

УДК 338.246.025:004

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ МАЛОГО И СРЕДНЕГО БИЗНЕСА

¹Иванченко П.Ю., ²Кацуро Д.А., ³Медведев А.В., ⁴Трусов А.Н.

¹Кемеровский филиал ФГБОУ ВПО «Российский экономический университет», Кемерово, email: pavel-ivanchenko@hotmail.com;

²Кемеровский филиал ФГБОУ ВПО «Российский экономический университет», Кемерово, email: davidkacuro@hotmail.com;

³Кемеровский филиал ФГБОУ ВПО «Московский государственный университет экономики, статистики и информатики», Кемерово, email: alexm_62@mail.ru;

⁴Кемеровский филиал ФГБОУ ВПО «Российский экономический университет», Кемерово, email: mors_kem@mail.ru

В статье рассмотрены понятия информационной и экономической безопасности в аспекте их использования в задачах бизнес-планирования. Выделены основные типы источников угроз, влияющие на обеспечение информационной и экономической безопасности на предприятиях малого и среднего бизнеса. Представлен ряд современных методик оценки рисков информационной безопасности. Предложено использование методов экономико-математического моделирования при решении задач информационной и экономической безопасности на предприятиях малого и среднего бизнеса. Разработана математическая модель минимизации рисков информационной безопасности на предприятиях в форме задачи линейного программирования. Сделан вывод о возможности использования математической модели информационной и экономической безопасности как составляющей при анализе инвестиционной привлекательности экономических систем и в частности, предприятий малого и среднего бизнеса.

Ключевые слова: информационная безопасность, математическое моделирование, риски, информационные технологии, инвестиционная привлекательность

MATHEMATICAL MODELING OF INFORMATION AND ECONOMIC SECURITY OF SMALL AND MEDIUM BUSINESS

¹Ivanchenko P.Y., ²Katsuro D.A., ³Medvedev A.V., ⁴Trusov A.N.

¹Kemerovo branch «Moscow State University of Economics, Statistics and Informatics», Kemerovo, email: pavel-ivanchenko@hotmail.com;

²Kemerovo branch «Moscow State University of Economics, Statistics and Informatics», Kemerovo, email: davidkacuro@hotmail.com;

³Kemerovo branch «Moscow State University of Economics, Statistics and Informatics», Kemerovo, email: alexm_62@mail.ru;

⁴Kemerovo branch «Moscow State University of Economics, Statistics and Informatics», Kemerovo, email: mors_kem@mail.ru

The article deals with the concept of information and economic security in the context of their use in the tasks of business planning. There are highlighted the main types of threats that affect information and economic security for small and medium-sized businesses. A number of modern methods of information security risk assessment. It is suggested to use the methods of economic-mathematical modeling for the decision of tasks of information and economic security for small and medium-sized businesses. A mathematical model of minimizing information security risks in enterprises in the form of linear programming tasks is considered. It is concluded that the use of mathematical models of information and economic security, as a component, in the analysis of investment attractiveness of economic systems and, in particular, small and medium enterprises.

Keywords: information security, mathematical modeling, risk, information technology, investment attractiveness

Информационная безопасность (ИБ) в настоящее время становится одним из важнейших аспектов общей экономической безопасности деятельности современной организации, характеризуя состояние защищенности ее бизнес-среды. Защита информации представляет собой особую деятельность по предотвращению утечки информации, несанкционированных изменений ее потоков и других воздействий, негативно влияющих на стабильную работу организации и связанных с ней экономических агентов (клиентов,

поставщиков оборудования, инвесторов, государства и др.). В этой связи своевременная, оперативная и корректная оценка рисков снижения или полной утери ИБ сегодня является актуальной проблемой в деятельности любой организации.

В современных публикациях, затрагивающих вопросы ИБ, выделяется 4 типа источников угроз, влияющих на информационную безопасность:

- природные;
- техногенные;

- человеческие преднамеренные;
- человеческие непреднамеренные.

Учитывая существенную разнотипность указанных источников, разработка методик и алгоритмов оценки риска снижения или полной утери ИБ – достаточно трудоемкая и значимая задача для любой информационной системы, требующая выполнения ряда условий.

Во-первых, необходимо построение гибких моделей информационной системы, важно описывать ее комплексно, с учетом программных, аппаратных ресурсов, внутренних и внешних угроз и уязвимостей, способных настраиваться в соответствии с особенностями конкретной организации.

Во-вторых, с учетом значительного количества факторов риска, математическая модель оценки ИБ должна допускать разработку эффективных численных алгоритмов обработки информации в моделях.

В-третьих, должна быть предельно прозрачна методика оценки рисков, чтобы владелец информации мог адекватно оценить применимость и эффективность методики к конкретной информационной системе.

