УДК 338.001.36

Охрименко С. А.
Солоненко О.

ИНФОРМАЦИОННЫЕ РИСКИ И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Аннотация. Проведен сравнительный анализ понятий информационный риск и экономическая безопасность, выполнены рекомендации и предложения для действенного механизма финансовой безопасности.

Ключевые слова: экономическая безопасность, техногенная безопасность, экологическая безопасность, информационная безопасность, научно-техническая безопасность, информационный риск.

Функционирование и развитие сферы предпринимательства в экономике любой страны требует наличия определенных условий, обеспечивающих эти процессы. Одним из важнейших условий выступает безопасность предпринимательства. Безопасность предпринимательской деятельности – это состояние защищенности субъекта предпринимательской деятельности на всех стадиях его функционирования от внешних и внутренних угроз, имеющих негативные, прежде всего экономические, а также организационные, правовые и иные последствия. Система безопасности предприятия включает в себя подсистемы: экономическая безопасность, техногенная безопасность, экологическая безопасность, информационная безопасность, психологическая безопасность, физическая безопасность, научно-техническая безопасность, пожарная безопасность.

Безопасность предпринимательства может оцениваться с разных сторон.

С организационной стороны. В этом случае предполагается сохранение как самой фирмы, так и ее организационной целостности, нормальное функционирование основных подразделений, отделов, служб и т.п..

С правовой стороны. Постоянное обеспечение соответствия деятельности фирмы действующему законодательству, что выражается в отсутствии претензий со стороны правоохранительных органов или контрагентов к фирме.

С экономической стороны. Это проявляется в стабильных или имеющих тенденцию к росту основных финансово-экономических показателях деятельности фирмы, таких как собственный капитал, объем годового оборота, прибыль, рентабельность

С информационной стороны. Безопасность может быть оценена как сохранение состояния защищенности внутренней конфиденциальной информации от утечки или разглашения в различных формах [1].

Первоначально понятие экономической безопасности рассматривалось как обеспечение условий сохранения коммерческой тайны и других секретов предприятия. Проблема экономической безопасности предприятия в указанном контексте решалась исходя из предпосылки, что степень надежности всей системы сохранности информации определяется уровнем безопасности самого слабого ее звена, которым считается персонал организации.

Несколько позже возобладал другой подход к трактовке понятия экономической безопасности предприятия. Согласно этому взгляду экономическая безопасность предприятия обусловлена влиянием внешней среды, которая в рыночной экономике все время изменяется, никогда не остается стабильной, постоянной или неизменной. Именно с позиций влияния внешней среды, защиты предприятий от ее отрицательного

влияния и рассматривается экономическая безопасность предприятия. Позже она стала рассматриваться намного шире – как возможность обеспечения ее устойчивости в разнообразных, в том числе и в неблагоприятных условиях, которые складываются во внешней среде, вне зависимости от характера ее влияния на деятельность предприятия, масштаба и характера внутренних изменений. Тогда экономическая безопасность предприятия определяется как – защищенность его деятельности от отрицательных влияний внешней среды, а также как способность быстро устранить разные угрозы или приспособиться к существующим условиям, которые не сказываются отрицательно на его деятельности.

Существует ресурсно-функциональный подход, в котором экономическую безопасность предприятия рассматривают как эффективное использование корпоративных ресурсов для предотвращения угроз и обеспечения стабильного функционирования предприятия в настоящее время и в будущем. С этой целью рассматривают совокупность процессов, протекающих в организации, со всеми их характерными особенностями и взаимосвязями. В ресурсно-функциональном подходе в качестве основных направлений экономической безопасности предприятия различают семь функциональных составляющих: интеллектуально-кадровую, финансовую, технико-технологическую, политико-правовую, экологическую, информационную и силовую. При таком подходе экономическая безопасность рассматривается в комплексе-исследуются важнейшие факторы, влияющие на состояние функциональной составляющей экономической безопасности предприятия, изучаются основные процессы, влияющие на ее обеспечение, проводится анализ использования ресурсов предприятия, рассматриваются экономические индикаторы, отражающие уровень обеспечения функциональной составляющей экономической безопасности предприятия, и разрабатываются меры по обеспечению максимально высокого уровня функциональной составляющей экономической безопасности предприятия.

Существуют иные точки зрения по поводу определения сущности экономической безопасности предприятия, в которых экономическая безопасность рассматривается с точки зрения минимизации потерь и сохранения контроля над собственностью. В качестве способов обеспечения экономической безопасности предприятия предлагается построение системы защиты его экономических интересов, в которой основное внимание уделено вопросам борьбы с недобросовестной конкуренцией, обеспечению информационной безопасности и правовой защите интеллектуальной собственности.

