Защищайтесь, господа предприниматели

И.С. Козьминых, *К.Т.Н*

Зарубежный и отечественный опыт обеспечения безопасности предпринимательской деятельности свидетельствует, что для борьбы с потенциально возможными и реальными угрозами необходима целенаправленная организация процесса противодействия. Причем реализация этого процесса должна включать в себя организационные и технические мероприятия, цель которых – недопущение, пресечение и ликвидация последствий нештатных ситуаций и чрезвычайных происшествий.

Проведение технических мероприятий и применение технических средств безопасности во многом помогают защитить объекты от угроз. Вместе с тем анализ чрезвычайных происшествий показывает, что причиной трагических ситуаций в большинстве случаев является слабая организация системы безопасности, проявляющаяся в непрофессиональных или несвоевременных действиях, отсутствии координации и взаимодействия, плохо подготовленных или отсутствующих планах, нормативных документах и инструкциях.

В связи с этим на передний план выдвигается проблема правильной организации системы безопасности объекта, фирмы, предпринимательской деятельности в целом. О том, что должен знать предприниматель при разработке концепции безопасности, расскажет данная статья.

Терминология

В книгах, статьях и технической документации можно встретить различные определения, касающиеся безопасности. Чтобы читателю проще было воспринимать материалы статьи, введем ряд понятий и определений, которые будут встречаться в данной статье.

Объект защиты – пассивная системная составляющая, к которой применяется методика обеспечения безопасности. Под ней следует понимать личность, природные ресурсы, источники и продукты жизнедеятельности общества, его духовный и нравственный потенциал, суверенитет, территориальную целостность, конституционный строй, государственную систему управления и т.п.

Угроза – потенциально возможное несанкционированное воздействие дестабилизирующих факторов на объект защиты, которое может быть реализовано в любой момент времени при выполнении определенных условий и причинить ущерб объекту защиты.

Риск – вероятность несанкционированного воздействия дестабилизирующих факторов на объект защиты, то есть, иными словами, вероятность реализации угрозы.

Ущерб – физические, моральные, материальные и другие потери, возникающие в результате несанкционированного воздействия дестабилизирующих факторов на объекты защиты. В качестве ущерба необходимо рассматривать не только прямые потери, но и любые, отрицательно влияющие на предпринимательскую деятельность факторы, такие, как снижение имиджа, недополученная возможная прибыль, временная приостановка деятельности, потеря высококвалифицированных кадров и др.

Безопасность – состояние объекта защиты, при котором организовано максимально возможное противодействие дестабилизирующим факторам (угрозам) как на этапе предупреждения и пресечения, так и на этапе ликвидации последствий от их реализации.

Концепция безопасности организации – система взглядов на проблему безопасности на различных этапах и уровнях предпринимательской деятельности, а также основные принципы, направления и этапы реализации мер безопасности.

Система безопасности – постоянно осуществляемый комплекс мер по предупреждению, пресечению и ликвидации последствий максимального количества угроз из полного набора возможных угроз для данного объекта или предпринимательской деятельности в целом.

Основы формирования концепции безопасности

В настоящее время вопрос обеспечения безопасности в сфере предпринимательства находится в стадии решения. В условиях несовершенства многих разделов законодательства, регулирующего предпринимательскую деятельность, главными источниками угроз для нее в существующих российских условиях являются:

- ✓ противоправные посягательства со стороны недобросовестных конкурентов и несостоятельных партнеров;
- ✓ ущемление прав и законных интересов предпринимателей государственными органами и должностными лицами;
- ✓ ограничительная деловая практика на внешних рынках;
- ✓ криминальное насилие, промышленный шпионаж, посягательства на коммерческую тайну и интеллектуальную собственность;
- ✓ низкий профессионализм, а в целом ряде случаев – недобросовестность, продажность собственного персонала.

На сегодняшний день не существует однозначных путей решения поставленной проблемы, поскольку каждое ведомство и учреждение решает вопросы безопасности своей деятельности собственными силами. Поэтому нередко возникают ситуации, когда проблемы решаются превентивными мерами, то есть объекты ставят под централизованную охрану, оборудуют пожарной сигнализацией, используя услуги част-

ных охранных предприятий, страховых фирм. Однако при этом не производится оценка системы и уровня безопасности фирмы, вероятности возникновения той или иной угрозы, степени риска, возможного ущерба. Без предварительной проработки концепции и методики обеспечения безопасности предприниматель несет значительные материальные затраты на установку избыточных технических средств, содержание раздутой службы безопасности, грабительские страховые взносы; вместе с тем, никто не дает ему гарантий защиты от краж, пожаров, утечки информации, криминальных разборок и других нештатных и чрезвычайных ситуаций. Если же таковые возникают, то чаще всего предприниматель бывает не готов к принятию необходимых мер по их пресечению и оперативной ликвидации последствий.

