Современная концепция управления корпоративной безопасностью

И. А. Бородин,
президент МОО «АКБ», член-корреспондент РАЕН

Представление о корпоративной безопасности за последние годы претерпело ряд изменений. В начале девяностых годов прошлого века акцент делался на защиту (охрану) предпринимателями своей собственности и жизни. Это определялось высокой криминализацией бизнеса. Ведущим фактором угрозы был криминал. От него можно было защититься, используя инженерно-технические средства и физическую охрану. В этот момент появилось большое число частных охранных предприятий (ЧОП) и возник институт телохранителей. Это дало ожидаемый результат. Число нападений на объекты и хищений материальных ценностей существенно сократилось.

Постепенно, по мере развития рыночных отношений и усиления мер правового регулирования рынка, акцент стал переноситься в сферу экономики. Тяжелый налоговый пресс не давал бизнесменам возможности быстро развиваться в рамках правового поля. В этот период не было практически ни одного предприятия, которое работало бы без нарушений действующего налогового законодательства. Вследствие этого появляется масса схем законной и незаконной минимизации налогов. Естественно, что при таком положении дел серьезным «фактором угрозы» для бизнеса стали контролирующие и правоохранительные органы. Формально использование таких схем можно отнести к системе мер обеспечения экономической безопасности. Как и операции по возврату долгов. Эти мероприятия проводились преимущественно силовыми методами. Часто в их реализации активное участие принимали и сотрудники правоохранительных органов. Для решения данного круга задач на предприятиях и фирмах создавались службы безопасности, на которые были возложены обязанности по обеспечению, прежде всего, экономической и информационной безопасности.

В это же время произошли серьезные кадровые изменения в силовых структурах. Часть сотрудников уволилась, часть перешла в налоговую полицию и другие вновь образованные структуры. Предложение породило спрос. Большинство уволенных нашли применение своему опыту и знаниям в ЧОПах и коммерческих структурах в качестве руководителей служб безопасности. Следует отметить, что основным критерием отбора служило количество связей в силовых структурах, оставшихся у кандидата на должность. Таким вот методом «старых связей» удавалось находить нужные контакты в правоохранительных и контролирующих органах.

Вторым эффективным методом избежать санкций стали откупы.

Приход в коммерческие структуры бывших сотрудников силовых структур привел к тому, что службы безопасности стали по своей структуре напоминать мини-копии ФСБ или МВД. Данное обстоятельство не могло не отразиться и на методах работы.

Основное внимание при обеспечении безопасности стало уделяться построению системы охраны, защите информации и экономики. Многие бизнесмены считают, что, создав у себя службу безопасности и поставив во главе ее бывшего сотрудника ФСБ или МВД, они могут спать спокойно. В какой-то степени они правы. При том уровне развития рынка защита от «обороны» была наиболее эффективной.

С каждым годом методы защиты все более совершенствовались и к настоящему времени достигли высокого уровня развития. Сегодня наиболее типичной является система безопасности, состоящая из служб охраны, экономической, информационной, инженерно-технической безопасности. Каждое из перечисленных направлений имеет свою идеологию и своих идеологов. Это приводит к тому, что приверженцы каждого из них стараются доказать, что именно их направление является наиболее важным в обеспечении корпоративной безопасности, формально признавая при этом необходимость комплексного подхода.

Декларируемый авторами комплекс мер по обеспечению безопасности не является системой в реальности, так как не соответствует требованиям, предъявляемым к структурам подобного типа.

По мере развития рынка и совершенствования законодательства меняются и методы управления бизнес-структурами. Соответственно, должны меняться и подходы к обеспечению безопасности. Появилась объективная потребность в разработке новой концепции корпоративной безопасности. Основой новой концепции должен стать именно системный подход. Но прежде чем говорить о самой концепции, было бы целесообразно рассмотреть некоторые базовые понятия. К ним в первую очередь относится сам термин «безопасность».

Любую фирму или организацию можно рассматривать как частный случай открытой системы. Действительно, для того чтобы производить какой-либо продукт или услугу, организация должна взаимодействовать со средой и другими участниками рынка. Во внешней среде существуют две группы факторов: позитивные, то есть способствующие развитию бизнеса, и негативные – затрудняющие его развитие. Последние принято называть факторами угрозы из-за содержащейся в них опасности.

