ISSN 2311-8768 (Online)
ISSN 2073-4484 (Print)

Математический анализ и моделирование в экономике

ОЦЕНКА ЭФФЕКТИВНОСТИ ОПТИМАЛЬНОГО ИНВЕСТИРОВАНИЯ В СИСТЕМУ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ*

Вадим Анатольевич БОРХАЛЕНКО

соискатель кафедры прикладной и бизнес-информатики, Московский энергетический институт,
Москва, Российская Федерация
vadikhide@yandex.ru

История статьи:
Принята 28.12.2015
Одобрена 03.02.2016

УДК 330.46+004.56
JEL: C21, C61, G24, G32

Ключевые слова:
инвестиционная деятельность, проектное финансирование, критерии эффективности, информационная безопасность, математические модели

Аннотация

Предмет. Параллельно с растущими темпами информатизации бизнеса и государственных органов бурно развиваются количество и изощренность угроз, направленных на нарушение свойств безопасности информационных ресурсов коммерческих и государственных организаций. Для проведения работ по улучшению работы системы менеджмента информационной безопасности необходимы предварительная оценка и обоснование возможных целевых индикаторов и (или) показателей в отношении мероприятий, связанных с обеспечением требуемого уровня защищенности информационных активов, а также обоснованность привлечения средств для реализации указанных мероприятий и размеры финансовых потребностей, необходимых для реализации этих мероприятий.

Цели. Обоснование и нахождение оптимального объема инвестиций в систему менеджмента информационной безопасности организации, а также предложение показателей эффективности инвестиционных вложений в качестве критериев оценки эффективности мероприятий, связанных с обеспечением требуемого уровня защищенности информационных ресурсов.

Методология. С помощью методов дифференциального исчисления и теории вероятностей проанализированы риски, связанные с информационной безопасностью организации, обусловленными неэффективной работой системы менеджмента информационной безопасности. Определены критерии оценки эффективности инвестиционных вложений в систему менеджмента информационной безопасности, снижающие количественную оценку информационного риска.

Результаты. Предложены методика поиска оптимального объема инвестиций в систему менеджмента информационной безопасности организации и критерии оценки эффективности оптимального инвестирования.

Выводы и значимость. В работе был рассмотрен метод нахождения и обоснования возможных целевых индикаторов и (или) показателей в отношении мероприятий, связанных с улучшением системы менеджмента информационной безопасности, а также обоснованность привлечения средств для реализации этих мероприятий и размеры финансовых потребностей, необходимых для их реализации.

Введение

В настоящее время роль информационных технологий в жизни общества приобретает особую значимость. При этом очевиден переход от подходов, сконцентрированных на рутинной поддержке существующих бизнес-процессов, к стратегическому развитию, созданию новых моделей ведения бизнеса и управленческой деятельности, обеспечивающих высокую эффективность инвестиций в эту сферу. Однако высокие темпы информатизации неминуемо сопровождаются быстрым ростом рисков[1] [1], связанных с появлением новых угроз информационной безопасности, которые являются следствием как действий злоумышленников, так и специфических угроз непосредственно процессам информатизации [2–4]. В современной литературе основное внимание уделяется техническим вопросам обеспечения информационной безопасности, в частности аппаратным и программным средствам защиты информации. Значительно меньше внимания уделяется вопросам, связанным с развитием экономических методов обеспечения информационной безопасности (ИБ). Существует всего несколько работ, преимущественно иностранных авторов, рассматривающих данную проблематику[2] [5–12]. Однако экономические методы обеспечения ИБ не менее важны, нежели технические. Исследование

*Автор выражает благодарность П.Б. Хореву, В.П. Перевалову, Г.К. Перевердиеву за ценные советы и замечания.

[1] *Авдошин С.М., Песоцкая Е.Ю.* Информатизация бизнеса. Управление рисками. М.: ДМК Пресс. 2011. 176 с.; *Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* Управление рисками информационной безопасности. М.: Горячая линия. 2014.130 с.

[2] *Войтик А.И., Прожерин В.И.* Экономика информационной безопасности. СПб.: НИУ ИТМО, 2012. 120 с.

посвящено вопросам использования экономических подходов при решении задач обеспечения высокого уровня эффективности систем информационной безопасности.