В данной статье рассмотрены основы формирования концепции безопасности объекта, предпринимательской деятельности, которая должна дать ответы на три вопроса:

- ***что защищать?***
- ***от чего защищать?***
- ***как защищать?***

Определение объектов защиты

Для начала рассмотрим основной принцип функционирования коммерческих организаций на основе обобщенной модели (рис.1). На наш взгляд, она достаточно полно иллюстрирует функционирование большинства коммерческих организаций. С точки зрения автора статьи, особое значение приобретает учет руководителем всех этапов процесса предпринимательской деятельности организации.

Данная модель наглядно представляет этапы предпринимательской деятельности и показывает, что угрозы могут возникнуть на любом из них, начиная с формирования ресурсов, затем в процессе производства или оказания услуг, а также на этапе получения и распределения прибыли. Поэтому при разработке концепции безопасности необходимо учитывать все объекты защиты, присутствующие на каждом этапе предпринимательской деятельности.

На следующей модели (**рис. 2**) центральный блок представляет собой саму организацию с основными видами коммерческой деятельности, которая включает в себя: экономическую деятельность (производство или оказание услуг), юридическую деятельность (документооборот организации), информационно-аналитическую деятельность (инновационная деятельность и разработка оптимальных стратегий получения прибыли) и обеспечение безопасности организации.

Входными воздействиями на эту систему являются ресурсы, экономическое и законодательное пространство, а также потенциально возможные угрозы.

На выходе системы – получаемая прибыль, стабильное положение на рынке и авторитет организации.

Если вернуться к модели функционирования коммерческой организации (см. **рис. 1**) и считать, что произведенный товар или оказанная услуга с полученной прибылью фактически является дополнительным ресурсом для осуществления даль-

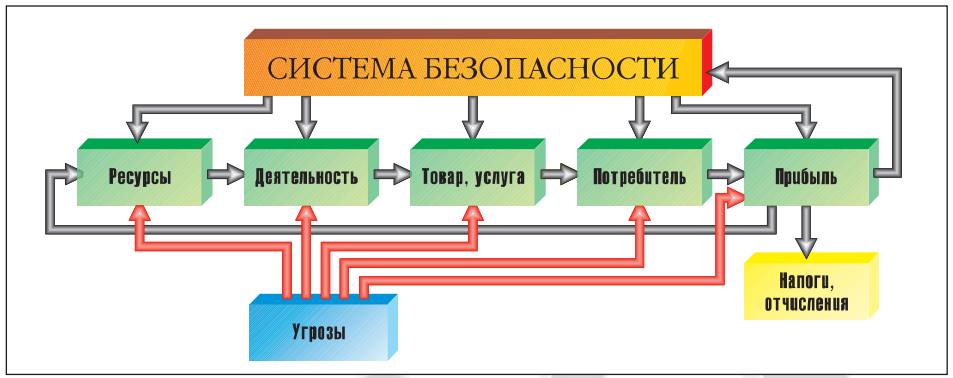


Рис. 1. Модель функционирования коммерческой организации

нейшей деятельности, то получается, что основными объектами защиты являются ресурс и деятельность. Более подробно перечень ресурсов и основных видов деятельности приведен в **таблице 1**.

При формировании концепции безопасности данная таблица может служить в качестве шпаргалки руководителю фирмы или начальнику службы безопасности. Проведя анализ штатной структуры фирмы, необходимо сразу отметить приоритетность сотрудников в зависимости от их ценности для фирмы: квалификации, взаимозаменяемости, степени осведомленности о деятельности фирмы, личного вклада в общее дело, перспективности, доступа к финансам, материальным и интеллектуальным ценностям. Не обладая такой информацией о своих сотрудниках, невозможно

