

У.Т.Хайитматов,
иқтисод фанлари номзоди, доцент,
О.Х.Азаматов, Р.Р.Мажидов,
А.Ф.Хакимов, ТГЭУ

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ В СОВРЕМЕННОМ БИЗНЕСЕ

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Так, постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; а также решаются некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

Немаловажную роль в развитии предприятия играет его экономическая безопасность. Экономическая безопасность предприятия – это состояние его защищенности от негативного влияния внешних и внутренних угроз, дестабилизирующих факторов, при котором обеспечивается устойчивая реализация основных коммерческих интересов и целей уставной деятельности.

Для каждого предприятия «внешние» и «внутренние» угрозы сугубо индивидуальны. Вместе с тем, на наш взгляд, указанные категории включают отдельные элементы, которые приемлемы практически к любому субъекту хозяйственной деятельности.

К внешним угрозам и дестабилизирующим факторам можно отнести противоправную деятельность криминальных структур, конкурентов, фирм и частных лиц, занимающихся промышленным шпионажем либо мошенничеством, несостоятельных деловых партнеров, ранее уволенных за различные проступки сотрудников предприятия, а также правонарушения со стороны коррумпированных элементов из числа представителей контролирующих и правоохранительных органов.

К внутренним угрозам и дестабилизирующим факторам относятся действия или бездействия (в том числе умышленные и неумышленные) сотрудников предприятия, противоречащие интересам его коммерческой деятельности, следствием которых могут быть нанесение экономического ущерба компании, утечка или утрата информационных ресурсов (в том числе сведений, составляющих коммерческую тайну и/или конфиденциальную информацию), подрыв ее делового имиджа в бизнес-кругах, возникновение проблем во взаимоотношениях с реальными и потенциальными партнерами (вплоть до утраты важных контрактов), конфликтных ситуаций с представителями криминальной среды, конкурентами, контролирующими и

правоохранительными органами, производственный травматизм или гибель персонала и т.д.

Количественный и качественный анализ перечисленных выше угроз позволяет сделать вывод о том, что надежная защита экономики любой компании возможна только при комплексном и системном подходе к ее организации. В связи с этим в лексиконе профессионалов, занимающихся обеспечением безопасности бизнеса коммерческих структур, появился термин «Система экономической безопасности» предприятия.

Системой экономической безопасности предприятия (СЭБ) является комплекс организационно-управленческих, режимных, технических, профилактических и пропагандистских мер, направленных на качественную реализацию защиты интересов предприятия от внешних и внутренних угроз.

К числу основных задач СЭБ любой коммерческой структуры относятся:

- защита законных прав и интересов предприятия и его сотрудников;
- сбор, анализ, оценка данных и прогнозирование развития обстановки;
- изучение партнеров, клиентов, конкурентов, кандидатов на работу в компании;
- своевременное выявление возможных устремлений к предприятию и его сотрудникам со стороны источников внешних угроз безопасности;
- недопущение проникновения на предприятие структур экономической разведки конкурентов, организованной преступности и отдельных лиц с противоправными намерениями;
- противодействие техническому проникновению в преступных целях;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников предприятия в ущерб его безопасности;
- защита сотрудников предприятия от насильственных посягательств;
- обеспечение сохранности материальных ценностей и сведений, составляющих коммерческую тайну предприятия;
- добывание необходимой информации для выработки наиболее оптимальных управленческих решений по вопросам стратегии и тактики экономической деятельности компании;
- физическая и техническая охрана зданий, сооружений, территорий и транспортных средств;
- формирование среди населения и деловых партнеров благоприятного мнения о предприятии, способствующего реализации планов экономической деятельности и уставных целей;
- возмещение материального и морального ущерба, нанесенного в результате неправомерных действий организаций и отдельных лиц;
- контроль за эффективностью функционирования системы безопасности, совершенствование ее элементов.

