Ученые записки Таврического национального университета имени В.И. Вернадского
Серия «Экономика и управление». Том 27 (66). 2014 г. № 4. С. 10-14.

УДК 004.056.5

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОВЫШЕНИИ КОНКУРЕНТОСПОСОБНОСТИ ПРЕДПРИЯТИЯ

Аметов Р.И.

Таврический национальный университет имени В.И. Вернадского, Симферополь, Республика Крым
E-mail: refat.ametov95@gmail.com

В статье рассматриваются проблемы обеспечения безопасности информационной среды предприятий. Проанализированы основные угрозы информационной безопасности промышленных секретов на примерах субъектов инновационной деятельности. Проведено исследование модели построения политики информационной безопасности хозяйствующих субъектов.
Ключевые слова: политика информационной безопасности, субъект инновационной деятельности, угрозы информационной безопасности.

ВВЕДЕНИЕ

Реалии российской экономической жизни таковы, что предприниматели в своей практической деятельности сталкиваются не только с экономическими, организационными, правовыми трудностями в процессе создания своего дела и его развития, но и негативным воздействием некоторых субъектов, зачастую носящим противоправный характер, с недобросовестной конкуренцией.

Значение для страны субъектов инновационной деятельности определяет соответствующие требования к обеспечению их безопасности, проведению методологических и конкретно эмпирических исследований по данной проблематике.

Криминологический аспект безопасности субъектов инновационной предпринимательской деятельности – неотъемлемая часть общей системы национальной экономической безопасности. С криминологической точки зрения негосударственные хозяйствующие субъекты могут быть дифференцированы по критерию уровня виктимизации. Эта проблема подробно рассматривается в научных трудах О.Б. Малежина [1]. Уровень криминологической виктимизации характеризуется отношением числа потерпевших от преступлений к общей численности обследуемой социальной группы, что наглядно представлено на рисунке 1.

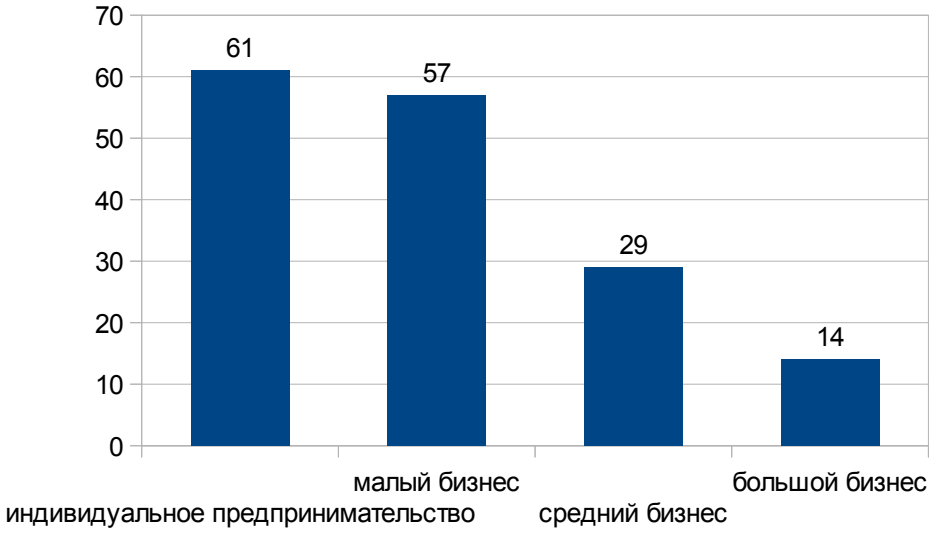

Рис. 1. Уровень виктимизации субъектов предпринимательской деятельности,%

Экономическая безопасность субъектов предпринимательской деятельности является необходимым и одним из основных принципов поддержания конкурентоспособности как предприятия в своей отрасли, так и страны в целом на мировом рынке. Как считает О.Ю.Казакевич, «обеспечение безопасности хозяйствующих субъектов необходимо рассматривать в контексте становления и развития системы обеспечения экономической безопасности страны, определения ее объектов и субъектов, источников внешних и внутренних угроз безопасности, элементов, функций системы, критериев ее надежности и эффективности» [2].

Таким образом, решение проблемы усовершенствования политики информационной безопасности в целях повышения конкурентоспособности предприятия является актуальной научной задачей.

Цель исследования состоит в исследовании методов построения политики информационной безопасности, которые являются одними из мер повышения конкурентоспособности предприятия.

ОСНОВНОЙ МАТЕРИАЛ

С учетом сложившейся политической и экономической ситуации в России сформировался интерес к проблемам обеспечения защиты субъектов инновационного предпринимательства от посягательств со стороны организованной преступности, промышленного шпионажа и иных правонарушений, сохранности коммерческой тайны.

Исследование проблемы показывает, что все факторы, способствующие преступным посягательствам на безопасность инновационного предпринимательства, условно могут быть разделены на внутренние и внешние.

В числе основных внутренних криминогенных факторов, позволяющих выделить субъекты инновационного предпринимательства среди иных объектов защиты в интересах задействования всех сил и средств такой защиты, следует отметить:

1. Наличие у данных субъектов заказов, связанных с созданием в государстве новейших образцов техники и технологий, фундаментальных и прикладных научных исследований, опережающих мировой уровень.
2. Участие этих фирм в продвижении на мировой рынок высокотехнологических товаров.
3. Уровень угроз для экономики отрасли, региона, государства, определяемый вынужденной остановкой или сбоями в функционировании субъектов предпринимательской деятельности.
4. Повышенная экологическая опасность, связанная с деятельностью этих субъектов.