Специфика факторов угрозы со-

стоит в том, что, будучи объективно обусловленными, они не поддаются управлению ни со стороны служб безопасности ни со стороны каких-либо иных подразделений. Таким образом, у бизнес-структур возникает необходимость в разработке эффективной системы мер противодействия факторам угрозы в случае их актуализации.

Наиболее активными факторами угрозы в настоящее время по оценкам большого числа опрошенных нами бизнесменов в более чем 50 субъектах Федерации являются:

- конкуренты;
- коррумпированные элементы госструктур;
- криминал;
- техногенные катастрофы и природные катаклизмы.

Каждый из факторов угрозы ориентирован преимущественно на определенные объекты защиты (Рис. 1).

Рис. 1

Большинство бизнесменов из всех факторов угрозы на первое место ставят конкурентов. Следует отметить, что конкуренция – естественный и даже необходимый процесс в условиях рыночных отношений. Однако конкурентную борьбу в зависимости от используемых методов можно условно подразделить на белую, серую и черную.

«Белая» – добросовестная конкуренция; реализуется в форме соревнования в рамках действующего правового поля.

«Серая» – соперничество, первая форма недобросовестной конкуренции; реализуется с использованием приемов и методов, направленных на дискредитацию конкурента, производимого им товара или предоставляемых им услуг.

«Черная» – противоборство; ориентирована на уничтожение конкурента и осуществляется с использованием приемов и методов, противоречащих действующему законодательству.

В свою очередь, недобросовестная конкуренция порождает два новых фактора угрозы:

- промышленный шпионаж;
- рейд (недружественные поглощения).

Сами по себе эти факторы можно классифицировать как ситуативно активные. Их активность пропорциональна спросу на предлагаемые ими услуги. Чаще всего их активность возрастает при получении заказа. На рынке услуг они, как правило, представлены небольшими группами специалистов. Так, например, на проведении акций промышленного шпионажа специализируются частные детективные агентства, укомплектованные бывшими сотрудниками силовых структур. На рейде – специально ориентированные на эту деятельность фирмы и компании.

Существенное негативное влияние на развитие, прежде всего, субъектов малого и среднего бизнеса оказывают коррумпированные сотрудники многочисленных проверяющих и контролирующих органов, готовые за определенное вознаграждение закрыть глаза на выявленные в ходе проверок недостатки. В случаях недобросовестной конкуренции представители этого фактора угрозы могут стать пособниками одной из сторон, используя административный ресурс.

Что касается криминала, то бизнесмены разных уровней считают в настоящее время этот фактор угрозы менее значимым и наиболее предсказуемым.

Статистика последних лет свидетельствует о недостаточном внимании со стороны бизнесменов к такому фактору угрозы, как техногенные катастрофы.

В рамках данной статьи мы воздержимся от детального описания форм и методов воздействия отдельных факторов угрозы на объекты защиты – они нашли свое отражение в многочисленных публикациях по вопросам обеспечения корпоративной безопасности. Отметим только, что для эффективного противодействия им необходима соответствующая система корпоративной безопасности.

Возможная принципиальная схема такой системы приведена на рис. 2.

Предложенная схема нуждается в некоторых комментариях.

Прежде всего договоримся, что под корпоративной безопасностью мы будем понимать такое состояние системы (фирмы, организации, корпорации), при котором вероятность актуализации опасности, содержащейся в факторах угрозы, минимизирована. Данное обстоятельство означает, что в каждый конкретный момент времени корпоративная безопасность определяется некоторой численной величиной, находящейся в интервале 0÷1. В свою очередь, эта величина производна от текущего состояния поля угроз и эффективности функционирования системы корпоративной безопасности.

Суммарная угроза, дифференцированно воздействуя на объекты защиты, может представлять реальную опасность для уровня экономической, информационной или социальной безопасности. Соответствующие подсистемы корпоративной безопасности должны эффективно противодействовать тем составляющим суммарной угрозы, на борьбу с которыми они ориентированы. В результате совместной деятельности этих подструктур достигается интегральная корпоративная безопасность как некоторое системное качество. Интегральный (синергетический) эффект достигается за счет того, что отдельные подсистемы при решении своих специфических задач помогают друг другу. Действительно, при решении задач обеспечения экономической безопасности нельзя игнорировать ее информационную и социальную составляющую. В решении вопросов социальной безопасности существенная роль принадлежит вопросам защиты экономики и информации.