С учетом перечисленных задач, условий конкурентной борьбы, специфики бизнеса предприятия строится его система экономической безопасности. Необходимо отметить, что СЭБ каждой компании также сугубо индивидуальна. Ее полнота и действенность во многом зависят от имеющейся в государстве

законодательной базы, выделяемых руководителем предприятия материально-технических и финансовых ресурсов, понимания каждым из сотрудников важности обеспечения безопасности бизнеса, а также от знаний и практического опыта начальника СЭБ, непосредственно занимающегося построением и поддержанием в «рабочем состоянии» самой системы.

Построение СЭБ предприятия должно осуществляться на основе соблюдения принципов законности, прав и свобод граждан, централизованного управления, компетентности, конфиденциальности, разумной достаточности, соответствия внешним и внутренним угрозам безопасности, комплексного использования сил и средств, самостоятельности и ответственности за обеспечение безопасности, передовой материально-технической оснащенности, корпоративной этики, координации и взаимодействия с органами власти и управления.

К основным элементам СЭБ предприятия относятся: защита коммерческой тайны и конфиденциальной информации, компьютерная безопасность, внутренняя безопасность, безопасность зданий и сооружений, физическая безопасность, техническая безопасность, безопасность связи, безопасность хозяйственно-договорной деятельности, безопасность перевозок грузов и лиц, безопасность рекламных, культурных, массовых мероприятий, деловых встреч и переговоров, противопожарная безопасность, экологическая безопасность, радиационно-химическая безопасность, конкурентная разведка, информационно-аналитическая работа, пропагандистское обеспечение, социально-психологическая, предупредительно-профилактическая работа среди персонала и его обучение по вопросам экономической безопасности, экспертная проверка механизма системы безопасности.

В настоящее время все большую актуальность приобретает защита интересов предприятия от противоправной деятельности коррумпированных представителей контролирующих и правоохранительных органов. В связи с этим, данное направление работы многими начальниками служб экономической безопасности коммерческих структур выделяется в качестве отдельного элемента СЭБ.

Основной смысл подобной системы состоит в том, что она должна носить упреждающий характер, а основными критериями оценки ее надежности и эффективности являются:

- обеспечение стабильной работы предприятия, сохранности и приумножения финансов и материальных ценностей;
- предупреждение кризисных ситуаций, в том числе различных чрезвычайных происшествий, связанных с деятельностью «внешних» и /или «внутренних» недоброжелателей.

Особенностью и, одновременно, сложностью при построении системы экономической безопасности является тот факт, что ее действенность практически полностью зависит от человеческого фактора. Как показывает практика, даже при наличии на предприятии профессионально подготовленного начальника службы безопасности, современных технических средств, Вы не добьетесь желаемых результатов до тех пор, пока в Вашем коллективе каждый

сотрудник не осознает важность и необходимость внедряемых мер экономической безопасности.

А они будут не популярны:

- кто-то утратит возможность в рабочее время или после работы развлекаться в Интернете, скачивать музыку и иную информацию, читать книги в электронном варианте и т.д.;

- кому-то покажется в тягость один раз в неделю менять пароль на своем компьютере;

- кто-то посчитает ниже своего достоинства всякий раз подниматься для того, чтобы уничтожить черновик в бумагорезательной машинке, убрать со стола документы и закрыть окно после окончания рабочего дня, опечатавать и сдавать свой рабочий кабинет под роспись в журнале службе охраны;

- у кого-то исчезнет возможность приводить на работу (в том числе и по выходным дням) своих друзей либо бахвалиться на стороне личными достижениями в работе или успехами фирмы;

- некоторые не смогут использовать служебные автотранспорт и мобильный телефон в личных целях, а также часами вести личные разговоры по служебным проводным каналам телефонной связи и т.д.

Поэтому для юридически правильного, эффективного и всестороннего использования СЭБ в защите интересов предприятия от всех видов недоброжелателей требования по обеспечению безопасности бизнеса излагаются в соответствующих приказах руководителя, трудовых договорах с сотрудниками и их должностных обязанностях, специальных инструкциях, положениях, контрактах с деловыми партнерами и т.д. После чего доводятся до персонала под роспись в процессе занятий и инструктажей.