К факторам, составляющим внешние угрозы криминологической безопасности хозяйствующих субъектов, относятся:

- Формирования организованной преступности.
- Негосударственные организации и отдельные лица, специализирующиеся на проведении промышленного шпионажа.
- Деятельность спецслужб иностранных государств, ставящие своей целью добывание информации по экономической проблематике [3].

Предприятия нового типа – это разветвленная сеть распределенных подразделений, филиалов и групп, взаимодействующих друг с другом. Распределенные корпоративные информационные системы становятся сегодня важнейшим средством производства современной компании, они позволяют преобразовать традиционные формы бизнеса в электронный бизнес. Электронный бизнес использует глобальную сеть Internet и современные информационные технологии для повышения эффективности всех сторон деловых отношений, включая продажи, маркетинг, платежи, финансовый анализ, поддержку клиентов и партнерских отношений.

Без должной степени защиты информации внедрение информационных технологий может оказаться экономически невыгодным в результате значительного ущерба из-за потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях.

Задача обеспечения информационной безопасности хозяйствующего субъекта традиционно решается построением системы информационной безопасности (СИБ). Особое внимание уделяется комплексному подходу к обеспечению информационной безопасности, предполагающему рациональное сочетание методов, технологий и средств информационной защиты, эффективное применение правовых, программно-технических и организационных мер. По данным аналитических исследований, приведенных в совместной работе Ю.Ф. Каторина,

Е.В. Куренкова, А.В. Лысова и А.Н. Остапенко, удельный вес каждого из перечисленных компонентов соответственно составляет:

- Правовые методы – 60%.
- Программно-технические – 30%.
- Организационные методы – 10%.

Из приведенных цифр наглядно видно, что правовые методы занимают лидирующее место по своей значимости, и именно поэтому правовое обеспечение рассматривается как приоритетное направление в политике обеспечения информационной безопасности инновационного предпринимательства [4].

Одним из основных методов является политика информационной безопасности. Ее можно причислить как к правовым, так и к организационным методам. Политика безопасности субъекта инновационной деятельности определяется в изданном специальном документе (или своде документов), в котором рассматриваются вопросы философии, задач, организации, стратегии, методов в отношении обеспечения конфиденциальности, целостности, доступности информации и информационных ресурсов предприятия. Исходным пунктом для формирования требований является установление среды информационной безопасности. При определении среды безопасности необходимо учитывать:

– Физическую среду, которая определяет все аспекты внешней среды, имеющие отношение к безопасности, включая условия физической безопасности защищаемого объекта, нормативно-правовую базу и данные, относящиеся к персоналу.
– Информационные активы, подлежащие защите, к которым должны применяться требования и меры безопасности.
– Назначение защищаемого объекта, в том числе, технические характеристики и область применения аппаратных и программных средств.

Анализ факторов внешней среды завершается описанием следующих параметров среды безопасности:

1. Угрозы безопасности, которые могут быть реализованы по отношению к защищаемому объекту. В описании угроз безопасности должны содержаться такие компоненты, как источник угрозы, способ ее реализации, уязвимости объекта, которые при этом используются и ресурсы, подверженные действию угроз.
2. Меры и правила политики безопасности организации, которые обеспечиваются по отношению к объекту защиты;
3. Предположения об условиях, которые должны быть обеспечены в среде, чтобы объект мог рассматриваться как безопасный.

В настоящее время отсутствует какая-либо универсальная методика, позволяющая четко относить ту или иную информацию к категории коммерческой тайны. Законопроектом «О коммерческой тайне» права по отнесению информации к категории коммерческой тайны предоставлены руководителям хозяйствующих субъектов. Поэтому при разработке политики информационной безопасности руководителям субъектов инновационной деятельности целесообразно определить функции по защите коммерческой тайны субъекта хозяйствования:

1. Выработать критерии выделения ценной информации, подлежащей защите.
2. Определить объекты интеллектуальной собственности, подлежащие охране.
3. Выбрать методы защиты.
4. Разработать для последующего утверждения Перечень сведений, составляющих промышленные секреты.
5. Установить правила допуска и разработать разрешительную систему доступа к сведениям, составляющим промышленные секреты.

ВЫВОДЫ

В результате проведенных исследований установлено, что одной из основных мер повышения конкурентоспособности предприятия является построение и поддержания должного состояния информационной безопасности, которое определяется необходимыми уровнями подготовки политики информационной безопасности. Также установлено, что при разработке политики информационной безопасности руководителям субъектов предпринимательской деятельности целесообразно определить функции по защите коммерческой тайны субъекта хозяйствования.

Список литературы

1. Максименко С.В. Технологическая модель обеспечения достоверности данных информационных технологий. / С.В. Максименко // Безопасность информационных технологий. – М., 1998. – №2. – С.14-15.
2. Измайлов А.М. Концептуальное проектирование интегрированных систем безопасности / А.М. Измайлов // БДИ . – М., 1998. – №4. – С.14.
3. Герасименко В.А. Комплексная защита информации в современных системах обработки данных. / Герасименко В.А. // Зарубежная радиоэлектроника. – М., 1994. – №2. – С.35-38.
4. Казакевич О.Ю. Предприниматель в опасности: способы защиты. Практическое руководство для предпринимателей и бизнесменов / О.Ю. Казакевич, Н.В. Конев, В.Г. Максименко // М.: Юрфак МГУ, 1992. – 119с.

Статья поступила в редакцию 11. 11. 2014 г.