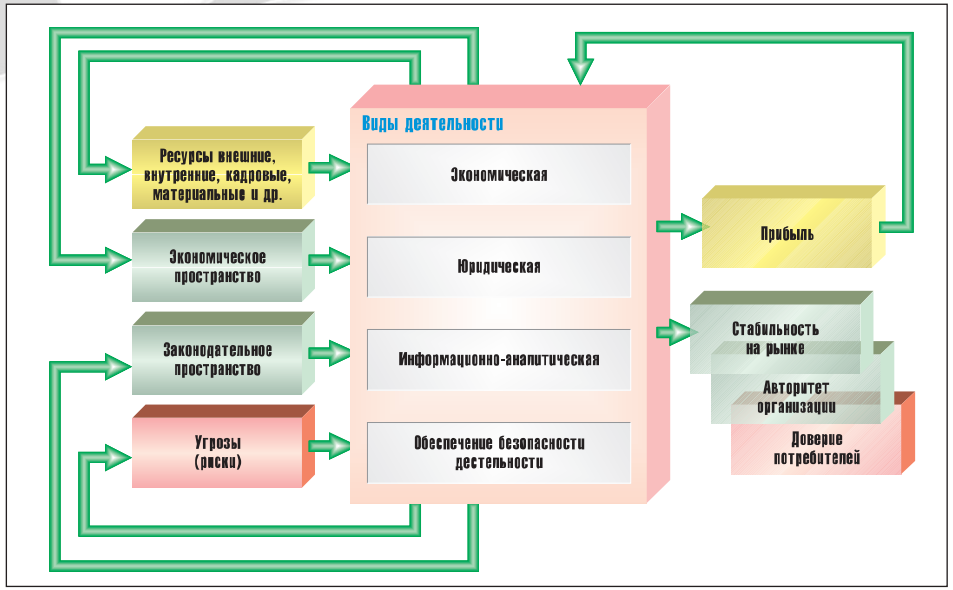


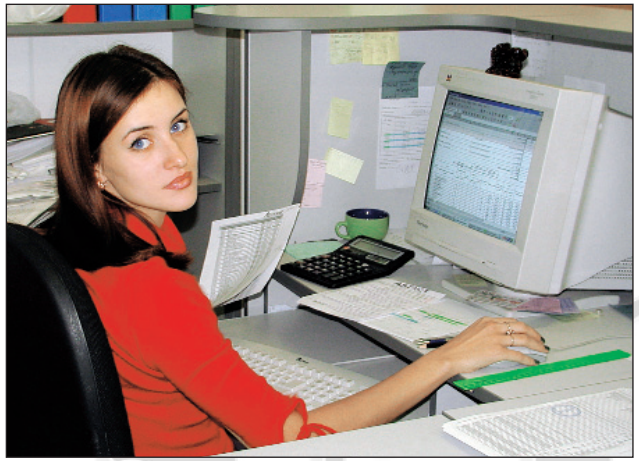
Рис. 2. Обобщенная схема получения прибыли коммерческой организации

Таблица 1. *Основные объекты защиты, которые необходимо учитывать при разработке концепции безопасности организации*

Что защищать	Для чего защищать
Ресурс	
Персонал организации (сотрудники)	Обеспечение безопасности жизни, здоровья, чести, достоинства, обеспечение положительного морально-психологического климата, нормальных условий труда.
Материальные ценности, включая недвижимость и транспортные средства	Обеспечение защиты от порчи, кражи, замены, полного или частичного уничтожения
Информация	Обеспечение защиты от фальсификации, утечки, порчи, кражи, копирования, подмены, полного или частичного уничтожения
Деятельность	
Экономическая	С целью предупреждения или снижения экономических рисков: дефолта; не возврата долгов, кредитов, инвестиций; недобросовестной конкуренции и недобросовестного партнерства; финансовых афер и т.п.
Юридическая	С целью предупреждения или снижения законодательных рисков: неправильного оформления уставных и лицензирующих деятельность документов; неграмотного оформления договоров, обязательств и других документов; непрофессиональной защиты своих интересов в судебных и других инстанциях; не отслеживания изменений законодательства и ведомственной нормативной базы; исключения деятельности, выходящей за рамки закона
Инновационная	С целью предупреждения или снижения инновационных рисков: неправильной оценки рынка потребления товара или услуги, цен, объемов производства и потребления; ошибочного расчета проектируемого и реального качества и функциональных характеристик изделия; завышенных или заниженных гарантийных обязательств; участия в проектах с недопустимой или высокой степенью риска

защитить их от реальных угроз. Если же Вы хорошо изучили свой персонал, то сможете для каждого из них или для группы сотрудников с достаточной степенью вероятности определить перечень угроз и разработать комплекс мер по противодействию им. Аналогично следует поступить с материальными ценностями, недвижимостью и транспортными средствами.

