ACTA TTPU

II ELECTRONICS AND INFORMATION TECHNOLOGY

MODELS OF INFORMATION SECURITY OF THE SYSTEM OF SMALL AND MEDIUM BUSINESS

Kubayev Ulugbek Rakhmatullayevich, Azamov Temur Narzullayevich

Tashkent University of Information Technologies named after Muhammad Al-Khorazmiy

Abstract

The article considers models of information security of small and medium – sized businesses taking into account sources of threats that affect information security.

Keywords: information security, security, information leakage, algorithm, mathematical model.

МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАЛОГО И СРЕДНЕГО БИЗНЕСА

Кубаев Улугбек Рахматуллаевич, Аъзамов Темур Нарзуллаевич

Ташкентский университет информационных технологий имени Мухаммеда Ал-Хоразмий

Аннотация

В статье рассматривается модели обеспечения информационной безопастности малого и средного бизнеса учитывая источников угроз, влияющих на целосности, несанкционированности и достоверности информационную среду.

Ключевые слова: Информационная безопасность, утечка информации, безопасность, алгоритм, математический модель.

В настоящее время информационная безопасность (ИБ) становится одним из важнейших аспектов общей экономической безопасности деятельности современной организации, характеризуя состояние защищённости 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 любой коммерческой деятельности компании.

В современной практике выделяется четыре 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 работоспособ-ности. На сегодняшний день существует ряд методов оценки рисков информационной безопасности. К основным таким методам можно отнести следующие [1]: метод оценки рисков, основанный на построении модели угроз и уязвимостей; 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, 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 инновационном аспекте, то их можно отнести к разновидности инновационных рисков. Определяя инновационный риск как «вероятность потерь вследствие неправильно поставленной или недостигнутой стратегической цели» [2], 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.

Рассмотрим краткую характеристику этапов алгоритма по решению описанной задачи. На первом этапе выделяются наиболее важные для организации направления деятельности, которые определяют 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 зависимости $r_i = f(x_i)$ рисков r_i отказа работоспособности системы от затрат xi 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 ,…, 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:

$$R = \sum_{i=1}^{n} r_i$$

1) R – суммарный риск отказа системы;

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:

$$R_i \rightarrow min$$

$$\sum_{i=1}^{n} x_i \le Z$$
$$\text{ZMINi} \le \text{xi} \le \text{ZMAX} \quad (1)$$

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

$$\sum_{i=1}^{n} b_i x_i \to max$$

$$\sum_{i=1}^{n} x_i \le Z \ .$$

$$ZMIN_i \le x_i \le ZMAX \quad (2)$$
$$x_i \ge 0$$

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.

Компания малого и среднего бизнеса сегодня являются частью той сферы экономики, которая наиболее восприимчива к технологическим, информационным, бизнес-инновациям. Между тем многие компании 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 компаний 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).

Заключения

Важной задачей при принятии управленческих решений в компании 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) и как задачи учета инвестиционных рисков, связанных с возможностью возникновения угроз потребительской, коммерческой, финансовой, управленческой, информационной, экологической, социальной, политической природы. В работе [3] 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.

Литература

1. Ильенкова Н.Д. Проблемы анализа инновационного риска / Инвестиции и инновации. – 2011. – № 5. – С. 90–92.

3. Медведев А.В. Моделирование стратегии социально-экономического развития региона на основе мезоэкономического подхода и оптимизационной математической модели // Вестник Красноярского госуниверситета. 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.