Демьянов А.А.
к.э.н. соискатель кафедры «Менеджмент» ВЗФЭИ

Информационный риск как угроза эффективности функционирования предприятия

Аннотация
В данной статье рассмотрен информационный риск представляющий угрозу для эффективности функционирования предприятия. Предложен комплексный подход по противодействию данному риску.
Ключевые слова
Информационный риск; конфиденциальная информация; коммерческая тайна

Summary
In given article it is considered information risk representing threat for efficiency of functioning the enterprises. The complex approach is offered on counteraction to the given risk.
Keywords
Information risk; the confidential information, a trade secret

Возникновение необходимости защиты сведений, связанных с производством, управлением, технологиями, финансами и т.д., в основном обязано появлению конкуренции между предприятиями, причем многочисленных фактов недобросовестной конкуренции, что, в свою очередь, предопределило недоверие между партнерами.

Сохранность производственных и коммерческих тайн - это важное условие получения предприятием максимальной прибыли и предотвращения ущерба.

Под **коммерческой тайной** в отечественной литературе принято понимать не относящиеся к государственным секретам сведения, знания и опыт, являющиеся собственностью предприятия и связанные с научными исследованиями, разработками, производством, сбытом, эксплуатацией, обслуживанием, информацией, управлением, финансами и иной деятельностью, которые имеют практическую ценность, могут быть использованы, носят конфиденциальный характер и разглашение (передача, утечка) которых может нанести материальный или моральный ущерб [1].

К таковым можно отнести любые сведения, которые прямо или косвенно,

полностью или частично раскрывают сущность состояния или перспективы создания, использования, внедрения, сбыта, производства и эксплуатации коммерческого продукта и содержатся в различной научной, технологической, патентной, лицензионной, правовой, финансовой и т.п. документации. Информацию, составляющую коммерческую тайну, следует дифференцировать таким образом:

- строго конфиденциальная - утрата которой может повлечь дестабилизацию деятельности или банкротство (например, ноу-хау, проблемы предприятия и т.д.);
- конфиденциальная - обеспечивающая устойчивую прибыль (например, сведения о перспективе развития, клиентуре, кредитовании и т.д.);
- не подлежащая огласке, т.к. ее разглашение нанесет вред положению на рынке (например, сведения о поставщиках, производстве, каналах сбыта, конфликтах и т.д.).

Пренебрежение вопросами защиты сведений, связанных с производством, технологией, управлением, финансами и др., может привести к серьезным негативным последствиям в случае утечки информации. Из зарубежного опыта известно, что в результате подобных действий можно потерять до 30 % возможной прибыли. Согласно данным иностранных экспертов, ежегодный ущерб американского бизнеса от краж коммерческой тайны превышает 4 млрд. долларов. Опыт общения с руководителями российских предприятий подтверждает, что далеко не все они осознали необходимость защиты своих производственных и коммерческих секретов. В большей мере это почувствовали пока руководители банковских учреждений. Основные каналы утечки конфиденциальной информации приведены на рис.1.

Рис 1. Основные каналы утечки конфиденциальной информации.

Под **раскрытием сведений, относящихся к коммерческой тайне,** следует понимать умышленные или неумышленные действия должностных лиц или иных работников предприятия, которые повлекли преждевременное, не

санкционированное руководителем открытое распространение или неправомерное использование имеющихся в их распоряжении сведений.

Действенным каналом несанкционированного съема конфиденциальной информации является кредитно-банковская система в настоящем ее состоянии (как, кстати, и система страхования).

Способствуют утечке конфиденциальной информации расширяющиеся связи преступных кругов с коррумпированными должностными лицами в структурах власти и управления, правоохранительных и контролирующих органах .

Проблема создания, сохранения, использования и коммерческой реализации интеллектуальной собственности относится к категории стратегических. От ее решения зависит не только экономическое благосостояние каждого промышленного предприятия, научного учреждения, но и государства. Обладая достаточным интеллектуальным потенциалом и рассчитывая на коммерческий успех в условиях реальной конкуренции, российские предприятия должны заботиться о создании эффективной системы защиты коммерческой тайны на основе гибкого сочетания организационных мер и ответственности должностных лиц.

