Ю.Г. ПЛЕСОВСКИХ
Ю.В. РОЖКОВ
Г.П. СТАРИНОВ

ДЕЛИКТ-МЕНЕДЖМЕНТ КАК ФАКТОР ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БИЗНЕСА

Хабаровск
2011

УДК 349:338.2(07)
ББК 67.623я7
П38

Плесовских Ю.Г., Рожков Ю.В., Старинов Г.П.

П38 Деликт-менеджмент в системе экономической безопасности бизнеса: монография / под науч. ред. Ю.В. Рожкова. – Хабаровск: РИЦ ХГАЭП, 2011. – 220 с. – **ISBN 978-7823-0560-4.**

Рецензенты: д-р экон. наук, профессор ТОГУ Третьяков М.М.

д-р экон. наук, профессор ДВИМБ Шишмаков В.Т.

В монографии изложены теоретические и практические основы комплексного правового регулирования экономической безопасности бизнеса на основе оценки современного состояния и прогнозов уровня развития субъектов предпринимательства.

Рассмотрена экономическая система и институциональные преобразования, способствующие повышению уровня экономической и информационной безопасности; проанализированы и предложены рекомендации по организации защиты собственного бизнеса.

В рамках теории деликт-менеджмента исследованы методы управления деликтными рисками с целью их предупреждения, нейтрализации и минимизации.

Для студентов, аспирантов и преподавателей экономических вузов и факультетов, руководителей организаций.

ББК 67.623я7

ISBN ISBN 978-7823-0560-4

СОДЕРЖАНИЕ

К читателю

Бурный процесс интеграции России в мировое рыночное хозяйство и её переход к информационной экономике предполагает самостоятельность субъектов предпринимательства в выборе и определении организационно-правовой формы предприятия, характера деятельности, ассортимента выпускаемой продукции и услуг, рынков снабжения и сбыта, производственной кооперации, системы управления, стратегии развития и т.д.

К сожалению, вышеуказанные процессы сопровождаются повышением уровня экономической преступности, мошенничеством и другими посягательствами на собственность и государства, и частного бизнеса, и физических лиц, что заставляет этих субъектов рынка уделять особое внимание обеспечению экономической безопасности.

Наличие у руководителей организаций, менеджеров, иных специалистов глубоких знаний в области обеспечения эффективной экономической безопасности, способствует оптимальному построению правоотношений в конкретных областях производственной, научной и маркетинговой и другой деятельности.

Разработка новых и адаптация существующих методов, механизмов и инструментов повышения уровня безопасности предпринимательства, что является предметом нашего исследования, позволит готовить специалистов, способных использовать механизмы и инструменты создания эффективной системы экономической безопасности бизнеса.

В такой экономической обстановке особо актуальной стала задача создания благоприятного климата для развития цивилизованного бизнеса, защищённости прав и интересов предпринимателей, так как преимущество, заложенное в стабильности и безопасности, становит-

ся основным конкурентным фактором для любой организации.

В монографии изложены теоретические основы и практические аспекты наиболее эффективного использования корпоративных ресурсов для минимизации угроз и обеспечения стабильного функционирования предприятия, на основе стратегического планирования и прогнозирования его экономической безопасности.

Преимущество, заложенное в экономической стабильности и безопасности, становится основным конкурентным фактором для организации. Только научившись управлять организацией с учётом её безопасности можно рассчитывать на достижение стабильности в обществе и устойчивого развития экономики.

Представляю авторский коллектив:

— Плесовских Юрий Гертурович, канд. юрид. наук, доцент Хабаровской государственной академии экономики и права (п. 1.1, 5.1);

— Рожков Юрий Владимирович, д-р экон. наук, профессор Хабаровской государственной академии экономики и права (р. 2, п. 7.2, п. 9.1 — совместно со Стариновым Г.П.);

— Старинов Геннадий Петрович, канд. экон. наук, доцент Комсомольского-на-Амуре государственного технического университета (р. 1, р. 2, п. 9.1 — совместно с Рожковым Ю.В. р. 3–10, кроме п. 1.1, 5.1).

Авторы признательны специалистам, имеющим богатый опыт работы в правоохранительной системе СССР и РФ, Куриленко Михаилу Николаевичу (г. Хабаровск) и Николенко Николаю Алексеевичу (с. Бельго) за ценные советы и пожелания, которые нами учтены при написании монографии.

С уважением,
научный редактор издания Ю.В. Рожков

1 Основы менеджмента экономической безопасности

1.1 Правовое обеспечение концепции национальной безопасности

Одним из основных нормативно-правовых актов, регулирующим вопросы безопасности, является Концепция национальной безопасности Российской Федерации (утв. Указом Президента РФ от 17 декабря 1997 г. № 1300, в редакции от 10 января 2000 г. № 24).

Концепция национальной безопасности представляет собой систему, направленную на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности. В Концепции отражены наиболее важные направления государственной политики РФ[1].

Под национальной безопасностью Российской Федерации понимается безопасность её многонационального народа как носителя суверенитета и единственного источника власти в России.

Национальные интересы РФ основываются на совокупности сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической, таможенной и других сферах жизни. Они носят долгосрочный характер и определяют основные цели, стратегические и текущие задачи внутренней и внешней политики государства. Национальные интересы обеспечиваются институтами государственной власти, осуществляющими свои функции на основе государственного права.

В концепции национальной безопасности РФ сформулированы основные угрозы безопасности личности, общества и государства по сферам жизнедеятельности, а также поставлены основные задачи в

[1] Корнилов М.Я. Экономическая безопасность России. М.: РАГС, 2007.

области обеспечения национальной безопасности России:

• превентивное прогнозирование и выявление внешних и внутренних угроз национальной безопасности Российской Федерации;

• комплексное проведение оперативных и долгосрочных мер по предупреждению и нейтрализации внутренних и внешних угроз;

• обеспечение суверенитета и территориальной целостности России, безопасности её пограничного пространства;

• подъём экономики страны, проведение независимого и социально ориентированного экономического курса развития общества;

• преодоление научно-технической и технологической зависимости Российской Федерации от внешних источников;

• обеспечение на территории России личной безопасности гражданина, его конституционных прав и свобод;

• совершенствование системы государственной власти РФ, федеративных отношений, местного самоуправления и законодательства России, формирование гармоничных межнациональных отношений, укрепление правопорядка и сохранение социально-политической стабильности общества;

• обеспечение неукоснительного соблюдения законодательства РФ всеми гражданами, должностными лицами, государственными органами, политическими партиями, общественными и религиозными организациями;

• обеспечение равноправного и взаимовыгодного сотрудничества России с ведущими мировыми государствами;

• подъём и поддержание на соответствующем уровне военного потенциала государства;

• правовое укрепление режима по нераспространению оружия массового уничтожения и средств его доставки;

• проведение превентивных мероприятий по выявлению и пресечению разведывательной и подрывной деятельности иностранных государств, направленной против России;

• коренное улучшение экологической ситуации в стране.

Реализация национальных интересов России возможна только на основе устойчивого развития экономики. Поэтому национальные интересы России в данной сфере являются ключевыми.

Экономическая безопасность — это такое состояние экономики, которое обеспечивает достаточный уровень социального, политического и оборонного существования и прогрессивного развития страны, неуязвимость и независимость её экономических интересов по отношению к потенциальным внешним и внутренним угрозам и воздействиям. Это такое состояние экономических, финансовых, юридических и иных связей, а также совокупность материальных и интеллектуальных ресурсов организаций, при которых гарантируются надёжность их функционирования, коммерческий успех, поступательное научно-техническое и социальное развитие.

К экономической безопасности следует относить не только защищённость национальных интересов, что само по себе крайне важно. Надо обращать внимание на готовность и способность всех институтов власти создавать и отстраивать механизмы реализации и защиты национальных интересов развития отечественной экономики, поддержания социально-политической стабильности государства.

1.2 Государственная стратегия в системе национальной экономической безопасности

Национальная экономическая безопасность — это такое состояние экономики и институтов власти, при котором обеспечивается гарантированная защита национальных интересов, гармоничное, соци-

ально направленное развитие государства и общества в целом, формирование достаточного экономического и оборонного потенциала страны.

Мы согласны с той точкой зрения, что национальная экономическая безопасность имеет внутреннюю материально-вещественную основу; достаточно высокий уровень развития производительных сил, способный обеспечить важную долю натуральных и стоимостных элементов расширенного воспроизводства национального продукта; внутреннюю социально-политическую основу экономической безопасности; необходимый уровень общественного согласия в отношении долгосрочных национальных целей, делающий возможными выработку и принятие стратегии социального и экономического развития, претворяемый в жизнь через государственную политику, устойчиво поддерживаемую большинством граждан России[2].

Глобализация, интернационализация производства, денежно-кредитной и иных сфер приводит к тому, что национальная экономическая безопасность всё более тесно интегрируется с международной экономической безопасностью.

Экономическая безопасность, как базис национальной безопасности, обнаруживаясь в сферах влияния других форм национальной безопасности (военной, социальной, политической, экологической, правовой, информационной, правовой и других), проникает в них и взаимодействует с ними, одновременно ощущая на себе их воздействие, то есть — налицо обратная связь.

Государственная стратегия экономической безопасности Российской Федерации является составной частью национальной безопасности страны в целом и ориентирована на реализацию осуществ-

[2] Доценко Д.В., Круглов В.Н. Социально-экономическая сущность понятия «экономическая безопасность» // Аудит и финансовый анализ. 2009. № 4. С. 422.

ляемых экономических преобразований в ближайшие годы.

Государственная стратегия развивает и конкретизирует соответствующие положения разрабатываемой концепции национальной безопасности Российской Федерации с учётом национальных интересов в сфере экономики.

Цель государственной стратегии — обеспечить такой уровень развития экономики, чтобы создать приемлемые условия для жизни и развития личности, социально-экономической и военно-политической стабильности общества и сохранения целостности страны для успешного противостояния влиянию внутренних и внешних угроз. Без достижения этой цели практически невозможно решить ни одну из задач, стоящих перед Россией, как на внутригосударственном, так и в международном плане.

Практическая реализация указанной стратегии должна создать необходимые условия для достижения общих целей национальной безопасности страны. В частности, она должна обеспечить:

• защиту гражданских прав и свобод населения, повышение уровня и качества его жизни, гарантирующих социальную стабильность в государстве и спокойствие в обществе;

• эффективное решение политических и социально-экономических задач с учётом национальных интересов страны;

• усиление влияния на процессы в мировых экономических системах, напрямую затрагивающие национальные интересы России.

Внешнеэкономическая направленность государственной стратегии состоит в эффективной реализации преимуществ международной департаментализации труда, устойчивости развития страны в условиях её равноправной интеграции в мировое экономическое пространство, недопущения критической зависимости России от зарубежных го-

сударств в жизненно важных вопросах экономического сотрудничества. Государственная стратегия включает:

1. Характеристику внешних и внутренних угроз экономической безопасности РФ как совокупности условий и факторов, создающих опасность для жизненно важных экономических интересов индивида, общества и государства, определение и мониторинг факторов, подрывающих устойчивость социально-экономической системы страны на краткосрочную и среднесрочную перспективу.

2. Определение критериев и параметров, характеризующих национальные интересы в области экономики и отвечающих требованиям экономической безопасности Российской Федерации.

3. Формирование эффективной экономической политики, институциональных преобразований и необходимых механизмов, устраняющих или смягчающих воздействие факторов, подрывающих устойчивость национальной экономики.

Практическую реализацию государственной стратегии следует осуществлять через систему конкретных мер, реализуемых на основе качественных индикаторов и количественных показателей: макроэкономических, финансовых, демографических, внешнеэкономических, экологических, технологических и других.

В государственной стратегии экономической безопасности РФ продекларировано, что выявление возможных угроз экономической безопасности и выработка мер по их предотвращению имеют первостепенное значение в системе обеспечения указанной безопасности. Далее в ней перечислены наиболее вероятные угрозы экономической безопасности России, на локализацию которых должна быть направлена деятельность федеральных органов государственной власти. К ним относятся:

1. Разрыв в имущественной дифференциации населения и повышение уровня бедности, что может привести к нарушению социального мира и общественного согласия. Достигнутый относительный баланс социальных интересов может быть нарушен в результате действия следующих факторов:

• расслоение общества на узкий круг богатых и преобладающую массу бедных, неуверенных в своём будущем граждан;

• рост уровня безработицы приводящего к различным социальным конфликтам;

• несвоевременные выплаты зарплат, фиктивное банкротство предприятий.

Отметим и деформацию структуры отечественной экономики, обусловленной:

• усилением топливно-сырьевой зависимости экономики;

• отставанием выявления запасов полезных ископаемых от их добычи;

• низкой конкурентоспособностью продукции большинства отечественных производителей;

• снижением уровня производства в жизненно важных отраслях обрабатывающей промышленности;

• разрушением технологического единства научных исследований и разработок, распадом сложившихся научных и научно-исследовательских коллективов, приведших к подрыву научно-технического потенциала России;

• поглощением иностранными фирмами внутреннего рынка России по многим видам товаров народного потребления;

• ростом внешнего долга России и увеличением расходов бюджета на его погашение.

2. Возрастание неравномерности социально-экономического развития регионов России. Важными факторами данной угрозы являются:

• объективно существующие различия в уровне социально-экономического развития регионов Российской Федерации, наличие депрессивных, кризисных и отсталых в экономическом отношении районов на фоне структурных сдвигов в промышленном производстве, сопровождающихся резким уменьшением доли обрабатывающих отраслей;

• нарушение производственно-технологических связей между юридическими лицами отдельных регионов России;

• увеличение разрыва в уровне производства национального дохода на душу населения между отдельными субъектами РФ.

3. Криминальная конкуренция в обществе, вызванная в основном такими факторами, как:

• рост уровня безработицы, ибо значительная часть деликтов совершается лицами, не имеющими постоянного источника дохода;

• коррупция в органах государственной власти, возможность доступа криминальных структур к управлению определённой частью производства, в том числе и через теневой рынок и их проникновение в различные властные структуры;

• ослабление системы государственного контроля, что привело к расширению деятельности организованной преступности на внутреннем финансовом рынке, в сферах приватизации недвижимого имущества, экспортно-импортных операций и торговли.

Государственная стратегия экономической безопасности Российской Федерации от 29 апреля 1996 г. была ориентирована на реализацию осуществляемых экономических преобразований в ближай-

шие 3–5 лет, однако все вышеперечисленные угрозы остаются в настоящее время полностью злободневными.

1.3 Субъекты и объекты экономической безопасности бизнеса

Основным субъектом, обеспечивающим безопасность в стране, является само государство, реализующее свои функции в этой области через все ветви законодательной, исполнительной и судебной властей. В соответствии с государственной стратегией, деятельность государства по обеспечению экономической безопасности России осуществляется по ряду основных направлений.

1. Обнаружение фактов, когда фактические или прогнозируемые параметры экономического развития страны не совпадают с допустимыми значениями экономической безопасности, с последующей разработкой комплекса государственных мер по выходу России из зоны критической опасности.

2. Организация работы по реализации комплекса мер для преодоления или предотвращения возникновения угроз экономической безопасности Российской Федерации.

3. Комплексная экспертиза принимаемых решений по принимаемым финансово-хозяйственным проблемам с точки зрения экономической безопасности России.

Кроме того, субъектами безопасности являются граждане, общественные организации и объединения, обладающие правами и обязанностями по обеспечению безопасности в соответствии с действующим законодательством.

Объекты безопасности — выделяемая субъектом часть матери-

ального мира в целях управления безопасностью[3]. К основным объектам безопасности государства относятся: а) личность — её права и свободы; б) общество — его материальные духовные ценности; в) государство — его конституционный строй, суверенитет и территориальная целостность. К объектам безопасности также относятся организации, предприятия, объединения, учреждения материальной либо нематериальной сферы экономики.

В соответствии со статьёй 4 Закона РФ «О безопасности», безопасность достигается посредством проведения единой государственной политики в области обеспечения безопасности с применением системы мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам государства, общества и личности.

С целью необходимого уровня защищённости объектов безопасности в Российской Федерации разрабатывается система правовых норм, регулирующих отношения в этой сфере, определяются основные направления деятельности органов государственной власти и управления, формируются или реорганизуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью в этой области.

Деятельность, обеспечивающая безопасность объектов, выстраивается по следующим иерархическим уровням: а) страна; б) регион; в) юридическое лицо; г) личность. Принципиальным является то, что решения, принимаемые на государственном уровне, распространяются на нижестоящие уровни.

Существует множество классификаций показателей экономиче-

[3] Проценко А.Н. Об основных принципах и механизмах управления региональной безопасностью. URL: http://www.dex.ru/riskjournal/2006/2006_3_3/256-292.pdf (дата обращения: 08.10.2011).

ской безопасности в зависимости от уровня объекта экономической безопасности. Мы приводим одну их них:

1. Макроэкономический уровень это — экономика государства в целом.

2. Мезоуровень (региональный или отраслевой). К нему относится экономика субъектов федерации и отраслей.

3. Микроэкономический уровень — экономика рынка или его отдельного сектора, организаций, предприятий, учреждений, кредитных организаций и т.д.

4. Уровень семьи (домохозяйства) и личности — экономическая безопасность каждого индивида, защиту и покровительство гражданам России, которые находятся за её пределами.

2 Экономическая безопасность бизнеса

2.1 Основы экономической безопасности организации

В условиях глобализации мировой экономики особую актуальность приобрела проблема создания благоприятного экономического климата для развития цивилизованного бизнеса, защищённости прав и интересов предпринимателей. Преимущество, заложенное в стабильности безопасного ведения бизнеса, становится весомым конкурентным фактором в деятельности любого хозяйствующего субъекта.

Под безопасностью предпринимательской деятельности обычно понимается состояние защищённости субъекта предпринимательской деятельности, его капитала и иных корпоративных ресурсов на различных стадиях их функционирования от внешних и внутренних угроз, которые могут иметь негативные последствия.

Экономическая безопасность организации — это состояние наиболее эффективного использования её корпоративных ресурсов (капитала, персонала и пр.) для предотвращения угроз и обеспечения стабильного функционирования предприятия в настоящее время. Мы согласны с Л.П. Гончаренко, что «Экономическая безопасность любого предприятия характеризуется совокупностью качественных и количественных показателей, важнейшим среди которых является уровень экономической безопасности»[4].

Справедливо считается, что уровень экономической безопасности организации — это оценка состояния использования корпоративных ресурсов по критериям уровня экономической безопасности организации (предприятия). Для достижения наиболее высокого уровня

[4] Гончаренко Л.П. Процесс обеспечения экономической безопасности предприятия // Справочник экономиста. 2004. № 12. С. 49.

экономической безопасности предприятие должно следить за обеспечением максимальной безопасности основных функциональных компонент своей текущей деятельности.

Функциональные компоненты экономической безопасности предприятия — это совокупность основных направлений его экономической безопасности, существенно отличающихся друг от друга по своему содержанию и формам.

Представим наиболее общую структуру функциональных компонент экономической безопасности организации:

- финансовая;
- интеллектуально-инновационная;
- кадровая;
- производственно-технологическая;
- регулятивно-правовая;
- экологическая;
- информационная;
- силовая и т.д.

Все функциональные компоненты экономической безопасности организации характеризуются собственным содержанием, набором функциональных критериев, а также формами и методами обеспечения безопасности в процессе использования предприятием своих корпоративных ресурсов.

Корпоративные ресурсы — факторы бизнеса, используемые владельцами и топ-менеджерами организаций и предприятий для формирования и развития бизнеса.

Среди них обычно выделяют[5]:

1. Ресурс капитала. Акционерный (или паевой) капитал органи-

[5] Гончаренко Л.П. Процесс обеспечения экономической безопасности предприятия // Справочник экономиста. 2004. № 12. С. 50.

зации в сочетании с заёмными денежными средствами позволяет приобретать и поддерживать все иные элементы корпоративных ресурсов, которые изначально отсутствовали у учредителей данной организации.

2. Ресурс персонала. Менеджеры, штат инженерного персонала, производственных рабочих и служащих, обладающие соответствующими знаниями, опытом и навыками, являются основным проводящим и связывающим звеном, связывающим воедино все факторы конкретного бизнеса, обеспечивающим проведение в жизнь идеологии бизнеса, а также достижения целей бизнеса.

3. Ресурс информации и технологии. Информация обо всех видах и формах бизнеса, является сегодня наиболее ценным и дорогостоящим из всех ресурсов предприятия. Именно информация об изменении политической, экономической и экологической ситуации, изменения рыночных факторов, научно-техническая и технологическая информация, конкретные патенты и ноу-хау, касающиеся каких-либо аспектов данного бизнеса, новации методов организации и управления бизнесом позволяют организации адекватно реагировать на любые изменения внешней среды бизнеса, осуществлять эффективное планирование и свою финансово-хозяйственную деятельность.

4. Ресурс техники, машин и оборудования. На основе наличествующих финансовых, информационно-технологических и кадровых потенциалов организация приобретает необходимое технологическое и другое оборудование.

5. Ресурс прав. В настоящее время наблюдается повышение ценности для бизнеса нематериальных активов, резко растёт роль прав. Этот ресурс состоит из прав на использование патентов, лицензий и квот на использование природных ресурсов, а также экспортных квот,

прав пользования землёй. Использование данного ресурса позволяет бизнесу приобщиться к технологическим инновациям, не проводя собственных дорогостоящих научных исследований, а также получить доступ к нестандартным возможностям развития бизнеса.

6. Силовой ресурс. Бизнес сегодня имеет все возможности для самостоятельной охраны своей предпринимательской среды через организацию частных охранных предприятий, служб экономической безопасности. Появилась широкая и вполне реализуемая возможность проведения политики эффективной защиты собственного бизнеса.

Основной причиной, доказывающей необходимость обеспечения экономической безопасности хозяйствующего субъекта, является стоящая перед каждым предприятием задача достижения стабильности своего функционирования и создания перспектив роста для выполнения миссии и цели данного бизнеса.

Под целями бизнеса обычно понимают систему побудительных мотивов, заставляющих предпринимателей начинать новое дело. К таким побудительным мотивам можно отнести:

• Сохранение и приумножение капитала акционеров/пайщиков организации[6].

• Самореализация через данный бизнес его учредителей и топ-менеджеров организации.

• Удовлетворение социальных и иных потребностей персонала организации и общества в целом.

Каким образом формируется на основе видения учредителями бизнеса философия бизнеса, таким образом и вырабатывается система ценностей и норм поведения, принятых в конкретной организации, а также её место и роль в системе как бизнеса, так общества в целом.

---

[6] В этих случаях обычно говорят о темпах роста прибыли, превышающих темпы инфляции, а также — среднюю ставку депозитного банковского процента.

Доминантная цель экономической безопасности организации — обеспечение её устойчивого и максимально эффективного функционирования сегодня и в будущем. Мы согласны с Л.П. Барышниковой в том, что наиболее эффективное использование корпоративных ресурсов предприятия, необходимое для выполнения целей данного бизнеса, достигается путём предотвращения угроз негативных воздействий на экономическую безопасность предприятия и достижения следующих основных функциональных целей экономической безопасности предприятия[7]:

• обеспечение высокой финансовой эффективности работы предприятия, его финансовой устойчивости и независимости;

• обеспечение технологической независимости предприятия и достижение высокой конкурентоспособности его технологического потенциала;

• высокая эффективность менеджмента предприятия, оптимальность и эффективность его организационной структуры;

• высокий уровень квалификации персонала предприятия и его интеллектуального потенциала, эффективность его корпоративных НИОКР;

• высокий уровень экологичности работы предприятия, минимизация разрушительного влияния результатов производственной деятельности на состояние окружающей среды;

• качественная правовая защищённость всех аспектов деятельности предприятия;

• обеспечение защиты информационной среды предприятия, коммерческой тайны и достижение высокого уровня информационно-

[7] URL: http://www.gortranscom.ru/bookinfo-baryshnikova-lp/baryshnikova-lp-ekonomika-pidpriyemstva-navchalniy-posibnik-razdel-4.html?start=77 (дата обращения: 06.10.2011).

го обеспечения работы всех его служб;

• обеспечение безопасности персонала предприятия, его капитала, имущества и коммерческих интересов.

Выполнение каждой из частных целей экономической безопасности предприятия крайне важно для достижения её основной цели. Отметим, что каждая частная цель экономической безопасности предприятия имеет собственную структуру подцелей, обусловливаемую функциональной целесообразностью и спецификой его деятельности. Именно поэтому детальная разработка, реализация и контроль за выполнением целевой структуры экономической безопасности предприятия, являются важным составным элементом процесса, обеспечивающего его экономическую безопасность.

2.2 Деликтные риски бизнеса, их сущность и содержание

Проблемы гражданско-правовой ответственности, деликтной ответственности, в частности, как важного средства борьбы с криминальными формами конкуренции и устранения их имущественных последствий, сегодня очень важны. Криминальная конкуренция затрагивает интересы практически всех субъектов предпринимательства.

В рамках рыночной экономики существенным образом возрастает экономическая свобода хозяйствующих субъектов, которая предполагает наличие у экономического актора (субъекта, производителя, потребителя) определённой совокупности прав, гарантирующих ему автономное и независимое принятие решений. Однако экономическая свобода является источником неопределённости и риска, ибо свободе одного экономического актора сопутствует одновременно и свобода других субъектов рынка.

Наличие неопределённости и риска является неотъемлемым

компонентом предпринимательства и выступает фактором поступательного движения экономической системы. Неустойчивость экономики обусловливает рост неопределённости экономической системы и, следовательно, уровня риска как показателя, характеризующего неопределённость. Анализ экономического содержания неопределённости и риска продиктован необходимостью учёта этих факторов при принятии решений в условиях рынка на всех уровнях экономического развития общества.

Обобщая различные трактовки риска, его можно определить как категорию, характеризующую поведение экономических субъектов в условиях неопределённости при выборе оптимального решения из числа альтернативных вариантов на основе оценки вероятности достижения желаемого результата и степени отклонения от него (как положительного, так и отрицательного). Неопределённость ситуации предопределяется тем, что она зависит от множества переменных, контрагентов и лиц, поведение которых не всегда можно предсказать с приемлемой точностью. Наряду с вероятностью целесообразно рассчитывать и массу риска, хотя применение этого показателя только начинает обсуждаться в экономической литературе[8].

Дальнейшее рассмотрение сущности риска связано с выполнением функций, которые он выполняет в экономике. В экономической литературе выделяют следующие функции риска**:**

• Инновационная. Эту функцию риск выполняет, стимулируя поиск нетрадиционных (инновационных) решений проблем, стоящих

[8] Рожков Ю.В., Дроздовская Л.П. О массе риска как инструменте банковского риск-менеджмента // Банковское дело. 2010. № 7; Рожков Ю.В., Дроздовская Л.П. Финансовые «пузыри» и масса риска // Финансы и кредит. 2010. № 46; Глущенко Е.Н., Дроздовская Л.П., Рожков Ю.В. Финансовое посредничество коммерческих банков: монография / под научной редакцией проф. Ю.В. Рожкова. Хабаровск: РИЦ ХГАЭП, 2011.

перед хозяйствующим субъектом.

• Регулятивная. Такая функция имеет противоречивый характер и выступает в двух формах: 1) конструктивная (преодоление рутины, консерватизма, косности, догматизма, препятствующих внедрению нововведений); 2) деструктивная (авантюризм, субъективизм, если решение принимается без должного учёта факторов экономической жизни и имеющихся реалий).

• Защитная. Она проявляется, ибо риск — устойчивое состояние экономической системы; ей необходима социальная защита, правовые, политические и экономические гарантии, исключающие в случае неудачи наказание и стимулирующие оправданный риск, приводящий к повышению доходности субъектов предпринимательства.

• Аналитическая. Такая функция связана с тем, что наличие риска предполагает необходимость выбора одного из возможных вариантов решений из ряда альтернативных, поэтому экономический субъект в процессе принятия решения анализирует все варианты, которые могут возникнуть.

Само понятие «неопределённость» характеризует ситуацию, при которой отсутствует (полностью или частично) информация о возможных состояниях стохастической экономической системы и внешней среды в целом.

По причинам неопределённости можно выделить её основные виды:

• «информационный разрыв»; он обусловлен наличием несовершенной и ассиметричной информации;

• «разрыв в компетентности»; он вызван несовершенством используемого инструментария, вычислительной трудностью, ограничениями по методам принятия решений, просчётами анализа, прове-

дённого моделирования и т.п.;

• «случайность»; её источник исходит из неисчерпаемости мироздания, его бесконечной сложности и многообразия;

• «противодействие»; оно проявляется в несовпадении интересов сторон (например, трудовые конфликты и споры, нарушение договорных обязательств и пр.)[9].

Говоря о динамике неопределённости в современной экономике России, следует отметить, что по мере формирования основ рыночной экономики станет снижаться неопределённость, обусловленная «разрывом в компетенции» и противодействием, связанным в первую очередь с процессом невыполнения договорных обязательств. Этот процесс будет сопровождаться усилением «информационного разрыва» прежде всего из-за изменения конъюнктуры рынка, спроса, цен, поведения потребителей и разрушительных финансовых кризисов (1998, 2008). По мере роста открытости экономики и вхождения России в мировое рыночное хозяйство, ожидается рост неопределённости, вызванный глобальной экономической нестабильностью.

Неопределённость является конституирующим признаком, то есть «питательной» средой появления рисковых ситуаций, поэтому возрастание неопределённости может повлечь за собой ещё бóльший риск. Можно говорить о наличии причинно-следственной связи нелинейного типа между неопределённостью и риском, когда следствия могут влиять на породившие их причины, а в качестве причин выступать ещё не наступившие последствия[10].

Фактор риска напрямую связан с ростом количества правонарушений, подрывающих стабильность имущественных правоотношений

---

[9] Малашихина Н.Н. Риск-менеджмент: учебное пособие. Ростов-на-Дону: «Феникс», 2004.

[10] Шутов В.С., Васин С.М. Управление рисками на предприятии: учебное пособие. М.: КНОРУС, 2010.

и правовых гарантий юридических лиц. В связи с этим с целью защиты прав и интересов коммерческих структур, целесообразно в общей системе рисков отдельно выделить и исследовать специфическую категорию рисков, которую мы называем «деликтные риски»[11]. Более того, мы полагаем, что следует выделить из риск-менеджмента и сформировать особую науку, которую мы вынесли в название данной монографии и назвали «деликт-менеджмент».

Сегодня и учёные, и управленческие структуры очень мало внимания уделяют данной категории рисков, хотя это игнорирование может привести к серьёзным проблемам в предпринимательской деятельности любого хозяйствующего субъекта.

Деликт (от лат. *delictum* — проступок, правонарушение) — это совершаемое субъектом неправомерное действие (бездействие), представляющее собой нарушение норм, принципов или договорных обязательств, которое влечёт за собой деликтную ответственность, возникающую в связи с причинением имущественного вреда одним лицом другому.

Под деликтными рисками следует понимать вероятность наступления деликта (правонарушения) на предприятии и организации, что может повлечь за собой негативные последствия для его финансово-хозяйственной деятельности.

Модель взаимосвязи основных факторов, влияющих на условия возникновения деликтного типа экономического поведения в обществе можно изобразить так, как показано на рисунке 1.

Чаще всего субъекты управления, своевременно не учитывающие фактор деликтных рисков, борются не с причинами его возник-

[11] Старинов Г.П. Деликтные риски организаций: идентификация, диагностика и управление: на примере предприятий Хабаровского края. Дисс. … канд. экон. наук: 08.00.05. Хабаровск, 2009.

новения, а с его последствиями, то есть с возможным возмещением нанесённого ущерба. Право на возмещение ущерба является конституционным правом (статья 52 Конституции России). В ГК РФ (подпункт 6 ст. 8) одним из оснований возникновения обязательств также является факт причинения вреда другому лицу.

Рисунок 1 — Условия возникновения деликтных рисков

Специфика рассматриваемых обязательственных отношений и их отличие от других обязательств определяется, прежде всего, основанием их возникновения — им является деликт, то есть противоправное, умышленное (прямое или косвенное) причинение вреда.

Таким образом, деликтным можно назвать обязательство, в силу которого лицо, причинившее вред имуществу субъекта управления,

обязано этот вред возместить с выплатой компенсации сверх возмещения вреда.

Общие условия деликтной ответственности за причинение вреда определены статьёй 1064 Гражданского кодекса Российской Федерации. К ним можно отнести:

• наступление имущественного вреда, выраженного в виде общественной опасности для субъекта управления;

• противоправность поведения причинителя вреда;

• наличие причинной связи между противоправным поведением и наступившими последствиями;

• вина правонарушителя, выраженная в виде прямого или косвенного умысла;

• наказуемость субъекта противоправного деяния.

Данные условия общей деликтной ответственности можно отнести к признакам состава противоправного поведения.

Перечисленные условия признаются общими, ибо для возникновения деликтного обязательства их наличие необходимо во всех случаях, если иное не предусмотрено законодательством.

Для субъекта управления бизнесом важно знать и действительную стоимость деликтного риска, его массу, которому подвергается его деятельность, то есть фактические убытки, затраты на снижение величины этих убытков, либо затраты по возмещению таких убытков и их последствий.

Правильная оценка действительной стоимости, массы деликтного риска создаст возможность объективно представить объём возможных убытков и наметить пути по их предотвращению или уменьшению, а в случае невозможности предотвращения — обеспечить их возмещение.

Эффективность учёта деликтных рисков во многом зависит от быстроты реакции на изменение условий рынка, экономической ситуации, финансового положения субъекта управления.

Деликтные риски можно классифицировать по направлениям:

• риск потери денежных средств организации в результате злоупотребления служебным положением либо полномочиями топ-менеджмента, вопреки законным интересам хозяйствующего субъекта;

• риск, связанный с потерей имущества в результате девиантного поведения персонала предприятия, из-за низкого квалификационного отбора кадров и, как следствие, низкого уровня корпоративной культуры;

• риск потери имущества в результате тайного хищения его третьими лицами, из-за невысокого профессионального и технического уровня службы охраны организации;

• риск потери готовой продукции в результате умышленного неисполнения хозяйственных договоров фиктивными контрагентами, из-за неквалифицированной работы службы экономической безопасности;

• риск, связанный со слабой охраной коммерческой тайны об экономических интересах и сведениях о различных сторонах и сферах производственно-хозяйственной, управленческой, научно-технической, финансовой деятельности фирмы, охрана которых обусловлена интересами конкуренции и возможными угрозами экономической безопасности;

• риск, недостаточной защиты деловой информации, определяемой как «конфиденциальная». В бизнесе это, как правило, «ноу-хау», сведения о перспективах развития фирмы, её клиентах, сроках и сумме кредитования, текущие планы работы, информация о кон-

фликтных ситуациях в коллективе и т.п.;

• риск криминальной конкуренции, направленной на распространение ложно-порочащих сведений, способных причинить убытки другому хозяйствующему субъекту;

• риск, связанный с силовым предпринимательством[12], то есть деятельности по конвертации организованной силы в рыночные блага (деньги, ценные бумаги, недвижимость и пр.).

Есть три основные формы силового предпринимательства:

— охранные отношения (так называемое «крышевание» по инициативе деликтных группировок), в которых под угрозой насильственных действий со стороны делинквентов (от лат. *delinquens*, родительный падеж *delinquentis* — совершающий проступок, нарушитель) коммерсанты были вынуждены отдавать часть своих доходов в обмен на услуги по уменьшению потенциальных угроз, исходящих от других силовых структур;

— силовое партнёрство, предполагающее установление между владельцами средств насилия и хозяйствующими субъектами стабильных и постоянных отношений. За долю в распределении прибыли или регулярные отчисления силовые структуры берут на себя решение вопросов, связанных со снижением хозяйственных рисков, обеспечивая благоприятную бизнес-среду для своего клиента;

— силовое посредничество, заключавшееся в «сотрудничестве» бизнеса с силовыми структурами на нерегулярной основе (возврат кредиторской задолженности, обналичивание денежных средств, разрешение хозяйственных споров и пр.).

