

Олег Захаров



Менеджмент безопасности бизнеса

Олег Захаров

Менеджмент безопасности бизнеса

«Автор»

2012

Захаров О. Ю.

Менеджмент безопасности бизнеса / О. Ю. Захаров — «Автор», 2012

Состояние безопасности является основой для полноценного ведения бизнеса в любой сфере. Наличие существенной собственности вынуждает многих представителей бизнеса заниматься обеспечением безопасности. В современном бизнес-сообществе особое значение приобретают навыки защиты информации, информационно-аналитической работы – сбора и анализа зачастую противоречивой и сомнительной информации, зачастую не количественной. Появились новые каналы угроз безопасности бизнеса связанные с кадровой работой и отбором персонала. Зачастую не каждый представитель бизнеса имеет возможность содержать штат высококвалифицированных специалистов по безопасности, однако противостоять угрозам безопасности бизнеса необходимо. Основная задача этой книги – помочь читателю сформировать систематизированное представление о безопасности бизнеса, как о комплексе мер в организационной, информационной, правовой, кадровой и других сферах, каждое из которых должно планироваться и осуществляться с учетом конкретных обстоятельств экономической деятельности.

© Захаров О. Ю., 2012

© Автор, 2012

Содержание

Введение	5
Глава 1	6
Глава 2	12
Глава 3	21
Конец ознакомительного фрагмента.	25

Олег Захаров

Менеджмент безопасности бизнеса

Введение

В последние годы большинство экономических структур, фирм и особенно банков стали уделять все больше внимания средствам повышения своей безопасности. Наличие существенной собственности вынуждает предпринимательские структуры самим заниматься обеспечением безопасности. Особую актуальность приобрели навыки поиска, сбора и анализа информации, зачастую противоречивой и сомнительной, большей частью неколичественной. Появились новые каналы создания угроз для безопасности организации, связанные с персоналом.

В сложной обстановке нашей действительности с особой остротой стоит задача создания благоприятного климата для развития цивилизованного бизнеса, защищенности прав и интересов предпринимателей. Преимущество, заложенное в стабильности и безопасности, становится основным конкурентным преимуществом для организации. Безопасность, по определению, должна лежать в основе ранжирования предприятий по эффективности управления своими ресурсами. Экономическая ценность безопасности, далеко превосходит все финансовые активы, капиталовложения и другие ресурсы большинства организаций. Задача исключительной важности – научиться управлять организацией через призму безопасности. Только решив эту задачу мы можем рассчитывать на достижение стабильности в обществе и устойчивого развития российской экономики.

Главная цель этой книги – помочь читателю приобрести систематизированное представление об обеспечении безопасности предприятия как о комплексе разнообразных мероприятий в организационной, финансовой, информационной, кадровой и других сферах, каждое из которых должно планироваться и осуществляться с учетом конкретных обстоятельств экономической деятельности.

В первых главах рассматриваются основные понятия предпринимательства и безопасности, связанные с ней риски в современном бизнесе. Отмечается, что предпринимательство неотделимо от рисков и проблемы безопасности тесно связаны с рисками. Четвертая глава посвящена противодействию мошенничеству. В ней подчеркивается, что мошенничество представляют серьезную опасность не только для бизнесмена, но и для персонала организации. Достойное место в книге занимает рассмотрение методов защиты информации. Предпоследняя глава предлагает рассматривать надежные команды организации как залог безопасности.

После освоения предложенного материала Вы будете способны: сформировать систематизированное представление об обеспечении безопасности бизнеса как о комплексе разнообразных мероприятий в организационной, финансовой и других сферах, каждое из которых должно планироваться и осуществляться с учетом конкретных обстоятельств;

- создать ясное представление о важнейших направлениях обеспечения безопасности бизнеса, включая понимание о возможных направлениях угроз, повышающих риски бизнеса, об организациях-агрессорах, и выбирать главные направления с учетом реально складывающейся обстановки;

- обеспечить юридическую составляющую системы комплексной безопасности предприятия;

- создать систему защиты конфиденциальной информации на Вашем предприятии;

- проводить мероприятия по сбору и анализу необходимой коммерчески важной информации о конкурентах.

Глава 1

Цели и задачи системы комплексной безопасности бизнеса

Реалии российской экономической жизни таковы, что предприниматели в своей практической деятельности сталкиваются не только с экономическими, организационными, правовыми трудностями в процессе создания своего дела и его развития, но и с негативным воздействием некоторых субъектов, зачастую носящим противоправный характер. Это, в свою очередь, обуславливает необходимость поддержания достаточного уровня безопасности бизнеса. Что же такое бизнес, в каких формах он реализуется, каковы угрозы его безопасности и на чем основаны способы защиты от них – все эти вопросы были и остаются актуальными в России.

Бизнес (предпринимательская деятельность), может быть охарактеризован с двух точек зрения – экономической и правовой.

С экономической точки зрения бизнес выполняет определенную функцию в экономическом развитии любой страны. Функция предпринимателей заключается в том, что они реализуют нововведения, играющие ведущую роль в развитии экономики. Нововведения включают внедрение новых продуктов, технологий, освоение новых рынков сбыта и источников сырья, применение организационных новшеств и т.п. Синонимом русского термина "нововведение" является все более часто употребляемое понятие "инновация".

Следовательно, с экономической точки зрения бизнес, это инновационная деятельность, а сам предприниматель является носителем новаторской функции.

Правовая точка зрения предполагает другие критерии предпринимательской деятельности. По российскому законодательству предпринимательство – это деятельность: самостоятельная;

осуществляемая на свой риск;

направленная на систематическое получение прибыли;

может заключаться в пользовании имуществом, продаже товаров выполнении работ, оказании услуг;

предполагающая государственную регистрацию лиц как предпринимателей.

Нормальное функционирование и развитие сферы предпринимательства в экономике любой страны требует наличия определенных условий, обеспечивающих эти процессы. Одним из важнейших условий выступает безопасность бизнеса.

Под безопасностью бизнеса следует понимать состояние защищенности субъекта предпринимательской деятельности на всех стадиях его функционирования от внешних и внутренних угроз, имеющих негативные, прежде всего экономические, а также организационные, правовые и иные последствия.

Безопасность бизнеса может оцениваться с помощью различных критериев, то есть признаков, на основании которых делается оценка.

Во-первых, ее можно оценить с организационной стороны. В этом случае предполагается сохранение как самой фирмы, так и ее организационной целостности, нормальное функционирование основных подразделений (отделов, служб и т.п.). Основные подразделения фирмы (например, отдел снабжения, производственный отдел, финансовый отдел или бухгалтерия, служба маркетинга) выполняют все свои функции для достижения основной цели фирмы.

Во-вторых, это оценка с правовой стороны. Имеется в виду постоянное обеспечение соответствия деятельности фирмы действующему законодательству, что выражается в отсутствии претензий со стороны правоохранительных органов (или контрагентов) к фирме. Кроме

того, отсутствуют потери от сделок с внешними партнерами вследствие нарушения последними законодательства (умышленно либо неумышленно). Это обеспечивается юридической экспертизой всех осуществляемых операций и сделок, заключаемых договоров.

