвестиций в информационную безопасность. Более того, будучи общепринятыми и хорошо зарекомендовавшими себя на практике, количественные подходы позволяют нам выяснить, являются ли затраты на информационную безопасность обоснованными, в частности, с экономической точки зрения.

Если организация настроена на последовательное внедрение количественной оценки величины риска информационной безопасности, следует выбирать способы моделирования, которые бы позволили учесть как исторические данные о потерях и реализациях угроз, так и экспертные знания.

Риск (R) рассматривается подавляющим большинством экспертов как комплексная величина, которая предполагает существование таких факторов, как угрозы, уязвимости и сам ущерб, и выражается формулой:

$$R = \lambda \cdot P_T \cdot P_V(z), \qquad (1)$$

где λ — размер ущерба (потерь) в случае нарушения безопасности информационного актива;

P_T — величина вероятности возникновения угрозы;

$P_V(z)$ — функция, описывающая вероятность реализации угрозы для информационного актива в зависимости от затрат на обеспечение защитных мер;

z — затраты на обеспечение защиты информационного актива в денежном выражении [1].

Размер ущерба, таким образом, зависит исключительно от защищаемой информации. Вероятность возникновения угрозы определяется также как фиксированная величина, которая является заданной первоначально. Что касается вероятности реализации угрозы, то путем вливания инвестиций (z) в информационную безопасность актива ее значение может быть снижено.

Среди мнений как зарубежных, так и отечественных экспертов, отмечается следующая тенденция: с увеличением объема инвестиций в информационную безопасность вероятность реализации угрозы в отношении информационного актива уменьшается по экспоненциальному закону.

Однако, когда речь идет о преднамеренных действиях людей, в частности, о получении несанкционированного доступа к защищаемой информации, оценка вероятностей возникновения и реализации угрозы представляет собой определенную трудность. Злоумышленник будет оценивать свои силы, и его действия в данной ситуации будут напрямую зависеть от существующей системы безопасности. Так, если система плохо защищена, он попытается произвести злонамеренные действия, в противном случае — не решится. Таким образом, инвестиции в информационную безопасность будут

также оказывать влияние и на вероятность возникновения угрозы.

Предположим, что с увеличением объема денежных средств, выделяемых на информационную безопасность, вероятность возникновения угрозы в отношении информационного актива уменьшается согласно экспоненциальному закону.

Тогда функция и график зависимости (рисунок 1) вероятности возникновения угрозы от затрат на информационную безопасность будут иметь вид:

$$P_T(z) = t \cdot e^{-\varphi \cdot z}, \quad (2)$$

$$\begin{cases} \forall t \in [0;1], \\ \forall z \in R, \end{cases}$$

где t — величина вероятности возникновения угрозы;

φ — поправочный коэффициент относительно затрат на ИБ;

z — затраты на обеспечение защиты информационного актива в денежном выражении [2].

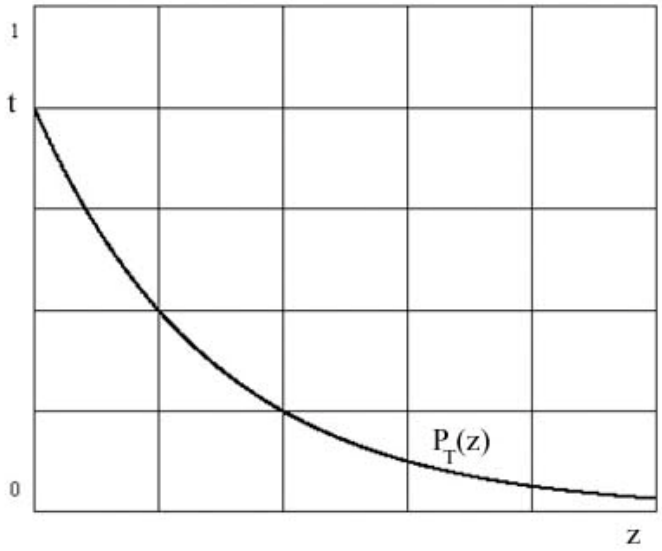

Рисунок 1. Зависимость вероятности возникновения угрозы (P_T) от инвестиций в ИБ (z)

С учетом опыта информационных атак прослеживается четкий тренд — со значительным ростом инвестиций в информационную безопасность актива, имеющего особую ценность для организации, вероятность возникновения угрозы действительно снижается, а вероятность ее реализации увеличивается.

