Алексей Гладкий

ОБМАН И ПРОВОКАЦИИ В МАЛОМ И СРЕДНЕМ БИЗНЕСЕ

- Детальное описание схем и методов обмана
- Нейтрализация опасности и меры по спасению бизнеса
- Большое количество конкретных примеров
- Практические рекомендации и полезные советы
- Легкий, доступный стиль изложения

bhv®

Алексей Гладкий

ОБМАН И ПРОВОКАЦИИ В МАЛОМ И СРЕДНЕМ БИЗНЕСЕ

Санкт-Петербург
«БХВ-Петербург»
2013

УДК 65.012
ББК 65.290
Г52

Гладкий А. А.

Г52 Обман и провокации в малом и среднем бизнесе. — СПб.: БХВ-Петербург, 2013. — 192 с.: ил.

ISBN 978-5-9775-0814-8

Книга адресована представителям малого и среднего бизнеса, работающим в России и странах бывшего СССР. В ней анализируются криминальные схемы и методы, представляющие серьезную опасность для любого бизнеса и его владельца. Раскрыто коварство многих используемых приемов и способов, основанных на том, что бизнесмен узнает о случившемся слишком поздно — когда предпринимать что-либо уже бесполезно. Поэтому, наряду с анализом криминальных схем (мошенничество, рейдерство и т. п.), в книге даются ценные советы, конкретные рекомендации и прямые руководства к действию, позволяющие вовремя нейтрализовать опасность и спасти бизнес.

Для широкого круга читателей

УДК 65.012
ББК 65.290

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Екатерина Капалыгина*
Редактор	*Елена Васильева*
Компьютерная верстка	*Людмилы Чесноковой*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Марины Дамбиевой*

Подписано в печать 31.05.13.
Формат 60×90$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 12.
Тираж 1500 экз. Заказ №
«БХВ-Петербург», 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография «Наука»
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-0814-8

Оглавление

Введение

Не секрет, что в современной России предпринимательство — это опасная сфера деятельности, и чем крупнее и мощнее бизнес, чем больше скорость, с которой вращаются деньги и совершают возвратно-поступательные движения товары, тем больше он таит в себе угроз. Многие сложности появляются извне и непосредственно связаны с конфликтными ситуациями, рейдерством, недобросовестной конкуренцией или просто с привычной коррупцией чиновников. Однако не меньше проблем скрыто и внутри бизнеса: это могут быть корыстные побуждения, воровство или просто халатность персонала и т. п.

Поскольку возможных неприятностей и опасностей в бизнесе существует немало, как следует подготовиться к каждой из них нереально. Абсолютной безопасности не бывает, но примерно оценить возможность возникновения той или иной проблемы, а также вероятный от нее ущерб относительно легко можно в любой компании.

В зависимости от вида деятельности и специфики нынешней ситуации субъекты хозяйствования могут подвергаться типовым угрозам. В частности, фирма, работающая в сфере IT-технологий, — это возможная жертва хищения интеллектуальной собственности, а компания, располагающая и не достаточно эффективно эксплуатирующая дорогостоящие и ликвидные активы, — вероятная жертва недружественного поглощения.

Данная книга представляет собой своеобразное «Руководство по противостоянию обманам, “подставам” и провокациям». Она поможет вам избежать многих неприятностей, сэкономив тем самым немало ваших денег и нервов.

При изучении этой книги помните, что все совпадения являются случайными, а рассматриваемые примеры носят условный характер.

Глава 1

Чего больше всего опасаются мелкие и средние бизнесмены?

Результаты проведенных исследований показывают: преимущественная часть опрошенных бизнесменов опасается того, что их компания тем или иным образом будет подчинена сторонним юридическим или физическим лицам, которые будут получать прибыль от деятельности «закабаленного» предприятия.

Также предприниматели серьезно опасаются «наездов» со стороны налоговых и фискальных органов. Не секрет, что даже не самая тщательная проверка любого предприятия может поставить жирный крест на его дальнейшей деятельности: контролеры легко обнаружат недоплату налогов, насчитают астрономические санкции, арестуют счета в банках и прочие активы и, чего доброго, еще и привлекут должностных лиц предприятия к уголовной ответственности, например, за неуплату налогов в крупном или особо крупном размере.

Если же «наезд» налоговиков или правоохранительных органов является «заказным» — можно не сомневаться, что даже успешный бизнес быстро и безнадежно зачахнет. Чем серьезнее «заказ», тем серьезнее последствия для предприятия и его руководителей.

Кстати, недавно в России были проведены интересные исследования, в ходе которых осуществлялся опрос охранных предприятий (и других подобных структур) на предмет того, с какими проблемами наиболее часто обращаются за помощью российские предприниматели и бизнесмены. Что же выяснилось?

Безусловным лидером среди причин обращений коммерсантов в охранные фирмы является проблема возврата долгов: кому-то не заплатили за отгруженные товарно-материальные ценности, кому-то не вернули вовремя кредит, кому-то не поставили товары, которые ранее были оплачены, и т. д. Если вы планируете в ближайшем будущем открыть свое дело — имейте в виду этот факт.

Далее следует проблема безопасности как самих коммерсантов, так и членов их семей в связи с поступающими угрозами, шантажом, вымогательством, запугиванием и т. п.

Следующая позиция в «топ-листе» принадлежит фактору хищения товарно-материальных ценностей на транспорте. Иначе говоря, в процессе перевозки отгруженные ценности до получателя полностью либо частично не доходят, а «испаряются» в дороге.

Личное имущество коммерсанта — лакомый кусок для любого вора. Поэтому кражи личного имущества являются одной из самых частых причин обращений предпринимателей и бизнесменов в охранные предприятия. Отметим, что крадут что угодно и откуда угодно: из квартир, с дач, из офисов, снятых помещений для «романтических встреч» и т. п. Коммерсанты подвергаются ограблениям, мошенничеству, у них угоняют автомобили, крадут мобильные телефоны...

Головной болью многих предпринимателей и бизнесменов является проблема похищения коммерческой и конфиденциальной информации — именно этой проблеме принадлежит следующая позиция в нашем «топ-листе». При этом мошенники не брезгуют никакими способами: в ход идет копирование и кража секретных документов, похищение информации с электронных и магнитных носителей, прослушивание телефонных переговоров, перехват электронной переписки, подкуп работников предприятия и т. п. Следует учитывать, что злоумышленники постоянно совершенствуют свое «мастерство» и повышают уровень «профессионализма».

Следующая по распространенности «головная боль» коммерсантов — кражи и ограбления в магазинах и иных объектах розничной торговой сети, в производственных и складских помеще-

ниях, в офисах, гаражах и т. п. Как показывает практика, стопроцентной защиты от воровства не дают ни наемные сторожа, ни современные охранные сигнализации, ни «навороченные» замки и запоры. Лучше всего, когда одновременно используются несколько разных средств защиты от воров и грабителей — например, сторож и сигнализация.

И еще одна проблема, с которой предприниматели и бизнесмены обращаются в охранные предприятия, — это умышленная порча имущества и товаров, в частности, путем поджога.

Агрессия как элемент современного российского бизнеса

Если провести небольшой опрос среди наших соотечественников и попросить респондентов ответить на вопрос: «Каким одним словом можно охарактеризовать современный российский бизнес?», наверняка большинство ответит: «Агрессия» или «Агрессивность».

С таким мнением согласно большинство независимых исследователей и экспертов. Действительно, агрессия является одной из характерных черт российского бизнеса, можно сказать — его «национальным колоритом». При этом реализация агрессивного ведения бизнеса осуществляется в России, как правило, весьма жесткими (если не сказать — жестокими) методами, зачастую не имеющими аналогов в других странах мира.

Что же следует понимать под термином «агрессивный бизнес» или «агрессивный стиль ведения бизнеса»?

В настоящее время среди отечественных специалистов не наблюдается единства мнений насчет того, что же следует считать агрессивным бизнесом. Некоторые полагают, что одним из проявлений агрессивного бизнеса является метод ведения агрессивных продаж, вполне официально используемый многими компаниями. Другие под агрессивным бизнесом понимают любые проявления недобросовестной конкуренции, включая физическое насилие, порчу имущества, дискредитацию конкурентов и т. п. Третьи полагают, что агрессивным бизнесом в первую очередь

следует считать такие явления, как недружественное поглощение или насильственный захват предприятий, а четвертые относят к агрессивному бизнесу все перечисленное и еще что-нибудь.

В этой книге мы будем считать, что агрессивный бизнес — это действия, направленные на завоевание доминирующего положения на рынке, а также на завоевание новых рынков всеми доступными средствами, в том числе и незаконными, включая недобросовестную конкуренцию и недружественное поглощение и насильственный захват других субъектов хозяйствования.

Какими же причинами может быть обусловлено появление на рынке агрессоров и какие цели они преследуют?

Главной причиной проявления агрессии всегда является борьба «за место под солнцем». Предположим, какое-то предприятие в своем регионе является монополистом в определенной отрасли (например, никто кроме него не продает импортные стиральные порошки). Вдруг в один прекрасный момент у него появляется конкурент, который, как показали предварительные исследования, может не только отобрать львиную долю рынка, но и вообще вынудить «старожила» уйти с рынка благодаря более гибкой ценовой политике, продуманной маркетинговой стратегии и иным факторам. Очевидно, что с таким положением вещей никто мириться не захочет, и в подобной ситуации вполне возможны проявления рыночной агрессии.

Как обычно действуют российские бизнесмены в таких случаях? Каждый, конечно, по-своему, но вот один из наиболее распространенных вариантов. Вначале новичку ненавязчиво предлагается «сбавить обороты» и «не мешать работать другим». Если не помогло — начинаются конкретные угрозы, запугивание и шантаж. Опять не помогло — у непокорного бизнесмена для острастки могут, например, сжечь машину. Дальше — больше, но в один прекрасный момент «старожил» может прийти к выводу, что воевать лучше бумажками, а не грубыми физическими и иными методами, и, проконсультировавшись со знающими людьми, тихомирно начнет процесс недружественного поглощения конкурирующей компании (более подробно о рейдерстве рассказывается в соответствующей главе).

Агрессивное поведение может быть спровоцировано таким явлением, как переманивание ценных работников. Например, ка-

кое-то предприятие давно и успешно работает на рынке, и вдруг появляется конкурент, который не только серьезно потеснил его, но и начал переманивать ценных работников (например, предлагая им на порядок более высокую заработную плату). Получается, что фирму, долго работающую на рынке, фактически вытесняют с этого рынка с помощью ее же работников (которых, между прочим, в свое время нужно было найти, заинтересовать, обучить, воспитать и т. д.). Поэтому реакция на подобные действия может быть довольно жесткой и весьма агрессивной.

Также проявлением агрессии в бизнесе может являться борьба — как за покупателей, так и за поставщиков. С покупателями все более-менее понятно: по сути, это есть та самая борьба «за место под солнцем», о которой мы говорили ранее. Но зачем же бороться за поставщиков?

Дело в том, что в некоторых видах деятельности от хорошего поставщика зависит чуть ли не половина бизнеса (а иногда и вообще его существование). Рассмотрим такую ситуацию: на рынке действует несколько предприятий, причем рынок давно поделен, и у каждого есть свое место. Предприятия работают с разными поставщиками, у которых примерно одинаковые ассортименты, цены, условия поставок и иные факторы. В общем, на рынке полная стабильность и спокойствие, и всех все устраивает.

Но вот внезапно появляется поставщик, который предлагает заведомо более выгодные условия сотрудничества, чем все другие поставщики в данном регионе. Это грозит полностью перевернуть ситуацию на рынке: доминирующее положение займет тот, кто сумеет заключить договор с новым поставщиком — это позволит ему, в частности, работать по более низким ценам, причем с возможностью отсрочки платежа и с иными условиями, которые не смогут предложить своим клиентам остальные рыночные игроки.

Примечание

Отметим, что возникновение такой ситуации возможно только в том случае, если нового поставщика своевременно не «урезонили» его действующие конкуренты (не вынудили уйти с рынка, не «поглотили» и т. п.). Правда, в современной России трудно представить иное — все «выскочки» оперативно и умело «ставятся на место».

Начинается борьба за поставщика: кто-то предлагает взятки его должностным лицам, кто-то сжигает машины конкурентов, кто-то на кого-то натравливает налоговую проверку и т. д. В целом, ситуация складывается не то что агрессивная, а даже криминальная.

В конце концов все это как-то успокаивается, и победитель схватки заключает договор с выгодным поставщиком, в результате чего вскоре после этого занимает доминирующее положение на рынке, заметно потеснив своих конкурентов. Однако затишье наблюдается недолго: через некоторое время конкуренты вполне могут сговориться и сбросить лидера с пьедестала. Для этого ими сообща могут предприниматься самые разные действия: дружное переманивание персонала, дискредитация конкурента и его торговой марки, организация налоговых и иных проверок и т. д. В конечном итоге заключение выгодного контракта с поставщиком выходит таким боком, что полученные выгоды теряют свой вес в свете появившихся проблем. Кстати, обиженные конкуренты могут действовать и более «цивилизованным» способом, организовав недружественное поглощение (насильственный захват) данного предприятия.

Веским поводом для проявления агрессии является наличие у субъекта хозяйствования привлекательных активов: дорогостоящих зданий либо земельных участков, иной недвижимости, а также нематериальных активов. Например, получить лицензию на торговлю нефтепродуктами (которая является нематериальным активом) очень сложно, поэтому предприятие, имеющее такую лицензию, вполне может стать объектом недружественного поглощения, даже если никаких других привлекательных активов оно не имеет. То же самое касается субъектов хозяйствования, имеющих в собственности дорогую недвижимость: предприятие может работать в убыток или вообще простаивать, либо иметь какие-то другие проблемы, но его могут насильственно захватить только из-за того, что оно владеет дорогим участком земли в центре города возле сразу трех станций метро и в окружении привлекательных объектов (бизнес-центров, пунктов общественного питания, паркингов и т. д.).

Иногда агрессивное поведение на рынке провоцируется непомерными амбициями, ложной гордостью и ложным чувством собственного достоинства, иначе говоря — из-за того, что кто-то просто не в состоянии сдержать свои эмоции. Кстати, это характерно именно для российского бизнеса — когда войны разгораются лишь по той причине, что «кто-то что-то не так сказал», «не так посмотрел», «куда-то послал» и т. п. Повод для агрессии смехотворный, но последствия «военных действий» могут быть очень серьезными, если не сказать — фатальными. В общем, бессмысленная и беспощадная война «понтов» — один из характерных признаков современного российского бизнеса.

Государственный бандитизм: шантаж со стороны госструктур и силовых органов

Особо следует отметить такое негативное явление, как государственный бандитизм. Суть его заключается в том, что предприятие подвергается серьезному «наезду» со стороны облеченных государственной властью органов: полиции, прокуратуры, налоговой инспекции, отдела по борьбе с экономическими преступлениями, налоговой полиции и др. В данном случае спорить тем более бесполезно: наделенные государственной властью и практически неограниченными полномочиями «оборотни» способны поставить на колени кого угодно. При этом в ход могут пойти любые методы, самые распространенные из которых перечислены ниже.

- **Физическое насилие и причинение ущерба здоровью.** Доказать свою правоту и факт беззакония со стороны «государевых людей» невозможно в принципе, поскольку сами вымогатели работают в правоохранительных органах, и, как правило, об их действиях прекрасно осведомлено их руководство.
- **Порча или уничтожение имущества.** Здесь то же самое — даже зная в лицо и пофамильно тех, кто причинил вам материальный ущерб, вы ничего не докажете, а если будете слишком

усердствовать в поисках правды — либо исчезнете бесследно, либо сами окажетесь на скамье подсудимых (самый простой вариант компрометации — вам подбросят пакетик с героином, осудят на долгий срок, а затем растиражируют вашу фамилию в СМИ), либо что-то случится с вашими близкими.

- **Давление на близких.** Если руководителю предприятия, где работает ваша жена, позвонят, например, из ФСБ и ненавязчиво посоветуют уволить ее по какой-нибудь компрометирующей статье — не сомневайтесь, так и будет сделано.
- **Инкриминирование непокорному коммерсанту совершения тяжких преступлений.** Человеку предъявляются обвинения в совершении, например, нераскрытого на данный момент убийства, либо в хранении наркотиков, либо в неуплате налогов в особо крупном размере, либо в злоупотреблении служебным положением — и т. д. и т. п., после чего к нему применяется мера пресечения в виде заключения под стражу. А уже в «казематах» его могут обработать по полной (в России богатые пыточные традиции), в результате чего он либо соглашается на сотрудничество с государственными бандитами, либо несет ответственность за несовершенное преступление.
- **Организация искусственного «наезда» со стороны криминальных структур.** То, что в России государство давно и прочно срослось как с бизнесом, так и с криминалом, знает даже младенец. Поэтому в один прекрасный день к вам могут пожаловать крепкие бритоголовые ребята с «убойным» для вашего бизнеса и заведомо невыполнимым «предложением о сотрудничестве» (например, они потребуют отдавать им процентов 70 выручки от реализации — этого не выдержит ни один бизнес). А через пару часов, когда вы выкурите полпачки сигарет и перестанете дрожать, вам позвонит представитель «оборотней в погонах» и ненавязчиво поинтересуется: с кем же вы предпочтете сотрудничать — с бритоголовыми «братками» или с «солидными людьми в погонах»?

Стоит ли говорить, что с государственными бандитами спорить еще опаснее, чем с обычными криминальными структурами?

В противном случае вас не только могут оставить без бизнеса, сделать калекой и осудить за несовершенное преступление, но еще и уничтожить как личность, втоптав в грязь ваше честное имя. Поэтому знайте: если на вас наехали государственные бандиты, придется либо соглашаться на сотрудничество, либо закрывать свой бизнес. Либо — тихо-мирно и незаметно искать защиту от них в вышестоящих органах, правда, только при обязательном наличии одного условия: там, куда вы хотите пожаловаться, у вас должны быть надежные и проверенные знакомые, желательно — из числа близких личных друзей или родственников. Иначе последствия поисков защиты будут катастрофическими.

Грязные методы конкурентной борьбы

Недобросовестная конкуренция как метод конкурентной борьбы имеет давнюю историю, и в современной России это явление развивается довольно успешно, повсеместно и бурно.

Сущность недобросовестной конкуренции заключается в том, чтобы всеми возможными (законными и незаконными) средствами укрепить собственные позиции за счет ослабления позиций конкурента либо за счет его устранения. В настоящее время наиболее часто недобросовестная конкуренция подразумевает использование следующих методов:

- экономический и промышленный шпионаж;
- распространение лживых сведений и рекламы;
- компрометация конкурента всеми возможными способами (в средствах массовой информации, перед налоговыми органами и др.);
- фальсификация и подделка продукции конкурента;
- прямое нанесение материального ущерба;
- психологическое подавление.

Экономический и промышленный шпионаж направлен на то, чтобы тайком выведать у конкурента секреты успешного менеджмента, производственные тайны, иные корпоративные тайны. Один из наиболее распространенных приемов такого шпионажа — это когда на фирму конкурента внедряется резидент, который, войдя в доверие к сотрудникам и руководству предприятия и получив доступ к секретным сведениям, передает всю полученную информацию своему руководству.

Конечно, никто не отменял различного рода «жучки», установленные в офисных и иных помещениях конкурента, подкуп работников телефонных станций с целью получения распечаток телефонных переговоров и т. п. Однако в настоящее время шпионаж может вестись и более «продвинутым» способом — с помощью специального программного обеспечения. Программы-шпионы внедряются на компьютеры сотрудников конкурирующего предприятия и передают полученные сведения «в центр». Наиболее опасными «виртуальными шпионами» с точки зрения бизнеса считаются клавиатурные шпионы (кейлоггеры).

Клавиатурный шпион — это программа либо устройство, с помощью которого осуществляется постоянное наблюдение за всеми нажатиями клавиш на клавиатуре (а во многих случаях — и за всеми щелчками мыши) с целью получения информации обо всех набираемых пользователем текстах. Зачем это нужно? Чаще всего таким способом можно получить деловую электронную переписку конкурента, а если он занимается разработкой программного обеспечения — то еще и исходные коды разрабатываемых программ.

Характерной особенностью клавиатурных шпионов является то, что они могут выступать не только в виде внедренного в компьютер вредоносного программного обеспечения, но и в виде отдельных устройств. Такие устройства обычно устанавливаются между клавиатурой и системным блоком и, поскольку имеют весьма небольшие размеры, могут долго оставаться незамеченными. Однако чтобы установить такое устройство, необходим доступ к компьютеру в отсутствие пользователя. Чтобы своевременно обнаружить такой «сюрприз», рекомендуется почаще

обращать внимание на то, не появилось ли новое устройство между клавиатурой и системным блоком.

Внедряться клавиатурные шпионы могут разными способами: с помощью электронной почты, путем несанкционированного доступа к компьютеру; иногда для того, чтобы «получить» в свой компьютер клавиатурного шпиона, достаточно зайти на определенный сайт.

Распространение лживых сведений и лживой рекламы — один из самых неприятных видов недобросовестной конкуренции, который можно сравнить с «ударом ниже пояса». Сущность метода заключается в том, что о конкуренте и о его продукции распространяются заведомо лживые и недостоверные сведения. Например, среди потенциальных потребителей продукции конкурента можно распространить слухи о том, что товар якобы изготовлен с нарушением действующих стандартов, а предприятие-изготовитель вообще скоро закроется, и некому будет предъявлять претензии за некондицию. Среди деловых партнеров конкурента можно распространить сведения о его ненадежности: мол, «не поставляйте им сырье и материалы — они могут за них не рассчитаться», «не предоставляйте им в аренду помещение для расширения производства — у них проблемы с налоговой, еще и до вас доберутся» и т. д. Умело поставленная «антирекламная» кампания может существенно снизить успешность предприятия-конкурента.

Несколько похожим на данный метод является другой способ недобросовестной конкурентной борьбы, который заключается в максимально возможной компрометации конкурента всеми доступными способами. Причем здесь речь может идти не только о самом предприятии и его продукции, но и об учредителях и должностных лицах, что не менее серьезно. Например, публикация в прессе заказной статьи о якобы нечистоплотности директора предприятия, его связи с криминальными кругами и имеющихся проблемах с законом может отбить охоту у многих потенциальных партнеров иметь дело с таким предприятием. Другая заказная статья, рассказывающая об «ужасном» качестве продукции конкурента, может серьезно навредить его планам

реализации, а следовательно — принести немалые незапланированные убытки.

Конкретнее? Вот пример, который недавно имел место быть в Вологодской области. Предприятие, специализирующееся на производстве детского питания, занимало лидирующее положение на рынке, что нравилось не всем, в частности, против были конкуренты, желающие потеснить лидера. Как-то в одной из местных газет появилась статья о том, что в баночках с детским питанием от этого производителя было обнаружено толченое стекло. Причем статья была подана хитро: в ней не назывались конкретные факты (поскольку их не было), а было сказано, что «по непроверенным данным в баночках с детским питанием от производителя Х было обнаружено толченое стекло». Факта клеветы в данной статье нет, поскольку четко сказано — «по непроверенным данным», но какая же мать после прочтения такой информации купит своему ребенку детское питание от этого производителя! Эффект был сногсшибательным и, возможно, превзошел все ожидания злоумышленников: предприятие-лидер не только было «сброшено с Олимпа», но ему пришлось даже сменить вывеску, т. е. поменять название фирмы-производителя, а также «раскрученную» торговую марку.

Правда, пострадавшие бизнесмены в долгу не остались и ответили достойно (благо, нашлись связи в налоговых и правоохранительных органах): к недобросовестным конкурентам (злоумышленников вычислили по своим каналам) пришла налоговая проверка и обнаружила такие нарушения, что дальше дело было передано в отдел по борьбе с экономическими преступлениями и параллельно — в налоговую полицию. У «провинившейся» фирмы арестовали счета, склады, и с тех пор о ней ничего не слышно.

Еще одним популярным проявлением недобросовестной конкуренции является фальсификация и подделка продукции конкурента. Здесь злоумышленники могут преследовать две цели: получение прибыли за счет «раскрученной» торговой марки (в данном случае они еще как-то заботятся о качестве) или преднамеренная дискредитация продукции конкурента. В последнем

случае под маркой продукции конкурента реализуется отвратительного качества подделка, не имеющая ничего общего с оригиналом, за исключением упаковки.

И в первом, и во втором случаях недобросовестных конкурентов можно привлечь к судебной ответственности как минимум за использование чужой торговой марки в корыстных целях. Однако злоумышленники вполне могут достичь своей цели: от торговой марки, под которой продается некачественная продукция, откажется если не большинство, то значительная часть покупателей.

Прямое нанесение материального ущерба — один из самых грубых и грязных методов конкурентной борьбы. В данном случае злоумышленники тем или иным способом стремятся уничтожить или повредить имущество и иные товарно-материальные ценности конкурента, вывести из строя производственное оборудование и т. д. Одним из наиболее распространенных способов нанесения материального ущерба является умышленный поджог: такое деяние трудно доказуемо, а ущерб можно нанести очень и очень приличный — вплоть до полного уничтожения зданий, сооружений, складских запасов, производственного инвентаря, деловой документации, оргтехники и т. д.

Отметим, что материальный ущерб злоумышленники могут причинять не только предприятию, но и его учредителям и должностным лицам. В настоящее время уже никого не удивляют факты сожжения автомобилей, коттеджей и дач, порчи личного имущества и т. п.

Одним из мощных средств недобросовестной конкуренции является психологическое подавление. В качестве «методов воздействия» могут использоваться угрозы, шантаж, непонятные намеки по телефону и т. п. Причем подвергаться ему могут не только учредители и ответственные лица компании, но и их близкие люди. Например: директор преуспевающей фирмы получает по электронной почте письма с угрозами и требованием «сбавить обороты» и «дать работать и другим хорошим людям», в это же время его жена подвергается гонениям и преследованиям на работе со стороны начальства, а ребенка в школе начинают травить одноклассники. Не всякий человек способен вы-

держать подобное давление и уж тем более — достойно противостоять ему!

Иногда изначально могут запугивать не учредителя или ответственное лицо фирмы, а его близких людей — жену, детей, родителей... Например, жена может рассказать о том, что ей постоянно звонят и угрожают какие-то люди, ребенок может пожаловаться, что его после школы встретил незнакомый дядя и долго расспрашивал о папе, и т. п.

Как утверждают многие психологи, чем непонятнее для жертвы оказываемое психологическое воздействие — тем больший эффект оно может принести. Например, если человеку просто позвонить по телефону и сказать нечто вроде «не мешай другим, а то будешь иметь проблемы» — это еще не самый плохой вариант: по крайней мере, можно обратиться в полицию или пожаловаться собственной охране, а некоторые подобные угрозы можно просто игнорировать. Психологически гораздо труднее перенести малопонятные намеки и обстоятельства, например:

- звонок по телефону без предъявления конкретных требований и угроз, а только с непонятными словами, вроде: «ну-ну, допрыгался», «все хорошее когда-то кончается» и т. п. (по аналогии со знаменитым «Грузите апельсины бочках братья Карамазовы» из «Золотого теленка»);
- после прохода на улице мимо малоприятной компании сомнительного вида молодых людей за спиной раздается их дружный злобный хохот или слышится фраза, вроде: «все мы смертные», «вот еще один пошел» и т. п.;
- под «дворником» машины обнаруживаются записки с непонятным содержанием или даже рисунками (вроде пиратской «черной метки), причем написанные не от руки, а распечатанные на принтере (современные злоумышленники осторожны);
- прямые и открытые угрозы от конкурентов навести на успешное предприятие налоговую проверку, отдел по борьбе с экономическими преступлениями и т. д. (не секрет, что современное российское законодательство позволяет при желании привлечь к ответственности даже младенца);

- постоянные звонки в дверь квартиры с исчезновением звонившего (при открытии двери в коридоре никого нет);
- другие подобные действия.