В-третьих, с информационной стороны. Безопасность может быть оценена как сохранение состояния защищенности внутренней конфиденциальной информации от утечки или разглашения в различных формах.

В-четвертых, с экономической стороны. Это проявляется в стабильных или имеющих тенденцию к росту основных финансово-экономических показателях деятельности фирмы (таких как собственный капитал, объем годового оборота, прибыль, рентабельность). В них отражаются общие результаты обеспечения безопасности с организационной, правовой, информационной и собственно экономической сторон. Сюда могут входить такие показатели, как отсутствие штрафов, санкций со стороны государственных органов за нарушение законодательства (например, налогового, антимонопольного), отсутствие потерь от сделок с недобросовестными контрагентами.

Таким образом, в наиболее общем виде о безопасности фирмы свидетельствуют сохранение ее как целостного структурного образования и юридического лица и устойчивые (либо растущие) значения основных финансово-экономических показателей. Применительно же к конкретной стороне деятельности фирмы, могут использоваться специфические показатели ее безопасности.

Однако в процессе хозяйствования субъекты предпринимательской деятельности могут испытывать воздействия различных физических и юридических лиц, которые несут негативные последствия, прежде всего для экономического состояния фирмы. В этом случае возникает понятие угрозы безопасности предпринимательства. Причем наиболее важное значение для субъекта предпринимательской деятельности приобретают угрозы экономической безопасности, поскольку все потери (организационные, информационные, материальные, имиджа фирмы) в конечном счете выражаются именно в экономических потерях, то есть потерях финансовых средств (и все прочие угрозы в основе имеют, как правило, экономические мотивы).

Деятельность предпринимателей в современных условиях хозяйствования в России является весьма сложной. И это связано с рядом специфических факторов, усиливающих активизацию угроз экономической безопасности предпринимательства. Среди этих факторов наибольшее значение имеют следующие.

Значительная степень монополизации рынка, частично сохранившаяся от прежней административно-командной системы, частично – вновь возникающая. Одновременно нарастает уровень конкурентной борьбы за российские рынки как со стороны отечественных, так и зарубежных производителей.

Сохранение значительного давления на субъекты предпринимательской деятельности со стороны государственных органов (например, в сферах лицензирования, налогообложения).

Наличие ряда социальных проблем – низкий уровень доходов населения, безработица вызванная мировым финансовым кризисом, текучесть кадров, все это снижает степень ответственности и увеличивает вероятность склонности работника к продаже секретов фирмы и прочим незаконным действиям.

Активизация шпионской и разрушительной деятельности со стороны спецслужб развитых стран и крупных компаний, имеющих большой опыт в данной сфере деятельности.

Кроме того, предпринимательская деятельность, по своей сути, является весьма разносторонней. Она связана с решением организационных вопросов, правовыми и экономическими проблемами, техническими аспектами, кадровыми и т.д. Особенно усложняется управление такой деятельностью когда фирма является крупным, диверсифицированным про-

изводственным предприятием, которое имеет широчайшие деловые связи и значительное количество контрагентов: поставщиков, кредиторов, заемщиков, клиентов.

В любом случае каждая фирма представляет собой систему, включающую основные элементы и связи между ними. Система – это совокупность объектов, взаимодействие которых обуславливает наличие интегративных качеств, не свойственных ее частям, компонентам. Как раз по линиям внутренних и внешних связей системы (фирмы) и могут реализоваться угрозы ее экономической безопасности. Для обеспечения максимальной степени защиты от этих угроз и необходима определенная деятельность, которая также должна носить системный характер.

Объектом системы обеспечения безопасности выступает стабильное экономическое состояние субъекта предпринимательской деятельности в текущем и перспективном периоде. Именно от объекта защиты во многом зависят основные характеристики системы обеспечения безопасности. Поскольку объект защиты является сложным, многоаспектным, то эффективное обеспечение безопасности должно основываться на комплексном подходе к управлению этим процессом. Комплексный подход предполагает учет в управлении объектом всех основных его аспектов и все элементы управляемой системы рассматриваются только в совокупности, целостности, единстве. Таким образом, необходимо создание комплексной системы обеспечения безопасности бизнеса.

Комплексная система безопасности бизнеса – это совокупность взаимосвязанных мероприятий организационно-правового характера, осуществляемых в целях защиты предпринимательской деятельности от реальных или потенциальных действий физических или юридических лиц, которые могут привести к существенным экономическим потерям.

В основе разработки комплексной системы безопасности бизнеса должна лежать определенная концепция. Концепция включает цель комплексной системы безопасности, ее задачи, принципы деятельности, объект и субъект, стратегию и тактику.

Цель данной системы – минимизация внешних и внутренних угроз экономическому состоянию субъекта предпринимательства, в том числе его финансовым, материальным, информационным, кадровым ресурсам, на основе разработанного и реализуемого комплекса мероприятий экономико-правового и организационного характера. Следует иметь в виду, что наибольшее значение в деле обеспечения безопасности бизнеса принадлежит первичным – экономико-правовым и организационным мерам, обеспечивающим фундамент, основу системы безопасности, в отличие от вторичных – технических, физических и пр.

В процессе достижения поставленной цели осуществляется решение конкретных задач, объединяющих все направления обеспечения безопасности.

Задачи, решаемые системой безопасности бизнеса:

- прогнозирование возможных угроз безопасности предприятия;
- организация деятельности по предупреждению возможных угроз (превентивные меры);
- выявление, анализ и оценка возникших реальных угроз безопасности предприятия;
- принятие решений и организация деятельности по реагированию на возникшие угрозы;
- постоянное совершенствование системы обеспечения безопасности предпринимательства.

Организация и функционирование комплексной системы безопасности бизнеса в целях максимальной эффективности должны основываться на ряде следующих принципов.

Принцип законности. Вся деятельность фирмы, в том числе ее службы безопасности должна носить безусловно законный характер, иначе система обеспечения безопасности может быть разрушена по вине самого субъекта предпринимательства. В качестве негативных последствий могут быть различного рода санкции правоохранительных органов, привлечение в качестве ответчика в суд, шантаж со стороны криминальных структур.

Принцип экономической целесообразности. Следует организовывать защиту только тех объектов, затраты на защиту которых меньше, чем потери от реализации угроз этим объектам.

Здесь также должны учитываться финансовые возможности фирмы по организации системы безопасности.

Сочетание превентивных и реактивных мер. Превентивные – меры предупредительного характера, позволяющие не допустить возникновения или реализации угроз безопасности. Реактивные – меры, которые предпринимаются в случае реального возникновения угроз или необходимости минимизации их негативных последствий.

Принцип непрерывности – предполагает, что функционирование комплексной системы безопасности бизнеса должно осуществляться постоянно.

Принцип дифференцированности. Выбор мер по преодолению возникших угроз происходит в зависимости от характера угрозы и степени тяжести последствий ее реализации.

Координация. Для достижения поставленных задач необходимо постоянное согласование деятельности различных подразделений службы безопасности, самой фирмы и сочетание организационных, экономико-правовых и прочих способов защиты.