Обращаем внимание на два существенных момента.

Каждая подсистема имеет обратную связь, которая позволяет корректировать ее эффективность за счет использования внутренних ресурсов в случаях, когда реальный уровень безопасности оказывается ниже заданного.

В свою очередь, каждая из подсистем представляет собой минисистему, состоящую из большого числа элементов.

Принято считать, что вопросы обеспечения экономической безопасности являются прерогативой службы безопасности, однако кроме нее в этом процессе задействован и ряд других участников, в том числе:

- топ-менеджмент;
- служба внутреннего аудита;
- информационно-аналитическая служба;
- служба персонала;
- юридическая служба.

Аналогичная ситуация складывается в отношении информационной и социальной безопасности. Данное обстоятельство диктует необходимость пересмотра подходов как к построению самой системы безопасности, так и к принципам управления ею.

Рис. 2

Помимо факторов внешней угрозы, на уровень корпоративной безопасности фирмы существенное деструктивное влияние оказывают и факторы внутренней угрозы. Они также обладают объективной природой и фактически присутствуют в любых фирмах и организациях. При активизации эти факторы способны взорвать компанию изнутри. Они имеют сложную структуру и требуют к себе не меньшего внимания, чем ранее рассмотренные. Факторы внутренней угрозы имеют выраженный субъектный характер. За каждым из них стоит отдельный человек или группа лиц. При этом один и тот же сотрудник может одновременно рассматриваться в составе двух и более факторов угрозы. Последствия для фирмы в результате актуализации опасностей, содержащихся в различных факторах угрозы, могут существенно отличаться. На этом основании можно условно выстроить некую иерархию внутренних факторов угрозы (Рис. 3.):

На первом, верхнем уровне располагаются хозяева или учредители фирмы, так как именно они закладывают «ген смерти» в тело компании. Только собственник или учредитель знают, для чего и на какой срок создана фирма. Только они могут в любой момент отказаться от своего бизнеса или от контрольного пакета акций. От них зависит стратегия формирования концепции корпоративной безопасности фирмы.

Второй уровень составляют топ-менеджеры. От их профессионализма зависят как успехи фирмы, так и поражения. Одной из предпосылок активизации рейда в отношении фирмы является неэффективное управление. Часто положение усугубляется тем, что для Российского бизнеса характерно совмещение роли собственника с ролями генерального директора или президента компании. Развернутую характеристику опасностям, содержащимся в этом факторе угрозы, дал Сидни Финкельштейн в своей книге «Ошибки топ-менеджеров ведущих корпораций: Анализ и практические выводы». Он выделяет семь типичных ошибок, приводящих фирмы к гибели. Вот их краткие характеристики:

Привычка 1: считать, что вы и ваша компания не зависите от обстоятельств.

Как правило, руководители такого типа считают, что достигнутые командой успехи являются результатом их гениального руководства, и нет таких ситуаций, из которых они не смогут найти выхода. Уверенность в том, что они контролируют все факторы среды, в том числе и факторы угрозы. Данное добросовестное заблуждение может поставить компанию на грань гибели или банкротства.

Привычка 2: полностью отождествлять себя с компанией, теряя способность отличать личные интересы от корпоративных.

Данная привычка присуща многим российским бизнесменам и особенно тем из них, кто совмещает роли хозяина и топ-менеджера. В чем опасность такой ситуации? Одна из проблем, которые возника-

ют тогда, когда владелец основного пакета акций является одновременно и основным управляющим, заключается в том, что слишком крупный пакет акций дает руководителю слишком много власти, и никто не сможет остановить его в случае, если он выберет опасную или сомнительную стратегию.

Самое неприятное проявление «неделимости» – это чрезмерное отождествление себя, руководителя, со своей компанией. В этом случае у них развивается склонность использовать корпоративные фонды в личных целях.

Привычка 3: Уверенность в том, что знаешь ответы на все вопросы.

Такие руководители всегда демонстрируют глубокую осведомленность в вопросах, имеющих принципиальное значение. Они стремятся быстро разобраться в самой сложной ситуации и немедленно принять решение.