Специфической группой деликтных рисков хозяйствующих субъектов являются риски, связанные с неготовностью защиты от

[12] Волков В.В. Силовое предпринимательство в современной России // Экономическая социология. 2002. Т. 3. № 1. С. 20–42.

профессионального вымогательства «гринмейла» (*greenmail*). Высокоинтеллектуальное вымогательство заключается в деятельности, направленной на получение третьими лицами сверхприбыли посредством спекуляций или злоупотреблений своими правами акционеров (участников) по отношению к предприятию.

Другой разновидностью деликтных рисков является риск, связанный с недружественным поглощением предприятия — «рейдерством». Рейдерство, как преступный способ захвата предприятий и бизнеса, появилось в 1920–1930 годах в США. В российской практике у термина «рейдерство» два значения. В первом случае речь идёт о незаконном завладении имуществом предприятия. Во втором, — об активной, но в рамках законов, регулирующих корпоративные отношения в сфере слияний и поглощений (M&A — *mergers and acquisitions*). Это совершенно разные понятия. Но часто они смешиваются либо по невежеству, либо сознательно, чтобы изменить общественное мнение в ту или иную сторону.

Все перечисленные активно-агрессивные действия рейдеров должны проводиться в рамках действующего законодательства РФ.

Отметим и наличие каперских рисков, связанных с насильственным захватом бизнеса, на основании одобрения соответствующих структур, которые по масштабу проявления и влияния можно разделить на макро- (риски экономических систем: война и пр.), мезо- (отраслевые: терроризм и др.), и микро-уровни (риски конкретных хозяйствующих субъектов: пиратство и т.п.)[13].

В системе правовых мер борьбы с подобными явлениями гражданско-правовые меры превентивного характера занимают не послед-

[13] Старинов Г.П., Абраменко Н.Н. Девиантость каперских рисков в системе экономической безопасности. В кн: Формирование модели новой экономики России: теория и практика. Краснодар, 2010.

нее место. Особую роль играют меры по введению деликтной ответственности, а также возможность применения системы «деликт-менеджмент». Именно поэтому обязательства, возникающие вследствие причинения вреда либо возможного причинения вреда, остаются одним из наиболее важных и сложных институтов, регулирующих управленческую деятельность бизнеса.

Деликтные риски могут привести к различным последствиям — от порчи ресурсов, нанесения ущерба, перерасхода средств, снижения доходности, упущенной выгоды, до банкротства хозяйствующего субъекта, с последующим отчуждением его собственности.

При этом законодательные инициативы, ориентированные на снижение девиантного поведения делинквентов на рынке корпоративного контроля, в большинстве случаев содержат лишь правовые меры, призванные повлиять на ситуацию, а экономические инструменты остаются незадействованными. Это связано с тем, что юридические меры оказывают влияние на стратегию и тактику делинквентов, тогда как адекватная экономическая политика способна лишить данную категорию самой мотивации к действиям.

Деликтные риски, формирующие деликтный климат в бизнесе, можно условно разделить на источники возникновения умышленных противоправных действий и последующие результаты воздействия, то есть их последствия (рисунок 2).

Деликтные риски, представляющие составную часть риск-менеджмента в бизнесе, напрямую зависят от состояния деликтного фона внешней и внутренней бизнес-среды. Внешняя деликтная среда бизнеса определяется основными факторами макросреды, а именно политическими, институциональными, социальными, демографическими, экологическими, технологическими и др.

Рисунок 2 — Деликтные риски предпринимательства

Политический фактор обусловлен возможностью имущественных или финансовых потерь, из-за изменения политической системы общества, либо политической нестабильностью и обусловливается способом управления всей экономической системой в условиях возможного изменения условий хозяйственной деятельности, способных привести к повышенным расходам ресурсов и потере прибыли из-за возможной модификации форм собственности, отчуждения имущества и денежных средств по мотивам политического характера.

Отсутствие демократического контроля, рассредоточения ответст-

венности, социальной вовлечённости, приводят к неоправданной осторожности предпринимателей, которая выступает как тормоз социальных преобразований. Игнорирование проблем социальной несправедливости приводит к «обвальным» социальным процессам, усиливающим степень деликтного фона внешней бизнес-среды.

Институциональный фактор обусловливается составом, структурой и взаимосвязями различных институтов, образующих побудительную структуру экономических систем. Согласно теории Д. Норта (Нобелевский лауреат 1993 г.), институциональное развитие экономики происходит под влиянием взаимодействия между институтами и организациями. При этом следует учитывать: крупные институциональные изменения проходят медленно. Это связано с тем, что институты являются результатом длительных исторических перемен, формирующих индивидуальное поведение. Эффективность политико-экономической системы формируется на гибких институциональных структурах, которые должны являться результатом длительного процесса.

Анализ институциональной компоненты предоставляет организации возможность определить для себя допустимые границы взаимоотношений с другими субъектами права и необходимые методы защиты своих интересов, базирующихся на степени правовой защищённости, развития правовой среды, степени уровня общественного контроля за деятельностью правовой системы государства.

Если говорить об экологическом факторе, то он характеризуется природными климатическими условиями, запасами и свойствами природных ресурсов, их размещением и степенью доступности, а также состоянием и безопасностью географической среды и внутренней среды конкретного хозяйствующего актора. Данные условия напрямую связаны с показателями загрязнения окружающей среды, за-

тратами, связанных с охраной окружающей среды, ликвидацией природных катаклизмов (форс-мажорные обстоятельства).

Социально-демографический фактор связан с определением влияния на бизнес таких социальных явлений и процессов, которые оказывают воздействие на формирование потребительских предпочтений, от которых непосредственно зависит направленность и величина потребительского спроса, а в соответствие с этим и возможность хозяйствующего субъекта результативно реализовывать свою продукцию и оказывать услуги.

Экономический фактор определяется эффективностью функционирования хозяйствующих субъектов и их инвестиционной привлекательностью. Роль инвестиций определяется способностью возобновления и увеличения производственного потенциала, что в свою очередь влияет на обеспечение заданных темпов экономического роста.

Инвестиции в производство являются одним из способов выхода из экономических кризисов, обеспечения научно-технического прогресса, повышения качественных показателей хозяйственной деятельности предприятий любого уровня. Эффективное управление инвестициями способно оказывать большое влияние на степень конкурентоспособности и финансовой устойчивости хозяйствующих субъектов, выраженной в получении дополнительного дохода или снижения затратной части инвестиционного проекта. В данном случае деликтный фон зависит от стабильности экономической обстановки и степени уровня инфляции в период мирового экономического кризиса, а также государственной экономической политики по возможному изменению механизма налогообложения, эффективному формированию и распределению государственного бюджета.

Деликтный фон внутренней среды бизнеса базируется на функ-

циональных компонентах, таких как коммерция, производство, финансы и кредит, информационное поле, управление (рисунок 3).

Рисунок 3 — Классификация факторов деликтного фона внутренней среды бизнеса

Деликтный фон внутренней среды бизнеса, оказывающий непосредственное влияние на деликтный климат хозяйствующего субъекта, можно разделить на функциональные факторы и формы проявления.

Функциональная компонента — коммерция — по своему экономическому содержанию определяется маркетинговой политикой, представляющей собой совокупную организацию производственно-сбытовой деятельности объекта управления, направленной на обеспечение оптимальной реализации продукции, для бесперебойного движения дифференцированного товара от производителя к потребителю для систематического получения прибыли.

Развитие маркетинга определялось политикой хозяйствующего субъекта, направленной на смещение приоритетов целей — с производства на рынок (продвижение новых разработок на рынок, органи-

зация сбытовой деятельности на основе рекламной составляющей).

Источники возникновения деликтных правонарушений в области маркетинговой политики могут проявляться в различных формах. Это, к примеру, завышения затрат материально-технического обеспечения, злоупотребления при сбыте готовой продукции.

Производственная функциональная компонента внутренней среды организации основывается на стремлении минимизации себестоимости товара с целью гарантированности потенциала прибыльности выпускаемой продукции.

Производство основывается на департаментализации труда по конкретным функциям, автоматизации производства, оптимизации масштабов организации. Научно-исследовательские, опытно-конструкторские разработки нацеливаются на снижение себестоимости продукции, совершенствования технологии производства и обеспечении надёжности продукции.

Деликтный фон внутренней среды бизнеса на стадии производства определяется возможным хищением основных или оборотных средств объекта управления.

Финансовые компоненты организации, которые определяют деликтный фон, возникают в процессе управления финансами или осуществления финансовых сделок; объектами деликтных рисков здесь выступает иностранная валюта, ценные бумаги, либо денежные средства.

Одним из важнейших видов, определяющих эффективную хозяйственную деятельность, является кредитная составляющая, в которой кредитный риск связан с возможностью невыполнения хозяйствующим субъектом (заёмщиком) своих финансовых обязательств перед инвестором в результате использования для финансирования сво-

ей деятельности внешнего займа. Деликтный кредитный фон возникает в процессе делового общения организации с его кредиторами (бенефициар, гарант, другая кредитная организация), контрагентами (поставщики, посредник), акционерами. Разнообразие видов кредитных операций предопределяет специфические особенности и причины возникновения деликтного кредитного риска. Здесь и неплатежи из-за недобросовестности заёмщика, получившего кредит; платежи по фиктивным сделкам из-за вхождения в договорные отношения с недееспособными или неплатёжеспособными партнёрами. Можно отметить искусственное снижение доходности инвестиционного портфеля, представляющего собой совокупность финансовых инструментов, принадлежащих коммерческой организации, либо группе лиц на праве долевого или общего участия и выступающей как целостный объект управления; возрастание кредиторской или дебиторской задолженностей для дальнейшего противоправного списания денежных средств с расчётного счёта организации.

Информационная компонента деликтного фона организации определяется потенциальной утечкой конфиденциальной информации по вине сотрудников объекта управления либо в результате проведённого конкурентами промышленного шпионажа. К категории «конфиденциальная информация» относятся секреты, связанные с производством, технологией, НИОКР, финансами, инвестициями и другой хозяйственной деятельностью организации, незаконное разглашение которых может нанести ущерб его интересам в виде утраты коммерческой тайны, напрямую связанной с утратой секретов производства.

Внутренние факторы управления производством связаны с:

- организационно-правовой формой организации;

- структурой акционерной собственности (капитала);
- функциями (НИОКР, производство, маркетинг);
- структурой предприятия;
- научно-техническим уровнем производства;
- социальным потенциалом организации;
- корпоративной культурой;
- всеми видами ресурсов (материальные, финансовые и пр.)[14].

Внутренние факторы управления определяются эффективной деятельностью управляющей подсистемы менеджмента. Источником возникновения деликтных правонарушений в области эффективного управления могут являться некомпетентность руководства, злоупотребления и/или хищения, осуществляемые субъектами управляющей и управляемой подсистем менеджмента. Степень деликтного фона напрямую зависят от полномочий субъектов управления и масштабов объекта управления.

2.3 Методы измерения эффективности управления деликтными рисками в системе экономической безопасности

Наряду с общей экономической теорией есть экономические теории различных специализированных направлений, связанных с характером производства продукта труда (экономика сельского хозяйства, экономика лёгкой промышленности и пр.).

Проводятся разработки по экономике классификационных видов противоправной деятельности: (экономика порнобизнеса, экономический анализ отмывания денежных средств, добытых преступным путём, экономика коррупции и т.д.).

Экономическая теория преступлений и наказаний и, в частно-

[14] Круглова Н.Ю. Хозяйственное право. М.: Издательство «РДЛ», 2004.

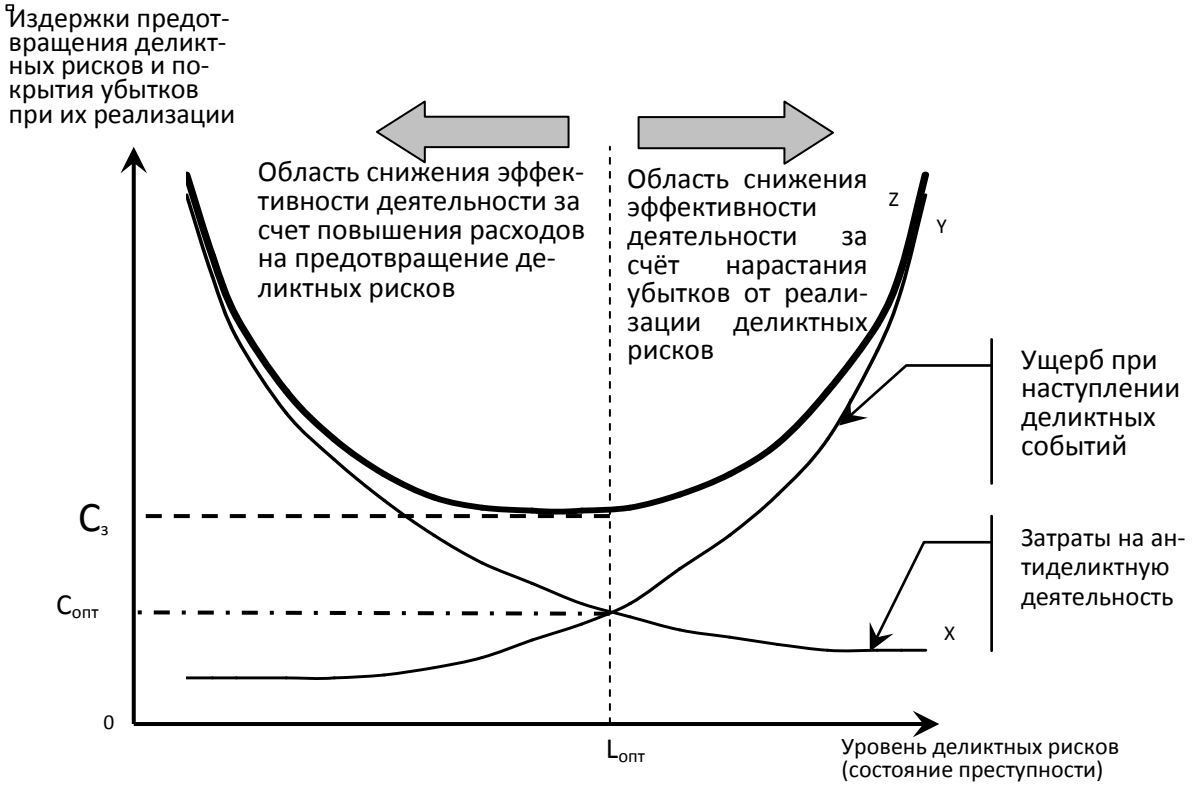
сти, деликт-менеджмент развиты гораздо слабее, чем теория прав собственности и экономика права. Развитие теории осложняется отсутствием достоверной информации о конкретных экономико-криминологических показателях, в связи с чем экономисты вынуждены ограничиваться общими моделями высокой степени вероятности.

Согласно формулировке американского экономиста Джорджа Стиглера (1911–1991), «для предельного сдерживания необходимы предельные затраты». То есть, чем сильнее степень защиты правопорядка, тем большее давление испытывают граждане, вынужденные содержать за счёт своих налогов силы правопорядка. Если все ресурсы общества будут брошены исключительно на правоохранительную деятельность, то большинство виновных будут наказаны.

Конечно, общество может, с другой стороны, вообще избегать необходимых расходов на защиту правопорядка, но в таком анархичном обществе неизбежно, причём катастрофически, возрастут экономические потери от преступности. Крайности в данном случае нежелательны. Факторный анализ оптимизирующего поведения граждан показывает минимизацию совокупных издержек экономической преступности, включающей как потери общества от совершённых преступлений, так и расходы государства на профилактику преступлений.

Экономическое решение проблемы необходимой оптимизации правоохранительной деятельности можно показать на базе экономико-математической модели, разработанной в 1970-е гг. американскими экономистами-криминологами — Лэдом Филлипсом, Гарольдом Вoти-мл. и Крисом Эскриджем. Исходя из преобразованной нами модели, можно выявить следующую тенденцию: чем больше фактическое количество деликтных рисков, тем выше потери общества от них; поэтому кривая **Y** (рисунок 4), показывающая зависимость из-

держек совершённых деликтов от уровня преступности, идёт снизу вверх.



Примечание — $C_{опт}$ – оптимальные затраты на антиделиктную деятельности, руб.; $C_з$ – совокупные издержки по деликтным рискам (убытки от их реализации + затраты на антиделиктную деятельность).

Рисунок 4 — Оптимизация антиделиктной деятельности общества и субъектов хозяйствования

Чтобы уменьшить число деликтов, общество должно тратить всё больше средств на правовую обеспеченность; поэтому кривая **X**, показывающая зависимость издержек предотвращенных деликтных рисков от общего уровня деликтов, идёт сверху вниз. Кривая **Z** показывает совокупные издержки общества от деликтов, она получена суммированием кривых **X** и **Y** и имеет U-образную форму. Очевидно, что с точки зрения общества необходимо, чтобы совокупные потери не превышали минимальной величины $\mathbf{C_{min}}$. Для этого, как видно из

рисунка 4, издержки предотвращенных деликтных рисков, или расходы на борьбу с ними, должны сравняться с издержками совершённых деликтных правонарушений.

Таким образом, общей целью правоохранительной деятельности должно быть не полное искоренение деликтов, а эффективное сдерживание их на оптимальном с точки зрения общества уровне. Сам этот криминальный оптимум достаточно подвижен и зависит как от эффективности использования фискальными органами отпущенных им ресурсов (повышение или понижение этой эффективности сдвинет кривую **X** вниз или вверх), так и от «эффективности» деятельности субъектов деликтных рисков (повышение или понижение наносимого каждым преступлением среднего ущерба сдвинет вверх или вниз кривую **Y**).

Эта модель носит общий характер и в большей степени её можно практически применить к деликтным правонарушениям, наносящим имущественные потери.

Совершенствование управления экономической безопасностью в определённой мере зависит от обоснованных методов измерения и оценки эффективности управления.

Измерение эффективности управления экономической безопасностью позволяет анализировать и сопоставлять различные варианты систем управления безопасностью, выявлять резервы их совершенствования, оказывать влияние на заинтересованность и повышать ответственность сотрудников безопасности за количественные и качественные показатели их труда.

В связи с тем, что управление экономической безопасностью требует финансовых затрат, которые составляют необходимую и относительно обособленную часть издержек производства, к нему в

полной мере должны предъявляться требования эффективного использования ресурсов и повышения результативности деятельности.

Управление экономической безопасностью является неотъемлемой частью производственно-хозяйственной деятельности организации и конечные её результаты выражаются в интегральных показателях работы хозяйствующего субъекта.

В настоящее время нет единообразия в подходах к проблеме измерения экономической эффективности управления экономической безопасностью. Можно предложить два основных направления, наметившихся в теории и практике. Первое заключается в том, что в качестве критерия эффективности управления экономической безопасностью принимают величину:

$$Э_у = \frac{Р_п}{З_у}$$

где Эу – эффективность управления экономической безопасностью;

Рп – конечный результат, полученный производственной системой в целом;

Зу – затраты на управление экономической безопасностью.

В работах второго направления эффективность управления экономической безопасностью Эу предлагается измерять, сопоставляя непосредственные результаты деятельности аппарата управления экономической безопасности Ру с затратами на управление экономической безопасностью Зу:

$$Э_у = \frac{Р_у}{З_у}$$

Выделяют типовые варианты, связанные с проведение комплекса мер по обеспечению эффективной экономической безопасности организации. К числу таких вариантов можно отнести мероприятия:

• снижающие затраты на управление экономической безопасностью при неизменном объёме работ и качестве их выполнения;

• обеспечивающие увеличение объёма работ и повышение качества их выполнения при стабильных затратах на управление экономической безопасностью;

• обеспечивающие повышение качества выполнения работ при увеличении их объёма и одновременном увеличении затрат на управление экономической безопасностью;

• направленные на повышение социальной эффективности, требующие затрат на управление экономической безопасностью.

На первом этапе должны быть зафиксированы формы проявления эффективности и исходные данные, необходимые для предварительной и последующей её анализа и оценки.

Второй этап осуществляется по окончанию разработки проекта мероприятий по совершенствованию управления экономической безопасностью. Здесь производится предварительная оценка эффективности на основе данных, полученных на первом этапе, и ожидаемые их изменения после реализации комплекса превентивных мероприятий.

Третий этап заключается в том, что после проведения комплекса мероприятий оценивают реальную эффективность, проводят анализ и определяют способы и пути дальнейшего её повышения. На этом же этапе, в силу специфики реализации мероприятий по совершенствованию управления экономической безопасностью, устанавливают необходимость и целесообразность проведения повторных оценок реальной эффективности, сроки и методы их проведения.

3 Приоритеты в системе обеспечения экономической безопасности бизнеса

3.1 Разработка внутрифирменной системы обеспечения безопасности бизнеса

Среди отечественных и зарубежных учёных хорошо известны теория общественного выбора и теория прав собственности, которые изучают влияние норм права на эффективное развитие легального бизнеса. В отличие от них экономическая теория преступлений (деликторатов) исследует и идентифицирует экономическое «подполье», связанное как с официально зафиксированной противоправной деятельностью, так и с её латентной составляющей.

Экономический подход к анализу, типизации и классификации экономических основ девиантного поведения в России практически совершенно не изучен. Хотя актуальность научного исследования данного направления для российского государства гораздо выше, чем для развитых стран западных экономических систем, где родилась эта теория.

Слово «правонарушение» на российском рынке прочно ассоциируется с масштабными захватами корпоративной собственности, «перетряхиванием» рынка корпоративного контроля, нарушением огромного количества законодательных актов с целью обеспечения свободы распоряжения привлекательными активами бизнеса. Такая ситуация во многом объясняется нашим «национальным своеобразием».

Деликтное (противоправное) поведение в России фиксируется в основном на уровне нормативно-правовой базы, которая ориентируется на фиксацию диспозиции девиантного поведения и последующее применение санкций.

Деликтность девиантного поведения идентифицируются следующими статьями Уголовного кодекса Российской Федерации:

1) Нарушение изобретательских и патентных прав — незаконное использование изобретений, полезной модели или промышленного образца, присвоение авторства или принуждение к соавторству (ст. 147 УК РФ).

2) Кража — тайное хищение чужого имущества, где под хищением понимается совершённые с корыстной целью противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества (ст. 158 УК РФ).

3) Мошенничество — хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием (ст. 159 УК РФ).

4) Присвоение или растрата — хищение чужого имущества, вверенного виновному (ст. 160 УК РФ).

5) Грабёж — открытое хищение чужого имущества (ст. 161 УК РФ).

6) Разбой — нападение в целях хищения чужого имущества, совершённое с применением насилия, опасного для жизни или здоровья, либо с угрозой применения такого насилия (ст. 162 УК РФ).

7) Вымогательство — требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких (ст. 163 УК РФ).

8) Причинение имущественного ущерба путём обмана или злоупотребления доверием — причинение имущественного ущерба собственнику или иному владельцу имущества путём обмана или злоупотребления доверием при отсутствии признаков хищения (ст. 165 УК РФ).

9) Умышленное уничтожение или повреждение имущества, если эти деяния повлекли причинение значительного ущерба потерпевшему (ст. 167 УК РФ).

10) Уничтожение или повреждение имущества по неосторожности — уничтожение или повреждение чужого имущества в крупном размере, совершённые путём неосторожного обращения с огнём или иными источниками повышенной опасности (ст. 168 УК РФ).

11) Воспрепятствование законной предпринимательской или иной деятельности — неправомерный отказ в государственной регистрации, неправомерный отказ в выдаче специального разрешения (лицензии) на осуществление определённой деятельности, незаконное вмешательство в деятельность предпринимателя или юридического лица, если эти деяния совершены должностным лицом с использованием служебного положения (ст. 168 УК РФ).

12) Регистрация незаконных сделок с землёй, а равно умышленное занижение размеров платежей за землю, если эти деяния совершены из корыстной заинтересованности должностным лицом с использованием служебного положения (ст. 170 УК РФ).

13) Лжепредпринимательство — создание коммерческой организации без намерения осуществлять предпринимательскую деятельность, имеющее целью имущественную выгоду или прикрытие запрещённой деятельности (ст. 173 УК РФ).

14) Легализация (отмывание) денежных средств или иного

имущества приобретённого преступным путём (ст. 174 УК РФ).

15) Незаконное получение кредита предпринимателем путём предоставления кредитору заведомо ложных сведений о финансовом состоянии организации (ст. 176 УК РФ).

16) Принуждение к совершению сделки или отказу от её совершения — принуждение к совершению сделки или отказу от её совершения под угрозой применения насилия, уничтожения или повреждения чужого имущества, а равно распространения сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего или его близких, при отсутствии признаков вымогательства (ст. 179 УК РФ).

17) Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну путём похищения документов, подкупа или угроз (ст. 183 УК РФ).

18) Преднамеренное банкротство — умышленное создание или увеличение неплатёжеспособности организации (ст. 196 УК РФ).

19) Фиктивное банкротство — заведомо ложное объявление о своей несостоятельности (ст. 197 УК РФ).

20) Злоупотребление полномочиями — использование лицом, выполняющим управленческие функции в коммерческой или иной организации, своих полномочий вопреки законным интересам этой организации и в целях извлечения выгод и преимуществ для себя либо нанесения вреда другим лицам, если это деяние повлекло причинение существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства (ст. 201 УК РФ).

21) Коммерческий подкуп, то есть незаконная передача лицу, выполняющему управленческие функции в коммерческой или иной

организации, денег, ценных бумаг, иного имущества, а равно незаконное оказание ему услуг имущественного характера за совершение действий (бездействия) в интересах дающего в связи с занимаемым этим лицом служебным положением (ст. 204 УК РФ).

22) Злоупотребление должностными полномочиями — использование должностным лицом своих служебных полномочий вопреки интересам службы, если это деяние совершено из корыстной или иной личной заинтересованности и повлекло существенное нарушение прав и законных интересов граждан или организаций, либо охраняемых законом интересов общества или государства (ст. 285 УК РФ).

23) Превышение должностных полномочий — совершение должностным лицом действий, явно выходящих за пределы его полномочий и повлекших существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства (ст. 286 УК РФ).

24) Присвоение полномочий должностного лица — присвоение государственным служащим или служащим органа местного самоуправления, не являющимся должностным лицом, полномочий должностного лица и совершение им в связи действий которые повлекли существенное нарушение прав и законных интересов граждан или организаций (ст. 288 УК РФ).

25) Получение взятки — получение должностным лицом лично или через посредника взятки в виде денег, ценных бумаг, иного имущества или выгод имущественного характера за действия (бездействие) в пользу взяткодателя или представляемых им лиц, если такие действия (бездействие) входят в служебные полномочия должностного лица, либо оно в силу должностного положения может способствовать такими действиями (бездействию), а равно за общее покрови-

тельство или попустительство по службе (ст. 290 УК РФ).

26) Дача взятки должностному лицу лично или через посредника (ст. 291 УК РФ).

27) Служебный подлог — внесение должностным лицом, а также государственным служащим или служащим органа местного самоуправления, не являющимся должностным лицом, в официальные документы заведомо ложных сведений, а равно внесение в указанные документы исправлений, искажающих их действительное содержание, если эти деяния совершены из корыстной или иной личной заинтересованности (ст. 292 УК РФ).

28) Халатность — неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло причинение крупного ущерба (ст. 293 УК РФ).

29) Самоуправство, то есть самовольное, вопреки установленному законом или иным нормативным правовым актом порядку совершение каких-либо действий, правомерность которых оспаривается организацией или гражданином, если такими действиями причинён существенный вред (ст. 330 УК РФ).

30) Похищение человека из корыстных побуждений (ст. 126 УК РФ).

31) Незаконное лишение свободы — незаконное лишение человека свободы, не связанное с его похищением из корыстных побуждений (ст. 127 УК РФ).

32) Заказное убийство — умышленное причинение смерти другому лицу из корыстных побуждений или по найму, а равно сопряжённое с разбоем, вымогательством или бандитизмом (ст.105 УК РФ).

В Кодекс об административных правонарушениях — хищение

имущества путём кражи, мошенничества, присвоения или растраты, при отсутствии признаков преступления (ст. 7.27).

Указанные классификационные признаки деликтных действий можно определить как фактор криминальной конкуренции. Она представляет собой деятельность социальных организаций и физических лиц, направленную на получение односторонних преимуществ в экономических сферах жизнедеятельности индивида, общества и государства с использованием запрещённых нормами права методов и средств.

Быстрое и масштабное распространение криминальной конкуренции является серьёзным дестабилизирующим фактором, препятствующим устойчивому развитию страны и создающим угрозу экономической безопасности страны.

Типологию криминальной конкуренции можно рассмотреть по способам захвата бизнеса (таблица 1)[15].

Таблица 1 — Типология криминальной конкуренции

Типология деликтных действий		Квалификационные признаки состава преступления, предусмотренные УК РФ
1	2	3
1. Противоправные действия с целью захвата активов иного предприятия, с использованием поддельных документов	1.1. Подделка документов, предоставляемых для гос. регистрации изменений, вносимых в учредительные документы компании-цели. Как правило, включает подделку печати и подписи нотариуса на заявлении о государственной регистрации изменений в учредительных документах юридического лица, либо коррупционную договоренность с нотариусом, либо хорошо	Статья 159 «Мошенничество» Статья170«Регистрация незаконных сделок с землёй» Статья 174, 174.1 (легализация (отмывание) денежных средств или иного имущества, приобретённых преступным путём) Часть 1 ст. 327 «Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков» Часть 3 ст. 327 «Использование заведомо подложного документа» Статья 202 «Злоупотребление полномочиями частными нотариусами»

[15] Астахов П.А. Противодействие рейдерским захватам. М.: Эксмо, 2008.

Продолжение таблицы 1

1	2	3
	подготовленный обман нотариуса	Статья 285 «Злоупотребление должностными полномочиями» Статья 286 «Превышение должностных полномочий» Статья 292 «Служебный подлог» Статьи 290, 291 (дача и получение взятки) и ст. 204 «Коммерческий подкуп»
	1.2. Подделка выписок из реестра акционерного общества для использования на собрании акционеров	Часть 1 ст. 327 «Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков» Часть 3 ст. 327 «Использование заведомо подложного документа» Статьи 174, 174.1 (легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем) Статья 202 «Злоупотребление полномочиями частными нотариусами» Статья 201 «Злоупотребление полномочиями» Статья 204 «Коммерческий подкуп» Статья 159 «Мошенничество Статья 169 «Воспрепятствование законной предпринимательской или иной деятельности» Статья 170 «Регистрация незаконных сделок с землей»
	1.3. Подделка решений (определение) судов общей юрисдикции и арбитражных судов	Статьи 174, 174.1 (легализация (отмывание) денежных средств или иного имущества, приобретённых преступным путем) Статья 202 «Злоупотребление полномочиями частными нотариусами» Статья 285 «Злоупотребление должностными полномочиями» Статья 286 «Превышение должностных полномочий» Статья 292 «Служебный подлог» Статьи 290,291 (дача и получение взятки) и статья 204 «Коммерческий подкуп» Часть 1 ст. 327 «Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков» Часть 3 ст. 327 «Использование заведомо подложного документа» Статья 159 «Мошенничество

Продолжение таблицы 1

1	2	3
2. Захват компании-цели с использованием неправосудных решений (определений) судов общей юрисдикции и арбитражных судов	2.1. Получение судебного решения/определения, вынесенного на основании принятия судом фальсифицированных документов в качестве действительных	Статья 169 «Воспрепятствование законной предпринимательской или иной деятельности» Статьи 174, 174.1 (легализация (отмывание) денежных средств или иного имущества, приобретённых преступным путем) Статья 202 «Злоупотребление полномочиями частными нотариусами» Статья 285 «Злоупотребление должностными полномочиями» Статья 286 «Превышение должностных полномочий» Статьи 290,291 (дача и получение взятки) Статья 292 «Служебный подлог» Часть 1 ст. 303 «Фальсификация доказательств по гражданскому делу» Статья 305 «Вынесение заведомо неправосудного решения или иного судебного акта»
	2.2. Получение судебного решения/определения, вынесенного на основании принятия судом фальсифицированных документов в качестве действительных, либо получение судебного решения/определения, вынесенного на основании законных (не поддельных) документов, но с заведомо неверным применением судом норм права или иными нарушениями, + нарушение правил подсудности	Статья 159 «Мошенничество Статья 169 «Воспрепятствование законной предпринимательской или иной деятельности» Статьи 174, 174.1 (легализация (отмывание) денежных средств или иного имущества, приобретённых преступным путем) Статья 285 «Злоупотребление должностными полномочиями» Статья 286 «Превышение должностных полномочий» Статьи 290,291 «Дача и получение взятки» Статья 305 «Вынесение заведомо неправосудного решения или иного судебного акта»
3. Злоупотребления в уголовно-правовой сфере	3.1. Возбуждение уголовного дела без достаточных оснований для уголовного преследования	Статья 169 «Воспрепятствование законной предпринимательской или иной деятельности» Статья 186 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» Статья 285 «Злоупотребление должностными полномочиями» Статья 286 «Превышение должностных полномочий» Статьи 290,291 «Дача и получение

Продолжение таблицы 1

1	2	3
		взятки» Статья 292 «Служебный подлог» Статья 299 «Привлечение заведомо невиновного к уголовной ответственности» Статья 301 «Незаконные задержание, заключение под стражу или содержание под стражей» Статья «Принуждение к даче показаний» Ч. 2 и 3 ст. 303 «Фальсификация доказательств по уголовному делу» Статья 306 «Заведомо ложный донос» Ч. 1 ст. 325 «Уничтожение, повреждение или сокрытие официальных документов, штампов или печатей»
	3.2 Отказ в возбуждении уголовного дела, несмотря на достаточные основания для уголовного преследования	Статья 285 «Злоупотребление должностными полномочиями» Статья 286 «Превышение должностных полномочий» Статьи 290, 291 (дача и получение взятки) Статья 292 «Служебный подлог» Части 2 и 3 ст. 303 «Фальсификация доказательств по уголовному делу»
4. Сбор информации о компании-цели		Статья 137 «Нарушение прикосновенности частной жизни» Статья 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» Статья 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» Статья 204 «Коммерческий подкуп»
5. Оказание психологического воздействия на руководство и акционеров компании-цели, не желающих продавать свои акции		Статья 119 «Угроза убийством или причинением тяжкого вреда здоровью» Статья 163 «Вымогательство» Статья 179 «Принуждение к совершению сделки или к отказу от её совершения» Статья 203 «Превышение полномочий служащими частных охранных или детективных служб»
6. Создание препятствий для участия акционеров в общем собрании		Статья 127 «Похищение человека» Статья 127 «Незаконное лишение свободы»

Продолжение таблицы 1

1	2	3
7. Захват с применением силовых действий		Статья 203 «Превышение полномочий служащими частных охранных или детективных служб» Статья 212 «Массовые беспорядки» Статья 330 «Самоуправство» Часть 4 ст. 162 «Разбой, совершенный организационной группой»
8. Гринмейл – корпоративный шантаж		Статья 163 «Вымогательство» Статья 179 «Принуждение к совершению сделки или к отказу от её совершения» Статья 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» Статья 201 «Злоупотребление полномочиями» Статья 330 «Самоуправство»

Такая постановка вопроса сводит участие правоохранительных органов по защите бизнеса исключительно к принятию мер по уже состоявшимся фактам нарушения закона, имеющих признаки состава преступления. Но нарушениями закона вовсе не исчерпывается перечень причин, по которым страдает экономическая безопасность бизнеса.

Образуется пробел между компетенцией государственных правоохранительных органов и потребностями организаций по обеспечению своей безопасности.