Как показывает российская практика, психологические методы воздействия нередко бывают наиболее эффективными. Например, если у кого-то сожгли машину или дачу либо «натравили» на фирму налоговую проверку, либо дискредитировали продукцию и торговую марку — реакция может быть прямо пропорциональная: человек может ожесточиться и предпринять ответные эффективные действия. Но если человек приходит домой, и жена ему говорит, что ей грозили плеснуть в лицо кислотой, а перепуганный и заплаканный сын, придя из школы, сообщает, что какой-то дядя грозился убить его, если папа не послушает «хороших людей» — здесь любой разумный человек наступит на горло собственной песне, забудет обо всех амбициях и сделает то, что от него требовали. Причем если в случае причинения материального ущерба человек может обратиться, например, в полицию, то при возникновении угрозы жизни и здоровью близких людей многие просто побоятся обращаться в правоохранительные органы.

Нездоровый интерес со стороны собственных работников

Какой владелец собственного бизнеса не мечтает о том, чтобы работники его предприятия испытывали истинный интерес к работе и исполняли свои служебные обязанности с удовольствием? Однако в своем стремлении заинтересовать работников многие упускают из виду тот факт, что этот интерес может принять нездоровые, мягко говоря, формы.

Например, какой-нибудь высокопоставленный сотрудник, на которого много чего «завязано», пользуясь доверием руководства, может выяснить какие-нибудь интересные секреты деятельности фирмы для того, чтобы впоследствии открыть свое дело

и использовать полученные сведения себе во благо. В таком случае вы рискуете не только остаться без одного из ключевых кадров, но и заполучить в его лице достойного конкурента.

Нередко работников преуспевающего предприятия подкупают его конкуренты с целью получения интересующих сведений (как уже отмечалось, это одно из проявлений экономической разведки или экономического шпионажа). Поэтому, если сотрудник проявляет неподдельный интерес к работе предприятия и живо интересуется многими вопросами — это еще не повод восторгаться им, повышать заработную плату, выписывать премию либо строить на него серьезные планы: очень может быть, что такой интерес подогревается исключительно получаемым от конкурентов вознаграждением.

Какие сведения могут получать конкуренты через подкупленных сотрудников компании? Да самые разные, и во многом это зависит от вида деятельности предприятия, особенностей выпускаемой продукции, специфики постановки учетных и управленческих процессов, а также иных факторов. Это может быть и размер уплачиваемой предприятием арендной платы, сумма получаемой прибыли, размеры заработных плат сотрудников предприятия, каналы обналичивания денежных средств, ключевые моменты технологического процесса, секреты организационной структуры предприятия, особенности организации менеджмента и т. д. Также многих интересует наличие у предприятия связей в налоговых и правоохранительных органах, организация охраны, подверженность влиянию криминальных структур и пр.

Если предприятие занимается разработкой программного обеспечения, то можно не сомневаться, что время от времени его сотрудники будут получать «непристойные предложения» извне. В частности, конкурентов, да и вообще посторонних, могут интересовать программные коды как вышедших, так и находящихся в разработке программных продуктов. Также большой популярностью пользуются разнообразные средства защиты программного обеспечения от несанкционированного (проще говоря, пиратского) доступа — аппаратные и программные ключи, конфигурационные файлы и т. п. За подобные «трофеи» завербованным

сотрудникам предприятия могут предлагать очень и очень солидное вознаграждение.

Интерес сотрудников к собственному предприятию может быть и более банальным. Например, если человек очень интересуется распорядком работы охранников, а также тем, как работает охранная сигнализация, и при этом по долгу службы не имеет никакого отношения к данным вопросам — очень может быть, что он хочет что-то украсть либо того больше — организовать ограбление.

«Наезды» со стороны криминалитета

В современной России любой более-менее прибыльный и рентабельный бизнес находится под пристальным влиянием криминальных структур. Причем, чем крупнее бизнес, чем больше денег в нем и вокруг него крутится — тем более серьезные «доны Корлеоне» положат на него глаз.

То, что сращивание бизнеса и криминала — это плохо, спорить не будет никто. И в первую очередь данное явление ощутимо бьет по репутации государства: что же это такое — криминальные структуры обкладывают бизнес данью, устраивают «разборки» с неугодными и непокорными бизнесменами, а государство со всей своей полицией, ФСБ и иными структурами даже пикнуть не смеет? Более того — коммерсант, который осмелится пожаловаться на бандитский произвол в правоохранительные органы, будет жестоко наказан, причем еще очень хорошо, если наказание ограничится материальным ущербом (например, сожженной машиной или дачей), а жизнь и здоровье «кляузника» и его близких не пострадают.

Примечание

Справедливости ради отметим, что в последние годы криминальные структуры стали действовать не так оголтело, жестоко и дико, как в «лихие 90-е». Конечно, бизнес регулярно платит дань бандитам, и дань немалую, но сейчас отношения криминала и бизнеса выглядят более цивилизованно. В частности, современные вымо-

гатели стали понимать, что для того, чтобы получать с коммерсанта деньги, нужно давать ему хоть что-то зарабатывать. В 1990-е же годы сплошь и рядом встречались ситуации, когда из-за непомерных поборов предприятия быстро разорялись, в результате чего у разбитого корыта оставались все: и бизнесмены, и их вымогатели.

О том, что в «подведомственном» районе появилось новое предприятие, бандиты узнают быстрее всех. Среди наиболее распространенных источников получения информации можно отметить следующие.

- Знакомые, друзья и соседи коммерсанта. В случайной доверительной беседе (например, в очереди за колбасой) у них выясняют, что «да, Петр недавно фирму открыл, будет мылом и порошками торговать», или «Иван предприятие только что зарегистрировал, планирует заняться производством металлического профиля». Кстати, настоящий «Клондайк» информации — это бабушки, сидящие у подъезда, в котором проживает будущий бизнесмен. Отсюда вывод: не стоит распространяться о своих коммерческих устремлениях без особой надобности. Конечно, рано или поздно «братки» все узнают, но лучше пусть это будет позже, когда фирма уже более-менее встанет на ноги.
- «Свои люди» в местном органе власти и в налоговой инспекции. У любой более-менее серьезной криминальной структуры есть проплаченные осведомители в государственных органах, которые своевременно сообщают обо всех зарегистрированных предприятиях и о том, каким видом деятельности те планируют заниматься.
- Визуальное внешнее наблюдение за человеком. Если кто-то занимается тем, что часто посещает орган, занимающийся регистрацией субъектов хозяйствования и выдачей лицензий на право осуществления тех либо иных видов деятельности, активно интересуется сдаваемыми в аренду помещениями и т. п. — значит, он явно планирует открыть свое дело, следовательно — достоин самого пристального внимания.

Помимо перечисленных, криминальные структуры могут использовать и иные методы получения информации, в зависимости от специфики конкретной ситуации.

Некоторые «продвинутые» вымогатели отказались от таких действий, как физическое насилие, порча имущества и т. п. Они действуют другими методами, например — организуют мощную налоговую проверку непокорному коммерсанту либо предпринимают меры для того, чтобы ни один субъект хозяйствования в «подведомственном» регионе не сотрудничал с «крамольным» предприятием.

Если вы и ваше предприятие попало в поле зрения криминальных структур — скорее всего, вам в любом случае придется сотрудничать с ними и делиться частью прибыли. Как правило, сопротивление бесполезно; в некоторых случаях можно лишь немного поторговаться, чтобы сбросить цену за «крышевание».

Глава 2

Изощренные методы мошенничества и обмана, используемые «офисным планктоном»

Воровство и мошенничество внутри предприятий являются неотъемлемой частью современного бизнеса. Причем не только российского, но и зарубежного. Да-да — вопреки многим рассказам, которыми нас щедро потчевали все годы после распада Советского Союза, даже на процветающем Западе такие понятия, как «деловая репутация», «честность по отношению к компании» и т. п., давно померкли и потеряли свою былую привлекательность, особенно на фоне возможности быстрого, значительного, а главное — реального обогащения. Примеры? Пожалуйста.

- Два ведущих топ-менеджера компании всемирно известной Dow Chemical были уволены за проведение сепаратных переговоров о продаже компании группе инвесторов.
- Руководство немецкого концерна Siemens потратило на различного рода подношения (говоря попросту — взятки) клиентам в разных странах около 556 миллионов долларов США.
- Топ-менеджеров французской нефтяной корпорации Total подозревают в совершении подкупа иранских и иракских чиновников.

Подобных примеров можно привести великое множество, но в принципе и без них картина ясна.

По оценкам многих независимых экспертов, в 21-м веке главная опасность для любого предприятия будет исходить не от конкурентов, недоброжелателей, проворовавшихся чиновников и т. д., а от собственных сотрудников.

Примерные объемы ущерба, причиняемого «оборотнями в офисе»

Опасность для современного предприятия может исходить от абсолютно любого его сотрудника — начиная от сторожа и уборщицы и заканчивая высшим руководством (директор, президент и т. п.).

Важно!

Результаты независимых исследований свидетельствуют о том, что убытки субъектов хозяйствования, причиненные собственными работниками, могут достигать 90% от суммы общего ущерба! Иначе говоря, практически весь ущерб предприятие может получить только по причине внутренней коррупции.

Стоит ли говорить, что такими показателями не может «похвастаться» ни один конкурент, недоброжелатель или коррумпированный чиновник!

Международная организация Association of Certified Fraud Examiners, которая специализируется на борьбе с внутренней коррупцией и мошенничеством на предприятиях, распространила следующие данные: в среднем около 6% своего оборота западные компании теряют по вине своих работников. Причем в данном случае речь идет не об ошибках или случайных просчетах сотрудников предприятий, а об их обдуманных действиях, направленных на получение личной выгоды и причиняющих немалый ущерб интересам компании.

Примечание

В развитых современных странах субъектам хозяйствования рекомендуется тратить на деловую разведку и промышленный шпионаж сумму, составляющую 0,5–1% от общей суммы оборота по предприятию.

Аналогичные исследования проводились и среди представителей российского бизнеса, и они дали примерно такие же результаты (убытки, причиненные собственными сотрудниками, составляют 5,5–6% от суммы оборота).

Ненамного отличаются и данные, полученные на американском рынке. Результаты исследований, проведенных американской Ассоциацией специалистов по борьбе с мошенничеством, свидетельствуют: ущерб от деятельности «оборотней в офисах» в 2006 году составил около 5% годовой выручки американских субъектов хозяйствования. В денежном эквиваленте этот показатель выражается умопомрачительной суммой — 652 миллиарда долларов США! Несложный математический подсчет показывает, что каждый рабочий час субъекты хозяйствования США теряют 300 миллионов долларов! Кстати, в Великобритании годовой ущерб компаний от деструктивной деятельности «офисных оборотней» оценивается примерно в 160 миллиардов долларов США.

Кто же из работников в первую очередь склонен к причинению ущерба родному предприятию?

Как показали проведенные в России исследования, порядка 83% работников предприятий и организаций в той или иной степени склонны к воровству, мошенничеству или иным деструктивным по отношению к предприятию действиям при наличии благоприятных для этого обстоятельств. Около 9% российских работников являются постоянными и активными участниками внутренней коррупции, и лишь 8% действительно честно работают на благо предприятия и не желают участвовать в сомнительных операциях.

Известная консалтинговая фирма PricewaterhouseCoopers в ноябре 2006 года провела опрос 3600 предприятий и организаций разных форм собственности, расположенных по всему миру. Результаты удивили всех: около 37% опрошенных сообщили о том, что их сотрудники в той или иной форме предпринимали противоправные действия, направленные на получение личной выгоды в ущерб интересам предприятия.

Подобные исследования проводились и в России, и выяснилось, что около 45% опрошенных субъектов хозяйствования по-

лагают: проблема внутренней коррупции их не касается в настоящее время и вряд ли коснется в ближайшем будущем. Однако этот показатель во многом базируется не на реальном положении вещей, а на специфическом, чисто «российском» отношении к мошенничеству и коррупции: на многих российских предприятиях факты мелкого злоупотребления всерьез никто не воспринимает, в то время как в западных странах тщательно фиксируется и скрупулезно анализируется все, что обнаружено.

Более того — многие российские руководители предприятий и организаций полагают: пусть подчиненные подворовывают, но не выше определенного уровня. В среднем этот уровень составляет порядка 10–15% от оборота предприятия, и суммы такого ущерба в управленческом учете просто списываются на издержки компании. Стоит ли говорить, что на такой благодатной почве внутренняя коррупция цветет пышным цветом!

Типичный портрет сотрудника-мошенника

Согласно проведенным исследованиям, около 90% «офисных оборотней» составляют мужчины, причем более трех четвертей из них имеют высшее образование. Ущерб, который родному предприятию могут причинить мужчины, примерно в четыре раза превышает потери, причиняемые женщинами. Во многом это обусловлено тем фактом, что в подавляющем большинстве российских компаний ключевые посты и должности (деструктивная деятельность работников именно этого звена приносит массу убытков) занимают именно мужчины.

Средний ущерб, причиняемый субъектам хозяйствования работниками с высшим образованием, примерно в пять раз превышает потери, приносимые мошенниками со средним образованием.

Представляет интерес и такой факт: на российских предприятиях злоупотребления со стороны сотрудников линейного персонала составляют 23% от общего числа случаев мошенничества, со стороны менеджеров и иных работников среднего звена — 27%, а на топ-менеджеров и высших руководителей — 50%.

Почему же один работник ворует практически постоянно, а другой — прямо «ангел во плоти», и мысли не допускает о том, чтобы пойти на злоупотребление?

Дело в том, что чаще всего на мошенничество и воровство идут представители определенных категорий людей. Кто же в первую очередь входит в «группу риска»?

- Работник, который является по своей сути азартным человеком. Вообще от таких работников желательно держаться подальше, иначе не исключено, что активы вашего предприятия будут постепенно становиться активами какой-нибудь букмекерской конторы.
- Работник, который является неуравновешенным человеком. Вспыльчивый, неуравновешенный человек склонен к совершению необдуманных поступков, легче поддается соблазнительным и сомнительным предложениям. Не исключено, что впоследствии он и сам будет жалеть о содеянном, но ведь вернуть что-то назад уже очень сложно, а иногда — почти невозможно. С другой стороны, таких людей проще вынудить добровольно рассказать о своих прегрешениях.
- Работник, который является безответственным человеком. Таких людей в принципе нельзя принимать на работу, а если такое уже случилось — от них нужно избавляться как можно быстрее.
- Работник, который является жадным и алчным человеком. Такому человеку всегда всего мало, и он будет воровать независимо от размера получаемой заработной платы.
- Работник, который страстно мечтает о какой-нибудь крупной, но пока недостижимой покупке (квартира, машина, дача, гараж и т. п.). Откладывать деньги на покупку с заработной платы — это так долго и мучительно, а жизнь — так коротка! Поэтому нередко человек решает «не терять время попусту», а использовать для достижения заветной мечты любые доступные способы.
- Работник с мягким и податливым характером. Такого человека относительно просто склонить к участию в сомнительной

сделке. Кроме этого, такие люди нередко находятся «под каблуком» у своих половин, и нередко поводом для злоупотребления становится желание ублажить эту самую половину.

- Работник, который часто меняет места работы (например, смена за последние пять лет трех и более мест работы). С какой стати нормальному и порядочному человеку постоянно менять работу? Не исключено, что причиной тому является либо его недостаточный профессионализм, либо склонность к мошенничеству и злоупотреблениям (по принципу «хапнул в одном месте — убежал на другое»).
- Работник, у которого в жизни случилась неприятность, связанная с большими материальными потерями (ограбление квартиры, пожар, автомобильная авария, болезнь близкого человека, требующая дорогостоящего лечения, потеря накоплений и т. д.). Желание побыстрее возместить понесенный ущерб или собрать деньги на предстоящие затраты вполне может толкнуть даже порядочного человека на путь мошенничества и злоупотреблений.

Однако, согласно статистическим данным, самый высокий ущерб приносят злоупотребления и мошенничества, совершенные работниками, состоящими в родстве. По данным проведенных исследований, доля таких правонарушений составляет около 73% от общего числа случаев внутренней коррупции. Не секрет, что людям, состоящим в родстве, удобнее вступить в сговор с целью злоупотребления служебным положением. Поэтому при комплектации персонала нельзя допускать ситуаций, когда, например, главным бухгалтером предприятия работает муж, его заместителем — жена, а простыми бухгалтерами — их сын и дочь. Если при этом на должности заведующего складом работает зять главного бухгалтера, финансовым директором — его брат, а кассиром — невестка, то в 100% случаев на таком предприятии будут присутствовать злоупотребления служебным положением, должностной подлог, фальсификации, хищения и еще целый ряд подобных явлений.

Также большой ущерб российским субъектам хозяйствования причиняют представители топ-менеджмента. Это неудивительно:

работники именно этого звена обычно имеют доступ к информационным, финансовым и другим активам предприятия. Также они, как правило, имеют многолетний опыт работы именно на данном предприятии, в результате чего очень хорошо осведомлены о его наиболее уязвимых и слабых местах, недостаточно контролируемых направлениях деятельности. Плюс ко всему, представители топ-менеджмента почти всегда обладают внушительными полномочиями и пользуются доверием высшего руководства компании.

Типичный портрет честного работника

Итак, мы уже знаем, от каких работников в первую очередь следует ожидать неприятностей. А вот среднестатистический портрет честного работника, составленный на основании многочисленных исследований, выглядит примерно так.

Семейный мужчина средних лет (примерно 35–45), с высшим образованием, имеющий работающую жену и детей в возрасте до 14 лет, обеспеченный жильем и прочими необходимыми благами (машина, дача, гараж и т. п.), обладающий ровным и спокойным характером. Солидный и «здравомыслящий» возраст позволяет трезво оценивать ситуацию и своевременно отказываться от нелицеприятных предложений, а также спокойно воздерживаться от иных соблазнов (не секрет, что человек в 25 лет скорее склонен к совершению необдуманных поступков, нежели в 35–45 лет). Должному исполнению служебных обязанностей во многом способствует ответственность главы семьи, а также желание сохранить заработанную к этим годам репутацию. Работающая жена — дополнительный доход в семью, что намного снижает зависимость сотрудника от соблазнов и «дополнительных возможностей» своей работы. Возраст детей до 14 лет позволяет пока не думать о предстоящих поступлениях в институт, репетиторах, платных учебах, будущих свадьбах и иных подобных событиях, требующих немалых дополнительных трат. В общем, человек живет спокойной, размеренной жизнью, у него сложилась карьера, личная жизнь, он имеет достаток, спокойно растит детей и дорожит своей работой.

Конечно, этот портрет не стоит воспринимать как догму, но какое-то впечатление о личности честного работника он дает.

Как ворует и злоупотребляет бухгалтер

Бухгалтерские злоупотребления для руководства компаний обычно являются полной неожиданностью: проблемы возникают там, где их меньше всего ожидаешь. Далее рассмотрим некоторые распространенные способы, с помощью которых бухгалтеры обманывают руководителей и учредителей предприятия.

Получение бухгалтером «откатов» от сторонних структур

Вот один из видов злоупотреблений, который нередко встречается на предприятиях, имеющих большое количество покупателей или заказчиков (от 100 до нескольких тысяч и больше). Характерный пример такого предприятия — это фирма, занимающаяся средне- и мелкооптовой торговлей товарами народного потребления (продукты питания, парфюмерия, бытовая химия, книги, одежда, обувь — т. е. все, что продается в магазинах), которая работает непосредственно с предприятиями розничной торговой сети. Причем товар покупателям отпускается не на условиях предоплаты, а с отсрочкой платежа (например, 5, 10 или 15 банковских дней или по мере реализации и т. д.).

Не секрет, что далеко не все покупатели строго выполняют договорные обязательства и рассчитываются с поставщиком вовремя. При этом всей информацией о задолженности владеет только бухгалтерия. И здесь открывается широкое поле для злоупотреблений.

Например, некое предприятие задолжало вашей фирме некую сумму, причем в ближайшее время погасить ее не сможет. Работник бухгалтерии вашей фирмы (это может быть как главный бухгалтер, так и бухгалтер по расчетам с контрагентами) связывается с бухгалтерией либо руководством должника и требует погасить

задолженность. При этом он сообщает, что при невыполнении этого требования о ситуации будет доложено руководству, и не исключено, что задолженность будет взыскиваться в судебном порядке.

В ответ представитель фирмы-должника предлагает вашему бухгалтеру лично встретиться и обсудить ситуацию. На этой встрече ему делают предложение, от которого ему трудно отказаться. А именно: он не предпринимает никаких действий по взысканию задолженности в течение определенного времени (например, 3 месяца), и за это ему будет выплачиваться своего рода «пеня», разумеется — строго конфиденциально и неофициально. Размер «пени» может варьироваться в зависимости от специфики конкретной ситуации (размер задолженности, жадность бухгалтера-«оборотня», финансовые возможности должника и др.). Например, если задолженность составляет 1000 долларов США, то за каждый рабочий день просрочки бухгалтеру вполне могут предложить 0,3% от этой суммы, т. е. 3 доллара в день. Если считать, что в месяце 20 рабочих дней, то за месяц это составит 60 долларов США, а за три месяца — 180 долларов США. Все это время деньгами вашей фирмы будет распоряжаться кто-то другой, а бухгалтер за свое преступно-молчаливое согласие будет получать наличные деньги. По истечении этого срока должник тихо-мирно погашает задолженность (в противном случае его договоренность с бухгалтером может быть «пролонгирована»), и вся эта история остается незамеченной руководством.

Поэтому каждый руководитель должен хотя бы в общих чертах владеть ситуацией о дебиторской задолженности (досконально все знать при большом количестве клиентов невозможно, да и не нужно) и знать своих проблемных клиентов (т. е. тех, кто часто оплачивает полученные товары либо услуги с опозданием). Периодически бухгалтеру по расчетам либо главному бухгалтеру рекомендуется устраивать выборочные проверки: например, попросить предоставить полную информацию о расчетах с проблемными клиентами (либо конкретно назвать клиентов) с указанием размера общей и просроченной задолженности, причин возникновения просроченной задолженности и предполагаемых сроков погашения. Если выяснится, что бухгалтер своевременно

не предпринял никаких мер по погашению просроченной задолженности (в частности, не довел информацию о возникновении такой задолженности до руководства), то к этому следует отнестись со всей внимательностью и строгостью.

Еще лучше в приказном порядке обязать бухгалтера докладывать вам о просроченной задолженности в день ее возникновения. Это позволит вам постоянно контролировать состояние расчетов с проблемными клиентами. А бухгалтеру впоследствии будет невозможно скрывать просроченную задолженность с целью получения личной выгоды, если эта задолженность находится на контроле у руководства.

Очень и очень распространенный вид злоупотреблений — откат бухгалтеру за перечисление денежных средств для участия в каком-либо семинаре (по исчислению НДС, по расчету таможенных платежей, по многовалютному учету и т. п.). Как известно, такие семинары в настоящее время не проводит только ленивый, и многие из них отнюдь не дешевы (особенно если семинар рассчитан не на один, а на два и более дней), поэтому и сумма отката очень даже привлекательна.

И еще полбеды, если ваш бухгалтер получил откат за оплату семинара, но при этом посетил этот семинар и получил там знания, которые будут полезны для выполнения должностных обязанностей. На практике бывает гораздо хуже: деньги за семинар перечислены, бухгалтер получает за это неплохой откат и затем один или несколько дней не появляется на работе, мотивируя это тем, что находится на семинаре. Директору и невдомек, что на самом деле никакого семинара нет, деньги у него попросту украдены, а бухгалтер организовал себе небольшой оплачиваемый отпуск. Причем бухгалтер может сам выдумать такую схему и привлечь для ее реализации кого-либо из своих знакомых — тогда речь будет идти уже не об откате, а просто о дележе поровну полученной суммы. Кроме этого, главный бухгалтер может организовать подобное «посещение семинара» не для одного себя, но и еще для кого-нибудь из бухгалтерии, например — «пойти на семинар» вместе со своим заместителем, приняв его «в долю» (разумеется, сумма оплаты и последующего вознаграждения соответствующим образом увеличится).

Поэтому, если ваш бухгалтер говорит, что он желает посетить семинар (курсы, занятия и т. п.), который нужно оплатить, к этому следует отнестись внимательно. Рекомендуется сразу же прояснить перечисленные ниже вопросы.

- Действительно ли так необходимо вашему бухгалтеру посещать этот семинар? Может, тема семинара никак не касается того, чем занимается ваше предприятие? Например, если вы занимаетесь торговлей строительными материалами, а бухгалтер желает посетить семинар, посвященный вопросам уплаты НДС на предприятиях общепита, то это следует расценивать как тревожный звонок.
- Кто проводит семинар? Имеет ли право организация, которой необходимо перечислить деньги за участие в семинаре, проводить подобные мероприятия? Не будет лишним поинтересоваться у своих коллег — руководителей предприятий: слышал ли кто-нибудь из них о такой организации, может — посещал ее семинары?
- Кто является получателем денежных средств, которые должны быть перечислены за участие в семинаре? Если в качестве получателя выступает какой-то посредник, а среди документов на оплату присутствует договор перевода долга либо какой-то аналогичный документ, то, скорее всего, ваш бухгалтер что-то темнит.
- Где будет проводиться семинар? Рекомендуется связаться с представителем организации, проводящей семинар, и выяснить этот вопрос. Если предполагается проведение семинара на арендной территории, то следует позвонить на предприятие, сдающее помещение в аренду, и уточнить — действительно ли тогда-то и в такое-то время там будет проходить семинар, который проводит такая-то организация?

Если же вы согласились оплатить семинар и отпустить на него бухгалтера, то рекомендуется обязательно посетить место проведения семинара и посмотреть, действительно ли ваш бухгалтер там присутствует. Если это не так — у вас появится серьезный повод для подозрений.

Широкое поле для злоупотреблений появляется у бухгалтера, когда предприятие постоянно или периодически испытывает нехватку денежных средств для осуществления текущих платежей. Например, на текущей неделе вам нужно сделать следующие платежи: предоплата поставщику «Торговый дом», предоплата поставщику «Торговля и кредит», вернуть излишне полученную сумму покупателю «Мир моды», оплатить налоги, а также аренду офиса и склада. Общая сумма платежей составляет, допустим, 300 000 рублей; реально же вы сможете оплатить только 200 000 рублей.

Из всех перечисленных платежей обязательным и не вызывающим сомнений является лишь оплата налогов — в противном случае родное государство не преминет обложить вас разными пенями, штрафами и т. д. А вот все остальное — это уже как бухгалтер решит, если только на этот счет он не получал от вас конкретных и строгих указаний.

В такой ситуации бухгалтер может позвонить, например, поставщику «Торговый дом» и сказать примерно следующее: «Вы знаете, на этой неделе, а скорее всего, и на следующей мы не сможем перечислить вам предоплату. Вы уж извините, финансовые проблемы… Уж и не знаю, как тут быть…». Возможно, поставщик просто ответит: «Ну не можете — и ладно, перечислите, когда сможете, но товар получите только после предоплаты». В этом случае можно тут же позвонить другому поставщику и произнести эту же фразу. Но не исключена и другая ситуация, например — когда поставщик ждет конкретно этих денег (ведь у него тоже есть актуальные, запланированные заранее платежи). В таком случае может последовать примерно такой ответ: «Давайте подумаем вместе — может, что-то и придумаем», с последующим предложением личной встречи.

А уже на личной встрече разговор пойдет конкретный: за перечисление денежных средств в полном объеме, который был запланирован ранее, бухгалтер получает откат — например, 5%. Несложно посчитать, что если сумма платежа составляет 100 000 рублей, то сумма отката составит 5000 рублей. И для

ее получения достаточно всего лишь выполнить свои служебные обязанности — перевести деньги на счет поставщика.

Кстати, наиболее наглые бухгалтеры практикуют подобное вымогательство даже тогда, когда их предприятие не испытывает никаких проблем с денежными средствами и способно все платежи осуществлять вовремя. В таких случаях бухгалтер просто идет на контакт с теми контрагентами, которые, насколько ему известно, в данный момент остро нуждаются в деньгах, и задержка платежа может стать для них причиной серьезных неприятностей.

Если бухгалтер, что называется, «вошел во вкус», то ради получения личной выгоды он может даже подставить под удар родное предприятие. Наиболее характерная ситуация — это когда после перечисления крупной денежной суммы, за что бухгалтер получил неплохой откат, у предприятия не остается денежных средств для осуществления других срочных платежей (например, налогов). Кроме этого, жажда наживы иногда толкает бухгалтера на то, что он «перегоняет» деньги, даже не удосужившись надлежащим образом документально оформить такой платеж. Впоследствии из-за платежа, который не подтвержден соответствующими документами, предприятие может иметь крупные неприятности.