Особенности оценки эффективности ИБ-проектов

В России традиционно сложилась практика и методология определения эффективности IT-проектов, когда во главу угла ставится оценка собственно экономической эффективности инвестиций. Существующие методы и методологии оценки экономической эффективности IT-проектов предназначены для обоснования реальности достижения в будущем поставленных целей, контроля за ходом выполнения проекта[3] [15]. Однако перед оценкой эффективности инвестиций в ИБ-проект, который является частным случаем IT-проекта, требуется определить оптимальную сумму инвестиций. Для решения этой задачи в работах [7, 9, 11, 14] были предложены математические модели поиска оптимальной доли инвестиций в информационную безопасность. Стоит заметить, что в качестве объекта инвестирования в этих работах выступал информационный ресурс предприятия. Согласно результатам аудита защищенности информационных систем, проведенного компанией Positive Technologies[4], важнейшей проблемой защищенности ресурса является не его уязвимость, а источник угроз, характеризующихся человеческим фактором[5]:

– халатностью;

– недобросовестным выполнением служебных обязанностей;

– ошибками персонала;

– нарушением персоналом организационных мер по обеспечению ИБ.

По сути менеджмент информационного ресурса и является основной угрозой для информационных активов, хранящихся на нем. Таким образом, встает вопрос о нахождении оптимального объема инвестиций в систему менеджмента информационной безопасности (СМИБ) [14], например, в подготовку, осведомленность и компетентность персонала[6], а также нахождение показателей эффективности инвестиций, хотя бы в первом приближении. Для достижения этой цели автором предложена математическая модель.

Оптимизация объема инвестиций в СМИБ

Рассмотрим функцию, характеризующую вероятность возможной реализации угрозы [7, 9, 12] при заданном объеме инвестиций $S(p, x)$, зависящую от двух параметров: p – начальной вероятности реализации угрозы, x – объема инвестиций, вложенных в снижение вероятности реализации угрозы (в работе [7] эти параметры обозначены как v и z соответственно). В работе [7] Гордоном и Лоубом было сделано несколько предположений о характере поведения этой функции:

а) если информационный ресурс абсолютно неуязвим, то он будет оставаться неуязвимым для любого количества инвестиций x, включая нулевые $\forall x \geq 0 : S(0, x) = 0$;

б) при отсутствии инвестирования в безопасность информационного ресурса вероятность атаки, обусловленной реализацией угрозы, является унаследованной от ресурса уязвимостью p, то есть $\forall p : S(0, x) = p$;

в) также предполагается, что $\forall p \in (0,1) : \lim_{x \to \infty} S(p, x) = 0$. При достаточно большом объеме инвестиций в защиту информационного ресурса вероятность его уязвимости можно сколь угодно приблизить к нулю, то есть $S(p, x)$ – функция бесконечно малая по x:

$$\forall x : \frac{\partial S}{\partial x} < 0, \frac{\partial^2 S}{\partial x^2} > 0; \quad \forall p \in (0,1).$$

Пусть данная функция удовлетворяет условиям *а – в*, а также усилим предположение *в*: $\forall p \in (0,1]$, так как исходное условие *в* предполагает невозможность уменьшения вероятности реализации угрозы на информационный ресурс при начальной вероятности реализации угрозы, равной единице,

[3] *Калачов В.Д., Кобко Л.И.* Экономическая эффективность внедрения информационных технологий. М.: МАИ, 2006. 180 с.

[4] Статистика уязвимостей корпоративных информационных систем в 2014 году. URL: http://www.ptsecurity.ru/download/PT_Corporate_vulnerability_2015_rus.pdf

[5] РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности». URL: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf

[6] *Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* Технические, организационные и кадровые аспекты управления информационной безопасностью. М.: Горячая Линия-Телеком, 2014. 214 с.

что вообще-то противоречит общепринятым представлениям о защите информационного ресурса. Рассмотрим функцию $S(p, x)$ для случая, связанного с недостатками СМИБ. Предположим, что темп изменения вероятности возможной реализации угрозы в зависимости от вложенных инвестиций обратно пропорционален произведению оценки результативности действий персонала и вероятности возможной реализации угрозы:

$$\frac{\partial S}{\partial x} = \alpha S, \quad (1)$$

где α – количественная оценка действия мер и средств контроля и управления[7], определяющаяся эмпирически экспертным путем.

Разрешая данное дифференциальное уравнение (1), получим

$$S(p, x) = C(p) e^{-\alpha x}. \quad (2)$$

Используя условие *б*, $S(p, 0) = p$, находим, что $C(p) = p$ и искомую функцию

$$S(p, x) = e^{-\alpha x}. \quad (3)$$

Предложенная функция удовлетворяет условиям Гордона-Лоуба *а* – *в*, а также удовлетворяет более «мягкому» условию *в* и следовательно *б*: $\forall p \in (0,1]: 0 < S(p, x) \leq 1$.