Как определить, что важнее и, соответственно, более всего нуждается в защите? Вначале необходимо обеспечить защиту тех материальных ценностей, без которых фирма не сможет работать или вообще прекратит свое существование. Для одних это может быть компьютер с базой данных, для других – офисное помещение, для третьих – транспортные средства. В каждой фирме эти материальные ценности определяются строго индивидуально. В качестве примера можно привести ситуацию с одним из крупных российских банков, у которого сначала горело здание в Санкт-Петербурге, а через некоторое время – в Москве, убытки от чего, по всей видимости, составили значительную сумму. Но, тем не менее, банк не разорился и выполнил все свои финансовые обязательства. То, что произошли два пожара, говорит о слабой системе защиты от возгорания, но, поскольку банк не разорился и выполнил свои



обязательства, следует отметить, что система безопасности этого банка функционирует на высоком уровне. Можно предположить, что ущерб, связанный с этими происшествиями, был восполнен за счет страховых выплат или резервного фонда. С помощью оперативных действий удалось уберечь от пожара большую часть зданий и наиболее ценное имущество. А результатом грамотной реализации антикризисных мероприятий стало то, что банк выполнил обязательства, не останавливал свою деятельность и заработал дополнительный имидж «непотопляемого и несгораемого банка».

Из сказанного выше можно сделать вывод:

определяя материальные объекты защиты, необходимо соотносить их с возможным ущербом, который понесет фирма в целом при их потере или порче.

Отдельно следует сказать о защите информации.

В первую очередь предприниматель должен определить:

✓ какая информация, имеющаяся у него, подлежит обязательной защите в соответствии с действующим законодательством;

✓ какая информация является коммерческой тайной и имеет право на защиту;

✓ кто и при каких обстоятельствах имеет право доступа к перечисленным видам информации.

При анализе следует учитывать информацию, хранящуюся как на бумажных носителях, так и в электронном виде. Также к объектам защиты необходимо отнести каналы приема-передачи информации. Не следует забывать при этом, что персонал организации может быть не только носителем, но и источником утечки информации. В организациях, имеющих конфиденциальную информацию, список объектов защиты будет достаточно внушительным. Рекомендуется ранжировать список информационных объектов защиты так же, как и материальных: по степени возможного причинения ущерба деятельности организации в случае воздействия на нее различных видов угроз.

Наиболее сложно ранжировать по степени важности объекты защиты, представляющие собой различные направления деятельности фирмы, организации. Однако во многих организациях имеются так называемые основные направления деятельности, приносящие большую часть прибыли, и не основные, которые можно назвать сервисными (материально-техническое обеспечение, административно-хозяйственная деятельность, подбор кадров, бухгалтерский учет и т.п.). Понятно, что в качестве

объектов защиты необходимо рассматривать прежде всего направления деятельности фирмы, приносящие наибольшую прибыль, нарушение которых приведет к остановке работы всей фирмы или большей ее части, а также деятельность, направленную на развитие новых направлений, расширение сферы интересов, повышение имиджа.

Анализ направлений деятельности фирмы, организации с точки зрения их прибыльности, перспективности, влияния на общий имидж необходим не только для обеспечения безопасности. Он необходим, в первую очередь, для руководства, чтобы оценить какие направления необходимо развивать, а какие сворачивать. Такой анализ помогает оптимизировать затраты, планировать инвестиции, способствует развитию предпринимательской деятельности.

Определение перечня угроз

При разработке концепции безопасности формирование полного перечня угроз является основным и наиболее трудоемким этапом. Источниками угроз (**рис. 3**) служат человеческий фактор, окружающая природная и техногенная среда.

