УДК 331

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА В АСПЕКТЕ РАБОТЫ С ПЕРСОНАЛОМ

© 2009 Д.А. Гаврилин, О.Л. Романова, О.В. Зимовец*

Ключевые слова: безопасность, субъект, персонал, руководство, работники, предприятие, государство, тайна, коммерческая тайна, информация.

Рассматриваются проблемы обеспечения экономической безопасности хозяйствующего субъекта и необходимые меры, принимаемые в организации, относительно найма, деятельности и увольнения работников.

Рыночная экономика актуализировала проблему обеспечения экономической безопасности для различных хозяйствующих субъектов (ХС)[1]. Предприятия, организации заботятся об обеспечении своей экономической безопасности.

Главная цель обеспечения экономической безопасности ХС - обеспечение его устойчивого и максимально эффективного функционирования в сложившихся условиях, создание высокого потенциала развития и роста ХС в будущем.

Подобное понимание экономической безопасности ХС позволяет показать, что любой его вид (производственное предприятие, банк и др.), находясь в ситуации неопределенности, изменения, как внутренних условий хозяйствования, так и внешних: политических, макроэкономических, экологических, правовых, - принимает рисковые решения в условиях жесткой конкуренции; добивается предотвращения, ослабления или защиты от существующих или прогнозируемых опасностей и угроз; в данных условиях обеспечивает достижение целей бизнеса. Ресурсы ХС используются не только для предотвращения опасностей и угроз, но и, прежде всего, для достижения поставленных целей бизнеса.

Российские организации вынуждены адаптироваться к условиям политической и социально-экономической нестабильности и вести поиск адекватных решений сложнейших проблем и путей снижения угроз своему функционированию. В результате перед большим количеством экономических субъектов России стоит проблема создания системы экономической безопасности, способной обеспечить снижение уровня угроз деятельности компаний в ключевых финансово-экономических сферах.

Экономическая безопасность ХС складывается из нескольких функциональных составляющих, которые для каждого конкретного ХС могут иметь различные приоритеты в зависимости от характера существующих угроз. Основным фактором, определяющим состояние экономической безопасности, является обладание ХС устойчивыми конкурентными преимуществами, которые должны соответствовать стратегическим целям ХС.

Практической задачей формирования концепции экономической безопасности для ХС является анализ примеров и ситуаций, складывающихся в отношениях и взаимоотношениях хозяйствующих субъектов, институтов. Пути решения включают идентификацию угроз и потерь, позволяющую предлагать меры по их преодолению.

В результате вырабатывается стратегия обеспечения экономической безопасности. Стратегия представляет собой программу действий, набор экономических технологий, которые предназначены для достижения поставленных целей.

Таким образом, безопасность хозяйствующего субъекта представляет собой состояние защищенности его жизненно важных интересов от недобросовестной конкуренции, противоправной деятельности криминальных формирований и от отдельных лиц, способность противостоять внешним и внутренним угрозам, сохранять стабильность функциони-

* Гаврилин Дмитрий Александрович, аспирант Саратовского государственного технического университета; Романова Ольга Леонидовна, кандидат экономических наук, доцент Саратовского государственного технического университета; Зимовец Олег Владимирович, кандидат экономических наук, доцент Тольяттинского государственного университета сервиса. e-mail: vestnik@sseu.ru.

рования и развития в соответствии с уставными целями.

Внешние угрозы ХС - негативные воздействия, возникающие без участия и помимо воли организации или ее служащих. Внутренние угрозы ХС - негативные воздействия, возникшие как следствие неэффективной работы организации в целом или ее работников в частности. Каждый из видов экономической безопасности ХС характеризуется собственным содержанием - набором функциональных критериев и способов обеспечения.

Среди видов экономической безопасности, проявляющихся в деятельности хозяйствующего субъекта, можно выделить следующие:

1) финансовую;
2) физическую;
3) технико-технологическую;
4) политико-правовую;
5) интеллектуальную и кадровую;
6) информационную.