Отсутствие возможности указать нижний предел вероятности реализации угрозы является одним из недостатков известных моделей. В современном мире даже очень значительный объем инвестиций, направленный на обеспечение безопасности, не может снизить вероятность нанесения ущерба до нулевого значения. Примером в данном случае может служить вероятность возникновения, к примеру, какой-либо аварии, катастрофы и т.п.

Определение объема денежных средств, выделяемых на защитные меры, при котором значение функции вероятности реализации угрозы достигает нижней границы β, т.е. точки z_0, представляет собой определенную трудность.

Известная экономическая модель Гордона-Лоеба показывает, что оптимальный уровень инвестиций не превышает $\frac{1}{e} \approx 36{,}8\%$ от общих потерь в случае нарушения безопасности информационного актива. Кроме того, другие авторы дали оценку и экспериментально подтвердили представленные в указанной модели предположения, доказав данный факт эмпирическим путем [3].

С учетом отсутствия статистических данных, и исходя из интуитивных соображений, нам представляется целесообразным увязать значение z_0 с величиной равной, $\frac{1}{e} \approx 36{,}8\%$ от размера ущерба вследствие нарушения ИБ актива.

Таким образом, функция зависимости вероятности реализации угрозы от затрат на информационную безопасность будет иметь следующий вид:

$$P_V(z) = \frac{(\alpha - \beta)}{(\lambda/e)^2} \cdot (z - \lambda/e)^2 + \beta, \quad (4)$$

где λ — размер потерь в случае нарушения безопасности информационного актива.

Необходимо отметить, что в исследовании рассмотрено несколько альтернативных классов функций зависимости вероятности реализации угрозы от затрат на информационную безопасность. Выбор же квадратичной зависимости в работе обусловлен сложностью определения дополнительных параметров (коэффициентов) в альтернативных функциях и их интерпретации для дачи экспертных оценок.

Для нахождения оптимального уровня инвестиций в информационную безопасность необходимо решить задачу минимизации значения общих потерь и затрат при имеющихся ограничениях, что графически показано на рис. 2.

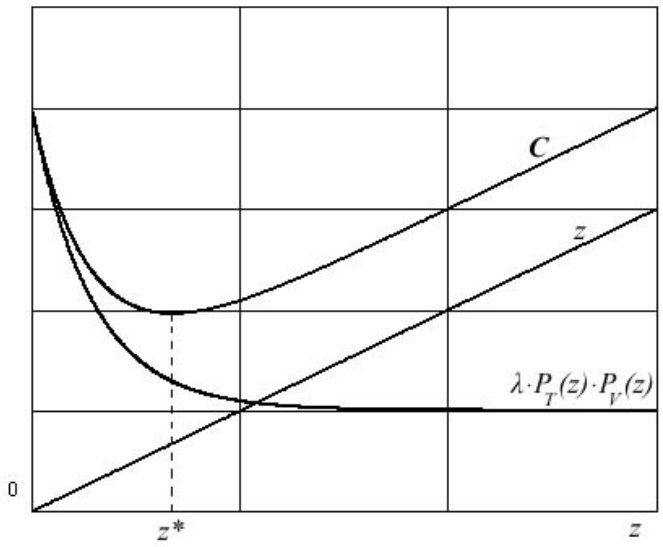

Рисунок 2. Оптимальный уровень инвестиций в ИБ (z*)

Тогда задача нахождения оптимального уровня инвестиций в информационную безопасность будет тогда иметь вид:

$$C = \lambda \cdot P_T(z) \cdot P_V(z) + z = \lambda \cdot t \cdot e^{-\varphi \cdot z} \cdot \left(\frac{(\alpha - \beta)}{(\lambda/e)^2} \cdot (z - \lambda/e)^2 + \beta \right) + z \to \min, \quad (5)$$

при имеющихся ограничениях.