Следует учитывать, что бухгалтер для осуществления подобных операций может вступать в сговор с каким-нибудь другим сотрудником своей фирмы — например, начальником отдела поставок или снабженцем, который выступает в качестве посредника и тоже участвует «в доле». Причем инициатива может исходить как раз от такого посредника, а не от бухгалтера. Это обусловлено тем, что посреднику проще обсуждать подобные деликатные вопросы с поставщиком, поскольку он непосредственно с ним работает. В результате посредник вначале ведет предварительные переговоры с поставщиком, а затем просто приходит к бухгалтеру и делает предложение, от которого трудно отказаться.

Примеры других бухгалтерских злоупотреблений

Рассмотрим способ злоупотребления, который имеет место быть на многих коммерческих фирмах, и в первую очередь на тех из них, которые занимаются торговлей средним и мелким оптом и работают непосредственно с магазинами.

Многие руководители вводят у себя на предприятии такую практику: товар, который был возвращен покупателем по какой-то причине (плохо продается, испорчена упаковка, истекает срок годности и т. п.), сотрудники фирмы могут приобрести для себя за наличный расчет — разумеется, неофициально (т. е. за «черный нал»). Причем своим сотрудникам товар отпускается со значительной скидкой — например, 30% (размер скидки может быть разным — и 15%, и 50%). Учет такого товара и его продажа сотрудникам обычно возлагается на бухгалтера предприятия.

Ушлый бухгалтер очень быстро сможет извлечь из этого для себя выгоду. Рассмотрим это на конкретном примере.

Предположим, некая фирма решила приобрести у вас партию товара с отсрочкой платежа (например, на 10 банковских дней). После отгрузки этого товара бухгалтер звонит покупателю и говорит: мол, так и так, есть возможность организовать вам этот же товар значительно дешевле.

Используемая в данном случае схема достаточно проста. Вначале покупатель возвращает вашей фирме весь полученный товар под каким-то предлогом (плохо продается, внезапно пришла налоговая проверка и т. д.). Затем выкупает его за «черный нал» с такой же скидкой, которая предназначена для работников вашего предприятия при приобретении ими возвращенного товара. Бухгалтер преподносит это руководителю как реализацию возвращенного товара своим работникам и получает от благодарного покупателя вознаграждение, размер которого оговаривается заранее. Например, если скидка для своих сотрудников составляет 30%, то 10% может взять себе бухгалтер, а 20% — это скидка покупателю; также доля бухгалтера может рассчитываться просто как определенный процент от суммы сделки — здесь уже все зависит от конкретной ситуации.

Одно из излюбленных злоупотреблений, которым нередко занимаются бухгалтеры и кассиры, — это оформление выплат наличных денежных средств сотрудникам, которые на предприятии не работают.

Наиболее примитивная реализация такого мошенничества — это просто добавление в ведомость по заработной плате вымышленных сотрудников, начисление им заработной платы и присвоение этих денег в момент выплаты. При этом подпись несуществующего работника в ведомости подделывается.

Если предприятие — относительно небольшое, то руководитель сам может обнаружить подобное хищение. Для этого нужно просто следить за тем, какую сумму бухгалтер получает в банке для выплаты заработной платы сотрудникам предприятия. Если, например, в текущем месяце эта сумма по сравнению с прошлым месяцем увеличилась, а изменений в штате предприятия не было (в частности, новые сотрудники на работу не устраивались), то следует уточнить у бухгалтера — что послужило причиной ее увеличения. Возможно, для этого были объективные причины — например, из отпуска по уходу за ребенком вышла сотрудница, и теперь она получает из кассы предприятия не положенное по закону пособие, а полноценную заработную плату.

Более хитрый бухгалтер поступает несколько иначе; для этого он просто дожидается увольнения какого-либо сотрудника. В этом случае бухгалтер просто «забывает» удалить его из ведомости по заработной плате, и продолжает начислять ему заработную плату, как будто он и не увольнялся. В этом случае подпись сотрудника, опять же, подделывается. В некоторых случаях бухгалтер может вступить в сговор с таким сотрудником — тогда уволенный будет сам расписываться в ведомости, а полученные деньги они с бухгалтером будут делить пополам. Наиболее наглые бухгалтеры «забывают» удалить из ведомости по заработной плате не одного, а нескольких сотрудников, получая ежемесячно несколько заработных плат (разумеется, подпись в ведомости при этом подделывается).

Кстати, при таком мошенничестве предприятие несет убытки не только в сумме напрямую похищенных денежных средств —

оно еще и переплачивает налоги, исчисляемые от фонда заработной платы предприятия.

Аналогичным образом бухгалтер может поступить при отправке сотрудницы в декретный отпуск и в отпуск по уходу за ребенком. Как известно, по закону такая сотрудница получает не заработную плату, а пособие в размере, установленном действующим законодательством (разумеется, это пособие значительно меньше обычной заработной платы). Однако бухгалтер продолжает начислять заработную плату в полном объеме, выплачивая сотруднице только причитающееся ей пособие, а излишек направляя в собственный карман.

Важные нюансы, которые нужно учитывать при смене бухгалтеров

Часто главный бухгалтер, который недавно устроился на работу, заранее пытается свалить вину за свои возможные будущие прегрешения на своего предшественника.

Нужно помнить, что даже после увольнения главного бухгалтера последствия его недобросовестной работы могут аукаться еще долго: ведь ведение бухгалтерского учета — это непрерывный процесс, одним из принципов которого является использование переходящих остатков. Поэтому даже ошибка, совершенная несколько лет назад, может проявиться в любой момент.

Вот при поступлении на работу бухгалтер и старается как бы обезопасить себя от последствий возможных пробелов и ошибок, которые он по тем либо иным причинам не заметил в процессе приемки-передачи дел. Обычно это выглядит следующим образом.

Новый главный бухгалтер уже через несколько дней работы перечисляет руководителю обнаруженные им на данный момент недостатки в ведении учета и отчетности, которые допустил его предшественник. Руководитель, конечно, старается найти предыдущего бухгалтера и пригласить его в офис для объяснений. Однако не секрет, что часто бухгалтер, уволившись и получив на руки расчет и трудовую книжку, не имеет ни малейшего желания возвращаться к «делам давно минувших дней». А если он и появляется в офисе, то эмоционально заявляет, что «у него все в пол-

ном порядке, работал он хорошо, есть же подписанный акт приемки-передачи дел, и вообще непонятно, чего от него хотят». Вникать в суть проблем прежний бухгалтер не желает, и разговор заканчивается ничем.

А новый бухгалтер пишет служебную записку на имя руководителя предприятия, в которой перечисляет обнаруженные недостатки, при этом щедро сгущая краски и указывая то, чего и в помине не было, и заканчивает ее словами: «Учитывая все изложенное выше, я как главный бухгалтер не могу гарантировать достоверность и точность ведения бухгалтерского учета».

Руководитель предприятия может, конечно, возмутиться: как же, мол, так, вы пришли работать главным бухгалтером и самоустраняетесь от ответственности? А бухгалтер в ответ говорит: «Я же не виноват в таком положении вещей. Любой более-менее грамотный бухгалтер в моем положении напишет такую служебную записку. Вы только посмотрите…». И дальше начнет сыпать непонятными для директора бухгалтерскими терминами, определениями, формулировками и т. д. В конечном итоге руководителю предприятия не остается ничего другого, как согласиться с бухгалтером. Иной директор еще и подумает: «Однако какой грамотный у меня бухгалтер — столько недостатков сразу увидел! Хорошо, что я его взял на работу». И невдомек ему, что бухгалтер у него — самый обычный, просто он заранее страхуется от возможных неприятностей в будущем, причем не исключено, что возникновение этих неприятностей будет связано именно с работой нынешнего бухгалтера.

А вообще при увольнении главного бухгалтера руководитель предприятия должен проявлять бдительность и быть внимательным. Перед тем как его уволить, рекомендуется лично позвонить в банк, в налоговую инспекцию, в Фонд социальной защиты населения, а возможно — еще и в иные организации, в зависимости от вида деятельности предприятия, и навести справки: нет ли у этих организаций каких-то вопросов к увольняющемуся главному бухгалтеру? При наличии таких вопросов нельзя отпускать бухгалтера до тех пор, пока он их не решит.

Рекомендуется перед увольнением главного бухгалтера провести независимую аудиторскую проверку вашего предприятия

за какой-то период деятельности (например, за последний год или, как минимум — за последний квартал). Конечно, это потребует дополнительных расходов (услуги аудиторов нынче недешевы), но, возможно, избавит вас от серьезных проблем в будущем — ведь если прежний бухгалтер оставил после себя какие-то недоработки или хуже того — следы злоупотреблений, то это нужно выявлять своевременно.

Если же по тем либо иным причинам вы не можете перед увольнением бухгалтера провести аудиторскую проверку, то можно хотя бы выборочно проверить его работу. В частности, можно обратиться в банк с просьбой провести проверку соблюдения кассовой дисциплины на вашем предприятии (у банка есть такие полномочия). Кроме этого, необходимо сделать инвентаризацию кассы, а также провести полную инвентаризацию товарно-материальных ценностей на складе предприятия.

Особое внимание рекомендуется уделить безналичным платежам, которые осуществляет главный бухгалтер предприятия в преддверии увольнения. Следует учитывать, что в настоящее время распространен такой вид мошенничества: в один из последних дней работы (или — вообще в последний день работы) бухгалтер переводит определенную сумму безналичных денежных средств по каким-нибудь одному ему известным реквизитам, проще говоря — ворует деньги перед увольнением. Конечно, для осуществления такой аферы ему требуется сообщник, с которым он делится и который помогает потом получить эти деньги в виде «черного нала», разумеется — уже после увольнения.

Особо наглый бухгалтер может поступить перед увольнением еще хитрее. Не секрет, что новому главному бухгалтеру в первый день работы придется непросто — надо и платежи провести, и текучку не упустить, а все кругом новое, как бы не забыть чего. Тут на помощь и приходит увольняющийся бухгалтер. В последний день своей работы он говорит новому бухгалтеру примерно следующее: «Я тут вам помог немного: исправил ведомость, внес в программу последние данные, а также подготовил платежи. Все они согласованы с руководством, поэтому вам останется лишь оплатить их. Так что завтра вам будет чуть проще».

Новый бухгалтер, конечно, благодарит своего увольняющегося коллегу, не подозревая о том, что его подставили. А «подстава» заключается в том, что среди подготовленных платежей есть один платеж, который является воровством — прежний бухгалтер подготовил его, чтобы не самому воровать деньги, а толкнуть на это нового бухгалтера. Если на предприятии используется система электронных платежей типа «Банк – Клиент», то, как известно, подготовленные заранее платежи отправляются буквально нажатием нескольких клавиш. В этом случае доказать впоследствии причастность прежнего бухгалтера к воровству будет очень сложно.

Если же система типа «Банк – Клиент» на предприятии не используется, то прежний бухгалтер может предварительно подписать все платежные поручения у директора, а на «воровском» платежном поручении просто подделать его подпись. Однако в этом случае после того, как обман раскроется, бухгалтера-«оборотня» можно привлечь к ответственности: почерковедческая экспертиза покажет, что подпись директора на «воровском» платежном поручении подделал именно уволившийся бухгалтер. Ситуация предельно упрощается, если подпись директора на документах может ставиться с помощью его факсимиле (такое нередко практикуется на предприятиях, руководитель которых часто бывает в отъезде и не может своевременно подписывать документы) — в этом случае доказать что-либо будет трудно.

Ситуация станет совсем неприятной, если «воровской» платеж был отправлен на фирму, которая занимается так называемым «обналичиванием» денежных средств. Если в этом случае вы напишете заявление в полицию о хищении у вас денежных средств, то полиция (или — налоговая полиция) может заинтересоваться — не пользовалось ли ваше предприятие ранее услугами подобных фирм? Не исключено, что в конечном итоге вы, кроме потери украденных денег, получите еще и внеплановую налоговую проверку.

Хитрые приемы мошенничества, используемые кассирами

Среди недобросовестных кассиров получил распространение такой способ легкой наживы, как неполное оприходование поступающих в кассу предприятия наличных денежных средств. Отметим, что этот вид мошенничества удобно реализовывать на предприятиях, где наличные деньги поступают в кассу регулярно (например, каждый день) и от многих контрагентов (покупателей, заказчиков, подотчетных лиц и др.), иначе говоря — при большом документообороте, связанном с наличными деньгами.

Что делает кассир, принимающий наличные деньги? Правильно — выписывает приходный кассовый ордер. А у приходного кассового ордера есть отрывной корешок, который выдается лицу, сдающему наличные деньги в кассу; этот корешок является подтверждением того, что деньги поступили по назначению. Сумма поступивших в кассу денег указывается и в приходном кассовом ордере, и в отрывном корешке, в обоих случаях — цифрами и прописью. Казалось бы, все просто и понятно, и какие здесь могут быть злоупотребления?

Оказывается, могут, причем осуществляются они довольно просто, если не сказать — примитивно. Кассир в отрывном корешке указывает реальную сумму, которую он получил от лица, сдающего деньги в кассу, расписывается на корешке, ставит печать, отрывает его и вручает человеку, который сдал деньги. Тот разворачивается и уходит — для него операция закрыта, вопросов никаких нет. А вот уже в самом приходном ордере, на основании которого будет производиться оприходование денег в кассу, кассир указывает сумму, которая ниже реально поступившей. Разницу, разумеется, он кладет себе в карман. Если человек, получивший корешок приходного ордера, выбросит его или потеряет, то вскрыть и доказать такой обман будет практически невозможно.

Однако подобные злоупотребления могут быть обнаружены при проведении налоговой проверки. Например, инспектор заинтересуется подробнее операцией, расчет по которой производил-

ся наличными деньгами. Если наличные деньги поступили от юридического лица или индивидуального предпринимателя, то инспектор проведет встречную проверку, попросив предоставить тот самый корешок приходного кассового ордера (этот корешок является документом, подтверждающим факт совершения платежа, и должен храниться в бухгалтерии). Если мошенничество имело место быть, то, сверив сумму в корешке приходного ордера и в самом ордере, инспектор легко его обнаружит.

Кстати, подобный обман может обнаружиться и с другой стороны — когда на предприятии (либо у индивидуального предпринимателя), от которого поступили наличные денежные средства, проводится налоговая проверка, и инспектор решит провести встречную проверку по данной сделке. В этом случае он попросит предоставить приходный ордер, корешок которого хранится в проверяемой организации. И здесь тоже обман, если он имел место быть, легко будет обнаружен.

Некоторые наглые кассиры иногда позволяют себе вообще не приходовать в кассу суммы по некоторым приходным ордерам. Они поступают так: принял от человека деньги, заполнил и выдал ему корешок приходного кассового ордера — и на этом все. Деньги — в карман, а сам приходный ордер — в мусорку. Сразу выявить подобный обман непросто, но он может обнаружиться при проведении встречной налоговой проверки.

Практика показывает, что неполное оприходование поступающих в кассу предприятия наличных денежных средств — одно из самых распространенных злоупотреблений среди кассиров. В некоторых случаях суммы украденных таким образом денежных средств выглядят очень впечатляюще.

Обман и воровство на складе

Сплошь и рядом злоупотребления совершают материально-ответственные работники, отвечающие за сохранность ценностей на складе: заведующие складом, кладовщики и др. Далее рассмотрим несколько таких примеров.

Списание естественной убыли

Как известно, существует категория товарно-материальных ценностей, количество которых в процессе хранения или перевозки может уменьшаться естественным образом. К таким ценностям, например, можно отнести некоторые сыпучие продукты питания (сахар, мука, крупа и т. д.). В частности, вес одного и того же мешка с мукой может изменяться в зависимости от влажности окружающего воздуха: выше влажность — мука отсыревает, и, соответственно, ее вес увеличивается, если воздух сухой, то имеющаяся в муке влага испаряется и ее вес уменьшается.

На этой почве может возникать целый ряд злоупотреблений, совершаемых складским работником. Конечно, директору трудно спорить и что-то доказывать, когда количество товара уменьшается в пределах норм естественной убыли (эти нормы регламентированы соответствующими нормативными актами), однако, глядя на вещи реально, можно выявить мошенничество. Например, если заведующий складом сообщает вам, что количество сахара и муки уменьшилось в результате усушки, в то время как на улице уже неделю, не переставая, льет дождь и на складе наблюдается повышенная влажность, то у вас есть все основания подвергнуть его слова сомнению. Еще лучше — лично прийти на склад, проверить целостность мешков с сахаром и мукой и пересчитать их количество, сверив полученную цифру со складскими и бухгалтерскими данными.

При перевозке стеклянных бутылок с напитками есть нормы списания товара на бой, который может случиться при перевозке (например, нормой может считаться бой 2 бутылок на машину). Однако бой ведь может и не случиться! Но даже если все бутылки уцелели, вряд ли кладовщик упустит возможность списать на бой то, что можно по закону, и присвоить этот товар.

Махинации с нормами расхода ценностей

Как известно, расход сырья и материалов на производстве часто нормируется. Иначе говоря, если в соответствующем нормативном акте указано, что на производство одной единицы из-

делия можно использовать не более 1 г платины, то отпуск платины со склада в производство должен осуществляться в соответствии с этой нормой.

Но на практике иногда это значение превышается — правда, только документально. Например, в расходном складском ордере указывается, что в производство отпущено 3 г платины. В нашем примере это означает, что отпущенной платины должно хватить на 3 изделия. Реально же выпускается 2 изделия, а оставшийся 1 г платины недобросовестные складские работники могут присвоить.

Подобное мошенничество принимает иногда довольно широкие масштабы, ведь руководство предприятия не всегда четко знает, какие нормы на производство каких изделий существуют. И если за драгоценными металлами и иным дорогим сырьем контроль обычно более-менее налажен, то такие виды сырья, например, как лакокрасочные изделия, строительные материалы (в первую очередь — цемент), сыпучие продукты питания (сахар, сухое молоко), иногда списываются и впоследствии разворовываются в значительных масштабах. И вскрываются такие преступления, как правило, только в результате проведения тщательной проверки.

Однако при отпуске сырья и материалов в производство злоумышленники могут не только завышать, но и занижать количество используемых ценностей, причем — не документально (по документам все будет законно), а реально. Например, в соответствующем нормативном акте указано, что на производство одной единицы изделия можно использовать не более 1 г платины. В таком случае в расходном складском ордере количество отпускаемой платины указывается именно из такого расчета (например, 3 г на 3 единицы изделия). Но реально на производстве используется, например, 0,75 г на единицу изделия. Несложный подсчет показывает, что неучтенный остаток после производства трех единиц изделия составляет 0,75 г платины ($0{,}25 \times 3 = 0{,}75$), который, несомненно, будет похищен при первой возможности.

И еще полбеды, если все обернется только убытком для предприятия, сумма которого будет равняться стоимости похищенного сырья и материалов. Гораздо хуже, если подобное воровство

приведет к снижению качества выпускаемой продукции — в этом случае предприятию придется еще и нести ответственность перед покупателями за поставленный им недоброкачественный товар. А это может быть и уплата штрафов, пеней и неустоек, и возврат недоброкачественного товара (его придется либо списывать, либо приводить в порядок, что в любом случае повлечет за собой немалые затраты), и отказ от дальнейшего сотрудничества, и т. д.

Для предотвращения или хотя бы снижения проявления подобного мошенничества на производственном предприятии руководитель должен знать нормы расхода сырья и материалов, установленные соответствующими нормативными актами, для производства продукции, выпускаемой на предприятии. Периодически рекомендуется проводить на предприятии внезапные внутренние проверки; пусть не всегда такая проверка позволит выявить воровство, но, по крайней мере, сотрудники будут знать, что руководство предприятия держит вопрос расхода сырья и материалов на особом контроле.

Несоответствие отпускных и учетных единиц измерения

Для личной наживы нередко используется такой нехитрый прием, как несоответствие отпускных и учетных единиц товарно-материальных ценностей, хранящихся на складе.

Суть мошенничества заключается в том, что на складе, например, товарно-материальная ценность учитывается в единицах измерения «десяток», а отпускается со склада в единицах измерения «штука» (т. е. учетная единица измерения — «десяток», а отпускная — «штука»). При выписке расходного складского ордера в нем указывается количество, например, 5, но единица измерения при этом не указывается. Затем в карточке складского учета делается расходная запись на 5 единиц измерения товарно-материальной ценности (т. е. 50 штук). При этом реально со склада отпускается 5 штук товарно-материальной ценности (поскольку отпускная единица измерения — «штука»). Таким образом, путем несложной махинации со склада оказалось списано 45 штук товарно-материальной ценности.

Чтобы выявить подобное мошенничество, нужно обратить внимание на то, как заполнен расходный складской ордер. Если в нем не указана единица измерения, то есть основания полагать, что она не указана преднамеренно, чтобы по учету провести списание не того количества товарно-материальных ценностей, которое реально было отгружено. А если в складском ордере и указана единица измерения, то рекомендуется проверить соответствие учетных и отпускных единиц измерения в карточке складского учета и в расходном складском ордере и сверить данные с данными бухгалтерского учета.

Наиболее часто для такого мошенничества используются следующие пары единиц измерений: литр — декалитр, миллиграмм — грамм, комплект — штука, десяток — штука, набор — комплект, набор — штука.

Инвентаризация как средство контроля

В некоторых случаях для восстановления истинной картины того, как на предприятии налажен учет товарно-материальных ценностей и не имеют ли место быть злоупотребления, хищения и иные негативные проявления, необходимо проведение полной инвентаризации хранящихся на складе товарно-материальных ценностей.

Отметим, что в действующем законодательстве четко определены ситуации, когда необходимо проведение инвентаризации: при смене материально-ответственных лиц, по окончании календарного года, после обнаружения кражи, после случившихся форс-мажорных обстоятельств (пожар, наводнение и т. п.) и др. Однако при наличии соответствующих оснований целесообразно проведение внеплановых инвентаризаций.

Перед проведением полной инвентаризации руководитель должен издать соответствующий приказ по предприятию. Также необходимо создать инвентаризационную комиссию, состав которой отражается в приказе о проведении инвентаризации. Нередко в состав комиссии включают и руководителя предприятия, причем в качестве председателя инвентаризационной комиссии.

Далее нужно дать распоряжение бухгалтерии подготовить инвентаризационную ведомость. Форма этой ведомости утверждена законодательно и известна любому бухгалтеру. В инвентаризационной ведомости указывается состав инвентаризационной комиссии, дата проведения инвентаризации и иные обязательные реквизиты, в частности — полный перечень номенклатуры. Кроме этого, в ведомости отражаются остатки товарно-материальных ценностей по данным бухгалтерского учета, фактические остатки, установленные в результате проведения инвентаризации, и отклонение фактических данных от данных бухгалтерского учета. Фактические данные вносятся в инвентаризационную ведомость в процессе проведения инвентаризации (по принципу «посчитал реальный остаток — записал в ведомость»).

По окончании инвентаризации осуществляется сверка остатков товарно-материальных ценностей, числящихся по данным бухгалтерского учета, с фактическими остатками. При обнаружении излишков или недостач составляется соответствующий акт, а также с материально-ответственных лиц берутся письменные объяснения.

Перед проведением полной инвентаризации, в отличие от выборочных и тематических проверок, не нужно выполнять сверку складских ордеров с первичными документами и бухгалтерской ведомостью движения и остатков товарно-материальных ценностей. Это обусловлено тем, что выполнение такой сверки по всей номенклатуре — это слишком большая и трудоемкая работа, которая отнимет очень много времени. Поэтому вначале нужно провести инвентаризацию, сверить фактические данные с бухгалтерскими, и уже по тем позициям, по которым обнаружен излишек или недостача, провести такую сверку. Не исключено, что где-то обнаружится либо несоответствие данных складских ордеров и первичных документов, либо несоответствие остатка в карточке складского учета и бухгалтерской ведомости по движению и остаткам товарно-материальных ценностей и т. п.

Обычно перед проведением полной инвентаризации об этом ставится в известность заведующий складом. Это необходимо для того, чтобы в день проведения инвентаризации не произво-

дился прием или отпуск товарно-материальных ценностей со склада. Однако при проведении внезапной инвентаризации можно никого не предупреждать: если какие-то товарно-материальные ценности были приняты на склад или отпущены со склада в день проведения инвентаризации, то это должно быть подтверждено соответствующими документами (накладными).

Злоупотребления снабженцев и сбытовиков

Особо внимательно следует относиться к сотрудникам отделов поставок и снабжения (менеджерам по снабжению, начальникам данных структурных подразделений и т. д.). Здесь часто происходит один из самых популярных видов мошенничества, известный еще со времен СССР.

Известно, что в любом субъекте хозяйствования снабженец играет одну из ключевых ролей. В наибольшей степени это касается производственных компаний: для любого производства необходима не только большая номенклатура сырья и материалов, но и соответствующий инструмент, технологическая оснастка, спецодежда, производственное оборудование и т. д. Все это компания получает через департамент поставок, и редкая поставка может осуществиться без выплаты сотруднику данного структурного подразделения соответствующего поощрения, называемого откатом.

Сущность откатов, на которых «сидят» снабженцы, довольно проста и очевидна. Допустим, в обязанности сотрудника входит снабжение компании какими-то материалами. Эти материалы в настоящее время реализуют семь субъектов хозяйствования, причем приблизительно на равных условиях: если где-то ниже стоимость — необходима предварительная оплата, у другого поставщика стоимость выше — зато можно платить с отсрочкой, и т. д. Качество материалов везде тоже приблизительно на одном уровне. Кого же из них выберет снабженец?

А выберет он, в конце концов, того поставщика, представители которого будут оборотистее своих конкурентов и предложат

сотруднику отдела снабжения материальное поощрение только за то, что он будет покупать для своей компании материалы именно у этого продавца.

Аналогично выплачиваются откаты и при выполнении работ (оказании услуг): сотрудник заказчика получает материальное поощрение от подрядчика за то, что компания подпишет контракт именно с этим предприятием.

Напомним, подобные действия снабженцев можно квалифицировать как злоупотребление служебным положением с целью личной наживы и даже как получение взятки — это будет полностью соответствовать действующему законодательству. Несмотря на это, откаты снабженцам в современной России распространены повсеместно, в первую очередь потому, что подобные преступления практически невозможно раскрыть, доказать и довести до суда.

Попытка выкупа предприятия собственным менеджментом

В современной России одним из распространенных приемов мошенничества является операция, которая неофициально называется «выкуп предприятия собственным менеджментом». Сущность ее заключается в следующем.

Акционерам или собственникам не самого, мягко говоря, преуспевающего (а чаще всего — убыточного) предприятия делается предложение о продаже его наемным работникам, а именно топ-менеджерам. Потенциальные покупатели объясняют, что они хотят приобрести предприятие за счет собственных сбережений (которые, если и имеются, то обычно похищены на этом же предприятии, у этих же собственников). Недостающую сумму предполагается получить за счет привлеченных кредитов.

Топ-менеджеры убедительно и красочно рассказывают собственникам о том, что предприятие является убыточным и неперспективным, что его целесообразнее продать, и что они (топ-менеджеры), используя свои знания и опыт, смогут вывести компанию на достойный уровень.

Стоит ли говорить, что в этих речах нет и малой доли правды? Кстати, в большинстве случаев предприятие доводится до банкротства преднамеренно, именно с целью последующего его выкупа по смехотворно низкой, бросовой цене.

Однако у грамотных собственников в подобной ситуации должны возникнуть многие вопросы. Например, что мешает оздоровить и вывести на более-менее приличную рентабельность предприятие уже сейчас? Отсутствие необходимых полномочий? Так у топ-менеджеров они зачастую почти неограниченные. Некомпетентность персонала? И откуда у топ-менеджеров появились средства для выкупа предприятия? Не имеет ли это прямой причинно-следственной связи с его банкротством? Может, предприятие просто банально разворовано? И почему, если есть возможность привлечения кредитных средств для оздоровления предприятия, ей не воспользовались ранее, а довели фирму до разорения?

