М.Е. Бешкинский[1]

БАЗОВЫЕ ЭЛЕМЕНТЫ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ВЕНЧУРНОЙ КОМПАНИИ

Усиление агрессивности конкурентной среды на внутреннем и внешнем рынках повышает значение системы обеспечения экономической безопасности в компаниях. Грамотная и поэтапная работа по обеспечению экономической защиты интеллектуальной собственности, лежащей в основе инновации, позволяет инновационной компании развиваться на современном рынке.

Ключевые слова: *безопасность инноваций, интеллектуальная собственность, конкурентная разведка, недобросовестная конкуренция, риск, промышленный шпионаж, экономическая безопасность предприятия, бенчмаркинг, служба безопасности, информационная безопасность.*

M.E. Beshkinskiy

BASIC ELEMENTS OF THE SYSTEM OF ECONOMIC SECURITY OF THE VENTURE COMPANY

Strengthening the aggressiveness of competitive environment in domestic and foreign markets increases the value of the system providing economic safety in the companies. Accurate and step by step work guarantees economic protection of the intellectual property, which lies at the basis of innovation, makes possible for Innovation Company to be developed on the contemporary market.

Keywords: *security innovation, intellectual property, competitive intelligence, unfair competition, risk, industrial espionage, economic security enterprise, benchmarking, security service, the information security.*

Маленькая течь топит большой корабль.
Бенджамин Франклин

На мировом рынке конкуренция за ресурсы и рыночные доли, необходимые бизнесу, проходит напряженно, а порой принимает и жестокие формы. В борьбе за выживание шансы на успех имеет тот, кто грамотно применяет технологии обеспечения безопасности в своей деятельности. Конкуренция в мире растет, и эффективная система безопасности при ее эффективном применении может стать решающим фактором, способным привести к успеху даже компанию, которой грозило разорение.

Условия ведения современного бизнеса характеризуются многими признаками, в их числе: повышение скоростей (быстрая смена технологий, быстрый рост темпов деловой жизни и, соответственно, скорости принятия управленческих решений); информационная перегрузка; возрастающая агрессивность конкуренции; сильное влияние политических рисков.

Разработка, принятие и осуществление обоснованных управленческих решений в обеспечении экономической безопасности предприятия является одной из важнейших проблем современного менеджмента. Об этом свидетельствуют и возрастающие масштабы потерь в результате даже небольших ошибок, допущенных при принятии решений.

Российские предприятия и организации подвержены воздействию многочисленных внутренних и внешних угроз, иногда криминального характера, что приводит к негативным последствиям для всего народного хозяйства. Поэтому обеспечение экономической безопасности предприятий является одним из приоритетных направлений в системе экономической безопасности России.

Цель у инвесторов и топ-менеджмента высокотехнологичного предприятия одна – не допустить использования инновации конкурентами и получить выгоду от монопольного использования. Главной целью обеспечения экономической безопасности инновационного предприятия является достижение максимальной стабильности функционирования, создание основы и перспектив роста для выполнения целей бизнеса, вне зависимости от объективных и субъективных угрожающих факторов.

Переход экономики страны на инновационный путь развития активизирует роль инноваций в бизнесе. В высокотехнологичной экономике ноу-хау составляет ключевую часть активов компании. *Инновация* – это результат инвестирования в разработку и получение нового знания, ранее не

[1] Кандидат экономических наук, доцент распределенной кафедры экономических дисциплин НОУ ВПО «Российский новый университет».

применявшейся идеи по обновлению сфер жизни людей (технологии; изделия; организационные формы существования социума, такие, как образование, управление, организация труда, обслуживание, наука, информатизация и т.д.) и последующий процесс внедрения (производства) этого с фиксированным получением дополнительной ценности (прибыль, опережение, лидерство, приоритет, коренное улучшение, качественное превосходство, креативность, прогресс) [1]. Процесс создания нового продукта состоит из следующих этапов: инвестиции – разработка – процесс внедрения – получение качественного улучшения. Предмет особой защиты инноваторов – секрет производства, или ноу-хау (от англ. *know how* – знать как) – любая конфиденциальная информация, способная обеспечить превосходство над конкурентами. Это – оригинальные технологии, знания, умения, которые еще не стали широко известны и могут быть предметом купли-продажи или использоваться для достижения конкурентного преимущества над другими людьми. Ноу-хау – определенный набор информационных подходов, включающих формулы, методы, схемы и наборы инструментов, необходимых для успешного ведения дела в какой-либо области или профессии.