Для определения оптимального объема инвестиций в СМИБ организация сравнивает ожидаемый доход от инвестиций:

$$EBIS(x) = [p - S(p, x)]L, \quad (4)$$

где L – средняя финансовая оценка ожидаемого ущерба от кибератаки, определенная как средний максимальный ущерб, полученный от нарушения одного из свойств информации (конфиденциальности, целостности, доступности[8], хранящейся на каждом из подверженных данной атаке информационных ресурсов).

Ожидаемая прибыль $Z(x, p)$ в данном случае будет равна:

$$Z(x, p) = [p - S(p, x)]L - x. \quad (5)$$

Оптимальный объем инвестиций, максимизирующий прибыль, находится там, где разница между доходом и издержками максимальна, то есть

$$\frac{\partial z}{\partial x} = 0. \quad (6)$$

Подставляя в уравнение (5) условие (3), получаем: $\alpha p L e^{-\alpha x} = 1$, откуда

$$x = \frac{\ln \alpha L p}{\alpha}, \quad (7)$$

где x – точка максимума, так как $\frac{\partial^2 Z}{\partial x^2} < 0$.

Итак, оптимальный объем инвестиций должен вкладываться не в сам объект защиты, как предполагается в работах [7, 9, 12], а в ликвидацию уязвимостей, связанных с субъектом управления защитой, идентичных для каждого ресурса, который равен $\frac{\ln \alpha L p}{\alpha}$.

Также стоит заметить, что согласно работе [7] вложение инвестиций невыгодно, если выполняется условие

$$L \leq \frac{1}{-\left.\frac{\partial S}{\partial x}\right|_{x=0}} \quad (8)$$

Докажем, что класс функций, предлагаемых автором для инвестирования в менеджмент ИБ, удовлетворяет условиям Гордона – Лоуба о том, что оптимальный объем инвестиций в ИБ не превышает 1/e от изначально ожидаемых потерь.

Продифференцируем выражение (7) по параметру α:

$$\frac{\partial x}{\partial \alpha} = \frac{1 - \ln \alpha L p}{\alpha^2}. \quad (9)$$

Выясним, при каком значении α превращается в 0:

$$\frac{\partial x}{\partial \alpha} = 0 \Rightarrow \ln \alpha L P = 1 \Rightarrow \alpha = \frac{e}{pL}. \quad (10)$$

Определим знак второй производной:

$$\frac{\partial^2 x}{\partial \alpha^2} < 0. \quad (11)$$

Из формулы (11) видно, что e / pL – точка максимума. При $p = 1$ выражение (10) примет вид $\alpha = e / L$.

[7] ГОСТ ИСО/МЭК 27005:2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

[8] Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах». URL: http://fstec.ru/component/attachments/download/812

Положив $p = 1$ и подставив $\alpha = e / L$ в выражение (7), мы доказали, что максимальный объем инвестиций в СМИБ не превышает $\frac{1}{e}L$:

$$x_{\max} \le \frac{1}{e}L \ . \qquad (12)$$

Найдя оптимальный объем инвестиций СМИБ, можно найти показатели эффективности инвестиций в СМИБ, такие, как, например, простая норма прибыли ROI[9]:

$$ROI = \frac{z(x_{opt})}{x_{opt}} \ . \qquad (13)$$

В качестве индикатора может служить оптимальный доход от инвестиций [7], выраженный в снижении величины риска в связи с введением соответствующих мероприятий по улучшению качества менеджмента информационной безопасности:

$$EBIS(x_{opt}) = [p - S(p, x_{opt})]L. \qquad (14)$$

Протестируем теперь полученные результаты на результатах статистики, полученной компанией Positive Technologies за предыдущий год, используя в качестве оценки актива методику, приведенную в РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» (далее – методика РС БР ИББС-2.2-2009), предполагая, что минимальный капитал банка – не менее 300 млн руб[10].

