Кришталюк А.Н.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ БИЗНЕСА

курс лекций

Академия МАБИВ
www.mabiv.ru

Александр Николаевич Кришталюк

Управление безопасностью бизнеса

http://www.litres.ru/pages/biblio_book/?art=8638167
Александр Кришталюк. Управление безопасностью бизнеса: МАБИВ; Орел; 2014

Аннотация

Скорее всего, многие согласятся с тем, что совершенно безразлично, будет ли предприятие разорено бандитами, вымогателями, штрафами налоговой инспекции, либо в результате недобросовестных действий деловых партнеров, конкурентов или собственного персонала, – в любом случае оно может прекратить свое существование. Следовательно – речь надо вести об обеспечении безопасности деятельности организации. Предназначено для преподавателей и студентов вузов специальностей по направлению безопасности, специалистов по безопасности, руководителей и менеджеров компаний.

Содержание

Лекция 1 6
1.1. Что такое безопасность 8
1.2. Когда надо задумываться о безопасности 13
1.3. Законы безопасности 15
1.4. Оцените Ваш бизнес – постарайтесь понять, для кого и какой он может представлять интерес 18
Конец ознакомительного фрагмента. 26

Александр Кришталюк
Управление безопасностью бизнеса
Курс лекций

Рецензент:

кандидат педагогических наук, доцент кафедры «Теория и методика физической культуры и спорта» ФГБОУ ВПО «Орловский государственный университет» Ю. И. Горлова

* * *

А. Н. Кришталюк, руководитель Национального социального проекта «Здоровая Нация», аспирант кафедры «Туризм, рекреация и спорт» ФГБОУ ВПО «Госуниверситет – УНПК»

Лекция 1
Безопасность и бизнес

Скорее всего, многие согласятся с тем, что совершенно безразлично, будет ли предприятие разорено бандитами, вымогателями, штрафами налоговой инспекции, либо в результате недобросовестных действий деловых партнеров, конкурентов или собственного персонала, – в любом случае оно может прекратить свое существование. Следовательно – речь надо вести об обеспечении безопасности деятельности организации.

Обеспечение безопасности необходимо для любых организаций, независимо от форм их собственности, начиная от государственных организаций и заканчивая маленькой палаткой, занимающейся розничной торговлей. Различие будет состоять лишь в том, какие средства и методы и в каком объеме требуются.

Что же следует понимать под безопасностью предприятия, из чего она собственно состоит и какие вопросы требуют Вашего повышенного внимания?

Конечно, о чем бы мы ни говорили – какие меры безопасности ни рассматривали, так или иначе, все направлено на обеспечение экономической стабильности в деятельности предприятия. Однако, достижение этой стабильности невоз-

можно без анализа всех сторон деятельности предприятия.

1.1. Что такое безопасность

Под безопасностью предприятия обычно понимается защита от угрозы нанесения ему ущерба, т. е. безопасность предприятия – это состояние защищенности его жизненно важных интересов от внутренних и внешних угроз (источников опасности). Подобная защищенность достигается применением комплекса мер правового, экономического, организационного, инженерно-технического и социально-психологического характера.

Существующее мнение о том, что безопасность – это, прежде всего, физическая защищенность, не совсем верно.

Безопасность предпринимательской деятельности сегодня – это не только автомат и бронестекло «шестисотого», а, прежде всего, это вычисление и всесторонний анализ угроз деятельности предприятия; прогноз и создание систем и мер защиты и минимизации коммерческих рисков.

При этом угрозами считаются не только такие очевидные факты, как, например, посягательство на личность: грабеж, рэкет или физическое насилие, то есть те, которые носят явно криминальный характер, но и такие неочевидные как: недобросовестность деловых партнеров и некомпетентность персонала, необоснованные претензии налоговых либо правоохранительных органов и т. д.

Для лучшего понимания того, что же такое система без-

опасности предприятия (для чего она создается, какие задачи решает, как строится) и для того чтобы в дальнейшем эффективно построить свою систему безопасности, необходимо четко определить следующие моменты:

– Правовые основы

– Цель построения системы безопасности

– Правила построения (см. Законы безопасности п.п. 1.3.)

– Рассмотрим эти вопросы подробнее.

Правовые основы обеспечения безопасности определяют соответствующие положения Конституции Российской Федерации, Закон "О безопасности" (см. Приложение 7.3.), федеральные законы и другие нормативные акты.

Правовая защита персонала, материальных и экономических интересов предприятия от преступных посягательств обеспечивается на основе норм Уголовного и Уголовно-процессуального кодексов, законов Российской Федерации о прокуратуре, о федеральной службе безопасности, о милиции, об оперативно-розыскной деятельности, о частной детективной и охранной деятельности, об оружии и др.