Полная подконтрольность системы обеспечения безопасности руководству субъекта предпринимательской деятельности. Это необходимо во-первых, для того, чтобы система безопасности не превратилась в замкнутое образование, ориентированное на решение узких задач, без учета интересов фирмы в целом, а во-вторых, для оценки эффективности деятельности системы и ее возможного совершенствования.

Объект и субъект системы обеспечения безопасности бизнеса тесно взаимосвязаны. Объектом системы в целом, как уже говорилось, выступает стабильное экономическое состояние субъекта предпринимательской деятельности в текущем и перспективном периоде. Конкретными же объектами защиты выступают ресурсы: финансовые, материальные, информационные, кадровые.

Субъект системы обеспечения безопасности бизнеса носит более сложный характер, поскольку его деятельность обуславливается не только особенностями и характеристиками объекта, но и специфическими условиями внешней среды, которая окружает субъект предпринимательской деятельности. Исходя из этого, можно выделить две группы субъектов, обеспечивающих безопасность предпринимательства:

- внешние субъекты;
- внутренние субъекты.

К внешним субъектам относятся органы законодательной, исполнительной и судебной власти призванные обеспечивать безопасность всех без исключения законопослушных участников предпринимательских отношений; причем деятельность этих органов не может контролироваться самими предпринимателями. Эти органы формируют законодательную основу функционирования и защиты предпринимательской деятельности в различных ее аспектах и обеспечивают ее исполнение.

К внутренним субъектам относятся лица, непосредственно осуществляющие деятельность по защите безопасности данного конкретного субъекта предпринимательства. В качестве таких субъектов могут выступать:

- работники собственной службы безопасности фирмы (предприятия);
- приглашенные работники из специализированных фирм, оказывающих услуги по защите предпринимательской деятельности.

Субъекты, обеспечивающие безопасность предпринимательства, осуществляют свою деятельность на основе определенной стратегии и тактики.

Стратегия – это долгосрочный подход к достижению цели. Генеральная стратегия безопасности выражается через общую концепцию комплексной системы обеспечения безопасности предпринимательской деятельности. Помимо генеральной стратегии выделяются также специальные стратегии (например, в зависимости от стадии предпринимательской деятельности). Наконец, могут применяться функциональные стратегии безопасности.

Стратегия безопасности включает, прежде всего, систему превентивных мер, реализуемая через регулярную, непрерывную, работу всех подразделений субъекта предпринимательской деятельности по проверке контрагентов, анализу предполагаемых сделок, экспертизе документов, выполнению правил работы с конфиденциальной информацией и т.п. Служба безопасности в этом случае выполняет роль контролера.

Стратегия реактивных мер, применяемая в случае возникновения или реального осуществления каких-либо угроз безопасности предпринимательства. Эта стратегия, основанная на применении ситуационного подхода и учете всех внешних и внутренних факторов, реализуется службой безопасности через систему мер, специфических для данной ситуации.

Тактика обеспечения безопасности предполагает применение конкретных процедур и выполнение конкретных действий в целях обеспечения безопасности субъекта предпринимательства. Этими действиями, в зависимости от характера угроз и тяжести последствий их реализации, могут быть, например:

- расширение юридической службы фирмы;
- принятие дополнительных мер по сохранности коммерческой тайны;
- создание подразделения компьютерной безопасности.
- предъявление претензий контрагенту-нарушителю;
- обращение с иском в судебные органы;
- обращение в правоохранительные органы;

Основными функциями службы безопасности фирмы являются следующие:

- организация и осуществление совместно с подразделениями фирмы защиты конфиденциальной информации;
- проверка сведений о попытках шантажа, провокаций и иных акций в отношении персонала, преследующих цель получения конфиденциальной информации о деятельности фирмы;
- организация сбора, накопления, автоматизированного учета и анализа информации по вопросам безопасности;
- проведение проверок в подразделениях фирмы и оказание им практической помощи по вопросам безопасности их деятельности;
- разработка и внедрение положения о коммерческой тайне;
- проверка правил ведения закрытого делопроизводства;
- проверка работников на предмет соблюдения правил обеспечения экономической, информационной и физической безопасности;
- оказание содействия отделу кадров по работе с персоналом в вопросах подбора, расстановки, служебного перемещения и обучения персонала;
- сбор, обработка, хранение, анализ информации о контрагентах с целью предотвращения сделок с недобросовестными партнерами;
- выполнение поручений руководства фирмы, входящих в компетенцию службы;
- взаимодействие с правоохранительными органами, проведение мероприятий по выявлению и предупреждению различного рода финансово-хозяйственных правонарушений;
- проведение служебных расследований по фактам разглашения конфиденциальной информации, потери служебных документов работниками фирмы и действий угрожающих экономической безопасности фирмы.

Целями обеспечения безопасности бизнеса являются:

- устранение внешних и внутренних угроз экономическому благосостоянию компании, фирмы, организации;
- обеспечение благоприятных условий реализации основных интересов, закрепленных в их учредительных документах.

Задачи обеспечения безопасности состоят в:

- своевременном выявлении реальных и потенциальных угроз жизненно важным интересам фирмы, компании, корпорации организации;

- эффективном противодействии и борьбе с факторами, препятствующими реализации законных прав, интересов компании, фирмы и их сотрудников;

- сохранении интеллектуальной и материальной собственности фирмы, компании, корпорации организации;

- вскрытии внутренних причин и условий, способствующих нанесению фирме, компании, корпорации, организации, их сотрудникам материального, психологического, физического или иного ущерба;

- разработке и реализации механизма оперативного реагирования на возникающие условия и негативные тенденции в развитии обстановки в отношении фирмы, компании, корпорации, организации;

- сборе, анализе, оценке и представлении руководству информации по поводу правонарушений в отношении фирмы, компании, корпорации, организации со стороны физических и юридических лиц;

- предотвращении проникновения в структуру криминальных элементов;

- противодействии техническому проникновению на предприятие субъектов противоправной деятельности;

- физической и технической охране фирмы, компании, корпорации, организации, их территории и транспорта;

- способствовании в формировании и повышении положительного имиджа фирмы, компании, корпорации, организации среди партнеров, клиентов, общественности и населения;

- локализации или ослаблении вредных последствий действий в отношении фирмы, компании, корпорации, организации со стороны внешних и внутренних факторов угрозы.

В заключение данной главы сформулирую ряд аксиом, которые должны отчетливо осознавать предприниматели:

- безопасность – это наука, которую надо изучать и развивать, это искусство, которое надо постигать, это культура, которую надо у бизнесменов воспитывать;

- всякий бизнес только тогда чего-нибудь стоит, когда он надежно защищен;

- опасность легче предупредить, чем с ней бороться;

- основа успеха в бизнесе – своевременно полученная, правильно понятая и умело использованная информация.

Глава 2

Основные источники угроз предпринимательской деятельности

Угрозы безопасности предпринимательства – это потенциальные или реальные действия физических или юридических лиц, нарушающие состояние защищенности субъекта предпринимательской деятельности и способные привести к прекращению его деятельности, либо к экономическим и другим потерям.