Для оценки рисков ИБ важно выделить и проанализировать основные угрозы и уязвимости, через которые реализуются угрозы, действующие на информационную систему в смысле отказов или снижения ее работоспособности. На сегодняшний день существует ряд методов оценки рисков информационной безопасности [5]. К основным таким методам можно отнести следующие:

- 1) метод оценки рисков, основанный на построении модели угроз и уязвимостей;
- 2) метод оценки рисков, основанный на построении модели информационных потоков.

Первая методика основана на использовании преимущественно экспертной и статистической информации об угрозах и уязвимостях. Для оценки рисков в информационной системе организации определяется защищенность каждого ценного ресурса при помощи оценки вероятностей реализации угроз, действующих на конкретный ресурс организации (например, вероятность сбоев в работе системы ИБ в связи с низкой квалификацией сотрудников, отсутствием или устареванием программного или аппаратного обеспечения и т.п.), а также уязвимостей, через которые данные угрозы могут быть реализованы. Указанная оценка вероятностей позволяет ранжировать угрозы и уязвимости по степени рисков.

Так как риски ИБ тесно связаны с применением современных информационных технологий, определяющих эффективность деятельности организации в ее инновацион-

ном аспекте, то их можно отнести к разновидности инновационных рисков. Определяя инновационный риск как «вероятность потерь вследствие неправильно поставленной или недостигнутой стратегической цели» [1], при характеристике рисков отказа работоспособности системы целесообразно использовать такой показатель, как уровень затрат (в материальном или стоимостном выражении) на восстановление работоспособности системы.

Исходя из экспертно определенных данных о рисках, уязвимостях и затратах по каждому из ресурсов, можно построить модель угроз и уязвимостей, актуальных для информационной системы организации, и провести анализ функционирования информационной системы с точки зрения минимизации рисков отказа или снижения работоспособности системы и, следовательно, максимизации ее эффективности по критерию ИБ.

Приведем ниже краткую характеристику этапов алгоритма по решению описанной задачи. На первом этапе выделяются наиболее важные для организации направления деятельности, которые определяют (с точки зрения ее руководства) уровень информационной безопасности. На втором этапе, по выделенным направлениям деятельности организации, на основе оценки экспертами вероятности реализации угрозы ИБ, рассчитывается значимость каждой угрозы, а также оценивается уровень затрат в стоимостном выражении на восстановление работоспособности системы. Далее рассчитывается суммарный риск отказа работоспособности системы как сумма рисков по каждому из направлений.

Результатом решения описанной задачи будем считать распределение финансового ресурса по выделенным направлениям деятельности организации, минимизирующего риски отказа работоспособности системы по критерию ИБ.

На практике в условиях многочисленных рисков угроз безопасности произвести подобную численную оценку без использования методов математического моделирования, очевидно, не представляется возможным. Рассмотрим математическую модель минимизации рисков ИБ.

Пусть в технической или социально-экономической системе заданы (найлены) зависимости $r_i = f(x_i)$ рисков r_i отказа работоспособности системы от затрат x_i на их избежание (исключение, уменьшение) в i -м направлении обеспечения информационной безопасности (отказ аппаратного, программного обеспечения, отказ работоспособности системы из-за недостаточной квалификации сотрудников, управленцев и т.п.)

($i = 1, \dots, n$), n – количество указанных направлений. Таким образом, при минимизации рисков информационной безопасности будем использовать такой показатель, как уровень затрат (в материальном или стоимостном выражении) на восстановление работоспособности системы в случае ее отказа по одному или нескольким направлениям.

Определим далее следующие величины:

1) $R = \sum_{i=1}^n r_i$ – суммарный риск отказа

системы;

2) Z – максимальная сумма затрат на уменьшение (устранение) выделенных рисков;

3) $ZMAX_i$ – максимальная сумма затрат на реализацию i -го направления;

4) $ZMIN_i$ – минимальная сумма затрат на реализацию i -го направления, то можно сформулировать следующую задачу математического программирования:

$$\begin{aligned} R_i &\rightarrow \min \\ \sum_{i=1}^n x_i &\leq Z \\ ZMIN_i &\leq x_i \leq ZMAX_i \\ x_i &\geq 0. \end{aligned} \quad (1)$$

Пусть $f(x) = a_i - b_i x_i$, то есть являются линейными функциями от x_i с отрицательными угловыми коэффициентами. Тогда (1) можно записать в виде следующей ЗЛП:

$$\begin{aligned} \sum_{i=1}^n b_i x_i &\rightarrow \max \\ \sum_{i=1}^n x_i &\leq Z \\ ZMIN_i &\leq x_i \leq ZMAX_i \\ x_i &\geq 0. \end{aligned} \quad (2)$$

Коэффициенты a_i в (2) можно трактовать как издержки, которые может понести система в случае отсутствия затрат или, иначе, как максимальные затраты на организацию бескризисной работы системы на i -м направлении обеспечения безопасности, а коэффициенты b_i – как весовые коэффициенты, отражающие относительную значимость i -го направления обеспечения безопасности [2].