Работа с персоналом - важнейший элемент обеспечения экономической безопасности. Интеллектуальная и кадровая составляющие экономической безопасности связаны с предотвращением негативных воздействий на экономическую безопасность ХС за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом. В современных экономических условиях уровень экономической безопасности в большей мере зависит от квалификации и профессионализма кадров. На предприятии должна быть создана гибкая структура управления, организована система подбора, найма, обучения и мотивации труда работников. Управленческому персоналу ХС необходимо постоянно анализировать состояние экономической безопасности. Кроме того, персонал также должен быть обучен действиям в условиях возникновения кризисных ситуаций.

Кадровый аспект экономической безопасности связан с информационной безопасностью, которая заключается в защите собственной информации, в том числе конфиденциальной, проведении деловой разведки, информационно-аналитической работы с внешними и внутренними субъектами и т.д. Хозяйствующий субъект должен иметь в своем составе определенные службы, которые должны заниматься накоплением и защитой информации, что также предполагает соответствующий персонал. Целью этих служб является накопление всей необходимой информации, касающейся деятельности того или иного субъекта хозяйствования (информация обо всех видах рынков, необходимая техническая информация, о тенденциях развития национальной и мировой экономики). Накопление полученных данных связано с анализом, и результатом этого анализа должен стать прогноз тенденций развития научно-технических, экономических и политических процессов в организации или на предприятии.

При формировании структур, обеспечивающих экономическую безопасность, следует учитывать внешние и внутренние угрозы интеллектуальной и кадровой безопасности.

Информационная безопасность в системе экономической безопасности связана также с рядом угроз, вызванных разными факторами, в том числе и с деятельностью персонала.

Нежелательное использование информационных ресурсов может быть произведено с помощью:

- неофициального доступа к конфиденциальной информации;
- подкупа лиц, работающих в ХС (например, в банке);
- прослушивания конфиденциальных переговоров;
- утечки информации, происходящей через переговорные процессы между руководителями ХС и иностранными или отечественными фирмами.

Экономическая безопасность организации может быть обеспечена, если будут определены важнейшие стратегические направления по безопасности бизнеса, построена четкая схема своевременного обнаружения и ликвидации возможных опасностей и угроз.

Для создания надежной системы безопасности ХС необходимо провести комплекс подготовительных мероприятий. От этого во многом зависят решения, принимаемые в этой области.

В целях сохранения коммерческой тайны целесообразно строить работу отделов, использующих конфиденциальную информа-

цию, в условиях максимальной изолированности друг от друга, с тем, чтобы каждый сотрудник знал только свою часть информации и не располагал сведениями, составляющими коммерческую тайну банка в целом. Основными источниками конфиденциальной информации являются люди, документы и информационные сети.

Противодействие огласке или хищению конфиденциальной информации посредством персонала основывается в первую очередь на профилактической работе, проводимой с персоналом. Направления работы могут касаться:

- организации процедуры приема на работу, ознакомление с правилами работы с коммерческой тайной (КТ) и юридическим фиксированием ответственности за ее разглашение;
- организации контроля и наблюдения за сотрудником в процессе его работы в банке;
- организации и контроля за допуском сотрудников к информации определенного уровня, а также к местам ее хранения.

Допуск сотрудников к информации определенной категории секретности осуществляется руководителем организации, его заместителями, руководителями структурных подразделений. Доступ в помещения и к технике, содержащие коммерческую тайну, должен быть строго персонифицирован. Важным условием обеспечения безопасности конфиденциальной информации является четкое регламентирование порядка общения с прессой и проведения PR-акций в целом.

Проблемы, связанные с защитой технических информационных каналов, компьютерных сетей зависят в первую очередь от степени информатизации организации. Необходимо четко знать технологии, которые необходимы той или иной организации. Защита технических каналов начинается с оборудования офиса соответствующими средствами блокирования возможной утечки.

Необходимо учитывать порядок работы с внутренними и внешними сетями. Для внутренних сетей выполняются следующие виды мероприятий в целях защиты от несанкционированного доступа: контроль надежности защиты, защита технических средств, учет технических средств. Проблемы информационной безопасности возникают при общении во внешних сетях с партнерами и контрагентами. Компьютерные преступления в банковской сфере во многом обусловлены постоянной связью автоматизированных систем банков, обслуживающих огромное количество платежей и пользователей. В связи с предоставлением новых банковских услуг, необходимостью вести расчеты с клиентами и корреспондентами в режиме реального времени открытость информационных и платежных систем объективно увеличивается. Эксплуатация стандартной техники и программного обеспечения способствует совершению преступлений путем введения фальшивых сведений в базы данных. Стандартными средствами защиты от внешнего проникновения являются антивирусные программы, сетевые экраны, виртуальные частные сети.