В вопросах экономической безопасности как никогда важна роль и понимание актуальности проблемы в первую очередь, самим руководителем предприятия. Директор и, при наличии, начальник службы безопасности, должны пропагандировать среди персонала одно из основных корпоративных правил: «Фирма - это твоя вторая семья. Предприятие дает всем сотрудникам работу, материальные блага, перспективы служебного роста и т.д. В связи с этим задача каждого сотрудника - приумножать успех и материальное положение компании (как и своей семьи). Ведь успех предприятия - это стабильность и перспективы его персонала».

Вместе с тем, как показывает практика, кто-то из Ваших сотрудников может не выполнять установленные в компании требования или допускать ошибки по забывчивости, кто-то по неаккуратности, а кто-то - из мести. У кого-то могут возникнуть финансовые затруднения в связи с болезнью близких или в связи с проигрышем в казино, и он решит их «компенсировать» за счет фирмы. Кто-то посчитает, что был незаслуженно наказан директором, что давно достоин повышения в должности или что его вклад в деятельность компании заслуживает гораздо более высокой зарплаты, а руководство этого не замечает и т.д.

Словом, с возрастом, изменением социального статуса, материального благосостояния, появлением вредных наклонностей, а также при

возникновении некоторых объективных обстоятельств люди могут меняться либо вести себя неадекватно.

При этом необходимо понимать, что в вопросах обеспечения экономической безопасности «второстепенных» должностных лиц нет, а есть только особенности (в связи с выполняемыми каждым из сотрудников функциями и обязанностями).

С учетом выше изложенного, можно сделать вывод о том, что СЭБ предприятия только тогда будет соответствовать предъявляемым к ней требованиям, когда весь персонал понимает важность обеспечения безопасности компании и сознательно выполняет все установленные указанной системой требования.

Достигается же данная цель в результате проведения непрерывной, кропотливой воспитательной и профилактической работы с сотрудниками предприятия, их обучения и специальной подготовки по вопросам действующего законодательства и различным аспектам экономической безопасности.

В современных условиях процесс успешного функционирования и экономического развития предприятий во многом зависит от совершенствования их деятельности в области обеспечения экономической безопасности. В качестве основных факторов, отрицательно влияющих на безопасность предпринимательской деятельности можно выделить следующие:

- активное участие представителей власти и управления в коммерческой деятельности;
- использование криминальных структур для воздействия на конкурентов;
- отсутствие законов, позволяющих в полном объеме противодействовать недобросовестной конкуренции;
- отсутствие в стране благоприятных условий для проведения научно-технических исследований;
- отсутствие подробной и объективной информации о субъектах предпринимательской деятельности и об их финансовом положении;
- отсутствие культуры ведения дел в предпринимательской среде;
- применение оперативных и технических методов с целью получения нужной информации о конкурентах.

Следует отметить, что сегодня не все руководители предприятий готовы в полной мере оценить необходимость создания надежной системы экономической безопасности. Понятие «безопасность» определяется как состояние защищенности жизненно важных интересов. Однако в общественном сознании все еще сильны стереотипы, согласно которым данная область относится многими к сфере компетенции государства и специальных органов. Именно в этом таятся корни «слабого» понимания специфики этих проблем, прежде всего, первыми руководителями предприятий и организаций, отнесение их к не основной деятельности.

Особенно же сложно бывает определить конкретные действия, необходимые для защиты тех или иных жизненно важных ресурсов. Вследствие этого, многие руководители ограничиваются созданием на предприятии

охранных структур, почти полностью исключая из арсенала организационно - технические и правовые методы, средства и способы защиты информации.

В итоге, например, вопросы защиты коммерческой тайны нередко упускаются в лицензионных соглашениях, договорах подряда на создание научно-технической продукции, что приводит к утечке коммерчески значимой информации.