Однако их проблема заключается в том, что подобный имидж совершенного топ-менеджера является самообманом. В условиях постоянно меняющихся условий игры, характерных для российского рынка, всегда знать ответы на все вопросы не может никто. Подобная уверенность в собственной непогрешимости приводит к тому, что такой руководитель мало обращает внимания на мнения других людей и не особенно долго раздумывает над отдаленными последствиями своих решений. Кроме того, для них характерна сниженная потребность в повышении своей квалификации. Из всей доступной им информации они некритично отдают предпочтение той, которая подтверждает их точку зрения.

Привычка 4: без колебаний освобождаться от всех, кто не проявляет 100%-го согласия с позицией руководителя.

Четвертая привычка коррелирует с предыдущей. Авторитарные люди считают, что только они знают правильное направление движения команды к поставленной цели. С одной стороны, такая позиция вызывает уважение, но с другой она может нанести фирме непоправимый ущерб. Беспощадно избавляясь от инакомыслящих, руководитель становится заложником своих собственных заблуждений и ошибочных мнений.

Привычка 5: быть неутомимым пропагандистом и имиджмейкером своей компании.

Перенос руководителем акцента с управления компанией на выполнение представительских функций – явление довольно опасное. Основное усилие в этом случае уделяется не работе компании, а формированию в глазах общественности и прессы ее положительного имиджа, часто не соответствующего действительному положению дел.

Привычка 6: недооценивать степень серьезности препятствий.

Эта привычка находит свое проявление в тенденции руководителя отмахиваться от любых проблем так, словно речь идет о незначительных затруднениях, в то время как в реальности во многих случаях они имеют дело с весьма серьезными препятствиями. Захваченные видением того, что они хотят совершить, они не замечают, насколько трудно будет им достичь желанной вершины. Им кажется, что все ожидающие их проблемы разрешимы, хотя на самом деле многие из этих проблем либо вообще не имеют решения, либо решаются только ценою слишком больших затрат.

Характерно, что руководители подобного типа легко вовлекают людей в задуманные ими проекты, заражают их своей уверенностью, заставляя делать все, что необходимо, и пребывают в уверенности, что эти люди должны справляться с возникающими трудностями и обеспечивать жизнедеятельность компании.

Когда же руководитель, наконец, осознает, что проблемы, которые казались ему такими незначительными, на самом деле весьма серьезны, он нередко пытается решить их, продолжая с еще большим усердием делать то же самое, что он делал до сих пор. Его усердие объясняется боязнью признания факта совершения им серьезной ошибки, поскольку это признание может привести к выводу о его несоответствии занимаемой должности.

Чтобы не потерять лицо, он предпочитает добиваться поставленной цели путем активизации направленных на ее достижение шагов. Вложение дополнительных ресурсов в реализацию изначального решения на некоторое время избавляет руководителя от необходимости сознаваться в ошибочности выбранного курса.

Однако такая тактика приводит к тому, что топ-менеджеру становится все труднее объявить об отступлении или смене направления. Масштаб ошибки, в которой предстоит признаться руководителю, становится в его сознании все более и более серьезным. Финансовые потери, о которых придется объявить, становятся все более и более значительными. В то же время расширение проекта, как правило, означает и рост возможной награды за его удачное завершение. Ни один из факторов, изначально обусловивших возникновение проблемы, не устранен, более того, влияние большинства из них только