Надо иметь в виду, что угрозой безопасности предпринимательства может быть не всякое действие, имеющее негативные последствия. Так, не следует считать угрозой безопасности предпринимательства деятельность руководства фирмы по вложению средств в ценные бумаги, внедрение новых организационных форм, организацию производства совершенно нового товара. Все эти управленческие решения являются рискованными и могут иметь негативные экономические последствия вследствие того, что может резко измениться конъюнктура на рынке ценных бумаг, потребности населения, либо новые организационные формы не оправдают себя. Но нужно иметь в виду, что в конечном счете все это направлено на достижение основной цели фирмы, на ее дальнейшее развитие. Такого рода решения составляют неотъемлемую часть самой предпринимательской деятельности, которая осуществляется на свой риск и предполагает определенные потери.

Действия же, определяемые как угрозы, сознательно направлены на получение какой-либо выгоды от экономической дестабилизации предприятия, от посягательств на ее безопасность.

Деятельность руководства предприятия, несмотря на рискованный характер, в общем и целом соответствует действующему законодательству. Угрозы, как правило, предполагают нарушение законодательных норм (той или иной отрасли права – гражданского, административного, уголовного) и предполагают определенную ответственность лиц, их осуществляющих.

Таким образом, можно отметить три признака, характерных для угроз безопасности предпринимательской деятельности:

- сознательный и корыстный характер;
- направленность действий на нанесение ущерба субъекту предпринимательства;
- противоправный характер.

При определении угроз необходимо руководствоваться рядом параметров:

- реальностью угрозы;
- сутью противоречий, породивших угрозу;
- остротой этих противоречий;
- срочностью их разрешения;
- определением сил и средств, которыми может располагать и воспользоваться оппонент;
- разработкой и выявлением признаков возможной угрозы.

К тому же необходимо разработать систему признаков и этапов подготовки и осуществления угрозы, выработки прогнозов и рекомендаций по локализации опасности.

По источнику возникновения все угрозы можно разделить на внешние и внутренние. К внешним могут относиться такие, например, как хищение материальных средств и ценностей лицами, не работающими в данной фирме, промышленный шпионаж, незаконные действия конкурентов, вымогательство со стороны криминальных структур. Внутренние – разглашение собственными сотрудниками конфиденциальной информации, низкая квалификация специалистов, разрабатывающих документы, неэффективная работа службы безопасности и лиц отве-

чающих за проверку контрагентов. Наибольшую опасность, как правило, представляют внешние угрозы, поскольку внутренние угрозы зачастую – это реализация внешних "заказов".

По степени тяжести последствий: угрозы с высокой, значительной, средней и низкой тяжестью последствий.

Высокая тяжесть означает, что эти угрозы могут привести к резкому ухудшению всех финансово-экономических показателей деятельности субъекта предпринимательства, что вызывает немедленное прекращение его деятельности либо наносят такой непоправимый вред, который приведет к этим же последствиям позднее. В этом случае происходит ликвидация фирмы. Значительная степень тяжести последствий реализации угроз предполагает возможность нанесения фирме таких финансовых потерь, которые окажут негативное воздействие на основные финансово-экономические показатели фирмы, на ее деятельность в будущем и преодолеваются в течение длительных сроков времени.

Средняя степень тяжести означает, что преодоление последствий осуществления этих угроз требует затрат (наносит потери), сопоставимые с текущими затратами фирмы и не требует значительного времени.

Последствия реализации угроз с низкой степенью последствий не оказывают какого-либо существенного воздействия ни на стратегические позиции фирмы, ни даже на ее текущую деятельность.

По степени вероятности угрозы могут быть маловероятными и реальными.

К маловероятным угрозам относится, например, посещение лицом без определенного места жительства помещений фирмы с требованием о выдаче ему денег с использованием нецензурной брани. Факторы малой вероятности данной угрозы:

- угрожает один человек (а не организованная группа);

- отсутствуют реальные возможности приведения угрозы в исполнение;

- существуют достаточно простые способы защиты (путем физического выдворения данного лица, либо сдача его правоохранительным органам).

К реальным угрозам относятся, например, те, которые:

- сопровождаются физическим насилием, повреждением имущества фирмы, похищением работников (руководителей);

- осуществляются организованной группой, выдвигающей конкретные требования и определенные суммы;

- осуществляются с участием "квалифицированных" криминальных "специалистов".

Угрозы могут различаться по воздействию на стадии предпринимательской деятельности. Наиболее вероятны и опасны угрозы на стадии создания фирмы и на стадии ее функционирования.

В первом случае это могут быть незаконные действия со стороны должностных лиц, препятствующие организации фирмы, либо вымогательство со стороны преступных группировок. На стадии функционирования угрозы могут возникать на подготовительном этапе (воспрепятствование нормальному снабжению сырьем, материалами, оборудованием), собственно производственном этапе (уничтожение или повреждение имущества, оборудования, кража "ноу-хау"), на этапе заключительном (воспрепятствование сбыту, ограничение конкуренции, незаконное ограничение рекламы).

Угрозы могут различаться по объекту посягательств. Объектом посягательств выступают прежде всего ресурсы: трудовые (персонал), материальные, финансовые, информационные. Угрозы персоналу – шантаж с целью получения конфиденциальной информации, похищение сотрудников, вымогательство и пр. Угрозы материальным ресурсам – повреждение зданий, помещений, систем связи, кража оборудования. Угрозы финансовым ресурсам – мошенничество, фальсификация финансовых документов, валюты, кража денежных средств. Угрозы

информационным ресурсам – несанкционированное подключение к информационной сети фирмы, изъятие конфиденциальных документов и пр.

По субъектам угроз:

- угрозы со стороны криминальных структур;
- угрозы со стороны недобросовестных конкурентов;
- угрозы со стороны контрагентов;
- угрозы со стороны собственных сотрудников.

По виду ущерба – угрозы, реализация которых несет прямой ущерб и угрозы, реализация которых приведет к упущенной выгоде.

Весьма своеобразная классификация угроз может быть предложена по характеру ответственности субъектов, деятельность которых может квалифицироваться как посягательство на безопасность предпринимательской деятельности.

В этом случае ответственность, наступающая в результате последствий деятельности, определяемой как посягательство на безопасность предпринимательства может носить как гражданско-правовой, так и уголовно-правовой характер.

По характеру ответственности лица (юридического или физического), несущего (или реализующего) угрозу безопасности предпринимательства можно выделить:

угрозы, в результате реализации которых к лицам их осуществляющим могут быть применены нормы гражданско-правовой ответственности;

– угрозы, в результате попытки или реализации которых к лицам их осуществляющим могут быть применены меры уголовно-правовой ответственности.