Меры обеспечения сохранности информации на отдельном предприятии могут быть различны по масштабам и формам и зависит от производственных, финансовых и иных возможностей предприятия, от количества и качества охраняемых секретов. При этом, выбор таких мер необходимо осуществлять, исходя их принципа разумной достаточности, придерживаясь в финансовых расчетах «золотой середины», так как чрезмерное закрытие информации, так же как и халатное отношение к ее сохранению, могут вызвать потерю определенной доли прибыли или привести к серьезным убыткам.

Итак, проект обеспечения экономической безопасности объекта представляет собой единый организационно-технический комплекс, в ходе формирования которого разрабатывается концепция обеспечения безопасности объекта или политика безопасности. Ее основу составляет перечень обязательных мероприятий, направленных на выработку плана действий по защите объекта: определение состава службы безопасности (СБ), ее место в организационной структуре предприятия, сфера ее компетенции, права и полномочия, варианты действий в различных ситуациях во избежание конфликтов между подразделениями. Их подоплека обычно лежит как раз в том, что многие считают требования, предъявляемые СБ, необоснованно завышенными либо из-за того, что СБ «везде сует свой нос».

Соблюдение вышеизложенных условий позволит ликвидировать почву для подобных ситуаций или разрешать их быстро и безболезненно. Политика экономической безопасности определяет правильный с точки зрения организации способ использования коммуникационных и вычислительных ресурсов, правила доступа на объект, правила обращения с конфиденциальной информацией, а также процедуры предотвращения нарушений режима безопасности и реагирования на них.

Следует отметить, что эффективность политики безопасности только тогда будет находиться на должной высоте, когда ее реализация будет представлять собой результат совместной деятельности сотрудников организации, способных понять все ее аспекты, и руководителей, способных влиять на ее претворение в жизнь.

Не менее важным фактором, влияющим на действенность политики безопасности, представляется готовность персонала к выполнению ее требований, доведение до каждого его обязанностей по поддержанию режима безопасности. Соблюдение политики безопасности должно гарантироваться наличием ответственного по каждому виду проблем.

Разумеется, все основные положения политики безопасности должны быть закреплены в соответствующих распорядительных документах, состав и содержание которых определяются спецификой объекта.

Однако, как правило, ни одна организация не сможет обойтись без положений о коммерческой тайне, о защите информации, об администраторе, безопасности сети, правил, разграничивающих доступ к информации, содержащейся в автоматизированных системах, правил допуска персонала и посетителей в помещения, где производится обработка критичной информации, порядка проведения служебного расследования по факту нарушения правил безопасности.

Работы по оснащению и поддержке деятельности системы защиты информации, создание системы распорядительных документов входят в комплекс организационных мер, на основе которого может быть достигнут высокий уровень безопасности информации.

Тем не менее, перечисленные меры не позволяют на должном уровне поддерживать функционирование системы защиты без проведения целого ряда организационно-технических мероприятий. Их полный перечень слишком широк для того, чтобы полностью приводить его в данной статье, скажем лишь, что они позволяют своевременно выявлять новые каналы утечки информации, принимать меры по их нейтрализации, совершенствованию системы защиты и оперативно реагировать на нарушения режима безопасности.

Разработанные документы определяют функции, необходимые для организации работы СБ, а также контрольно-проверочные и другие специальные функции, осуществляемые ею в процессе деятельности. Основными функциями являются:

- административно - распорядительная - подготовка решений по поддержанию режимов безопасности и конфиденциальности; определению положений, прав, обязанностей и ответственности должностных лиц по вопросам безопасности, а также по осуществлению представительских функций предприятия в данной области ее деятельности;

- хозяйственно - распорядительная - определение (совместно с другими подразделениями предприятия) ресурсов, необходимых для решения задач по обеспечению безопасности предприятия, подготовка и проведение мероприятий организационно - технического и правового характера, направленных на сохранность его собственности, в том числе интеллектуальной;

- учетно-контрольная - определение критически важных направлений финансово-экономической, производственно - коммерческой и других видов деятельности, подлежащих защите, а также возможных каналов утечки информации и других угроз финансовой стабильности и устойчивости предприятия, оценка источников их возникновения; налаживание действенного контроля;