Ответы на эти, а также другие подобные вопросы помогут многое прояснить, а также разоблачить мошенников.

«Подводные камни» при покупке программного обеспечения

Один из наиболее бурно распространяющихся видов мошенничества — это получение работниками предприятий взяток и откатов при покупке предприятием программного обеспечения. Как известно, в последние полтора-два десятка лет в России активно и успешно развиваются предприятия, занимающиеся разработкой программного обеспечения. В большинстве случаев данная продукция ориентирована на предприятия и организации — по крайней мере, это относится к серьезным программным разработкам, стоящим немалых денег и предназначенным для автоматизации тех либо иных сфер деятельности: инженерных и исследовательских работ, медицинского обслуживания, бухгалтерского учета и т. д.

Для успешного продвижения и увеличения реализации своей продукции разработчики предлагают потенциальным покупате-

лям (вернее, некоторым их представителям) откаты. Например, если предприятие купило лицензий какой-либо программы на 10 000 долларов США — тогда его работник, ответственный за выбор программного обеспечения, получает на руки 300–500 долларов США наличными.

Причем таким работником может быть как руководитель предприятия, так и другой сотрудник. И если в первом случае все более-менее понятно, то во втором ситуация сложнее: «заинтересованный работник» должен убедить руководство компании, что для нее наиболее оптимальным является выбор именно вот этой программы. И далеко не все руководители предприятий понимают, что нередко выбор той или иной программы зависит не столько от ее функциональности и иных важных качеств, сколько от суммы отката, которую предлагают «офисному оборотню» разработчики той или иной программы за выбор именно их продукта (обычно эта сумма варьируется в пределах 3–10% от суммы сделки).

Следует отметить, что приобретенный программный продукт требует постоянного сопровождения и обновления, иногда — индивидуальных платных доработок, а это стоит немалых денег. Поэтому предприятие регулярно будет уплачивать поставщику программного обеспечения абонентскую плату, а индивидуальные платные доработки будут оплачиваться отдельно. Отметим, что без платных доработок удается обойтись далеко не каждому предприятию. А абонентская плата далеко не всегда подразумевает проведение бесплатных консультаций, вызова специалиста в случае необходимости в офис и некоторых других действий по сопровождению программы — часто их приходится оплачивать отдельно.

В связи с этим у «офисного оборотня» открываются новые возможности для злоупотреблений. Еще на этапе беседы поставщик может предложить ему откат не только от суммы приобретения, установки и внедрения программы, но и от суммы последующих платежей (абонентское обслуживание, платные доработки и т. д.). Иначе говоря, менеджер регулярно будет получать прибавку к заработной плате, причем фактически за счет предприятия. Более того, будучи лично заинтересованным в увеличе-

нии суммы платежей за сопровождение программы, он, возможно, будет выдумывать и заказывать разные платные доработки, которые на самом деле предприятию совершенно не нужны.

Есть даже такие «деятели», которые убеждают руководство компании, что необходимо приобрести не одну, а две или даже более программ аналогичного назначения. Мотивируют они это примерно так: мол, в «Программе 1» лучше всего делать то-то и то-то, в «Программе 2» — выполнять вот такие операции, в «Программе 3» — обрабатывать итоговые данные «Программы 1» и «Программы 2», и т. д. Если руководство по своей наивности соглашается с такими, с позволения сказать, «аргументами», то компания будет нести лишние затраты в огромном количестве, а менеджер — получать откаты сразу от нескольких поставщиков.

Откаты товароведам

Вид отката, который мы рассмотрим в данном разделе, почти повсеместно используется на торговых предприятиях, которые занимаются средне- и мелкооптовой торговлей товарами народного потребления (продукты питания, парфюмерия, бытовая химия, книги, одежда, обувь — т. е. все, что продается в магазинах). Эти предприятия поставляют свою продукцию непосредственно объектам розничной торговой сети (магазинам, торговым павильонам и т. п.).

Вы никогда не задумывались, почему в магазинах одни и те же сходные товары совершенно по-разному представлены на витринах? Одни находятся на самом видном месте и сразу бросаются в глаза, другие заметны не сразу, третьи вообще нужно искать на витрине долго и упорно, четвертые скрыты за третьими и т. д. А между прочим здесь многое зависит от того, насколько товаровед магазина заинтересован в реализации того или иного товара.

Многие предприятия, поставляющие свои товары в магазины, предлагают товароведу откат, рассчитываемый как процент от суммы реализации их продукции по итогам месяца. Например, поставщик макарон говорит товароведу: «Вы будете получать ежемесячно 5% от общей суммы реализации нашей продукции

в вашем магазине». Если, допустим, за отчетный месяц в данном магазине продалось макарон на 300 долларов США, то нетрудно посчитать, что «гонорар» товароведу составит 15 долларов.

Немного? А где вы видели магазин, торгующий одними макаронами? Ведь откаты предлагают поставщики и шоколада, и соков, и пива, и сигарет, и жевательных резинок, и всевозможных других товаров. Конечно, в крупных магазинах работает не один, а несколько товароведов, и их обязанности, как правило, разделены: один занимается мясом, другой — напитками, третий — бакалейными изделиями, четвертый — парфюмерией и т. д. Однако большинство из них получают откаты не от одного, а сразу от нескольких поставщиков, и в результате получается неплохая прибавка к заработной плате.

Размер отката может различаться и зависит от вида продукции, объемов продаж, щедрости и возможностей поставщика, а также от целого ряда иных факторов. Например, поставщик соков предлагает товароведу откат в размере 3% от суммы реализации, а поставщик макарон — 5%. Однако в данном магазине соков продается ежемесячно минимум на 500 долларов США, а макарон данного вида — только на 200 долларов. Несложный математический подсчет показывает, что товаровед получает от реализации соков больше дохода (500 × 3 / 100 = 15 долларов США), чем от реализации макарон (200 × 5 / 100 = 10 долларов США), несмотря на то, что процент отката за реализацию макарон выше.

Некоторые поставщики предлагают товароведам так называемые «скользящие» откаты. Экономический смысл таких откатов заключается в том, что процент отката зависит от суммы реализации. Например, сумма отката может рассчитываться по следующей шкале: при объеме месячной реализации данного вида продукции до 200 долларов США откат составляет 5%, от 200 до 500 долларов США — 6%, а свыше 500 долларов США — 8%. Подобная система стимулирования товароведов заставляет их стремиться к постоянному увеличению объемов продаж данного вида товара.

Во многом именно от того, насколько заинтересован товаровед в реализации тех либо иных товаров, и зависит их расстанов-

ка в торговом зале магазина. Разумеется, те товары, за реализацию которых товаровед получает максимальный откат, будут представлены в магазине на самом видном для покупателей месте. Далее — по убывающей: меньше откат за реализацию товара — и место для него на витрине выделяется похуже. Нет отката — хорошо, если этот товар вообще появится в торговом зале.

Как подсказывает практика, наиболее щедро выплачивают откаты товароведам представительства иностранных компаний: иногда процент отката доходит до 20% от общей суммы реализации. Вы никогда не задумывались, почему в каждом продовольственном магазине на самых видных местах расположена продукция популярных брендов?

Глава 3

Проверка, провокация или шантаж?

Проверка деятельности субъекта хозяйствования — малоприятная, но неизбежная процедура. Проверяют все подряд: правильность и полноту начисления и уплаты налогов, соблюдение кассовой дисциплины, валютного законодательства, санитарно-гигиенических норм, правил пожарной безопасности и т. д. Нередки случаи, когда в течение календарного года одно и то же предприятие проверяется несколько раз, и высокие комиссии едва успевают сменять друг друга (или вообще работают параллельно). В этой главе мы узнаем, как вести себя в случае проверки и каким образом можно минимизировать обусловленные ею потери.

Классификация современных проверок

Полномочиями проведения всевозможных проверок наделены многие государственные учреждения. В первую очередь среди них следует отметить налоговую инспекцию — именно этого органа больше всего боятся российские предприниматели и бизнесмены. Также мало приятного сулит встреча с работниками налоговой полиции и отдела по борьбе с экономическими преступлениями — эти организации тоже имеют право проведения проверок, причем последствия таких проверок могут быть гораздо более серьезными, нежели обычной налоговой проверки. От-

метим, что иногда проверка предприятия налоговой полицией либо отделом по борьбе с экономическими преступлениями начинается по результатам проверки, проведенной налоговой инспекцией.

Время от времени российские субъекты хозяйствования подвергаются проверкам со стороны других организаций: санитарно-эпидемиологической службы (сокращенно — СЭС, или, попростому — санстанция), пожарной службы, антимонопольного комитета, природоохранного комитета и т. д. О них мы расскажем ниже, а пока подробно остановимся лишь на проверках, проводимых налоговыми и правоохранительными органами, поскольку именно этих проверок больше всего боятся предприниматели и бизнесмены, и именно эти проверки чреваты наиболее серьезными (иногда даже фатальными) последствиями.

Все налоговые проверки можно разделить на пять групп: *плановые*, *тематические*, *выборочные*, *встречные* и *внезапные*. Кратко остановимся на каждой из них.

Плановым проверкам время от времени подвергается каждое предприятие. Целью такой проверки является соблюдение субъектом хозяйствования правил ведения бухгалтерского учета и отчетности, а также полноты и правильности исчисления и уплаты налогов и налоговой дисциплины. О такой проверке налоговые органы обычно предупреждают заранее. Если проведение проверки предполагается в помещении налоговой инспекции, то должностное лицо предприятия (обычно это главный бухгалтер) должно подготовить все необходимые документы за указанный период времени, сделать их опись и доставить в налоговую инспекцию, где будет оформлен акт приема-передачи документов согласно описи.

В ходе плановой проверки полностью исследуется вся деятельность предприятия за проверяемый период.

В среднем на российских предприятиях плановые налоговые проверки проводятся примерно раз в три года. Обычно плановая проверка охватывает последние два-три года деятельности предприятия и проводится в течение одного-трех месяцев (при условии, что в ходе проверки не выяснились обстоятельства, требующие ее продления).

Основное отличие *тематической проверки* от плановой заключается в том, что в ходе тематической проверки исследуется не вся деятельность предприятия, а только некоторые ее участки. Например, налоговые органы могут заинтересоваться тем, как предприятие уплачивает акцизы, и в ходе проверки будет исследоваться только торговля подакцизными товарами. Или проверка будет посвящена только реализации спиртных напитков, а остальные виды деятельности предприятия затрагиваться не будут.

Название *«выборочная проверка»* говорит само за себя: в ходе нее проверяются только выборочные документы, факты и др., интересующие в данный момент налоговую инспекцию. Выборка документов для проверки производится в соответствии с критериями, установленными проверяющим органом. Например, налоговая инспекция может потребовать для проверки все документы за последние полгода, подтверждающие реализацию табачных изделий на сумму не менее 10 000 рублей, или все приходы товарно-материальных ценностей от всех поставщиков за последние три месяца, и т. д.

Суть *встречной проверки* заключается в том, чтобы подтвердить (или, наоборот, — опровергнуть) сведения, которыми располагает налоговый орган о каком-либо контрагенте предприятия. Вот простой пример: ООО «Протон» отгрузило продукцию в адрес ЗАО «Торговля». Налоговая инспекция проводит плановую проверку ООО «Протон», и у нее вызвал сомнение товарно-сопроводительный документ, по которому ЗАО «Торговля» получило товарно-материальные ценности. В этом случае для подтверждения операции налоговая инспекция может потребовать у ЗАО «Торговля» копию товарно-сопроводительного документа на получение товаров от ООО «Протон». Подобные проверки и называются встречными.

Однако все без исключения предприниматели и бизнесмены больше всего опасаются *внезапных проверок*. О таких проверках никто заранее не предупреждает. Поэтому совершенно неожиданно (как правило, в самый неподходящий момент) в офисе, а возможно — и в других помещениях компании (на складе, в цеху и т. д.) внезапно появляются проверяющие. Именно при проведении внезапных проверок чаще всего работники налого-

вой инспекции и (или) правоохранительных органов обнаруживают и изымают приличные суммы «черного нала», неучтенные товарно-материальные ценности, а также фиксируют иные нарушения действующего законодательства.

Если при проведении проверки было выявлено много нарушений, то налоговая инспекция может передать результаты проверки для дальнейшего рассмотрения в правоохранительные органы (отдел по борьбе с экономическими преступлениями либо налоговая полиция).

Как действовать во время проверки

Любой контролер при определенном желании всегда без особых усилий найдет нарушения у любого субъекта хозяйствования. Бизнесмену же важно понять, чем руководствуется проверяющий в своем необузданном рвении найти нарушения, так как лишь четкое представление мотивов, которыми он руководствуется, позволит принять оптимальное решение насчет того, как лучше всего поступить в сложившейся непростой ситуации.

Если вашу компанию посетил враждебно и предубежденно настроенный контролер, то подобное поведение может быть обусловлено одним из указанных ниже факторов.

- У контролера отсутствует личная заинтересованность, и он лишь пытается добросовестно достичь запланированных его руководством показателей по «раскрываемости нарушений».
- Контролер старается «откопать» все, к чему только можно придраться, с единственной целью — получить взятку, и подобные действия можно объяснить следующими мотивами:
  - он действительно желает получить «мзду»;
  - данное вымогательство представляет собой не что иное, как заранее спланированную и направленную конкретно против вас провокацию.

Помимо указанных факторов объективного характера, на поведение контролера могут оказывать влияние и субъективные причины: плохое настроение, зависть и ненависть по отношению

ко всем подряд «буржуям-бизнесменам», личная неприязнь к владельцу бизнеса, склочный и «конфликтный» характер проверяющего и другие.

Чтобы своевременно определить, какие мотивы управляют контролером, важно получить хотя бы общие сведения о его личностных качествах. Для этого желательно иметь нечто вроде досье или картотеки с информацией обо всех местных налоговых инспекторах, контролерах со стороны пожарных и санитарных служб, сотрудниках иных контролирующих органов, в должностные обязанности которых входит контроль вашей компании.

Как правило, контролеров, находящихся в одном районе (там, где функционирует ваше предприятие), не очень много — в пределах пары-тройки десятков человек, и опытные коммерсанты обычно помнят всех «своих» проверяющих. Тем более им хорошо известны (а нередко — и лично знакомы) руководители районных инспекций разного ранга и профиля — это уж, как говорится, «сам бог велел».

Чтобы подобрать оптимальный подход к государственному служащему, необходимо выяснить его «подноготную»: кто ему покровительствует, за счет чего он продвигается по карьерной лестнице, кто его родственники, какая у него репутация, не брезгует ли взятками, какие у него сложились отношения с вашими конкурентами. Все эти полезные сведения легко получить, поговорив с коллегами бизнесменами, не забывая при этом систематизировать и анализировать полученную информацию. Подобные сведения на самом деле представляют собой важное условие гарантии безопасности компании в сложной или конфликтной ситуации, в особенности если она возникла благодаря стараниям недоброжелателей и конкурентов. Если же имеет место быть стандартная налоговая проверка, то сведения о личности контролера дают возможность бизнесмену грамотно определить его мотивацию и выработать оптимальный порядок действий.

Во время проведения проверок на предприятии рекомендуется организовать для проверяющих всестороннее содействие и лояльность. Очень хорошо, если помощь проверяющим будет оказывать специально назначенный работник, который «в курсе всех

дел и пояснит все, что надо». Было бы очень неплохо, если бы это был один из топ-менеджеров компании, имеющий внушительные полномочия, владеющий основами кризис-менеджмента, психологическими навыками и хорошо понимающий, как следует вести любые переговоры.

Как правило, работу с проверяющими поручают тем работникам, в обязанности которых входит ведение переговоров с деловыми партнерами: ведь умение грамотно договариваться и выходить из конфликтных ситуаций дано далеко не каждому. И если ваша компания располагает таким грамотным переговорщиком, то сотрудничество с государственными служащими и контролерами целесообразно поручить именно ему.

Сотрудника, который «работает» с представителями государственного аппарата, следует наделить эксклюзивными и неофициальными полномочиями. О них никто и ничего не должен знать, кроме высшего руководства компании. Ведь показать проверяющим интересующую их документацию может, в принципе, кто угодно, а вот иметь право предлагать чиновнику любой «нетрадиционный» или не совсем законный вариант решения проблемы может только «избранный».

Следует учитывать, что подобный «нетрадиционный» вариант не всегда означает прямой подкуп контролеров. Например, в ситуации, когда работники контролирующего органа просто обязаны дать отчет своему руководству об обнаружении какого-то количества нарушений, они не могут прийти к нему с пустыми (т. е. не содержащими штрафных санкций) актами. В подобных случаях с ними можно договориться, условившись о минимальной сумме штрафов и иных финансовых санкций. Ведь все мы знаем, что поговорка: «Кто ищет, тот всегда найдет» как ни к чему другому подходит к любым проверкам любого субъекта хозяйствования, поэтому нередко не имеет смысла расходовать время и нервы свои и контролеров, особенно тех, с которыми уже давно имеются неплохие отношения, и особенно тогда, когда сами они могут найти много разнокалиберных нарушений. Для этого специалист-переговорщик, имеющий соответствующие полномочия, просто заранее уведомляет контролеров, какие штрафы и финан-

совые санкции в состоянии понести компания. А контролеры, в свою очередь, предлагают «прейскурант» нарушений на предложенную сумму.

При этом контролеры могут «по знакомству» выполнить действительно хороший аудит и указать на серьезные ошибки, которые администрация компании впоследствии «обнаружит» собственными силами и без всяких финансовых и иных санкций. Подобный «аудит», само собой, должен оплачиваться, особенно если он действительно сделан на высоком уровне. Причем причитающееся вознаграждение вполне может быть официально перечислено специализированной аудиторской компании, которая впоследствии предоставит официальное аудиторское заключение, где будут перечислены все упущения, обнаруженные налоговиками. Стоит ли говорить, что реквизиты этой компании предоставят контролеры!

Отметим, что далеко не всегда имеет место материальное вознаграждение контролеров. Как правило, напрямую «получают благодарность» только работники самого нижнего звена и лишь в самом начале «сотрудничества». А вообще непосредственная дача взяток наиболее характерна лишь для мелких и средних компаний; что касается более высоких государственных служащих, то влиятельные бизнесмены находят с ними общий язык с помощью других методов поиска взаимной выгоды.

Как бы там ни было, полезно знать, что все виды взяток можно неофициально разделить на две категории: подкуп и вознаграждение.

- Подкуп — в данном случае материальное поощрение преподносится заранее, перед тем как государственный служащий предпримет какие-то действия (либо наоборот — платят за бездействие госслужащих).
- Вознаграждение — это материальное поощрение за уже произведенную работу, за использованное для этого личное время, за качество и оперативность, за внимательное отношение и т. д. Иначе говоря, вознаграждение по своей сути представляет собой презент и благодарность за оказанную помощь и гарантию благосклонного отношения в перспективе.

Если сотрудничество с государственными служащими подразумевает их материальное поощрение, то более привлекательным в данном случае будет вознаграждение. Однако следует сказать, что оно не всегда является оптимальным, если сотрудничество с работником государственного аппарата только начинается. Что касается подкупа, то он по своей сути более опасен и доказуем, к тому же получивший материальное подношение государственный служащий может оказаться ненадежным партнером и не выполнить то, что от него ожидает коммерсант или бизнесмен.

Имеется масса примеров, когда представители государственного аппарата принимают подношения за содействие в решении тех задач, которые вообще не входят в рамки их служебных полномочий, и впоследствии ничего не предпринимают для положительного решения вопроса либо, при наилучшем раскладе, предлагают лишь посреднические услуги для передачи «мзды» непосредственному исполнителю. По своей сути подобное поведение представляет собой не что иное, как банальное мошенничество, причем совершенное путем злоупотребления служебным положением, однако в таких ситуациях коммерсанты не могут оказать никакого влияния на мошенников: ведь, давая взятку, бизнесмен сам идет на совершение противоправного действия.

Именно с целью предотвращения вероятности мошенничества со стороны взяточников-обманщиков необходимо владеть максимальным количеством сведений о том государственном служащем, с которым вы предполагаете сотрудничать.

Предположим, в вашу компанию прибыл контролер, который ведет себя предубежденно и даже агрессивно, всем своим видом показывая, что с пустыми руками он отсюда не уйдет. Наиболее простой вариант — когда компании уже доводилось иметь дело с этим контролером и точно известно, что это действительно полезный человек. В данном случае необходимо понять, по какой причине он пришел вне графика, а также полюбопытствовать относительно «размера его заинтересованности». При желании вы можете даже поторговаться и существенно уменьшить запрошенную сумму: в конце концов, это нормальная практика деловых отношений.

А вот если бизнесмен отдает себе отчет в том, что за его предприятием действительно водятся грешки, и об этом знает контролер (который может даже делать соответствующие намеки) — ситуация будет гораздо сложнее. В данном случае сэкономить почти нереально, поскольку налицо — характерный признак утечки секретной информации от своих же работников. Стоит ли говорить, что эту утечку следует максимально быстро найти и нейтрализовать!

Еще более запутанная ситуация — это когда «набивается в друзья» новый и совершенно незнакомый контролер. Здесь не нужно торопиться с принятием решения: лучше всего максимально затягивать время и всячески пытаться навести справки об этом человеке. Следует выяснить, может ли этот государственный служащий принести в будущем пользу, имеет ли смысл для компании такое «сотрудничество» и, конечно, — во сколько оно обойдется. Также необходимо взглянуть на ситуацию и с другой стороны, в частности — прикинуть, какими последствиями чревато игнорирование требований контролера. Бывает так, что наиболее подходящим вариантом действия является обращение в правоохранительные органы.

Тем более что всегда есть вероятность стать жертвой организованной провокации. При наличии малейших сомнений следует сразу предпринимать оборонительные меры и стараться разрешить конфликт официальными средствами, например — в судебном порядке.

Не следует при появлении проверяющих опережать события и говорить о том, о чем они не спрашивают (некоторые люди пытаются таким образом запутать проверяющих, уводя их от сути дела): отвечать нужно только на поставленные вопросы, следуя принципу «сказал много, и в то же время — ничего не сказал». Опытный проверяющий быстро поймет, к чему клонит сотрудник предприятия, пытающийся отвлечь его внимание, а это в данном случае совершенно недопустимо.

В первую очередь следует учитывать, что в подобной ситуации представители проверяющих могут вести себя достаточно бесцеремонно и даже нагло, демонстрируя свое превосходство

и, как говорят, «кидая понты». Необходимо понимать, что таким поведением они пытаются не унизить того или иного сотрудника, а обескуражить его, заведомо убедить в том, что он совершил тяжкое преступление (особенно если человек был пойман с «черным налом»), добиться его растерянности. Если это им удастся — с высокой долей вероятности можно утверждать, что этот сотрудник окажет содействие налоговым или правоохранительным органам.

Поэтому в любой ситуации, как бы трудно не пришлось, важно сохранить самообладание и уверенность в себе. Кстати, как только проверяющие вошли в помещение, следует сразу же попросить их предъявить документы, подтверждающие их полномочия, и переписать данные этих документов.

В некоторых случаях (разумеется, при наличии серьезных оснований) представители налоговой полиции или иных фискальных органов могут появиться в помещении с криками «Не двигаться!», «Всем стать лицом к стене!» и т. п. Не стоит забывать, что, скорее всего, они действуют по закону (мало ли что — может, какой-то «доброжелатель» из числа ваших конкурентов им сообщил, что в помещении вашей компании готовится террористический акт). В подобной ситуации не стоит корчить из себя героя и требовать «немедленно покажите ваши документы»; лучше дождаться прояснения ситуации и уже тогда попросить незваных гостей показать свои документы. До предъявления ими документов не нужно идти на контакт, отвечать на вопросы — вы имеете на это законное право: не обязаны же вы беседовать неизвестно с кем и тем более — давать показания неизвестно кому.

На каверзные вопросы и реплики проверяющих лиц рекомендуется либо вообще не реагировать, либо отвечать так, чтобы не подставить себя и предприятие. Например, на каверзный вопрос (насчет «черного нала»): «Так, значит, вы с наличкой имеете дело?» — можно достойно ответить: «Да, имею — получаю аванс и заработную плату в бухгалтерии нашего предприятия. Подтверждением моих слов являются мои подписи в ведомостях по заработной плате, где я расписывался в получении». На ответную реплику: «Будем делать вид, что ничего не знаем, дурачком прикидываться?» в свою очередь можно ответить: «Да, я не очень

понимаю, что происходит, но хотел бы это узнать». И через минуту добавить: «Тем не менее, как честный гражданин, я готов оказать любое посильное содействие налоговым (правоохранительным) органам в установлении истины». Подобные беседы следует вести спокойным и уверенным в себе тоном; если это не получается, то каверзные вопросы и реплики проверяющих лучше пропускать мимо ушей.

Даже если, на ваш взгляд, представители правоохранительных органов ведут себя бесцеремонно и грубо, отвечать им тем же не следует. Помните: на их стороне сила, а на вашей — ничего.

Ни в коем случае не нужно строить из себя человека, у которого «все схвачено», и грозить проверяющим своими связями с их начальством, мэром, прокурором, министром, депутатом или кем-то там еще, даже если у вас такие связи действительно есть. Поверьте: подобные угрозы проверяющие в силу специфики своей работы выслушивают регулярно, и вы этим ровным счетом ничего не добьетесь (разве что дополнительно настроите их против себя). Если же вы действительно имеете хорошие связи, то тихо-мирно воспользуйтесь ими позже.

Превентивные меры, позволяющие предотвратить возможные неприятности

Чтобы минимизировать возможные неприятности от предстоящих проверок, следует заранее позаботиться о безопасности и по мере возможности «прикрыть» все имеющиеся на предприятии «узкие места».

К сожалению, многие предприятия пренебрегают элементарными правилами безопасности. Однако не стоит забывать, что если ваше предприятие окажется не готовым к встрече с проверяющими, то последствия для него могут быть очень печальными, если не сказать — катастрофическими: за многие виды нарушений российским законодательством предусмотрены очень суровые санкции. Конечно, очень хорошо, если ваше предприятие до настоящего момента миновали всякие внезапные провер-

ки, налеты фискальных органов и т. п.; будем надеяться, что так будет и в дальнейшем. Но всегда нужно быть готовым к тому, что события пойдут совсем по иному, не такому благополучному сценарию — такая готовность поможет с честью и минимальными потерями выйти из любых затруднительных ситуаций.

В частности, рекомендуется иметь в офисе такой полезный аппарат, как уничтожитель бумаг. С его помощью можно оперативно уничтожить все бумаги и документы, которые могут представлять интерес для проверяющих: долговые и расчетные записи, ведомости по начислению и выплате «черной» заработной платы, записи по прочим выплатам, координаты «финансовых компаний», с которыми сотрудничает предприятие, и т. д. Уничтожитель бумаг должен быть из числа тех, которые превращают бумаги и документы в труху (в частности, нежелательно использовать уничтожители, разрезающие бумаги по полоскам, поскольку уничтоженные таким образом бумаги можно восстановить если не полностью, то хотя бы частично).

Если ваше предприятие ведет «черную» бухгалтерию, и ею занимается отдельный сотрудник, то для него рекомендуется оборудовать отдельное неприметное помещение, которое будет располагаться в стороне от других помещений фирмы. Это может быть, например, комната в самом конце коридора (например, возле лестницы «черного хода»), подальше от бухгалтерии, кабинета директора и финансового отдела, с табличкой на двери, на которой написано что-нибудь совершенно постороннее («Отдел по технике безопасности», «Комната приема пищи» и т. п.). В таком случае внезапно появившиеся проверяющие могут просто не обратить на нее внимание, что позволит сотруднику, ответственному за ведение «черной» бухгалтерии, своевременно уничтожить все компрометирующие материалы и принять другие необходимые меры безопасности.

Совет

Было бы очень неплохо, если бы помещение «черной» бухгалтерии имело два разных выхода: один — самый обыкновенный, как и у других помещений, другой — незаметный, ведущий куда-нибудь на лестницу «черного хода» или вообще прямо на улицу.