Поэтому собственную безопасность конкретных предпринимательских структур обеспечивают обычно сами предприниматели. Основной целью внутрифирменного управления обеспечением экономической безопасности является получение предпринимательской прибыли, на основе создания условий защищённости организации от деликтных посягательств.

Анализ практики показывает, что безопасность бизнеса обеспе-

чивается, зачастую, непрофессионально. К числу типичных недостатков организации процесса, имеющего отношение к данному направлению, можно отнести:

• отсутствие научно обоснованной концепции создания и развития системы обеспечения экономической безопасности;

• игнорирование мер превентивного характера, с рассмотрением только повседневной деятельности, наносящей ущерб бизнесу;

• фрагментарность мер по обеспечению экономической безопасности, произвольность и необдуманность в выборе объектов обеспечения безопасности; игнорирование и ограниченное использование возможностей инфраструктуры рыночной экономики;

• инертность в решении задач обеспечения экономической безопасности;

• отсутствие среди топ-менеджмента организации персоны, осуществляющей непосредственное руководство службой безопасности, ограниченность финансирования таких служб;

• малые полномочия службы безопасности по отношению к другим функциональным управлениям и отделам организации, ограниченность информации, поступающей от них;

• неполное применение возможностей средств обеспечения безопасности;

• слабая подготовленность персонала к применению форм безопасного бизнеса, действиям в экстремально-деликтных ситуациях;

• недостаточная информированность сотрудников о характере и состоянии защищённости предприятия;

• ограниченное использование экономических рычагов и стимулов в отношении лиц, отвечающих за экономическую безопасность;

• нарушение требований законодательства, корпоративной, деловой служебной этики;

• использование персонала службы безопасности для организации силового давления на конкурентов или промышленного шпионажа;

• пренебрежение элементарными мерами безопасности при заключении и осуществлении хозяйственных и финансовых сделок.

Для конкретного предприятия необходима индивидуальная система безопасности, разработанная с учётом сферы его деятельности, этапа существования, содержания функций предпринимательства. В связи с этим возникает целесообразность образования собственных служб экономической безопасности.

3.2 Служба безопасности как основа антиделиктной политики

Служба безопасности на предприятии — это функциональное подразделение, специально созданное для обеспечения безопасности его законных прав и интересов от деликтной конкуренции со стороны социальных организаций и физических лиц и функционирующее в соответствии с Законом РФ от 21.03.2002 г. «О детективной и охранной деятельности», а также на основании Федерального Закона РФ «Об оперативно-розыскной деятельности» от 20.05.2005 г.

К числу основных направлений деятельности частных охранно-сыскных служб относятся:

• сбор информации гражданского и уголовно-правового характера по вопросам защиты бизнеса от противоправных посягательств;

• организация розыска;

• консультирование граждан по проблемам возврата утраченного имущества;

• охрана физических лиц и их имущества;

• охрана помещений и имущества юридических лиц;

• обеспечение безопасности перевозки денежных средств и ценных грузов;

• обеспечение безопасности массовых мероприятий и деловых встреч.

Федеральный Закон «О детективной и охранной деятельности», а также применение некоторых из оперативно-розыскных гласных действий позволяет производить:

• устный опрос граждан и должностных лиц (с их согласия);

• наведение справок;

• исследование предметов и документов (с письменного согласия их владельцев);

• внешний осмотр строений, помещений и других объектов;

• наблюдение.

Опрос выступает в виде специальной беседы с гражданами, которым могут быть известны сведения, необходимые для решения конкретной задачи по охране бизнеса. Результативность такой беседы с конкретным лицом зависит от подготовки к ней, степени осведомлённости о личности опрашиваемого, его психологических качествах, отношении к противоправным деяниям, степени лояльности.

Наведение справок — это способ сбора информации, необходимой для решения задач по обеспечению безопасности бизнеса, путём непосредственного изучения документов, а также направления запросов в различные организации и учреждения. Такое мероприятие предполагает сбор сведений о биографии проверяемого, родственных свя-

зей, роде занятий, имущественном положении, судимости и других данных, позволяющих установить признаки противоправной деятельности.

Исследование предметов и документов представляет собой непроцессуальное исследование тех объектов, которые сохранили следы противоправной деятельности или были орудием совершения деликта. При исследовании предметов, веществ, документов может быть получена информация об их назначении, времени, месте изготовления, качественных характеристиках, о содержании документов и иных свойствах и характеристиках исследуемых предметов.

Обследование помещений, зданий, сооружений, транспортных средств — это осмотр объектов, производимый для получения информации, необходимой для решения задач по противодействию криминальной конкуренции, деликтных проявлений.

Наблюдением считается негласное физическое слежение в общественных местах за лицами, причастными к совершению криминального события.

Службы безопасности являются неотъемлемой частью хозяйственной и иной предпринимательской деятельности в странах с развитой рыночной экономикой. В Западной Европе финансовые ресурсы на мероприятия, связанные с обеспечением безопасности, составляют от 15 до 20 процентов стоимости охраняемых ценностей. В России эти цифры в большинстве случаев не превышают одного процента. Отказ хозяйствующего актора от применения необходимых мер обеспечения безопасности, экономия на защитных мероприятиях, содействует экономической преступности, объектом которой всё чаще становятся сами предприятия и организации.

Службы безопасности решают главным образом задачи превен-

тивного характера, предупреждения девиантного поведения, затрагивающих интересы конкретных предприятий.

К основным принципам деятельности службы безопасности относят:

• соблюдение законности, уважение прав и свобод человека и гражданина, личной, семейной тайны;

• приоритет превентивных контрмероприятий;

• взаимодействие с государственными правоохранительными органами и службами безопасности заинтересованных сторон;

• системный подход, предполагающий учёт всех факторов, оказывающих влияние на уровень безопасности организации, полный охват защитными мерами всех объектов в соответствии с их значимостью, применение не только режимных и административных методов, но и использование экономических рычагов и стимулов;

• употребление легкодоступных средств и систем безопасности;

• активность, опережающий, по сравнению с имеющими место посягательствами, поиск новых форм, методов и возможностей обеспечения безопасности бизнеса;

• сочетание гласных и негласных форм деятельности, ибо применение предприятиями-конкурентами, службами промышленного шпионажа, организованной преступностью негласных форм деятельности обусловливает необходимость использования аналогичных форм противодействия;

• рациональное использование ресурсов на основе текущего и перспективного планирования деятельности.

Целью создания служб безопасности является обеспечение для организации условий защищённости от деликтной конкуренции, направленной на получение односторонних бизнес-преимуществ и ос-

нованной на нарушениях действующего законодательства, деловой этики, наносящей экономический или иной ущерб цивилизованному бизнесу.

Основными задачами службы безопасности на предприятии являются:

• своевременное распознавание угроз безопасности предприятия;

• предотвращение потенциального ущерба от криминальной конкуренции;

• минимизация последствий от состоявшихся фактов криминальной конкуренции.

К важнейшим направлениям деятельности службы безопасности относятся:

• обеспечение физической безопасности руководителей и персонала предприятия;

• обеспечение безопасности сотрудников от проникновения в коллектив лиц с криминальным прошлым, которые могут разрушить благоприятный психологический климат;

• недопущение несанкционированного доступа к информации, представляющей собой коммерческую тайну;

• обеспечение сохранности материальных ценностей и финансовых ресурсов организации;

• предотвращение нанесению потенциального ущерба имиджу организации; создание условий, максимально способствующих сохранению собственниками и руководством предприятия контроля над бизнесом;

• противодействие возможным попыткам со стороны конкурентов заполучить явные и тайные рычаги управления бизнесом.

Если говорить о функциях, то подразделения службы безопасности выполняют охранные, информационно-аналитические, организаторские, воспитательные, директивные и контрольные функции.

Охранные функции включают в себя:

• физическую охрану руководства и сотрудников организации (по месту работы и жительства, на маршрутах передвижения);

• формирование и поддержание безопасных условий хранения и использования материальных ценностей и финансовых ресурсов; осуществление эффективного пропускного режима;

• участие в обеспечении режима секретности проводимых работ и мероприятий;

• локализация негативных последствий утечки информации, иных чрезвычайных происшествий.

Информационно-аналитические функции подразумевают:

• сбор и систематизацию информации, характеризующую степень защищённости бизнеса;

• выявление вероятных деликвентов, планирующих посягательства на безопасность организации, каналов утечки информации, предпосылок, могущих привести к чрезвычайным происшествиям;

• проверку надёжности и иных имеющих значение для обеспечения безопасности бизнеса качеств и аспектов деятельности лиц при приёме на работу, а также (выборочно) персонала предприятия;

• проведение частных расследований по фактам промышленного шпионажа, хищений на охраняемых объектах;

• аналитические исследования для выработки тактически и стратегически важных решений по защите деятельности организации;

• подготовка рекомендаций по совершенствованию форм и методов работы в сфере безопасности.

Организаторские функции предполагают:

• организацию режима секретности осуществляемых работ; для этого совершенствуется организационная структура предприятия с учётом требований безопасности производственной, коммерческой, финансовой и иной его деятельности;

• планирование предупреждения и противодействия посягательствам на безопасность организации по расстановке ресурсов, используемых для обеспечения безопасности бизнеса;

• координацию и взаимодействие с другими частными службами безопасности, правоохранительными структурами; организацию работы в чрезвычайных ситуациях, когда наблюдается явная угроза безопасности бизнесу.

Воспитательные функции — это:

• своевременное информирование персонала о выявленных фактах посягательства на безопасность организации;

• пропаганда и объяснение правил обращения с информацией, являющейся коммерческой тайной;

• обучение персонала формам и методам использования средств индивидуального обеспечения безопасности;

• подготовка сотрудников в части, касающейся организации безопасности бизнеса;

• формирование соответствующего психолого-нравственного климата, который бы сводил к минимуму ситуации, провоцирующие персонал к совершению деликтных действий, наносящих ущерб предприятию, облегчал бы выявление таких попыток и повышал эффективность действий сотрудников в экстремальных ситуациях;

• обеспечение готовности персонала организации к отпору в случае посягательства на их личную безопасность и безопасность ор-

ганизации.

Директивные функции сводятся к принятию управленческих решений тактического характера для обеспечения безопасности, а также по совершенствованию работы с персоналом. Все управленческие решения принимаются только согласно определённым процедурам, правилам, инструкциям и методическим указаниям.

Контрольные функции охватывают проверку исполнения принимаемых решений в сфере обеспечения безопасности, включая оценку их эффективности.

Контроль представляет собой такой вид управленческой деятельности, задачей которой является количественная и качественная оценка и учёт результатов деятельности по обеспечению экономической безопасности хозяйствующего субъекта.

К основным причинам необходимости указанного контроля относятся:

• неопределённость, сложность и динамичность развития внутреннего и внешнего деликтного фона;

• предупреждение возникновения деликтных ситуаций посредством обнаружения несоответствия девиантных действий персонала и третьих лиц до того, как они нанесут организации ощутимый экономический вред;

• поддержание успешной деятельности организации путём сопоставления фактических затрат на обеспечение экономической безопасности и показателей предотвращённого ущерба.

3.3 Основные подразделения службы безопасности

В зависимости от специфики деятельности предприятия его служба безопасности может состоять из разных подразделений. Это

режимное, сыскное, охранное, техническое и другие (рисунок 5).

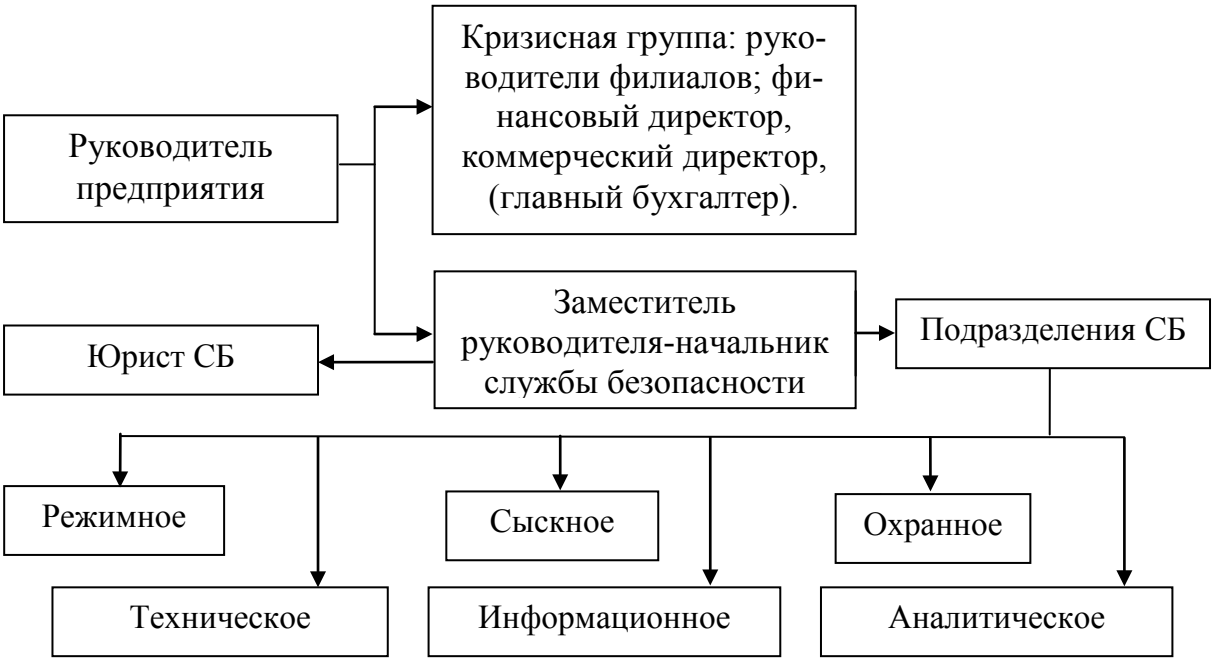


Рисунок 5 — Организационная структура внутрифирменной службы безопасности

Режимное подразделение создаётся, когда работа предприятия связана с коммерческими тайнами или его деятельность предполагает наличие информации конфиденциального характера. Это подразделение выполняет, как правило, следующие функции:

• определение состава сведений и информации, представляющих собой конфиденциальную тайну;

• подготовка внутренних инструкций и положений о порядке работы с конфиденциальной информацией и коммерческой тайной;

• осуществление допуска персонала к работе с документами, содержащими конфиденциальную информацию и коммерческую тайну;

• организация и ведение закрытого делопроизводства;

• формирование инструментария по учёту документов, содержащих коммерческую тайну, а также учёт фактов ознакомления персонала с такой информацией;

• проверка документов, материалов и т.п., выходящих за пределы организации, на наличие в них сведений для служебного использования и коммерческой тайны;

• контроль за выполнением персоналом режимных требований, а также посещений посторонними лицами предприятия.

Спецрежим вводится в таких служебных помещениях, где персонал работает с информацией ограниченного распространения. Это имеет отношение и к помещениям производственного назначения, когда к коммерческой тайне отнесены образцы товаров и изделий или технологическая информация (приёмы работ и пр.).

Аналитическое подразделение подключается к работе режимного подразделения и взаимодействует с ним в части определения состава сведений, подлежащих грифованию, и мер обеспечения их безопасности. Режимное подразделение получает от аналитического сведения о характере взаимосвязи коммерческой тайны с другими служебными сведениями; это даёт возможность судить об этой тайне по таким параметрам и характеристикам, которые сами по себе к категории коммерческой тайны не относятся.

Взаимодействие необходимо и с охранным подразделением по вопросам, связанным с посещением предприятия сторонними лицами. Совместно с техническим подразделением службы безопасности они находят решение вопросов использования технических средств для осуществления режимных мер, контроля за доступом к документам и иным носителям секретной информации.

Контакты с информационным подразделением службы безопасности связаны с решением проблем фиксирования объёма осведомлённости сотрудников, создания автоматизированной системы в интересах режимного подразделения. Вместе с сыскным подразделени-

ем расследуются факты и устраняются причины утечки информации.

Сыскное подразделение создаётся, прежде всего, если в организации есть значительный объём работ, связанных с выполнением функций сыска, когда предполагается, что предприятие может стать объектом промышленного шпионажа. Это подразделение выполняет следующие функции:

- проверяет граждан и организации, оказывающихся в поле зрения службы безопасности;
- изучает отдельных сотрудников, клиентов и партнёров, включая потенциальных, жителей ближайшего окружения, в действиях которых могут содержаться угрозы безопасности предприятия;
- разрабатывает и проводит в соответствии со своими полномочиями спецмероприятия в отношении предприятий-конкурентов.

Сыскное подразделение взаимодействует:

- с кадровым аппаратом — в процессе контроля и проверки кандидатов, принимаемых на работу, а в случае необходимости и всего персонала организации;
- со всеми отделами предприятия по расследованию выявленных фактов криминальной конкуренции;
- с правоохранительными структурами, службами безопасности других организаций, с частными сыскными агентствами и бюро.

Охранное подразделение создаётся в случаях, когда необходимо ограничить или полностью исключить посещение предприятия посторонними лицами, в тех случаях, когда в помещениях имеются материальные ценности или денежные средства, производятся работы закрытого характера, хранятся секретная информация или предметы, содержащие коммерческую тайну.

К основным объектам охраны относятся руководители и со-

трудники предприятия, офисы, складские помещения, производственные цехи, грузы, денежные средства, финансовые и бухгалтерские документы.

В функции охранного подразделения входят:

- охрана зданий, сооружений, помещений;
- физическая охрана руководителей организации, отдельных лиц из утверждённого перечня сотрудников;
- разработка правил пропускного режима и его осуществление;
- охрана грузов и денежных средств при их транспортировке;
- выявление угроз для безопасности охраняемых объектов.

Особую роль в работе охранного подразделения играет учёт посещений, дежурств и происшествий в специально заведённых журналах. В них обычно отражаются наблюдения, результаты контрольных проверок, замечания, жалобы персонала и сторонних граждан, фиксируются случаи срабатывания охранной сигнализации, происшествия, записываются распоряжения руководства организации и т.п.

В состав охранного подразделения может входить оперативная группа, прибывающая на место происшествия при непосредственной угрозе жизни и здоровью сотрудников предприятия или в иных, заранее определённых инструкциями и положениями, ситуациях.

Охранным подразделением осуществляется тесное взаимодействие с техническим подразделением по проблемам оборудования организации охранно-противопожарной и другой сигнализацией, проведения её своевременного обслуживания и ремонта.

Сыскным подразделением предоставляются сведения, характеризующие ситуацию окружения охраняемого объекта. Для прогнозирования обстановки вокруг охраняемого объекта осуществляется согласование действий с аналитическим подразделением. Безусловно,

что надо также установить сотрудничество с рядом находящимися подразделениями органов внутренних дел.

Состав и численность сотрудников охранного подразделения устанавливаются приказом руководителя предприятия в зависимости от количества и состава объектов, подлежащих охране, поставленных задач, режимов охраны — круглосуточного, ночного — и работы его персонала.

Техническое подразделение создаётся, когда есть предположения, что в отношении организации будут применяться электронные средства разведки. Причём, когда безопасность предприятия обеспечивается в основном с помощью применения технических средств — охранно-противопожарной сигнализации, средств видеонаблюдения и т.п.

Считается, что техническое подразделение целесообразно формировать, если имеются, по крайней мере, два других подразделения службы безопасности, использующие в своей работе технические средства[16].

Техническое подразделение обычно осуществляет:

• разработку инженерно-технологической и технической сторон системы обеспечения безопасности предприятия;

• заказ, приобретение, установку, настройку и обслуживание, включая текущий ремонт, проведение профилактических мероприятий, технических средств обеспечения безопасности (сигнализации, видеонаблюдения, связи, пожаротушения и др.);

• проведение экспертизы рынка технических средств обеспечения безопасности, технического обеспечения мероприятий сыскного подразделения;

---

[16] URL: http://library.tuit.uz/skanir_knigi/book/informasionnaya_bezopasnost/infor_bezopas_1.htm (дата обращения: 11.09.2011).

• разработку мер с целью выявления фактов применения технических средств промышленного шпионажа и противодействие ему с использованием собственных технических средств организации.

Согласованные действия с информационным подразделением необходимы при проведении работ, связанных с категорированием объектов вычислительной техники, с целью предотвращения утечки информации по техническим каналам. С охранным подразделением эти действия осуществляются при разработке концепции охраны, установке различных видов технических средств. Вместе с сыскным подразделением они находят решение проблемы технического обеспечения проводимых спецмероприятий.

Информационное подразделение создаётся при наличии существенного объёма данных, имеющих значение для обеспечения безопасности организации и, при необходимости, проведения сложных процедур их обработки в рамках короткого периода времени.

Указанное подразделение осуществляет:

• сбор, накопление, хранение, обработку и ликвидацию информации, играющей важную роль для обеспечения безопасности бизнеса, в том числе в интересах других подразделений службы безопасности;

• формирование и развитие информационной системы службы безопасности;

• приобретение, а в необходимых случаях разработку программных средств, предназначенных для обеспечения безопасности информации.

Сведения для этого подразделения поступают из всех подразделений предприятия, в том числе из иных подразделений службы безопасности, специализированных информационных учреждений и организаций, как частных, так и государственных (информация бирж, кон-

сульских отделов посольств, кредитных организаций и т.д.).

Аналитическое подразделение создаётся при наличии сложной обстановки, многоплановых угрозах безопасности предприятия, множественности всевозможных притязаний со стороны субъектов деликтной конкуренции (рейдерство и пр.).

Основные функции аналитического подразделения связаны:

• с разработкой концепции обеспечения безопасности бизнеса, её стратегии; анализом угроз безопасности предприятия;

• с выявлением лиц, являющихся потенциальными субъектами деликтной конкуренции; постановкой задач перед другими подразделениями службы безопасности;

• с аналитическим обеспечением мероприятий по локализации последствий конкретных фактов деликтной конкуренции.

Аналитическое подразделение получает информацию в основном непосредственно от руководителей предприятия и службы экономической безопасности, а также информационного подразделения.

Деятельность аналитического подразделения предполагает создание различных защитных моделей, имеющих отношение к сфере безопасности предпринимательства[17]. Эта деятельность включает формирование методик по необходимым организации исследованиям, а также расчёты вероятного ущерба от утечек информации, определение рыночной стоимости коммерческой тайны и др.

Анализ деятельности подразделений службы безопасности предприятия показывает, что в ней существенную роль играет взаимодействие с внешними организациями и правоохранительными органами.

Общеизвестны проблемы, связанные с нестабильностью российского законодательства. Поэтому деятельностью всех подразделений

[17] Одинцов А.А. Экономическая и информационная безопасность предпринимательства. М.: Изд-во «Академия», 2008.

службы безопасности требует квалифицированной юридической поддержки. Мы убеждены — в штаты службы безопасности на предприятиях следует обязательно вводить должность юрисконсульта, специализирующегося на вопросах обеспечения защиты бизнеса от деликтной конкуренции.

3.4 Анализ деятельности партнёрской организации службой безопасности

Мы считаем существенным моментом проведения анализа деятельности партнёров по бизнесу для того, чтобы выявить потенциальную криминальную направленность, спрогнозировать деликтное поведение партнёров, получить негативную информацию, компрометирующую партнёрскую фирму.

Преимущественными источниками и методами получения информации являются: прямое наблюдение; опросы руководства, носящие разведывательный характер; оперативно-технические средства получения информации; внедрение к партнёрам сторонних специалистов и предложение таким предприятиям полного или частичного набора услуг в области безопасности.

Проверка и контроль благонадёжности партнёра является серьёзным фактором стабильности и эффективности деятельности любой предпринимательской структуры.

До подписания хозяйственного и иного договора (контракта) с будущим партнёром по бизнесу следует проверить ряд документов. К ним относятся:

- устав предприятия;
- свидетельство о государственной регистрации юридического лица (ОАО, ООО и т.д.);

• свидетельство о постановке на учёт в налоговом органе;

• информационное письмо органов статистики;

• имеющиеся лицензии;

• протокол общего собрания или иного уполномоченного органа о назначении первого лица (руководителя);

• доверенность на конкретную сделку;

• разрешение органа управления на совершение данной сделки;

• паспорт лица, подписывающего договор от имени данного юридического лица;

• выписки движения денежных средств по счетам (за год или более), заверенные банком.

Для принятия решения о благонадёжности партнёра руководителю необходима объективная информация. Служба безопасности должна ответить на вопросы:

• какой срок и как стабильно функционирует предполагаемый партнёр?

• есть ли основание считать, что юридическое лицо зарегистрировано только для осуществления одной или нескольких операций?

• находится ли партнёр фактически по указанному адресу?

• каков профессиональный опыт руководящего состава фирмы-партнёра?

• какова деловая история и репутация юридического лица?

• кто является наиболее значимым партнёром по бизнесу и их отзывы?

• есть ли зарегистрированные и латентные случаи мошенничества руководителей юридического лица?

• какова иерархическая структура хозяйствующего субъекта, включая количество филиалов (подразделений) и их назначение, на-

личие дочерних, зависимых, сестринских и других компаний?

• может ли юридическое лицо отвечать по своим обязательствам, есть ли у него в наличии недвижимость, товарно-материальные ценности и иные видов залогов?

• сохраняется ли стабильность состава учредителей и руководства?

• имеется ли наличие фактов участия проверяемого юридического лица в судебных и административных разбирательствах, кто выступал в качестве истца или ответчика, принятые по таким делам решения, кто представлял интересы указанного лица в суде?

• каков уровень отношений данной организации с властными структурами?

• есть ли связь руководителей юридического лица с криминальными структурами, наличие сомнительной деятельности и неэтичного поведения?

• каково финансовое состояние потенциального партнёра (рентабельность, себестоимость, наличие денежных средств на расчётном и депозитных счетах, ликвидность, платёжеспособность и пр.) и есть ли финансовые нарушения?

Необходимую аналитическую информацию о финансово-хозяйственной деятельности фирмы-партнёра можно получить из ряда источников:

1) из открытых источников:

1.1. От самого партнёра: устав, лицензия, свидетельство о государственной регистрации, бухгалтерский баланс, письменные ответы на вопросы путём анкетирования, разведбеседы с различными представителями этого предприятия.

1.2. На основе статистического учёта регистрационных органов:

запросы в регистрирующий орган, федеральную налоговую службу по месту постановки на налоговый учёт, пенсионный и иные фонды, торгово-промышленную палату и т.д.

3.3. Из средств массовой информации, включая интернет-источники.

2) из иных источников:

2.1. Из имеющихся информационных баз данных.

2.2. От правоохранительных органов относительно участия данного предприятия и его руководителей в уголовных делах в качестве подозреваемых; арбитражных и гражданско-правовых судебных разбирательствах;

2.3. От специалистов маркетинга, обладающих достоверной и новой информацией об официальной стороне бизнеса данного предприятия на основе сбора информации об определённом секторе рынка;

2.4. Из кредитных организаций, у которых проверяемое юридическое лицо получает ссуды, и которые осуществляют его расчётно-платёжное обслуживание;

2.5. Из информационных материалов детективных агентств.

3) оперативными методами:

3.1. От персонала проверяемого предприятия, включая уволенных лиц.

3.2. Методами технической разведки.

3.3 Сбором косвенной информации (скрытое наружное наблюдение, посещение проверяемого хозяйствующего субъекта под видом потенциального клиента, пожарной службы и т.д.).

Выделяют несколько основных направления сбора информации в отношении потенциального партнёра:

1. Сведения о рынке или секторе рынка, в котором функциони-

рует данное предприятие, включая:

• физический и стоимостный объёмы, тенденции и прогноз сбыта продукта, имеющего конкурентный характер;

• ценовые параметры, условия договора, спецификацию продукта, наличие скидок и льгот;

• объём занимаемого рыночного пространства и перспектива (потенциал) его изменения;

• характер рыночной политики и уровень текущего и перспективного планирования;

• характер отношений с потребителями товара (услуг) и меры, направленные на возможный количественный рост их числа;

• численность и расстановка торговых представителей;

• каналы, политика, формы и методы сбыта продукции или оказания услуг;

• уровень рекламной деятельности.

2. Информация о производстве продукции:

• номенклатура изделий, перечень услуг;

• оценка качества товара и эффективности производственной деятельности;

• инновационный уровень технологического процесса, машин и оборудования;

• характеристика производственных мощностей;

• уровень издержек на производство товаров;

• способы упаковки товара, действующие логистические цепи и схемы поставки товара;

• характер размещения структурных подразделений, имеющих производственный характер, и мест складирования товара;

• перспективы, связанные с использованием потенциала пред-

приятия для проведения научно-исследовательских, опытно-конструкторских и иных разработок.

3. Характеристика информационного поля об организационных особенностях, экономике и финансах предприятия:

• выявление и анализ деятельности менеджеров, принимающих главные решения;

• ценностная ориентация менеджеров, принимающих ключевые решения;

• анализ программ расширения деятельности и описание перспектив возможных приобретений;

• основные проблемы, стоящие перед предприятием и возможности их решения.

Важно определиться с неблагонадёжностью юридического лица**.** В процессе проверки потенциального партнёра, необходимо обращать внимание на основные признаки, характеризующие его правовую дееспособность. Данные признаки (факторы) являются основными индикаторами неблагонадёжности, как показателя, характеризующего неэффективную хозяйственную деятельность анализируемого предприятия. В их числе:

1. Имеющиеся факты значительного числа дел, связанных с арбитражными разбирательствами, с частой заменой юрисконсультов.

2. Отсутствие внутрифирменного аудита, а при его наличии частая замена аудиторов, факты отказов аудитора от вынесения аудиторского заключения.

3. Факты частых и непредсказуемых отставок членов совета директоров и/или правления.

4. Факты отзывов лицензий контролирующими органами.

5. Проблемы со своевременным перечислением налогов в бюд-

жеты разных уровней.

6. Высокий уровень текучести кадров (персонала).

7. Чрезмерно высокая задолженность перед кредиторами.

8. Предприятие зарегистрировано и имеет счета в оффшорной зоне.

9. Регулярная структурная реорганизация.

10. Низкий уровень комплексной системы безопасности предприятия.

11. Систематическая пролонгация исполнения обязательств, неоднократная и длительная просроченная задолженность и её рост.

12. Рост активов неудовлетворительного качества, факты использования переоценки нематериальных активов.

13. Для кредитных организаций: рост процентных ставок по депозитам и долговым ценным бумагам при стабильной ситуации на финансовом рынке.

14. Информация о перечислении причитающихся платежей на счета третьих лиц либо на иные счета, не указанные организацией в официальных реквизитах.

15. Факты того, что организацией руководят менеджеры, с именем которых была ранее связана процедура банкротства возглавляемых ими предпринимательских структур.

16. Предприятие слишком часто меняет фактический и юридический адреса.

17. В правоустанавливающих документах имеются признаки изменений и подделок (дописки, травление текста и т.п.)

18. Учредители (акционеры) предприятия очень часто преобразовывают свой юридический статус без решения вопросов правопреемства.

19. Чрезмерно низкий по отношению к объёму проводимых операций (хотя и соответствующий законодательству) или неоправданно высокий уставный капитал.

20. Организация демонстрирует «нулевую» или отрицательную прибыльность.

21. Предприятие, из уставного капитала которого выходит владелец крупного пакета (нескольких десятков процентов) акций/паёв.

22. Наличие поручителей, не считающихся надёжными.

23. Факт того, что у предприятия отсутствует собственное помещение или фирма арендует помещение недавно.

24. Организация имеет счета в банках с низким рейтингом.

25. Несовпадение юридического адреса предприятия и фактического местонахождения, регистрация (прописка) руководителя организации в другом городе или регионе.

26. Факт наличия двойного гражданства у владельцев и топ-менеджеров организации.

Особое внимание надо уделить криминальным связям проверяемых фирм-партнёров с государственными структурами. Изучение криминальных связей — одна из первоочередных задач обеспечения экономической безопасности в современных условиях ведения бизнеса. Сбор и анализ такой информации даёт возможность оценки внешних угроз, может помочь спрогнозировать развитие бизнеса и спланировать свои действия на перспективу.

Подчеркнём, что надо обращать внимание на поведение партнёра, которое может косвенно говорить о его ненадёжности:

• необычная поспешность и суетливость в процессе проведения переговоров о получении авансов, ссуды или получении товаров на реализацию;

• демонстративный показ завышенных возможностей в деловом мире, которые трудно или невозможно подтвердить фактически;

• предложение условий договора значительно более выгодных, чем сложилось на рынке;

• отсутствие тщательности письменного оформления договора, с последующей устной оговоркой ряда пунктов;

• отсутствие договорных гарантий возврата ссуды или наличие иных оговорок, не дающих возможности получения долга через арбитражный или третейский суд[18].

После сбора общей аналитической информации о проверяемом объекте (предприятии, организации) делается анализ полученных сведений и определяется степень его компетентности и надёжности как потенциального партнёра. На основании проверки принимается одно из следующих решений: а) отказ от оферты; б) об акцепте оферты на иных условиях; в) об акцепте оферты.

Офертой в соответствии со ст. 435 ГК РФ признаётся адресованное одному или нескольким конкретным лицам предложение, которое достаточно определено и выражает намерение лица, сделавшего предложение, считать себя заключившим договор с адресатом, которым будет принято предложение.

Акцептом в соответствии со ст. 438 ГК РФ признаётся ответ лица, которому адресована оферта, о её принятии. При этом ответ о согласии заключить договор на иных условиях, чем предложено в оферте, не является акцептом.

При ведении преддоговорной деятельности необходимо руководствоваться следующими моментами:

1. При заключении договора надо договориться, что оплата то-

[18] Яскевич В.И. Секьюрити: Организационные основы безопасности фирмы. М.: «Ось-89», 2005.

вара будет производиться по факту его поступления.

2. Чётко понимать: несколько эффективных, но мелких сделок, проведённых ранее, не являются основанием для проведения крупной сделки.

3. В процессе заключения договора, следует включить в него пункты, обеспечивающие контроль и личное участие в расходовании средств и распределении прибыли.

4. Договор должен содержать конкретные условия, содержащие свой экономический интерес, для недопущения двоякого толкования его положений.

5. Следует быть крайне внимательным, когда предлагаются необычно выгодные условия договора.

6. Частыми фактами бывают многократные перезакладывания залогов, что требует тщательной проверки.

7. Проверка содержания счётов-фактур и актов приёма-сдачи выполненных работ и оказанных услуг требует личного участия.

8. Требуется контроль за достоверностью полномочий представителя организации-партнёра и гарантий сторонних организаций.

3.5 Этапы проверки фирмы-партнёра на степень благонадёжности

Работники службы безопасности, осуществляющие проверку потенциальной фирмы-партнёра на предмет ведения совместной предпринимательской деятельности, на преддоговорной стадии обязаны уведомить её о проведении проверки и предложить заполнить особую анкету («опросник»), запросить копии, а в необходимых слу-

чаях подлинники документов, перечисленных нами выше[19].

После этого оформляются запросы в регистрационный реестр юридических лиц, налоговый орган по месту нахождения или регистрации, при необходимости — в таможенный орган. На потенциального партнёра заводится специальная карточка учёта.

Материалы проверяемого предприятия отрабатываются по всем доступным службе безопасности базам данных, включая обзоры прессы, рекламные продукты и пр. Для проведения комплекса оперативных мероприятий создаётся план-задание, принимаемое к исполнению соответствующими структурами.