Защиту имущественных и иных материальных интересов, деловой репутации коммерческих предприятий призваны обеспечить, также, гражданское, гражданско-процессуальное, арбитражное и арбитражно-процессуальное законодательство (более подробная информация в Приложении).

Целью создания системы безопасности предприятия является комплексное воздействие на потенциальные и реаль-

ные угрозы, позволяющее организации:

– успешно функционировать в нестабильных условиях внешней и внутренней среды,

– предотвращать угрозы собственной безопасности,

– защищать свои законные интересы от противоправных посягательств,

– охранять жизнь и здоровья персонала,

– не допускать хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств, обеспечения производственной деятельности, включая и средства информатизации.

Достижение этой цели требует решения следующих задач:

– выявления угроз стабильности работы предприятия и его развитию и выработка мер противодействия;

– обеспечения защиты технологических процессов;

– реализации мер противодействия всем видам шпионажа (промышленного, научно-технического, экономического и т. д.);

– своевременного информирования руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия;

– предупреждения переманивания сотрудников предпри-

ятия, обладающих конфиденциальной информацией;

– всестороннего изучения деловых партнеров;

– своевременного выявления и адекватного реагирования на дезинформационные мероприятия;

– разработки и совершенствования правовых актов предприятия, направленных на обеспечение его безопасности;

– реализации мер по защите коммерческой и иной информации;

– организации мероприятий по противодействию недобросовестной конкуренции;

– обеспечения защиты всех видов ресурсов предприятия;

– реализации мер по защите интеллектуальной собственности;

– организации и проведения мер по предотвращению чрезвычайных ситуаций;

– выявления негативных тенденций среди персонала предприятия, информирования о них руководства предприятия и разработки соответствующих рекомендаций;

– организации взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;

– разработки и реализации мер по предупреждению угроз физической безопасности имуществу предприятия и его персоналу;

– возмещения материального и морального ущерба, нане-

сенного предприятию в результате неправомерных действий организаций и отдельных физических лиц.

– Результатом деятельности по обеспечению комплексной безопасности предприятия являются: стабильность (надежность) его функционирования и финансово-экономического состояния, личная безопасность персонала.

1.2. Когда надо задумываться о безопасности

Безопасность предпринимательской деятельности, а часто это и Ваша личная безопасность – это тот случай, когда лучше предупредить возможные неприятности, чем решать возникающие проблемы. Многие риски в предпринимательской деятельности можно просчитать заранее.

Лучше всего задуматься о безопасности Вашего бизнеса в тот момент, когда Вам пришла идея создать свое предприятие. Потратить некоторое количество сил и средств на начальном этапе и исправить свои возможные просчеты и ошибки на бумаге, когда Ваше представление о том, что такое Ваш бизнес, как он выглядит, как будет развиваться, еще только формируется, – значительно проще и дешевле чем ломать уже выстроенный и работающий механизм.

Кроме того, задумываться о проблемах безопасности надо всякий раз, как Ваш бизнес претерпевает какие-либо изменения. Постарайтесь ответить на вопрос: кто от Ваших действий (хотя бы косвенно) может пострадать?

Например: Вы решили установить систему автоматизации бухгалтерского учета. В результате двое из четырех работников бухгалтерии становятся не нужны. Одну из работниц Вы переводите на новый участок, другую увольняете, и она направляет к Вам налоговую полицию. Даже если проверка

налоговыми органами ничего криминального не выявит, то время и нервы отнимет точно.

Другой вариант: Вы решили внедрить новую технологию, существенно упрощающую и удешевляющую процесс переработки нефти. Можете не сомневаться, что компании занятые в этой отрасли сделают все, чтобы Ваше техническое решение так и осталось нереализованным – для них это потеря дохода (рынок любит стабильность и добровольно начинать ценовые войны, передел зон влияния никто не хочет). Возможно, последний пример кому-то покажется надуманным, но … это случай из практики.

Вы решили распространить через сеть розничной торговли новый вид товара, выгодно отличающийся от того, что сейчас представлено на рынке. И все начинается довольно неплохо – спрос высокий, продажи растут. Но при этом продукция кого-то другого, кто на этом рынке работал до Вас, безнадежно «встала». Скорее всего, этот «кто-то» обязательно поинтересуется, кто Вы такой, насколько Вы сильны и нельзя ли Вас каким-то образом "потеснить"…

1.3. Законы безопасности

Система безопасности предприятия должна быть построена с соблюдением следующих правил:

Профилактика возможных угроз.

Необходимо своевременное выявление возможных угроз безопасности предприятия. Анализ которых позволит разработать соответствующие профилактические меры.

Законность.

Меры по обеспечению безопасности разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

Комплексное использование сил и средств.

Для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен, в рамках своей компетенции, участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа (план работ) обеспечения безопасности предприятия.