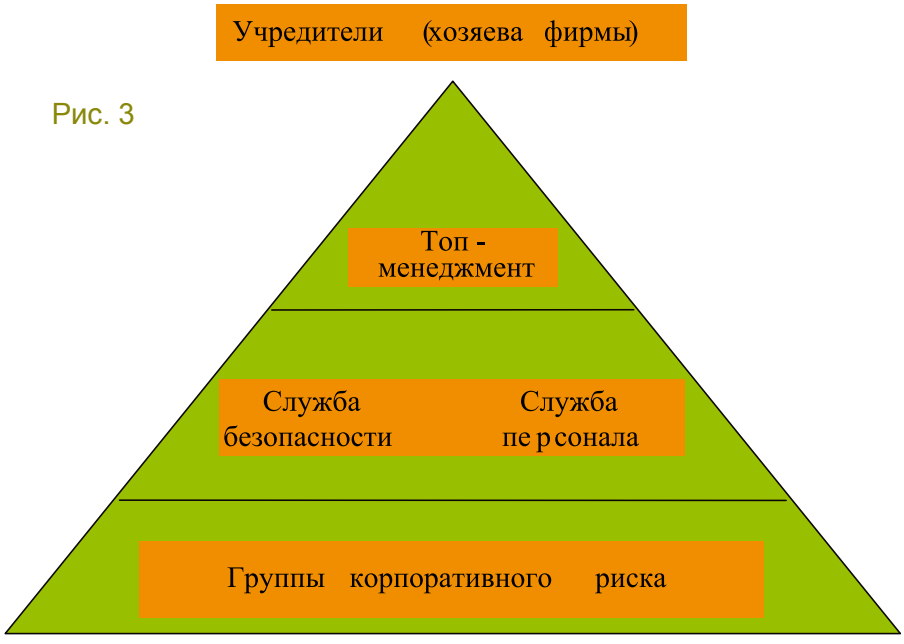

Рис. 3

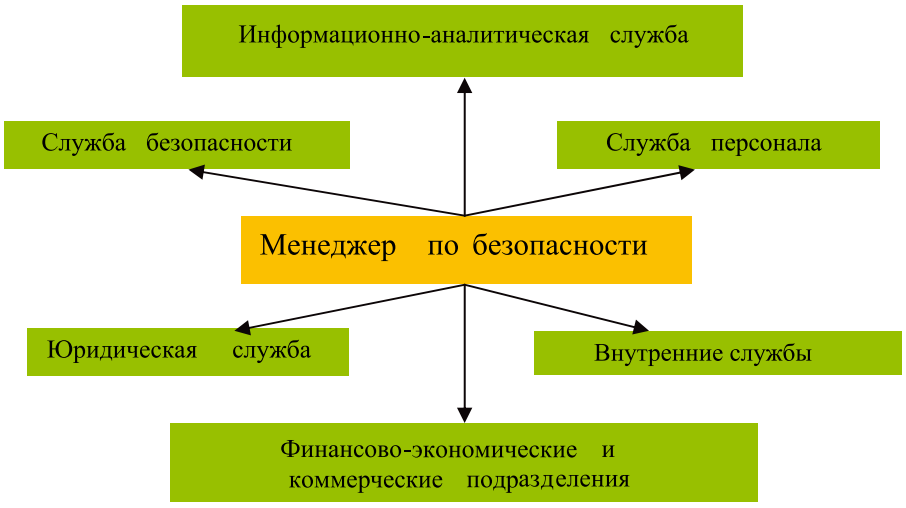

Схема 1

усилилось.

Привычка 7: упрямо придерживаться старых подходов, когда-то обеспечивших тебе успех.

Руководители такого типа предпочитают испытанные методы и проверенные средства. Для успешной работы им нужна стабильность. В их тактике принятия решения четко просматривается ориентация на статическую бизнес-модель. Вместо того чтобы рассматривать широкий спектр вариантов, при выборе курса действий эти руководители ограничивают себя стратегиями, которые позволяли им добиваться успеха в прошлом. Очень часто такие топ-менеджеры отдают предпочтение опасной или неподходящей стратегии под влиянием некоторых «определяющих моментов», которые имели место ранее в их карьере.

Третий уровень среди факторов внутренней угрозы занимают службы безопасности и персонала.

Опасности, содержащиеся в таком факторе угрозы, как служба безопасности, проистекают из двух первопричин. Во-первых, это единственное подразделение компании, функциональной задачей которого является поддержание на заданном уровне корпоративной безопасности. И, следовательно, от уровня профессионализма ее сотрудников зависит, будет ли поставленная перед компанией цель достигнута. Во-вторых – уровень безопасности напрямую связан с лояльностью сотрудников службы по отношению к фирме.

Что касается службы персонала, то, как и в случае со службой безопасности, на уровень корпоративной безопасности в большой мере будут влиять профессионализм сотрудников в сфере подбора персонала, выявлении и разрешении конфликтных ситуаций. Именно в этой службе концентрируется конфиденциальная информация о личностных качествах персонала фирмы. То есть материалы, представляющие интерес для конкурентов и криминала.

Четвертый уровень внутренних угроз можно классифицировать как «Группы корпоративного риска». Эти группы, в отличие от ранее рассмотренных, являются условными, т.е. включаемые в них сотрудники объединены на основании наличия у них некоего общего признака. При этом они могут даже не знать о своей принадлежности к одной из этих групп и лично не контактировать друг с другом.