$$\lambda := \begin{pmatrix} 15000000 \\ 6000000 \\ 24000000 \\ 21000000 \\ 23000000 \\ 44000000 \\ 47000000 \\ 53000000 \\ 18000000 \\ 17000000 \\ 20000000 \\ 26000000 \\ 14000000 \\ 16000000 \\ 15000000 \\ 38000000 \\ 5000000 \\ 42000000 \\ 43000000 \\ 36000000 \\ 14000000 \\ 12000000 \\ 30000000 \\ 34000000 \\ 49000000 \\ 8000000 \\ 9000000 \\ 32000000 \\ 28000000 \\ 4000000 \\ 10000000 \end{pmatrix} \quad t := \begin{pmatrix} 0.5 \\ 0.7 \\ 0.75 \\ 0.5 \\ 0.41 \\ 0.3 \\ 0.6 \\ 0.1 \\ 0.28 \\ 0.3 \\ 0.6 \\ 0.7 \\ 0.7 \\ 0.2 \\ 0.25 \\ 0.22 \\ 0.25 \\ 0.1 \\ 0.12 \\ 0.13 \\ 0.15 \\ 0.16 \\ 0.5 \\ 0.3 \\ 0.41 \\ 0.2 \\ 0.25 \\ 0.65 \\ 0.5 \\ 0.18 \\ 0.15 \end{pmatrix} \quad v := \begin{pmatrix} 0.8 & 0.2 \\ 0.9 & 0.3 \\ 0.85 & 0.2 \\ 0.8 & 0.2 \\ 0.5 & 0.2 \\ 0.5 & 0.1 \\ 0.45 & 0.1 \\ 0.35 & 0.1 \\ 0.2 & 0.05 \\ 0.2 & 0.05 \\ 0.9 & 0.2 \\ 0.8 & 0.2 \\ 0.9 & 0.3 \\ 0.6 & 0.1 \\ 0.7 & 0.4 \\ 0.6 & 0.1 \\ 0.5 & 0.1 \\ 0.7 & 0.2 \\ 0.7 & 0.2 \\ 0.6 & 0.2 \\ 0.6 & 0.1 \\ 0.6 & 0.1 \\ 0.8 & 0.4 \\ 0.65 & 0.1 \\ 0.8 & 0.4 \\ 0.63 & 0.1 \\ 0.62 & 0.1 \\ 0.8 & 0.3 \\ 0.9 & 0.2 \\ 0.5 & 0.2 \\ 0.6 & 0.3 \end{pmatrix}$$

$$\phi := 0.000008$$

$$C(z) := \sum_{i=0}^{30} \left[\lambda_i \cdot \left[t_i \cdot e^{\left(-\phi \cdot z_i\right)} \right] \left[\frac{\left(v_{i,0} - v_{i,1}\right)}{\left(\frac{\lambda_i}{e}\right)^2} \left(z_i - \frac{\lambda_i}{e} \right)^2 + v_{i,1} \right] + z_i \right]$$

Given

$i := 0 .. 30$

$b_i := \lambda_i \cdot t_i \cdot v_{i,0}$

$0 \le z \le b$

$$\sum_i z_i \le \sum_i b_i$$

$z' := \text{Minimize}(\tilde{N}, z)$

$$\sum_{i=0}^{30} b_i = 1.851 \times 10^8$$

$$\sum_{i=0}^{30} z'_i = 1.285 \times 10^7$$

$$T'_i := t_i \cdot e^{\left(-\phi \cdot z_i\right)} \quad S'_i := \frac{\left(v_{i,0} - v_{i,1}\right)}{\left(\frac{\lambda_i}{e}\right)^2} \left(z_i - \frac{\lambda_i}{e} \right)^2 + v_{i,1}$$

$$\sum_{i=0}^{30} \left(\lambda_i \cdot T'_i \cdot S'_i \right) = 8.183 \times 10^7$$

Рисунок 3. Фрагмент области рабочего листа «Mathcad»

Задача нахождения оптимального уровня инвестиций в информационную безопасность при известных ограничениях относится к классу задач нелинейного программирования. [4] Для ее решения был использован программный продукт «Mathcad». Фрагмент области рабочего листа программы проиллюстрирован на рисунке 3. Расчет оптимального объема инвестиций в обеспечение информационной безопасности системы ДБО представлен в табл. 1.

Таблица 1

Расчет оптимального объема инвестиций в обеспечение информационной безопасности системы дистанционного банковского обслуживания

Угрозы	*t* (СВВ)	*v* (СВР)		λ, р. (СТП)	Риск (R) ДО, р.	*z**, р.	*PT(z)**	*PV(z)**	Риск (*R*) ПОСЛЕ, р.
A1	0,5	0,8	0,2	15 000 000	6 000 000	471 926	0,22	0,78	2 623 354
A2	0,7	0,9	0,3	6 000 000	3 780 000	404 342	0,31	0,85	1 598 190
A3	0,75	0,85	0,2	24 000 000	15 300 000	590 642	0,34	0,84	6 756 321
A4	0,5	0,8	0,2	21 000 000	8 400 000	516 228	0,22	0,78	3 701 553
A5	0,41	0,5	0,2	23 000 000	4 715 000	448 081	0,18	0,49	2 088 717
A6	0,3	0,5	0,1	44 000 000	6 600 000	491 290	0,13	0,50	2 936 348