Инновационный продукт, в основе которого – интеллектуальная собственность (ноу-хау), приходится продвигать в высококонкурентной, агрессивной среде, в которой есть место недобросовестной конкуренции, конкурентной разведке, промышленному шпионажу, дезинформации, мошенничеству, экономическим преступлениям.

В высокотехнологичном секторе у бизнеса те же противники, что и в обычной жизни. Это и профессиональные, и начинающие преступники, и конкуренты, устраивающие охоту за секретами, различные недоброжелатели, начиная с хакеров и завершая психически неуравновешенными лицами. А для определенных категорий бизнеса – это и разведывательные структуры иностранных государств.

Комплексная защита инноваций предполагает использование различных методов защиты, в первую очередь патентование и использование режима коммерческой тайны. В числе применяемых современных технологий – *бенчмаркинг*, обеспечение информационной безопасности, активное применение современных технологических новинок в области безопасности.

Для определения угроз внешней и внутренней среды важно отметить понятие *деловая конкуренция* в бизнес-среде как особое соревнование, возникающее между хозяйствующими субъектами, каждый из которых своими действиями ограничивает возможность конкурента односторонне воздействовать на условия обращения товаров на рынке, то есть о степени зависимости рыночных условий от поведения отдельных участников рынка.

Среди составляющих деловой конкуренции можно отметить: конкуренцию между уже существующими участниками или игроками на рынке; конкуренцию между потенциальными участниками рынка; конкуренцию со стороны суррогатов какого-либо товара или услуги; рыночное давление со стороны покупателей, направленное на занижение цены; рыночное давление со стороны поставщиков сырья, направленное, естественно, на завышение цены.

Виды внутренней и внешней конкуренции.

Недобросовестная конкуренция. Недобросовестная конкуренция представляет собой нарушение общепринятых правил и норм конкуренции. При этом нарушаются законы и неписаные правила.

На рынке новых продуктов широко применяются различные формы недобросовестной конкуренции, в частности: распространение ложных, неточных или искаженных сведений, способных причинить убытки другому хозяйствующему субъекту либо нанести ущерб его деловой репутации; введение потребителей в заблуждение относительно характера, способа и места изготовления, потребительских свойств, качества товара; некорректное сравнение хозяйствующим субъектом производимых или реализуемых им товаров с товарами других хозяйствующих субъектов; продажа товара с незаконным использованием результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации юридического лица, индивидуализации продукции, выполнения работ, услуг; получение, использование, разглашение научно-технической, производственной или торговой информации, в том числе – коммерческой тайны, без согласия ее владельца.

Существуют и такие методы недобросовестной конкуренции, как демпинг, тайный сговор на торгах и создание тайных картелей, распространение ложной информации и рекламы, применение часто используемого в конкурентной борьбе в России «административного ресурса» и пр.

Нарушение авторских прав. Нарушение авторских прав подразумевает несанкционированное правообладателем распространение материала, защищенного авторским правом. Различают нарушение неимущественных авторских прав (плагиат) и нарушение имущественных авторских прав (контрафакция).

Дезинформация. Способов манипулирования информацией множество – это введение кого-либо в заблуждение путем предоставления неполной информации или полной, но уже не нужной информации, искажение контекста, искажение части информации. Цель такого воздействия всегда одна – оппонент должен поступить так, как это необходимо манипулятору. Среди видов дезинформации – введение в заблуждение конкретного лица или группы лиц; манипулирование поступками одного человека или группы лиц; создание общественного мнения относительно какой-то проблемы или объекта [2].

Промышленный шпионаж. В ситуации, когда необходимость выживания или повышения конкурентоспособности существует объективно, а о наличии законных методов достижения результата предприятие не информировано, часть компаний встает на путь промышленного шпионажа (нарушающего нормы законодательства, прежде всего – уголовного). Основное предназначение промышленного шпионажа как одной из форм недобросовестной конкуренции – экономия средств и времени, которые требуется затратить, чтобы догнать конкурента, занимающего лидирующее положение, либо не допустить в будущем отставания от конкурента, если тот разработал или разрабатывает новую перспективную технологию, а также чтобы выйти на новые для предприятия рынки.

