НЕЧЕТКО-МНОЖЕСТВЕННЫЙ ПОДХОД К ФОРМИРОВАНИЮ ИНФОРМАЦИОННЫХ СОСТАВЛЯЮЩИХ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Людмила МАЛЯРЕЦ, Михаил ДОРОХОВ
Харьковский Национальный Экономический Университет, (Украина)

The general structure of economic's safety systems for the enterprises has been considered. The main criterias and characteristics of information safety are allocated. The application of SWOT-analysis in fuzzy conditions for models of an estimation of information safety has been offered.

В условиях конкуренции стабильное функционирование любого коммерческого и производственного предприятия в значительной степени обеспечивается надежностью его экономической безопасности. Практика показывает, что для этого требуется создание и поддержание интегрированной, многоуровневой и комплексной системы экономической безопасности, обеспечивающей обнаружение, анализ и оценку возникающих, существующих и потенциальных угроз по каждой функциональной составляющей экономической безопасности, а затем – разработка и осуществление соответствующих противодействующих им превентивных мероприятий. В общем случае экономическая безопасность предприятия может рассматриваться с внепроизводственной и внутреннепроизводственной стороны. Первая включает рыночную и интерфейсную безопасность. Вторая, в свою очередь, содержит такие составляющие безопасности, как финансовая, интеллектуальная, кадровая, технологическая, правовая, экологическая, силовая, информационная.

Необходимо подчеркнуть, что хотя в узком смысле информационная безопасность выделяется, как отдельная составляющая, реально (в широком понимании) она всегда присутствует и в значительной степени определяет обеспечение всех остальных компонент. Прежде всего информационная безопасность состоит в осуществлении эффективного, оперативного и достоверного информационно-аналитического обеспечения бизнес-процессов.

К информационным составляющим системы безопасности предприятия относятся:

- сбор всех видов информации, касающихся как функционирования собственно самого предприятия, так и состояния рыночной окружающей среды, клиентов-заказчиков, контрагентов, партнеров, поставщиков, конкурентов;
- накопление, систематизация и анализ полученной и имеющейся информации;
- прогнозирование тенденций развития рынка, научно-технологических, экономических, социальных процессов на нем и в обществе в целом (касающихся деятельности данного предприятия);

- оценка и мониторинг состояния экономической безопасности предприятия в целом и по отдельным компонентам, разработка рекомендаций и мер по ее обеспечению и усилению;
- другие виды деятельности и меры по обеспечению информационной безопасности (организационные, финансовые, технологические, кадровые и так далее).

При этом, рассматривая потоки внешние (входящие)информации, следует разделять ее по источникам формирования на открытую (официальную, общедоступную, из средств массовой информации, интернета и т.п.) и вероятностную несекретную информацию (полученную через неформальные контакты и каналы с носителями такой информации).

Практическая реализация и организация мероприятий по охране информационной составляющей экономической безопасности обеспечивается последовательным выполнением комплекса действий – сбором различных видов необходимой информации, ее обработкой и систематизацией, анализом с привлечением компетентных экспертом и использованием специальных математических методов, практическими действиями по информационной защите всей составляющих жизнедеятельности охраняемого обьекта. Обычно такая защита направлена на противодействие промышленному и экономическому шпионажу со стороны конкурентов или иных заинтересованных юридических и физических лиц; техническую безопасность средств связи, хранения информации, корреспондении, переговоров и исключение несанкционированного доступа (как извне, так и изнутри) к закрытой, конфиденциальной, служебной информации; сбор информации из внешних источников о потенциальных инициаторах промышленного шпионажа, ожидаемых попытках нарушения информационной безопасности и принятие предупредительных мер с целью их пресечения и недопущения.

Уровень информационной безопасности тесно взаимосвязан со степенью использования неполной, неточной и противоречивой информации в процессе принятия управленческих решений на предприятии. Поэтому при принятии решений основными факторами становятся:

- полнота информации (характеризующая соотношение имеющейся в распоряжении лица,принимающего решение информации к общему обьему имеющейся, необходимой информации по данному вопросу);
- точность информации (отношене обьема релевантой – достоверной информации к общему обьему имеющейся информации);
- противоречивость информации (количество суждений за предлагаемое решение к общему количеству мнений в суммарном обьеме доступной релевантной информации).

Очевидно, что в процессе организации системы информационной безопасности, как части общего комплекса мероприятий по экономической безопасности предприятия, необходимо учитывать ряд труднопрогнозируемых и слабо-

формализованных факторов [1]. Среди них – сложность самой среды существования обьекта информационной защиты (предприятия в рыночном конкурентном окружении) среды принятия решений, информационные ограничения, временные факторы, поведенческие ограничения, возможные побочные негативные последствия, личностные оценки и предпочтения руководителей и лиц принимающих решения, взаимосвязь решений, факторы неоднозначности и неопределенности.

Наличие факторов слабой структурированности задач обеспечения информационной безопасности, экспертных оценок и предпочтений, позволяет утверждать, что в данном случае необходимо совместно обрабатывать как данные, так и знания, при этом для обоих компонент должны быть учтены факторы неопределенности. Представляется, что одним из адекватных инструментов для решения таких задач является аппарат теории нечетких множеств.

Нами предлагается использовать для решения таких многокритериальных задач комплексного оценивания уровня информационной безопасности предприятия (компонент его жизнедеятельности и функционирования) методологию SWOT-анализа в нечетко-множественной постановке [2]. Такой подход позволяет учесть различного вида и точности исходные данные и оценки – экспертные (индивидуальные и коллективные), числовые и лингвистические, представленные в различных и несогласованных шкалах измерений, с различной степенью недостоверности (неточности). При этом не требуется (в отличие от статистический методов) обеспечение определенных характеристик выборок, количества и состава опрошенных экспертов (или данных) и тому подобного.

Развитие программного обеспечения и практическая доступность компьютерных средств нечеткого моделирования (Matlab Fuzzy logic toolbox, Fuzzytech, Fuzicalc, Cubicalc) позволяют создавать соответствующие компьютерные модели, доступные для практического использования непосредственно на предприятиях руководителями, отвечающими за информационную и, в более широком смысле, общую экономическую безопасность предприятий.

Литература

1. S.Kavun, R.Brumnik, O.Dorokhov, I.Zolotaryova. The uncertainly-plural model for the estimation of enterprises economic safety level. Social control in contemporary society – practice and research: policing in Central and Eastern Europe: conference proceedings / the 7th biennial International Criminal Justice Conference, Ljubljana, September 2008. – Ljubljana: Faculty of Criminal Justice and Security, 2008. – PP.53-54.
2. А.Дорохов, В.Чернов. Целесообразность и возможность использования нечеткого моделирования для оценки рисков в информационных системах. Securitatea informațională 2010 : Conf. intern., 15-16 apr. 2010. - Ch.: ASEM, 2010. - P.18-21