Теперь рассмотрим внешние и внутренние угрозы более подробно. К внешним угрозам можно отнести следующие:

- рост промышленного шпионажа с использованием агентурного и технического проникновения в коммерческие, технологические и производственные тайны предприятия;
- безналичная форма расчетов с использованием компьютерных систем;
- несанкционированное проникновение в банки данных;
- отсутствие единой действенной стратегии обеспечения безопасности бизнеса и механизма ее реализации;
- недобросовестная конкуренция, часто носящая криминальные формы;
- кризисные явления в экономике;
- непредсказуемые изменения конъюнктуры рынка;
- социальная напряженность;
- чрезвычайные происшествия;
- административные гонения на рынок;
- неблагоприятная для частного бизнеса экономическая политика государства;
- манипулирование учетной ставкой, валютным курсом, таможенными пошлинами, налогами;

– угрозы, исходящие от несогласованности нормативных актов, издаваемых законодательными и исполнительными органами государства, а также различными министерствами и ведомствами, которые иногда противоречат законам и друг другу, однако все равно подлежат исполнению.

Бороться с этими актами и инструкциями теоретически можно только с помощью судебных органов, однако на практике это, как правило, себе дороже. Поэтому вероятность негативных последствий для предприятий от этой группы угроз может быть уменьшена только путем повышения качества юридического и бухгалтерского оформления проводимой деятельности.

Эту вероятность может повысить или понизить характер взаимоотношений с конкретными представителями контролирующих организаций.

С учетом того, что эти угрозы объективно являются серьезными, данные вопросы должны быть постоянно в поле зрения руководства предприятия. Как правило, это достигается путем подбора квалифицированных кадров, как непосредственно юристов и бухгалтеров, так и людей их контролирующих или обеспечивающих соответствующие направления деятельности предприятия.

К этой группе угроз следует отнести и не спровоцированные претензии со стороны различных контролирующих организаций (пожарные, санэпидемические и др.).

Следующая по значимости группа угроз вытекает из невыполнения партнерами, заказчиками, поставщиками, клиентами и другими своих обязательств по оплате контрактов, поставке товаров и т.п.

В этом случае ущерб возникает из-за неправильного прогноза всех возможных последствий того или иного мероприятия, что, в свою очередь, обусловлено следующими обстоятельствами:

- неосведомленностью наличия у партнера долгов перед другими предприятиями или физическими лицами или недооценкой таких факторов;

- неосведомленностью о контактах партнера с криминальными структурами и о характере их взаимоотношений, в результате чего деньги или товары предприятия, попавшие к партнеру, могут бесследно исчезнуть в этих структурах. В этом случае возместить ущерб практически невозможно из-за специфики многообразных не писанных правил, действующих в данной сфере;

- при длительном успешном сотрудничестве с партнером, как правило, притупляется бдительность, что, как показывает практика, совершенно не обосновано. Как бы ни складывались взаимоотношения в любой момент может возникнуть угроза невыполнения партнером своих обязательств. Это может произойти как в силу субъективных намерений партнера обмануть Ваше предприятие, так и в силу независящих от него обстоятельств, в частности, обусловленных предыдущими обстоятельствами, но уже в отношении его фирмы.

Поэтому, как бы хорошо ни складывались отношения с партнером каждую сделку следует рассматривать и проверять как первую: заманчивость отдельных предложений часто мешает руководству предприятия объективно оценивать их реальность с точки зрения реальных экономической, юридической, финансовой и криминальной сторон предлагаемого договора, особенно если партнер ранее зарекомендовал себя надежным исполнителем обязательств.

Как правило, при тщательной объективной оценке указанных сторон проекта возникают сомнения, заставляющие обоснованно от него отказаться, не подвергая себя угрозам или минимизировать их при реализации проекта.

Получая какие-либо коммерческие предложения от незнакомого партнера, не следует торопиться с проверкой этого партнера, а попытаться подыскать партнера ранее хорошо себя зарекомендовавшего или имеющего солидные рекомендации (в том числе со стороны службы безопасности), реально способного осуществить аналогичную операцию.

Это объясняется тем, что для специалистов, работающих в рассматриваемых сферах безопасности, как правило, легче подыскать через свои каналы подходящего надежного партнера, чем с достаточной степенью надежности проверить неизвестную фирму. Возможны не спровоцированные попытки нанесения ущерба предприятию со стороны других юридических и физических лиц.

Выявление и предупреждение данной группы угроз лежит в сфере функциональных обязанностей службы безопасности.

В сфере бизнеса постоянно существуют потенциальные и реальные угрозы со стороны субъектов противоправных действий. К таким субъектам относятся:

Криминальные элементы: *К криминальным элементам относятся:*

- организованная преступность;

- случайные (временные) преступные группы;
- преступники-одиночки.

Организованная преступность: *Организованная преступность представлена в виде:*

- сообществ "воров в законе", не имеющих аналогов в мировой криминальной практике;
- банд;
- группировок;
- организованных групп.

Отличительными признаками организованных преступных группировок являются:

- наличие материальной и финансовой базы;
- коллегиальный орган управления – "совет";
- устав организации в форме неформальных норм поведения, традиций, законов, санкций за их нарушение;
- функционально-иерархическая система построения организации;
- наличие информационных баз коррумпированных чиновников, положения дел в органах власти и управления, особенно в правоохранительной системе, банках, фирмах и других предпринимательских структурах, товародвижении, конъюнктуре рынка, ценах на наркотики и т.д.;

наличие своих людей в органах власти, судебной и правоохранительной системах;

- специфическая языково-понятийная система, которая включает жаргон, особенности письменной речи.

Случайные (временные) преступные группы

Такие группы возникают, как правило, спонтанно или для совершения одного преступления. Они отличаются неустойчивостью во времени и отсутствием строго регламентированных систем взаимодействия и подчиненности.

Преступники-одиночки

Эта категория криминальных элементов как правило, действует индивидуально, а если имеют сообщников, то используют их либо в темную, либо не информируя в полном объеме о своих преступных намерениях. Преступниками-одиночками могут быть как лица с криминальным прошлым, так и пошедшие на совершения преступления под влиянием неблагоприятных обстоятельств.

Российские фирмы, занимающиеся промышленным шпионажем

На рынке услуг появилось большое число фирм, предоставляющих клиентам такие услуги, как несанкционированное проникновение в чужие базы данных, прослушивание телефонных переговоров, установка подслушивающей аппаратуры во время переговоров, хищение документов, содержащих коммерческую тайну и т.п.

Конкуренты

Конкуренты это – фирмы, компании и другие организации, которые:

- занимаются аналогичной деятельностью;
- претендуют на использование тех же помещений, оборудования, офисов и производства;
- используют одни и те же коммуникации;
- испытывают нужду в специалистах, работающих в банке, фирме. *Конкуренция обычно выражается в таких формах, как:*
- соперничество,
- противоборство.

Соперничество предполагает цивилизованную борьбу между компаниями или группами компаний за потребителя, поставщика, выгодные условия кредитования, голоса избирателей. При соперничестве конкуренты действуют в рамках закона или на грани его нарушения.

При противоборстве, предпочтение отдается таким формам недобросовестной конкуренции, которые позволяют уничтожить конкурента или нанести ему серьезный ущерб.