Экономическая (конкурентная) разведка. Среди инструментов экономической разведки различаются: подкуп (подкупаются лица, способные передать документацию или образцы продукции по интересующей тематике); шантаж (в отношении тех же лиц); кража (документов или продукции); диверсия (временный или постоянный вывод из строя образцов продукции, людей или предприятий конкурента); тайное физическое проникновение на объект конкурента, связанное с умышленным преодолением рубежей защиты, созданных конкурентом для обеспечения сохранности информации или продукции; внедрение агента на предприятие или в страну конкурента с заданием получить доступ к информации или продукции, которые составляют предмет коммерческой или государственной тайны конкурента; хищение информации с помощью незаконного использования технических средств снятия информации (прослушивание чужих телефонных линий, незаконное проникновение в чужие компьютерные сети и т.п.).

Мошенничество. Основной принцип мошенничества – ввести жертву в заблуждение, установив с ней доверительные отношения, и, воспользовавшись этим доверием, побудить ее под тем или иным предлогом добровольно передать деньги, имущество, права на что-либо мошеннику.

Экономические преступления. Эти действия охватываются составами преступлений, предусмотренных российским уголовным законодательством.

Среди задач инвесторов и топ-менеджмента инновационной компании в области обеспечения безопасности – это постоянная, циклическая последовательность действий, на основе совершенствования процесса принятия соответствующих управленческих решений.

Экономическая безопасность предприятия – это такое состояние его функционирования, которое характеризуется защищенностью от внешних и внутренних угроз, наличием конкурентных преимуществ, обусловленных устойчивым развитием материального, финансового, кадрового, технико-технологического потенциалов, отвечающих стратегическим целям и задачам предприятия.

Фундаментальная цель по обеспечению безопасности – обеспечить в компании чувство защищенности вследствие осознания того факта, что судьба предприятия находится в его собственных руках и что фирма не станет внезапно жертвой обстоятельств, либо чьих-то враждебных действий.

Среди задач обеспечения безопасности: информационное обеспечение процесса выработки управленческих решений как на стратегическом, так и на тактическом уровнях; создание эффективной системы раннего предупреждения (насколько возможно, раннее привлечение внимания лиц, принимающих решения, к угрозам, которые потенциально могут причинить ущерб бизнесу); выявление благоприятных для бизнеса возможностей; выявление попыток конкурентов получить доступ к закрытой информации компании; управление рисками с целью обеспечить эффективное реагирование компании на быстрые изменения окружающей среды.

Желая монопольно использовать некоторый способ производства или техническое решение, предприятие может выбрать один из двух методов защиты – патент или коммерческую тайну. Цель у патента и коммерческой тайны одинаковая – не допустить использования инновации конкурентами и получить выгоду от монопольного использования. Так, коммерческая тайна (как режим конфиденциальности информации) позволяет ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Но *методы защиты* принципиально отличаются.

• *Патентование* подразумевает раскрытие сведений и дальнейшую (предоплаченную авторами) защиту со стороны закона, в том числе – право запрещать иным лицам использовать такое же решение без согласия держателя патента под угрозой судебного преследования.

• *Защита при помощи тайны* (*ноу-хау*) отличается тем, что сведения никому не раскрываются, но в случае разглашения или независимого открытия иным лицом запретить использование такого способа (технического решения) уже невозможно. Права на ноу-хау действуют до тех пор, пока сохраняется конфиденциальность [3].

В современных условиях обычно используется комплексная защита инноваций: авторы получают патент (чаще – пакет патентов) и к ним прилагают пакет ноу-хау, который страхует авторов от несанкционированного применения инновации в странах, где не осуществляется патентная защита, а также от похищения изобретений государством (например, для приоритетных нужд военно-промышленного комплекса).

Все больше компаний в своей деятельности усиливают роль различных *элементов системы безопасности*. К важнейшим из них относят *конкурентную разведку* (англ. *Competitive Intelligence*, сокр. CI). Она осуществляется с целью повышения конкурентоспособности коммерческой организации для выработки управленческих решений, сбора и обработки данных из разных источников. Другие часто встречающиеся названия конкурентной разведки – *бизнес-разведка*, *деловая разведка*.

Ключевая роль разведки в жизни предприятия – это опережение конкурентов в тендерах; оценка потенциальных рисков и благоприятных возможностей при инвестициях; опережение шагов конкурентов в рамках маркетинговых кампаний с помощью продуманных упреждающих действий, выработанных на основе данных, предоставленных конкурентной разведкой; получение выгод от слияний и поглощений.