В процессе проверки учитывается специфика финансово-хозяйственной деятельности конкретной фирмы-партнёра. Выстраивается чёткая схема проверки и линия поведения в отношении проверяемого юридического лица. Обязательной проверки подлежит информация, которая является общедоступной, то есть той, которая не относится к категории «коммерческая тайна». Эта информация анализируется как по учредительным документам, так и документам, предоставляющим право организации занятия предпринимательской деятельностью. Также подлежат проверке и анализу:

• бухгалтерские балансы, годовые отчёты, статистическая отчётность, формы, показывающие начисление налогов и других обязательных платежей;

• порядок начисления и задолженность по выплатам заработной платы, а также другим выплатам социального характера;

• если речь идёт об акционерном обществе, то раскрывается информация об эмитенте ценных бумаг в соответствии с Федеральным законом РФ «О ценных бумагах»;

---

[19] Нежданов И.Ю. Проверка благонадёжности юридического лица. URL: http://www.it2b.ru/blog/arhiv/672.html (дата обращения: 08.09.2011).

• возможность преобразования, слияния или поглощения, а также ликвидации фирмы-партнёра; учитывается возможный порядок и сроки выполнения требований кредиторов по выполнению своих обязательств;

• выясняются факты наличия задолженности в местный, региональный и федеральный бюджеты;

• в обслуживаемом коммерческом банке проверяется наличие инкассовых поручений.

Анализ устава потенциального партнёра на преддоговорном этапе связан с необходимостью:

• выявления различного рода ограничений в проведении конкретных видов предпринимательской деятельности;

• выявления цели образования данного предприятия, имеющей криминальный характер;

• выяснения полномочий топ-менеджеров, наличие утверждённой процедуры назначения и увольнения членов совета директоров и членов правления;

• установления видов гражданских правоотношений, степени абсолютных и абсолютно-относительных вещных прав учредителей (акционеров, пайщиков) организации;

• уяснения порядка наложения права вето на принимаемые решения, процедуры голосования, регламента принятия решений советом директоров; учитываются сроки избрания, переизбрания, включая досрочное, оснований, предусматривающих созыв экстренного собрания акционеров (пайщиков) и т.п.

Любая, даже самая краткая информация может при тщательном изучении устава организации выявить непоследовательность решений, принимаемых руководителями потенциальной фирмы-партнёра.

Анализ рекламной деятельности и самих рекламных продуктов потенциального партнёра производят с целью выявления:

• агрессивности поведения проверяемой организации на рекламной площадке, что может свидетельствовать о криминальных мотивах фирмы-партнёра. Это особенно ярко проявляется в банковской сфере, когда испытывающий финансовые неурядицы коммерческий банк повышает ставки вкладных процентов и проводит агрессивную рекламную компанию с целью привлечения денежных средств;

• куда направлена рекламная акция, на какой аудиторный или рыночный сегмент;

• партнёров рекламной акции, то есть тех, кто занимается её реализацией (сама организация, рекламное агентство и пр.);

• разнообразие рекламы, её творческий потенциал, степень воздействия на аудиторию.

Анализ рекламной деятельности проверяемого бизнес-партнёра обычно проводят с помощью контент-анализа[20]. Такой анализ направлен на выявление смысловых единиц и подсчёте частоты их появления.

Выделяют следующие этапы контент-анализа:

— анализ стратегии проверяемого партнёра по бизнесу, его негативные и лидерские качества, миссии, девизы, лозунги и т.п.;

— выявление прямых индикаторов (смысловая нагрузка, облечённая в конкретные слова, слоганы, деепричастные обороты, фразы и т.д.). После этого выбирается единица измерения: частота появления смысловых единиц, строк, площадь газетных полос, длительность трансляции по радио и телевидению, частота размещения на соответ-

[20] Контент-анализ (от англ. *contens* – содержание) – специальный достаточно строгий метод качественно-количественного анализа содержания документов в целях выявления или измерения социальных фактов и тенденций, отраженных этими документами. (URL: http://www.slovari.yandex.ru).

ствующих интернет-ресурсах;

— сам анализ, дающий информацию к размышлению об устремлениях рекламодателя, методах его работы и факторах риска[21].

Платёжеспособность, финансовая надёжность и устойчивость являются важнейшими характеристиками финансово-экономической деятельности предприятия. Чем выше эти показатели, тем меньше риск возможного банкротства, тем больше организация не зависит от колебаний рыночных конъюнктуры и неопределённости.

В целях оперативного (упрощённого) финансового анализа проверяемого партнёра по бизнесу целесообразно воспользоваться методикой, разработанной Л. Ващенко и А. Бережным[22], которая включает ряд этапов:

1-й этап**.** Получение документации, необходимой для финансового анализа. Это: бухгалтерский баланс (форма № 1); отчёт о прибылях и убытках (форма № 2); отчёт о движении капитала (форма № 3).

2-й этап. Проверка подлинности полученных для анализа документов, основанная на итоговой части аудиторского заключения по балансу.

3-й этап. Проведение предварительного анализа баланса.

4-й этап. Оценка финансовой устойчивости проверяемого партнёра. Если планируются длительные деловые отношения, связанные с приобретением акций, разработкой инвестиционных проектов, то проверяется уровень финансовой устойчивости или уровень степени защищённости инвесторов или акционеров. Для этого рассчитывается коэффициент автономии. Он определяется отношением собственных средств к общему итогу баланса.

---

[21] Яскевич В.И. Секьюрити: Организационные основы безопасности фирмы. М.: «Ось-89», 2005.

[22] URL: http://bre.ru/security/53.html (дата обращения: 21.09.2011).

5-й этап. Оценивается ликвидность организации.

6-й этап. Рассматривается оценка эффективности управления.

Дополнительную информацию о степени корпоративного уровня организации может дать анализ визитной карточки руководителя фирмы-контрагента. Этот метод основывается на том, что любой индивид при выборе варианта оформления визитки, руководствуется своими внутренними предпочтениями, перенося своё мировосприятие на материальное отображение.

Получение информации начинается с изучения материала носителя (в порядке увеличения ценовых качеств):

1) бумага обычной структуры;
2) «лощёная» бумага;
3) бумага повышенной плотности;
4) рисовая или хлопковая бумага.

Обычная бумага — свидетельство режима жёсткой экономии у контрагента, либо — показной аскетизм. Дорогая бумага, напротив, свидетельствует либо о высоких доходах, либо о желании произвести впечатление. Меньше всего информации дают варианты 2 и 3.

Следует проанализировать способы печати, которые определяют особое отношение руководства к фирменному стилю. Они располагаются в порядке возрастания цены:

1) обычный;
2) офсетный;
3) глубокий;
4) трафаретный;
5) с подъёмом.

Изображение логотипа на визитке определённым образом отражает намерение своих создателей:

• расплывчатость формулировки в ряде случаев определяет характер аферистов;

• замкнутость — символ направлен в себя или вовне, является показателем направленности деятельности самой организации (например, символ, заключённый в круг, считается самым замкнутым вариантом, в многоугольник предполагает тенденцию к прорыву во внешнюю среду).

Цветовое оформление визитной карточки даёт информацию о характерологических параметрах её владельца:

• фиолетовый цвет предполагает некую утончённость, то что владелец избегает резких противоречий, тяготеет к творчеству без лишних эмоций;

• синий цвет может означать артистичность, переходящую в аферизм, а также повышенную меру подозрительности и скрытности владельца;

• зелёный цвет говорит о спокойствии и уравновешенности;

• жёлтый цвет предполагает креативность, неустойчивость;

• золотой цвет обычно означает высокое самомнение, высокомерие, амбициозность;

• красный цвет это — импульсивность, агрессия, возможно поверхностное суждение о многих явлениях, включая экономические;

• коричневый — говорит о высоком уровне работоспособности при возможно ограниченных интеллектуальных ресурсах;

• монохром — чёрный, белый, серый это — стойкость, принципиальность, воля и максимализм.

Цветовое оформление визитной карточки, отображающее невербальную сторону общения с контрагентом, подразумевает её мотивы, связанные с:

• созданием иллюзии (лат. *illusio* — заблуждение, обман) или попыткой деформации реального состояния дел на данном предприятии;

• чрезмерным или недостаточным финансированием;

• крайней мерой персонификации руководителя, навязывающего своим подчинённым и сторонним организациям собственное решение деловых вопросов.

Проведение тщательного анализа с учётом вышеприведённых мотивов может выявить как нестабильное финансовое положение, авторитарный стиль руководства и дисгармонию в развитии организации, так и интеллектуальные пробелы (например, образовательные) руководителя.

Сбор информации о потенциальных партнёрах по бизнесу осуществляется исключительно в рамках действующего законодательства, с соблюдением морально-этических норм.

4 Кадровое обеспечение безопасности бизнеса

4.1 Система работы с персоналом с учётом требований безопасности предпринимательства

Способности, деловой настрой, опыт и квалификация персонала — залог эффективность предпринимательской деятельности организации. Профессиональный отбор кадров для нужд предприятия является одним из наиболее важных этапов работы с персоналом.

К персоналу относят работников организации, с которыми установлены трудовые отношения с учётом их квалификации, деловых и личных качеств.

Сегодня персонал — главная производительная сила предприятия, определяющая эффективность действия все других факторов, влияющих на развитие производства. С другой стороны, — персонал является источником основных угроз экономической безопасности. В соответствии с данными статистики с участием собственного персонала организации может наноситься до 80 % совокупного ущерба[23].

Механизм работы с персоналом включает в себя:

- решение организационно-штатных вопросов;
- выбор критериальных требований к каждому сотруднику по конкретному виду деятельности; их подбор, изучение, оценку, расстановку, воспитание, обучение, повышение квалификации;
- создание необходимых условий для труда и быта работников, мотивационное повышение эффективности их деятельности, сопровождаемое одновременным укреплением трудовой дисциплины.

Главными требованиями, обеспечивающими экономическую безопасность для персонала всех структурных подразделений пред-

[23] URL:http://parolesdici.net/content/view/7/9 (дата обращения: 18.08.2011).

приятия, являются:

- надёжность как фактор противодействия деликвентам;
- лояльность по отношению к собственникам своей организации;
- способность противостоять преступным посягательствам на экономическую безопасность предприятия;
- неуязвимость со стороны конкурентов и криминалитета.

Мы согласны с тем выводом, что «Грамотно поставленная и отлаженная работа с персоналом становится одной из составляющих успеха в любом бизнесе. Одним из важнейших элементов успешного менеджмента выступает эффективно организованный подбор персонала»[24].

Руководство организации должно контролировать, отвечает ли кадровая политика стратегии предприятия в целом, способствует ли проводимая работа с персоналом достижению поставленных бизнесом целей. Важен расчёт штатной численности персонала и его соответствие структуре предприятия, корректное наименование должностей, в соответствии с утверждённым перечнем.

К основным причинам угроз персонала относятся:

— некачественный подбор кадров, плохое изучение их деловых и личных качеств, упущения при оформлении договорных отношений (трудовых, материальной ответственности, авторских прав и др.);

— несоответствие квалификации работника занимаемой должности;

— отсутствие или низкая мотивация на достижение целей предприятия;

— неэффективная система менеджмента, включая деликт-менеджмент;

---

[24] Кадровая безопасность. Центр правовых инноваций [сайт]. URL: http://www.cpisb.com/business/security/personnel (дата обращения: 14.07.2011).

— отсутствие системы оплаты труда стимулирующего свойства;

— некачественная организация системы обучения и переподготовки работников;

— негативная психологическая атмосфера как на самом предприятии, так и в его удалённых подразделениях;

— недобросовестное поведение, отсутствие законопочитания и дисциплинированности, желание нанести ущерб, если ощущение риска попасть в поле зрения службы безопасности минимально;

— частые контакты с конкурентами и от этого попадание в зависимость от них;

— факты внедрения фирмами-конкурентами своих людей на предприятие, подкуп персонала для использования его в криминальных целях;

— отсутствие системы защиты интеллектуальной собственности;

— неправомерные деяния конкурентов, криминальных сообществ, злоупотребления госужарственных служащих и работников органов внутренних дел;

— сокрытие и/или искажение нанимаемым работником персональных сведений, о своих родственниках, имеющихся отношениях и связях с внешним миром и персоналом данного предприятия;

— перетаскивание конкурентами наиболее одарённых и трудоспособных работников, иногда запугивание с целью увольнения с данного места работы;

— компрометация руководителей, распространение сплетен и слухов, нечестная, так называемая «чёрная» реклама (например, в виде распространяемого по Интернету спама).

Основными источниками информации о кандидатах на работу могут служить социальные сети Интернета, СМИ, центры занятости,

рекрутинговые, аутстафинговые фирмы, работники предприятия, знакомые с кандидатом, соседи, бывшие сокурсники и т.п.

В процессе изучения принимаемых на работу кандидатов, а также переводе работников на ключевые должности применяют ряд методов. К ним относятся:

— проведение глубокого анализа анкетно-биографических данных кандидата, сторонних отзывов, характеристик, поручительств и рекомендаций с предыдущих мест работы;

— проведение бесед с кандидатом, с целью оценки его деловых и личных качеств, выявление фактов достижений в профессиональной деятельности, его способности занимать должность, на которую он претендует;

— оценку психологической устойчивости кандидата на основе тестирования и анкетирования;

— выявление нежелательных хобби, опасных и вредных привычек кандидата;

— проведение исследования, позволяющего выявить соответствие интеллектуальных способностей кандидата имеющемуся образованию и профессиональному опыту работы;

— во время испытательного срока изучение потенциальных возможностей, качества выполнения работы, выявление степени инициативности, работоспособности, взаимоотношений в коллективе, выявления фактов несоблюдения установленного режима работы;

— изучение соответствия требованиям для принятия решения о допуске к работе данного кандидата со сведениями, составляющими в данной организации коммерческую тайну.

К угрозам, направленным на персонал, относятся:

1) Конкуренция, включая недобросовестную.

Недобросовестная[25], нечестная конкурентная борьба связана с нарушением принятых норм и правил конкуренции, противоречащая положениям действующего законодательства, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости. Она создаёт нездоровую бизнес-обстановку вместо реализации цивилизованных стратегий соперничества, уступок и партнёрства.

Конкуренция связана:

— с переманиванием профессионалов высокого уровня на новую работу;

— с формированием на данном предприятии условий для ухода из фирмы одарённых работников;

— с внедрением в организацию людей на должности, имеющие доступ к коммерческой и служебной тайнам;

— с поиском новых идей, новаторских подходов и решений на конференциях, семинарах и совещаниях, которые специально организуются для последующего приглашения на работу в конкурентную фирму необходимых специалистов;

— с приглашением на работу специалистов по совместительству, чтобы затем склонить их к переходу на новое место (эта форма близка к коммерческому подкупу);

— с ограничением доступа на рынок или устранением с рынка, включая, прежде всего, действия по физическому воспрепятствованию деятельности конкурентов на рынке (крайняя форма, широко применяемая в России, — убийство ключевых лиц организации);

— со сбором информации, составляющей коммерческую, служебную и государственную тайну, с экономическим (промышленным) шпионажем;

[25] Подробно см., например: URL: http://newasp.omskreg.ru/bekryash/ch7p2.htm.

— выпуск некачественной продукции от имени фирмы-конкурента;

2) Действия криминальных структур.

3) Распространение ложных сведений, дезинформация, слухи, домыслы, направленные на снижение эффективности механизма управления, ликвидацию мотивации персонала.

Угроз, исходящих от персонала множество**.** Приведём лишь некоторые из них:

1. Кражи, хищения, порча оборудования, саботаж, вредительство, приводящее к крупным авариям, пожарам и пр.

2. Мошеннические действия, частые контакты с конкурентными структурами и попадание к ним в зависимость.

3. Тайное проведение работ и оказание услуг конкурентам за вознаграждение с использованием служебного положения, оборудования, ресурсов предприятия.

4. Передача конкурентам информации, содержащей коммерческую и служебную тайны, а также интеллектуальной собственности.

5. Распространение ложных сведений, дезинформация, распространение слухов, «чёрная реклама».

6. Тайный сговор с конкурентами.

7. Намеренное разжигание трудовых конфликтов, духа нездорового соперничество, разрушение психологического климата.

8. Неквалифицированное выполнение работ и оказания услуг.

9. Несоблюдение предусмотренных правил, нарушение режимных и других положений, принятых на данном предприятии.

Основные задачи по работе с персоналом состоят:

— в определении потребности в специалистах необходимого профиля;

— в проведении качественного подбора, изучении, оформлении кандидатов на работу;

— в адаптации, мотивации, обучении и переквалификации персонала.

Есть признаки, по которым можно выявлять сотрудников, склонных к внутренним кражам, хищениям, торговле и передаче коммерческой тайны. Сотрудник:

— работает на предприятии три года и более;

— приходит на работу раньше всех, задерживается дольше других, в отдельных случаях работает в субботу и воскресенье;

— прекрасно осведомлён о режиме работы службы охраны и специфике срабатывания охранной сигнализации;

— имеет прямой или косвенный (например, через родственников или друзей) доступ к ключам от основных служебных помещений;

— делает всё возможное, чтобы завоевать высокую степень доверия у руководства, получения права работать самостоятельно, без осуществления контроля со стороны службы безопасности предприятия;

— восторженно и часто восхищается деловыми качествами своих руководителей;

— замкнут, не поддерживает дружеских и деловых отношений с другими сотрудниками;

— относится к типу служащего, часто получающего премии и поощрения;

— для того чтобы завоевать доверие начальства часто информирует руководство об ошибках и/или проступках других работников.

В процессе профессиональной деятельности могут быть выявлены и другие особенности (например, психологические) поведения сотрудника, свидетельствующие о его ненадёжности и уязвимости от

конкурентов.

Особого внимания требует процесс подбора квалифицированных специалистов на ключевые должности и должности, связанные с коммерческой тайной (топ-менеджеры, работники АСУ, отдела кадров, службы охраны и др.). Следует выделить те сферы деятельности, где возможны хищения, мошенничество, утечка информации и взять их под контроль. Большое значение в этом отношении имеет отлаженное взаимодействие службы безопасности с отделом кадров и юридической службой.

Подчеркнём, что меры безопасности не должны сковывать инициативу работников, не позволяя предприятию успешно двигаться к достижению стратегических целей.

4.2 Проверка лояльности управленческого персонала на уровень девиантного поведения, противоречащего целям бизнеса

Как показывает анализ практики, латентность девиантного поведения персоналом на производстве очень высока. Однако наносимый ущерб можно свести к минимуму, если учитывать, что нелояльность персонала сама по себе не является главной причиной такого поведения. Это следствие сложного узла проблем в управлении организацией, коренящихся в наличии неизбежных противоречий между владельцем и наёмным персоналом.

Поэтому стержневая задача — постоянно убеждать персонал предприятия в необходимости оказания помощи службе безопасности на возмездной и без возмездной основах при проведении служебных расследований по фактам имущественных преступлений. Однако это не исключает проведение профилактических проверок персонала. Проверки делятся на:

• оперативные (носят выборочный характер, в случае чрезвычайных происшествий, разглашения конфиденциальной информации, подозрений в отношении конкретных работников и т.д.);

• регулярные (по заранее определённому графику).

Проверки могут гласными (порядок соблюдения инструкции по сохранности конфиденциальной информации, учёт корреспонденции, проведение ревизий и т.д.), что дисциплинирует персонал предприятия. Негласные проверки (негласное наблюдение) проводятся с целью выявления поведения сотрудника на работе и дома, во время отдыха, во время проведения праздничных мероприятий. Выявляются также его внешние и внутренние контакты.

Основная часть убытков организации образуется за счёт конкретных девиантных действий персонала. Причины таких действий различны, однако все они порождены самими сотрудниками, их отношением к своим функциональным обязанностям. Речь идёт об умышленном нанесении ущерба экономической безопасности хозяйствующему субъекту её работниками. Причём это может быть как инициативное деликтное деяние в целях личного обогащения и/или мести руководителю организации, так и по заданию недобросовестных конкурентов, партнёров по бизнесу или криминальных структур.

Потенциал наносимого экономического ущерба напрямую зависит от должностного позиции работника в иерархической структуре предприятия. Опасность данных имущественных преступлений может исходить, прежде всего, от самого первого лица. К первому уровню можно также отнести сотрудников, имеющих право подписи финансовых документов и выписки материальных пропусков, много знающих о движении финансовых потоков организации и контролирующих движение материальных ценностей. Это заместители дире́ктора

(управляющего) или же директора́ (где есть должность генерального директора) по сбыту, финансам и пр., главного бухгалтера и экономиста, кассира, программистов, заведующего складом и т.д.

Этот уровень работников может проявлять девиантное поведение в процессе:

• изготовления фиктивных финансовых документов, а также контрактов, договоров, дополнительных соглашений и т.д.;

• присвоения наличных денежных средств непосредственно из кассы;

• расходования наличных денег и средств на корпоративных пластиковых картах не по назначению;

• фальсификации денежных сумм, находящихся на банковских счетах;

• фальсифицирования накладных, записей и подписей в счетах, платёжных поручениях и требованиях, бухгалтерских книгах, чеках на получение наличных денежных средств;

• прямого хищения денег и материальных ценностей;

• завышении или занижении установленных цен;

• завышении числа отработанных сверхурочных часов;

• оплате работ и услуг сторонних организаций и частных лиц (например, по договорам подряда), которые фактически не выполнялись и т.д.

К признакам девиантного поведения топ-менеджеров относят:

1) Дезорганизацию работы предприятия, которая заключается в:

• частой смене председателя и членов совета директоров, а для АО — ещё и правления;

• заключении сомнительных и авантюрных сделок;

• формировании неповоротливой в управленческом смысле

слова организационной структуры;

• отвлечении от основной работы из-за частого участия в судебных процессах;

• непрофессиональных решениях из-за чего предприятие постоянно находится на грани несостоятельности и разорения;

• прямую зависимость организации от продажи продукции нескольким компаниям;

• нежелании создать своё подразделение аудита, частой смене внешних аудиторских компаний.

2) Чрезмерное отклонение финансовых показателей от ранее имеющихся и планируемых. Это заключается в:

• резком увеличении фактических доходов при уменьшении различного вида запасов, уменьшении оборота по кассе и расчётному счёту;

• росте запасов при снижении кредиторской задолженности;

• увеличении запасов при уменьшении затрат на обслуживание складской инфраструктуры;

• резких скачках показателей статей квартальной балансовой отчётности;

• росте дебиторской задолженности и возникновении проблем по её возврату;

• резком росте расходов на фоне снижения доходов и т.д.

Кроме топ-менеджеров девиантное поведение также присуще и нижестоящему персоналу (специалистам, служащим). Признаки такого поведения:

1) Нарушение правил ведения бухгалтерского учёта:

• неправомерное задерживание платежей;

• предоставление вместо подлинников копий платёжных доку-

ментов;

• указание неточных платёжных реквизитов заказчиков, получателей платежей и их банков;

• наличие чрезмерной дебиторской и кредиторской задолженности.

2) Существенные отклонения показателей от средних значений:

• допущение фактов недостач или излишков;

• резкое увеличение остатков товарно-материальных ценностей.

Наиболее уязвимой сферой, где проявляется девиантное поведение, дающее персоналу использовать служебное положение в корыстных интересах, — торговый бизнес. Обычно это складские операции, связанные с получением товаров, расходование денежных средств, взятых под отчёт и т.д.

Следует обращать внимание на девиантное поведение сторонних организаций. К признакам такого поведения относятся**:**

• слишком частые увольнения юристов;

• привлечение данного предприятия к судебным процессам;

• частые смены аудиторских компаний и внутренних аудиторов;

• привлечение сторонних налоговых и иных консультантов, имеющих навыки ведения теневого бизнеса;

• частое и неплановое проведение проверок контролирующих органов (налоговая инспекция и пр.);

• наличие нескольких расчётных счетов в банках, регулярная смена кредитных организаций;

• наличие просроченной задолженности по кредитам коммерческих банков;

• наличие просроченной кредиторской задолженности;

• работа с сомнительными юридическими лицами и криминалитетом.

Минимизация экономического ущерба бизнесу должна не только состоять в создании профилактического многоуровневого механизма предупреждения девиантного поведения сотрудников, но и сопровождаться перестройкой системы мотивации производственного звена персонала (основных и вспомогательных работников), напрямую связанных со степенью валентности[26].

Самые строгие меры безопасности, выстроенные на инновационных технологиях, не могут дать необходимого эффекта, если они не будут подвергаться на предприятии регулярным видоизменениям. Именно поэтому следует постоянно осуществлять ряд мероприятий. К ним относятся:

• увольнение по инициативе работодателя работников, допускающих девиантное поведение, или принуждение их к увольнению по собственному желанию;

• показательное увольнение работников, вина которых установлена в соответствии с действующими правилами;

• передача дел, связанных с имущественными деликтами в правоохранительные органы, о чём широко оповещаются все сотрудники предприятия;

• выплата более высокого уровня вознаграждений и зарплат, чем у предприятий-конкурентов;

• выплата премиальных работникам тех участков, на которых не было хищений;

• формирование социального пакета (организация доставки ра-

[26] Валентность – это предполагаемая степень относительного удовлетворения или неудовлетворения, возникающая вследствие получения определённого вознаграждения. Для более полного понимания этого процесса советуем читателю изучить теорию ожиданий В. Врума.

ботников на работу и обратно, питания в обеденный перерыв; медицинского обслуживания, страхования, выдач займов и т.д.);

• внедрение систем материального стимулирования за лояльное отношение к предприятию;

• применение нематериальных стимулов к труду, связанных с направлением работников на курсы повышения квалификации стажировки и командировки, установлением гибкого графика работы и дополнительных отпусков;

• пропагандирование системы как стандартных корпоративных правил и моделей поведения[27], так и разработанных предприятием и выражающих согласованную волю собственников и коллектива работников, руководствующихся данными правилами;

• разработка и применение программ повышения уровня мотивации, лояльности и приверженности работников своему предприятию;

• проведение мероприятий по преодолению негативного отношения к частной собственности[28].

Мы убеждены, что такие меры могут помочь персоналу более уважительно относиться к собственности в правовом и нравственном аспектах.

---

[27] См., например, «Кодекс корпоративного поведения», разработанный Федеральной комиссией по рынку ценных бумаг (ФКЦБ) России (URL: http://www.intalev. ru/agregator/press/id_8917) или «Кодекс делового поведения» разработанный российской Торгово-промышленной палатой при участии российско-американского Комитета по развитию делового сотрудничества (URL: http://www.academy-go.ru/Site/EconomEtica/Seminar/KDP.shtml).

[28] Яскевич В.И. Секьюрити: Организационные основы безопасности фирмы. М.: «Ось-89», 2005.

5 Коммерческая тайна как механизм защиты интересов бизнеса

5.1 Понятие коммерческой тайны и коммерческих секретов

Предпринимательская деятельность связана с получением, хранением и последующим использованием различного рода сведений и информации. Сегодня информация представляет собой товар, имеющий определённую, иногда очень высокую, стоимость. Наиболее ценной считается та информация, которую предприятие использует для достижения уставных целей, ради которых оно создано, и разглашение которой лишит её возможности реализовать данные цели. Утечка этой информации создаёт реальную угрозу экономической безопасности организации.

В Гражданском кодексе Российской Федерации (ст. 128) отмечено, что информация является самостоятельным объектом гражданских прав. Правовой же статус информации, составляющей коммерческую тайну, определён в ст. 139 ГК РФ. В соответствии с её положениями информация составляет служебную или коммерческую тайну в том случае, если информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к её конфиденциальности.

Полный перечень сведений, составляющих коммерческую тайну, невозможно определить, ибо для каждого предприятия они специфичны.

К информации, составляющей коммерческую тайну, относят научно-техническую, финансово-экономическую, учётную и другую информацию, которая имеет коммерческую ценность.

Под режимом коммерческой тайны в соответствии с п. 3, 4 и 5 ст. 3 Закона «О коммерческой тайне» понимают административные, правовые, технические, организационные меры, принимаемые обладателем информации, по охране её конфиденциальности.

В практической деятельности коммерческая тайна всегда приобретает форму коммерческих секретов. Исходя из этого постулата, конструируются понятия «коммерческая тайна и «коммерческий секрет».

Коммерческая тайна — это умышленно скрываемые по коммерческим мотивам экономические интересы и сведения о различных сторонах и сферах управленческой, финансово-хозяйственной, научно-технической и иной деятельности организации, охрана которых обусловлена интересами конкуренции и возможными угрозами экономической безопасности данного предприятия.

Справедливо считается, что коммерческие секреты — форма проявления коммерческой тайн[29].

Такие секреты предстают в виде сведений, оформленных как документы, схемы, изделия, относящиеся к коммерческой тайне; они подлежат всесторонней защите со стороны службы безопасности от хищений, утечки информации и иных неправомерных деяний.

Меры по защите коммерческой тайны должны быть целесообразными и экономически обоснованными. Иначе засекречивание той или иной информации может лишь нанести вред предприятию.

В первую очередь следует защищать информацию, утечка которой может привести организацию сначала к проблемам в деятельности (неплатежи и пр.), а потом и к банкротству. Такую информацию следует вносить в перечень строго конфиденциальной. К ней относят ноу-хау, промышленные образцы, сведения о планах и пер-

[29] URL: http://www.ropnet.ru/info/articles/20.php (дата обращения: 24.10.2011).

спективах развития предприятия, реквизиты клиентов, сроках и суммах полученных ссуд и выданных контрагентам авансов. Нельзя разглашать информацию, которая менее важна, чем вышеуказанная, но её раскрытие тоже может нанести ущерб экономической безопасности. Это адреса топ-менеджеров, работников, номера их домашних и сотовых телефонов, информация о текущих планах деятельности организации, имеющихся конфликтных ситуациях в коллективе, судебных процессах и т.д.[30].

Порядок составления перечня сведений, отнесённых к коммерческой тайне, не определён. Однако, представляется, что при его составлении необходимо исходить из следующего:

- принцип засекречивания информации — баланс интересов экономической выгоды (затрат от засекречивания) и экономической безопасности предприятия;
- посторонние (третьи лица) должны знать как можно меньше об организационной структуре, принципах управления предприятием, его рыночных целях и задачах;
- особый режим должен применяться к охране как самих договоров и контрактов, заключаемых организацией, так и к держанию в секрете самих фактов их заключения.

Сегодня в Российской Федерации процесс правового регулирования коммерческой тайны как формы интеллектуальной собственности ещё несовершенен. Это предполагает применение и других мер защиты:

• проведение административных мероприятий (создание подразделения экономической безопасности, формирование механизма защиты производственных и финансовых секретов, обучение и инст-

[30] Соловьёв Э.Я. Коммерческая тайна и её защита. М.: Дрофа, 2001.

руктаж персонала по защите коммерческой тайны и т.п.);

• формирование корпоративного климата, поддерживающего на предприятии соблюдение морально-этических норм поведения;

• осуществление физических мер защиты (установка замков, запоров, решёток, стальных дверей и пр.);

• установка технических систем охраны (электромеханические, акустические, ёмкостные, радиотехнические и магнитометрические средства и системы);

• применение криптографических методов защиты (преобразование информации с целью сокрытия её логической сущности);

• установление трудовыми контрактами чётких пунктов о недопустимости разглашения коммерческих секретов и форм наказания за такое деяние.

Потенциальными угрозами безопасности информации могут выступать различные форс-мажорные обстоятельства (природные катаклизмы, пожары, наводнения и пр.), политическая нестабильность (страновые риски и пр.), ошибки и неисправности программного обеспечения, включая внедрение в компьютеры предприятия вирусов и троянов, хакерство.

Значительная утечка информации может происходить в процессе проведения переговоров, связанная с неверным пониманием личного имиджа и престижа (бахвальство, болтливость и пр.), неудачным рекламированием своих услуг и продукции и т.д.

5.2 Классификация информации, составляющей коммерческую тайну в бизнесе

Для сопоставления информации по категории «значимость» её классифицируют по следующим параметрам (рисунок 6):

1) концептуальная;
2) организационная;
3) технологическая;
4) параметрическая;
5) эксплуатационная.

Рисунок 6 — Виды информации, составляющие коммерческую тайну

Концептуальная информация выступает в качестве содержания основной концепции конкретной формы бизнеса, связанного со стратегией развития предприятия.

Указанная информация может относиться к сфере промышленного производства, кредитно-финансовой области, НИОКР, торговли и пр.

К данной категории коммерческой тайны могут быть причислены также основные элементы концепции экономической и информационной безопасности, относящиеся к конкретному виду бизнеса (промышленный, торговый и пр.).

Второй вид информации — организационный — отражает специфику внутренней системы управления предприятия, характер деловых взаимоотношений данной предпринимательской структуры с другими юридическими лицами, иные факторы, относящиеся к «организационным», которые приносят конкурентные преимущества или играющие важную роль в процессе эффективного функционирования бизнеса.

Для сферы внутрифирменного управления выделяют следующие виды организационной информации и сопутствующие ей процессы:

а) долгосрочные прогнозы, планы производства и развития предприятия;

б) планы формирования интереса к осуществлению предпринимательской деятельности;

в) создание оригинальных методов управления персоналом, осуществления эффективных продаж;

г) установление порядка рассмотрения предложений потенциальных партнёров по бизнесу.

Для финансово-кредитной сферы — это различные технико-экономические обоснования и планы инвестирования в бизнес-проекты финансовых ресурсов, предварительные договорённости об условиях авансирования затрат контрагентами и кредитования (текущего и долгосрочного) банками.

Для сферы внешнеэкономических связей выделяют следующие виды организационных сведений — это информация о реквизитах подрядчиков, поставщиков и потребителях продукции данного предприятия, осуществляемых переговорах с потенциальными деловыми партнёрами из-за рубежа: оферты, сроки подготовки и заключения договоров, выбор стратегии, тактики и границ полномочий менеджеров, ведущих переговоры и заключающих сделки и т.п.

К вышеозначенной сфере относится информация об уже заключённых контрактах и договорах. Это — номенклатура, объём и количество товаров по взаимным обязательствам, бартерным операциям, сведения об условиях компенсационных договоров, купли-продажи лицензий, патентов, товарных знаков, привлечении капитальных вложений, особых условий фрахтования речных и морских судов, аренда самолётов, раздела сфер влияния и другая информация.

Третий вид — технологическая информация — состоит из сведений о процессах, определяющих качество менеджмента, маркетинга, всего того, что имеет отношение к системе организации и управления предприятием и осуществления производственной, коммерческой, финансовой или иной деятельности, о технологических достижениях, ноу-хау, обеспечивающих предприятию конкурентные преимущества на рынке и заданный уровень безопасности бизнеса.

Научно-техническая и промышленная сферы предоставляют информацию, относящуюся к показу технологических процессов, ре-

жимов и методик, которые устанавливают заданный уровень качества производимой продукции и оказания услуг, эффективное использование сырья, материалов, топлива, энергетических ресурсов. Важна демонстрация перспективных технологий, инновационного оборудования, скорости выполнения основных технологических процессов, причём которые соответствуют требованиям Ростехнадзора (Федеральная служба по экологическому, технологическому и атомному надзору, сайт службы — http://www.gosnadzor.ru) по экологической безопасности.

Параметрическая[31] информация — это такие количественные параметры менеджмента и осуществления финансово-хозяйственной деятельности организации, по которым у неё имеются серьёзные конкурентные преимущества. К данному виду коммерческой тайны в экономической литературе относят сравнительные расчёты эффективности реализации различных вариантов предпринимательских проектов. Для финансовых расчётов — это структура цены на изделия, внутренние прейскуранты и тарифы, данные о себестоимости продукции, калькуляция издержек производства, сведения о представляемых скидках, льготах и т.д.[32].

Этот вид информации применительно к научно-технической продукции предполагает закрытие сведений, касающихся характеристик массы и габаритов товаров, изделий и промышленных образцов, объёмных, временны́х (скорость и пр.) параметров технологических процессов, изготовления и обработки заготовок (проточки, резания, фрезерования и т.д.), а также других характеристик протекания физико-химических и иных процессов.

---

[31] Её в литературе экономического и юридического характера ещё называют «характеристическая информация».

[32] URL: http://library.tuit.uz/skanir_knigi/book/informasionnaya_bezopasnost/ infor_bezopas_1.htm (дата обращения: 27.08.2011).