Результаты моделирования

Согласно методике РС БР ИББС-2.2-2009 степень возможной реализации одной или более угрозы на ИС организации, вызванной с помощью уязвимости, обоснованной некомпетентностью менеджмента, несоблюдения правил парольной политики, оставления заводских настроек оборудования, отсутствием своевременного обновления для ПО, хранением чувствительных данных в открытом виде, недостаточной осведомленностью пользователей автоматизированных рабочих мест, в вопросах ИБ очень близка к 1 (0,99999). Так как функция, предлагаемая автором, удовлетворяет условию $0 < S(p, x) \le 1$, то примем для удобства вычислений $S(0, p) = 1$, тогда средние потери от реализации атак, связанных с этой уязвимостью, могут быть оценены по методике, используемой автором, в 55,063 млн руб.

Исходя из перечисленных предположений были получены следующие результаты при $\alpha = 0{,}35$:

X_{opt} = 8,453302 млн руб.

ROI = 5,176.

$EBIS$ (8,453302) = 52,206 млн руб.

Заключение

В работе рассмотрен метод нахождения и обоснования возможных целевых индикаторов и показателей в отношении мероприятий, связанных с улучшением системы менеджмента информационной безопасности, а также обоснованность привлечения средств и размеры необходимых финансовых потребностей для реализации указанных мероприятий.

[9] *Калачов В.Д., Кобко Л.И.* Экономическая эффективность внедрения информационных технологий. М.: МАИ, 2006. 180 с.

[10] Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» (ред. от 13.07.2015).

Список литературы

1. *Радько Н.М., Скобелев И.О.* Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: Радио Софт, 2010. 232 с.

2. *Сердюк В.А.* Организация и технология защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. М.: ГУ–ВШЭ, 2011. 572 с.

3. *Деднев М.А., Дыльнов Д.В., Иванов М.А*. Защита информации в банковском деле и электронном бизнесе. М.: КУДИЦ-Образ. 2004. 512 с.

4. *Голдовский И.* Безопасность электронных платежей в Интернете. СПб.: Питер, 2001. 240 с.

5. *Finne T.* A conceptual framework for information security management // Computers & Security. 1998. № 17. P. 303–307.

6. *Tanaka H., Matsuhara K*. Vulnerability and Effects of Information Security Investment: A Firm Level of Empirical Analysis of Japan // An international forum of financial information systems and cybersecurity: A public policy perspective, College park. 2005. С. 589–599.

7. *Gordon L.A., Loeb M.P.* The Economics of Information Security Investment // ACM Transactions on Information and Systems Security. 2002. Vol. 5. № 4. P. 438–457.

8. *Задірака В.К., Олесюк О.С., Смоленюк Р.П., Штаблюк П.І.* Фінансування витрат на захист інформації в економічній діяльності // Університетські наукові записи. 2006. № 3-4. С. 479–490.

9. *Левченко Є.Г., Демчишин М.В., Рабчун А.О.* Математичні моделі економічного менеджменту інформаційної безпеки // Системні дослідження та інформаційні технології. 2011. № 4. С. 88–96.

10. *Левченко Є.Г., Ворбовська Г.В.* Динамічне управління ресурсами захисту інформації // Захист Інформації. 2011. № 1. С. 11–17.

11. *Ажмухамедов И.М., Ханжина Т.Б.* Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник Астраханского ГТУ. Сер. Экономика. 2011. № 1. С. 185–190.

12. *Собакин И.Б.* Анализ подходов к определению оптимального объема инвестиций в информационную безопасность // Труды ИСА РАН. 2012. Т. 62. № 3. С. 63–68.

13. *Скрипкин К.Г.* Экономическая эффективность информационных систем. М.: ДМК Пресс, 2002. 256 с.

14. *Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* Основы управления информационной безопасностью. М.: Горячая линия-Телеком, 2014. 244 с.

ISSN 2311-8768 (Online)
ISSN 2073-4484 (Print)

Mathematical Analysis and Modeling in Economics

EVALUATING THE EFFICIENCY OF OPTIMAL INVESTMENT IN THE CORPORATE INFORMATION SECURITY MANAGEMENT SYSTEM

Vadim A. BORKHALENKO

Moscow Power Engineering Institute, Moscow, Russian Federation
vadikhide@yandex.ru

Article history:
Received 28 December 2015
Accepted 3 February 2016

JEL classification: C21, C61, G24, G32

Keywords: investing activity, project finance, efficiency criteria, information security, mathematical models

Abstract

Importance To improve the information security management system, there should be a preliminary evaluation and substantiation of possible target indicators and/or activities needed to ensure the required security of information assets, rationale for raising funds to implement the activities, and respective financial needs.