Модель (2) представляет собой многопараметрическую задачу линейного программирования. Учитывая ограниченность всех переменных задачи и нестрогость ограничений, можно утверждать, что допустимое множество представляет собой непустой компакт, и данная задача может

быть решена с помощью симплекс-метода Дж. Данцига, который на компьютерах современной вычислительной мощности позволит рассматривать практически неограниченное количество (n) угроз информационной безопасности.

Предприятия малого и среднего бизнеса сегодня являются частью той сферы экономики, которая наиболее восприимчива к технологическим, информационным, бизнес-инновациям. Между тем многие предприятия малого и среднего бизнеса, находясь в информационной среде, не обращают внимания на различного рода угрозы, которым подвержена их информационная система, тем самым подвергая себя риску финансовых потерь.

Для предприятий инновационного типа характерны следующие виды рисков деятельности:

- организационные (низкая квалификация разработчиков проекта, задержка выполнения этапов его реализации);

- научно-технические (изношенность технологического оборудования, отсутствие резервов мощностей или типовых проектных решений);

- финансово-экономические (маркетинговый, риск финансирования проекта, инфляционный, процентный, налоговый и операционный риски).

Важной задачей при принятии управленческих решений в организации всегда была задача оценки инвестиционной привлекательности экономической системы. Решение указанной задачи требует рассмотрения ее двоякой сущности – как задачи оценки экономического потенциала (что влечет необходимость использования оптимизационных подходов и методов анализа [3]) и как задачи учета инвестиционных рисков, связанных с возможностью возникновения угроз потребительской, коммерческой, финансовой, управленческой, информационной, экологической, социальной, политической природы. В работе [4] предложена математическая модель оценки инвестиционной привлекательности предприятия как совокупности выраженной в едином стоимостном измерении оценки инвестиционного потенциала производителя и оценки рисков, выраженных в затратных характеристиках деятельности производителя. Рассмотренная в данной работе модель (2) представляет собой составляющую модели инвестиционной привлекательности, учитывающую вопросы анализа информационных, инвестиционных и других видов рисков деятельности, и может рассматриваться как прототип модели для оценки инвестиционной

привлекательности предприятий малого и среднего бизнеса.

Разработка и использование моделей экономической безопасности на предприятиях, а также алгоритмов и методов их анализа, являются необходимым условием для создания систем поддержки принятия решений по управлению экономической и информационной безопасностью организации.

Список литературы

1. Ильенкова Н.Д. Проблемы анализа инновационного риска / Инвестиции и инновации. – 2011. – № 5. – С. 90–92.
2. Конструктор и решатель дискретных задач оптимального управления («Карма») / Программа для ЭВМ. Свидетельство о регистрации в Роспатенте № 2008614387 от 11.09.2008. Правообладатели: А.В. Медведев, П.Н. Победаш, А.В. Смольянинов, М.А. Горбунов.
3. Медведев А.В. Моделирование стратегии социально-экономического развития региона на основе мезоэкономического подхода и оптимизационной математической модели // Вестник Красноярского государственного университета. Серия «Физико-математические науки». – 2006. – № 1. – С. 208–214.
4. Медведев А.В. Математическая модель оценки инвестиционной привлекательности региона // Современные наукоемкие технологии. – 2013. – № 8–2. – С. 357–361.
5. Digital Security. [Электронный ресурс]: Режим доступа <http://www.dsec.ru/> – дата обращения 29.10.2013.

References

1. Ilyenkova N.D. The problems of innovation riskanalysis / nvestitsiiniinnovatsii. 2011. no. 5. pp. 90–92.
2. Designer and Solver of discrete optimal control problems /computer program. Certificate of the trademarks registration № 2008614387 dated 9/11/2008. Copyright Holders: A.V. Medvedev, P.N. Pobedash, A.V. Smolyaninov, M.A. Gorbunov.
3. Medvedev A.V. Modeling strategy of the region's socio-economic development on the basis of mesoeconomic approach and optimal control problem model // Bulletin of the Krasnoyarsk State University. A series of physical and mathematical sciences. 2006. no. 1. pp. 208–214.
4. Medvedev A.V. A mathematical model of evaluation investment appeal of region // Sovremenniyenaukoyomkiyetekhnologii. 2013. no. 8–2. pp. 357–361.
5. Digital Security. [Electronic resource]: access mode <http://www.dsec.ru/>-treatment date of 29.10.2013.

Рецензенты:

Алексеев Д.В., д.т.н., профессор кафедры вычислительной техники и информационных технологий Кемеровского института (филиала) Российского государственного торгово-экономического университета, г. Кемерово;

Зыков В.С., д.т.н., профессор, заместитель директора по науке Института угля Сибирского отделения РАН, г. Кемерово.

Работа поступила в редакцию 29.11.2013.