Для всех видов информации, составляющих коммерческую тайну предприятия (концептуальная, организационная, технологическая, параметрическая и эксплуатационная), характерны специфические подходы к обеспечению её защиты от несанкционированного доступа. Выделение специфики информации облегчает идентификацию коммерческой тайны, позволяет разрабатывать эффективные меры по защите, анализу причин возникновения и устранению последствий утечки информации.

Коммерческая тайна зависит и от действенности применяемых систем маркетинга. Здесь целесообразно контролировать работу по защите информации о результатах маркетинговых исследований, не допускать утечки сведений о намерениях и фактически начавшихся продажах товаров на новых рынках, что позволит оставить конкурентов до поры до времени в неведении о реальных, особенно инновационных, возможностях предприятия.

Коротко охарактеризуем эксплуатационную информацию. Подобная информация состоит из описания процедур (профилактических, ремонтных и др.), необходимых для формирования системы, позволяющей более эффективно эксплуатировать оборудование, машины и механизмы. Важной процедурой является также процесс защиты информации службой экономической безопасности о ликвидации и утилизации устаревшей продукции (это зачастую бывает весьма дорогостоящим мероприятием!), что не позволяет конкурентам повторить их с таким же эффектом без разрешения владельца информации о методиках ликвидации и утилизации.

В са́мом обобщённом виде основные объекты информационной базы обеспечения безопасности бизнеса нами представлены на рисунке 7.

Рисунок 7 — Основные объекты информационной базы обеспечения безопасности бизнеса

5.3 Организация процесса защиты коммерческой тайны

В основе механизма защиты коммерческой тайны лежит уровень этики, культуры и производственной дисциплины персонала. Охрана коммерческой тайны организации осуществляется, как правило, собственными силами. Следует защищать только ту информацию, получение которой может позволить конкурентам быстро и без осо-

бых затрат добиться рыночных преимуществ.

Структура нормативно-правовой базы предприятия, формируемая с целью защиты коммерческой тайны, может включать следующие документы:

• перечень сведений, составляющих для данной предпринимательской структуры коммерческую тайну и подлежащих охране;

• положение о порядке охраны (обеспечения безопасности) коммерческой тайны;

• должностные инструкции сотрудников, допущенных к работе с документами и иными сведениями, составляющими коммерческую тайну;

• памятка (инструкция, наставление, руководство) конкретному работнику о защите коммерческой тайны, составленная с учётом специфики определённого участка работы;

• перечень пунктов, включаемых в трудовой контракт при приёме сотрудника на работу.

В литературе предлагается также иметь совокупность документов, подготавливаемых на случай возможного увольнения сотрудников, имеющих доступ к сведениям, составляющим коммерческую тайну[33].

В Положение о порядке обеспечения (охраны) безопасности коммерческой тайны целесообразно включать следующие разделы: порядок определения грифа, ограничивающего распространение информации («Для служебного пользования», «Секретно» и др.); порядок допуска сотрудников к работе с информацией, составляющей служебную тайну; принципы (основополагающие моменты) организации режима работы с такой информацией.

---

[33] URL: http://library.tuit.uz/skanir_knigi/book/informasionnaya_bezopasnost/ infor_bezopas_1.htm (дата обращения: 23.08.2011).

Положение о порядке обеспечения (охраны) безопасности коммерческой тайны[34] должно содержать виды введённых на предприятии грифов ограничения доступа к информации. При его составлении надо учитывать статью 5 Федерального закона от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». Надо полностью исключить из перечня информацию, к которой не может быть ограничен доступ. Ранее в СССР существовал следующий подход к выделению категорий информации с ограниченным доступом: государственная тайна (грифы «особая важности» и «совершенно секретно»); служебная тайна (гриф «секретно»); информация «Для служебного пользования». Однако со временем ситуация изменилась, поэтому поменялся порядок использования специальных грифов на документах.

На практике применяются понятия: «фирменный секрет», «конфиденциально», «для служебного пользования», «тайна предприятия», «коммерчески ценная информация», «сведения ограниченного распространения», «секретно» и др. Но применение таких понятий не всегда носит нормативный характер. Налицо явные пробелы в российском законодательстве[35].

Мы согласны с мнением юристов, предлагающих организовать на предприятии *конфиденциальное (особое) делопроизводство*. Оно предусматривает:

- назначение должностного лица, ответственного за учёт, хранение и использование конфиденциальных документов;

---

[34] Он может носить и другое название. Например, «Перечень конфиденциальной информации».

[35] В 1993 г. принят Закон РФ от 21.07.1993, № 5485-1 «О государственной тайне». С этого времени гриф «секретно» стал относиться только к сведениям, составляющим государственную тайну. Поэтому гриф «ДСП» не может быть проставлен на документах, содержащих сведения, отнесённые к государственной тайне, так как для них есть свои грифы, соответствующие степени секретности: «Особой важности», «Совершенно секретно» и «Секретно».

- установление порядка подготовки и размножения таких документов;
- отдельную регистрацию документов и формирование дел;
- организацию выдачи и хранения документов;
- проверку наличия документов;
- соответствующее архивное хранение и уничтожение конфиденциальных документов[36].

Ведение конфиденциального делопроизводства, как мы считаем, для определённой категории организаций хоть и затратно, но явно имеет смысл.

Определение необходимости присвоения информации грифа производится тем исполнителем, который подписывает документ, на основании Перечня сведений, составляющих для данной организации коммерческую тайну. Сроки действия грифа могут определяться этим работником в каждом конкретном случае как «бессрочно», «до даты такой-то», «до завершения НИОКР» и другими способами.

На первом листе конфиденциального документа следует указывать его гриф и номер экземпляра. На обратной стороне листа даётся рассылка, в которой фиксируются: количество отпечатанных экземпляров, адреса, в которые предполагается направить экземпляры документа, фамилия лица ответственного за исполнение и отпечатавшего документ, его (их) контактный телефон, а также срок действия грифа.

Допуск сотрудников к работе с конфиденциальной информацией, составляющей коммерческую тайну, осуществляется первыми лицами организации. Руководитель организации (генеральный дирек-

[36] Смольянинова М.В. Могут ли коммерческие организации использовать гриф «ДСП»? Институт проблем предпринимательства: [сайт]. URL: http://www.ippnou.ru/article.php?idarticle=007218 (дата обращения: 19.10.2011).

тор, управляющий и пр.) может оставить такую работу только за собой. При этом издаётся соответствующий приказ. Как мы уже отмечали выше, для принятия решения о допуске сотрудника к конфиденциальной информации, необходимо предварительное изучение работника в течение испытательного срока.

К работе с коммерческой тайной допускаются сотрудники, прошедшие испытательный срок, только после изучения ими требований соответствующих документов по защите тайн организации, сдачи зачётов на соответствие знаний изложенных в них требований, оформления ими в письменном виде обязательств по её неразглашению. Ряд предприятий после окончания испытательного срока просят работника заполнить специальный документ «Оценочный лист сотрудника прошедшего испытательный срок», где есть специальный пункт «Я ознакомился с перечнем сведений, составляющих коммерческую тайну»[37]. Ответственность за неразглашение тайны фиксируется трудовым контрактом.

Последующая работа должна строиться так, чтобы каждый работник имел доступ только к той информации, которая необходима ему для выполнения прямых служебных обязанностей.

Сотрудник, допущенный к работе к информации, составляющей коммерческую тайну, обязан:

- строго хранить коммерческую тайну, ставшую им известной в связи с выполнением служебных обязанностей или полученной случайно;
- принимать меры по пресечению девиантных поступков третьих лиц, которые могут привести к утечке служебной информации;
- немедленно сообщать первым лицам предприятия о фактах

[37] URL: http://www.hr-portal.ru/tool/otsenochnyi-list-sotrudnika-proshedshego-ispytatelnyi-srok (обращения: 18.10.2011).

несанкционированного доступа к охраняемой информации либо о создании предпосылок к этому;

• не использовать производственные, финансовые и иные секреты организации в личных целях;

• препятствовать предложениям ознакомиться с теми документами, к которым у него нет доступа в рамках выполнения определённых должностных обязанностей;

• при подготовке документов, содержащие охраняемые сведения, принимать меры к ограничению их количества, что будет облегчать конфиденциальный документооборот;

• чётко соблюдать порядок учёта и хранения информационных носителей (печатные документы, магнитные и оптические носители, образцы товаров и т.д.).

В памятку о защите коммерческой тайны, выдаваемой сотруднику, следует включать следующее:

• основные обязанности и права сотрудника, обусловленные необходимостью защиты коммерческой тайны;

• стержневые моменты, определяющие режим секретности проводимых сотрудником работ;

• перечень основных документов организации, регламентирующих порядок охраны коммерческой тайны.

Особо важным направлением в работе с персоналом предприятия является проведение воспитательной работы. Это может значительно снизить масштабы промышленного шпионажа, который приобрёл чудовищные масштабы. Так, ежегодный ущерб, который немецкие предприятия несут от промышленного шпионажа, составляет, по меньшей мере, 20 миллиардов евро, сообщает Deutschlandradio со ссылкой на главу Комитета по экономической безопасности Бертоль-

да Штоппелькампа (Berthold Stoppelkamp). При этом точное число шпионских атак, которым подвергаются немецкие предприятия, остаётся неизвестным. По данным статистики, из ста случаев промышленного шпионажа становится известно лишь о шести. «В большинстве случаев важные данные пропадают совершенно незаметно», — отмечает Б. Штоппелькамп[38].

Специалисты дают следующие рекомендации с целью противодействия промышленному шпионажу:

• разрабатывать специальные программы для пропаганды обеспечения режима секретности, используя для этого любую даже самую мелкую возможность;

• создать эффективную систему стимулирования и материально стимулировать заинтересованность работников по соблюдению режима секретности;

• проводить периодическое обучение и переобучение персонала, чтобы каждый сотрудник чётко знал объёмы охраняемой информации, за безопасность которой он несёт личную ответственность, понимал характер и ценность сведений, с которыми он работает;

• обучение передовым правилам и методам хранения и защиты секретных данных.

Все правила, процедуры, действия по защите конфиденциальной информации должны сопровождаться разъяснением их сути, их разумности, эффективности и целесообразности. Это связано с психологией человека — он привыкает к работе с коммерческой тайной и начинает зачастую ненамеренно делать ошибки.

Порядок проведения закрытых совещаний и переговоров. Разрешение на проведение совещаний и переговоров по вопросам, со-

[38] http://lenta.ru/news/2011/07/08/spionage (дата обращения:20.10.2011).

ставляющим коммерческую тайну, имеют право давать руководитель предприятия или, как мы отметили выше, специально уполномоченные им лица, о чём уведомляется начальник службы [экономической] безопасности.

Ответственный за проведение мероприятия (им может быть сотрудник службы безопасности) составляет список потенциальных участников совещаний и переговоров с указанием фамилий, имён и отчеств и занимаемой должности на предприятии или вне его.

Председательствующий — обычно это руководитель организации, где проводится совещание — обязан перед началом процедуры напомнить участникам встречи о необходимости сохранности коммерческой тайны и конкретно уточнить, какие сведения являются охраняемыми, с фиксацией напоминания в протоколе совещания. Отдельные предприятия принимают от участников письменные обязательства о неразглашении коммерческой тайны. Мы считаем такой порядок чрезмерным, хотя понимаем, что определённое психологическое давление на участников совещания это оказывает.

Процедуры переговоров и совещаний проводятся в специально отведённых местах — изолированных помещениях, — исключающих возможность незаконного применения визуально-оптических, акустических и других технических специальных средств шпионажа. До начала процедуры эти помещения ещё раз проверяются службой безопасности. После этого посторонние лица туда уже не допускаются.

На каждом совещании ведётся протокол, которым впоследствии можно использовать для наказания лиц, виновных в нарушении коммерческой безопасности, или для передачи дел в суд.

В основе организации режима работы с документами, которые содержат информацию, составляющую коммерческую тайну, лежат

следующие принципы:

• все входящие и исходящие документы, содержащие охраняемые сведения, подлежат обязательной регистрации в порядке, установленном для данной организации;

• все копии документов, полученных при их размножении, подлежат строгому учёту;

• рассылка грифованных документов осуществляется только на основании разрешений первых лиц организации;

• грифованные документы после исполнения группируются в особые номенклатурные дела и хранятся в специально отведённых местах;

• при использовании технических средств связи передача сведений, составляющих коммерческую тайну, допускается только по закрытым каналам связи.

Чтобы работа с документами, содержащими коммерческую тайну, была более эффективной, следует соблюдать определённые правила. В этих целях следует обязательно:

• разработать инструкцию (памятку, положение) по работе с грифованными документами;

• назначить ответственных лиц для контроля над конфиденциальным делопроизводством;

• осуществлять строгий контроль за допуском работников к грифованным документам.

Наиболее значимые грифованные документы хранятся в сейфе, менее важные — в специальном металлическом контейнере. Они опечатываются сразу после закрытия сейфа или контейнера.

Грифованные документы, которые на законном основании могут потребовать для работы компетентные органы, следует держать от-

дельно от остальных конфиденциальных документов.

Организация должна применять все меры, чтобы ограничить количество экземпляров конфиденциальных документов. Это связано с тем, что чем больше секретной информации в них имеется, тем больше потребуется затрат для её защиты.

Копирование документов является одним из способов получения сведений, составляющих коммерческую тайну, поэтому множительная техника должна находиться под строгим контролем службы безопасности. Количество копий подлежит строгому учёту, а их уничтожение — контролю. Следует использовать только то копировальное оборудование, которое снабжено счётчиками и ключами, запускающими копировальные машины в действие. Такой копировальный аппарат должны иметь первые лица, чтобы наиболее ценные документы копировать самим.

Сегодня владельцы сотовых телефонов имеют техническую возможность мгновенно сфотографировать любой документ и переслать его по Интернету. Поэтому в процессе копирования работникам следует запретить пользоваться телефонами, имеющими фотоаппарат.

Для работы с грифованными документами на предприятии должны быть оборудованы спецпомещения с надёжной свето- и звукоизоляцией. Служба безопасности должна контролировать, чтобы в указанные помещения не допускались посторонние лица и сотрудники, не имеющие допуска на работу с конфиденциальной информацией.

Черновики грифованных документов, которые в первоначальном виде готовятся от руки, должны писаться в тетрадях с пронумерованными листами. После подготовки документов в чистовом варианте, черновики хранятся в установленном порядке либо своевременно уничтожаются.

Анализ практики показывает, что вероятность утечки конфиденциальной информации из документов особенно велика в процессе их пересылки[39]. Поэтому если нет возможности воспользоваться услугами фельдегерьской связи, то доставку грифованных документов следует организовать с привлечением сотрудников собственной службы безопасности.

Мероприятия, которые следует проводить в процессе защиты документации, представлены в таблице 2.

Таблица 2 — Мероприятия по защите документации от несанкционированного доступа

Наименование мероприятий		
Организационные	Технические	Специальные
Работа с сотрудниками предприятия	Монтаж сигнализаций и проведение контроля за её функционированием	Применение средств защиты от несанкционированного доступа и копирования документов и (или) отправке их с использованием факсов, электронной почты, сотовых телефонов и иными техническими средствами
Введение и осуществление режима контроля для защиты документов	Использование специальных средств, запирающих устройств и других механизмов защиты	Применение устройств скрытого фиксирования и слежения для выявления незаконного доступа к секретным документам
Определение форм, содержания, уровня важности документов и способов их охраны	Использование специального офисного оборудования для уничтожения секретных документов	Защита от промышленного шпионажа
Классификация и грифование документов, даты снятия грифа	Обеспечение сотрудников, работающих с секретными документами, сейфами и специальными контейнерами для хранения грифованных документов	Проведение служебного расследования по фактам утраты документов, содержащих коммерческую тайну

[39] URL: http://bre.ru/security/10345.html (дата обращения: 20.10.2011).

Система организации архивного хранения документов, представляющих коммерческую тайну, заключается в следующем. Документы текущего делопроизводства по истечении календарного года могут быть переданы на хранение в архив предприятия. Оформление и передача документов, представляющих коммерческую тайну, должна осуществляться по инструкции, которая регламентирует организацию архивного хранения таких документов.

Ярочкин В.И. и Бузанова Я.В. предлагают в Инструкции по организации хранения дел отражать основные технические операции, в том числе[40]:

- приём документов, содержащих коммерческую тайну в архив;
- составление и оформление сводной описи дел с грифом «Коммерческая тайна»;
- составление и оформление сводной описи сотрудников допущенных к сведениям, составляющим коммерческую тайну;
- учёт документов, содержащих конфиденциальную информацию.

Приняв во внимание указанные требования, руководитель предприятия даёт указание на их основе разработать должностные инструкции для сотрудников, отвечающих за режим сохранения коммерческой тайны, а также подготовить памятку сотрудникам организации в части сохранения соответствующих документов.

Персонал, отвечающий за подготовку, сохранность и своевременное уничтожение грифованных документов, должен быть в максимальной степени ограждён от соблазна незаконной передачи секретной информации сторонним лицам. Лучше всего это делать самым проверенным способом, применяя материальное стимулирование.

---

[40] Ярочкин В.И. и Бузанова Я.В. Основы безопасности бизнеса и предпринимательства. М., 2005. С. 23.

6 Организация охраны объектов бизнеса

6.1 Интегрированный подход к созданию комплексной системы безопасности бизнеса

Эффективная организация охраны объектов, обеспечивающая надёжную защиту от внешних и внутренних посягательств, невозможна без применения системного подхода к созданию механизмов, обеспечивающих безопасность бизнеса и охрану коммерческой тайны на предприятии.

Реальный контроль за всеми процессами, регулирующими деятельность организации, возможен лишь на базе создания мощной, глубоко интегрированной системы технических средств и программных продуктов.

Эта система (комплекс технических средств и программных продуктов) должна решать следующие основные задачи:

- осуществлять проведение коммерческого учёта и контроля;
- контролировать аварийную и пожарную обстановку;
- осуществлять охранные функции на предприятии;
- контролировать доступ сотрудников и автотранспорта на предприятие;
- осуществлять телевизионный контроль за обстановкой на предприятии;
- противодействовать утечке конфиденциальной информации, хищению и утере грифованных документов.

Эти и ряд других задач вытекают из самой сущности потенциальных угроз, возникающих при осуществлении предпринимательской деятельности, о чём мы уже выше говорили. Это угрозы:

— направленные против жизни и здоровья сотрудников;

— материальным ценностям, принадлежащим предприятию;

— имеющие экономико-правовой характер.

Источников угроз великое множество. Однако это всегда — индивиды, экономическое окружение, внешняя и внутренняя среда предприятия. Поэтому высокоэффективная, надёжная и современная система безопасности должна включать в себя ряд подсистем, к которым относятся:

- охранно-пожарная сигнализация;
- телевизионная система охраны и видеонаблюдения;
- тревожная сигнализация;
- оборудование, обеспечивающее контроль над управлением доступа к режимным объектам;
- оперативные средства связи;
- надёжное электроснабжение и системы подключения аварийного освещения.

При создании системы охраны складской инфраструктуры необходимо провести подготовительный комплекс мероприятий, который заключается в:

- создании периметрального ограждения, не позволяющего деликвенту или обычному гражданину-нарушителю режима, беспрепятственно проникать на охраняемый объект;
- установке периметральной сигнализации, которая в реальном масштабе времени позволит службе охраны принять адекватные меры;
- установке охранного освещения, дающего возможность вести наблюдение за объектом в ночное время суток;
- монтаже охранно-пожарной сигнализации, предупреждающей об огнеопасной обстановке на объекте;
- подключении системы видеонаблюдения, записывающей со-

бытия на объекте на современные электронные носители;

• создании системы контроля доступа, позволяющей документировать продвижение работников и третьих лиц по территории предприятия;

• блокировании входов, выходов, окон, дверей, вентиляционных шахт и люков инженерно-механическими средствами защиты (решётки на окнах, железные двери, въездные ворота, укреплённые шлагбаумы и т.д.);

• хранении ценностей в сейфах, металлических ящиках в разных, то есть изолированных друг от друга складских помещениях.

Перечень этих требований прост, но их выполнение позволяет в превентивном порядке обеспечить эффективную охрану имущества организации. В дальнейшем для крупных предприятий и организаций, применяющих уникальное оборудование для производства товаров (естественно, при наличии финансовых возможностей), целесообразно формировать из отдельных вышеперечисленных элементов непосредственно интегрированную систему безопасности бизнеса. Внедрение интегрированной системы безопасности необходимо формулировать как одну их основных задач стратегического менеджмента организации.

6.2 Тактика охраны стационарных объектов предпринимательства

Справедливо считается, что процесс обеспечения безопасности стационарных объектов предпринимательства состоит из проведения комплекса охранных мер превентивного свойства. Поэтому эффективность деятельности охраны заключается в недопущении не только фактов проникновения деликвента на охраняемый объект, но и пресе-

чения незаконных посягательств на имущество предприятия на более ранних стадиях.

Основными элементами тактики охраны стационарного объекта являются:

• выбранный руководителем режим охраны предприятия;

• комплекс используемых службой безопасности тактических приёмов охраны;

• уровень профессиональной подготовки работников службы безопасности.

На выбор приёмов и средств охраны предприятия влияет целый набор факторов. Основные из них:

1) Применение деликвентами наиболее распространённых способов противоправных посягательств на охраняемый объект.

2) Характеристика и наиболее уязвимые места в инженерно-технической укреплённости объекта.

3) Наличие средств охранно-пожарной сигнализации на охраняемом объекте.

4) Специфика условий местности, её рельефа, на которой расположен охраняемый объект.

5) Временно́й режим и характер работы (ночные смены, непрерывный цикл производства и пр.) сотрудников предприятия.

6) Действующий режим охраны (имеющиеся силы, средства и т.д.).

7) Наличие экипировки, вооружения, автомототранспорта, средств связи и специальных средств[41].

Наличие соответствующей экипировки и вооружения даёт возможность службе охраны демонстрировать свою силу и решимость

[41] См.: URL: http://e-lib.info/book.php?id=112100022&p=12 (дата обращения: 20.10.2011).

защищать имущество собственника и безопасность персонала.

В зависимости от характера производства и ведения бизнеса руководитель предприятия устанавливает режим охраны объектов. По времени он может быть круглосуточным, частичным (в определённые часы), выборочным, а также носить характер простого или усиленного. На большинстве охраняемых объектах работники службы безопасности дежурят круглосуточно. В дневное время в их ведении контрольно-пропускной режим, в ночное время они осуществляют закрытую охрану объекта с целью своевременного обнаружения признаков готовящегося девиантного поведения и грамотной нейтрализации его всеми имеющимися силами и средствами.

Службой охраны применяются приёмы контроля и осмотра охраняемого объекта, которые носят типовой характер. Это:

1) Фронтальный осмотр объекта, когда работники службы охраны движутся в одном направлении до границы объекта, а затем перемещаются в обратную сторону.

2) Движение работников службы охраны навстречу друг другу. После сближения охранники сразу же расходятся в противоположном направлении.

3) Осуществление движения охранников по спирали от центра объекта к его границам.

4) Последовательный осмотр объекта по стохастической (произвольной, случайной) траектории, что запутывает потенциальных деликвентов.

5) Проведение выборочного осмотра объекта в зависимости от значимости охраняемого имущества и наличии на нём персонала предприятия.

6) Движение по объекту с постоянно меняющимся маршрутом.

7) Движение по маршруту охраняемого объекта с остановками, осмотром имущества из засады или специально оборудованного для таких целей поста.

Выбор того или иного приёма контроля и осмотра охраняемого объекта зависит от специфики объекта (местонахождение и пр.), вида охраняемого имущества и профессиональной подготовки частных охранников.

Охрана объекта может организовываться с применением сторожевых собак. Служебные собаки являются важным специальным средством в повышении надёжности охраны любого объекта. К охране объектов наиболее пригодны кавказская, среднеазиатская, южнорусская и немецкая (восточноевропейская) овчарки, чёрный терьер, московская сторожевая.

Различают несколько категорий служебных собак, использующихся в целях охраны объекта:

- патрульно-розыскные — предназначены для использования в патруле, службе на контрольно-пропускном пункте, поиске лиц, незаконно проникших на объект, охране задержанных за противоправные действия лиц;
- минно-розыскные — предназначены для розыска взрывчатых веществ, проверке и разминирования охраняемых объектов;
- караульно-сторожевые — предназначены для усиления охраны объектов.

В зависимости от специфики объекта охраны и способа применения сторожевых собак существуют следующие виды постов караульных собак:

- пост свободного окарауливания;
- блокпост;

• пост глухой привязи.

При организации охраны относительно небольших объектов (квартира, офис, служебное помещение) целесообразно использовать собак, являющихся собственностью кинолога (инструктора). Он держит собаку у себя дома, ухаживает, самостоятельно тренирует и воспитывает её. Поэтому отпадает необходимость сооружать специальные помещения для собак и содержать обслуживающих их штат работников.

Правильное использование служебных собак повышает надёжность охраны объектов, облегчает розыск и задержание правонарушителей, пытающихся незаконно проникнуть на территорию охраняемого объекта, и является сдерживающим, устрашающим фактором для любого деликвента.

6.3 Требования, предъявляемые к контрольно-пропускным пунктам охраняемого объекта

Контрольно-пропускной режим на предприятии обязательно должен соответствовать законодательству и нормативным актам Российской Федерации, а также его уставу.

В любом случае основной целью введения контрольно-пропускного режима является защита от посягательств на собственность предпринимателя.

Основные задачи указанного режима:

• санкционированный внутренними положениями проход на охраняемую территорию сотрудников и посетителей, ввоз/вывоз товаров, продукции и иных материальных ценностей;

• предотвращение несанкционированного проникновения посторонних лиц и транспортных средств на территорию охраняемого

предприятия.

Важно сделать так, чтобы требования контрольно-пропускного режима были доведены до каждого работника предприятия.

Предприятие, организуя контрольно-пропускной режим, должно оборудовать контрольно-пропускные пункты (КПП). Для эффективной работы КПП и решения всех вопросов, связанные с пропускным режимом, следует применять инструкцию, которая определяет:

• лиц, ответственных за соблюдение режима, их права, обязанности и ответственность за его несоблюдение;

• процедуру, регламентирующую проход на охраняемую территорию предприятия, а также порядок пропуска на территорию автотранспорта, принадлежащего хозяйствующему субъекту и сторонним организациям;

• порядок, предусматривающий правильность вывоза материальных ценностей с охраняемой территории;

• правила оформления документации на вывоз/вынос материальных ценностей;

• виды пропусков (постоянные, временные, разовые и др.), их описание, порядок выдачи и замены при утрате пропусков сотрудниками предприятия;

• порядок, регламентирующий способы хранения пропусков и печатей.

Современные контрольно-пропускные пункты должен обеспечивать санкционированный проход работников предприятия и посетителей в помещение с применением специального оборудования (автоматизированных контрольно-пропускных кабин, турникетов и пр.). Вид и число такого оборудования должны выбираться исходя из норматива пропуска всего персонала в период наибольшей загрузки КПП

(начало и конец рабочего дня, пересмены).

Оформление пропусков для прохода в помещение должно организовываться непосредственно в бюро пропусков или на небольших предприятиях в отделе кадров. По действующему законодательству отдельные категории лиц пользуются правом прохода на объект без пропуска при предъявлении служебного удостоверения (работники прокуратуры, полиции, инспекторы труда, котлонадзора, энергонадзора по территориальности, работники санитарно-эпидемиологических станций и т.п.).

КПП обычно оборудуются либо в самом здании, либо, при наличии внешнего ограждения, в специально предназначенных для этой цели помещениях — так называемых «проходных», расположенных в разрывах контура ограждения территории охраняемого объекта.

КПП, размещённое в здании, должно быть организовано только на основном входе. Дополнительные входы, наличие которых определяется требованиями СНиП (строительные нормы и правила) и технологическими особенностями конкретного здания, должны находиться в закрытом виде, под контролем объектовой сигнализации и видеонаблюдением. Следует предусмотреть быстрое вскрытие таких входов в случае пожара или иных стихийных бедствий.

При размещении внутри здания КПП следует планировать его расположение на значительном удалении от входных дверей главного входа, чтобы иметь естественное свободное пространство перед КПП, что облегчает наблюдение за обстановкой.

В холле перед КПП целесообразно разместить камеру хранения, используемую в течение всего рабочего дня для хранения личных вещей сотрудников и посетителей охраняемого объекта. По возможности здесь же размещается раздевалка.

Эффективность деятельности контрольно-пропускного пункта зависит от обеспечения им:

• необходимых условий (включая бытовых) для охранников, что важно для качественного выполнения ими должностных обязанностей и обеспечения их безопасности;

• необходимой (скорость и пр.) пропускной способности;

• регламентированного порядка прохода людей на территорию предприятия (объекта);

• возможности быстрого задержания нарушителей режима подачей сигнала тревоги;

• возможности маневрирования силами и средствами охраны вне зависимости от масштабности потоков входа/выхода людей.

К оборудованию КПП относится:

• система контроля и управления доступом в помещение;

• объектовые средства обнаружения (датчики положения дверей и пр.);

• телекоммуникационное оборудование, предназначенное для обнаружения и наблюдения;

• оперативные средства связи и тревожной сигнализации;

• специальные средства технического досмотра, к которым относятся рамки, металлоискатели и т.д.

Рядом с КПП должно быть предусмотрено специальное помещение для несения круглосуточного дежурства охранниками и их отдыха в соответствии с принятым на предприятии режимом.

Размещённые на посту охранника КПП образцы пропусков и другой служебной документации (приказы и т.п.) должны быть недоступны для просмотра посторонними лицами.

В последние годы всё большее распространение получили элек-

тронные пропуска. Контроль за их применением требует от службы безопасности (охраны) особых навыков.

Двери помещения КПП должны быть оборудованы запорами фиксации в ночное время суток, блокироваться концевыми выключателями, а за дверями необходимо устанавливать кнопку звонка.

КПП оборудуется современными средствами для осуществления проезда автомобильного и железнодорожного транспорта. Это:

- электродвигатели, привод ворот;
- магнитные пускатели электродвигателей;
- электрооборудование светофоров;
- конечные выключатели автоматического отключения электродвигателей при полностью открытых и закрытых ворот или их створках.

Предприятие, формируя контрольно-пропускной пункт, обычно поручает это профессионалам из соответствующих фирм. При этом на этапе разработки системы режима обычно используется комплексный подход, который позволяет предотвратить лишние финансовые затраты, сократить время в случае последующего создания интегрированной системы безопасности бизнеса.

6.4 Требования, предъявляемые к средствам и системам санкционированного доступа

Средства и системы санкционированного доступа должны обеспечивать управление доступом и контроль проходов на территорию охраняемых объектов и входов в обособленные помещения, что предусматривает российский ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие техниче-

ские требования. Методы испытаний»[42].

Все средства и системы санкционированного доступа должны выстраиваться на общем принципе: доступ без потерь времени, но с обеспечением эффективного контроля.

В состав средств и систем санкционированного доступа должны входить[43]:

• пропуска, включая электронные (в последнее время стали получать распространение пропуска, встроенные в телефоны сотовой связи, а также биометрические пропуска), выдаваемые сотрудникам предприятия;

• считыватели — устройства для снятия информации с пропусков;

• контро́ллеры — устройства обработки информации, которая поступает со считывателей, её анализа и принятия решения о разрешении на санкционированный проход;

• исполнительные (преграждающие) устройства (электрозапорные устройства, турникеты, электроприводы ворот и пр.).

На КПП в зависимости от численности персонала должны устанавливаться несколько электронно-механических турникетов со считывателями, объединённые в локальную компьютерную сеть системы контроля управления доступом (СКУД).

Турникеты должны оснащаться средствами автоматического блокирования по истечении времени прохода, запрограммированного для одного обладателя пропуска (персонального идентификатора): внешним управлением через пульт на рабочем месте сотрудника безопасности и блокировкой с помощью зубчатого тормоза.

---

[42] Дата введения ГОСТа – 01.01.2000.

43 URL: http://www.standards.narod.ru/gosts/other/51241-98.htm (дата обращения: 29.08.2011).

В СКУД должны использоваться турникеты со считывателями, обеспечивающими выполнение следующих функций:

• доступ только одного лица по одному идентификатору;

• защиту от прохода двух или более человек по одному пропуску (невозможность повторного прохода по одному идентификатору, двойного прохода по факту одной регистрации идентификатора);

• подачу сигнала тревоги при попытке несанкционированного прохода через турникеты.

СКУД должна обеспечивать:

• регистрацию, документирование и отображение, а при необходимости запись всех событий;

• возможность сопряжения со средствами охранной сигнализации и телекоммуникационными средствами наблюдения (ТВСН);

• автоматическое включение телекамеры для обзора «контрольной площадки доступа» в момент прохода человека и в момент регистрации идентификатора при подготовке к выходу;

• возможность разблокировки по команде с постов охраны любых электронных запирающих устройств, при возникновении необходимости срочной эвакуации работающего персонала.

Системы санкционированного доступа (ССД) должны обеспечивать:

• предотвращение несанкционированного проникновения на охраняемый объект лиц, не имеющих идентификационной пластиковой карты или другого специального устройства;

• санкционированный проход персонала на территорию охраняемого предприятия;

• дистанционное управление и осуществление контрольных функций за электромагнитными запирающими устройствами;

• возможность разблокировки любых электронных запирающих устройств, установленных на входах, непосредственно с постов охраны.

В качестве систем санкционированного доступа (ССД) могут применяться механизмы ограничения доступа (считыватели идентификаторов автономного типа, электронные запирающие устройства, кодированные запирающие устройства и пр.).

Системы ограничения доступа автономного типа должны обеспечивать санкционированный проход в режимные помещения ограниченного круга лиц посредством автоматической идентификации этих лиц при входе. Проход в дверь авторизированных пользователей в предусмотренное для каждого время программируется непосредственно со считывателя.

При необходимости вызова персонала охраняемого объекта прибывающими лицами во внешнем ограждении устанавливается средство вызывной сигнализации (кнопка звонка, телефон).

С учётом специфики функционирования объектов, связанной с периодическим пребыванием обслуживающего персонала, для контроля прохода в помещение могут устанавливаться видеофоны.

Кодированные запирающиеся устройства (КЗУ) должны обеспечивать предотвращение проникновения на охраняемый объект посторонних граждан, которые не знают цифрового кода.

КЗУ должны обеспечивать:

• разблокировку электромеханических замков при нажатии правильного цифрового кода;

• возможность использования сменных кодов;

• выдачу тревожных сообщений при попытках несанкционированного прохода или неправильно набранного кода.

В состав КЗУ могут входить блоки набора и считывания кода,

устройства программирования доступа, электромагнитные замковые устройства и другие устройства подачи сигналов «тревога» от систем санкционированного доступа (ССД) и кодированных запирающих устройств. (КЗУ) должны подключаться к общей системе охраны (ОСО).

В последние годы стали активно применяться биометрические системы контроля (идентификации) доступа. Такие системы имеют ряд преимуществ:

1)Безопасность**.** Самое важное свойство биометрии — это возможность идентифицировать именно личность человека. Биометрические идентификаторы нельзя похитить или передать третьему лицу.

2) Удобство**.** Определённая часть сотрудников забывает или теряет карточки для входа через КПП на работу, что приводит к потере времени службы охраны на организацию доступа. Биометрические идентификаторы лишены такого недостатка.

3) Имидж**.** Внедрение биометрических технологий придаёт компании инновационный имидж.

4) Выгода. Совокупная стоимость современной биометрической системы ниже, чем стоимость системы с традиционными идентификаторами, то есть польза от внедрения новой системы перекрывает стоимость внедрения.