Торговые предприятия и фирмы конкурируют за счет контрабандного ввоза продукции из-за рубежа, беспошлинного ввоза за счет фирм, освобожденных от таможенных сборов. Ярким примером является компания «Евросеть» практиковавшая ввоз сотовых телефонов по черным и серым схемам.

К недобросовестной конкуренции относятся также:

- нарушение прав конкурентов (незаконное использование марки товаров конкурента, воспроизводство его продукции худшего качества, раскрытие его секретов производства и торговли, промышленный шпионаж);

- подрыв репутации конкурента: распространение ложных сведений, дискредитация предприятия, его продукции, торговой деятельности, ложная реклама;

- дезорганизация производства конкурентов: сманивание специалистов, демпинг;

- конкуренции дополняют протекционистские барьеры на государственном уровне, монополистическое давление.

В конкурентной борьбе широко используются:

- получение налоговых и иных льгот;
- коррупция;
- использование запрещенных методов добывания информации;
- дезинформация;
- использование криминальных методов борьбы;
- работа через подставные фирмы, пользующиеся льготами.

Наиболее популярными приемами и методами являются:

- дискредитация конкурента и его продукции в глазах потребителей, партнеров, кредитных организаций;

- вредительство;
- диверсии (поджоги, взрывы);
- захват заложников;
- шантаж;
- убийство предпринимателей и т.д.

Как правило, для проведения подобных акций конкуренты прибегают к услугам криминальных структур или фирм, занимающихся промышленным шпионажем.

Иностранные компании и фирмы, прежде всего транснациональные компании.

В мире насчитывается не менее 55 тысяч компаний, весьма активно занимающихся промышленным шпионажем, в том числе и в России. В их деятельности по добыванию конфиденциальной информации прослеживается закономерность: чем выше рост инфляции и социальной напряженности, тем активнее ведется добывание сведений о конкурентах, по экономическим, научно-техническим, политическим и иным аспектам.

Транснациональные компании создают свои подразделения разведки и контрразведки, филиалы за рубежом, группы лоббирования своих интересов, вербуют осведомителей. В необходимых случаях транснациональные компании используют и свои государственные специальные службы.

Американские, германские и другие западные исследовательские структуры в виде фондов, университетов, ассоциаций и т.д., осуществляют легальную разведку по экономическим, научно-техническим, политическим и военным вопросам. В последнее время они проявляют интерес и к информации о предпринимательских структурах.

К источникам **внутренних угроз** безопасности относятся:

- руководители фирмы, компании, организации;

- менеджеры среднего звена;
- сотрудники фирмы;
- персонал службы безопасности.

Угроза безопасности фирмы, компании, организации со стороны этой группы субъектов может носить:

- целенаправленный характер;
- произвольный характер;
- случайный характер.

Угроза безопасности с их стороны выражается в:

- принятии ошибочных решений, реализация которых может иметь негативные последствия для экономического, политического или иного положения фирмы;

умышленных или ошибочных действиях, приводящих к выходу из строя оборудования, сложной оргтехники и т.п.;

- умышленном нанесении ущерба за счет разглашения сведений, содержащих коммерческую тайну;

- нарушениях требований должностных инструкций и правил внутреннего распорядка;

- распространении слухов, подстрекательстве к групповому отказу от деятельности;

- инспирировании конфликтных ситуаций;

непроизвольном разглашении третьим лицам информации, содержащей коммерческую тайну.

К внутренним угрозам относятся и внутренние конфликты между руководителями предприятия, управленческая некомпетентность, отсутствие глубокого профессионализма в работе, а также кражи и различные нарушения со стороны собственного персонала предприятия. Рассмотрим данные положения подробнее.

Конфликты на предприятии

Разногласия в коллективе могут возникать по разным причинам. Наиболее часто разногласия между руководителями возникают из-за борьбы за руководящую должность, при распределении «грязных» доходов фирмы, при психологической несовместимости отдельных сотрудников. Руководителю предприятия необходимо просчитывать рост своих сотрудников на несколько лет вперед. Ибо два-три сотрудника, претендующие в будущем на какую-то руководящую должность, ведут между собой конкурентную борьбу за получение этой должности. При достижении одним из них своей цели другие окажутся обиженными и из лояльных сотрудников фирмы могут стать ее врагами. Подобный вариант конкуренции может сложиться и между генеральным директором и его заместителем, что неизбежно приведет к серьезному осложнению отношений между ними. Стрессовые ситуации в коллективе создают люди психически неуравновешенные, амбициозные, преувеличивающие свои возможности, завистливые, конфликтные, жадные и нечестные.

Некомпетентность руководства

Некомпетентность и низкий профессиональный уровень руководства в конечном счете приводит к экономическому и финансовому краху предприятия. Подобную картину можно наблюдать в ряде акционерных обществ и в финансовых структурах. Особенно сложное положение складывается в фирмах, где руководящие должности распределяются между родственниками и лично преданными людьми, не являющимися профессионалами. Поэтому, при подборе руководящих кадров, значительное внимание должно уделяться их профессиональной компетентности, степени лояльности, анализу и учету личных устремлений, надежности, психологической грамотности в общении с партнерами, изучению поведения в экстремальных ситуациях, стремлению к лидерству.

Персонал предприятия

Наибольший ущерб собственный персонал приносит в банковском деле и торговле. В области финансов и экономики 95% хищений финансовых средств совершается персоналом банков.

К объектам защиты относятся от потенциальных и реальных угроз относятся:

материальные ценности, включая:

– здания, сооружения, территории, принадлежащие фирме, компании, корпорации, организации;

– технологическое оборудование, оргтехнику, мебель и предметы интерьера; деньги и ценные бумаги;

– автотранспорт и т.п.;

информация и информационные потоки, такие как:

– компьютерные базы данных;

– документооборот по каналам локальных внутренних сетей и каналам обмена информацией с внешними адресатами в отношении наличия в них сведений, содержащих коммерческую тайну;

– различного рода документы, выполненные на бумажных, аудио-, видео- и иных, носителях и содержащие сведения, составляющие коммерческую тайну;

– сведения, передаваемые во время переговоров, совещаний в ходе телефонного общения, затрагивающие жизненно важные для фирмы, компании, организации вопросы;

руководители и персонал.

Угрозы помещениям, оборудованию и материальным ценностям выражаются в:

– их повреждении или уничтожении;

– захватах;

– поджогах;

– минировании;

– обстрелах;

– взрывах.

Угрозы информации проистекают из промышленного шпионажа.

Структуры, занимающиеся промышленным шпионажем в отношении своих конкурентов-банков, фирм и других коммерческих организаций, интересуются прежде всего следующими вопросами:

– стратегией и планами развития;

– финансовыми прогнозами, отчетами и положением;

– маркетингом;

– условиями оказания услуг;

– характеристиками производимой и перспективной продукции;

– сведениями о партнерах, клиентах и содержанием договоров с ними;

– организационной структурой;

– системой безопасности, прежде всего по защите конфиденциальной информации и т.д.