Определение необходимости проставления грифа “коммерческая тайна” (“КТ”) производится на основании перечня сведений, составляющих коммерческую тайну. На документах, делах, изданиях, содержащих коммерческую тайну, проставляется гриф “КТ” с указанием ее обладателя, а в документах и изданиях, кроме того, количество экземпляров и их номер. Документы, дела и издания с грифом “КТ” должны храниться в специальных охраняемых и технически контролируемых помещениях в условиях, обеспечивающих их физическую сохранность. Документы, содержащие информацию, составляющие КТ, регистрируются либо в службе экономической безопасности (СЭБ), либо в общем делопроизводстве уполномоченным сотрудником СЭБ. Снятие копий, производство выписок с документов и изданий с грифом “КТ” осуществляется только по разрешению руководителей подразделений под контролем сотрудников СЭБ. Проверки соблюдения режима работы с материалами с грифом “КТ” проводятся не реже 1 раза в год сотрудниками СЭБ, имеющими допуск к материалам. Проверки проводятся в присутствии руководителя соответствующего структурного подразделения. В случае установления факта утраты документов с грифом “КТ” СЭБ проводит по данному факту внутреннее расследование, результаты которого докладываются руководителям системы безопасности и самой организации. Уничтожение документов с грифом “КТ” производится по реше-

нию руководителя специально назначенной комиссией, обязательно включающей уполномоченного сотрудника СЭБ и руководителя соответствующего структурного подразделения.

В процессе пересылки целесообразно применять средства обнаружения несанкционированного доступа к корреспонденции, а также использовать двойной пакет, когда опечатанные пакет с секретной корреспонденцией находится внутри другого опечатанного пакета, причем реквизиты истинного адресата указаны только на внутреннем пакете.

Личные нормы проведения при работе с документами с грифом "КТ" предписывают не допускать к этим документам посторонних лиц, не держать на столе сразу несколько документов различной степени значимости, при отлучках из комнаты убирать документы в сейф.

Прием на работу связан с проведением собеседования, число которых варьируется в зависимости от конкретных обстоятельств. В ходе отбора на ключевые должности могут использоваться тестирование (выявление типа личности, аналитических способностей, логического мышления), а также специальные методы - экспертиза почерка и т.п.

Кроме вышеназванных, важной целью СЭБ в рамках работы с персоналом является получение верифицированной информации о действиях и намерениях сотрудников. Информация о том, как исполняется политика руководства на нижних звеньях - это необходимое условие принятия управленческих решений. Организация СЭБ получает информацию о происходящих в организации нарушениях в среде персонала (этот вид деятельности в службе безопасности занимает особое место).

Важным элементом работы СЭБ по персоналу является и момент увольнения сотрудника: специалисты отдела кадров и производящие увольнение менеджеры должны найти возможность сохранения психологического контакта с сотрудником во избежание разглашения конфиденциальной информации с его стороны после увольнения. В этих целях проводится доверительная беседа, например, в форме обмена мнениями.

Минимизация рисков, связанных с увольнением сотрудников, основывается на следующих правилах:

♦ увольнять сотрудников нужно таким образом, чтобы у них не оставалось психологических причин для мести;

♦ необходимо построить технологию профилактики проблем, связанных с увольнением тех или иных работников.

Обеспечение всей системы мероприятий по работе с персоналом, позволяет снизить угрозу в организации деятельности хозяйствующего субъекта.

---

[1] См.: *Сенчагов В.К.* Экономическая безопасность России. М., 2005. С. 741; Что такое кадровая безопасность компании // Кадры предприятия. 2004. □ 2; *Завгородний В.И.* Комплексная защита информации в компьютерных системах. М., 2001. С. 17-19; *Судоплатов А.П., Лексаре С.В.* Безопасность предпринимательской деятельности. М., 2001. С. 206-208.