6.5 Требования, предъявляемые к охранному освещению объекта

К функции охранного освещения относится обеспечение дополнительного освещения периметра территории охраняемого объекта и зон безопасности в ночное и тёмное время суток. Устанавливая охранное освещение, следует ориентироваться на руководящий норма-

тивный документ «Системы и комплексы охранной сигнализации. Элементы технической укреплённости объектов. Нормы проектирования» (РД 78.143-92).

Охранное освещение обычно делят на самостоятельные участки периметра, отдельно от наружного освещения. Охранное освещение целесообразно монтировать, чтобы оно работало в комплексе с охранной сигнализацией объекта.

Включение охранного освещения должно осуществляться следующими способами:

- вручную, чтобы иметь возможность просмотра периметра по участкам или на всём протяжении для проверки работы электроосвещения и проверки охраняемых зон в ночное и тёмное время суток;
- автоматически, как только срабатывает охранная сигнализация на участке охраняемого периметра.

Для охраняемых объектов, имеющих внешние ограждения, указанное освещение должно осуществляться специальными светильниками или прожекторами, устанавливаемыми с внутренней стороны в пределах запретной зоны на опорах или на стойках ограждения.

Для объектов, которые не имеют внешних ограждений, светильники охранного освещения следует устанавливать над входом в техническое здание.

Светильники охранного освещения должны устанавливаться на кронштейнах на ограждении периметра, на высоте не менее 2,5 метров от земли. Если охранное освещение осуществляется прожекторами, то опоры под прожекторы следует устанавливать непосредственно на линии ограждения; при этом лучи прожектора должны быть направлены вдоль ограждения в одну сторону.

Светомаскировка объекта обеспечивается принудительным от-

ключением охранного освещения с пульта приёмно-контрольной аппаратуры по согласованию со службой безопасности предприятия.

По решению первых лиц организации допускается использование охранного освещения во время пребывания обслуживающего персонала на объектах в качестве обычного технологического наружного освещения.

В вечернее и ночное время должно предусматриваться охранное освещение по всему периметру территории объекта, коридоров и холлов внутри зданий, а также помещения контрольно-пропускного пункта. На случай прекращения поступления электроэнергии от основного источника, электропитание обеспечивается от резервной энергетической установки.

Помещение КПП должно дополнительно оборудоваться аварийным освещением, которое переходит на аварийный режим и обратно автоматически.

Источники света в помещении КПП должны располагаться таким образом, чтобы исключить возможность ослепления службы охраны, персонала предприятия, проходящего через контрольно-пропускной пункт.

Охранное освещение должно быть экономичным, надёжным, безопасным, простым и удобным в использовании как в процессе повседневной эксплуатации, так и проведении профилактических и ремонтных работ.

6.6 Требования, предъявляемые к обеспечению противопожарной безопасности

Пожар, возможно, ещё более опасен по экономическим последствиям для предприятия, чем хищения. Меры пожарной безопасности

организуются и осуществляются силами и средствами организации на основе требований отраслевых нормативных актов, правил пожарной безопасности в РФ. Допустимо устанавливать лишь то оборудование пожарной сигнализации, которое сертифицировано и разрешено к применению на территории Российской Федерации соответствующими федеральными службами.

Сигнализацией пожарной безопасности оборудуются все помещения вне зависимости от их производственного или бытового назначения. Дымовые извещатели устанавливаются во всех коридорах и служебных помещениях. Помещения общего назначения оборудуются дымовыми оптико-электронными извещателями. Помещения, в которых находится большое количество электронного и электрического оборудования, оснащаются ионизационными извещателями, обнаруживающими практически полный спектр дымов.

В организациях, где даже малейший пожар может принести огромные убытки, устанавливают аспирационные дымовые пожарные извещатели. Но обходятся они предприятию недёшево.

Тепловые извещатели устанавливают в местах, оборудованных для курения. Помещения общего назначения должны быть оборудованы тепловыми пороговыми извещателями. В помещениях, в которых разовое повышение температуры имеет низкую степень вероятности, должны применяться дифференцированные тепловые извещатели.

На лестничных площадках основных и запасных входов (выходов) на каждом этаже устанавливаются ручные извещатели в виде небольших пультов с кнопкой. Обычно они защищены стеклом, которое при пожарной тревоге легко разбить подручными средствами.

Аппаратура контроля работоспособности (или пульт техниче-

ского контроля) средств пожарной сигнализации устанавливается в помещении службы безопасности (или аналогичной охранной структуры). Современные системы пожарной сигнализации должны иметь сопряжение с сервером автоматизированной системы безопасности с выводом информации на центральный пост службы безопасности.

Указанные требования предъявляются к объектовым техническим средствам обнаружения, к средствам тревожно-вызывной сигнализации, к средствам связи, к приёмно-контрольной аппаратуре, к системе электропитания, к системе кабелепровода, к средствам технического обслуживания, а также к специальным техническим средствам.

6.7 Обнаружение взрывчатых веществ и взрывных устройств

Криминалитет использует взрывные устройства как средство устрашения, так и устранения конкретных индивидуумов. Современные взрывчатые устройства стали мощнее и разнообразнее, они стали преимущественно дистанционными и позволяют деликвентам находиться на отдалении от предполагаемого места подрыва.

Мероприятия, направленные на обеспечение безопасности от взрывных устройств, представляет собой комплексную программу превентивных мероприятий и чрезвычайных процедур. Превентивные меры направлены на ограничение наиболее уязвимых секторов и снижение ущерба от возможного подрыва. Такие меры помогают выявить возможности взрывного устройства, до того как оно будет приведено в действие. Они также создают возможность прогнозировать правильные действия в случае обнаружения взрывного устройства, что, безусловно, может минимизировать негативные последствия взрыва или даже полностью исключить его угрозу.

Главный принцип, правило, выполнение которого позволяет предупредить девиантное действие, связанное с закладкой взрывного устройства, — минимизация дистанции несанкционированного проникновения. Для реализации данной задачи применяется комплекс мер по установлению ограждения периметра, установке освещения, сигнальных датчиков, осуществлению регулярного патрулирования объекта охраны.

Автотранспорт, въезжающий на территорию организации, обязательно должен проверяться на наличие в кузове и кабине взрывчатых веществ и оружия. По возможности целесообразно запланировать парковку автомобилей на удалении, а пассажиров доставлять к месту назначения на транспорте, принадлежащем данному предприятию. Правильно поступают руководители организаций, которые запрещают своему персоналу пользоваться стоянкой или гаражом фирмы, доплачивая им за парковки на коммерческих стоянках.

Профессионалы охранной деятельности предлагают иметь на предприятии два рубежа в виде контрольно-пропускных пунктов, между которыми размещаются устройства, которые могут при необходимости ограничить или заблокировать движение автотранспорта.

Целесообразно защищать оконные проёмы особо важных кабинетов посредством установки пуленепробиваемых и тонированных стёкол.

Санитарное состояние территории имеет важное значение, поскольку если она захламлена, то на ней можно легко спрятать подрывное устройство.

Регулярной проверке подлежат вентиляционные шахты, водосточные и дождевые трубы, урны и другие места, где возможна закладка взрывного устройства.

Отдельно от входа необходимо оборудовать шкафы с ячейками, в которые посетители должны помещать свой ручной багаж, а также по возможности раздевалку, ибо пальто или шуба могут служить идеальным местом вноса в служебные помещения взрывных устройств.

Поскольку есть технологическая возможность присылать взрывные устройства во входящей корреспонденции, целесообразно уделять этому серьёзное внимание. Следует оценивать такую корреспонденцию по наличию ряда подозрительных признаков:

- нет обратного адреса;
- на конверте указан незнакомый адрес;
- адреса нанесены при помощи наклеенных букв из газет или журналов;
- конверт, бандероль или посылка слишком тяжёлы для своих размеров, имеют грязные пятна на коробке или подтёки;
- от письма, бандероли или посылки исходит специфический запах;
- посылка имеет иной необычный вид;
- на посылке, бандероли или письме просматриваются очертания, не присущие почтовым отравлениям.

В целях безопасности все вентиляционные шахты следует оборудовать защитными решётками. Надо установить системы сигнализации и видеонаблюдения в тех помещениях, где хранятся конфиденциальные документы, уникальное или дорогостоящее оборудование.

Служба безопасности должна быть готовой к телефонным сообщениям о готовящемся взрыве. Для этой цели используется телефонный регистратор речевых сообщений, имеющий звукозаписывающую функцию, и способного определить номер звонившего.

Как часть процесса защиты следует разработать план и регуляр-

но проводить тренировочные занятия по эвакуации персонала с территории предприятия.

Рассеиванию возможной взрывной волны помогает открытие окон и дверей во всех помещениях зданий, подверженных взрыву.

Сразу после эвакуации персонала следует обеспечить охрану помещений силами собственной службы безопасности для недопущения посторонних лиц на территорию объекта. Производится выемка всех кассет и CD-дисков аудио- и видеонаблюдения и устанавливаются новые на случай возможного подрыва. Анализ изъятых кассет и дисков позволит выявить ошибки в работе службы охраны и может быть полезен для правоохранительных органов.

В любом случае надо немедленно вызвать подразделение пожарной охраны. По прибытию полиции и взрывотехников ФСБ, человек, обладающий соответствующими полномочиями, знающий расположение здания и его производственно-бытовых помещений, должен сопровождать группу поиска с ключами ко всем дверным замкам, а также иметь при себе поэтажные планы и чертежи здания. Все портативные радиостанции следует выключить — это предотвратит срабатывание взрывного устройства от радиосигнала, настроенного на соответствующую волну.

Если автомобили припаркованы рядом с предприятием, то для устранения (минимизации) фактов возможной закладки взрывного устройства в автомашине, следует их ставить в хорошо освещаемых и охраняемых местах (с теленаблюдением). Гражданин должен поставить автомобиль на сигнализацию.

Владелец или водитель сам должен проводить внешний осмотр автомашины, особенно если она находилась без присмотра в течение длительного промежутка времени. Надо убедиться, что на замках

дверей, багажника и капота автотранспорта нет признаков взлома. Работник особо режимного предприятия должен позаботиться о сигнализации, которая позволяет производить запуск двигателя автомобиля при помощи дистанционного устройства, находясь при этом на безопасном расстоянии.

6.8 Методика выбора охранного агентства

Не всегда экономически выгодно или целесообразно иметь на предприятии собственную службу охраны. В этих случаях заключают договор с частными охранными агентствами.

Основные элементы процесса общения с руководством частного охранного предприятия (ЧОП) по поводу возможного сотрудничества должны включать в себя:

1. Ознакомление с лицензией охранного предприятия. Надо проверить срок действия лицензии — первый раз она выдаётся на три года, затем продлевается на пять лет. Необходимо обратить внимание на наличие в организации необходимого числа лицензированных охранников, поскольку одно из главных требований лицензионно-разрешительной системы органов МВД — все сотрудники ЧОПа были лицензированы.

2. Следует проанализировать расценки ЧОП на оказание услуг. Если предлагаются услуги с меньшими, чем среднерыночные (региональные), расценками, то можно сделать вывод о слабых возможностях такой структуры обеспечить эффективную защиту. В таких охранных предприятиях обычно недостаточно ресурсов для развития (не закупается необходимое оборудование и оснащение, мало платят охранникам, что лишает их стимулов к эффективному труду и т.п.).

3. Подлежит анализу наличие и состояние профессиональных

радиостанций, количество служебных автомашин, включая бронеавтомобили представительского класса, инкассаторские машины.

4. Следует с выездом на место уточнить, имеет ли ЧОП собственный офис и круглосуточную дежурную часть.

5. Выясняется наличие у сотрудников ЧОП различных комплектов формы. В традициях охранных предприятий выдавать каждому сотруднику трёх комплектов рабочей одежды: а) специальная — для охраны офиса; б) гражданский костюм — для охраны и сопровождения клиента; в) камуфляжная форма — для сопровождения грузов.

6. Следует выяснить, каково число охраняемых объектов данного ЧОП, какой оборот денежных средств имеет оно за охрану клиентов.

7. Наличие заверенных рекомендаций клиентов, включая иностранные фирмы, что позволяет сделать вывод о возможности заключения договора. Участие охранного предприятия в профессиональных ассоциациях ЧОП свидетельствует о признании опыта и активности на рынке охранных услуг. Участие в деятельности международных союзов может быть оценкой интереса компании к общепринятым стандартам деятельности, хотя таких ЧОП в России не так уж и много.

В процессе заключения договора от солидного, нацеленного на долгую рыночную деятельность охранного предприятия, можно требовать включения в договор пункта о страховании профессиональной ответственности.

Никогда и ни при каких обстоятельствах нельзя отдавать все объекты под охрану одному частному охранному предприятию. Важная задача — выстроить такую систему физической защиты объектов организации, которая предусматривает распределение охранных функций между отделом вневедомственной охраны, несколькими ЧОП и собственной службой охраны.

7 Экономическая разведка как элемент предпринимательской деятельности

7.1 Технология и этика в деятельности экономической разведки

В нашем изложении мы неоднократно касались проблем управления рисками, показывали особенности их возникновения в условиях глобализации и усложнения экономических процессов. Трансформация старых рисков, появление новых — естественный процесс развития любой социально-экономической системы. Поэтому субъекты рынка должны не только приспосабливаться к новой ситуации, но и активно развивать систему риск-менеджмента, способную продемонстрировать гибкость управления, мгновенность реакции на быстро возникающие внешние факторы и внутренние угрозы.

Регулярное и практически всегда стохастическое изменение внешних факторов заставляет бизнес осознать ключевую роль аналитической составляющей риск-менеджмента, которая позволяет обеспечить топ-менеджмент предприятия актуальной информацией о состоянии внешней среды.

Критерий «учёт факторов неопределённости» российские предприниматели ещё слабо используют в своей практике. По данным агентства Reuters, только 28% российских менеджеров полагают, что информация является ключевым фактором, влияющим на принятие решений, в отличие от 91% менеджеров Франции и 95% менеджеров США[44].

Этот факт свидетельствует о наличии благодатной почвы для девиантного поведения граждан, представители которого комфортно

[44] URL: http://bre.ru/security/17838.html (дата обращения: 25.10.2011).

чувствуют себя в ситуации «правового нигилизма», извлекая личную выгоду из любой ситуации неопределённости среды и асимметричности информации.

Дефицит информации, её некорректность и несвоевременное получение даёт существенный рост деликтных рисков в предпринимательской деятельности.

Для успешного достижения бизнес-целей необходимо постоянно проводить мониторинг изменений внешней и внутренней сфер осуществления предпринимательства. Основой управления деликтными рисками является наличие полной и достоверной информация, которая позволяет оценить характер угроз и их степень, выработать меры безопасности бизнеса для минимизации рыночных угроз. Действия топ-менеджмента предприятия по физической, технической и другим видам защит от девиантного поведения деликвентов являются производными по отношению к оценке состояния защищённости данной организации. Эту разведку часто называют деловой или конкурентной разведкой.

Именно для этих целей используется экономическая разведка, предназначение которой — разрешённая законодательством деятельность, направленная на получение, обработку и использование информации для обеспечения конкурентоспособности организации, её экономической безопасности, защиты от недобросовестной конкуренции и криминалитета.

Важно в этой деятельности действовать в соответствии с законодательством России, ибо незнание и неумение применять правовые акты не освобождает от ответственности за их нарушение, а с другой стороны — это есть одна из причин их нарушения.

Информационная среда — это очень мощный ресурс организа-

ции и от того, как он используется, зависит статус хозяйствующего субъекта, его деловая репутация, выбор контрагентов для заключения выгодных сделок и эффективность взаимодействия с ними.

Какая же информация для этого нужна? Во-первых, надо отсечь информацию, не относящуюся к делу (иррелевантную). Во-вторых, информация должна быть прогнозной. Необходимо также исключить так называемый информационный шум, всё то, что «засоряет» информационные каналы и не требуется для нормального функционирования и развития организации.

Прогнозная информация со временем может стать релевантной (относящейся к делу), поэтому надо относиться к ней как к прогностической и учитывать, что её использование для достижения целей предприятия носит вероятностный характер.

Очень важна информация, предназначенная для тех сотрудников и высшего руководства организации, которые занимаются подбором партёров по бизнесу. Это важно и для выбора стратегии поведения с ними — от самой близкой, до индифферентной.

Характер и объёмы получаемой информации для каждого иерархического уровня управления могут значительно различаться. В связи с этим в деятельности подразделения экономической разведки (группы в составе службы экономической безопасности) предприятия выделяют два направления.

1. Стратегическое (или макроэкономическое), связанное со сбором и анализом стратегической информации о глобальных процессах в экономике, политике, технологических инновациях и пр.

2. Оперативно-тактическое (или микроэкономическое), направленное на сбор и анализ оперативной информации, и предназначенное для целей принятия руководством обоснованных решений по теку-

щим проблемам организации.

Эффективное информационно-аналитическое обеспечение финансово-хозяйственной деятельности предприятия направлено на проведение всестороннего анализа и полной обработки получаемых данных применительно как к компетенции отдельных функциональных подразделений, так и в разрезе проблем, касающихся общекорпоративной политики юридического лица.

Основными задачами, которые ставятся перед экономической разведкой, являются:

1. Регулярный сбор значимой для предприятия информации.

2. Выявление угроз организации, причин и источников их возникновения.

3. Автоматический предварительный анализ массива собираемых сведений, его классификация, оценка возможных экономических ущербов и своевременное информирование руководителей и персонала организации о критически важных событиях. Обеспечение подготовки возможных вариантов решений, а также оценка сценариев развития событий[45].

4. Управление отношениями предприятия с клиентами.

5. Выработка краткосрочных и долгосрочных прогнозов влияния окружающей экономической среды на финансово-хозяйственную деятельность предприятия. Разработка рекомендаций по локализации и нейтрализации активизирующихся факторов, влияющих на деликтные риски.

Экономическую разведку следует отличать от шпионажа. У них разные цели: шпионаж проводится в подрывных целях, разведка —

[45] Митрофанов А.А. Экономическая безопасность коммерческих предприятий и деловая разведка. URL: http://www.rscip.ru/base/A9738409-3441822.html (дата обращения: 18.10.2011).

для обеспечения конкурентоспособности организации, получения необходимой информации легальными, открытыми, разрешёнными законодательством способами. Деловая разведка получает свои результаты, в основном, проводя аналитическую обработку огромного количества разнообразных открытых информационных источников. Хотя отдельные формы и методы шпионажа и конкурентной разведки могут совпадать. Это использование психологических приёмов опроса, выведывания, наблюдения, маршрутирования сотрудников по местам дислокации объектов разведустремлений, легендирования, легализации, контент-анализа текстовой информации и ряд других.

Охота за чужими коммерческими тайнами позволяет сэкономить собственные финансовые ресурсы на ведение исследований и опытно-конструкторских работ, быть в курсе дел конкурента, использовать его научно-технические достижения и разработки, сосредоточив всё внимание на менеджменте, маркетинге и производстве на своём предприятии.

Экономическая разведка, может принимать форму недобросовестной конкуренции; она по своему содержанию является мощным скрытым каналом движения идей и технологий, которые похищаются, продаются и перепродаются на рынке. Отсутствие механизмов эффективного взаимодействия с государственными структурами и недостатки в правовом регулировании экономических отношений вынуждают предпринимателей создавать собственные базы данных и заниматься на свой страх и риск конкретным видом деятельности.

Что бы ни говорилось, но сегодня экономическая разведка — составная часть корпоративной культуры осуществления современного бизнес-процесса. Основные требования к ведению деловой (конкурентной) разведки в России — работа в правовом поле и соблюдение

этических норм. В условиях существования ожёсточённой конкуренции, правового нигилизма большинство российских предпринимателей тревожат конечные результаты, а не методы их получения. На самом деле проблема, выраженная в известной максиме «Цель оправдывает средства», должна звучать как «Цель должна не оправдывать, а определять средства». Владельцы предприятий должны чётко транслировать топ-менеджерам свои указания, которым необходимо постоянно взвешивать, что важнее: мгновенная прибыль или ведение бизнеса с использованием этических и правовых норм, обеспечивающих работу без судебных разбирательств, поддержание деловой репутации организации, уверенности персонала, ясности заданных целей. При этом нельзя давать указание на выбор очень сложных, дорогостоящих, неоправданно рискованных или незаконных способов получения информации, которая ещё неизвестно как и когда будет использоваться на предприятии.

Экономическая разведка в процессе своей деятельности использует следующие источники информации:

- открытые издания, включая материалы, размещённые в сети Интернет;
- сотрудников конкурирующих организаций;
- консультантов, экспертов, кандидатов, принимаемых на работу и т.п.;
- беседы и опросы на выставках, ярмарках, конференциях, семинарах и иных подобных мероприятиях;
- случайную оперативную информацию, попадающую в поле зрения сотрудникам деловой разведки.

Доступности информации, полученной из открытых источников, бесплатных или недорогих баз данных, программных продуктов, рас-

пространяемых в основном в рекламных целях, сопутствует серьёзная проблема её достоверности.

Ценность добываемой оперативной информации определяется не только быстрым получением информации, но и получением её в результате предварительного планирования самого́ замысла, цели проекта, что позволяет выделять из всего массива приобретённых данных нужные организации сведения.

Сотрудники экономической разведки должны постоянно осуществлять тотальный сбор оперативной информации, используя[46]:

- Сотрудников предприятия. Каждый из них в состоянии давать информацию, на основе которой составляются сводки и аналитические отчёты, которые размножаются и сообщаются заинтересованным лицам, а после использования — уничтожаются в установленном порядке.
- Опросы покупателей, клиентов и посетителей организации.
- Отчёты персонала о командировках, посещениях выставок, ярмарок, конференций, семинаров, курсов повышения квалификации и т.д.
- Беседы с кандидатами, принимаемыми на работу.
- Устройство на работу к конкуренту.
- Посещение объекта изучения под различными предлогами.

Понимая, что данная организация тоже является объектом внимания конкурентов, сотрудники службы экономической разведки должны не только выявлять их, но периодически смотреть на своё предприятие «глазами» конкурентов, чтобы выявить наиболее уязвимые места и обеспечить их защиту. Такие действия подходит под понятие «контразведка».

---

[46] Центр правовых инноваций. Системная безопасность [сайт]. URL: http://cpisb.com/business/competitive-intelligence/requirement (дата обращения: 27.10.2011).

Цель проведения экономической контрразведки — предоставление доступа конкурентов лишь к той информации, которая не даст им односторонних конкурентных преимуществ в соответствии с заключаемыми договорами, но позволит быть успешными, если они предпочтут не конфронтацию, а партнёрские отношения.

Контрагент, о котором всё известно заранее и информация эта полна и достоверна — это всегда предсказуемый результат выгодного заключения хозяйственных и иных договоров.

Существует несколько вариантов, в которых отражён перечень вопросов для сбора информации о контрагентах. Обобщим эти вопросы:

— полное название, юридический адрес, телефон, факс контрагента;

— дата, номер регистрации, место и организационно-правовая форма;

— сведения о его партнёрах и конкурентах, их деловые характеристики;

— реквизиты владельцев (акционеров и пр.), топ-менеджеров, история их профессиональной деятельности, адреса́ и пр.;

— информация об участии контрагента в арбитражных и иных разбирательствах, переданного в залог имущества, выдержки из газетных и журнальных публикаций, информация из Интернета, их анализ и объективная оценка;

— информация о своевременности исполнения различного рода платежей: какие суммы, в какие сроки и с какими издержками;

— коммерческие банки, с которыми работает контрагент, адреса и номера расчётных и депозитных счетов;

— экономическая характеристика состояния проверяемого пред-

приятия за последние три года (анализ финансово-хозяйственной деятельности);

— рассчитанные коэффициенты ликвидности, покрытия, прибыльности вложений, отношение основных средств к инвестициям и другие аналитические показатели;

— выписки из последнего балансового отчёта, отчёта о прибылях и убытках;

— наличие дочерних, зависимых, сёстринских обществ, филиалов, представительств и иных подразделений;

— виды осуществляемой хозяйственной деятельности: производимые работы или оказанные услуги, состояние экспорта-импорта, условия исполненных и заключённых договоров;

— наличие и предположения о возможных связях в криминальной бизнес-среде.

Обобщив предлагаемые специалистами методы и формы ведения экономической разведки на современном информационном пространстве, мы объединили их по следующим основным признакам:

1. Сбор и анализ открыто опубликованной информации, включая официальные документы: статьи, бюллетени, рефераты, пресс-релизы, интернет-источники и т.д. (аналитический открытый метод).

2. Использование сведений, случайно или намеренно разглашаемых персоналом конкурирующей организации или получаемых в результате действий, не выходящих за рамки законодательства (тайный метод).

3. Анализ биржевой информации (документов и отчётов), а также финансовых отчётов конкурирующих организаций и других финансовых документов, имеющихся в распоряжении брокеров, маклеров и консультантов. Изучение и сбор сведений о выставочных экс-

понатах, анализ проспектов (брошюр). Сбор и изучение донесений различного вида, которые направляются филиалами в центральный аппарат по существующим между ними каналам связи (сочетание аналитического открытого и тайного технического методов).

4. Изучение качественных характеристик выпускаемой продукции (состава, комплектующих деталей, технологии изготовления) конкурирующих юридических лиц. Анализ данных, полученных из бесед, проводимых в рамках закона, заданных вопросов персоналу конкурирующих организаций на научно-технических конференциях, совещаниях или симпозиумах (аналитический открытый метод).

5. Осуществление непосредственного скрытного наблюдения, (тайный метод).

6. Беседа с помощью специально разрабатываемых вопросников при найме на работу бывшего персонала конкурирующей организации, без намерения принять такого работника на вакантную должность (аналитический открытый метод).

7. Организация фиктивных переговоров с фирмой-конкурентом относительно приобретения лицензии на интересующую их продукцию (аналитический полуоткрытый метод).

8. Наём на работу сотрудников конкурирующей организации в целях получения производственной информации о порядке изготовления продукции или содержащейся в ней инновационной технологии, определяемой как ноу-хау (аналитический открытый метод).

9. Подкуп сотрудника конкурирующей организации или лица, занимающегося реализацией её продукции (экономическая разведка).

10. Использование привлечённого на конфиденциальной основе сотрудника фирмы-конкурента, для получения информации на основе изучения и сопоставления переданной им информации и имеющейся

документации (аналитический и тайный методы).

11. Прослушивание переговоров, ведущихся в фирмах-конкурентах перехватом сообщений и переговоров, проводимых по техническим средствам связи с помощью спецсредств (экономическая разведка).

12. Кража образцов продукции, чертежей, документации по технологии её производства и т.д. (экономическая разведка).

13. Использование компрометирующих материалов в отношении сотрудников фирмы-конкурента (экономическая разведка).

14. «Утечка мозгов», то есть переманивание наиболее грамотной инженерно-технической элиты из конкурирующих организаций (собственно экономическая разведка)[47].

Сотрудники экономической разведки регулярно отслеживают, собирают, анализируют и группируют актуальную, необходимую для деятельности предприятия информацию. Такое информационное преобразование превращает разрозненные материалы в комплект аналитически полных разведывательных данных о фирмах-конкурентах.

Рутинные действия по сбору, обработке и анализу рыночной информации дают возможность получить не только материалы для принятия соответствующего управленческого решения, но и данные, которые можно использовать персоналом конкурентной разведки.

Действия экономической разведки должны быть эффективными для чего можно воспользоваться четырьмя основными количественными критериями, которые показывают что:

• разведка привела к экономии времени принятия решений предприятием;

---

[47] Климов В. Промышленный шпионаж как основа грязных информационных технологий и современных информационных войн // Мир и безопасность. 2002. № 3. URL: http://daily.sec.ru/publication.cfm?pid=4899 (дата обращения: 20.09.2911).

• она позволила сэкономить финансовые ресурсы;

• привела к минимизации лишних затрат, благодаря наличию необходимой оперативной информации;

• дала возможность увеличить прибыль.

Указанных показателей можно достичь, если создана информационная система сбора данных, что в свою очередь требует соответствующих масштабов финансирования для поддержания структуры обеспечения доступа к информационному пространству.

Как видим, глобализация экономики, диверсификация бизнеса, распространение информационных технологий, ставит деятельность экономической разведки в разряд жизненно необходимых элементов сопровождения основных бизнес-процессов.

7.2 Управление системой безопасности как фактор противодействия внешним и внутренним деликтным угрозам

Действующие в настоящее время нормативно-правовые акты Российской Федерации не содержат запретов для организаций на разработку собственной концепции системы безопасности, направленной на противодействие деликтным угрозам и девиантному поведению граждан.

Анализ основных угроз безопасности организации показывает, что к главным направлениям деятельности по обеспечению её безопасности относятся:

1) Проведение информационно-аналитических исследований и прогнозных оценок экономической безопасности.

2) Безопасность персонала.

3) Сохранность и физическая защита предприятия и его объектов;

4) Защита от угроз, направленных на безопасность информационных ресурсов (защита от несанкционированного доступа и т.д.).

5) Защита финансовых ресурсов предприятия.

Первая задача связана:

• с получением и анализом информации о местном, региональном и национальном рынках и прогнозированием их развития;

• с проведением мероприятий по выявлению и грифованию конфиденциальной информации и её документальным оформлением в виде перечней коммерческих сведений, подлежащих защите;

• со сбором экономической и инновационной (научно-технической информации) для обеспечения эффективности деловых отношений с бизнес-партнёрами, для выявления среди них недееспособных, неплатёжеспособных и криминально настроенных предпринимателей;

• с учётом направленных официальных претензий правоохранительных и контролирующих (налоговые и др. органы) инстанций к партнёрам по бизнесу и возможным контрагентам;

• с изучением, анализом и оценкой криминальной ситуации на рынке, в том числе состояния экономической преступности в региональной банковской системе, функционирования рынка сбыта производимых товаров и предоставляемых услуг;

• анализ и прогнозирование тенденций девиантного поведения персонала для оценки социально-экономического развития предприятия и негативного влияния на его безопасность;

• информационное обеспечение акционеров и иных владельцев организации в сфере экономической безопасности;

• координация действий всех отделов службы безопасности и обеспечение взаимодействия с другими структурными подразделе-

ниями организации для эффективного противостояния внутренним и внешним деликтным угрозам и рискам.

Вторая задача предусматривает необходимость обеспечения безопасности персонала от любых противоправных посягательств на жизнь, здоровье, материальные ценности и их личную информацию.

Третья задача ориентируется:

• на формирование специального режима охраны производственных объектов и объектов жизнедеятельности организации;

• на осуществление эффективного допускного и пропускного режимов;

• на обеспечение действенной защиты хранимых на предприятии ценного имущества и документации, представляющей коммерческую и служебную тайны;

• организация физической безопасности, определённой приказом по предприятию категории топ-менеджеров, ведущих специалистов, а при необходимости членов их семей.

Четвёртая задача обеспечивает:

• формирование и организацию деятельности разрешительной системы допуска исполнителей к работе с документами, представляющими коммерческую и служебную тайны;

• организацию хранения, использования и уничтожения конфиденциальных документов на любых носителях информации;

• формирование механизма осуществления закрытой переписки и шифрования связи, защищённых от внешних и внутренних деликтных угроз;

• защиту коммерческой информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;

• обеспечение защиты речевой информации, появляющейся в

процессе проведения конфиденциальных совещаний, переговоров, конференций;

• контроль за сохранностью конфиденциальных документов и материалов, обеспечением программной и криптографической защиты информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи.

Важно обеспечить выполнение мероприятий по предупреждению девиантного поведения персонала организации. К ним относятся:

• правильный подбор кадров, создание резерва потенциальных кандидатов по всем должностям. Набор целесообразно проводить перемещением и продвижением по службе своих работников. Использование внешних трудовых ресурсов следует проводить по личным рекомендациям проверенных людей;

• отбор кандидатов следует осуществлять на основе профессиональных, образовательных, деловых и личных качеств, а не по личному указанию третьих лиц;

• после заключения трудового договора получать от сотрудника добровольное письменное согласие по соблюдению требований, регламентирующих режим безопасности и сохранения коммерческой тайны;

• постоянное проведение текущего мониторинга за деятельностью сотрудника, воспитание его личных качеств для повышения бдительности в отношении потенциальных угроз безопасности организации.

8 Система комплексной безопасности как составная часть противодействия рейдерству

8.1 Влияние макроэкономических факторов на недружественное поглощение бизнеса

Как и многие страны (например, США в начале XX-го века), Россия в конце девяностых годов прошлого столетия, осуществляя переход к рыночным отношениям, столкнулась с небывалым ростом девиантного поведения граждан. В десятки раз возросло количество потерь имущества организаций и предприятий в форме отчуждения собственности, краж, хищений, растрат, присвоения, коммерческого подкупа, взяточничества, вымогательства, заказных убийств, разбоя, бандитизма, мошенничества, коррупции, должностного подлога, шантажа, рейдерства и т.д.[48].

Если говорить о рейдерстве, то оно имеет в России глубокие социально-экономические корни. Недееспособность, умышленные действия потребителей и поставщиков, противоправность методов ведения конкурентной борьбы, давление организованных преступных групп, коррумпированность органов государственного и отраслевого управления федерального, регионального и муниципального уровней привели к тому, что ресурсы экономики от государственного до первичного хозяйствующего звена истощались, а потери возрастали, снижая доходность хозяйственной деятельности. Поэтому убыточность функционирования, отчуждение собственности посредством фиктивных банкротств и рейдерских захватов получили массовое

[48] Усанов Г.И., Старинов Г.П. Деликтыне риски организаций: идентификация, диагностика и управление / Учёные записки Комсомольского-на-Амуре государственного технического университета. 2010. № 1–2 (1). С. 121.

распространение.

«Вложив несколько сот тысяч долларов в рейдерский захват, можно получить активы стоимостью несколько десятков, а то и сотен миллионов долларов», — заявил член Общественной палаты России адвокат П. Астахов на слушаниях ОП по противодействию рейдерству. По его словам, коррупция, отсутствие сильной независимой судебной власти и несовершенство законодательной базы привели к тому, что сегодня в России дешевле отнять бизнес, чем приобрести его[49].

Причина состоит ещё и в том, что смычка административного ресурса и крупного, олигархического, как его называют в России, капитала — это мощная сила, потенциал которой способен поглотить любой бизнес.

Сегодня в РФ есть несколько крупных центров концентрации капитала. Эти центры обладают существенным преимуществом перед остальными акторами рынка, ибо уже «подмяли» под себя важные ресурсы: судебный, силовой и административный. Некоторые из них, достигнув максимального экономического роста за счёт внутренних источников, расширяют хозяйственную деятельность за счёт внешних ресурсов, поглощая новые виды бизнеса; другие, — стремясь к монополизации определённого сектора рынка, формируют свои активы путём поглощения бизнеса конкретной отрасли, либо создавая вертикально интегрированные компании.

Добавим, что в последнее время инвестиционный интерес корпоративных игроков переместился с крупных объектов на средние и небольшие.

Второй макроэкономический фактор определяется существен-

[49] URL: http://www.city-n.ru/view/91843.html (дата обращения: 26.09.2011).

ной зависимостью успешности рейдерского бизнеса от наличия административного ресурса.

Под определением «рейдерство» (*raid* — внезапное нападение, набег) принято понимать особый вид враждебного поглощения, при котором наиболее ценные активы бизнеса, подвергшейся рейдерской атаке организации, распродаются законно на незаконном основании и бизнес прекращает своё существование.

В России бизнес по захвату активов предприятия в данное время чрезвычайно выгоден: прибыль по разным оценкам составляет от 100 до 500% от вложенных средств[50]. Реалии российской экономики принципиально отличаются от классической практики слияний и поглощений США и Европы, где за приобретение бизнеса платят деньги, в России же его просто отнимают.