Координация и взаимодействие внутри и вне предприятия.

Меры противодействия угрозам осуществляются на основе взаимодействия и координации усилий всех подразде-

лений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия. Организовать координацию и взаимодействие внутри и вне предприятия может служба безопасности (СБ) предприятия (либо руководитель предприятия, если СБ в организации нет).

Сочетание гласности с секретностью.

Доведение информации до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль – предотвращение потенциальных и реальных угроз.

Компетентность.

Сотрудники должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

Экономическая целесообразность.

Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

Плановая основа деятельности.

Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-тех-

ническая, экологическая, технологическая и т. д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

Системность.

Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников, использование всех сил и средств.

1.4. Оцените Ваш бизнес – постарайтесь понять, для кого и какой он может представлять интерес

Необходимо отметить, что среди возможных проблем чаще всего, отмечаются случаи неправомерного использования материальных (финансовых) ресурсов предприятия. Но, кроме того, существует угроза непосредственного подчинения предпринимателя (или его фирмы) сторонним организациям и тем самым получения экономических выгод от его деятельности.

Рейтинг обращений отечественных бизнесменов за помощью в охранные фирмы выглядит следующим образом (по убывающей):

1) Проблема возврата средств (не поступает плата за отгруженный товар, не поступает оплаченный товар, не возвращается в указанный срок кредит);

2) Проблема личной безопасности бизнесменов и членов их семей в связи с угрозами и вымогательством;

3) Хищение грузов на транспорте;

4) Кражи личного имущества в квартирах, офисах, коттеджах, загородных строениях; ограбления; угоны автомобилей;

5) Похищение коммерческой информации (кража доку-

ментов, их копирование, съем информации с компьютеров и факсов, прослушивание и запись телефонных сообщений, разговоров в помещениях, подкуп сотрудников);

6) Кражи и ограбления в магазинах, складских и производственных помещениях;

7) Порча имущества и товаров. Поджоги.

Итак, Вы посмотрели статистику обращений отечественных предприятий в охранные фирмы. Теперь попробуем понять, как определить, для кого и какой интерес будет представлять деятельность Вашей фирмы.

В настоящее время в России, деятельностью любого хозяйствующего субъекта в основном интересуются: государство, конкуренты, криминальные структуры и его собственный персонал.

Государство в основном контролирует правовую основу Вашей деятельности – зарегистрировано ли предприятие, есть ли лицензии, соответствующие вашему виду деятельности и исправно ли вы платите налоги. Кроме того, у правоохранительных органов интерес могут вызвать любые ваши действия нарушающие действующее законодательство. Поэтому, для того чтобы определить степень интереса государства к вам, посмотрите, какие ваши действия могут быть расценены различными контролирующими государственными органами как сомнительные или противоправные. Например, налоговой инспекцией.

У остальных «интересующихся» интерес носит, как пра-

вило, сугубо материальный характер.

Интерес криминальных структур – необходимо отдавать себе отчет в том, что если ваше предприятие в силу специфики своей деятельности попадает в зону повышенного интереса криминальных структур, то избежать общения с ними вам вряд ли удастся. Так что в этом случае лучше заранее оценить свои силы. Круг этих интересов на данной территории, если вы сами их не очень хорошо представляете, вам помогут определить специалисты (например, сотрудники детективных агентств или информационно-аналитических служб)

Кроме того, необходимо помнить, что Вы рискуете привлечь к себе повышенное внимание преступных группировок, применяя методы, нарушающие требования законодательства или деловой этики.

Но, даже если Вы будете вести бизнес по всем правилам, все равно есть риск встретиться с криминальным давлением.

Такое давление может возникнуть не только в случае проявления непосредственного интереса к Вашей деятельности со стороны криминальных структур, но и как форма недобросовестной конкуренции.

Дело в том, что часто недобросовестная конкуренция не только осуществляется незаконными методами, но и при этом, в качестве средств воздействия используются криминальные структуры.

Кроме того, предприятие, а вернее его финансовые средства, представляют большой интерес и для разного рода мо-

шенников, деятельность которых так же можно отнести к криминальной.

Мошенничество в экономической сфере

Основными способами для достижения цели у мошенников являются обман, введение в заблуждение, злоупотребление доверием.

Один из видов мошенничества – использование фальшивых документов (подделка печатей и штампов) реальных или вымышленных фирм. Данный способ основан на индивидуальных способностях мошенника, использующего доверие сотрудников, внушаемость, некомпетентность, халатность.

Встречаются и более изощренные способы мошенничества. Например, фирмы, созданные только для того, чтобы, набрав заказы, получить деньги по предоплате и исчезнуть. Здесь встречаются и довольно хитроумные комбинации.