В процессе ведения промышленного шпионажа применяются следующие способы:

использование агентов, внедренных в фирму, компанию, организацию;

– привлечение к сотрудничеству служащих банков, фирм;

– сманивание сотрудников, обладающих ценной, конфиденциальной информацией;

– выведывание;

– подкуп ведущих специалистов и иных сотрудников;

– ложное приглашение сотрудников на работу с проведением с ними бесед для получения конфиденциальных сведений;

– ведение наблюдения за объектом и его сотрудниками;

– подслушивание переговоров с помощью технических средств;

- похищение необходимых документов;
- негласное фотографирование объекта, его сотрудников и документов;
- добывание информации через партнеров, клиентов, особенно пострадавших по вине конкурента;
- получение информации через коррумпированных сотрудников государственных структур;

- копирование документов;
- подделка документов и печатей и т.д.

Угрозы персоналу фирм, компаний, организаций заключаются в:

- нападениях;
- шантаже;
- вымогательствах;
- похищениях руководителей, сотрудников, членов их семей.

Система предупредительных мер включает деятельность по изучению контрагентов, анализ условий договоров, соблюдение правил работы с конфиденциальной информацией, защита компьютерных систем и т.д. Эта деятельность осуществляется регулярно и непрерывно. Она обеспечивает безопасность предпринимательской деятельности на основе постоянно действующей системы организационных мероприятий.

Однако даже самая лучшая система предупредительных мер не может предвидеть, а тем более преодолеть внезапно возникающие нестандартные угрозы, которые могут причинить значительный ущерб фирме, например мошеннического характера. Для противодействия этим угрозам необходимо применять специфический механизм. Американские специалисты в области выявления, расследования и предупреждения мошенничества, предлагают, например, использовать активную модель реагирования при обнаружении мошенничества. Отличительной особенностью этой оригинальной модели является во-первых, то, что она предусматривает обязательное реагирование на каждый случай на каждый случай мошеннических угроз, и, во-вторых, включает такие блоки, которые повышают эффективность работы службы безопасности.

В то же самое время, какую бы модель обеспечения безопасности ни выбрал предприниматель (руководитель фирмы), следует учитывать тот факт, что организация эффективной системы профилактических, предупредительных мер обойдется гораздо дешевле, чем борьба с последствиями уже случившихся правонарушений, реализованных угроз.

Глава 3

Правовая защита бизнеса

Сущность юридической защиты предпринимательства состоит в эффективном и всестороннем правовом обеспечении деятельности данного предприятия, четком соблюдении предприятием и его сотрудниками всех аспектов действующего законодательства при оптимизации затрат корпоративных ресурсов на достижение этих целей при активной работе соответствующих служб предприятия по благоприятному изменению внешней политико-правовой среды предприятия.

Процесс обеспечения юридической составляющей комплексной безопасности предприятия включает в себя предотвращение ущерба от негативных воздействий как субъективного, так и объективного характера. Негативные воздействия субъективного характера включают в себя недоработки в юридическом обеспечении деятельности предприятия, влекущие за собой финансовые и другие потери, причины которых лежат в сфере деятельности самого предприятия. К таким внутренним причинам низкой эффективности обеспечения юридической составляющей безопасности предприятия можно отнести низкую квалификацию сотрудников юридической службы предприятия, недостаточное финансирование данной службы, а также недостаточное внимание со стороны руководства предприятия к важности квалифицированного юридического обеспечения всех аспектов работы предприятия и непонимание необходимости комплексной юридической экспертизы любых планируемых и осуществляемых предприятием действий на предмет их соответствия требованиям действующего законодательства.

К внутренним причинам негативных воздействий на политико-правовую безопасность предприятия следует отнести также непонимание важности или финансово-техническую неспособность предприятия проводить активную внешнюю политику по изменению существующей внешней политико-правовой среды предприятия в лучшую сторону.

Среди основных негативных воздействий внутреннего характера на политико-правовую безопасность предприятия следует, прежде всего, выделить слабую проработку договорных отношений предприятия с контрагентами по бизнесу, с персоналом по трудовым договорам, в также неэффективное юридическое отстаивание интересов предприятия в конфликтных ситуациях и слабое юридическое планирование обеспечения поддержки бизнеса.

Кроме того, важная группа негативных воздействий внутреннего характера включает в себя проблемы, связанные с отсутствием или низким уровнем стратегии деятельности предприятия по улучшению внешней политико-правовой среды своего бизнеса.

В соответствии с Конституцией РФ каждый имеет право на свободное использование своих способностей и имущества для предпринимательской и иной не запрещенной законом экономической деятельности.

В российском гражданском законодательстве предусмотрена определенная система гарантий предпринимательской деятельности. К ним относятся такие как:

- наличие права заниматься разрешенными видами предпринимательской деятельности, создавать предприятия и приобретать необходимое для их деятельности имущество;
- недопустимость отказа в регистрации предприятия по мотивам нецелесообразности;
- юридическое равенство всех субъектов предпринимательской деятельности;
- равное право доступа всех субъектов предпринимательской деятельности на рынок, к материальным, финансовым, трудовым, информационным и природным ресурсам;
- ограничение монополистической хозяйствующих субъектов и их недобросовестной конкуренции;

– правовая защита интересов всех субъектов предпринимательской деятельности – как на внутреннем, так и на внешнем рынке в соответствии с международным правом.

В условиях рыночной экономики у предпринимателей возникает объективная потребность во взаимодействии с другими субъектами хозяйственного оборота: поставщиками, потребителями, партнерами, кредитными организациями, посредниками, страховщиками и т.д. Это взаимодействие осуществляется, как правило, в форме сделок. В сделках могут "закладываться" угрозы предпринимательской деятельности, в связи с чем они требуют тщательной подготовительной работы.

Сделками признаются действия граждан и юридических лиц, направленные на установление, изменение или прекращение прав и обязанностей. Каждый участник сделки принимает на себя определенные обязательства и получает определенные права. Эти права и обязательства предпринимателя закрепляются в договоре. Договор есть соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей. В договоре закрепляются предмет договоренности, взаимные права и обязанности лиц, последствия нарушения договора.

Все многообразие предпринимательских договоров можно распределить на несколько групп:

- обязательства по передаче имущества в собственность (договоры купли-продажи, поставки, товаров, контрактации, энергоснабжения, продажи недвижимости и предприятия, мены);
- обязательства по передаче имущества в пользование (договоры аренды транспортных средств, зданий, сооружений, предприятий, лизинга);
- обязательства по оказанию услуг (договоры перевозки, транспортной экспедиции, займа, кредита, банковского счета, хранения, страхования, поручения, комиссии, агентского договора, доверительного управления);
- обязательства по реализации творческой деятельности (договоры на выполнение научно-исследовательских, опытно-конструкторских и технологических работ).

Для обеспечения безопасности предпринимательской деятельности при заключении договоров необходимо учитывать ряд положений гражданского законодательства и соблюдать определенные правила.

Процесс заключения договора может быть разделен на три этапа: подготовительный этап (подготовка к подписанию), основной (процесс определения условий договора), заключительный (оформление и непосредственное подписание). Каждый этап имеет свою специфику в обеспечении безопасности субъекта предпринимательской деятельности.