Рейдерство осуществляется следующими методами:

1. Внесение недействительных сведений в реестр юридических лиц, с направлением фиктивного протокола собрания учредителей с решением об избрании нового директора (генерального директора), с дальнейшей перепродажей имущества новому добросовестному приобретателю.

2. Рейдерский захват имущества предприятия базируется на умышленном вынесении судом заведомо неправосудного решения, с нарушением принципов подсудности имущественных споров, вследствие умышленного сговора.

3. Хищение имущества посредством государственной регистрации права собственности на недвижимость на основании решения третейского суда. Недвижимость по решению третейского суда передавалась без уведомления собственника. Третейские суды являются

[50]URL: http://www.mosuruslugi.ru/consultation/q/230 (дата обращения: 22.10.2011).

частными судами, в которые участники споров обращаются на основании соглашения и сами же выбирают арбитров. Закон о третейских судах[51] позволяет им рассматривать любые споры гражданско-правового характера, участниками которых могут быть как юридические лица, так и граждане. При этом собственник имущества может не знать о третейском разбирательстве, так как от его имени по поддельной доверенности выступают представители рейдерства.

4. Присвоение имущества путём проведения доверительного управления «поневоле»[52]. Акции мажоритарного акционера по фиктивным договорам передаются в псевдодоверительное управление сторонней компании и договор регистрируется у реестродержателя. При этом «доверительный управляющий» приобретает право голоса по акциям на собраниях акционеров, но не имеет права собственности на них. Далее по стандартной схеме проводится собрание акционеров, назначается подконтрольный генеральный директор, осуществляется физический «заход» на территорию организации, бывших менеджеров изгоняют, а активы выводят на сторону. В действиях рейдеров состава преступления нет, так как доверительный управляющий не получает права собственности на акции.

5. Приобретение имущества хозяйствующего субъекта через инициирование уголовного дела в отношении директора организации, в которой рейдер приобретает небольшой пакет акций предприятия. Параллельно идёт сбор компромата на руководителя, с дальнейшей передачей материала в правоохранительные органы, на основании которого проталкивают судебное решение о наложении ареста на мажоритарный пакет акций. После этого небольшой пакет акций рейдера

[51] Федеральный закон от 24 июля 2002 г. № 102-ФЗ «О третейских судах в Российской Федерации».

[52] http://www.apkit.ru/committees/defence/news/aticles/article2.php (дата обращения: 02.10.2011).

превращается в контрольный пакет. Затем созывается собрание акционеров, выбирающее нового генерального директора, который в свою очередь продаёт активы той компании, которая связана с рейдерами.

6. Учреждается подставная фирма, которая скупает задолженность хозяйствующего субъекта. Попытки погасить долги ни к чему не приводят, денежные перечисления возвращаются плательщику. Предприятие, скупившее задолженность, фиктивно перепродаёт её другой организации, которая в свою очередь меняет и юридический адрес, и реквизиты. Хозяйствующий субъект предпринимательства фактически не может вернуть долг и становится либо банкротом, либо деятельность предприятия парализуют арбитражные управляющие. Параллельно с проведением процедуры банкротства рейдеры приступают к скупке акций фирмы у членов трудового коллектива, которые избавляются от них из-за опасения их обесценивания или от страха.

7. Скупка акций предприятия с использованием в судебных инстанциях имевшихся фактов незаконной приватизации или допущенных в её ходе нарушений.

8. Осуществление сделок с активами в результате вступления в сговор с должностными лицами «компании-мишени».

9. Лоббирование интересов в различных государственных органах власти и управления путём вступления в преступный сговор с государственными служащими.

Как мы отметили выше, перечисленные агрессивные действия рейдеров могут проводиться в рамках законодательства о корпоративной политике в сфере слияний и поглощений (антимонопольное законодательство). Однако рейдеры используют и чисто криминальные методы (вынужденная передача активов или бизнеса из-за психо-

логического давления на акционеров и руководителей, вплоть до физической расправы, с целью временного «паралича» хозяйственной деятельности предприятия, с последующим осуществлением негласного контроля за движением финансовых потоков и пр.).

Другим способом можно отнять бизнес через профессиональное вымогательство — «гринмейл» — (*greenmail*). Вымогательство заключается в деятельности, направленной на получение третьими лицами сверхприбылей в процессе спекуляций или злоупотреблений своими правами акционеров. Есть следующие методы профессионального вымогательства.

1. Захват организации посредством «перехвата» управления — смены исполнительных органов, вопреки интересам его владельцев, аффилированных лиц, крупнейших акционеров, а также топ-менеджеров. Это и есть враждебное поглощение. Такой вид деятельности доступен, конечно, только крупным структурам. Они обладают значительными связями в органах власти и управления, штатом профессиональных юристов, специалистов PR, а также имеют неограниченные финансовые возможности по отношению к потенциальному объекту поглощения.

2. Понуждение предприятия к выкупу собственных акций (доли, паи) по завышенной цене. Для этого первоначально приобретается пакет акций чуть более 10 процентов, позволяющего использовать законодательство об АО или ООО для юридических действий с целью приостановки (саботажа) финансово-хозяйственной деятельности предприятия, с последующим инициированием многочисленных арбитражных разбирательств, с количеством и сложностью которых штатные юристы предприятия справиться не могут[53].

[53] Котляр Э. Гринмейл: русская версия // Консультант. 2005. № 5.

3. Применяется также эффективный способ воздействия на субъект предпринимательства с помощью подконтрольного профсоюза, созданного гринмейлерами. Ст. 29 Трудового кодекса (ТК РФ) предполагает, что профсоюз является представителем работников, а ст. 30 позволяет ему представлять интересы даже тех работников, которые в нём не состоят. Ст. 399 ТК РФ предполагает, что профсоюз имеет право выдвигать ряд требований при коллективном трудовом споре, то есть фактически инициировать такой трудовой конфликт, который способен парализовать финансово-хозяйственную деятельности компании.

Опасность корпоративного шантажа достаточно велика, прежде всего, в силу его неожиданности и неспособности предприятия выдержать давление, ибо гринмейлеры никогда не нападают на сильные структуры или предприятия готовые к такому нападению[54]. В России вышеозначенная опасность бизнесу пока недооценивается ни законодательными структурами, ни владельцами бизнеса, ни экспертами, ни компетентными органами.

На Пятом экономическом форуме (2009 г.) в Красноярске президент РФ Д. Медведев представил свою экономическую программу, где в одном из тезисов прозвучало отношение к частной собственности: «… Уважение к частной собственности должно стать одной из основ проводимой государством политики… Одним из проявлений неуважения к собственности, к труду других людей выступают по прежнему носящие массовый характер незаконные захваты фирм (так называемое «рейдерство»)… Считаю крайне необходимым скорейшее принятие антирейдерского закона. Причём в таком виде, чтобы это не было банальной декларацией, а реально создало инструменты для

[54] Фёдорова А.Э. Экономический терроризм: тяжелые болезни российского бизнеса // Безопасность, менеджмент, бизнес. 2009. № 1–2. С. 57.

предотвращения рейдерства …».

Потенциальным объектом рейдерского захвата предприятие становится в случаях, если:

• Оно является хозяйствующим субъектом в сфере малого и среднего бизнеса в отрасли, которую монополизировали крупные рыночные акторы.

• Оно не отладило продвинутых контактов с органами управления («административный ресурс», особенно региональный) перед потенциальным захватчиком.

Источники возникновения девиантного поведения характеризуются как деликты следующими признаками:

— общественная опасность;

— противоправность;

— виновность;

— наказуемость.

Кроме того важно учесть состав деликтного деяния, который определяется:

— объектом исследуемых отношений;

— субъектом противоправного деяния;

— объективной стороной, выраженной в действии или бездействии рыночного актора;

— субъективной стороной деяния, выраженной в форме вины и умысла.

Захват активов конкретного предприятия рейдерами облегчатся если:

• собственник имущества имеет очень слабые рыночные позиции;

• юридическое лицо допускало серьёзные нарушения дейст-

вующего законодательства в процессе ведении бизнеса.

Слабый собственник всегда характеризуется:

• распылённостью (раздробленностью) неконсолидированного пакета акций, паёв, долей;

• постоянными внутренними конфликтами и разногласиями собственников бизнеса;

• глубокими противоречиями между владельцами бизнеса и топ-менеджерами;

• наличием на предприятии мощной неформальной оппозиции топ-менеджерам и/или владельцам бизнеса;

• информационной доступностью компрометирующих сведений в отношении руководителей предприятия и его владельцев;

• наличием неподконтрольной предприятию кредиторской задолженности;

• отсутствием эффективных механизмов использования владельцами бизнеса своей собственности;

• серьёзными нарушениями при заключении крупных сделок, природоохранных и технических регламентов, таможенного законодательства;

• наличием активно-агрессивных схем оптимизации налогов, пошлин, сборов и т.п.

Бороться с рейдерскими захватами нелегко. Поэтому в системе правовых мер борьбы с такими захватами гражданско-правовые меры превентивного характера занимают первостепенное место. Ведь реализованное девиантное поведение приводит к различным негативным последствиям — от порчи и нанесению ущерба имуществу, перерасходу денежных средств, снижению доходности, упущенной выгоды, до несостоятельности субъекта рынка с последующим отчуждением в

пользу рейдеров собственности.

8.2 Превентивные методы защиты от недружественных поглощений

Превентивная система безопасности бизнеса имеет очевидные преимущества, хотя в России многие её недооценивают.

К превентивным мерам относятся методы защиты, внедряемые предприятиями до самого́ факта появления непосредственной угрозы поглощения. Эти методы имеют своей целью минимизацию деликтных рисков агрессивного захвата бизнеса.

Превентивная система безопасности бизнеса строится на комплексной основе с учётом проведения мероприятий по следующим направлениям.

I. Для своевременного обнаружения признаков угрозы захвата активов организации следует осуществлять регулярный мониторинг внешнего информационного поля. Для этого необходимо обязательно проводить:

- региональную оценку рейтинга общей деликтной активности;
- рейтинг деликтной активности в конкретной отрасли (сфере) бизнеса;
- отслеживание появления на рынке региона или в отрасли представителей рейдеров;
- проверку в регистрирующих органах сведений, содержащихся в Едином государственном реестре юридических лиц;
- мониторинг сделок с мелкими пакетами акций на внебиржевом рынке;
- контроль за состоянием журнала «Лицевые счета», открытого в реестре акционеров.

В процессе анализа внешнего информационного поля следует обращать внимание на типичные признаки подготовки рейдерского захвата. К таким признакам относят:

1. Сбор информации о предприятии:

• запросы в Федеральную службу государственной регистрации, кадастра и картографии (Росреестр) и проектно-инвентаризационные бюро неустановленных лиц о фактическом состоянии недвижимости конкретного субъекта рынка;

• поступление запроса в налоговый орган, с целью получения сведений о компании из Единого государственного реестра юридических лиц (ЕГРЮЛ);

• проведение несанкционированного доступа к компьютерным базам и документам, составляющих коммерческую тайну;

• попытки доступа неустановленных лиц к реестру акционерного общества;

• внезапные деловые предложения маркетологов, рыночных консультантов, предлагающих провести исследование в конкретной отрасли промышленности.

2. Внезапный рост числа сделок с мелкими пакетами акций, проводимых на внебиржевом рынке.

3. Резкий всплеск активности миноритарных акционеров:

• запросы информации о различных сторонах деятельности предприятия;

• обращение миноритариев к регистратору с целью получения информации о деятельности акционерного общества;

• запросы о необходимости созыва внеочередного общего собрания акционеров;

• направление заявлений в налоговые и иные контрольно-

надзорные органы о проверке деятельности общества;

• инициирование подачи многочисленных исков к обществу.

4. Массовые предложения о прямой продаже акций или долей, поступающие от финансовых компаний.

5. Неожиданные судебные процессы, ставящие своей целью легальное получение копии реестра, бухгалтерской и финансовой отчётности и т.д.

6. Неплановые и неожиданные посещения контрольно-надзорных и правоохранительных органов с требованием предоставления копий документов, касающихся активов общества, кредиторской задолженности и иных данных.

7. Возникновение непрогнозируемых (то есть «вдруг возникших») проблем с контрагентами и бизнес-партнёрами, связанных с:

• внезапным отказом этих экономических субъектов работать без предоплаты;

• неожиданным предъявлением векселей к оплате со стороны третьих сторон;

• внезапным возникновением проблем по исполнению кредитных линий, выдаче заранее оговоренных банковских кредитов, отказами в предоставлении гарантии банков и поручительств частных лиц;

• непрогнозируемым предъявлением требований кредитных организаций о досрочном погашении ранее выданных ссуд и т.д.

8. Получение акционерами предприятия заказных писем без письменного содержания (имитация приглашения на внеочередное собрание акционеров).

9. Проведение интенсивной информационной компании в прессе и Интернете по дискредитации собственников и топ-менеджеров кон-

кретной организации. Рейдеры ставят цель:

• отвлечь внимание и ресурсы компании-мишени поглощения от повседневной деятельности;

• создать чувство неуверенности и даже страха миноритарных акционеров о предстоящем банкротстве, облегчая тем самым скупку акций данного предприятия;

• при захвате банков создать у вкладчиков впечатление о возможных неурядицах данной кредитной организации, а это приводит к оттоку вкладов, которое носит в литературе название «набеги вкладчиков»[55].

Появление таких рыночных «индикаторов» уже можно считать характерными признаками начавшегося захвата бизнеса, а их фиксация топ-менеджерами сигнализирует об ограниченности времени для разработки эффективных мероприятий по защите предприятия от рейдерского захвата.

II. Построение системы защиты инсайдерской информации, имеющей высокую степень надёжности.

Частично мы этого вопроса уже касались (см. подраздел 5.2 настоящей монографии). Напомним, кратко, что обеспечение информационной безопасности бизнеса связано с наличием следующих обязательных элементов:

• созданы должные условия хранения документации (протоколы собрания заседаний совета директоров, правления, собрания акционеров; доказательства уведомления акционеров общества о проведении собраний; печати, штампы, хозяйственные договоры, свидетельства о праве собственности на недвижимость и т.д.) в надёжно

[55] Глущенко Е.Н., Дроздовская Л.П., Рожков Ю.В. Финансовое посредничество коммерческих банков. Хабаровск: РИЦ ХГАЭП, 2011. 240 с. (URL: http://www.fin-econ.ru/4r.htm).

защищённых местах;

• хорошо защищены внутренние информационные сети организации, если они имеются;

• аутсорсинг бухгалтерских функций (передача) изолированной подконтрольной организации;

• разработка и внедрение собственных положений о системах делопроизводства, защите коммерческой тайны и конфиденциальной информации;

• подписание с топ-менеджерами и ответственными работниками индивидуальных контрактов, с обязательным отражением в них имущественных санкций в случае намеренного или случайного разглашения секретной информации;

• надёжно защищены внутренне информационные сети организации, если они имеются, что гарантирует защиту от внешних источников угроз, надёжность инфраструктуры, защиту информации при её передаче по закрытым каналам связи, защиту компьютерных систем и баз данных и т.п.

III. Формирование структуры учредительных и внутренних корпоративных документов предприятия**,** являющейся оптимальной с точки зрения минимизации возможностей по «перехвату» корпоративного контроля.

В первую очередь надо устранить возможные противоречия между положениями учредительных и других внутренних документов и требованиями действующего законодательства. Именно этим пользуются рейдеры, захватывая фирму-мишень. Следует детально проанализировать:

• порядок уведомления акционеров о проведении общего собрания общества;

• процедуру проведения и принятия решений на внеочередном собрании акционеров общества;

• полномочия, механизм образования и досрочного прекращения этих полномочий как единоличного исполнительного органа;

• определение количества акционеров, определяющего необходимый кворум общего собрания или совета директоров по вопросам исключительной компетенции;

• порядок конвертации акций (например, в облигации и т.д.);

• процедура одобрения и совершения крупных сделок;

• процедура внесения изменений в учредительные документы АО и т.д.

IV. Проведение внутренней экономической политики, способствующей появлению у топ-менеджмента и акционеров общества соответствующих мотиваций на эффективное и безопасное развитие бизнеса.

Заинтересованность в конечных результатах деятельности топ-менеджеров и управленцев среднего звена обеспечивается заключением стимулирующих контрактов (за рубежом они носят название *«incentive contracts»*).

Вознаграждение в стимулирующем контракте складывается из двух частей: а) фиксированная; б) переменная. Фиксированная часть вознаграждения не зависит от результатов финансово-хозяйственной деятельности организации, переменная же — несёт в себе основные материальные стимулы. Базой для расчёта переменной части могут являться:

• абсолютные показатели деятельности предприятия, где вознаграждение зависит от финансовых показателей — рентабельности, объёма прибыли, величины денежных потоков, заключённых и ис-

полненных контрактов и т.д.;

• относительные показатели хозяйственной деятельности организации, отражающие её конкурентные позиции на рынке;

• стоимость организации, напрямую связанная с теорией ценностно-ориентированного менеджмента (VBM).

Текущая эффективность бизнеса в целом и адекватное ей вознаграждение топ-менеджеров определяется с помощью коэффициентов, которые выводятся при помощи методов дисконтированных денежных потоков или экономической добавленной стоимости и основываются на сочетании текущих показателей, отражающих результаты хозяйственной деятельности предприятия за конкретный период времени и предписываемых финансовой теорией индикаторов максимизации ценности для акционеров[56].

Если говорить о превентивной защите, то необходимо уделить серьёзное внимание работе с акционерами. Общеизвестно, что часть акционеров весьма пассивно относятся к своим функциям как владельцев бизнеса. Надо сделать так, чтобы внутренняя управленческая информация должна быть структурирована должным образом и, главное, чтобы она подчёркивала ценность общества для каждого, даже са́мого мелкого, акционера.

V. Важной нам представляется деятельность по контролю за долговой нагрузкой и осуществлению функций по управлению кредиторской и дебиторской задолженностью. Особо это актуально именно для превентивной защиты бизнеса от захвата.

Текущая работа с кредиторской задолженностью должна осуществляться по следующим направлениям:

---

[56] Системы добавленной акционерной стоимости (SVA), рыночной добавленной стоимости (MVA), экономической добавленной стоимости (EVA®), доходности инвестиций на основе денежного потока (CFROI®), ожидаемой рентабельности инвестированного капитала (EROIC) и т.д.

• следует крайне осмотрительно относительно к выбору контрагентов и партнёров по бизнесу;

• необходимо применять все меры для недопущения появления просроченной кредиторской задолженности;

• целесообразно создать несколько подконтрольных предприятий для передачи туда и накапливания кредиторской задолженности основной организации.

Такие меры в определённой степени могут повысить шансы предприятия противостоять попыткам захвата бизнеса.

VI. Защита акционеров от утраты или хищений, принадлежащих им ценных бумаг, прежде всего — акций.

Анализ практики враждебных поглощений говорит о том, что можно выстроить превентивную защиту владельцев от утраты акций. Для этого необходимо:

• создать условия, препятствующие массовой скупке акций;

• сформировать консолидированный пакет акций;

• использовать схемы перекрёстного владения акциями.

Главный способ борьбы с хищением акций: создание условий, препятствующих возможности внесения нелегитимных изменений в записи по лицевым счетам в реестре акционеров общества. Это могут сделать на основе предоставления реестродержателю поддельного передаточного распоряжения.

Ещё один способ защиты — включение в договор на ведение реестра акционеров пункта, в соответствии с которым регистратор будет обязан информировать эмитента в течение суток обо всех случаях, когда производятся записи по лицевым счетам держателей контрольного пакета акций, связанные с отчуждением или обременением акций.

Ещё один способ — передача акций в доверительное управление, на основании которой ценные бумаги списываются со счёта акционера и при этом происходит обособление акций от иного имущества собственника акций.

К другим способам относятся:

• передача акций номинальному держателю;

• выход на западный фондовый рынок через начальное публичное предложение (*initial public offer* — IPO). Возможность применения криминальных методов в отношении публичной компании практически исключена;

• размещение акций по программе американских депозитарных расписок (*American depository receipt* — ADR). Депозитарные расписки были разработаны, чтобы инвесторы США могли получать дивиденды на акции неамериканских компаний без непосредственного контакта с иностранными рынками. Общеизвестно, что публичный статус компании повышает степень защиты от нелегитимных действий рейдеров;

• формирование защищённой корпоративной структуры, связанной с изменением организационно-правовой формы, ликвидацией общества (предприятия) с передачей её активов другому юридическому лицу, реорганизацией в форме образования холдинговой структуры и др.

Для защиты активов применяются также концентрация основных активов в дочерней организации, которая практически не участвует в текущей хозяйственной деятельности основного общества; вывод активов; обременение имущества; использование иностранных

трастов[57] и фондов для защиты активов и т.п.

8.3 Экстренные методы защиты от недружественных поглощений

Когда подготовка к рейдерству «поглотителем» уже в основном проведена и мероприятия по враждебному поглощению вступают в самую активную стадию, то в качестве экстренных мер защиты применяют:

• добровольное блокирование операций по лицевому счёту акционера (выписывается соответствующее распоряжение), позволяющей блокировать операции в течение трёх дней;

• скупка (контрскупка) собственных акций**,** так как бороться с этим способом для рейдеров является наиболее затратным, ибо требует концентрации значительных финансовых ресурсов причём в очень короткие сроки;

• дополнительная эмиссия акций, осуществляемая в порядке закрытой подписки, предназначенная для увеличения уставного капитала фирмы-мишени, что размывает доли, принадлежащие рейдеру, доводя их до незначительных размеров;

• принятие общим собранием акционеров поглощаемого общества решения о размещении ценных бумаг, конвертируемых в акции, в том числе опционов («опцион помощи» — *leg-up option*);

• размещение фирмой-мишенью неконвертируемых в акции облигаций, но обладающих возможностью досрочного погашения посредством выкупа эмитентом, а также приобретение (или выкуп) обществом ранее размещённых собственных облигаций;

---

[57] Это очень интересная форма защиты бизнеса. Бенефициар не является собственником имущества, переданного в траст. Поэтому отнять у него имущество невозможно.

• использование резервного фонда или иных фондов акционерного общества или организации иной организационно-правовой формы, средства которых направляются на борьбу с рейдером;

• срочный перевод активов в другие предприятия с целью снижения общей инвестиционной привлекательности поглощаемого бизнеса;

• *scorched earth* — тактика «выжженной земли», когда поглощаемая компания продаёт свои активы, оставляя только проблемную собственность;

• применение компенсационных парашютов (в зарубежной практике их называют: а) «золотые», б) «серебряные» и в) «оловянные»), связанных с включением в контракты топ-менеджеров условий, по которым им гарантируются значительные выплаты в случае их увольнения в результате недружественного поглощения предприятия;

• организация информационной компании против рейдеров и их представителей в СМИ;

• веерные обращения в правоохранительные, надзорные органы, а также в государственные структуры, призванные противостоять рейдерству.

Это только часть применяемых тактических приёмов. Можно отметить и такие, как «ядовитые пилюли» («poison pills»), защита «белый сквайр» и другие[58].

[58] См. более подробно: Елонова Н.Ю.Слияния и поглощения: виды, причины, защитные тактики // Советник юриста. 2010. № 2. URL: http://www.s-yu.ru/articles/ 2010/2/ 4878.htmln (дата обращения: 22.09.2011).

9 Методы деликт-менеджмента

9.1 Стратегические методы управления деликтными рисками

В традиционной практике риск-менеджмента известны следующие стратегические методы управления рисками, которые могут с успехом использоваться при разработке деликт-менеджмента предприятия:

- избегание рисков или отказ от них;
- принятие рисков на себя;
- предотвращение убытков;
- уменьшение размеров убытка;
- страхование;
- самострахование;
- передача рисков другим субъектам;
- диверсификация и т.п.

Метод избегания деликтных рисков или отказа от них применяется тогда, когда выявляются крупные катастрофические деликтные риски, избежать которых иногда бывает невозможно. Одним из способов предотвращения их является создание таких финансово-хозяйственных условий, при которых шанс возникновения подобных деликтных рисков ничтожен.

Другим примером использования указанного метода является в одних случаях полное прекращение производства определённого вида продукции, в других — уход из сферы бизнеса, в котором присутствуют деликтные риски. Данный метод особенно эффективен, когда велики и вероятность возникновения убытков, и масса возможного убытка.

Избегание рисковых ситуаций как наилучшая альтернатива

применяется как к однородным и разнородным, так и к единичным или массовым деликтным рискам. Основной критерий здесь — размер возможного ущерба, который не должен достигать катастрофического порога.

Метод принятия деликтного риска на себя применяется, когда есть финансовые возможности противодействия им или покрытия убытков за счёт собственных средств организации. Используют данный метод, если вероятность наступления событий и величина потенциальных убытков от них невелики, и они могут быть покрыты за счёт текущего потока денежных поступлений, либо у организации имеются возможности противодействия, чтобы свести деликтные риски до минимального уровня.

Метод предотвращения убытков предполагает проведение предупредительных антиделиктных мероприятий, направленных на снижение вероятности наступления деликтных событий и массы риска. Применять этот метод целесообразно, когда вероятность реализации деликтного риска и наступления убытка достаточно велики, а размер потенциального ущерба небольшой. В противном случае целесообразен метод отказа от рисков (см. выше), применение которого оправдано, когда вероятность реализации деликтного риска и размер возможного ущерба высоки.

Метод предотвращения убытков применяется как к однородным, так и неоднородным деликтным рискам, которые могут носить как единичный, так и массовый характер. Этот метод управления деликтными рисками реализуется посредством разработки и внедрения программы превентивного деликт-менеджмента, методы которого должны контролироваться и периодически пересматриваться. Для выявления источников убытков и разработки программы превентив-

ных мероприятий предприятие обычно нанимает специалистов или создаёт собственные службы безопасности, поскольку разработка и реализация таких программ и мероприятий требует особых профессиональных знаний и навыков.

Безусловно, превентивные мероприятия значительно уменьшают частоту возникновения деликтных событий. Однако их применение обосновано тогда, когда затраты на их проведение существенно меньше выигрыша, обусловленного этими мероприятиями. Следует учесть, что превентивные меры могут оправдать себя лишь через длительное время, поэтому оценить этот выигрыш нелегко.

Применение данного метода связано с изменением функций персонала, в частности, с появлением дополнительных обязанностей сотрудников и структурных подразделений, которые в первую очередь обусловлены само́й спецификой превентивных мероприятий.

Метод уменьшения размера убытков применяется, когда все усилия по снижению деликтных рисков не приносят успеха, а исключить убытки полностью не представляется возможным. Суть метода состоит в планировании и проведении мероприятий, направленных на снижение размера возможного ущерба. Сфера целесообразного использования данного метода определяется больши́м размером возможного убытка и небольшой вероятностью реализации риска, то есть когда вероятность наступления убытка невелика. Если вероятность реализации риска высока, как и размер возможного ущерба, рациональнее использовать метод отказа или уклонения от риска.

К специфике применения данного способа, как и метода предотвращения убытков, относится необходимость разработки и реализации предупредительных программ и мероприятий, а также подбор источников покрытия вероятного ущерба.

Страхование — один из наиболее распространённых методов управления девиантным поведением и риском. Сущность данного метода управления заключается в снижении участия самой организации в возмещении ущерба за счёт передачи страховой компании ответственности по несению всего или части материального ущерба.

В экономической литературе даётся множество определений страхования как экономической категории. Дадим одно из них. «Как экономическая категория страхование представляет систему экономических отношений, включающую совокупность форм и методов формирования целевых фондов денежных средств и их использование на возмещение ущерба при различных рисках, а также на оказание помощи гражданам при наступлении определённых событий в их жизни. Оно выступает, с одной стороны, средством защиты бизнеса и благосостояния людей, а с другой — видом деятельности, приносящим доход»[59].

Использование страхования целесообразно, когда вероятность появления ущерба невысока, но размер возможного ущерба достаточно большой или вероятность появления ущерба высокая, но размер ущерба незначительный; страхование применяется независимо от степени однородности или неоднородности девиантного поведения граждан.

Страхование для предприятия представляет собой процесс цедирования[60] (процесс, связанный с передачей риска) деликтного риска, который может привести к критическим и катастрофическим

[59] Сильченкова Т.Н. Страхование как экономическая категория. URL: http://www.silchenkova.ru/st_ek_kateg/index.html (дата обращения: 02.11.2011).

[60] Для страховой компании это передача страхового риска в перестрахование Имеет место в правоотношениях между цедентом и цессионарием. Цедент – страховая компания, передающая риск в перестрахование, цессионарий (цессионер) – страховщик, принимающий риск в перестраховании.

последствиям для бизнеса. В случае критического риска возможны потери в сумме предполагаемой выручки по данной сделке. Катастрофический риск, как правило, приводит к потере всего имущества предприятия.

В большинстве случаев страхование лежит в основе программ по управлению девиантным поведением.

Страхование осуществляется на основе договоров имущественного или личного страхования. К имущественному страхованию относятся:

- риск утраты (гибели), недостачи или повреждения определённого имущества;
- риск ответственности по обязательствам, возникающим вследствие причинения вреда жизни, здоровью или имуществу других лиц (страхование ответственности за причинение вреда);
- риск ответственности за нарушение договоров в случаях, предусмотренных законодательством (страхование ответственности по договору);
- риск убытков от предпринимательской деятельности из-за нарушения своих обязательств контрагентами предпринимателя или изменения условий этой деятельности по независящим от предпринимателя обстоятельствам, в том числе неполучения ожидаемых доходов (страхование предпринимательского риска).

По договору имущественного страхования одна сторона (страховщик) обязуется за обусловленную договором плату (страховая премия) при наступлении предусмотренного в договоре события (страховой случай) возместить другой стороне (страхователь) или иному лицу, в пользу которого заключён договор (выгодоприобретатель), причинённые вследствие данного события убытки в застрахо-

ванном имуществе или убытки в связи с иными имущественными интересами страхователя (выплата страхового возмещения) в пределах определённой договором суммы (страховая сумма).

Страхователем может выступить как собственник имущества, так и обладатель иного вещного или обязательственного права на конкретное имущество (залогодержатель, арендатор, доверительный управляющий и т.д.). Разные заинтересованные лица могут иметь различные страховые интересы в отношении одного и того же имущества, и каждый из них может застраховать данное имущество в пределах своего интереса.

При заключении договора имущественного страхования между страхователем и страховщиком должно быть достигнуто соглашение:

- об определённом имуществе либо ином имущественном интересе, являющемся объектом страхования;
- о характере девиантного события, на случай наступления которого осуществляется страхование (страховой случай);
- о размере страховой суммы;
- о сроке действия договора.

При заключении договора страхования имущества или предпринимательского риска, страховая сумма не должна превышать их действительной стоимости (страховая стоимость). Такой стоимостью считается:

- для имущества — его действительная стоимость в месте его нахождения на момент заключения договора страхования;
- для предпринимательского риска — убытки от предпринимательской деятельности, которые страхователь мог бы понёсти при наступлении страхового случая.

Договор страхования вступает в силу в момент уплаты страхо-

вой премии или первого её взноса и распространяется на страховые случаи, происшедшие после вступления договора в законную силу.

Для обеспечения выполнения принятых страховых обязательств страховщики образуют из полученных страховых взносов необходимые для предстоящих страховых выплат страховые резервы по личному страхованию, имущественному страхованию и страхованию ответственности.

Страхование может и должно являться частью превентивного деликт-менеджмента. Оно сопровождается возникновением дополнительных функций управления, появление которых связано с использованием страхования как метода управления девиантными событиями, среди которых:

- сбор и изучение информации по девиантным событиям и полученным убыткам, определение вероятности реализации деликтных рисков (вероятности наступления ущерба) и размеров возможных убытков;
- выбор страховой компании, формы и вида страхования, условий страхования и т.д.;
- контроль за исполнением условий договора страхования.

Выполнение этих функций может быть возложено на специализированное структурное подразделение (например, службу экономической безопасности), либо финансовую службу. На малых предприятиях эти функции может выполнять непосредственно предприниматель.

Самострахование можно понимать двояко — и как метод принятия деликтного риска на себя, и как форму страхования, реализуемого в рамках данной организации или холдинга. Источниками самострахования являются собственные страховые фонды, либо резервы,

предназначенные для покрытия убытков от реализованных деликтных событий, аналогичных фондам страховых компаний.

В процессе самострахования целесообразно заранее создавать целевые фонды для покрытия возникающих убытков.

Преимуществами самострахования как метода управления девиантным поведением является усиление потенциала деликт-менеджмента, формирование превентивного механизма сокращения рисков и ускорение процедуры возмещения убытков.

Недостаток самострахования как метода управления девиантным поведением — необходимость создания штата компетентных специалистов, способных выполнять дополнительные функции аналогичные страховым компаниям.

Метод передачи деликтного риска другим субъектам означает, что одна сторона, подверженная риску возникновения убытков от деликтных событий, находит другого субъекта, который может принять на себя риск за страховую премию.

Основной способ передачи риска — через заключение контракта. Примером может служить аренда, когда часть рисков, связанных с арендованным имуществом, лежит на собственнике: полностью (например, риск физических повреждений собственности) или частично. Однако весомая часть рисков может быть передана путём специальных оговорок в договоре аренды. Согласно ст. 669 ГК РФ к арендатору полностью переходит риск случайной гибели и риск случайной порчи арендованного имущества в момент передачи ему этого имущества.

Диверсификация — процесс распределения вкладываемых средств между различными не связанными друг с другом объектами вложений с целью снижения риска.

9.2 Правовые способы защиты бизнеса от девиантного поведения

В процессе применения деликт-менеджмента хозяйствующим субъектом могут быть использованы следующие правовые способы защиты бизнеса — хеджирование, аренда, поручительство, доверительное управление имуществом, банковская гарантия и т.п.

Хеджирование — передача ценового риска при помощи торговых опционов, фьючерских и форвардных контрактов, направленная на его минимизацию. Хеджирование представляет собой систему мер, позволяющих исключить риски спекулятивных (финансовых) операций в результате неблагоприятных изменений курса иностранных валют, цен на товары, плавающих процентных ставок и т.д.

Хеджирование — одна из специфических форм страхования имущественных интересов. Оно является по своей сути передачей риска другому лицу. В отличие от традиционных методов страхования, хеджирование может не предусматривать выплату страховых взносов.

Например, хеджирование при помощи опционов предусматривает право (но не обязанность) страхователя за определённую плату приобрести конкретное количество иностранной валюты по фиксированному курсу в согласованный срок. При этом стоимость опциона (опционная премия) выступает в качестве аналога страхового взноса.

Сущность срочных валютных операций (форвардные, фьючерсные сделки) заключается в том, что стороны договариваются о поставке обусловленной суммы иностранной валюты через определённый срок после заключения сделки по курсу, зафиксированному в момент её заключения.

Об аренде мы ранее уже писали. Она позволяет арендатору пе-

редать деликтный риск (хищение и пр.) собственности её владельцу. По договору аренды (имущественного найма) арендодатель (наймодатель) обязуется предоставить арендатору (нанимателю) имущество за плату во временное пользование и распоряжение, создавая тем самым абсолютно-относительные вещные правоотношения.

Договор поручительства предусматривает передачу риска невыполнения обязательств первого участника перед вторым, третьему лицу — поручителю. По договору поручительства поручитель обязывается перед кредитором другого лица отвечать за исполнение последним его обязательства полностью или частично. Договор поручительства может быть заключён также для обеспечения обязательства, которое возникнет в будущем. При неисполнении или ненадлежащим исполнении должником обеспеченного поручительством обязательства поручитель и должник отвечают перед кредитором солидарно, если законом или договором поручительства не предусмотрена субсидиарная ответственность.

Доверительное управление имуществом предназначено для эффективного управления доверительным управляющим имущества собственника.