На некоторых предприятиях руководители периодически устраивают своеобразные тренинги, на которых каждый сотрудник отрабатывает линию поведения на случай внезапной проверки. В процессе тренинга все выглядит «по-настоящему»: на предприятие приходят злобные и агрессивно настроенные проверяющие, кричат «всем оставаться на своих местах!», проводят обыск во всех помещениях, грубо и бесцеремонно допрашивают сотрудников и т. д. В качестве проверяющих могут выступать, например, друзья и коллеги директора (такие же руководители предприятий) либо его знакомые из правоохранительных органов, либо работники соседнего офиса и т. п. Наиболее предпочтительный вариант — это, конечно, участие в тренинге работников фискальных органов (налоговой инспекции, отдела по борьбе с экономическими преступлениями, налоговой полиции и т. п.): в данном случае все будет выглядеть наиболее правдоподобно, следовательно — тренинг будет эффективным.

Совет

На компьютере сотрудника, который занимается ведением «черной» бухгалтерии, должна быть установлена программа, предназначенная для быстрого удаления информации с компьютера — это позволит в случае необходимости оперативно уничтожить все хранящиеся в компьютере компрометирующие материалы. Если же для удаления данных использовать традиционные методы (клавишу F8, сочетание клавиш Shift+Delete), то их впоследствии можно восстановить, и это очень хорошо умеют делать специальные службы в фискальных органах.

Если на расположенном в офисе принтере распечатывались «левые» документы (фальшивые накладные, фиктивные договоры и т. п.), а также поддельные печати и штампы — то при появлении в офисе проверяющих следует незамедлительно выбросить картридж из этого принтера. Дело в том, что проверяющие могут распечатать на принтере образцы, чтобы впоследствии сравнить их с изъятыми в офисе подозрительными документами. Образцом может быть произвольный текст: важно лишь то, что он будет распечатан на определенном принтере с помощью определенного картриджа, с характерным составом чернил, особенностями печати и иными признаками, позволяющими идентифицировать конкретный картридж принтера.

После этого выполняется экспертиза изъятых в офисе документов и полученных образцов, и сравниваются результаты. В итоге может случиться так, что, например, приходная накладная, подтверждающая приход на вашу фирму товарно-материальных ценностей от некоего поставщика, находящегося за пару тысяч километров, на самом деле распечатана (вместе с печатью этого поставщика) на принтере вашего же предприятия. Как говорится, без комментариев…

Кстати, иногда на «левых» документах за руководителей и иных должностных лиц несуществующих фирм расписываются сотрудники своего же предприятия (мол, какая разница, лишь бы подпись была). Учтите, что почерковедческая экспертиза все покажет с почти стопроцентной достоверностью: у всех сотрудников офиса будут взяты образцы почерка и сравнены с подписями на сомнительных документах. Опять же — может оказаться так, что на документе, выписанном от имени расположенной за несколько тысяч километров фирмы, за директора этой фирмы расписался сотрудник вашего предприятия. Как минимум, этому сотруднику придется отвечать за подделку документов.

Если вы виноваты. Как незаметно для контролеров устранить некоторые нарушения

Далее — несколько рекомендаций относительно того, как устранить некоторые допущенные в учете и отчетности нарушения и сделать их незаметными для контролеров.

Оформление неучтенной реализации товара

Реализация товаров (работ, услуг) за наличный расчет без соответствующего отражения данной операции в бухгалтерском учете (т. е. без оприходования в кассу предприятия поступивших наличных денег, без оформления соответствующих товарно-сопроводительных документов на реализованный товар и др.) —

наиболее распространенный источник возникновения неучтенных денежных средств, попросту говоря — «черного нала».

Предположим, ваша компания реализовала сколько-то товара за наличный расчет без оформления соответствующих документов. Что получилось в результате? С одной стороны — сумма неучтенных наличных денежных средств, которые можно использовать по своему усмотрению (выплатить сотрудникам заработную плату «в конвертах», приобрести «за наличку» бензин для машины директора и т. д.). С другой стороны — недостача товарно-материальных ценностей на складе (ведь отпуск реализованных товаров не отражен соответствующим образом в официальном учете). При проведении внезапной инвентаризации товарно-материальных ценностей на складе (это вполне могут сделать налоговые органы) недостача будет легко обнаружена.

Значит, на сумму недостачи необходимо найти оправдательные документы. В подобных ситуациях наиболее распространенным оправдательным документом является акт на списание товарно-материальных ценностей. В качестве причины списания можно указывать, например, истечение сроков годности, потерю товарного вида, порчу грызунами и т. д. Акт на списание утверждается руководителем предприятия, после чего бухгалтерия принимает его к исполнению.

Еще один распространенный вариант для оправдания недостачи товарно-материальных ценностей, реализованных за наличный расчет, — это «отправка» их на ответственное хранение. В данном случае следует заключить с какой-либо организацией договор ответственного хранения и выписать накладную, по которой товар «сдается» на ответственное хранение (разумеется, эта накладная должна быть соответствующим образом заверена «принимающей» организацией). В таком случае при проведении внезапной инвентаризации вопросов по недостаче не возникнет; однако если налоговые органы захотят немедленно проверить наличие недостающих товарно-материальных ценностей на складе ответственного хранения, где они должны находиться согласно оформленной накладной, то может возникнуть весьма нелицеприятная ситуация, из которой трудно будет найти правдоподобный выход.

Легализация активов через вклады собственников и учредителей предприятия

В российской практике широко распространен такой способ легализации активов предприятия, как прием новых членов в состав его учредителей либо пополнение уставного капитала предприятия нынешними его участниками. Рассмотрим несколько таких ситуаций на конкретных примерах.

Предположим, что предприятию необходимо поставить на баланс новый объект основных средств, приобретенный неофициально, т. е. без оформления соответствующих товарно-сопроводительных документов и отражения данной хозяйственной операции в бухгалтерском учете. В данном случае надо внести соответствующие изменения в учредительный договор предприятия, отразив в нем тот факт, что кто-то из нынешних учредителей компании, либо ее новый учредитель передает личное имущество предприятию в виде вклада в его уставный капитал. Этим имуществом и является объект основных средств, которые необходимо поставить на баланс.

После оформления необходимых документов и проведения их по бухгалтерскому учету активы и пассивы предприятия изменились, как и положено, на одинаковую сумму: в активы добавлена стоимость объекта основных средств, а в пассивы — задолженность по расчетам с учредителями.

Впоследствии эта задолженность списывается на прирост уставного капитала; тем самым будет документально подтверждено увеличение уставного капитала предприятия за счет легализованного объекта основных средств.

В результате несложных (а самое главное — полностью легальных и законных) бухгалтерских операций на баланс предприятия поставлен объект основных средств, который ранее был приобретен неофициально. Это увеличение активов предприятия сбалансировано увеличением на эту же сумму его пассивов, а именно — увеличением уставного капитала предприятия.

Пополнение уставного капитала предприятия как средство легализации активов удобно использовать и для «отмывания» неуч-

тенных наличных денежных средств (попросту говоря, «черного нала»). Отметим, что в данном случае также следует внести изменения (дополнения) в учредительный договор предприятия. В этих изменениях (дополнениях) должно быть указано, что кто-то из участников предприятия (либо его новый участник) делает вклад в уставный капитал в виде наличных денежных средств, сдаваемых в кассу предприятия.

После формирования соответствующей бухгалтерской проводки активы и пассивы компании изменятся на одинаковую сумму: в активы добавится сумма «отмытых» денежных средств (увеличился остаток по кассе), а в пассивы — задолженность по расчетам с учредителями.

Впоследствии эта задолженность, как и в предыдущем примере, списывается на счет прироста уставного капитала; тем самым будет документально подтверждено увеличение уставного капитала предприятия за счет легализованных денег.

Аналогичным образом можно легализовать неучтенные в бухгалтерском учете товарно-материальные ценности, хранящиеся на складе предприятия (сырье, материалы, предназначенные для реализации товары и т. д.). Как и в предыдущих примерах, вначале следует внести соответствующие изменения в учредительный договор предприятия. В изменениях требуется указать, что кто-то из участников предприятия (либо его новый участник) делает вклад в уставный капитал в виде товарно-материальных ценностей (перечень товарно-материальных ценностей и их стоимость, составляющая сумму вклада, прилагается).

Подобным образом можно легализовать и поставить на баланс и другие активы предприятия: оборудование к установке, нематериальные активы, безналичные денежные средства, ценные бумаги и др.

Уменьшение налогооблагаемой базы

Многие предприятия на протяжении долгого времени применяют метод минимизации прибыли, подлежащей налогообложению, основанный на списании мнимых расходов.

Например, внутри компании вполне реально списать расходы на приобретение хозяйственных и канцелярских товаров, расходных материалов, бухгалтерской литературы, а также иных активов, наличие которых проверить трудно или невозможно. Для оправдания расходов, само собой, необходимо иметь соответствующие оправдательные документы (товарно-транспортные и товарные накладные, кассовые чеки, бланки строгой отчетности и др.). Стоит ли говорить, что подобная документация в изобилии имеется на любом уважающем себя «черном рынке»! А некоторые документы можно изготовить своими силами — например, распечатать кассовые чеки с помощью собственного незарегистрированного кассового аппарата.

Совет

Немногие знают, что сумму средств в пределах 4% от фонда заработной платы вполне официально можно списывать на представительские расходы — разумеется, при наличии соответствующих оправдательных документов. Например, под видом представительских расходов удобно покрывать стоимость питания работников компании в столовой.

Настоящий «Клондайк» для создания мнимых расходов — это компьютерный парк. Не секрет, что компьютеры могут выходить из строя по причине поломки или из-за вируса, а устранение подобных неисправностей может вылиться в кругленькую сумму. Услуги по ремонту и обслуживанию компьютеров вполне может «оказывать» дочерняя фирма, работающая по упрощенной системе налогообложения.

Для уменьшения налогооблагаемой прибыли можно «арендовать» у своих работников автомобили, офисные компьютеры и другую оргтехнику — помимо минимизации прибыли это позволит выплачивать сотрудникам-«арендодателям» необлагаемую налогами заработную плату в виде арендной платы.

Но если налоговые органы заподозрят, что расходы, о которых мы рассказали в данном разделе, «притянуты за уши», то санкции могут быть весьма суровыми, причем наказано будет как предприятие, так и его ответственные лица.

Минимизация НДС через штрафы и неустойки

Эта хитрая схема зародилась довольно давно, и широко используется российскими субъектами хозяйствования. Суть ее заключается в том, что в договоре купли-продажи цена товарно-материальных ценностей искусственно и значительно занижается. При этом она делится на две части, первая из которых представляет собой платеж за полученные товары, а вторая — сумму штрафных санкций, которые налагаются на покупателя за «ненадлежащее исполнение договорных обязательств». Это «ненадлежащее исполнение» может заключаться в чем угодно: просрочка платежа, некачественная и несвоевременная транспортировка, иные обстоятельства, которые вызывают неудобства у другого участника сделки. Разумеется, применение штрафных санкций должно быть отражено в договоре.

Зачем это нужно? Дело в том, что штрафы, пени и неустойки, полученные предприятием от контрагента за ненадлежащее исполнение договорных обязательств, относятся к внереализационным доходам, следовательно — не облагаются НДС. Юридически размер неустойки может быть каким угодно, но при использовании подобных схем следует придерживаться здравого смысла и чрезмерно не занижать стоимость товарно-материальных ценностей, чтобы не вызвать лишних подозрений у налоговых и фискальных органов.

В результате наша сделка полностью закрыта: задолженность по счету 60 (как дебиторская, так и кредиторская) отсутствует, на баланс предприятия поставлены неучтенные ранее товарно-материальные ценности, в результате чего увеличились активы предприятия. В то же время на такую же сумму увеличились и пассивы предприятия, а именно кредитовое сальдо по счету 98 «Доходы будущих периодов» либо по счету 90 «Продажи» (субсчет «Выручка»).

Специфика «неналоговых» проверок

Как уже отмечалось, предприятие может подвергаться не только налоговым проверкам и «налетам» правоохранительных ор-

ганов. «Сунуть свой нос» на ваше предприятие могут и представители иных государственных структур: пожарной охраны, санстанции, природоохранных организаций, антимонопольного комитета и других. Далее речь пойдет о том, чем чревато появление таких контролеров в вашей компании.

Все перечисленные инстанции объединяет одно: имеющиеся у них полномочия позволят им практически парализовать работу предприятия под любым удобным предлогом.

Проверки санстанции

С проверками, которые проводит санитарно-эпидемиологическая служба, приходится сталкиваться почти каждому предпринимателю или бизнесмену. Последствия подобных проверок могут быть самыми серьезными: наложение крупных штрафных санкций, приостановка либо полное прекращение производственного процесса, изъятие продукции и т. д. Отметим, что нередко подобные санкции контролеры накладывают благодаря правовой неграмотности коммерсантов, а не в связи с имеющимися нарушениями.

Следует помнить, что санитарно-эпидемиологическая служба подчиняется Министерству здравоохранения Российской Федерации, а также то, что должностные лица этой структуры наделены полномочиями только на соответствующих административных территориях. Среди наиболее существенных полномочий можно выделить следующие:

- разрешение на выделение земельного участка (без подписи санитарного врача вы не откроете торговую палатку, не построите магазин или производственный цех и т. д.);
- заключение о соответствии уже построенных либо реконструированных зданий, сооружений, помещений и т. п. действующим санитарным нормам и требованиям;
- заключение о необходимости проведения санитарно-гигиенической экспертизы производимой продукции и продаваемых товаров;
- контроль соблюдения санитарных и противоэпидемических мероприятий на предприятиях и в организациях;

- выдача разрешения на право осуществления определенных видов деятельности;
- беспрепятственный вход на территорию предприятия во все его офисные, производственные, подсобные и иные помещения (разумеется, при предъявлении соответствующего документа).

Представители санстанции наделены правом отбора образцов сырья, продукции или товаров для проведения санитарно-гигиенических исследований в соответствии с действующим законодательством. Ну и, само собой, работники СЭС имеют право наказывать нарушителей санитарного законодательства. Среди наиболее распространенных мер воздействия можно отметить следующие:

- ограничение или приостановка деятельности субъекта хозяйствования;
- введение временного или полного запрета на деятельность предприятия;
- введение запрета на строительство либо реконструкцию объектов;
- введение временного запрета на производство либо реализацию продукции, товаров, работ, услуг;
- временная остановка либо полное прекращение инвестиционной деятельности предприятия;
- распоряжение руководству компании на отстранение от исполнения своих обязанностей определенных должностных лиц;
- конфискация либо временное изъятие опасных для здоровья граждан и состояния окружающей среды продуктов, товаров, химических веществ.

Работники СЭС могут делать выводы на основании фактов, которым на предприятии не придают особого значения. Например, на склад внезапно пришли контролеры из санстанции и увидели на полу лужу. Это дает им все основания полагать, что, во-первых, товарно-материальные ценности хранятся в ненадлежащих условиях (если ваша компания работает с продуктами пита-

ния, ждите крупных неприятностей), а во-вторых — работники склада вынуждены выполнять свои должностные обязанности во вредных условиях (сырость и т. п.). Предписание в таком случае может быть строгим: до устранения выявленных недостатков эксплуатация помещения запрещается.

А если в реальности эта лужа никакой опасности и дискомфорта не создает, но для устранения необходимо выполнение длительных и дорогостоящих работ (устранение щели в фундаменте, ремонт кровли и т. п.)? Получается, все это время склад будет простаивать. Хорошо, если у вас в запасе имеются другие складские помещения или есть возможность временного размещения товаров на ответственное хранение. В противном случае ваша компания может понести серьезные убытки.

Важно!

Помните, что санстанция настроена на применение суровых санкций в первую очередь при обнаружении следующих нарушений: наличие грызунов (крыс, мышей), вредных насекомых (тараканов, прусаков и др.), испорченных продуктов, повышенной влажности, несоблюдении температурного режима для данного вида помещений, отсутствие либо неисправность вентиляции, хранение рядом несовместимых ценностей (например, бензина и продуктов питания).

Все проверки, которые проводят представители СЭС, можно разделить на два вида: *плановые* и *внеплановые*. *Плановые проверки* проводятся тогда, когда их необходимость очевидна для всех: обследование зданий (помещений) после строительства или реконструкции; выделение земельного участка; выдача разрешения на право осуществления того или иного вида деятельности и т. д. Что касается *внеплановых проверок*, то они проводятся внезапно при получении сигналов либо при возникновении подозрений о том, что на предприятии имеются факты нарушения санитарного законодательства.

Результаты проверки оформляются соответствующим актом, который подписывает представитель санстанции и руководитель предприятия (один экземпляр акта остается на предприятии). При обнаружении нарушений составляется протокол о нарушении санитарного законодательства и постановление (предписание), в котором указываются наложенные штрафные санкции.

Проверки пожарных служб

Проверка со стороны пожарной службы также может создать проблемы. Нет, никто не спорит с тем, что противопожарная безопасность — это исключительно важно для всех и каждого. А если в то время, когда фирма начинала работу, действовали одни нормы и правила, а к моменту прихода контролеров они изменились?

Например, ваши производственные помещения расположены на первом этаже, окна которых защищены распашными решетками для защиты от несанкционированного проникновения. Но проверяющие из пожарной службы говорят, что раньше такие решетки разрешалось использовать, а сейчас нет (мол, в случае пожара они помешают людям покинуть помещение через окна). На все возражения, вроде: «Так ведь решетки распашные, в течение рабочего дня мы их открываем, окна становятся свободными» и т. п., следует хорошо знакомый каждому жителю бывшего СССР ответ: «Не положено!»

Что делать? Остается два выхода: либо давать взятку пожарным за «закрытие глаз» на нарушение, либо подыскивать другие производственные помещения (нельзя же оставить дорогостоящее оборудование в помещении без защитных решеток на окнах). Очевидно, что первый вариант — и логичней, и практичней.

Особо строго пожарные подходят к следующим нарушениям: неисправность или ненадлежащий вид электропроводки (оголенные провода и т. п.), отсутствие пожарных выходов и невозможность быстрой эвакуации, несоблюдение правил эксплуатации электрических приборов (кипятильнику в офисе не место), нарушение техники противопожарной безопасности, курение в неустановленных местах и др.

Проверяющие из пожарной службы наделены следующими полномочиями:

- проведение обследований и проверок зданий, сооружений, территорий и внутренних помещений субъектов хозяйствования (как в рабочее, так и в нерабочее время);
- беспрепятственный вход в жилые помещения и доступ на земельные участки при наличии сведений об угрозе пожара или нарушении требований противопожарной безопасности;

- проверка технической документации предприятия, имеющей отношение к противопожарной безопасности (приказы, распоряжения и т. д.);
- выдача руководителям субъектов хозяйствования предписания по устранению выявленных нарушений требований противопожарной безопасности;
- привлечение к ответственности виновных в нарушении действующих норм противопожарной безопасности.

Что касается ответственных работников предприятия, которое подвергается проверке органами пожарной службы, то они имеют право присутствовать при проверке и задавать любые интересующие их вопросы, касающиеся проведения проверки и правил противопожарной безопасности. Представитель предприятия обязан предоставить контролерам журнал учета проверок, в котором работник пожарной службы должен сделать запись о проведенной проверке.

Важно!

Администрация предприятия, на котором проводится проверка соблюдения правил противопожарной безопасности, обязана обеспечить беспрепятственный доступ контролеров во все здания и помещения, а также по всей территории предприятия. Кроме этого, инспекторам пожарной охраны необходимо предоставить всю запрошенную документацию (разумеется, речь идет о документации, которая касается вопросов пожарной охраны).

Если в результате проверки были обнаружены нарушения, то выписывается соответствующее предписание, которое имеет юридическую силу независимо от того, согласен с ним руководитель субъекта хозяйствования либо нет. Свое несогласие с предписанием администрация компании может выразить в десятидневный срок с момента его выписки, обратившись устно или письменно к начальнику местного отделения пожарной службы.

Примечание

В соответствии с действующим законодательством, к должностным лицам предприятия, виновным в нарушении правил противопожарной безопасности, могут применяться два вида взыскания: административное предупреждение либо штраф.

Проверки, проводимые пожарной службой, можно разделить на два вида: *плановые* и *внеплановые*. *Плановые проверки* проводятся в соответствии с графиком, который утвержден главным государственным инспектором по пожарному надзору данного города (района, области, иной административно-территориальной единицы). На такой проверке в обязательном порядке должен присутствовать уполномоченный представитель проверяемого предприятия, поэтому предварительно проверяющие должны уведомить администрацию компании о своем предстоящем визите.

Что касается *внеплановых проверок*, то они делятся на три вида.

- **Контрольные.** Такая проверка проводится в том случае, если при проведении плановой проверки были выявлены нарушения, которые необходимо устранить в соответствии с выданным предписанием. В ходе контрольной проверки инспекторы проверяют устранение этих нарушений; проверять что-то кроме этого они не имеют права.
- **Оперативные.** Такие проверки проводятся в том случае, если работникам пожарной службы стало известно о наличии на предприятии нарушений требований противопожарной безопасности, из-за чего существует угроза пожара. Также оперативные проверки проводятся после случившегося пожара.
- **По поступившим сигналам (жалобам).** Такая проверка будет проведена, если от юридических либо физических лиц в пожарную инспекцию поступила жалоба о наличии на предприятии нарушений требований противопожарной безопасности.

Помните, что проблемы с пожарной службой способны полностью парализовать работу даже преуспевающего предприятия. Причем для решения этих проблем вовсе не обязательно действительно устранять имеющиеся недостатки. Иногда вопрос решается с помощью обыкновенной (или не совсем обыкновенной) взятки контролерам. В последнее время получил распространение еще один способ «решения проблем»: предприятие, на котором были обнаружены нарушения правил противопожарной безопасности, просят сделать «добровольный» взнос в какой-нибудь «фонд поддержания пожарной службы» либо что-то в этом

роде. Отметим, что такой взнос делается вполне официально: пожарная организация пишет письмо на имя руководителя провинившегося предприятия с просьбой «оказать посильную добровольную помощь пожарной службе и перечислить любую сумму на свое усмотрение по указанным реквизитам».

Это письмо является основанием для официального перечисления безналичных денежных средств со счета предприятия на счет пожарной службы (сумма «добровольного» взноса, само собой, оговаривается заранее). После того как деньги перечислены и получены, все предприятие получает «добро» со стороны пожарной службы на продолжение (либо начало) своей деятельности.

Не стоит забывать, что представители пожарной службы имеют законное право периодически посещать предприятие и проверять соблюдение правил противопожарной безопасности. Поэтому будет очень неплохо, если вы сумеете наладить дружеские отношения с местным отделением пожарной службы: это позволит вам избежать многих проблем и неприятностей. Иногда бывает целесообразно, как принято говорить, «посадить пожарных на откат», периодически «отстегивая» им определенное вознаграждение (например, определенную сумму денег ежемесячно или ежеквартально).

Проверки природоохранных служб

Неприятностями может обернуться и проверка со стороны природоохранных служб. Вам вполне могут сообщить, что, например, гараж вашей компании расположен слишком близко к водоему, нанося тем самым вред окружающей среде. Или — отходы вашего производства являются экологически вредными, и чтобы «вписаться» в действующие нормы и правила, вам придется полностью заменить производственное оборудование. В любом случае, убытки от посещения контролеров природоохранного ведомства могут превысить даже потери от серьезной налоговой проверки.

В качестве мер воздействия к виновным представители природоохранных служб могут применять санкции, такие как: штраф, временная остановка или запрет деятельности предприятия,

административное предупреждение и т. д. Результаты проверки оформляются соответствующим актом, который подписывает руководитель предприятия и представитель природоохранного ведомства.

Если в ходе проверки были обнаружены нарушения, то выписывается соответствующее предписание, которое является обязательным для исполнения. В нем перечисляются санкции, которые наложены на предприятие и на его должностных лиц. При своем несогласии с предписанием администрация компании может обжаловать его в установленном законом порядке.

Решение проблемы во многих ситуациях чаще всего решается через дачу взятки. Правда, нет никакой гарантии, что через некоторое время проверяющие не появятся вновь и не укажут повторно на те же самые нарушения.

В первую очередь природоохранные ведомства наказывают за следующие нарушения: токсичность и вредность отходов производства, расположенность производственных, складских и иных помещений слишком близко к водоемам, паркам, санаториям и иным подобным объектам, несоблюдение правил утилизации отходов (слив в реку вместо переработки и безопасной последующей утилизации).

Глава 4

Коррупция, мошенничество, аферы, подставы

В данной главе речь пойдет об опасных для малого и среднего бизнеса коррупционных проявлениях, а также распространенных аферах и прочих видах мошенничества, распространенных в российской бизнес-среде.

Коррупция в современной России

В настоящее время большинство специалистов сходятся на следующем определении коррупции.

Коррупция — это характерная для любого государства форма преступной интеграции (симбиоза) деловых кругов (бизнеса) с представителями государственного аппарата. В настоящее время имеется масса самых разных (правдоподобных и не очень) теорий, объясняющих сущность коррупции, но в данном случае нас не интересуют теоретические моменты. Ведь обычному коммерсанту совсем неинтересно, какой вред наносит коррупция экономическому развитию государства, равно как и безразличны ее макроэкономические аспекты.

Степень коррумпированности государственных служащих — это один из макроэкономических показателей. Он может быть высоким или средним, он даже может быть совсем незначительным, но никогда не будет нулевым. Коррупция была, есть и «будет есть» при любом государственном строе, и одной из целей

любого коммерсанта является основание и развитие своего дела, не обращая внимания на коррупцию и даже вопреки ее существованию. Поэтому старайтесь планировать систему бизнес-безопасности своей компании таким образом, чтобы неожиданные нашествия контролеров и замаскированные вымогательства со стороны работников государственного аппарата никак не могли помешать ее работе.

Такое явление, как коррупция, игнорировать нереально — когда-нибудь столкнуться с ним приходится каждому коммерсанту. Некоторые бизнесмены сами способствуют коррупции, превращая ее в средство конкурентной борьбы. В конечном итоге сами эти бизнесмены превращаются в элемент коррупционной системы. Часто коммерсанты привыкают к «мирному и взаимовыгодному сосуществованию» с чиновниками и начинают полностью зависеть от такого сращивания бизнеса и государства — как следствие, их компании теряют подвижность, характерную для частных компаний, и становятся намного менее конкурентоспособными. При потере номенклатурной поддержки такие субъекты хозяйствования в большинстве случаев теряют способность к существованию.

Однако не следует полагать, что коррупционный механизм нельзя использовать ни в коем случае. Каждый сам определяет стратегию развития своего предприятия, и если «дополнительное стимулирование» государственного служащего может защитить компанию от чувствительных потерь, то почему бы не воспользоваться этим методом? Тем более что бывают случаи, при которых подобная мера — единственный приемлемый вариант выхода из затруднительной (или даже безнадежной) ситуации.

Однако стоит помнить, что это не только противозаконно, но и опасно — и далее речь пойдет о том, к чему должен быть готов любой предприниматель или бизнесмен, пусть даже самый честный и принципиальный.

Как бизнесменов провоцируют и ловят на взятках

Любого делового человека могут провоцировать на дачу или получение взятки. Какие цели преследуют провокаторы, как вести себя в случае, когда вы поняли, что вас провоцируют на дачу/получение взятки, как распознать провокацию и как можно ей противостоять? Ответы на эти вопросы вы найдете далее.

Обычно провокация человека на дачу или получение взятки происходит по одной из двух причин: желание его дискредитировать либо разоблачение преступника (взяточника). В последнем случае провокацию осуществляют правоохранительные органы (возможно — при содействии иных граждан); такая операция обычно носит название «оперативный эксперимент». Что же касается дискредитации человека, то она может быть выгодна самым разным людям.

Кто же подвержен провокации в первую очередь?

Можете смело занести себя в «группу риска», если вы относитесь к одной из следующих категорий людей:

- крупный государственный или общественный деятель;
- бизнесмен, предприниматель любого уровня;
- известный политик;
- государственный служащий (чиновник) любого уровня;
- должностное лицо на предприятии;
- представитель силовых структур;
- работник фискальных органов;
- руководитель любого ранга.

Обычно представители именно этих категорий населения в первую очередь рискуют стать жертвой провокации. Но, само собой, от этого не застрахованы и представители других слоев общества.

Важно!