А. Подготовительный этап.

Основная задача предпринимателя на данном этапе – определить свое отношение к предполагаемому договору, или – точнее – к потенциальному партнеру.

Здесь следует учитывать, что гражданское законодательство предусматривает свободу договора. Предпринимателя никто не может принудить к заключению договора. Он сам волен выбирать партнера при заключении договора, вид и условия договора.

Для обеспечения собственной безопасности, прежде всего, следует собрать предварительные сведения о предполагаемом партнере (технология получения данной информации подробно описана в девятой главе).

Далее необходим сбор и анализ общей информации о партнере:

финансово-экономической – производится экспресс-анализ бухгалтерского баланса на последнюю отчетную дату. Могут рассчитываться такие финансовые показатели, как рентабельность производства, финансовые коэффициенты – автономии, текущей ликвидности, покрытия и их основные тенденции в течение ряда лет);

организационной (количество работающих, структура фирмы, система управления, степень самостоятельности фирмы, наличие филиалов, территориальный охват деятельности);

рыночной (контролируемая доля рынка, имидж фирмы, возможность конкуренции с ней, постоянные контрагенты);

специфической (наличие "теневого оборота", участие в нелегальных сделках, связи с преступными группировками и т.п.);

сведения об управленческом персонале фирмы (образование, наличие судимости, компетентность, деловая репутация).

После сбора общей информации о фирме необходимо проанализировать полученные сведения и определить степень надежности фирмы как потенциального контрагента. В самом общем виде все потенциальные партнеры по степени надежности могут быть разделены на три группы:

Первая группа – наиболее надежные партнеры. Вся собранная информация по вышеназванным критериям является положительной – это позволяет сделать вывод о том, что данный партнер выполняет свои обязательства и имеет высокую исполнительскую дисциплину по совершаемым сделкам.

Вторая группа – партнеры средней степени надежности. Информация свидетельствует, что в большинстве случаев партнер старается выполнять свои обязательства, хотя имели место единичные нарушения условий сделок.

Третья группа – контрагенты с низкой степенью надежности. Они, как правило, не выполняют взятых на себя обязательств, используют нелегальные методы в своей деятельности, зачастую занимаются запрещенными видами деятельности, либо связаны с организованными преступными группировками.

Отнесение потенциального партнера к одной из групп позволяет в конце данного (предварительного) этапа принять одно из возможных решений:

отказ от подписания договора с данным контрагентом;

подписание протокола о намерениях – это может быть использовано в случае, когда собранной информации оказалось недостаточно и необходима дополнительная проверка для определения надежности потенциального партнера;

согласие на подписание договора.

Б. Основной этап (процесс определения условий договора).

После принятия решения о выборе контрагента стороны приступают к обсуждению условий соглашения, которые составляют содержание договора. Каждый предпринимательский договор должен иметь ряд обязательных элементов. Так, договор купли-продажи, включает:

Преамбулу – в которой указывается наименование договора (например, купли-продажи), место и время его заключения, наименование сторон.

Основную часть – предмет договора (количество товара), цена товара, качество, базисные условия поставки, скидки с цены, форма платежа, срок поставки, односторонний отказ от договора, маркировка, упаковка товара, сдача-приемка товара, ответственность сторон. Сюда же относятся общие условия договора – порядок рассмотрения споров и форс-мажорные обстоятельства.

Заключительную часть – юридические адреса сторон, все приложения, подписи сторон.

Разработку текста договора целесообразнее осуществлять с помощью собственных специалистов предприятия, поскольку в этом случае в проекте полнее можно отразить собственные интересы фирмы, что позволит повысить степень безопасности сделки.

В своей практической деятельности предприниматель должен четко оговаривать в договоре распределение между сторонами обязанностей по транспортировке продаваемого товара и по его страхованию на период транспортировки. Это обусловлено тем, что цена товара прямо зависит от того, кто оплачивает расходы по транспортировке: продавец или покупатель.

Значительные возможности для противодействия угрозам предпринимательской деятельности кроются в выборе формы расчетов между контрагентами, поскольку в настоящее время весьма распространены преступления именно в сфере расчетных отношений. Наиболее надежной считается наличная, однако она не всегда возможна, так как закон ограничивает ее применение. Безналичные же расчеты могут осуществлять с помощью платежных поручений, аккредитивной формы расчетов, платежных требований-поручений, а также с помощью различного рода ценных бумаг, например, векселей, чеков. Необходима тщательная проверка наличия денег на счете контрагента и подлинности ценных бумаг.

После того как все условия договора согласованы необходимо еще раз проверить содержание договора в целом и на предмет отсутствия в договоре пунктов, запрещенных законом, например о разделе рынков, соглашении фирм и т.п., поскольку их наличие может привести к санкциям против фирмы.

В. Заключительный этап (подписание договора).

Договор может заключаться в устной или письменной форме. Следует иметь в виду, что сделки, которые должны совершаться в простой письменной форме – это сделки юридических лиц между собой и с гражданами. Для некоторых же видов сделок требуется нотариальное удостоверение, либо государственная регистрация. Для того чтобы сделка не могла быть признана недействительной, следует соблюдать требуемую законодательством форму.

Предприниматель должен иметь в виду, что он обязан выполнить условия договора. К нему применяются меры гражданско-правовой ответственности, на него ложится вина за неисполнение договорных обязательств, даже если это произошло из-за нарушения обязанностей со стороны его поставщиков, перевозчиков, отсутствия на рынке нужных товаров. Освободиться от ответственности предприниматель может только вследствие непреодолимой силы (стихийные явления, военные действия и т.д.).

В соответствии с российским законодательством (ГК РФ ст. 56) по обязательствам предпринимателя – юридического лица взыскание может быть обращено на любое имущество, принадлежащее ему на праве собственности, либо хозяйственного ведения.

В практике хозяйствования для обеспечения безопасности предприниматель может также использовать предусмотренные гражданским законодательством меры оперативного воздействия на предпринимателя-нарушителя договорных обязательств без обращения в судебные инстанции. Например, в договоре купли-продажи получатель некачественной продукции имеет право отказаться от ее принятия и от платежа за эту продукцию; если же состоялась предоплата, то получатель продукции имеет право возврата суммы платежа или замены этой продукции другой, качественной.

Гражданское законодательство регулирует имущественные отношения, которые основаны на равенстве их участников, а гражданско-правовая ответственность носит так называемый компенсационный характер, т.е. она призвана восстановить имущественные интересы потерпевшей стороны на эквивалентной основе.

Сам предприниматель-потерпевший также может возбудить требование о взыскании санкций с партнера по хозяйственному договору. Если ответчик не удовлетворяет его требований, то спор передается в арбитражный суд путем предъявления иска, в случае если договором не определен другой порядок разрешения разногласий.

В случае нарушения договорных обязательств ответственность за это возможна в двух формах:

взыскание неустойки (штраф, пени), предусмотренной законом либо договором. Неустойка – это определенная договором (или законодательством) сумма, которую должник должен уплатить кредитору в случае неисполнения или ненадлежащего исполнения условий договора;

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.