Угрозы	t (СВВ)	v (СВР)		λ, р. (СТП)	Риск (R) ДО, р.	z^*, р.	$PT(z)^*$	$PV(z)^*$	Риск (R) ПОСЛЕ, р.
A7	0,6	0,45	0,1	47 000 000	12 690 000	572 224	0,27	0,45	5 650 834
A8	0,1	0,35	0,1	53 000 000	1 855 000	335 302	0,04	0,35	827 414
A9	0,28	0,2	0,05	18 000 000	1 008 000	257 193	0,13	0,20	442 741
A10	0,3	0,2	0,05	17 000 000	1 020 000	258 407	0,13	0,20	447 411
A11	0,6	0,9	0,2	20 000 000	10 800 000	545 846	0,27	0,88	4 750 852
A12	0,7	0,8	0,2	26 000 000	14 560 000	585 422	0,31	0,79	6 440 168
A13	0,7	0,9	0,3	14 000 000	8 820 000	518 981	0,31	0,88	3 861 480
A14	0,2	0,6	0,1	16 000 000	1 920 000	333 978	0,09	0,58	838 491
A15	0,25	0,7	0,4	15 000 000	2 625 000	375 745	0,11	0,69	1 161 333
A16	0,22	0,6	0,1	38 000 000	5 016 000	456 595	0,10	0,59	2 227 059
A17	0,25	0,5	0,1	5 000 000	625 000	193 221	0,11	0,46	257 067
A18	0,1	0,7	0,2	42 000 000	2 940 000	391 698	0,04	0,69	1 308 853
A19	0,12	0,7	0,2	43 000 000	3 612 000	417 212	0,05	0,69	1 608 366
A20	0,13	0,6	0,2	36 000 000	2 808 000	385 755	0,06	0,59	1 249 061
A21	0,15	0,6	0,1	14 000 000	1 260 000	282 366	0,07	0,58	548 011
A22	0,16	0,6	0,1	12 000 000	1 152 000	270 621	0,07	0,58	498 306
A23	0,5	0,8	0,4	30 000 000	12 000 000	565 321	0,22	0,79	5 343 313
A24	0,3	0,65	0,1	34 000 000	6 630 000	490 165	0,13	0,64	2 938 906
A25	0,41	0,8	0,4	49 000 000	16 072 000	603 872	0,18	0,80	7 181 664
A26	0,2	0,63	0,1	8 000 000	1 008 000	251 567	0,09	0,59	427 470
A27	0,25	0,62	0,1	9 000 000	1 395 000	290 719	0,11	0,59	595 537
A28	0,65	0,8	0,3	32 000 000	16 640 000	605 254	0,29	0,79	7 397 780
A29	0,5	0,9	0,2	28 000 000	12 600 000	567 919	0,22	0,89	5 576 462
A30	0,18	0,5	0,2	4 000 000	360 000	131 090	0,08	0,46	149 015
A31	0,15	0,6	0,3	10 000 000	900 000	242 750	0,07	0,58	393 553
					185 111 000	12 851 731			81 825 630

Таким образом, процесс разработки модели управления угрозами можно разделить на следующие этапы:

— идентификация типов информационных активов, входящих в область оценки рисков;

— определение перечня типов объектов среды, соответствующих каждому из типов информационных активов;

— определение источников угроз для каждого из типов объектов среды, определенных в рамках выполнения предыдущего этапа.

Примечание:

1. Королев В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска: учеб. пособие. М.: ФИЗМАТЛИТ, 2011. 620 с.

2. Покровский В.В. Математические методы в бизнесе и менеджменте: учеб. пособие. М.: БИНОМ. Лаборатория знаний, 2012. 111 с.

3. Tanaka H., Matsuura K. Vulnerability and effects of information security investment: A firm level empirical analysis of Japan // Paper presented at forum on financial information systems and cyber security / College Park. Maryland, 2005. May.

4. Экономико-математические методы и прикладные модели: учеб. пособие / В.В. Федосеев [и др.]. М.: ЮНИТИ-ДАНА, 2012. 304 с.

References:

1. Korolev C.Y., Bening C.E., Shorgin S.J. Mathematical Foundations of the theory of risk: textbook. M.: FIZMATLIT, 2011. 620 pp .

2. Pokrovsky V.V. Mathematical methods in business and management: textbook. M.: BINOM. Knowledge laboratory, 2012. 111 pp.

3. Tanaka H., Matsuura K. Vulnerability and effects of information security investment: A firm level empirical analysis of Japan // Paper presented at forum on financial information systems and cyber security / College Park. Maryland. May. 2005.

4. Economic and mathematical methods and applied models: textbook / V.V. Fedoseev [and others]. M.:UNITY-DANA, 2012. 304 pp.