К этим группам относятся следующие категории сотрудников:

1. Носители информации, содержащей коммерческую тайну;
2. Лица, находящиеся в состоянии конфликта (ролевого, личностного, группового);
3. Лица, имеющие дорогостоящие хобби, увлекающиеся азартными играми или экстремальными видами спорта;
4. Нелояльные сотрудники.

Опасность, содержащаяся в этом факторе угрозы, имеет выраженную личностную природу и реализуется в форме умышленных или неумышленных действий сотрудников, способных привести к снижению уровня корпоративной безопасности. Так, например, носители сведений, составляющих коммерческую тайну, могут стать источником информации для конкурентов — либо по собственной инициативе, либо в качестве жертв манипулятивных приемов выведывания.

Что же касается сотрудников, находящихся в состоянии конфликта любого рода, то их профессиональная надежность и лояльность в этот период резко падает. Довольно часто, решая свои проблемы, они совершают поступки, наносящие серьезный урон корпоративной безопасности.

Лица, имеющие дорогостоящие хобби, не соответствующие их уровню денежного содержания, могут стать растратчиками казенных средств или попасть в долговую зависимость. Это в равной мере относится и к любителям азартных игр. Определенную опасность представляют собой и «экстремалы». Рискуя своей жизнью, они, в случае травм или увечий, могут нанести фирме большой ущерб благодаря длительному периоду неработоспособности.

Нелояльные сотрудники – предмет особого рассмотрения. Если рассматривать лояльность как степень преданности группе, то всех членов команды можно условно разделить на три подгруппы:

1. Лояльные — те, кто ни при каких условиях не покинет группу;
2. Ситуативно-лояльные — это демонстрирующие свою преданность групповым идеалам, но только до тех пор, пока достижение групповых целей не противоречит удовлетворению их личностных интересов;
3. Нелояльные – использующие свое пребывание в команде только для удовлетворения своих личностных потребностей, которые реализуются асоциальными и антисоциальными приемами и методами. Следует отметить, что нелояльность, как правило, имеет латентный (скрытый) характер, и выявлять ее довольно трудно.

Таким образом, система корпоративной безопасности, рассмотренная нами в предыдущей статье, должна быть настроена на противодействие не только факторам внешней, но и внутренней угрозы.

После того как мы разобрались с факторами угрозы и рассмотрели

структуру системы корпоративной безопасности, функционирующую по принципу отрицательной обратной связи, пришло время разобраться в вопросах, связанных с ее управлением. Действительно, какую бы идеальную систему корпоративной безопасности вы ни создали, – эффективность ее функционирования напрямую зависит от того, кто и как будет ею управлять. Многие предприниматели, создав у себя службу безопасности, считают, что дело сделано, и теперь можно спать спокойно. Это ничто иное, как добросовестное заблуждение. Попробуем это доказать.

Служба безопасности любой фирмы или корпорации является одним из субъектов управления корпоративной безопасностью. То есть, не единственным в этом роде! Круг задач этой службы – ограничен. В них входят выявление, мониторинг факторов внешней угрозы и противодействие им, исполнение контрольно-фискальных функций в отношении факторов внутренней угрозы. Но это – только часть задач, решение которых возложено на систему корпоративной безопасности.

Создание и управление системой взаимодействующих динамичных процессов для достижения поставленной цели способствует повышению результативности и эффективности деятельности организации.

Рассматриваемый нами системный подход требует координации всех аспектов деятельности, применения «проектного стиля» организации работ.

Применение этого принципа предполагает:

- формирование системы на основе определения или разработки процессов, влияющих на достижение поставленной цели;
- структурирование системы для достижения цели самым эффективным способом;
- понимание взаимозависимостей процессов в системе, разрушающих барьеры между подразделениями, задействованными в обеспечении корпоративной безопасности;
- постоянное улучшение системы на основе измерения, анализа процессов и оценки их результатов;
- установление ограничений на ресурсы до начала действий.

Успешное применение принципа дает следующие преимущества:

- для формулировки политики и стратегии – создание исчерпывающих и способствующих улучшению планов, которые связывают функциональный и процессный подходы;
- для установления целей и показателей – цели и показатели отдельных процессов по обеспечению корпоративной безопасности согласуются с ключевыми целями организации;
- для оперативного управления – получение возможности широкого обзора эффективности процессов, ведущего к пониманию причин проблем и к своевременным действиям по улучшению;
- для управления человеческими ресурсами – обеспечение лучшего понимания ролей и ответственности при достижении общих целей путем организации командной работы, ведущей к устранению барьеров между подразделениями.