Понятно, что любая криминальная деятельность, направленная против предпринимательства, как правило, представляет для него существенную угрозу. Однако имеется целый набор угроз предпринимательской деятельности, который, по причине несовершенства законодательства, отсутствия возможности сбора доказательств или по другим причинам, не попадает под статьи действующих законов, например: недобросовестная конкуренция, коммерческие взятки, забастовки, экономические кризисы, демпинг цен и другие. Это не означает, что от этих угроз нет способов защиты, а говорит лишь о необходимости учитывать не только те виды угроз, которые

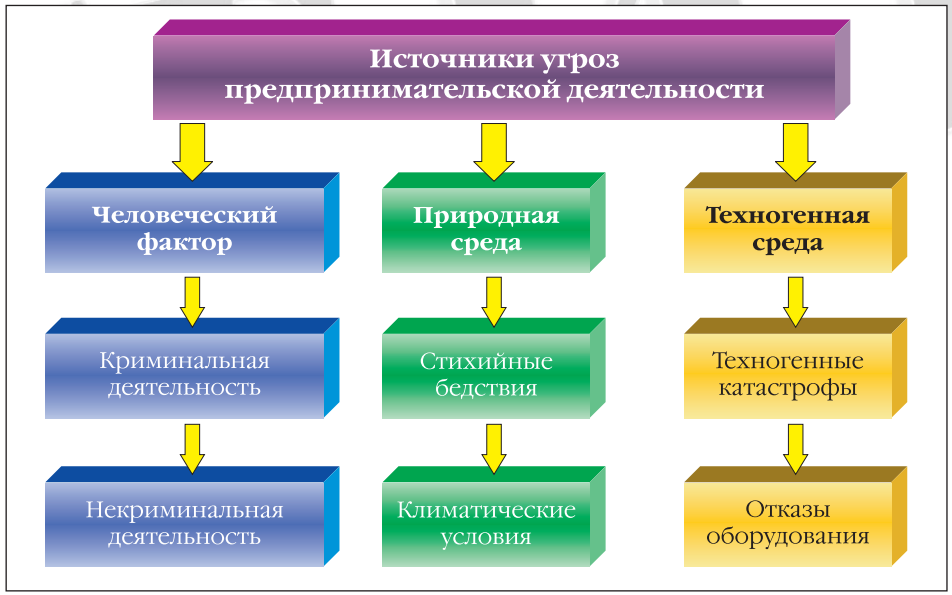


Рис. 3. Классификация источников угроз предпринимательской деятельности

определены как преступления, но и те, которые могут возникнуть в результате стихийных бедствий, суровых климатических условий, техногенных и экологических катастроф, полного выхода из строя и временного отказа технологического оборудования.

Способы защиты от угроз

В настоящее время существует достаточно много способов защиты от угроз предпринимательской деятельности. Условно их можно поделить на четыре класса (**рис. 4**): организационные, технические, физические и оперативные, хотя, по сути, все они связаны с проведением организационных и технических мероприятий.

Как же определить, какие способы защиты необходимы для нейтрализации угроз?

Защита от конкретной угрозы, как и от набора угроз, осуществляется путем проведения комплекса мероприятий. Причем реализация одного и того же комплекса мероприятий сможет противостоять различным наборам угроз. Приведем пример. Установка на объекте охранного телевидения способствует как защите от краж мате-