В современной России любая провокация, в том числе и на дачу/получение взятки, является одним из излюбленных и распространенных способов расправы с неугодными, устранения конкурентов, компрометации оппонентов, мести и т. п.

Провоцировать человека на получение взятки могут его конкуренты, завистники либо недоброжелатели. При этом предложение взятки может быть высказано не в беседе «один на один», как вообще-то строжайше положено элементарными правилами конспирации, а «два или более на один». При этом «один» — это тот, кому предлагают взятку. В данном случае факт получения взятки доказывается элементарно, если все представители взяткодателя подтвердят его. Это одна из самых простых, если не сказать — примитивных провокаций, поддаться на которую может разве что совсем уж неопытный и наивный человек.

Кроме этого, при провокации объект взятки (деньги, ценности и др.) может передаваться при проведении скрытой фото- или видеосъемки, при записи на магнитофон, диктофон или иное устройство или при наличии иных обстоятельств, которые могут помочь в получении доказательств факта взятки.

Помните, что для скрытого прослушивания, записи, фото- и видеосъемки удобно использовать современные и доступные многим технические средства. Например, многие мобильные телефоны имеют диктофон.

Как распознать провокацию

Можно ли каким-то образом определить, что в вашем отношении проводится провокация?

Один из верных признаков провокации — это когда вас неоднократно и настойчиво подталкивают к получению взятки, заходя «со всех сторон». Характерный пример — когда один и тот же человек пытается дать вам вознаграждение за решение разных вопросов: вы отказали ему в одном вопросе — через какое-то время он предлагает мзду за решение другого вопроса; вновь получив отказ, он через какое-то время предлагает взятку за решение третьего вопроса и т. д.

Подобная ситуация может иметь место с точностью «до наоборот»: к вам приходят разные люди и предлагают вознаграждение за решение одного и того же вопроса: вы отказали одному — через какое-то время приходит другой, отказали ему — приходит третий и т. д. При этом вам поступают такие заманчивые предложения, от которых, как говорил дон Корлеоне, невозможно отказаться.

В преследовании своей цели провокаторы могут использовать самые разные способы. Один из самых верных подходов — «давить на болевые точки»; нередко для его реализации провокаторам приходится провести определенную подготовку: узнать о ваших жизненных планах, имеющихся проблемах, пожеланиях, случившихся неприятностях и т. п.

Предположим, вы давно и безнадежно мечтаете о том, чтобы построить себе и своей семье небольшой дом в пригороде. Но денег, даже с вероятным привлечением кредита, все равно не хватает. Секрета из своей мечты вы не делаете, и о ней знает все ваше окружение.

И вдруг, как по мановению волшебной палочки, к вам приходит человек и просит посодействовать в решении важного для него вопроса, что не потребует от вас почти никаких дополнительных усилий (достаточно лишь должным образом исполнить свои служебные обязанности). При этом вам предлагается вознаграждение в сумме, которой как раз не хватает для реализации давнишней мечты. Помните: подобное счастливое совпадение чрезвычайно редко бывает подарком судьбы — вероятнее всего, это провокация, которая может иметь весьма печальные для вас последствия.

К подобным предложениям всегда следует относиться предельно критично. Тем более, если вы знаете, что у вас есть недоброжелатели или завистники.

Примечание

Кстати, полезно знать, что провокация, даже если она достигла своей цели (человек принял взятку), при определенных условиях отличается от обычной взятки, и юристы четко знают, где проходит эта граница. Отличительным признаком в данном случае может являться отсутствие согласия со стороны взяткополучателя

на получение взятки. Под отсутствием согласия подразумевается то, что вы ни в какой форме (ни явно, ни завуалировано, ни еще каким-то образом) не заявляли о намерении получить взятку.

Это положение имеет большое значение в случаях, когда вас провоцируют на получение взятки сотрудники силовых органов (например, в рамках проводимого оперативного эксперимента). В данном случае по закону вы будете отвечать не за получение взятки, а за покушение на получение взятки или коммерческого подкупа. Почему? А потому, что присутствуют не все признаки получения взятки или коммерческого подкупа: взятка была передана не в интересах взяткодателя, который таким образом хотел добиться от вас определенных действий (или наоборот — бездействия).

Почему же сотрудники правоохранительных органов иногда идут на такой шаг, как провокация на получение взятки?

Обычно этот прием применяется к лицам, о которых сотрудникам правоохранительных органов точно известно, что они нечисты на руку, и в первую очередь — в плане получения взяток. Если по-другому изобличить взяточника не получается (например, он является человеком опытным и соблюдает меры предосторожности), то проводится оперативный эксперимент с попыткой дачи взятки.

Совет

Старайтесь никогда не конфликтовать с правоохранительными, силовыми и фискальными органами, особенно если вы входите в «группу риска» (см. выше). В противном случае ваши шансы попасть под подобный оперативный эксперимент существенно увеличиваются.

Однако человека можно провоцировать не только на получение, но и на дачу взятки. Если вернуться к рассмотренному выше примеру с мечтой о собственном доме, то в данном случае провокатор может сказать человеку, что стоит лишь дать тому-то определенную сумму денег — и, например, вопрос о выделении участка под строительство будет благополучно решен.

Аналогичным образом провокаторы могут спекулировать и на других человеческих желаниях, проблемах и слабостях. Причем это иногда бывает сопряжено с настоящей подлостью. Вот харак-

терный пример: у человека, которого хотят спровоцировать на дачу взятки с целью компрометации, имеется тяжело больной родственник. Само собой, человек готов использовать все свое влияние и возможности, только бы помочь больному в борьбе с недугом. В один момент «доброжелатель» ему сообщает: за определенную мзду больному будет оказано лечение на высшем уровне. А затем в момент передачи этой самой «мзды» несчастного взяткодателя берут с поличным.

Как грамотно противостоять провокатору?

Как вести себя, если в ходе беседы вы понимаете, что вас провоцируют на дачу взятки?

В первую очередь помните: нужно соблюдать предельную осторожность и понимать, что разговор, возможно, записывается или прослушивается. Не допускайте никаких поспешных и опрометчивых высказываний, которые впоследствии можно будет трактовать как готовность дать взятку.

Постарайтесь хорошо запомнить условия дачи взятки, которые вам предлагают (форма взятки, сроки и варианты ее передачи, предполагается ли привлечение посредника и т. п.). Это пригодится, если вы решите писать заявление в правоохранительные органы по данному факту (это будет своего рода «игра на опережение», причем вы будете выглядеть в ней как добропорядочный и законопослушный гражданин, решивший сообщить компетентным органам о готовящемся преступлении).

Совет

Если ваш мобильный телефон имеет встроенный диктофон, будет очень неплохо, если вам удастся записать разговор.

И еще один важный момент: в подобном разговоре не стоит проявлять инициативу. Пусть собеседник выскажет все, что желает сказать, а вы будьте внимательным слушателем. Иначе говоря — работайте на получение информации, не предлагая ничего со своей стороны и не вступая в полемику.

Если вы получили провокационное предложение о даче/получении взятки, можете сразу обращаться с соответствующим заяв-

лением в правоохранительные органы. Даже если провокация исходит именно оттуда (например, в рамках оперативного эксперимента), своими действиями вы ясно дадите всем понять, что нарушать закон и заниматься взяточничеством не намерены. А принятое у вас заявление будет являться документальным подтверждением вашей честности и порядочности.

В заявлении можете не только изложить суть дела (что само собой разумеется), но и потребовать для установления истины проведения всех необходимых оперативно-следственных и (или) иных мероприятий, предусмотренных действующим законодательством в подобных случаях. Работники правоохранительных органов должны будут либо прислушаться к вашим требованиям, либо, в случае отказа, дать вам четкие и недвусмысленные объяснения, почему проведение подобных мероприятий считается нецелесообразным.

Если провокацию против вас проводят, например, конкуренты или недоброжелатели, то такое ваше заявление, послужившее поводом для начала активных действий со стороны правоохранительных органов, может полностью перевернуть ситуацию — как говорится, «с ног на голову». В результате у вас будут все шансы инкриминировать провокаторам совершение преступных действий (в частности, дачу или получение взятки). Будет замечательно, если вы имеете какие-то личные связи в правоохранительных органах и воспользуетесь ими с той целью, чтобы провокаторы сами получили то, чего другим (т. е. вам) желали.

Поддельные документы, печати и штампы

Сплошь и рядом в современной России используются поддельные документы, печати и штампы. В настоящее время не представляет никакой проблемы купить их на обыкновенном рынке. Причем продавцы реализуют фальшивки совершенно открыто, никого не боясь и ничего не опасаясь: со всех сторон только и слышно бормотание, вроде: «Документики, бланочки на все случаи жизни, печати-штампики, недорого»... Потом многое из этой «бланочной продукции» используется для мошенничества

и впоследствии всплывает в заполненном виде в кабинете у следователя.

Между прочим, подделка и сбыт поддельных документов подпадает под юрисдикцию Уголовного кодекса РФ и карается в соответствии со статьей 327, текст которой приводится ниже.

Статья 327. Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков.

Подделка удостоверения или иного официального документа, предоставляющего права или освобождающего от обязанностей, в целях его использования либо сбыт такого документа, а равно изготовление в тех же целях или сбыт поддельных государственных наград Российской Федерации, РСФСР, СССР, штампов, печатей, бланков — наказываются ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до двух лет.

Те же деяния, совершенные неоднократно, — наказываются лишением свободы на срок до четырех лет.

Использование заведомо подложного документа — наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок до двух лет, либо арестом на срок от трех до шести месяцев.

Как можно использовать поддельные документы? Один из наиболее распространенных приемов — для получения товара под якобы совершенную предоплату. Суть заключается в следующем: предприятие-продавец отпускает продукцию только на условиях полной предоплаты, в качестве подтверждения которой принимается либо факт зачисления денег на расчетный счет предприятия, либо предъявление заверенного банком документа, подтверждающего оплату (платежного поручения).

Не секрет, что если покупатель перечислил деньги сегодня, то подтверждающий документ он может получить в своем банке сразу, а вот зачислены на счет продавца деньги будут только на следующий день.

Этим и пользуются мошенники: они говорят, что деньги перечислены сегодня, и предъявляют продавцу поддельный банковский документ о совершении предоплаты (со штампом банка, подписью банковского работника — все, как положено). Доверчивый продавец отпускает мошенникам «оплаченный товар» и… На этом, собственно, все и заканчивается: никакие деньги на счет предприятия-продавца, само собой, не поступают ни завтра, ни в последующее время.

Каким образом можно защититься от подобного обмана? Можно порекомендовать такой вариант: надо позвонить в обслуживающий банк предприятия-покупателя и уточнить, действительно ли было перечисление такому-то получателю по такому-то документу с таким-то номером на такую-то сумму. При этом телефонный номер банка следует узнать самостоятельно через справочную службу, а не звонить по номеру, который, не исключено, предложат покупатели (они ведь могут дать телефон своего сообщника, который все подтвердит). При разговоре с работником банка следует узнать его фамилию и должность.

Еще один распространенный прием — использование поддельных доверенностей для получения товарно-материальных ценностей. Главное отличие данной аферы от рассмотренной выше заключается в том, что, если товар продается только на условиях предоплаты, эти деньги действительно поступают на счет предприятия-продавца. Только вот отпускать этот товар приходится дважды.

Как известно, получать товарно-материальные ценности можно по доверенности, выданной представителю предприятия-получателя. Эта доверенность остается у предприятия-отправителя и хранится вместе с накладной на отпуск товарно-материальных ценностей.

Когда в фирму за оплаченным товаром с доверенностью приходит представитель покупателя, редко у кого вызывает сомнения достоверность предъявленного документа: печать стоит, подпись руководителя и главного бухгалтера есть — казалось бы, что еще надо? Получатель отправляется на склад, ему выдают оплаченный товар, после чего он благополучно уезжает.

А через некоторое время выясняется, что товар был отпущен не тому, кому надо: в фирму приезжает настоящий представитель покупателя, предъявляет доверенность и требует отпустить ему оплаченные товарно-материальные ценности. Через короткое время выясняется, что фирма стала жертвой мошенников.

Стопроцентной защиты от подобной аферы нет. Однако шансы мошенника на успех намного сократятся, если работник, ответственный за отпуск товара, сверит паспортные данные получателя с данными, указанными в доверенности, после чего позвонит на предприятие, оплатившее товар, и узнает, действительно ли этот человек приехал оттуда.

Искусственное занижение цен с целью обмана

Иногда жертвами мошенников за короткое время становятся многие предприниматели и бизнесмены. Вот конкретный пример одной из распространенных схем мошенничества, который несколько лет назад имел место быть в Ярославской области.

Одно из коммерческих предприятий занималось тем, что перепродавало на территории области товар, завезенный из-за рубежа. Чтобы привлечь максимальное число покупателей, цены на реализуемую продукцию были беспрецедентно низкими — даже ниже закупочных. Разумеется, в клиентах недостатка не было — каждый хотел «затариться» по дешевке. Единственным условием отпуска товара была его полная предоплата, но учитывая смехотворно низкие цены, это выглядело вполне логично.

Первое время все договорные условия продавцом педантично соблюдались. Таким образом, через короткий срок эта фирма получила репутацию надежного поставщика дешевых товарно-материальных ценностей. По сути же она представляла собой самую обыкновенную финансовую пирамиду.

В один прекрасный момент случилось то, что должно было случиться: фирма набрала огромную сумму предоплат от многих субъектов хозяйствования и прекратила свое существование. Вернее, мошенники быстро перевели часть денег в надежное место, часть — обналичили и благополучно скрылись, предоставив

обманутым клиентам возможность совершенно впустую сотрясать воздух гневными восклицаниями.

Для защиты от подобного мошенничества достаточно помнить хорошо известное всем правило: бесплатный сыр бывает только в мышеловке. Если где-то кто-то вам предлагает товары по баснословно низкой цене — это должно не привлекать, а настораживать. Даже если вы сможете получить оплаченный товар — очень может быть, что он окажется ненадлежащего качества, с истекающим сроком годности и т. п.

Манипуляции с «фирмами-однодневками»

Одним из популярных и изощренных способов мошенничества является использование «фирм-однодневок». Цели создания таких фирм могут быть самыми разными: получение предоплаты якобы под поставку товара, выманивание кредитов или дотаций, приобретение товарно-материальных ценностей в рассрочку и т. д. В любом случае, сущность заключается в том, что после получения денег или иных ценностей фирма прекращает свое существование или просто оставляется на произвол судьбы.

Вот один из наиболее характерных примеров. Мошенники открывают «фирму-однодневку», которая якобы реализует товарно-материальные ценности на условиях предоплаты. Само собой, последний факт никого не удивляет — сегодня почти все работают только по предоплате. Поэтому предприниматели безо всякой задней мысли заключают договоры и перечисляют деньги на счет фирмы, рассчитывая через день-другой получить оплаченный товар.

Важно!

Для пущей надежности мошенники могут в договоре указать, что товарно-материальные ценности отпускаются не на следующий день после осуществления платежа (когда, по идее, деньги должны поступить на расчетный счет), а через три или пять дней после получения предоплаты. Мотивировать это они могут тем, что, мол, очень много покупателей, поэтому склад не успевает своевременно отпускать товар всем, кто его оплатил.

Ну а далее — все не просто, а очень просто. Собрав за несколько дней приличную сумму предоплат от доверчивых субъектов хозяйствования, мошенники быстро их переводят в надежное место или просто обналичивают, после чего скрываются.

Самое интересное, что привлечь истинных мошенников к ответственности удается далеко не всегда, даже если их поймали и пострадавшие опознали их в лицо. Дело в том, что истинные хозяева «фирм-однодневок» вполне могут оставаться в стороне, не «засвечиваясь» в учредительных и иных документах. При этом учредителями и должностными лицами (директор, главный бухгалтер) предприятия являются подставные фигуры, на роль которых вполне годятся наши опустившиеся соотечественники (пьяницы, бомжи). Также в качестве подставных фигур мошенники могут использовать людей, потерявших некоторое время назад свой паспорт, который будет использован без ведома прежнего хозяина.

Важно!

В «фирмах-однодневках» учредитель предприятия может являться одновременно и его директором, а иногда — еще и главным бухгалтером.

Предположим, правоохранительные органы разоблачили такое предприятие. Как правило, в этом случае налагается арест на счета этого предприятия в банке, а также на его складские помещения (при наличии таковых, что, учитывая «вид деятельности», весьма сомнительно).

А дальше выясняется, что предприятие не имеет практически никаких активов, и его единственный «учредитель» (и он же — «директор») — хронический алкоголик, с которым вести какие-либо разговоры бессмысленно и даже просто неприятно. Максимум, что можно сделать здесь по закону — это привлечь вечно пьяного «учредителя» к уголовной ответственности. Но очевидно, что никакого смысла такое наказание иметь не будет.

Отметим, что некоторые «фирмы-однодневки», а также их реальные хозяева находятся под покровительством «власть имущих», т. е. людей, занимающих видные посты в государственных структурах. Это позволяет им осуществлять свою деятельность

в течение длительного времени, не опасаясь правоохранительных органов. Разумеется, такое покровительство не бесплатно, и здесь уже речь будет идти о коррупции.

Каким же образом можно распознать «фирму-однодневку»? Абсолютно надежного способа для этого не существует, но, проявив определенную бдительность, можно защитить себя от множества неприятностей.

Например, можно поинтересоваться, как долго предприятие осуществляет финансово-хозяйственную деятельность, когда оно было зарегистрировано, когда открыло счет в банке, на протяжении какого времени арендует офисные помещения. Причем задавать эти вопросы следует не работникам фирмы, а представителям соответствующих инстанций. В частности, сведения о государственной регистрации предприятия, а также о его должностных лицах можно получить в местном органе власти. Узнать, как давно фирма арендует помещение, можно в отделении жилищно-коммунального хозяйства или, опять же, — в местном органе власти.

Если на предприятии одно и то же лицо является учредителем, директором и главным бухгалтером — от такой фирмы следует держаться подальше. Особенно, если встретиться и побеседовать с этим человеком никак не получается.

Неплатежеспособность должников и хитрости безнадежных дебиторов

Известно, что проблемы с «дебиторкой» представляют собой серьезную угрозу для функционирования предприятия. Далее мы узнаем, какие причины наиболее часто называют должники в качестве оправдания неплатежей и на какие хитрости они идут, чтобы выиграть безнадежное дело в суде, если вдруг кредитор пожелает взыскивать долг в судебном порядке.

Самая распространенная «отмазка» звучит предельно банально: нет денег. Мол, дела идут не очень хорошо, налоговая проверка наложила большие санкции и т. п. Почти всегда отсутствие денег — не более чем отговорка. Потому что если их нет на са-

мом деле — предприятие закрывается. А если оно платит заработную плату сотрудникам, рассчитывается с бюджетом и другими контрагентами, выплачивает банковский кредит с процентами, арендную плату и т. п. — значит, деньги есть, просто идут на другие, более важные с точки зрения дебитора нужды. В подобных ситуациях следует вести себя быстро, решительно и жестко, чтобы не превратить свое предприятие в «доброго кредитора».

Часто должники пытаются оправдаться тем фактом, что, мол, имелись другие неотложные платежи (аренда, налоги, зарплата...). Отговорка совершенно бессмысленная: ведь все подобные платежи планируются заранее, да и срок погашения задолженности стал известен не сиюминутно. В любом случае, видимых серьезных причин для неоплаты в данном случае не существует.

Еще более глупая «отмазка» — якобы забывчивость (мол, мы просто забыли оплатить, извините, пожалуйста). Это полная ерунда, однако, чтобы не выслушивать подобные бессмыслицы, периодически напоминайте дебитору об имеющемся долге и сроках его погашения. Разумеется, подобные напоминания следует делать не тогда, когда эти сроки истекли, а заблаговременно.

Часто дебиторы пытаются оправдать просрочку платежей реорганизацией предприятия (мол, тут у нас пока неразбериха, но как только немного придем в себя, сразу же все оплатим). Подобные причины не имеют под собой никаких оснований: какая бы реорганизация не проводилась на предприятии, его бухгалтерия все равно будет работать, а сроки оплаты никто не отменял. Отправить платеж в настоящее время — дело нескольких секунд, если на предприятии используется система электронных платежей типа «Банк – Клиент», и максимум пары часов — если нужно напечатать платежное поручение и отвезти его в обслуживающий банк.

Наиболее серьезная причина из тех, которые называют должники, — это налоговая проверка либо «налет» правоохранительных органов. Как известно, в подобных случаях у предприятия могут арестовать банковские счета (хотя в большинстве случаев ссылка на последнее обстоятельство — полный вымысел). В любом случае, при желании предприятие всегда сможет выполнить

свои обязательства тем либо иным образом (возврат товара, проплата от третьей организации...).

Если кредитор решил взыскать задолженность в судебном порядке, то он должен знать и понимать: в современной России его справедливый гнев может обернуться против него самого. В российской практике имеется немало парадоксальных случаев, когда дебитор в результате судебных разбирательств умудрялся не только не вернуть долг, но еще и получить с кредитора какую-то сумму (отечественное законодательство позволяет «выкидывать» и не такие фортели!).

Важно!

Помните: если кредитору ситуация представляется ясной и бесспорной, то для судьи все может быть не так очевидно, особенно после того, как над ситуацией «поколдуют» грамотные адвокаты. И еще: почти всегда, когда суд принимал решение в пользу дебитора, его адвокаты активно использовали допущенные кредитором ошибки, нередко банальные, примитивные и предельно обидные.

Одним из способов избежания уплаты долга является механизм банкротства. Дебитор может выступить инициатором этой процедуры, чтобы добиться от суда отсрочки исполнения обязательств не менее, чем на полгода. Еще один вариант — когда во время подготовки к банкротству «всплывают» новые кредиторы с «липовыми» договорами, актами сверок и иными документами, в соответствии с которыми дебитор несет умопомрачительные финансовые обязательства. В подобных ситуациях обычно принимается решение погасить в первую очередь задолженность перед самыми крупными кредиторами (которые в реальности «левые»), а претензии «настоящего» кредитора по сравнению с ними выглядят незначительными.

Иногда недобросовестные дебиторы в судебном порядке добиваются признания сделки недействительной или оспаривают сам факт совершения сделки. Это, конечно, парадоксально, но грамотные адвокаты и юристы могут добиться подобного решения суда.

Отличной зацепкой в суде для безнадежных должников является наличие тех либо иных неточностей в документах. При нормальном сотрудничестве предприятий такое встречается сплошь

и рядом и никак не мешает осуществлению сделок: например, может отличаться адрес поставки товарно-материальных ценностей, способ транспортировки и т. д. В случае же разногласий подобные нестыковки могут повернуть ситуацию совершенно противоположным образом.

То же самое касается и отсутствия тех или иных документов, имеющих отношение к сделке: недобросовестные дебиторы, имеющие хороших адвокатов, могут доказать всю несостоятельность намерений кредитора при отсутствии хотя бы одной счет-фактуры либо акта выполненных работ, либо акта приемки-передачи и т. п. Если в нормальных условиях на подобное никто бы не обратил внимания, то иногда при проведении судебного разбирательства такие факты становятся ключевыми.

Перед обращением в суд следует проверить, все ли чисто со своей стороны. Бывает, что кредитор отступает от тех или иных договорных обязательств: например, поставку товара осуществил на день-другой позже, нежели указано в договоре, либо ассортимент поставляемого товара отличается от спецификации, являющейся неотъемлемой частью договора, и т. д. В подобных случаях дебитор может добиться такого судебного решения, в соответствии с которым он не только будет освобожден от своих финансовых и иных обязательств, но еще и получит от кредитора денежную компенсацию.

Чтобы не попадать в подобные неожиданные и неприятные ситуации, уже с самого начала работы с контрагентом следует предусмотреть возможность предстоящего судебного разбирательства и строить отношения с ним исходя именно из этой позиции.

Форс-мажор и его «подводные камни»

Форс-мажор — это действия непреодолимой силы, которые могут оказать отрицательное влияние на состояние бизнеса.

Виды и специфика форс-мажора

Форс-мажорные обстоятельства могут иметь природное, политическое, бытовое или экономическое происхождение.

Важно!

При возникновении форс-мажорных обстоятельств природного или политического характера, которые отрицательно повлияли на деятельность компании, предприятие имеет право отказаться от исполнения договорных обязательств по заключенным ранее договорам с деловыми партнерами (обычно соответствующий пункт присутствует в каждом договоре или контракте). Что касается форс-мажорных обстоятельств бытового или экономического происхождения, то здесь все может зависеть от конкретной ситуации.

Природными форс-мажорными обстоятельствами признаются различного рода катаклизмы и стихийные бедствия, например: наводнение, землетрясение, обильный снегопад, сход лавины, непредвиденно жаркая погода, пожар (который произошел и по причине природных явлений — например, в результате молнии) и т. д. Очевидно, что если случается нечто подобное, то предприятие может полностью или частично прекратить свою деятельность, более того — понести существенные убытки.

Политические форс-мажорные обстоятельства в истории России случались, к сожалению, довольно часто. Таковыми обычно признаются различные войны (как международные, так и локального характера), революции, государственные перевороты (в принципе, это те же революции), разъединение либо объединение государств и т. п.

Примечание

В большинстве случаев возникновение политических форс-мажорных обстоятельств связано с дележом власти и денег между очередными рвущимися к управлению страной кланами и группировками.

Как известно, любой политический форс-мажор всегда влечет за собой полный хаос и разруху, а также изменение законодательной базы. Причем если хаос и разруха со временим либо устраняются (что является большой редкостью), либо люди к ним просто привыкают (обычно так и бывает), то неграмотное, грубое и бесцеремонное изменение законов и иных нормативно-правовых документов может привести к правовому коллапсу. В таких условиях даже честным предпринимателям и бизнесменам трудно исполнять обязанности по заключенным ранее договорам;

что касается жуликов и проходимцев, то их деятельность расцветает пышным цветом, причем остается полностью безнаказанной.

Возникновение бытовых форс-мажорных обстоятельств связано с проблемами бытового характера. Например, это может быть пожар, но в отличие от природного форс-мажора, когда к пожару приводит разряд молнии, в данном случае он происходит по бытовым причинам — замыкание электропроводки, неисправность электрических приборов, нарушение правил противопожарной безопасности и т. п. Если это затопление — то вызвано неисправностью (прорывом) трубы водоснабжения (канализации, отопительной системы). К бытовым форс-мажорам относят также воровство из офиса (например, злоумышленники похитили оргтехнику).

Любые форс-мажорные обстоятельства бытового характера могут нанести существенный ущерб предприятию и самым негативным образом повлиять на возможность исполнения им договорных обязательств.

В современной России наибольшее распространение получили форс-мажорные обстоятельства экономического характера. Такие обстоятельства можно перечислять долго; напомним те из них, которые являются наиболее актуальными:

- разорение «финансовой компании», куда были перечислены деньги для обналичивания;
- откровенный обман («кидалово») со стороны деловых партнеров;
- форс-мажорные обстоятельства у деловых партнеров, негативно влияющие на исполнение ими своих обязательств;
- неприятности с налоговыми и (или) правоохранительными органами (арест банковских счетов, складских и производственных помещений и т. п.);
- дефолт, инфляция;
- неожиданное принятие правительством мер экономического характера, отрицательно влияющих на функционирование предприятия (обмен денежных купюр, внезапный запрет на использование валюты в расчетах, обязательная продажа валютной выручки по заведомо невыгодному курсу и т. п.).

Многие российские предприятия теряют значительные суммы денег в результате того, что «финансовая компания» (по простому — «финка»), куда были перечислены средства для обналичивания, была разоблачена правоохранительными органами. Отметим, что подобные ситуации обычно оговариваются «финансовой компанией» и ее клиентом заранее, и в большинстве таких случаев «финансовая компания» ответственность не несет (это считается форс-мажорными обстоятельствами).

Для тех, кто не в курсе, о чем идет речь, вкратце поясню. «Финансовые компании» — это фирмы, которые осуществляют свою деятельность путем планирования и направления безналичных и наличных финансовых потоков, откровенно нарушая налоговое и иное законодательство. Хозяева «финансовых компаний» уже более-менее знают свою клиентуру и владеют информацией о том, когда, сколько и каких денежных средств им необходимо для удовлетворения потребностей клиентов. Например, обычно после окончания отчетного периода (год или квартал) возрастает спрос на безналичные деньги, поскольку приходит время уплаты субъектами хозяйствования налогов и неналоговых платежей. Спрос на наличные деньги существенно возрастает ко времени выплаты заработной платы и т. д.