Система корпоративной безопасности фирмы или компании должна быть ориентирована на решение задач трех типов:

- Мониторинг факторов угрозы;
- Предупреждение актуализации опасностей, содержащихся в факторах угрозы;
- Пресечение деструктивного воздействия на фирму или отдельные ее подразделения и подсистемы актуализировавшихся опасностей.

Напомним, что факторы угрозы существуют как элемент среды. Они сравнимы, с одной стороны, со спящим вулканом, а с другой – с хищником, активно ищущим жертву. Но независимо от логики своего существования и развития все они содержат в себе потенциальную или реальную опасность. Факторами угрозы управлять нельзя, но можно снизить вероятность актуализации содержащейся в них опасности по отношению к конкретному субъекту деятельности путем грамотного маневрирования в их среде. Такие маневры в управленческой литературе принято называть управлением рисками. Таким образом, управление системой корпоративной безопасности, по сути своей, является управлением рисками. А конечная цель такого управления – поиск оптимального соотношения рисков и желаемых результатов. Именно оптимизации, а не исключения или минимизации. Вулканолог не может не идти на риск при изучении действующего вулкана. Он не сможет предвосхитить направления и динамики развития ситуации. Но если, с его точки зрения, ожидаемый результат для него жизненно важен, он готов рискнуть. Даже, если есть реальная угроза жизни

Аналогично и с хищниками. Не

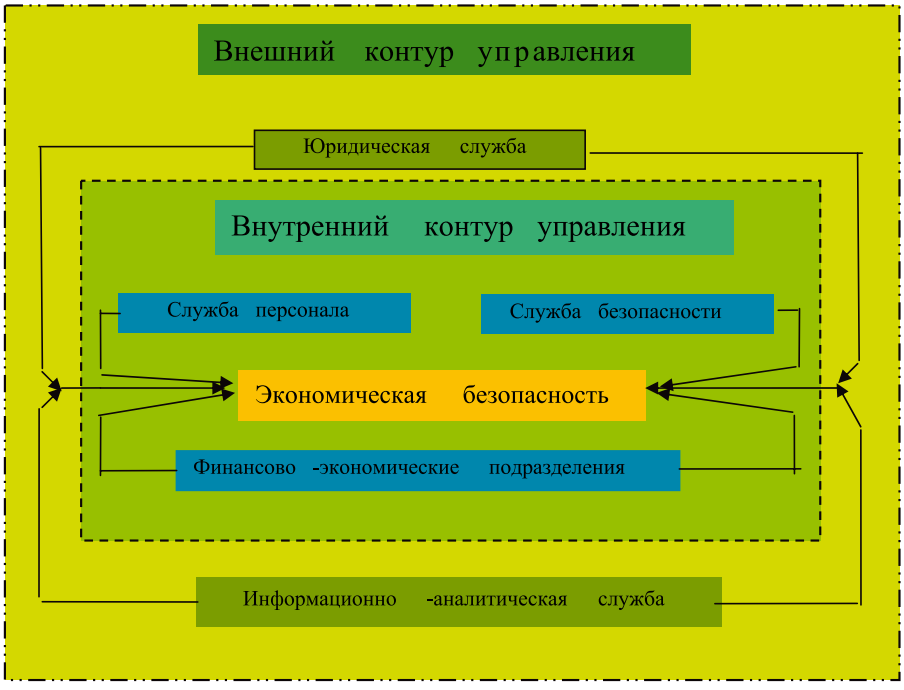

Схема 2

даром в пословице говорится: «Волков бояться – в лес не ходить». Следовательно, рисками можно и нужно управлять. Но кто это будет делать?

В управленческой пирамиде максимумом власти и ответственности обладает первое лицо. Будь то президент или генеральный директор. И обычно именно он в малом и среднем бизнесе курирует службу безопасности. Но такой подход далек от совершенства. Президент вынужден решать широкий круг вопросов, связанных с функционированием фирмы, и, следовательно, уделять внимание вопросам безопасности он может только эпизодически, делегировав свои полномочия начальнику службы безопасности. Слабость такой системы управления в том, что выделенных полномочий явно недостаточно для того, чтобы в полном объеме реализовать принцип системности. Как уже отмечалось, в обеспечении корпоративной безопасности задействовано еще несколько подразделений, руководители которых находятся в равной статусной позиции с начальником службы безопасности.