- организационно-техническая - создание организационной структуры СБ, а также других структур по отдельным направлениям работы (защита информации, экономическая безопасность); организация взаимодействия между отдельными структурными подразделениями предприятия, способствующими достижению целей политики безопасности;

- планово-производственная - разработка комплексных программ и отдельных планов обеспечения безопасности предприятия, подготовка и проведение соответствующих мероприятий;

- материально-техническая - направляемая на материально-техническое и технологическое обеспечение деятельности СБ, оснащение ее специальной техникой;

- научно-методическая - накопление и распространение передового опыта в области обеспечения безопасности; организация обучения сотрудников других подразделений (в необходимом им объеме);

- информационно-аналитическая - сбор, накопление и обработка данных, относящихся к сфере безопасности, создание и использование необходимых для этого технических и методических средств.

Тем не менее, следует иметь в виду, что обеспечение СБ надежным инструментарием, грамотная расстановка приоритетов ее деятельности, как и всякая квалифицированная работа, требует участия в ней специалистов, имеющих соответствующую профессиональную подготовку и, что не менее важно, обладающих достаточно большим практическим опытом в этой области. Систему безопасности предприятия должны создавать профессионалы, а сотрудничество с ними может быть плодотворным, только если оно долгосрочное.

В условиях рыночной экономики от руководителей предприятий требуется не только разработка рыночной стратегии, но и стратегия безопасности, обязательно включающей специальные программы по защите интеллектуальной собственности и экономической безопасности.

Соответственно, роль подразделения, ответственного за проведение данной работы на предприятии, выполняющего функции соблюдения правил политики безопасности и плана защиты, управления средствами защиты, контроля за правильностью их эксплуатации, выявления попыток и фактов нарушений и принятия мер по их нейтрализации, также выходит на первый план. Ослабление практически любой составляющей инфраструктуры предприятия непосредственно отражается на его безопасности, поэтому процесс управления предприятием находится в тесной взаимосвязи с вопросами безопасности.

В заключение можно сказать, что в интересах стабильного функционирования фирмы, предприниматели должны в тех или иных объемах заниматься обеспечением безопасности бизнеса или экономической безопасности. Размер, капиталоемкость, технологическая сложность и публичность бизнеса определяют лишь объем тех работ, которые предприниматели проводят по обеспечению безопасности бизнеса и их бюджет.

Не заботясь о соблюдении элементарных мер экономической безопасности бизнеса, фирма может оказаться на грани банкротства, например в результате неплатежей: любой выданный товарный кредит может повлечь за собой риск неплатежа, если не предприняты определенные меры по сбору минимальной информации о фирме, не проведена элементарная бизнес-разведка.

Участвуя в сделке в качестве покупателя или инвестора, необходимо проводить определенный набор процедур, цель которого – проверка

достоверности излагаемых о себе продавцом или получателем средств сведений. Безопасность бизнеса предполагает, что на фирме также должны быть продуманы определенные меры по снижению потерь, вызываемых действиями проверяющих структур, например в рамках оперативно-розыскной деятельности уполномоченных структур, которая также может закончиться для предпринимателя невосполнимыми потерями.

В любом случае вовремя проведенный профессиональный аудит безопасности позволит предприятию предотвратить большинство форс-мажорных затрат, направленных на ликвидацию последствий просчетов в обеспечении безопасности бизнеса.

Размер мероприятий по безопасности бизнеса индивидуален для каждого предприятия. Практика показывает, что зачастую причиной провалов в системе экономической безопасности фирмы служат некачественное юридическое сопровождение, или вообще его отсутствие. И наоборот, часто можно сделать вывод о том, что предприниматель, который уделил должное внимание обеспечению качественного юридического сопровождения своего бизнеса, а также добился высокой правовой дисциплины на различных участках работы, уже предпринял минимальный пакет мер по безопасности своего бизнеса.

Обид ака Азаматов

Ифн катта укиувчи