Существуют подходы к экономической безопасности предприятия, которые называют узкофункциональными. Экономическая безопасность предприятия рассматривается с позиции отдельного аспекта его деятельности. Тогда важнейшим направлением формирования системы экономической безопасности, в том числе и предприятий, является создание действенного механизма финансовой безопасности. Учет – одна из основных функций управления, именно учет исключает возможность прямых хищений без установленных законом последствий, создает информационные условия для осуществления контроля целесообразности и законности использования ресурсов в превентивном, текущем и следующем режимах и оказывает содействие предотвращению реализации угроз, которые снижают экономическую устойчивость предприятий. Разработка узкофункциональных направлений обеспечения экономической безопасности предприятия позволяет провести всесторонние и глубокие исследования выбранного аспекта деятельности предприятия и показать конкретные пути и способы обеспечения экономической безопасности предприятия в той или иной сфере его деятельности [2].

В условиях рыночной экономики риск – ключевой элемент предпринимательства. Предприниматель, умеющий вовремя рисковать, зачастую оказывается

вознагражденным. В условиях политической и экономической нестабильности степень риска значительно возрастает. Риск в предпринимательской деятельности естественным образом сопряжен с менеджментом, со всеми его функциями — планированием, организацией, оперативным управлением, использованием персонала, экономическим контролем. Каждая из этих функций связана с определенной мерой риска и требует создания адаптивной к нему системы хозяйствования. То есть необходим и особый менеджмент риска, или специфическая система управления, основывающаяся на познании экономической сущности риска, разработке и реализации стратегии отношения к нему в предпринимательской деятельности [3].

Термин – «информационный риск» приобрел широкое применение, однако пока не существует единой принятой учеными и практиками трактовки. Проблемы, которыми занимался узкий круг специалистов, стали настолько острыми, что назрела необходимость осмысления данного понятия как важной экономической категории и решаться она должна на всех уровнях управления. Для этого необходимо определить места информационных рисков в общей системе экономических рисков.

Одна группа специалистов вкладывает в понятие информационного риска смысл того, что это возможное событие, в результате которого несанкционированно удаляется, искажается информация, нарушается ее конфиденциальность или доступность. То есть понятие информационного риска используется как синоним понятия угроза безопасности информации. Управление такими информационными рисками сводится к защите информации. Причем под защитой информации понимают защиту в основном от злоумышленных действий. Некоторые специалисты еще в большей степени сужают понятие информационного риска. Они рассматривают информационный риск как угрозу безопасности информации только в компьютерных системах. Сторонниками таких подходов, как правило, стали специалисты в области защиты информации. Практически отсутствуют подходы к трактовке понятия информационного риска, в которых в качестве возможных нежелательных событий рассматривались бы события, приводящие к снижению достоверности, полноты и актуальности информации на стадии ее получения и ввода в информационную систему. В понятие информационный риск не включают также риски, связанные с возможным наличием ошибок в моделях, алгоритмах обработки информации, программах, которые используются для выработки управляющих решений. Не всегда понятие информационный риск связывают с возможностью снижения качества информации ниже допустимого предела в результате сбоев и отказов программных и технических средств.

Другая группа специалистов рассматривает информационные риски как экономическую категорию. Они трактуют информационные риски как возможность возникновения убытков, неполучение прибыли и другие негативные последствия для предприятия. Тогда информационный риск – это опасность возникновения убытков или ущерба в результате применения компанией информационных технологий. Риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи. Недостатком подобных определений является нечеткое указание на объекты, с которыми связаны возможные события, приводящие к ущербу, исключение из рассмотрения рисков, связанных с традиционным документооборотом, с воздействием злоумышленников на информационные ресурсы методами шпионажа и диверсий.