По договору доверительного управления имуществом одна сторона (учредитель управления) передаёт другой стороне (доверительному управляющему) на определённый срок имущество в доверительное управление, а другая сторона обязуется осуществлять управление этим имуществом в интересах учредителя управления, за определённое вознаграждение. Размер и форма вознаграждения позволяет минимизировать уровень девиантного поведения в процессе пользования и распоряжения имуществом собственника.

Банковская гарантия позволяет владельцу исключить негатив-

ные деликтные последствия для своего бизнеса, так как обеспечивает исполнение денежных обязательств. В силу банковской гарантии кредитное учреждение (гарант) дают по просьбе другого лица (принципала) письменное обязательство уплатить кредитору принципала (бенефициару) в соответствии с условиями даваемого гарантом обязательства денежную сумму по предоставлению бенефициаром письменного требования об её уплате.

Залог. Сущность залога состоит в том, что кредитор по обеспеченному залогом обязательству (залогодержатель), в случае неисполнения должником этого обязательства, имеет преимущественное перед другими кредиторами право получить удовлетворение из стоимости заложенного имущества.

При закладе залогодержатель, как правило, сохраняет за собой по отношению к заложенному имуществу все три правомочия: владение, пользование и распоряжение.

Удержание. Кредитор, у которого находится вещь, подлежащая передаче должнику, вправе в случае неисполнения должником в срок обязательства по оплате этой вещи или возмещению кредитору связанных с ней издержек и других убытков удерживать её до тех пор, пока соответствующее обязательство не будет исполнено.

Право удерживать вещь существует до момента исполнения соответствующего обязательства. По соглашению сторон срок для удержания вещи может быть сокращён. Принадлежащее кредитору требование удовлетворяется так же, как и право залогодержателя, то есть из стоимости вещи путём обращения взыскания и реализации её в установленном для предмета залога порядке. Кредитор может удерживать находящуюся у него вещь, несмотря на то, что после того, как эта вещь поступила во владение кредитора, права на неё приобретены

третьим лицом.

Задаток. Задатком признаётся денежная сумма, выдаваемая одной из договаривающихся сторон в счёт причитающихся с неё по договору платежей другой стороне, в доказательство заключения договора и в обеспечение его исполнения.

Задаток отличается от других способов защиты бизнеса тем, что сразу обеспечивает выполнение трёх функций:

- удостоверяющая — удостоверяет факт начала исполнения обязательства;
- обеспечительная — обеспечивает часть обязательства;
- платёжная — является формой платежа.

К специфике задатка относятся:

- обеспечение лишь тех обязательств, которые возникают из договоров;
- выполнение роли доказательства заключения договора;
- обеспечение лишь исполнения денежных обязательств.

Неустойка. Неустойкой признаётся определённая законодательством или договором денежная сумма, которую должник обязан уплатить кредитору в случае неисполнения или ненадлежащего исполнения обязательства, в частности, в случае просрочки исполнения.

Неустойка делится на два вида: пеня и штраф. Пеня устанавливается на случай просрочки исполнения и определяется в процентах по отношению к сумме обязательства, не исполненного в установленный срок. Она взыскивается непрерывно, нарастающим итогом. Штраф — неоднократно взыскиваемая неустойка. Иногда он устанавливается в твёрдой сумме, но обычно выражается в процентах или иной пропорции к определённой величине.

Предпочтение неустойки объясняется, как правило, тем, что

расчёт убытков может быть осложнён необходимостью доказать их размер, а неустойка определена заранее и не требует особых доказательств.

Уступка права требования. Право (требование), принадлежащее кредитору на основании обязательства, может быть передано им другому лицу по сделке (уступка права требования) или перейти к другому лицу на основании закона.

Для перехода к другому лицу прав кредитора не требуется согласие должника, если иное не предусмотрено законом или договором. Если должник не был письменно уведомлён о состоявшемся переходе прав кредитора к другому лицу, новый кредитор несёт риск вызванных этим для него неблагоприятных последствий.

Первоначальный кредитор, уступивший требование, отвечает перед новым кредитором за недействительность переданного ему требования, но не отвечает за неисполнение этого требования должником, кроме случая, когда первоначальный кредитор принял на себя поручительство за должника перед новым кредитором. Перевод должником своего долга на другое лицо допускается лишь с согласия кредитора.

Защита прав участников бизнес-отношений может также осуществляться следующими способами:

• признания права как средства защиты, которое реализуется в юрисдикционном (судебном) порядке. Требование истца о признании права обращено не к ответчику, а к суду, который должен официально подтвердить наличие или отсутствие у истца спорного права;

• восстановление положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения. Восстановление положения, существовавшего до

нарушения права, может происходить посредством применения как юрисдикционного так и не юрисдикционного порядка защиты;

• признания оспоримой сделки недействительной и применения последствий её недействительности, применения последствий недействительности ничтожной сделки. Данный способ защиты нарушенных прав представляет собой восстановление положения, существовавшего до нарушения права (реституция);

• признания недействительным акта государственного органа или органа местного самоуправления. Это предполагает, что юридическое лицо, охраняемые законом интересы которого нарушены изданием не соответствующего закону или иным правовым актам административного акта, имеет право на их обжалование в суде;

• самозащиты прав, связанных с пресечением действий, нарушающих право либо создающих угрозу его нарушения;

• прекращения или изменения правоотношений. Чаще всего данный способ защиты реализуется в юрисдикционном порядке, так как связан с принудительным прекращением или изменением правоотношения;

• неприменения судом акта государственного органа или органа местного самоуправления, противоречащего закону. Указанная мера распространяется как на индивидуально-правовые, так и нормативные акты государственных органов и органов местного самоуправления, которые не соответствуют вышестоящим источникам права.

Защиту нарушенных или оспоренных гражданских прав осуществляет в соответствии с подведомственностью дел суд, арбитражный или третейский суды, а в некоторых случаях, предусмотренных законом, — орган исполнительной власти и управления в административном порядке.

Целью макроэкономического управления девиантным поведением является снижение общих потерь бизнеса, связанных с возможной реализацией антиделиктной программы в рамках деликтменеджмента на уровне предпринимательской организации. Достижению этой цели способствует использование таких методов макроэкономического управления деликтными рисками как инициирование на уровне государства законов, указов, постановлений, нормативных актов, предписаний.

Целью микроэкономического управления девиантным поведением является минимизация возможных убытков на уровне конкретной организации. Достижению этой цели способствует использование тех методов микроэкономического управления антиделиктной программой, которые решают данную задачу. Примером может быть уже апробированное введение законодательных мер в период мирового экономического кризиса по выдаче кредитов и займов для компенсации убытков и восстановления производства.

Государственные методы могут реализовываться посредством различных специальных программ, в частности, через программы социального страхования и программы, реализующие коллективную помощь.

10 Правовая основа безопасности бизнеса

10.1 Состав правовой основы безопасности

Правовая основа безопасности бизнеса является фундаментальной частью правового регулирования экономической и информационной безопасности предпринимательства, осуществляемого государственными органами власти и управления, общественными и коммерческими организациями, индивидуальными предпринимателями и т.д.

Российское законодательство понимает под источником права государственную волю, выраженную в правовом акте компетентного государственного органа, то есть источник права — это форма выражения права.

Правовыми актами безопасности российского предпринимательства являются:

• Конституция Российской Федерации как основной источник всей системы права.

• Федеральные конституционные законы Российской Федерации, определяющие основные начала государственного и общественного строя, правовое положение личности и организаций, на основе которых выстраивается и детализируется вся система нормативно-правовых актов.

• Федеральные законы, принимаемые и действующие в строгом соответствии с федеральным конституционным законом, регламентирующие определённые и ограниченные сферы общественной жизни.

• Указы и распоряжения Президента РФ, издаваемые в дополнение или развитие законов, а при необходимости — оперативного установления правовых норм.

• Постановления и распоряжения Правительства РФ, издавае-

мые в пределах его компетенции в развитие и исполнение законов.

• Акты министерств и ведомств, направленные на исполнение законов, Указов Президента РФ и постановлений Правительства РФ.

• Акты региональных органов власти и управления, издаваемые в пределах их компетенции в соответствии с разграничением полномочий между Российской Федерацией и субъектами Российской Федерации.

• Правовые акты местных органов власти и управления, имеющие хозяйственно-правовое содержание по обеспечению безопасности бизнеса.

• Технические регламенты на продукцию, процессы производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнение работ и оказание услуг

• Приказы и распоряжения руководства хозяйствующего субъекта.

В правовой системе действует принцип непротиворечивости. Он предполагает, что правовые акты органов власти и управления нижестоящего уровня не должны противоречить соответствующим правовым актам вышестоящего уровня.

Отметим, что во внешнеэкономической коммерческой деятельности источниками права являются также правовые акты тех государств, на территории которых российские предприниматели осуществляют коммерческую деятельность, и международные правовые акты. Например, возможность применения торгового обычая зафиксирована в различных арбитражных регламентах, в том числе в Регламенте Международного коммерческого арбитражного суда при Торгово-промышленной палате РФ, в Арбитражном регламенте Европейской экономической комиссии ООН и Арбитражном регламенте Ко-

миссии ООН по праву международной торговли.

Правовую основу безопасности бизнеса составляют группы нормативно-правовых блоков. К основным из них можно отнести:

А. К первой группе следует отнести блок, который формирует основополагающие (фундаментальные) правовые источники регулирования функционирования в области обеспечения безопасности личности, общества, государства.

К указанным источникам относится Конституция Российской Федерации**,** применяемая на всей территории России и имеющей непосредственное отношение к защите предпринимательской деятельности. Так, глава 2 включает в себя основные положения, составляющие основы правового статуса личности в Российской Федерации, основные права и свободы человека и гражданина. В соответствии с ч. 1, ст. 46 каждому гражданину гарантируется судебная, экономическая и информационная безопасность его прав и свобод. Указанные права и свободы могут быть ограничены только в той мере (ч. 3, ст. 55), в какой это необходимо в целях экономической и информационной безопасности основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

В соответствии с Законом «О безопасности» с целью создания и поддержания необходимого уровня защищённости объектов безопасности в России разрабатывается система правовых норм, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления, формируются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью. Для непосредственного выполнения функций по обеспечению безопасности личности, общества и

государства в системе исполнительной власти в соответствии с законом образуются государственные органы обеспечения безопасности.

Уголовный кодекс Российской Федерации даёт определение законодательных моделей общественно-опасных противоправных деяний — их конкретные составы, имеющие значение для экономической и информационной безопасности бизнеса. Своевременное определение признаков состава преступления позволяет предпринимателю, с одной стороны, самому проводить комплекс превентивных мер по минимизации деликтов, а с другой, — обоснованно обращаться с заявлениями в правоохранительные и иные государственные органы управления.

Вторая группа источников формируется из законодательных актов, регулирующих предпринимательскую деятельность, связанную с экономической и информационной защитой бизнеса.

К данному правовому источнику можно отнести Гражданский кодекс Российской Федерации. В частности, гражданское законодательство регулирует отношения между лицами, осуществляющими предпринимательскую деятельность или с их участием. Данные виды правоотношений формируются на основе гражданского права.

Гражданское право — такая отрасль права, нормы которой регулируют товарно-денежные отношения и связанные с ним личные неимущественные отношения. Гражданское законодательство основывается на признании равенства прав участников регулируемых им отношений, неприкосновенности собственности, свободы договора, недопустимости вмешательства кого-либо в частные дела, необходимости беспрепятственного осуществления гражданских прав, обеспечения восстановления нарушенных прав, их судебной защиты. Оно определяет правовое положение участников хозяйственного оборота,

основания возникновения и порядок осуществления права собственности и других вещных прав, регулирует договорные и иные обязательства.

Гражданское право использует, помимо законодательных актов, обычаи делового оборота, аналогии законов и аналогии права, что расширяет возможности формирования альтернативных хозяйственных правоотношений. При этом предметом хозяйственного права являются в основном макроэкономические отношения (инвестиции, ценообразование, монополистическая, эмиссионная деятельность и т.п.). Бóльшая часть хозяйственных отношений урегулирована специальным законодательством, базирующемся на публично-правовых, а не частно-правовых началах (регистрация, лицензирование, сертификация, предписания, запреты, рекомендации)[61].

Закон РФ от 27 июля 2010 г. № 193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)» определил альтернативную процедуру урегулирования хозяйственных споров с участием в качестве посредника независимого лица, который носит название — «медиатор». Посредством медиации указанный закон допускает возможность разрешения споров, возникающие из гражданских правоотношений, из предпринимательской и иной экономической деятельности. Процедура медиации позволила значительно расширить спектр правовых способов разрешения споров, возникающих между хозяйствующими субъектами.

В России существует проблема защиты интеллектуальной собственности. В начале мая 2011 г. торговый представитель США Рон Кирк выступил с заявлением о том, что Россия и Китай попали в число 12 стран, в которых в недостаточной степени соблюдаются права

[61] Дойников И.В. Введение в хозяйственное (предпринимательское) право: учебное пособие. М., 2006. С. 41–43.

на интеллектуальную собственность. Британская корпорация BBC утверждает, что РФ попадает в этот список уже 14 год подряд, КНР — седьмой. Подобное упоминание не влечёт для стран никаких санкций, но напоминает правительствам этих стран, что проблема интеллектуального пиратства существует и требует активнее бороться с ней[62].

24 мая 2011 г. Д.А. Медведев подписал Указ о создании новой Федеральной Службы по интеллектуальной собственности в системе государственной власти РФ. Указ направлен на создание единого целостного и одновременно эффективного механизма для распоряжения правами России на результаты интеллектуальной деятельности и их обязательной защиты путём чёткого распределения функций всех федеральных органов исполнительной власти. При этом на неё будут возложены функции по контролю и надзору в сфере правовой охраны и использования результатов интеллектуальной деятельности, в том числе, гражданского, военного, специального и двойного назначения, которые созданы за счёт средств федерального бюджета.

Данный Указ предусматривает признание утратившим силу Указ Президента РФ от 14 мая 1998 года № 556 «О правовой защите результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального и двойного назначения», по которому функции по правовой защите интересов государства в процессе экономического и гражданско-правового оборота результатов научно-исследовательских, опытно-конструкторских и технологических работ военного, специального и двойного назначения были возложены на Министерство юстиции РФ.

Ранее, в апреле 2011 г., Д.А. Медведев поручил рассмотреть вопрос о создании в России специального суда по интеллектуальным

[62] URL: http://intellect-patent.ru/news/1274/ (дата обращения: 02.11.2011).

правам. Президент отметил, что суд по интеллектуальным правам должен быть создан в рамках системы арбитражных судов в наукограде «Сколково». Проект закона о создании в РФ суда по интеллектуальным правам был внесён Высшим арбитражным судом (ВАС) в Госдуму ещё в октябре 2010 года. Создание специализированного суда обусловлено значительным ростом в РФ количества споров, связанных непосредственно с интеллектуальной собственностью.

Предложение Президента РФ, направленное на создание суда по интеллектуальным правам, позволит более оперативно и качественно разбираться с фактами незаконного использования интеллектуальной собственности.

Третья группа источников включает в себя законодательные и иные нормативно-правовые документы, регулирующие непосредственную защиту бизнеса.

К данной группе можно отнести Закон РФ «О частной детективной и охранной деятельности». В законе частная и охранная деятельность рассматривается как оказание на возмездной и безвозмездной договорной основе таких услуг, которые обеспечивают экономическую и информационную безопасность законных прав и интересов своих клиентов.

Основная часть оказания услуг относится к процессу возмещения ущерба, нанесённого вследствие криминальной конкуренции, и локализации его последствий. Только несколько видов услуг (обзор и анализ рынка, сбор информации для переговоров с клиентами, выяснение характеризующих личность данных) ориентированы на предупреждение возможного ущерба.

Закон РФ об «Оперативно-розыскной деятельности» позволяет проводить силами службы экономической безопасности комплекс ме-

роприятий, не ограничивающий конституционные права граждан. К их числу можно отнести:

• сбор и анализ информации гражданского и уголовно-правового характера по вопросам защиты от противоправных посягательств;

• консультирование населения по вопросам, связанным с утратой имущества и пропавших без вести физических лиц;

• физическую охрану граждан, имущества и помещений физических и юридических лиц;

• обеспечение безопасности перевозки денежных средств и ценных грузов (ценных бумаг, драгоценных металлов и пр.);

• обеспечение безопасности при проведении массовых мероприятий и деловых встреч.

Арбитражное процессуальное право определяет порядок разрешения арбитражным судом хозяйственных споров, права и обязанности органов правосудия, истцов, ответчиков и иных участников арбитражного процесса. В соответствии с РФ арбитражному суду подведомственны дела по экономическим спорам и другие дела, связанные с осуществлением предпринимательской или иной экономической деятельности, с участием юридических лиц и предпринимателей-физических лиц, а в случаях, предусмотренных законом, с участием иных организаций и органов государственной власти. В 2009 году в законодательстве было закреплено понятие «корпоративный спор» (а надо бы ещё определиться с понятием «экономический спор») и все корпоративные споры, независимо от состава участников спорных правоотношений, отнесены к ведению арбитражных судов. В 2010 году дальнейшее развитие получили положения о подведомственности дел об оспаривании нормативных правовых актов, регули-

рующих отношения в различных областях экономики.

Суды общей юрисдикции рассматривают дела по защите прав и интересов бизнеса в случае, если дело возникло не в связи с осуществлением предпринимательской деятельности или если хотя бы одной из сторон спора является физическое лицо, не имеющее статус предпринимателя.

Постоянно действующие третейские суды образуются торговыми палатами, биржами, общественными объединениями предпринимателей и потребителей, иными организациями-юридическими лицами, созданными в соответствии с законодательством РФ, и их объединениями (ассоциациями, союзами), и действуют при этих организациях-юридических лицах. Третейский суд не рассматривает споры, вытекающие из публично-правовых отношений, и они не входят в судебную систему РФ.

В Хабаровске действует третейский суд при Дальневосточном объединении промышленников и предпринимателей (ДВОПП)[63]. Один из авторов данной монографии (проф. Рожков Ю.В.) длительное время является членом такого суда.

Международный коммерческий арбитражный суд (МКАС) является разновидностью третейского суда. Рассмотрение спора в МКАС возможно лишь при наличии письменного соглашения об этом между сторонами или в силу международного договора. К процедуре производства дел в МКАС применяется российское право.

К функциям непосредственной защиты предпринимательства целесообразно отнести большой массив ведомственных нормативных актов, касающихся экономической и информационной безопасности интеллектуальной собственности и коммерческой тайны.

---

[63]URL: http://dvop.ru/index.php/aboutus/2010-10-03-02-16-07/293-2010-10-03-02-15-46.

В частности, к ним можно отнести дополнение к трудовому договору, призванного нести персональную ответственность сотрудника за деликтную деятельность принимаемого на работу кандидата по рекомендации (поручительству). Составление письменного обязательства сотрудника о неразглашении коммерческой тайны в период трудовых отношений с предприятием (его правопреемником) и в течение определённого срока и т.д.

10.2 Недостатки существующей правовой базы безопасности бизнеса

Российские реалии таковы, что наметилась тенденция к детализации законодательства и по предпринимательской деятельности, и по защите бизнеса. Однако эта тенденция не имеет пока поступательного движения. Поэтому правовая база экономической и информационной безопасности бизнеса обладает недостатками. К ним можно отнести:

1. Существует рассредоточение правовых норм, регламентирующих формы и способы защиты бизнеса, по нормативно-правовым актам различного уровня, что затрудняет практическое их использование.

2. Ряд правовых норм можно толковать по-разному, а это порождает экономическую преступность в бизнес-сфере и коррупцию в органах государственного управления.

3. Экономическая и информационная безопасность бизнеса обеспечивается в основном использованием ведомственных нормативных актов.

4. В правовом отношении не урегулированы вопросы взаимодействия предпринимательских структур с правоохранительными ор-

ганами в целях превентивного обеспечения экономической и информационной безопасности бизнеса.

5. Обеспечение экономической и информационной безопасности бизнеса не носит превентивного характера, ибо не урегулированы правовые вопросы взаимодействия предпринимательских структур с системой правоохранительных органов.

6. Ряд поправок, внесённых в Уголовный кодекс РФ за экономические преступления, бесполезны, ибо они не отражают реальную социальную и криминологическую ситуацию в стране.

7. Судебная система, как отмечают многие юристы, превратилась в замкнутую корпорацию, в особую «касту», которая пока мало приспособлена к самоочищению. Это приводит к серьёзным нарушениям, которые в свою очередь через прецеденты ведут к искажению судебной практики. Отметим, что недавно Европейский союз признал, что неправосудное решение приравнивается к пытке[64].

8. Огромная нагрузка на судей по рассматриваемым искам, что в свою очередь приводит к некачественному рассмотрению имущественных споров.

9. Отсутствие специализированных комплексных федеральных законов «О борьбе с организованной преступностью», «О противодействии коррупции», «О борьбе с теневой экономикой», недостатки в Федеральном законе от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём» не позволяет эффективно развивать экономическую систему.

10. На законодательном уровне не определены понятия, как мы уже отмечали выше, «экономический спор», «экономическая деятельность», что в свою очередь отрицательно сказывается на определении

[64] URL: http://www.rg.ru/2011/06/09/lukyanova.html (дата обращения: 17.08.2011).

компетенции арбитражных судов.

11. Высокий уровень налоговых платежей вынуждает предпринимателей занижать прибыль, «выдавливает» их из цивилизованных экономических рамок в теневой бизнес.

При разработке нормативно-правового акта на государственном уровне целесообразно исходить из:

• необходимости формирования такой системы экономической и информационной безопасности, которая соответствует цивилизованному бизнесу, требованиям законодательства и корпоративной этики;

• системного, комплексного характера управления защитой предпринимательства;

• необходимости разумного сочетания мер экономической и информационной безопасности, осуществляемых конкретным хозяйствующим субъектом и реализуемых на государственном уровне;

• признания ведущей роли государства по формированию системы управления экономической и информационной безопасностью предпринимательства;

• обеспечения права предпринимателей на защиту бизнеса с помощью государства.

Структурная политика в области защиты бизнеса предполагает решение задач высокоэффективного и качественного обеспечения безопасности бизнеса на базе формирования развитой инфраструктуры, которая будет ориентирована на обеспечение комплексной безопасности.

Социальная политика должна быть направлена на сокращение безработицы, рост благосостояния людей, всестороннюю поддержку малого и среднего предпринимательства.

Экономическая политика должна стимулировать управление организацией не только административными, но и экономическими методами, мотивировать персонал на использование в своей профессиональной деятельности приёмов безопасного бизнеса.

Информационная политика должна строиться на основе формирования позитивного общественного мнения по отношению к предпринимательству. Важно обеспечить эффективность пропаганды профессиональной этики делового бизнеса, государственный контроль за процессами накопления, хранения и использования баз данных социально-экономического характера.

Если говорить о кадровой политике, то её необходимо направить на недопущение проникновения в трудовые коллективы бизнес-структур граждан, имеющих деликтные наклонности.

Правовая политика должна базироваться на основе создания развитой законодательной базы экономической и информационной безопасности бизнеса.

Контроль государства за соблюдением законодательства в области экономико-информационной безопасности бизнеса должны осуществлять в соответствии со своими полномочиями органы законодательной, исполнительной и судебной ветвей власти государства. Государственная политика в этой сфере должна быть направлена на:

• создание и развитие федерального и регионального механизмов защиты бизнеса, обеспечивающих их взаимодействие в едином экономическом пространстве;

• защиту и сохранение ресурса предпринимательства как национального достояния;

• обеспечение интересов общегосударственной безопасности в сфере конкретного бизнеса;

• применение единой трактовки российских государственных стандартов защиты бизнеса, их соответствие международным рекомендациям и требованиям;

• формирование государственной, инвестиционной, экономической, социальной, структурной, информационной, кадровой политики в сфере защиты бизнеса на основе использования мирового опыта развития соответствующих институтов;

• поддержку российских и международных проектов, обеспечивающих развитие механизма управления экономической безопасностью бизнеса.

Координацию работы по реализации государственной политики в области экономической и информационной безопасности бизнеса целесообразно осуществлять аппарату Президента Российской Федерации. В соответствии с направлениями общегосударственной политики должны создаваться соответствующие правомочные органы субъектов Российской Федерации с привлечением профессионалов в области экономики, права и других наук.

Заключение

Одним из важнейших условий становления демократического государства является развитие и эффективное применение знаний в области экономической и информационной безопасности бизнеса топ-менеджерами организаций.

Реалии российской действительности свидетельствуют о том, что необходимо создавать систему экономической безопасности бизнеса, обеспечивающую защищённость жизненно важных интересов физических и юридических лиц, предпринимательства от недобросовестной конкуренции, противоправной деятельности, деликтного поведения криминальных группировок и отдельных граждан.

Способность противостоять внешним и внутренним угрозам, сохранять стабильность функционирования и развития бизнеса предопределяется формированием такой системы безопасности, которая может стать гарантом защищённости жизненно важных интересов личности, общества и государства.

Основная цель системы экономической безопасности состоит в обеспечении устойчивого функционирования организации и предотвращение угроз её безопасности, защиты законных интересов предпринимателей от деликтных посягательств, охраны жизни и здоровья персонала, недопущения хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утраты, искажения и уничтожения коммерческой информации, нарушения работы технических средств, обеспечения производственной деятельности.

Концепция экономической безопасности бизнеса предполагает прямую связь с формированием целостного представления о системе безопасности бизнеса, а взаимоувязывание различных элементов этой

системы определяет пути реализации мероприятий, обеспечивающих необходимый уровень надёжной защищённости предпринимательства.

Эффективная система экономической безопасности повышает имидж предпринимательской структуры, обеспечивает прирост прибыли за счёт обеспечения высокого качества предоставляемых услуг по защите бизнеса и гарантий его безопасности.

В монографии рассмотрены цели и задачи системы экономической безопасности, принципы её организации, функционирования и правовые основы, виды угроз безопасности и ресурсы, подлежащие защите, а также основные направления разработки системы безопасности, включая правовую, организационную, инженерно-техническую и иные виды защит.

Действующие в настоящее время и разрабатываемые нормативно-правовые акты предусматривают право организации на выработку собственной концепции системы безопасности и создания соответствующей службы как системы исполнительных органов, реализующей данную концепцию. Федеральный закон РФ от 28 декабря 2010 г. № 390-ФЗ «О безопасности», который заменил аналогичный закон 1992 года, определил основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации.

Список использованных источников

1 Конституция Российской Федерации. М.: Юрлит, 2000.

2 Гражданский кодекс Российской Федерации. М.: Экзамен, 2004.

3 Уголовный кодекс Российской Федерации. М.: Элит, 2004.

4 Федеральный Закон «О государственной тайне». URL: http:// base.garant.ru/10102673.

5 Федеральный закон «О частной детективной и охранной деятельности в Российской Федерации». URL: http://base.consultant.ru/cons/cgi/ online.cgi?req=doc;base=LAW;n=110221.

6 Астахов П.А. Противодействие рейдерским захватам. М.: Эксмо, 2008.

7 Глущенко Е.Н., Дроздовская Л.П., Рожков Ю.В. Финансовое посредничество коммерческих банков. Хабаровск: РИЦ ХГАЭП, 2011. URL: http://www.fin-econ.ru/4r.htm.

8 Гончаренко Л.П. Управление безопасностью: учебное пособие. М.: КНОРУС, 2009.

9 Доценко Д.В., Круглов В.Н. Социально-экономическая сущность понятия «экономическая безопасность» // Аудит и финансовый анализ. 2009. № 4.

10 Захаров О.Ю. Практическая секьюритология. Ростов-на-Дону: Феникс, 2010.

11 Ващекин Н.П. Безопасность предпринимательской деятельности. М.: Экономика, 2002.

12 Вихорев С., Соколов А. Как оценить угрозы безопасности корпоративной формации // Connect. 2000. № 12.

13 Волков В.В. Силовое предпринимательство в современной России // Экономическая социология. 2002. Т. 3. № 1.

14 Гончаренко Л.П. Процесс обеспечения экономической безопасности предприятия // Справочник экономиста. 2004. № 12.

15 Гусев В.С. Экономика и организация безопасности хозяйствующих субъектов. СПб.: Питер, 2004.

16 Дойников И.В. Предпринимательское (хозяйственное) право: учебное пособие. М.: Брандес, 1997.

17 Доронин А.И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия. Тула: Гриф и К, 2000.

18 Елонова Н.Ю. Слияния и поглощения: виды, причины, защитные

тактики // Советник юриста. 2010. № 2. URL: http://www.s-yu.ru/articles/ 2010/2/ 4878.htmln.

19 Захаров О.Ю. Обеспечение комплексной безопасности предпринимательской деятельности: теория и практика. М.: АСТ, Астрель, 2008.

20 Иванов Ю.В. Слияние, поглощение и разделение компаний: стратегия и тактика трансформации бизнеса. М.: Альгаша Паблишер, 2004.

21 Ионцев М.Г. Корпоративные захваты: слияния, поглощения, гринмэйл. М.: Ось-89, 2006.

22 Кадровая безопасность. Центр правовых инноваций [сайт]. URL: http://www.cpisb.com/business/security/personnel.

23 Климов В. Промышленный шпионаж как основа грязных информационных технологий и современных информационных войн // Мир и безопасность. 2002. № 3.

24 Корнилов М.Я. Экономическая безопасность России. М.: РАГС, 2007.

25 Котляр Э. Гринмейл: русская версия // Консультант. 2005. № 5.

26 Круглова Н.Ю. Хозяйственное право. М.: РДЛ, 2004.

27 Курносов Ю.В. Аналитика: методология, технология и организация информационно-аналитической работы. М.: РУСАКИ, 2004.

28 Малашихина Н.Н. Риск-менеджмент: учебное пособие. Ростов-на-Дону: «Феникс», 2004.

29 Митрофанов А.А. Экономическая безопасность коммерческих предприятий и деловая разведка. URL: http://www.rscip.ru/base/A9738409-3441822.html.

30 Нежданов И.Ю. Проверка благонадёжности юридического лица. URL: http://www.it2b.ru/blog/arhiv/672.html.

31 Одинцов А.А. Экономическая и информационная безопасность предпринимательства. М.: Академия, 2008.

32 Полуэктов А.А. Новые методы оценки компаний в сделках слияния и поглощения. М.: МАКС-Пресс, 2004.

33 Проценко А.Н. Об основных принципах и механизмах управления региональной безопасностью. URL: http://www.dex.ru/riskjournal/2006 /2006_3_3/256-292.pdf.

34 Рожков Ю.В., Дроздовская Л.П. О массе риска как инструменте банковского риск-менеджмента // Банковское дело. 2010. № 7.

35 Рожков Ю.В., Дроздовская Л.П. Финансовые «пузыри» и масса риска // Финансы и кредит. 2010. № 46.

36 Сильченкова Т.Н. Страхование как экономическая категория.

URL: http:// www.silchenkova.ru/st_ek_kateg/index.html.

37 Смольянинова М.В. Могут ли коммерческие организации использовать гриф «ДСП»? Институт проблем предпринимательства: [сайт]. URL: http://www. ippnou.ru/article.php?idarticle=007218.

38 Соловьёв Э.Я. Коммерческая тайна и её защита. М.: Дрофа, 2001.

39 Старинов Г.П. Деликтные риски организаций: идентификация, диагностика и управление: на примере предприятий Хабаровского края. Дисс. … канд. экон. наук: 08.00.05. Хабаровск, 2009.

40 Старинов Г.П., Абраменко Н.Н. Девиантость каперских рисков в системе экономической безопасности. В кн: Формирование модели новой экономики России: теория и практика. Краснодар, 2010.

41 Центр правовых инноваций. Системная безопасность [сайт]. URL: http:// cpisb.com/business/competitive-intelligence/requirement.

42 Усанов Г.И., Старинов Г.П. Деликтные риски организаций: идентификация, диагностика и управление / Учёные записки Комсомольского-на-Амуре государственного технического университета. 2010. № 1–2.

43 Фёдорова А.Э. Экономический терроризм: тяжелые болезни российского бизнеса // Безопасность, менеджмент, бизнес. 2009. № 1–2.

44 Шаваев А.Г. Система борьбы с экономической разведкой. М.: Правовое просвещение, 2000.

45 Шаповалов П.П. Коммерческий технический шпионаж и пути его нейтрализации. М.: Щит, 1999.

46 Шлубков Д. Особенности корпоративного управления в России. М.: Альпина, 2005.

47 Шнайдер Б. Секреты и ложь. Безопасность данных в цифровом мире. СПб.: Питер, 2003.

48 Шпак В.Ф. Методологические основы обеспечения информационной безопасности объекта // Конфидент. 2000. № 1.

49 Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004.

50 Шутов В.С., Васин С.М. Управление рисками на предприятии: учебное пособие. М.: КНОРУС, 2010.

51 Энциклопедия деловой разведки и контрразведки. М.: Русь-Олимп, 2007.

52 Юданов А.Ю. Конкуренция: теория и практика. 3-е изд. М.: ЭКМОС, 2001.

53 Ярочкин В.И. и Бузанова Я.В. Основы безопасности бизнеса и предпринимательства. М.: Академический Проект: Фонд «Мир», 2005.

54 Яскевич В.И. Секьюрити: Организационные основы безопасности фирмы. М.: «Ось-89», 2005.

55 URL: http://www.academy-go.ru/Site/EconomEtica/Seminar/KDP.shtml).

56 URL: http:// www.bre.ru/security/53.html.

57 URL: http:// www.intellect-patent.ru/news/1274/.

58 URL: http://www.intalev. ru/agregator/press/id_8917.

59 URL: http://www.gortranscom.ru/bookinfo-baryshnikova-lp/baryshnikova-lp-ek-onomika-pidpriyemstva-navchalniy-posibnik-razdel-4.html?start=77.

60 URL: http:// www.library.tuit.uz/skanir_knigi/book/informasionnaya_bezopasnost/in-for_bezopas_1.htm.

61 URL: http://www.slovari.yandex.ru.

62 URL: http:// www.parolesdici.net/content/view/7/9.

63 URL: http://www.cpisb.com/business/security/personnel.

64 URL: http://newasp.omskreg.ru/bekryash/ch7p2.htm.

65 URL: http://www.ropnet.ru/info/articles/20.php.

66 URL: http:// www.library.tuit.uz/skanir_knigi/book/informasionnaya_bezopasnost/ infor_bezopas_1.htm.

67 URL: http://www.hr-portal.ru/tool/otsenochnyi-list-sotrudnika-proshedshego-is pytatelnyi-srok.

68 URL:http:// www.lenta.ru/news/2011/07/08/spionage.

69 URL: http://www.bre.ru/security/10345.html.

70 URL: http://www.e-lib.info/book.php?id=112100022&p=12.

71 URL: http://www.standards.narod.ru/gosts/other/51241-98.htm.

72 URL: http:// www.bre.ru/security/17838.html.

73 URL: http:// www.daily.sec.ru/publication.cfm?pid=.

74 URL: http://www.city-n.ru/view/91843.html.

75 URL: http://www.mosuruslugi.ru/consultation/q/230.

76 URL: http://www.apkit.ru/committees/defence/news/aticles/article2.php.

77 URL: http://www.dvop.ru/index.php/aboutus/2010-10-03-02-16-07/293-2010-10-03-02-15-46.

78 URL: http://www.rg.ru/2011/06/09/lukyanova.html.

Научное издание

Плесовских Юрий Гертурович
Рожков Юрий Владимирович
Старинов Геннадий Петрович

Деликт-менеджмент как фактор экономической безопасности бизнеса

Печатается в авторской редакции
с готового оригинал пакета

Подписано к печати 30.11.2011 Формат 60х84/16 Бумага писчая
Печать офсетная. Усл. печ.л. 12,8. Уч.-изд.л. 9,2. Тираж 700 экз. Заказ № 619.

Редакционно-издательский центр ХГАЭП
680042, Хабаровск, ул. Тихоокеанская, 134