Отметим, что, несмотря на откровенно противозаконный характер деятельности, «финансовые компании» играют весьма серьезную роль в экономике современной России, и их услугами пользуются не только коммерческие структуры, как это принято считать, но и государственные, общественные, бюджетные, финансово-кредитные и иные предприятия и учреждения.

Возникновение у порядочного делового партнера форс-мажорных обстоятельств — это действительно неприятно и даже «больно». Представьте, что фирма, у которой внезапно арестовали расчетный счет в банке, должна вам за поставленную продукцию порядка 100 000 долларов США! Готовы ли вы к таким потерям? Или похожая ситуация: у предприятия, которому вы перечислили предоплату за продукцию, внезапно арестовали все складские помещения, а заодно и счет в банке, в результате чего оно не может ни отгрузить вам оплаченные товарно-материаль-

ные ценности, ни вернуть полученные деньги. Это уже называется «кидалово» со стороны государства.

Неприятности с налоговыми или правоохранительными органами (отдел по борьбе с экономическими преступлениями, налоговая полиция и др.) — это форс-мажор, который может иметь далеко идущие последствия. Если с потерей денег еще худобедно можно смириться (в конце концов, можно взять кредит на пополнение собственных оборотных средств или воспользоваться кредитной линией), то фискальные органы могут надолго «прикрыть» деятельность предприятия. Арест всех или большинства активов (денежных средств на счетах в банках, товарно-материальных ценностей на складах предприятия, оргтехники, производственного оборудования и др.) грозит их последующей конфискацией в доход государства, а подобные убытки не покроешь никакими кредитами. Если в финансовом плане и удастся как-то выкрутиться, то в любом случае придется открывать новую фирму, регистрировать новую торговую марку, заново завоевывать рынок. Поэтому в подобных случаях предприниматели и бизнесмены не жалеют никаких средств для того, чтобы «полюбовно» решить вопрос с представителями фискальных органов, соглашаясь «дать на лапу» столько, сколько потребуют.

Что касается дефолтов и инфляций, то перед подобным форс-мажором все равны. Исключение составляют лишь те субъекты хозяйствования, которые относятся к категории «приближенных к императору», а точнее — имеющие высокопоставленных покровителей (в администрации президента, Государственной думе, министерствах и ведомствах и т. п.). Им в какой-то степени еще удается возместить свои убытки за счет инсайда, а также предоставленных льгот, компенсаций, преференций. Всем же остальным можно только посочувствовать — еще свежи в памяти печальные воспоминания об августе 1998 года.

Неожиданное принятие правительством тех либо иных мер, законодательных актов и т. п. можно сравнить с тем же дефолтом, только в несколько ином проявлении: в частности, форс-мажор может коснуться не всех субъектов хозяйствования, а только тех, кто, например, осуществляет определенные виды деятельности либо зарегистрированы в определенном регионе.

Минимизация потерь от форс-мажора

Можно ли каким-то образом если не избежать потерь при наступлении форс-мажорных обстоятельств, то хотя бы минимизировать их? Можно, хотя и не всегда.

Труднее всего обстоит дело с форс-мажорными обстоятельствами природного характера. Если вам в офис, на склад или в производственное помещение ударила молния, в результате чего начался пожар — остается лишь покинуть помещение, вывести из него людей и вызвать пожарную бригаду.

Что касается наводнения, то к нему можно хоть как-то подготовиться — об опасности подобных явлений сообщают метеослужбы. Если вы полагаете, что помещения вашего предприятия могут быть затоплены — вывозите технику, оборудование, товарно-материальные ценности и документацию в безопасное место.

Кстати, если в результате форс-мажора оказались безвозвратно утеряны документы, то некоторые из них можно восстановить. Например, если компьютеры остались целыми и невредимыми, то следует немедленно сохранить имеющиеся в них данные на нескольких независимых носителях информации: например, на съемном винчестере, на другом компьютере и на компакт-диске. Впоследствии эти данные помогут восстановить истинное положение вещей. Конечно, после утраты документов большинство этих данных теряет свою юридическую силу, но, по крайней мере, они помогут существенно прояснить ситуацию.

В банке можно получить копии банковских выписок и платежных документов (платежных поручений, требований, чеков и др.). На основании этих документов можно восстановить значительную часть товарно-сопроводительных документов, договоров, контрактов и т. п.

В инспекции Министерства по налогам и сборам можно получить информацию о начисленных и уплаченных предприятием налогах, а также получить копии расчетов налогов и неналоговых платежей, предоставленных в ИМНС. Аналогичным образом можно получить информацию из Фонда социальной защиты населения о начисленных и уплаченных страховых взносах, размере фонда оплаты труда и другую.

У контрагентов, с которыми работает или работало предприятие, можно попросить копии всех документов (договоров, накладных и других), подтверждающих совершение сделок, а также баланс расчетов из бухгалтерии.

Что касается бытовых форс-мажорных обстоятельств, то некоторые из них по степени непредвиденности можно сравнить с природными: например, никогда не знаешь, в какой момент прорвет водопроводную трубу или замкнет электропроводку. Поэтому следует соблюдать общеизвестные правила: не оставлять включенными электроприборы, хранить документы в несгораемом шкафу, установить в офисе противопожарную сигнализацию или хотя бы автономный пожарный извещатель, нанять сторожа или поставить охранную сигнализацию.

Политические форс-мажорные обстоятельства можно предвидеть. Причем если рядовой обыватель может не обращать внимание на происходящие вокруг события, то предприниматели и бизнесмены, как правило, держат руку на пульсе. Поэтому если вы видите, что в стране либо в вашем регионе назревают какие-то перемены — наверняка имеет смысл на какое-то время если не законсервировать предприятие, то работать с меньшей интенсивностью. Это позволит в случае необходимости успеть быстро все закрыть, обезопасить активы (продать имущество, перевести деньги на зарубежные счета либо обналичить их) и тихо-мирно дожидаться спокойных времен (не исключено — где-нибудь за границей). Исключением могут являться лишь предприятия, торгующие оружием, спецсредствами (резиновыми дубинками, газовыми баллончиками и т. п.), медикаментами и иными подобными товарами, имеющими повышенный спрос в условиях политических катаклизмов и военных конфликтов.

Что касается экономических форс-мажорных обстоятельств, то от многих из них бизнесмен может подстраховаться заранее. При этом предпринимаемые меры могут зависеть от целого ряда факторов, таких как: месторасположение предприятия, вид его деятельности, отношения с фискальными органами и государством, специфика конкретной ситуации и т. д.

Например, на случай дефолтов, инфляций и прочих «инсинуаций» рекомендуется руководствоваться известным правилом: не

стоит хранить все яйца в одной корзине. Пусть у предприятия будет несколько счетов в разных валютах, нелишним будет приобрести какие-нибудь надежные активы (например, недвижимость), причем иногда целесообразно оформить их на подставных физических или юридических лиц, иногда бывает полезно вложить свободные денежные средства в ценные бумаги.

На случай внезапного ареста расчетного счета в банке рекомендуется заранее вступить в сговор со своим операционистом. За определенное вознаграждение можно попросить его о том, чтобы он сразу после получения распоряжения (устного или письменного) о наложении ареста на счет клиента быстро перевел весь остаток имеющихся на счете денежных средств по заранее указанным реквизитам. Разумеется, все соответствующие документы (договор, счет-фактура, накладная), подтверждающие актуальность и законность платежа, должны быть подготовлены предварительно.

Что касается платежного поручения на перевод остатка денег (ведь работники правоохранительных органов, увидев, что вся сумма «ушла» со счета, немедленно потребуют подтверждающий документ), то дело обстоит следующим образом. Если на предприятии используется система электронных платежей типа «Банк – клиент», то операционист может позвонить на предприятие и попросить немедленно оформить и отправить соответствующую платежку — в данном случае вообще ни к чему не придерешься. Если же такая система не используется, придется немедленно готовить платежное поручение в печатном виде и срочно везти его в банк: если работник фискального или налогового органа обнаружит, что операционист перевел деньги без соответствующего документа — его могут привлечь не только к дисциплинарной или административной, но и к уголовной ответственности.

Чтобы не допустить ареста активов предприятия, целесообразно не учитывать их в балансе, а оформить на подставные фирмы с последующим взятием в аренду. Например, дорогостоящее производственное оборудование однозначно рекомендуется «взять в аренду» у какой-нибудь незаметной фирмы, а находя-

щиеся на складе товарно-материальные ценности можно документально «передать на ответственное хранение» другому предприятию.

Обман с доверительным управлением финансами на валютных и фондовых рынках

Все гениальное просто, и это крылатое выражение находит свое подтверждение в том, как мошенники обманывают бизнесменов, располагающих временно свободными денежными средствами, на валютном рынке, а также на фондовых рынках, где ведется торговля ценными бумагами.

На валютном рынке предлагается такая услуга, как размещение временно свободных денежных средств под доверительное управление. Суть операции состоит в том, что трейдер (биржевой игрок) распоряжается деньгами инвестора (заключает сделки) по своему усмотрению. Иначе говоря, инвестор разрешает трейдеру пользоваться своими средствами на бирже как угодно, лишь бы это приносило прибыль.

Если в результате биржевой игры действительно удается получить доход — клиент отдает трейдеру предварительно оговоренную часть (например, 30% или 50% прибыли). Если же биржевая игра получилась неудачной и принесла убыток, то стороны сразу определяют его максимально допустимый размер (обычно где-то треть от суммы вклада), при достижении которого игра должна прекратиться. В данном случае все потери ложатся полностью на инвестора, трейдер ничем не рискует — таковы правила, о которых инвестор знает заранее.

Этот нюанс и позволил появиться гениально простому и в то же время очень эффективному способу мошенничества. Трейдер через Интернет находит двух инвесторов, располагающих временно свободным капиталом, убеждает их в своем высоком профессионализме и уверяет, что распорядится деньгами лучше, чем кто-то другой. Получив средства в доверительное управление,

трейдер-мошенник выбирает позицию и на одном счете открывает ее вверх, а на другом — вниз (иначе говоря, играет одновременно на повышение и на понижение курса). В результате у одного инвестора образуется доход, а у другого — убыток такого же размера.

Когда убытки инвестора, которому не повезло, достигают оговоренной заранее суммы — трейдер сворачивает деятельность на его счете. Инвестор забирает свои оставшиеся деньги — но трейдер-то при этом ничего не теряет! Зато со счета другого инвестора, где получился доход, мошенник законно получает причитающуюся часть прибыли.

Аналогичным образом мошенники действуют не только на валютном, но и на фондовых рынках, на которых ведутся торги ценными бумагами.

Глава 5

Экономическая разведка и промышленный шпионаж

Экономическая разведка и промышленный шпионаж являются одним из наиболее распространенных методов получения необходимой информации. В общем случае можно дать следующее определение.

Экономическая разведка — это комплекс взаимосвязанных и координируемых активных действий, направленных на получение важной и ценной информации, скрытой от посторонних лиц, любыми доступными средствами, а также накопление и обработка этой информации.

Если же посмотреть с юридической точки зрения, то несомненный интерес представляет собой формулировка, которую дает Интерпол.

Экономическая разведка — это приобретение любым обманным путем интеллектуальной собственности, принадлежащей какому-либо юридическому лицу, которая была создана или законно приобретена этим юридическим лицом с целью производства чего-либо, что имеет или может иметь промышленную ценность и в более широком плане — ценность для национальной экономики.

Какая информация интересует шпионов?

Экономические разведчики и промышленные шпионы охотятся за самой разной информацией. Кого-то интересуют основные финансово-экономические показатели конкурирующей организа-

ции, кому-то важно знать принципы ценообразования, кто-то ищет производственные секреты, а кто-то интересуется наличием у конкурента связей в государственных структурах. Последнее бывает полезно знать, например, чтобы сделать вывод о том, стоит ли «натравливать» на конкурента налоговую проверку либо это бесполезно, потому что у него все схвачено и куплено.

Тем не менее, можно выделить несколько категорий сведений, которые интересуют промышленных шпионов. В первую очередь это информация, содержащаяся в финансовых отчетах (причем в реальных, а не в официальных), а также сведения стратегического характера и прогнозная информация.

Многих интересуют сведения о постановке маркетинговых процессов, а также ценовая стратегия конкурента. Всегда ценилась и наверняка еще будет цениться продолжительное время информация об условиях договоров и контрактов, причем всяких: с арендодателями и арендаторами, с покупателями и поставщиками, с собственными сотрудниками и др.

Одним из ключевых направлений деятельности экономических разведчиков является поиск информации о перспективах развития предприятия как в ближайшем будущем (год-два), так и на отдаленную перспективу (три-пять лет). Особую ценность подобные сведения имеют в отношении производственных и строительных предприятий, разработчиков программного обеспечения, крупных торговых предприятий, а также в добывающей и перерабатывающей отраслях. Шпионов интересуют оперативные и стратегические планы компании, перспективы развития менеджмента, совершенствование механизма работы с персоналом, планирование реструктуризации активов и иные ключевые факторы.

Особую старательность проявляют экономические разведчики при добывании информации, касающейся условий продажи или слияния субъектов хозяйствования. Не секрет, что многие предприниматели и бизнесмены заранее определяют, при каких условиях они согласны продать свой бизнес, согласиться на дружественное поглощение или подвергнуться недружественному поглощению. Такое планирование вовсе не означает, что коммерсант заранее готовится к продаже своего предприятия: это,

как правило, всего лишь один из возможных вариантов действий в случае возникновения непредвиденных обстоятельств.

Однако при наличии такой информации конкурент вполне может всеми доступными силами и средствами «посодействовать» наступлению этих самых непредвиденных обстоятельств, дабы вынудить владельца конкурирующей компании отказаться от дальнейшего ведения бизнеса и продать ее. Также подобные сведения способны намного упростить процесс недружественного поглощения предприятия, поскольку захватчик заранее знает, какие шаги может предпринять руководство захватываемой компании.

Большую ценность для промышленного шпиона представляют собой данные об организационной структуре компании. Зачем это нужно? Чтобы было понятнее, рассмотрим один из характерных примеров.

Предположим, предприятие-захватчик решило предпринять недружественное поглощение в отношении компании-конкурента (либо просто какой-нибудь преуспевающей фирмы) и направило туда экономического разведчика для получения необходимых сведений, а также для «зондирования почвы». Через некоторое время выяснилось, что компания, которую предполагалось захватить, практически не имеет никакой собственности и более-менее ценных активов, хотя и осуществляет успешную деятельность. Оказывается, из собственных активов оно имеет на балансе всего пару-тройку не первой свежести компьютеров, древнюю и добитую «Газель», а также мизерный остаток готовой продукции и иных товарно-материальных ценностей на складе.

В процессе дальнейших разведывательных действий выяснилось, что компания, которую агрессор предполагал захватить, имеет сложную организационную структуру, в частности — у нее есть ряд дочерних фирм, в каждой из которых «голове» принадлежит примерно по 20% акционерного капитала. При этом все составляющие бизнеса равномерно распределены по «дочкам»: у одной из них головная фирма получает сырье и материалы и на нее же «вешает» кредиторскую задолженность, у другой арендует складские помещения, у третьей — производственные мощности, у четвертой — офис, а пятой сразу после выхода из цеха отгру-

жается готовая продукция для последующей реализации непосредственным потребителям.

Наличие столь продуманной организационной структуры вынуждает потенциального агрессора отказаться от своих намерений. Ведь чтобы получить то, на что рассчитывал захватчик, ему придется поглощать не одну, а сразу шесть фирм (головное предприятие и пять дочерних структур)! Если же захватить только одну «голову», координирующую работу всей структуры, то полученный результат можно сравнить разве что с пустым орехом. Ведь за эту фирму никто и бороться особо не будет, поскольку у нее нет активов, а есть только какая-то абстрактная небольшая прибыль, показываемая налоговой инспекции. Поэтому хозяева ее отдадут с дорогой душой (предварительно разобравшись с акционерным капиталом «дочек» и иными организационными вопросами) и спокойно откроют другое аналогичное предприятие.

Сведения об организационной структуре компании могут быть полезны и в целом ряде других случаев. Например, если кто-то из конкурентов желает «натравить» на предприятие налоговую проверку, то при наличии такой разветвленной структуры ему придется серьезно подумать: на какую из фирм, входящих в корпорацию, отправить проверяющих? Логика подсказывает, что на «голову», но это может иметь совершенно «никакой» эффект. Тем более, что на случай возникновения непредвиденных обстоятельств, коими так богата современная российская действительность, многие предприниматели и коммерсанты держат в запасе заранее открытую фирму, на которую при малейшей опасности переоформляется бизнес.

Системы доступа к информационным центрам и сетям, а также составные элементы этих систем являются одним из ключевых объектов экономической разведки. Не секрет, что в настоящее время множество ценной и конфиденциальной информации хранится в электронном виде, поэтому владение средствами доступа позволяет получить много интересных сведений, как говорится, «малой кровью». Промышленные шпионы стремятся получить пароли, пин-коды, аппаратные ключи и иные средства доступа, не жалея для этого ни времени, ни средств.

Отметим, что нередко важная информация хранится не на сменных носителях или в офисных компьютерах, а в Интернете: считается, что это один из наиболее безопасных способов хранения данных. Однако следует учитывать, что для современных хакеров ничего невозможного не существует (взламываются даже сайты Пентагона), поэтому излишне доверять сети не рекомендуется.

Результаты многочисленных независимых исследований показывают: затраты на экономическую разведку и промышленный шпионаж в крупных компаниях составляют в среднем 1,5% от оборота. Стоит ли говорить, что сумма получается довольно внушительная! При этом для ведения экономической разведки предприятия выделяют значительные кадровые ресурсы: в частности, в некоторых японских компаниях промышленным шпионажем занимается более 200 человек. Что касается США, то, по некоторым оценкам, американские субъекты хозяйствования от ущерба, причиняемого промышленным шпионажем, теряют порядка 20 миллиардов долларов в год. Причем многие независимые эксперты полагают, что эта сумма явно занижена.

Источники информации, которыми пользуются разведчики и шпионы

В любом случае одной из ключевых задач экономической разведки и промышленного шпионажа является получение конфиденциальных сведений. Из данного раздела вы узнаете, какие категории источников получения информации могут содержать секретные сведения.

Первым и главным источником является *человек*, а точнее — люди. Эта категория включает в себя сотрудников конкурирующего предприятия: рабочих, служащих, представителей обслуживающего персонала, продавцов и т. д. Наибольшую ценность в качестве источников информации представляют собой работники закрытых и секретных структурных подразделений предприятия, а также представители высшего руководства компании (топ-менеджмент). К данной категории источников информации

также относятся покупатели и клиенты предприятия, его деловые партнеры, поставщики, арендаторы и арендодатели и т. д. Характерной особенностью человека как источника информации является то, что он является активным элементом, который не только может быть источником сведений, но и выполнять деструктивные функции, будучи завербованным конкурирующей организацией.

Следующая категория источников секретных сведений — это *документы*, причем представленные не только на бумажных, но и на электронных носителях информации. В общем случае документ — это информация, имеющая юридическую силу и представленная на носителе, позволяющем не сомневаться в ее подлинности. Документы представляют собой наиболее распространенный способ накоплений и хранения информации, а также обмена информацией. Характерной особенностью документа как источника секретных данных является то, что он отличается функциональным разнообразием. Система документации у любого субъекта хозяйствования имеет разветвленную структуру, причем документы различаются не только по содержимому, но и по типу носителя (бумага, дискета, съемный винчестер и др.).

Много секретных сведений можно найти в *публикациях* — это еще одна категория источников получения конфиденциальной информации. Сюда входят самые разные статьи (экономические, аналитические, публицистические и т. д.), книги, рекламные буклеты и проспекты, листовки, монографии, доклады, тексты выступлений и т. д.

Технические носители информации: бумага, кино- и фотопленка, магнитные носители (ленты, дискеты и др.), компакт-диски, информация на экранах (мониторов, телевизоров, табло) и т. д. являются одной из ключевых категорий источников секретных данных. Многие ошибочно относят документы и технические носители к одной категории источников конфиденциальной информации, но это не так: документ как источник ведь может быть представлен и на бумажном, и на электронном носителе, а вот далеко не всякий технический носитель может быть признан документом.

Технические средства обеспечения деятельности субъектов хозяйствования, а также физических лиц — это, можно сказать, кладезь ценной и секретной информации. Сюда входят телефоны (причем как отдельные аппараты, так и системы коммуникационных связей), факсы, автоматизированные системы обработки информации, телевизоры, радиоприемники, системы громкоговорящей связи, а также иные аппараты, средства и приспособления, которые могут являться местом утечки конфиденциальных сведений.

Одним из наиболее ценных источников получения секретных данных является *продукция* предприятия, как выпускаемая в настоящее время, так и образцы продукции, находящейся в разработке. Основные характеристики выпускаемой продукции всегда интересовали конкурентов, и эта тенденция, несомненно, сохранится и в обозримом будущем. Особую ценность представляет информация, касающаяся только планируемых к выпуску или находящихся на стадии разработки видов продукции: получение секретных сведений с высокой долей вероятности позволит конкуренту быстро и дешево (ведь не пришлось тратиться на разработку — секреты конкурента доставил шпион!) создать и вывести на рынок аналог.

Не меньшую ценность в некоторых отраслях и видах деятельности могут представлять собой *производственные отходы*. С помощью их изучения и анализа конкурент может узнать много интересного об используемых технологиях, тонкостях производства и т. д. Несомненным преимуществом данной категории является то, что необходимые сведения можно получить вполне легально и безопасно — на свалках, в местах складирования металлолома, иногда даже в мусорных корзинах офисных и производственных помещений компании.

Способы добычи интересующих сведений

Все методы получения необходимой информации можно разделить на две большие группы: законные и незаконные. Экономическая разведка оперирует законными методами, а когда начи-

нается применение незаконных — речь уже будет идти о промышленном шпионаже.

Наиболее распространенными законными методами получения конфиденциальной информации являются:

- сбор, накопление и анализ сведений, получаемых из официальных источников (средства массовой информации и т. п.);
- посещение презентаций, ярмарок, выставочных мероприятий и т. п.;
- приобретение продукции, выпускаемой конкурирующими предприятиями, с целью ее всестороннего анализа и изучения.

Что касается методов промышленного шпионажа, то наиболее распространенными и востребованными из них являются следующие:

- внедрение промышленных шпионов на конкурирующее предприятие, желательно — в окружение ведущих специалистов либо высшего руководства;
- похищение документов, схем, чертежей, а также образцов планируемой к выпуску продукции;
- переманивание персонала у конкурента;
- проведение ложных переговоров, а после получения интересующих сведений — отказ от якобы имеющихся намерений о сотрудничестве;
- подкуп и шантаж работников конкурирующего предприятия с целью получения у них необходимой информации (особую ценность представляют агенты, работающие в закрытых структурных подразделениях конкурента);
- ведение негласного контроля деловой корреспонденции;
- получение важных сведений с помощью технических средств (подглядывающая и подслушивающая аппаратура, «жучки», программные разработки шпионской направленности и т. п.);
- незаконное получение важной и секретной информации у представителей государства (чиновники, работники налоговых органов и т. п.).

Помимо перечисленных, промышленные шпионы могут использовать и другие способы получения информации в зависимости от конкретной ситуации.

Далеко не все понимают, что подавляющее большинство необходимой информации можно получить из открытых источников. В экономической разведке и промышленном шпионаже доля таких сведений может составлять до 70%, доля информации, полученной из полуоткрытых источников — 15–25%, и лишь от 5 до 15% сведений разведчики черпают из действительно закрытых и секретных источников.

Примечание

Следует отметить, что открытыми источниками получения информации могут пользоваться не только конкуренты, но также налоговые и правоохранительные органы либо представители государственной власти.

Наиболее емким, доступным и открытым средством получения информации является периодическая печать. Следует учитывать, что работа представителей масс-медиа (в первую очередь имеются в виду журналисты и корреспонденты) во многом напоминает работу спецслужб, разведывательных органов и т. п. Это неудивительно: чтобы получить те или иные сведения, на основании которых можно сделать рейтинговый материал, журналисты нередко идут на самые разные ухищрения, демонстрируя чудеса смекалки, изобретательности и, кстати, смелости. Иной журналист способен собрать, систематизировать и представить в открытом источнике такое количество ценной информации, перед которым спасует целая служба экономической разведки предприятия.

Наряду с этим сведения, почерпнутые из средств массовой информации, позволяют дополнять и уточнять данные, полученные с помощью оперативных средств, а также подсказать новые направления разведывательной и шпионской деятельности предприятия.

Кто-то может возразить: «Все это, конечно, так, но для полноценного изучения и анализа сведений, содержащихся в средствах массовой информации, потребуется времени больше, чем 24 часа

в сутки». Стоит ли говорить, что это распространенное ошибочное мнение, не имеющее никакого отношения к действительности!

На самом деле все гораздо проще, и необходимо лишь четко спланировать и систематизировать свою работу с открытыми источниками. При этом необходимо уделить внимание перечисленным ниже аспектам.

- Правильный подбор источников получения информации. Если вы хотите добыть сведения о компании, занимающейся нефтепереработкой, — очевидно, что издания, вроде «Активный отдых» или «Советский спорт», вам вряд ли пригодятся.
- Грамотная обработка источников информации с применением метода так называемых «ключевых слов».
- Рациональная классификация, сортировка и хранение полученной информации.

Следует учитывать, что нередко сведения, находящиеся в разных источниках, могут дублироваться (особенно это относится к тем изданиям, которые выходят ежедневно либо несколько раз в неделю). Поэтому увеличение количества изучаемых источников далеко не всегда может привести к качественным результатам (иначе говоря, количество не всегда переходит в качество).

Примечание

Специализированные издания в процессе формирования ежедневной сводки размером примерно в одну страницу, содержащей оценочные сведения по одной проблеме, обрабатывают массив информации объемом примерно 7–8 миллионов слов.

При работе с конкретной статьей, публикацией или иным подобным материалом, необходимо из всех поднятых в ней вопросов уметь выбирать только те, которые имеют непосредственное отношение к вашей проблеме, и не «распылять» свое внимание на постороннюю и ненужную информацию, какой бы увлекательной она не показалась.

Еще одним эффективным источником открытой информации являются выставочные мероприятия, в которых принимают участие конкуренты. Разведчик может просто подойти к стенду (разумеется, при том условии, что его не знают в лицо) и находиться

в непосредственной близости, внимательно слушая и вникая во все, о чем представители конкурента рассказывают посетителям. Еще более эффективный способ — это когда разведчик прикидывается потенциальным клиентом предприятия: данный прием позволяет легко и быстро получить массу интересных и полезных сведений, которые иным способом добыть невозможно. Например, если вы — разведчик, то можно спросить, почему продукция конкурента лучше продукции вашего предприятия, почему потенциальным клиентам не стоит обращаться в вашу фирму, а нужно идти только к конкуренту и т. д.

Техническое обеспечение современного промышленного шпионажа

В настоящее время на российском рынке представлено великое множество самых разнообразных технических средств, рассчитанных на любых, даже самых взыскательных потребителей. Вот наиболее популярные из них.

- Специальная звуко- и видеозаписывающая аппаратура (в том числе различного рода «жучки»).
- Приспособления для получения информации с линий телефонной связи.
- Специально разработанные системы наблюдения и передачи видеоизображения на расстояние.
- Микрофоны направленного действия.
- Фотоаппаратура.
- Приборы слежения и ночного видения.
- Различного рода радиозакладки и тому подобные приборы.
- Приспособления, предназначенные для снятия информации с окон и стеклянных перегородок, принцип действия которых основан на использовании лазерных излучателей.
- Аппараты, предназначенные для выявления радиоактивного фона и (или) другого излучения.

В целях промышленного шпионажа могут использоваться и другие технические средства. Главное, чтобы они удовлетворяли основным критериям: простота в использовании, а также доступность в приобретении (говоря по-простому — приемлемая цена). Получение необходимых сведений не должно выливаться в умопомрачительные суммы — в противном случае шпионаж не будет иметь никакого экономического и практического смысла. Вот пример доступного технического средства: комплект аппаратуры, с помощью которого можно осуществлять дистанционное получение информации на расстоянии до одного километра, должен стоить порядка 400 долларов США.