Правильно организованная конкурентная разведка не ограничивается изучением конкурентов, а проводит работу в отношении всей среды, в которой живет предприятие. В частности, изучается политическая и законодательная обстановка, кадровые перемещения людей, чья деятельность может оказать влияние на компанию, эксперты, способные проконсультировать по тому или иному специальному вопросу, новые технологии, собственные клиенты и поставщики компании [4].

В качестве источников информации для конкурентной разведки могут выступать периодические издания, мнения аналитиков, личные наблюдения специалистов на месте, беседы с сотрудниками, конкурентами и контрагентами конкурента, выставки и конференции, исследования легально приобретенных образцов продукции конкурента и проч.

В информационный век роль экономической разведки постоянно возрастает, поскольку именно она становится основным инструментом извлечения действительно необходимых для принятия решения данных из обильного информационного потока.

Современные методики и алгоритмы решения проблем безопасности компаний.

Бенчмаркинг. Все более широкое распространение приобретает бенчмаркинг (англ. *benchmarking*) – подход к планированию деятельности компании, искусство обнаружения того, что другие делают лучше, изучение, усовершенствование и применение их методов работы.

Концепция бенчмаркинга (анализа превосходства) позволяет постоянно повышать производительность, качество и быть впереди конкурентов, предоставляет организации сигналы раннего предупреждения об ее отставании; выясняет уровень организации по сравнению с лучшими в мире; ведет к быстрому внедрению новых подходов при меньшем риске; сокращает затраты на процесс улучшения. Бенчмаркинг помогает объяснить причины успеха компании, посредством бенчмаркинга компания изучает «лучшую» продукцию и маркетинговый процесс, используемый прямыми конкурентами и фирмами, работающими в других подобных областях.

Использование новейших технологических достижений. В качестве примера можно привести технологии поиска и обработки информации. Профессиональный поиск информации обеспечивается применением: *программно-аппаратных комплексов* (так называемые ситуационные центры принятия решений, или командные пункты); *программного обеспечения*, позволяющего анализировать текст по принципу негатив/позитив в отношении изучаемого объекта; *организации мониторинга информации* с помощью специальных программ – роботов слежения; *платных баз данных,* способных после наполнения материалом вручную графически показывать связи между людьми или компаниями, проанализировав заведенную информацию [5].

Обеспечение информационной безопасности. Обеспечение безопасности информации складывается из трех составляющих: конфиден-

циальности, целостности, доступности. Точками приложения процесса защиты информации к информационной системе являются аппаратное обеспечение, программное обеспечение и обеспечение связи (коммуникации) [6].

Информационная безопасность организации – состояние защищенности информационной среды организации, обеспечивающее ее формирование, использование и развитие. *Политика безопасности информационно-телекоммуникационных технологий* (англ. *ICT security policy*) – это правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию. Политика информационной безопасности оформляется в виде документированных требований на информационную систему.

Эффективная система обеспечения безопасности инновационного предприятия включает эффективную методику анализа и оценки проблемных ситуаций, определение целевых установок, создание методологического инструментария, расчет средств для обеспечения безопасности, систематизацию мер по ее реализации.

Противодействие экономическим правонарушениям и преступлениям на любом предприятии предполагает создание многоцелевой системы управления, учет норм международных стандартов, применение более совершенных технологий в принятии управленческих решений, обоснование новых направлений кадровой политики, многопрофильную подготовку кадров.

Таким образом, надежное решение задач обеспечения безопасности инновационного бизнеса, защиты интеллектуальной собственности во многом зависит от активного поиска новых, более эффективных форм и методов, соответствующих современному развитию общества и передовых информационных технологий.

Литература

1. Ивина, Л.В., Воронцов, В.А. Венчурный бизнес : толковый словарь трудноперевод имых англоязычных терминов. – 2006. – 165 с.

2. Кузин, А.В., Нежданов, И.Ю., Ющук, Е.Л. Дезинформация и активные мероприятия в бизнесе. – Казань : Яналиф, 2009. – 134 с.

3. ГК РФ, глава 75. Право на секрет производства (ноу-хау).

4. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). – М. : Оружие и технологии, 2009.

5. Интернет-сайт «Технологии разведки для бизнеса» http://it2b.ru/.

6. Лепехин, А.Н. Расследование преступлений против информационной безопасности : теоретико-правовые и прикладные аспекты. – М. : Тесей, 2008. – 176 с.