Понятие информационный риск можно трактовать в широком смысле, рассматривая негативные явления, которые непосредственно не связаны с информационной системой предприятия. К ним относятся нарушение авторских прав на использование и распространение продукции интеллектуального труда,

распространение заведомо ложных сведений о предприятии (дезинформация), незаконное использование торговой или производственной марки. То есть к информационным рискам относятся также события, связанные с незаконным использованием информации или искажением информации, имеющей отношение к предприятию, но возникающие во внешней среде и оказывающие воздействие на внешнюю среду, непосредственно не воздействуя на информационную систему. В результате изменений внешней среды бизнес-процессам предприятия наносится ущерб. Тогда информационный риск – это возможность наступления случайного события, приводящего к нарушениям функционирования и снижению качества информации в информационной системе предприятия, а также к неправомерному использованию или распространению информации во внешней среде, в результате которых наносится ущерб предприятию. Информационный риск вызывается внутренними или внешними причинами. Факторы информационных рисков в меньшей степени связаны с конкретными источниками риска, чем причины рисков. Они в основном отражают состояние информационной системы предприятия в целом и особенно состояние подсистемы противодействия информационным рискам. Факторы риска близки к понятию уязвимости системы, которые используются специалистами по защите информации. Для наступления рискового события необходимо одновременное наличие причины и фактора риска.

Причинения ущерба предприятию в результате реализации информационного риска быть следствием использования в бизнес-процессе управляющей информации, качество которой в результате воздействия информационного риска снизилось до неприемлемого уровня. Также предприятия несут убытки за счет прямого воздействия информационных рисков на объекты информационной системы, в результате которого объекты приходят в неработоспособное состояние. Такие риски называют прямыми информационными рисками. Для восстановления их работоспособности предприятие вынуждено расходовать ресурсы. Примерами таких рисков являются уничтожение технических средств в результате аварий и стихийных бедствий, утраты программных средств, информационных баз данных и т. п. Еще один путь причинения ущерба предприятию в результате реализации информационных рисков является изменение внешней среды, которое сказывается на эффективности функционирования предприятия. Например, при нарушении конфиденциальности информации ухудшается конъюнктура рынка, возможен срыв переговоров с партнерами и другие последствия, приносящие ущерб материальным или интеллектуальным ресурсам предприятия. Ущерб предприятию наносится при попадании во внешнюю среду сведений об имевших место информационных рисках, касающихся предприятия. В некоторых случаях деловой репутации предприятия наносится такой ущерб, который может привести к банкротству предприятия. Информационные риски, которые наносят ущерб предприятию, являющийся следствием воздействия рисков на бизнес-процессы предприятия или внешнюю среду называют косвенными информационными рисками.

Информационные риски приводят к ущербу предприятия. Поэтому они с полным правом могут быть отнесены к экономическим рискам. При выделении информационных рисков в отдельный вид экономических рисков важно определить соотношение и взаимосвязи информационных и других экономических рисков. Проблема заключаться в том, что не существует единой общепризнанной универсальной классификации, имеющей научное обоснование. Это объясняется, прежде всего, большим количеством видов рисков и возможных признаков их классификации [4].

Любой экономический риск включает в себя информационную составляющую. Соотношение информационной составляющей в экономическом риске определяется

значением информации для определенных видов экономической деятельности предприятий и особенностями бизнес-процессов. Управление информационными рисками выходит на одно из первых мест среди проблем обеспечения экономической безопасности предприятия. Придание экономического смысла информационному риску позволяет применять экономические методы управления этим риском. В соответствии с логической схемой классификации и с целью исключения многократного применения названия «информационный риск» на разных уровнях классификации целесообразно включать конкретные информационные риски в состав соответствующих групп экономических рисков. Часть экономических рисков по существу является полностью информационными рисками. К ним относятся, например, управленческий и инвестиционный риски. В значительной степени информационными являются такие риски как банковский, валютный, процентный, производственный риск предприятий, оказывающие информационные услуги, и другие риски, в которых основное место занимает риск принятия управленческого решения или производственные процессы являются информационными процессами [4].

Литература

1. Белозеров И. П. Теневая экономика и экономическая преступность: электронный учебник, http://newasp.omskreg.ru/bekryash/index.htm.

2. Козаченко А. В., Пономарев В. П., Ляшенко А. Н. - "Экономическая безопасность предприятия: сущность и механизм обеспечения" http://www.safetyfactor.narod.ru/doc/notion.html.

3. Тэпман Л. Н. Риски в экономике : Учеб. пособие для вузов / Под ред. проф. В. А. Швандара. - М. : ЮНИТИ-ДАНА, 2002. - 380 с.

4. Завгородний В.И. Парадигма информационных рисков http://www.fa-kit.ru/main_dsp.php?top_id=591.

Summary. In the article the comparative analysis of concepts information risk and economic safety is carried out, recommendations and offers for the effective mechanism of financial safety are executed.

Keywords: Economic safety, technogenic safety, ecological safety, information safety, scientific and technical safety, information risk.

Стаття надійшла до редакції 30.03.2010