Objectives The research substantiates and determines the optimal amount of investment in the corporate information security management system; proposes investment efficiency indicators as criteria to evaluate the efficiency of activities for ensuring the required security of information resources.

Methods Using methods of differential calculus and probability theory, we analyzed the risks associated with corporate information security and its ineffective management. The article determines criteria to evaluate the efficiency of investment in the information security management system, which reduce the information risk.

Results The article sets out the methods for assessing the optimal amount of investment in the corporate information security management system and criteria to evaluate the efficiency of optimal investment.

Conclusions and Relevance The research reviews the method to find and substantiate possible target indicators and/or activities for improving the corporate information security management system, and rationale for raising funds to implement the activities and respective finance.

Acknowledgments

I am especially grateful to P.B. KHOREV, V.P. PEREVALOV, G.K. PEREVERDIEV for valuable advice and comments.

References

1. Rad'ko N.M., Skobelev I.O. *Risk-modeli informatsionno-telekommunikatsionnykh sistem pri realizatsii ugroz udalennogo i neposredstvennogo dostupa* [Risk models of information and telecommunications systems in terms of remote and immediate access threats]. Moscow, Radio Soft Publ., 2010, 232 p.

2. Serdyuk V.A. *Organizatsiya i tekhnologiya zashchity informatsii: obnaruzhenie i predotvrashchenie informatsionnykh atak v avtomatizirovannykh sistemakh predpriyatii* [Data protection organization and technology: detection and prevention of information attacks in corporate automated systems]. Moscow, National Research University – Higher School of Economics Publ., 2011, 572 p.

3. Dednev M.A., Dyl'nov D.V., Ivanov M.A. *Zashchita informatsii v bankovskom dele i elektronnom biznese* [Information security in banking and e-commerce]. Moscow, KUDITs-Obraz Publ., 2004, 512 p.

4. Goldovskii I. *Bezopasnost' elektronnykh platezhei v Internete* [Security of electronic payments via the Internet]. St. Petersburg, Piter Publ., 2001, 240 p.

5. Finne T. A Conceptual Framework for Information Security Management. *Computers & Security*, 1998, vol. 17, iss. 4, pp. 303–307.

6. Tanaka H., Matsuhara K. Vulnerability and Effects of Information Security Investment: A Firm Level of Empirical Analysis of Japan. An International Forum of Financial Information Systems and Cybersecurity: A Public Policy Perspective. College Park, 2005, pp. 589–599.

7. Gordon L.A., Loeb M.P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 2002, vol. 5, no. 4, pp. 438–457.

8. Задірака В.К., Олесюк О.С., Смоленюк Р.П., Штаблюк П.І. Фінансування витрат на захист інформації в економічній діяльності. *Університетьскі наукові записи*, 2006, no. 3-4, pp. 479–490.

9. Левченко Є.Г., Демчишин М.В., Рабчун А.О. Математичні моделі економічного менеджменту інформаційної безпеки. *Системні дослідження та інформаційні технології*, 2011, no. 4, pp. 88–96.

10. Левченко Є.Г., Вербовська Г.В. Динамічне управління ресурсами захисту інформації. *Захист Інформації*, 2011, no. 1, pp. 11–17.

11. Azhmukhamedov I.M., Khanzhina T.B. Otsenka ekonomicheskoi effektivnosti mer po obespecheniyu informatsionnoi bezopasnosti [Analyzing the cost-effectiveness of information security measures]. *Vestnik Astrakhanskogo GTU. Ser. Ekonomika = Vestnik of Astrakhan State Technical University. Series: Economics*, 2011, no. 1, pp. 185–190.

12. Sobakin I.B. Analiz podkhodov k opredeleniyu optimal'nogo ob"ema investitsii v informatsionnuyu bezopasnost' [Analyzing approaches to determining optimal investment in information security]. *Trudy ISA RAN = Proceedings of Institute for Systems Analysis of Russian Academy of Sciences*, 2012, vol. 62, no. 3, pp. 63–68.

13. Skripkin K.G. *Ekonomicheskaya effektivnost' informatsionnykh system* [Economic efficiency of information systems]. Moscow, DMK Press Publ., 2002, 256 p.

14. Kurilo A.P., Miloslavskaya N.G., Senatorov M.Yu., Tolstoi A.I. *Osnovy upravleniya informatsionnoi bezopasnost'yu* [Fundamentals of information security management]. Moscow, Goryachaya liniya-Telekom Publ., 2014, 244 p.