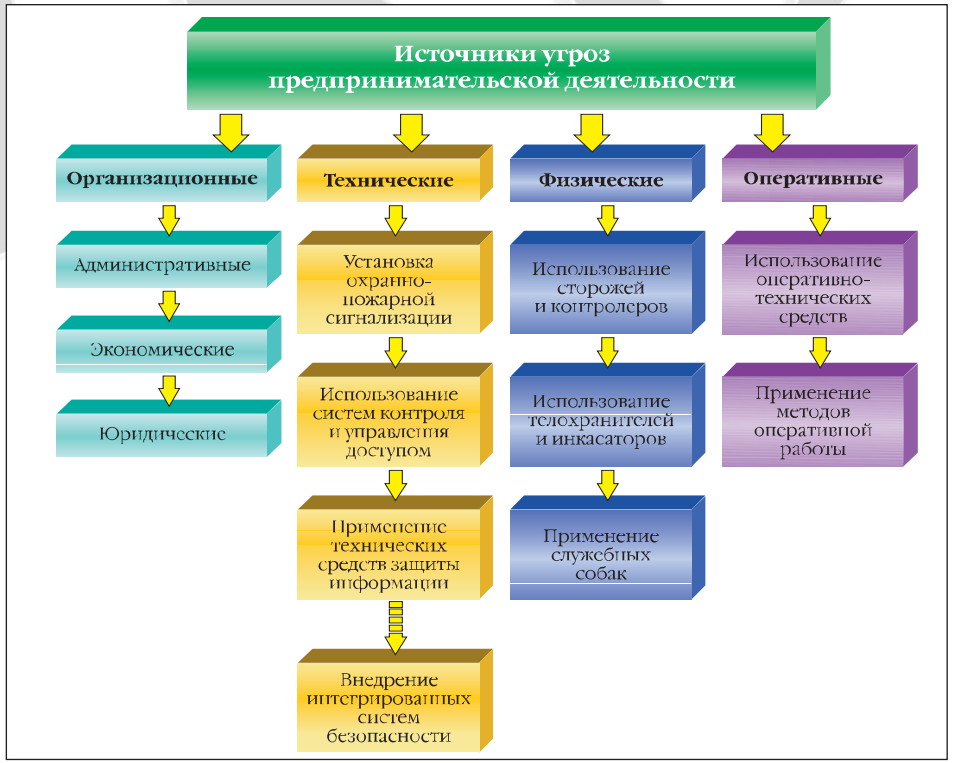


Рис. 4. Классификация способов защиты от угроз предпринимательской деятельности

риальных ценностей или информации, так и защите от актов терроризма, разбойных нападений, хулиганства или вандализма. Но это не означает, что установка на объекте только охранного телевидения решит все проблемы. С помощью охранного телевидения можно получить информацию о нарушениях в тех зонах объекта, где установлены телекамеры, но нельзя одновременно контролировать весь объем помещения: это под силу только охранной сигнализации. Охранные телевизионные системы не в состоянии контролировать повышение температуры в помещении на ранней стадии возникновения пожара: это могут сделать только тепловые пожарные извещатели, задействованные в системе пожарной сигнализации, однако при появлении дыма, видеокамеры его зафиксируют и выдадут сигнал тревоги.

Таким образом, можно сделать вывод:

для обеспечения комплексной безопасности объекта или предпринимательской деятельности необходимо проведение полного комплекса мер безопасности, который формируется в зависимости от выбранного перечня объектов защиты и набора наиболее вероятных угроз, способных причинить максимальный ущерб.

Разработка системы безопасности объекта или предпринимательской деятельности в целом является основной частью концепции безопасности. Существует достаточно много форм и названий документов, по сути являющихся концепциями безопасности. На наш взгляд, если речь идет об обеспечении безопасности конкретного объекта (завода, обменного пункта валюты, магазина, склада, жилого здания, офиса или коттеджа), то название и содержание документа должны отражать цели, задачи, пути и методы решения проблемы обеспечения безопасности для этого объекта. Если поставлена задача разработки концепции безопасности всей организации, фирмы или предприятия в целом, а не только его зданий, территорий, материальных ценностей, а также всех или основных видов предпринимательской деятельности, то решение ее значительно усложняется. Не следует забывать, что для правильной постановки такой задачи и достижения определенных результатов имеет значение все: начиная с разработки названия и количества разделов и заканчивая конкретным заданием на разработку системы безопасности

В заключение хотелось бы подвести некоторые итоги. Итак, разрабатывая концепцию безопасности, необходимо учитывать следующее:

1 ***Концепцию безопасности фирмы, организации, предприятия и систему безопасности как практическую реализацию концепции безопасности необходимо рассматривать в более широком плане. Не только как систему обеспечения безопасности предпринимательской деятельности, но и как систему, помогающую повысить её эффективность, оптимизировать***

затраты, расширить сферу применения и развивать новые направления.

2 ***Разработка и реализация системы безопасности не должна быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов совершенствования и развития системы безопасности, непрерывном контроле и управлении ею, выявлении ее слабых мест и ликвидации недостатков.***

3 ***Система безопасности будет эффективна лишь при комплексном использовании всего арсенала сил и средств, то есть участия в её разработке и реализации не только руководителя организации и службы безопасности, а практически всего персонала, и в первую очередь – ведущих специалистов по каждому направлению деятельности.***

4 ***Никакая система не может обеспечить требуемый уровень безопасности без надлежащей подготовки службы безопасности и персонала организации, без проведения обучения, тренировок, игр и учений.***

(Более подробно вопросы обеспечения комплексной безопасности освещены в готовящемся к изданию в конце этого года методическом пособии С.И. Козьминых «Обеспечение комплексной безопасности объекта, фирмы, предпринимательской деятельности» – прим. автора).