Основными методами защиты информации, согласно общепринятой классификации, являются патентование и засекречивание. Патентование предполагает открытую публикацию сведений об изобретении и осуществляется с целью получения прибыли в случае использования изобретений третьими лицами.

Засекречивание сведений заключается в установлении, путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта, исходя из баланса жизненно важных интересов государства, общества, граждан.

Институт коммерческой тайны, получившей широкое распространение в промышленности, регламентируется рядом законов («О конкуренции и ограничении монополистической деятельности на товарных рынках» от 22 марта 1991г. № 948-1, «Об информации, информатизации и защите

информации» от 20 февраля 1995г. № 24-ФЗ, «О коммерческой тайне» от 29 июля 2004 года № 98-ФЗ и др.) [2].

Для устранения данного риска или значительного снижения вероятности его проявления необходим комплексный подход, как к самой конфиденциальной информации, так и к источникам владения ею. Вопрос защиты конфиденциальной информации предприятия в основе своей решается организационными методами и не требует капитальных вложений, в то время как результат успешно поставленной организационной работы позволяет поднять на качественно новый уровень экономическую безопасность предприятия.

Причиной данного риска является сама конфиденциальная информация, представляющая определенный интерес для потенциальных конкурентов и иных лиц, обладание которой позволяет им добиться определенных ранее намеченных целей. ледствием данной причины являются определенные действия со стороны заинтересованных лиц по получению конфиденциальной информации, а также неумышленная утечка ввиду отсутствия или слабого контроля за ее защитой.

Для успешного решения проблемы утечки конфиденциальной информации на предприятии, помимо патентования и засекречивания, необходимо [3]:

1. При приеме на работу новых работников предъявлять требования не только к их профессиональным, но и к человеческим качествам в плане умения хранить полученную информацию, грамотно работать с секретной коммерческой документацией, уметь предвидеть ситуации, при которых может произойти несанкционированный съем информации, составляющей коммерческую тайну.

2.Заблаговременно, до начала работы, ознакомить сотрудников предприятия с перечнем сведений, носящих конфиденциальный характер, порядком обращения с документами, имеющими прямое или косвенное отношение к данной информации, возможными негативными ситуациями и путями выхода из них.

3.Заключение договора в письменной форме со всеми работниками предприятия о неразглашении доверенных им по службе или работе либо ставших им известными другим путем сведений, несущих конфиденциальную информацию. Договор также обязывает каждого работника после увольнения с предприятия соблюдать принятые на себя обязательства о неразглашении конфиденциальной информации в течение определенного времени.

4.Со стороны руководства необходим строгий контроль за соблюдением всеми работниками и служащими порядка доступа, обращения и использования сведений, составляющих коммерческую тайну, и их носителей, а также принятие мер по обеспечению сохранности информации, носящей конфиденциальный характер и составляющей коммерческую тайну.

5.При заключении договоров с потенциальными партнерами, в процессе исполнения которых будет прямо или косвенно предоставляться определенная часть информации, носящей конфиденциальный характер, необходимо заключение между двумя сторонами договора о неразглашении данной информации.

6.Государственным и иным органам следует предоставлять только ту информацию, на доступ к которой они имеют право в соответствии с действующим законодательством Российской Федерации.

Подводя итог вышеизложенному, можно сделать вывод, что информационный риск, выраженный в возможности утечки конфиденциальной информации, несет в себе серьезную угрозу дестабилизирующей направленности для эффективности функционирования предприятия.

Литература

1.Большой экономический словарь. М., Книжный мир,2004. А.Б. Борисов.
2.Федеральный закон РФ «О государственной тайне» (ст. 6).
3.Черкасов В. Н. Бизнес и безопасность. Комплексный подход. М., «Аркада-пресс», 2001.