Для устранения этого недостатка необходимо введение должности менеджера по безопасности. Эту должность должен занимать специально подготовленный топ-менеджер на уровне вице-президента или заместителя генерального директора. Он должен обладать опытом управленческой деятельности в области экономики и быть знакомым с основами оперативно-розыскной деятельности. Лучше, если он не будет выходцем из силовых структур.

Задача этого топ-менеджера – координировать действия всех структур, задействованных в системе корпоративной безопасности. Без такого координатора достичь согласованности в действиях отдельных подразделений не представляется возможным.

Схема 1

На схеме 1 представлена сокращенная структура управления корпоративной безопасностью. Безусловно, что при решении конкретных задач у каждого участника процесса будет своя определенная роль. Рассмотрим это на примере управления процессом обеспечения экономической безопасности.

Схема 2

Как видно из схемы 2, управление экономической безопасностью осуществляется посредством двухконтурной системы. Во внутренний контур управления включены подразделения, непосредственно отвечающие за поддержание заданного уровня экономической безопасности.

Во внешний – информационное и правовое сопровождение.

Подсистема экономической безопасности, как и другие подсистемы, настраивается на несколько режимов работы:

- дежурный;
- повышенной готовности;
- экстремальный.

Дежурный режим рассчитан на рутинную работу по поддержанию заданного уровня экономической безопасности при штатном функционировании фирмы.

Режим повышенной готовности включается в моменты работы над жизненно важными для фирмы проектами при наличии информации о готовящихся против фирмы враждебных акциях со стороны факторов внешней угрозы.

Экстремальный режим включается в периоды актуализации опасностей, содержащихся в факторах угрозы в отношении защищаемых объектов.

В каждом из этих режимов ведущая роль отводится двум подразделениям: службе безопасности и службе персонала.

Так, в случае работы в дежурном режиме, служба безопасности выполняет преимущественно контрольно-фискальные функции. В частности, она осуществляет мониторинг факторов внешней угрозы, контроль режима работы с информацией, содержащей коммерческую тайну, участвует в проведении предварительного изучения некоторых категорий кандидатов на работу и т.п.

При режиме повышенной готовности акценты переносятся на отработку мер, повышающих защищенность информационных потоков, содержащих информацию о разрабатываемых проектах и стратегических планах развития компании, повышения степени защищенности объектов, в отношении которых есть сведения о готовящихся враждебных акциях.

При работе в экстремальном режиме служба безопасности использует все свои силы и средства для надежного обеспечения высокой защищенности охраняемых объектов от деструктивного воздействия факторов внешней угрозы или при расследовании ЧП, случившихся в результате актуализации факторов внутренней угрозы.

Служба персонала в дежурном режиме занимается мониторингом факторов внутренней угрозы, поддержанием на должном уровне исполнительской дисциплины и внутреннего распорядка, комплектованием команды высококвалифицированными сотрудниками.

В режиме повышенной готовности акценты переносятся на контроль за группами корпоративного риска и, прежде всего, тех сотрудников, которые задействованы в работе над жизненно важными для фирмы проектами.

При работе в экстремальном режиме служба персонала совместно со службой безопасности разрабатывает мероприятия защитного характера, позволяющие обеспечить эффективное противодействие актуализировавшимся факторам угрозы с акцентом на их внутреннюю составляющую.

Оба эти субъекта управления ориентированы на минимизации рисков.

В отличие от них третий участник внутреннего контура управления — финансово-экономические подразделения — в большей степени ориентированы на максимизацию прибыли даже в условиях повышенных рисков. Эффективное управление этм внутренним противоречием и становится задачей менеджера по безопасности. При принятии управленческих решений он должен активно использовать и вспомогательные в данном вопросе структуры – информационно-аналитическое подразделение и юридическую службу

Что касается службы внутреннего аудита, то ей отводится особая роль. Она преимущественно работает в период дежурного режима. А результаты ее деятельности используются для профилактики актуализации угроз корпоративной безопасности.