Одна из фирм, занимающаяся перепродажей товара из-за рубежа, для того чтобы привлечь клиентов снизила отпускные цены на товары ниже закупочных. От клиентов не было отбоя. Договоры поначалу точно выполнялись, имидж компании сомнений не вызывал, число клиентов росло. Создалась обычная пирамида. Естественно, вскоре руководство фирмы исчезло с деньгами, перечисленными по предоплате.

Изощренные мошенники часто проходят процедуру регистрации вполне легально и некоторое время добросовест-

но работают. При этом ни учредители, ни непосредственные руководители могут и не быть замеченными в каких-либо махинациях ранее. Выявить таких можно только с помощью системы достаточно сложных проверок руководителей, учредителей, их связей и анализа деятельности. Это под силу только специализированной фирме.

Но обычно, для выявления возможного мошенничества достаточно получить информацию об организации, ее деятельности (прошлой и настоящей) и учредителях. Поэтому, всегда нужно четко знать, где и какую информацию Вы можете получить.

Выбор способа получения информации зависит от Вас. Но нецелесообразно использовать какой-то один: рациональное решение лежит в области их комбинирования в зависимости от ситуации.

Конкуренты всегда проявляют интерес к вашей деятельности, даже если вы об этом и не догадываетесь. Вопрос лишь в том – что является предметом столь пристального внимания, и какие методы используются для его удовлетворения.

Наиболее вероятно, что интерес вызовут используемые вами новые технологии, методы работы, программы расширения и НИОКР и т. д.

Другое направление проявления повышенного интереса – это информация по настоящим и предполагаемым партнерам, клиентам, перехват выгодных контрактов и инвестици-

онных проектов, поставщиков и каналов сбыта.

Но не стоит забывать и о недобросовестной конкуренции. Основной принцип которой заключается в стремлении любыми, даже незаконными средствами, укрепить свое положение за счет ослабления позиций конкурентов, либо за счет обмана потребителей, или путем сочетания того и другого.

Недобросовестная конкуренция осуществляется в форме:

– экономического шпионажа,

– лживой рекламы,

– компрометации фирмы,

– фальсификации и подделки продукции,

– и, наконец, посредством прямого обмана, нанесения материального ущерба, психологического и физического подавления.

Персонал, как правило, интересует стабильность в деятельности Вашей организации, так как от этого зависит и стабильность заработной платы. Но бывают и исключения – это те, кто о размере своего дохода заботится сам, но… за ваш счет. Основные способы при этом – мошенничество либо воровство.

Внутреннее мошенничество

К таковому относятся любые действия самих сотрудников, либо совершенные при их пособничестве и направленные на использование активов предприятия в личных целях.

Формы его бывают различными: это и хищение, и растрата, и присвоение, и приобретение права на чужое имущество.

В соответствии с американской статистикой, в среднем каждая организация в США теряет от мошенничества более $9 в день на каждого работника и приблизительно 6 % годового дохода от мошенничеств всех своих, нечистых на руку сотрудников.

Однако стоимость мошенничества и злоупотреблений в целом трудно поддается количественному измерению. Причин тому несколько: не все мошенничества и злоупотребления раскрываются; не все раскрытые факты предаются огласке; о некоторых случаях мошенничества собрана неполная информация; гражданское или уголовное преследование часто не возбуждается.

Каким бывает внутреннее мошенничество?

Выделяют три категории внутреннего мошенничества, характеризуемые такими образующими признаками, как незаконное присвоение активов, коррупция и мошеннические утверждения.

Незаконное присвоение активов является основной формой внутреннего мошенничества, составляя более четырех пятых известных нарушений, причем нарушения с наличными средствами и чековыми расчетами организаций равны общей доле потерь всех других активов (инвентарь, поставки, оборудование и информация). Это получение “навара” с продажи “неучтенки”, незаконное списание, неприкрытое

изъятие и т. д.

Коррупция, в смысле внутреннего мошенничества, обычно заключается в том, что должностное лицо, менеджер или служащий организации вступает в сговор с посторонними. Известны несколько основных типов внутренней коррупции, ведущих к ущербу для интересов предприятия: взяточничество, запрещенные денежные вознаграждения, специальное завышение цены по договоренности и пр. На долю коррупции приходится около 10 % всех случаев внутреннего мошенничества.

Кто сколько ворует?

Статистические данные указывают, что приблизительно 58 % известных случаев мошенничества и злоупотреблений совершаются служащими, 30 % – менеджерами и 12 % – топ-менеджерами и собственниками.

Семейные служащие совершают самое большое количество мошенничеств и злоупотреблений и наносят самый высокий средний ущерб – в 72 % случаев. А потери, вызываемые мужчинами, в 4 раза больше потерь, вызываемых женщинами. Средние потери, вызванные виновными с высшим образованием, более чем в пять раз превышают потери, вызванные выпускниками средней школы.

Конец ознакомительного фрагмента.