Примечание

Некоторые сообщения (например, ранее это касалось пейджинговых сообщений) может перехватывать среднего уровня программист с помощью старенького компьютера (с процессором Pentium 200 или его аналогом) и специально предназначенного сканирующего приемника.

Инсайд как причина многих неприятностей

По оценкам независимых экспертов, одной из самых существенных угроз для любого бизнеса являются так называемые инсайдеры. **Инсайдер** — это тот, кто в силу своего служебного или семейного положения имеет доступ к конфиденциальной информации (инсайду), касающейся деятельности предприятия либо имеющей прямое или косвенное отношение к собственникам компании, и т. п. Исходя из этого определения становится понятно, что инсайдерами, как правило, являются высшие должностные лица, представители исполнительной дирекции, топ-менеджмента, держатели крупных пакетов акций и т. д. Однако часто забывается, что инсайдерами могут быть и менее высокопоставленные работники: наиболее характерные примеры — системные администраторы, а также работники финансовых и бухгалтерских служб предприятия.

Возможно, у читателя возникнет вопрос: со служебным положением все понятно, а при чем тут семейное положение? Дело в том, что члены семьи высокопоставленных работников или крупных акционеров субъекта хозяйствования также могут иметь доступ к конфиденциальной информации. Особенно часто это встречается среди супругов или взрослых детей инсайдеров.

Среди наиболее известных результатов «деятельности» инсайдеров за последние несколько лет (особенно «щедрыми» на подобные события оказались 2005 и 2006 годы) можно отметить следующие:

- появление на «черном» рынке базы данных Центробанка Российской Федерации с платежами, которые были совершены в 2003–2004 годах;
- появление на «черном» рынке базы данных компании «НИКойл», которая вела реестры акционеров МТС, «ЛУКойла» и иных известных компаний федерального значения;
- появление на «черном» рынке базы данных Министерства по налогам и сборам РФ, где содержались сведения о доходах жителей Москвы за 2004 год;
- появление на «черном» рынке базы данных, содержащей сведения о российских получателях потребительских кредитов, в которой имелось более 700 000 записей.

Можно привести еще немало подобных примеров, но и этого достаточно, чтобы понять: инсайдерство в современной России процветает и чувствует себя вольготно.

Среди наиболее вредоносных действий, совершаемых инсайдерами, многие коммерсанты и владельцы бизнеса отмечают вынос документов и (или) баз данных, рассекречивание списка клиентов и деловых партнеров компании, а также иной конфиденциальной информации. Как ни странно, немногие отмечают такую серьезную угрозу со стороны инсайдеров, как преднамеренное уничтожение либо искажение информации — а это иногда чревато более существенными неприятностями, чем простое разглашение секретных сведений.

Характерной особенностью инсайдеров является то, что они могут рассекретить конфиденциальные данные либо исказить информацию не по злому умыслу и не с целью личной наживы, а просто по халатности или по ошибке, иначе говоря — непреднамеренно. Подобное может возникать по причине пресловутого человеческого фактора, перед которым, к сожалению, бессильны самые современные меры безопасности: как известно, стопроцентной «защиты от дурака» в природе не существует.

По этой же причине очень сложно бороться с таким негативным явлением, как утечка данных. Можно сколь угодно ограничивать доступ людей к секретным сведениям, но всегда останутся каналы для «сливания» данных. Вот несколько наиболее характерных из них, с которыми не только трудно бороться — они зачастую просто выпадают из зоны внимания тех, кто отвечает за сохранность информации:

- секретные сведения можно прочитать на экране монитора у того, кто имеет к ним доступ и слишком халатно относится к защите этих данных;
- человек может просто забыть важнейший документ в принтере, в ксероксе, оставить без присмотра свой рабочий стол и компьютер;
- человек может наговорить секретную информацию на телефонный диктофон;
- при необходимости можно запомнить содержимое случайно увиденного важного документа.

Для наиболее эффективной борьбы с утечкой информации необходимо реализовать систему самоконтроля инсайдеров, чтобы они непреднамеренно не рассекретили важные сведения и не позволили получить к ним доступ посторонних. На руководящие и ответственные должности необходимо назначать надежных, серьезных, морально устойчивых сотрудников (банально звучит, но это так). Причем периодически следует обращать внимание этих работников на то, что далеко не вся информация, к которой они в силу специфики служебных обязанностей имеют доступ, предназначена для разглашения.

Чтобы предотвратить опасность, которая может исходить от инсайдеров, или по крайней мере вовремя разоблачить того, кто виновен в утере важной информации или разглашении секретных сведений, необходимо соблюдать определенные меры безопасности. В частности, компьютерный доступ к конфиденциальным данным (финансовая, бухгалтерская и управленческая отчетность, списки клиентов, сведения о заработной плате сотрудников и др.) должен быть строго персонифицированным. Посторонним вообще следует закрыть доступ к этой информации (офис-менеджеру совсем не нужно знать, какие активы числятся на балансе предприятия), а всем остальным он будет открываться только после полной авторизации. Это позволит узнать, кто и когда работал с данными и какие действия при этом совершал (чтение, редактирование, копирование...).

Эффективным средством защиты является аппаратная аутентификация. Суть ее заключается в том, что для доступа к секретным данным сотрудник должен использовать аппаратное средство контроля (смарт-карта, аппаратный ключ и т. п.).

Надежно защитить конфиденциальную информацию позволяет постоянный аудит всех действий, совершаемых пользователями в локальной сети. Для этого можно использовать специальные системы, разработкой которых занимаются многие компании. Такая система обеспечит постоянный мониторинг состояния и защиту локальной сети как внутри фирмы, так и от внешних воздействий (проникновение в сеть извне, запись или редактирование данных и т. п.).

Защитить секретные сведения, к которым имеют доступ инсайдеры, от посторонних можно путем их шифрования — это один из наиболее надежных способов. Как известно, многие руководители высшего звена хранят множество ценных сведений в собственных ноутбуках, которые являются объектом повышенного внимания со стороны злоумышленников. Их просто крадут, причем не ради компьютера, а с целью получения доступа к хранящимся в нем данным. Поэтому все, что инсайдер хранит в своем ноутбуке, обязательно должно быть зашифровано.

Противостояние шпионажу: экономическая контрразведка

Поскольку экономическая разведка существует и успешно развивается, логично предположить, что должна существовать и экономическая контрразведка, направленная на борьбу с экономическими разведчиками и промышленными шпионами, а также негативными явлениями и тенденциями, имеющими место быть на предприятии и в той или иной степени угрожающими его интересам. Идеологическая основа системы контрразведки базируется на том, что, поскольку предприятие имеет собственную службу экономической разведки, конкуренты наверняка имеют аналогичные службы, и им необходимо противостоять. Это и является основной задачей экономической контрразведки.

Если же говорить более подробно, то главные цели экономической контрразведки можно сформулировать следующим образом.

- Предупреждение, своевременное распознавание и жесткое пресечение попыток вербовки конкурентами агентов из числа сотрудников собственного предприятия.
- Пресечение попыток любого сотрудничества работников предприятия, выходящего за рамки должностных обязанностей, с деловыми партнерами, контрагентами и т. п., а также с представителями криминальных структур.
- Пресечение попыток ведения на предприятии разведывательной и иной подобной деятельности со стороны государственных органов. Если законными способами это невозможно — введение их в заблуждение (например, если известно, что такой-то представитель государственного органа ведет деструктивную или разведывательную деятельность — щедро предоставлять ему дезинформацию).
- Недопущение утечки важных сведений и конфиденциальной информации.
- Периодическое выполнение проверки сотрудников на предмет их лояльности своему предприятию.

- Проведение служебного расследования фактов хищений, злоупотреблений служебным положением, должностного подлога, фальсификаций и т. п.
- Оперативная защита сотрудников предприятия, а также его активов (зданий, сооружений, производственных площадей...).

На конкретном предприятии перед службой экономической контрразведки могут стоять и другие задачи, в зависимости от вида деятельности компании, формы собственности и иных факторов. В частности, нередко в обязанности работникам контрразведки вменяется профилактика и пресечение тех или иных негативных процессов, которые в принципе могут возникнуть у любого субъекта хозяйствования. Таковыми, в частности, являются: конфликты и споры между работниками, различного рода трудовые конфликты сотрудников предприятия с его администрацией, угрозы саботажа или забастовок, массовые нарушения общественного порядка, межнациональные конфликты.

Важно!

Различного рода кризисные ситуации, негативные явления, конфликты, споры, забастовки и т. п. вполне могут быть инициированы службой экономической разведки и промышленного шпионажа конкурирующего предприятия.

Для борьбы с подобными явлениями используют как специальные, так и социально-психологические методы. В первом случае речь идет об административных и дисциплинарных мероприятиях, во втором отыскиваются возможные пути для согласования интересов всех участников конфликта.

Следует знать и помнить: несмотря на свои широкие полномочия и большие возможности, служба контрразведки предприятия не может являться адекватной заменой правоохранительным и силовым органам. Поэтому при появлении любой информации, свидетельствующей о подготовке преступления либо о том, что оно уже свершилось, необходимо в обязательном порядке обращаться в соответствующие органы (полиция, прокуратура, ОБЭП, ФСБ).

Как должна функционировать служба экономической контрразведки

При планировании и организации работы службы контрразведки на предприятии в первую очередь необходимо обдумать, какими силами и средствами будет оперировать данное подразделение службы безопасности. В данном случае силы — это комплектация службы контрразведки оперативными работниками, т. е. теми, кто непосредственно занимается контрразведывательными действиями. Иначе говоря — хорошо подумайте, сколько оперативных работников вам потребуется, чем конкретно будет заниматься каждый из них, а также какие финансовые затраты вам придется для этого понести. Причем финансовые затраты включают не только заработную плату сотрудников службы контрразведки, но и финансовое обеспечение некоторых операций (например, расходы на взятки или на подкуп, приобретение аппаратуры прослушивания и т. п.).

Что касается средств службы экономической контрразведки, то их можно разделить на две категории. Первая категория — это оперативные возможности оперативного состава, попросту говоря — имеющаяся агентурная сеть. Ко второй категории относятся оперативно-технические средства, используемые службой контрразведки (например, техника для видеонаблюдения, аппаратура прослушивания и съема информации, «жучки», «маячки» и т. п.).

Также необходимо провести всесторонний анализ сил и средств как существующих, так и потенциальных противников. Если конкурирующая организация имеет с вами много общего — это может существенно упростить задачу: наверняка службы экономической разведки у нее и у вашей компании будут во многом похожи, да и методы борьбы могут иметь много общего.

Если же вами интересуются предприятия других видов деятельности (бывает и такое — например, чтобы прозондировать почву для открытия такого же бизнеса, как ваш) — здесь уже все сложнее. Еще хуже — если вы знаете, что вами интересуется какое-нибудь частное детективное агентство либо сыскная контора:

противостоять профессионалам чрезвычайно сложно. Тем не менее, попытайтесь найти ответы на следующие вопросы.

- Что именно может заинтересовать «любопытных» в деятельности вашего предприятия? Например, если вы занимаетесь разработкой нового вида продукции и планируете вот-вот приступить к его серийному производству — ответ на данный вопрос очевиден.
- Как бы вы поступили на месте конкурентов, если бы захотели получить те же сведения, что и они?
- Насколько профессионально и слаженно работает экономическая разведка ваших противников?
- Какие преимущества либо недостатки имеет служба безопасности вашего предприятия по сравнению с аналогичными службами других известных вам субъектов хозяйствования?
- Применяют ли экономические разведчики конкурентов незаконные методы получения информации, и если да — можно ли это обернуть против них (в частности, использовать как компромат или средство дискредитации)?
- Какие средства и методы ведения экономической контрразведки вы планируете применять, и могут ли их аналогичным образом использовать ваши конкуренты?

Конечно, не на все перечисленные вопросы вы сможете ответить, но даже размышление над ними может навести вас на очень полезные соображения.

Планируя деятельность службы контрразведки, необходимо провести полноценный анализ лиц, которые, с одной стороны, могут использоваться как источники получения важной информации, а с другой — представлять собой опасность ввиду возможной вербовки подразделениями экономической разведки конкурирующих предприятий.

В конечном итоге вам необходимо четко представлять себе основной принцип работы контрразведывательного подразделения вашего предприятия, конкретные задачи службы контрразведки (как оперативные, так и стратегические), а также порядок

распределения предстоящих работ между сотрудниками данной службы.

После того как вы обдумаете и спланируете все то, о чем говорилось выше в данном разделе, у вас хотя бы в общих чертах должен сформироваться план работы подразделения контрразведки.

Отметим, что служба экономической контрразведки использует следующие основополагающие принципы работы: *объектовый* и *линейный*. Сущность *объектового принципа* заключается в том, что за каждым сотрудником службы контрразведки закрепляется один или несколько объектов предприятия, например: бухгалтерия, склад, здание администрации. Отметим, что в качестве таких объектов могут выступать как структурные подразделения предприятия, так и отдельные помещения, здания, участки и т. п.

Работник подразделения контрразведки обязан обеспечивать оперативное прикрытие вверенных ему объектов от различного рода проблем, неприятностей, внедрений со стороны. Например, он должен не только следить за тем, чтобы на вверенном объекте не появились подслушивающие устройства либо иные технические средства тайного получения информации, но и своевременно распознавать и предотвращать попытки саботажа, сговора, коллективного недовольства, тем более что все это вполне может быть спровоцировано конкурентами.

Что касается *линейного принципа* работы, то суть его заключается в следующем: сотруднику контрразведки выделяется определенное направление (линия), которое он курирует. Например, один работник контрразведки должен следить за фактами утечки конфиденциальной информации из любого места предприятия, своевременно выявлять их и ликвидировать каналы утечки. Другой может отвечать за состояние морально-психологического климата в коллективе (пресекать попытки саботажа или забастовок и т. п.), третий — за разоблачение экономических разведчиков и промышленных шпионов, засланных конкурентами, и т. д.

Однако в некоторых случаях бывает целесообразно работать по комбинированному принципу, т. е. путем сочетания объектно-

го и линейного принципов. Например, сотрудник службы контрразведки может одновременно отвечать за сохранность конфиденциальной информации и — параллельно — обеспечивать оперативное прикрытие отдела маркетинга и (или) департамента снабжения.

Как можно определить, какой принцип организации работы контрразведки является оптимальным? Обычно это зависит от целого ряда факторов: числа оперативных работников и имеющегося у них опыта (одно дело — когда у вас в контрразведке работают отставные офицеры спецслужб, и другое — когда этим занимаются рано уволившиеся милиционеры), объемов финансирования контрразведывательной деятельности и др. Обычно последнее слово остается за начальником службы безопасности либо за руководителем предприятия (однако в последнем случае все равно должно учитываться мнение начальника службы безопасности).

Дезинформация как один из самых эффективных элементов контрразведки

Дезинформация как инструмент борьбы контрразведчиков появился задолго до того, как стали возникать какие-то экономические конфликты между субъектами хозяйствования. На протяжении долгих веков дезинформация использовалась в основном политиками и военными с целью введения противника в заблуждение. Несомненное лидерство в этой области принадлежит спецслужбам разных стран, в первую очередь — СССР и США.

Характерной особенностью дезинформации является тот факт, что она представляет собой мирное средство ведения борьбы. В самом деле: если разоблачен вражеский агент, совсем не обязательно его тут же арестовывать, привлекать к ответственности, раздувать международный скандал и т. п.: гораздо проще и, кстати, целесообразнее позволить ему спокойно выполнять свою работу, но при этом постоянно и щедро «сливать» ему дезинформацию, заводя таким образом противника в полнейший тупик.

В настоящее время дезинформация нашла широкое применение в различного рода экономических конфликтах, представляя собой ключевой элемент оперативной, стратегической и тактической маскировки истинных намерений субъекта хозяйствования. С помощью дезинформации противника вы можете предпринять контрмеры внезапно, мощно и массированно, с немалой экономией собственных средств и ресурсов.

Итак, на основании вышеизложенного можно дать следующее определение термину «дезинформация»:

Дезинформация представляет собой метод маскировки, сущность которого заключается в преднамеренном распространении заведомо недостоверной информации об объектах, структурных подразделениях и иных элементах субъекта хозяйствования, их направлениях деятельности, сферах ответственности, составе, а также в имитации деятельности этих объектов в соответствии с распространяемыми сведениями. Также дезинформация подразумевает проведение различного рода мероприятий, операций, событий, основная цель которых — сокрытие от конкурента конфиденциальной информации и введение его в заблуждение при принятии решений, дабы его последующие действия были выгодны дезинформатору.

Кроме этого, понятие «дезинформация» включает в себя различного рода бумаги, информацию, документы и материалы, содержащие недостоверные сведения и заведомо рассчитанные на преднамеренное введение кого-либо в заблуждение.

Говоря о таком средстве ведения экономической войны, как дезинформация, необходимо знать и понимать значение некоторых терминов и понятий, которые перечислены ниже.

- Легенда — внутренняя, внешняя, собственная либо сторонняя информация, основной целью которой является сокрытие и маскировка истинного положения вещей. Например, вы внедряете своего контрразведчика в службу экономической разведки конкурирующего предприятия, куда его без задней мысли принимают на работу на должность финансового разведчика. В данном случае истинное положение вещей, заключающееся в том, что в реальности данный сотрудник является

внедренным контрразведчиком, скрывается для конкурента под легендой, что он тихо-мирно работает у него финансовым разведчиком.

- Легендирование конкурента — преднамеренное дезинформирование конкурирующей организации с целью введения его в заблуждение относительно своих истинных действий, направлений деятельности, мотивов. Иначе говоря, если ваше предприятие планирует заняться производством зубной пасты, а вы всеми возможными способами убеждаете конкурентов, что на самом деле будете заниматься пошивом брюк — это есть легендирование.
- Дезинформационное мероприятие — комплекс тесно взаимосвязанных между собой действий обманного характера, основная цель которых — введение конкурента в заблуждение относительно тех либо иных событий, ваших предполагаемых действий, текущих мероприятий, проводимых операций и т. д. Отметим, что наиболее действенными дезинформационными мероприятиями считаются манипулирующие мероприятия и операции. Суть их заключается в том, что они формируют в сознании конкурента чувство полной реальности происходящего, что позволяет быстро и с относительно небольшими затратами средств и ресурсов склонить того к нужным (разумеется, с точки зрения дезинформатора) действиям.
- Мишень дезинформации — лицо, группа лиц или предприятие, на введение которых в заблуждение направлены проводимые дезинформационные мероприятия. Например, в качестве мишени дезинформации может быть выбран работник руководящего звена (топ-менеджер) конкурирующего предприятия, ответственный за принятие управленческих, оперативных, стратегических и иных ключевых решений. Иногда вместо термина «мишень дезинформации» используется понятие «цель дезинформации».
- Разработчик — конкретное лицо или группа лиц (например, тот или иной отдел подразделения экономической контрразведки), которые занимаются разработкой программы (плана,

проекта и т. п.) дезинформационных мероприятий. К разработчику всегда предъявляются высокие требования. В частности, он должен обладать нестандартным мышлением, иметь богатое воображение, уметь быстро принимать эффективные решения. Каждый разработчик понимает, что умение планировать и реализовывать на практике эффективный ввод в заблуждение непосредственно зависит от имеющегося творческого потенциала, который необходим для разработки и обеспечения ключевой легенды мероприятия.

- Любой разработчик должен четко знать и представлять:
  - задачи, поставленные перед каждым структурным подразделением предприятия;
  - зоны ответственности подразделений предприятия;
  - задачи по дезинформации каждого компонента;
  - концепцию внезапности, секретности, оправданного риска;
  - возможности службы экономической разведки и контрразведки как на собственном предприятии, так и в конкурирующей организации;
  - информацию о факторах психологического, социального и культурного плана, которая теоретически может оказать влияние на действия противника и на принятие им ключевых решений;
  - возможности конкурирующей организации по разработке и претворению в жизнь дезинформационных мероприятий (как неформального, так и формального характера).
- Оперативная игра — агентурно-оперативная операция (комплекс мероприятий), в ходе которой используются различного рода «подставы», разоблаченные и перевербованные агенты конкурирующих предприятий, легендированные организации, средства оперативной техники, срыв запланированных конкурентами мероприятий и действий, дезинформирование, выявление и использование нелояльности персонала к собственному предприятию.

На что же в первую очередь необходимо обращать внимание при проведении дезинформационных мероприятий? Об этом речь пойдет в следующем разделе.

Практическое применение дезинформации

Процесс планирования и разработки дезинформационного мероприятия должен базироваться на следующих принципах:

- определение объекта, в отношении которого проводится дезинформационное мероприятие;
- формулировка цели проведения дезинформационного мероприятия;
- предварительная оценка ожидаемых результатов от проведения операции;
- наличие централизованного управления дезинформационным мероприятием, обеспечение координации действий;
- проведение разведывательных и контрразведывательных мероприятий, направленных на прикрытие операции и призванных обеспечивать любое необходимое содействие;
- актуальность и своевременность дезинформационного мероприятия;
- согласованность операции.

Определение объекта, в отношении которого проводится дезинформационное мероприятие, — ключевой этап любой операции. Если мишень дезинформации выбрана ошибочно, то все дальнейшие действия не только однозначно потеряют всякий смысл, но и могут нанести невосполнимый вред собственному предприятию.

В подавляющем большинстве случаев в качестве мишени дезинформационного мероприятия выбирается лицо, принимающее ответственные решения. Кстати, многие ошибочно полагают, что мишенью дезинформации является служба экономической разведки конкурирующего предприятия. Это не так: служба развед-

ки почти всегда используется лишь как удобный и надежный канал передачи «дезы» тому, кто на ее основании будет принимать решение.

Важно!

Любая дезинформация должна соответствовать реальной ситуации, не содержать в себе лишних подробностей: в них легко запутаться самим дезинформаторам, к тому же слишком подробная «деза» может вызвать подозрение у объекта дезинформационного мероприятия. Кроме этого, она должна быть достаточно эластичной в течение всего своего развития и существования, и в ней обязательно должны присутствовать место для маневра и путь к отступлению.

Искусный разработчик операции сумеет преподнести дезинформацию таким образом, что она будет предельно близка к реальному положению вещей, но в то же время в ней будет нечто такое, что несомненно вызовет интерес у объекта операции и введет его в заблуждение. Например, если ваша компания занимается производством задних мостов для самосвалов и колесных тягачей, и вы попытаетесь вбросить своим конкурентам «дезу» о том, что в ближайшем будущем перепрофилируете свое производство на выпуск дамских часиков — это вызовет у конкурентов лишь снисходительную улыбку. Если же вы дезинформируете их о том, что переводите производство на выпуск шасси для подъемных кранов — это будет, по крайней мере, ближе к истине.

Определившись с мишенью дезинформационного мероприятия, следует четко обозначить его цели и задачи, которые должны иметь конкретную и понятную формулировку. Например: *целью проводимой операции является введение конкурента в заблуждение относительно дальнейшего выпуска данного вида продукции и склонение его к перепрофилированию производства*. В подобной ситуации важно убедить конкурента в том, что те, от кого он получил эти сведения, давно уже приняли такое решение и активно занимаются переводом предприятия на выпуск других видов продукции. Отметим, что приведенная в качестве примера цель дезинформационного мероприятия является комплексной, так как в ней определены не только действия дезинформатора, но

и действия, к которым необходимо склонить руководство конкурирующей организации.

Что касается предварительной оценки ожидаемых результатов операции, то это можно сделать на основании четко сформулированной цели мероприятия и знания специфических особенностей конкурирующего предприятия.

Важнейшим этапом планирования является выбор метода доведения дезинформации до объекта дезинформационного мероприятия. Иначе говоря, вы должны решить — каким образом конкурент узнает то, что вы хотите ему сообщить? В настоящее время обычно используются следующие способы доведения «дезы»: *прямой* и *опосредованный*.

Сущность *прямого способа* заключается в том, что объект дезинформационного мероприятия получает «нужные» сведения напрямую от дезинформатора. Это может произойти при личной встрече, во время телефонного разговора, при переписке по электронной почте либо ICQ.

Что касается *опосредованного способа* донесения дезинформации, то он подразумевает использование посредников, в большинстве случаев — людей, которые пользуются доверием у объекта дезинформации и могут влиять на принятие им тех или иных решений. Кроме этого, в качестве «передатчика» можно использовать заведомо подложные документы, средства массовой информации, почтовую связь и т. п.

Важным условием успешности операции является наличие централизованного управления дезинформационным мероприятием, а также обеспечение координации действий всех занятых в нем сотрудников. Важно знать и все время следовать правилу: координация, контроль и управление операцией должны находиться в одних руках. В противном случае будет, как в той поговорке — «правая рука не знает, что делает левая», и это приведет к полному провалу дезинформационного мероприятия, да еще и к разоблачению контрразведчиков. Необходимо предпринять все меры для того, чтобы не допустить любых несогласованных действий и обеспечить неуклонное исполнение задуманного, причем без отрицательного воздействия на реализацию других целей мероприятия.

На всех этапах дезинформационного мероприятия должно обеспечиваться его разведывательное и контрразведывательное обеспечение. Для чего? Да хотя бы для того, чтобы выяснить, что именно конкурент уже знает о текущей ситуации и каковы его ожидания относительно дальнейшего развития событий. Это важно, в частности, с той точки зрения, чтобы доводимая до конкурента дезинформация казалась ему правдоподобной и в то же время не выходила за рамки действий, которые он в силах предпринять. Иначе говоря, получив порцию «дезы», противник должен предпринять то, что в его силах; если же «переборщить» с дезинформацией, то он, увидев, что изменить ничего не сможет, просто оставит все в состоянии «как есть» и махнет на это рукой. В результате дезинформационное мероприятие окажется неэффективным и бесполезным.

Кроме этого, разведчики и контрразведчики должны обеспечить возможность постоянной и надежной обратной связи. Это имеет исключительно важное значение с точки зрения адекватной оценки восприятия конкурентами вброшенной «дезы», а также того, насколько они ей доверяют. Если у противника возникли сомнения в достоверности полученной дезинформации — значит, необходимо внести соответствующие корректировки в ход реализации мероприятия. Обратная связь может обеспечиваться как с помощью имеющихся в стане конкурента собственных агентов («засланных казачков»), так и путем постоянного наблюдения за его реакцией, предпринимаемыми действиями (либо наоборот — бездействием). Кстати, на языке разведчиков это называется отслеживание динамики косвенных разведывательных признаков конкурента.

Также прикрытие со стороны разведки и контрразведки подразумевает строгое обеспечение необходимых мер конспирации. Стоит ли говорить, что любая утечка информации о проводимой операции, особенно касающаяся плана ее проведения, поставит жирный крест на всем дезинформационном мероприятии! Кстати, в качестве надежного средства предотвращения утечки информации рекомендуется использовать принцип четкого разделения значимой информации. Суть его заключается в том, что

каждый участник дезинформационного (да и любого другого контрразведывательного) мероприятия должен знать только то, что ему необходимо для исполнения своих обязанностей в рамках выполнения общего плана (задания), а количество тех, кто полностью владеет деталями операции, должно быть минимизировано.

Принцип актуальности и своевременности проводимого дезинформационного мероприятия подразумевает в первую очередь тот факт, что время осуществления операции должно быть тщательно продумано. При этом необходимо учесть сроки, которые потребуются всем участникам мероприятия для его успешной реализации, а также оценить время, необходимое службе экономической разведки конкурента для оценки и анализа полученной дезинформации и передачи ее мишени дезинформационного мероприятия (т. е. лицу, ответственному за принятие важного решения). Также следует учесть время, которое нужно для принятия объектом мероприятия требуемого решения, а также на реализацию этого решения.

Одним из ключевых факторов успешного осуществления дезинформационного мероприятия является принцип согласованности действий. Он подразумевает, что все подобные мероприятия требуют неторопливой, тщательной, продуманной подготовки, а также четкой координации действий всех участников.

Как перевербовать экономического разведчика

Предположим, что служба собственной безопасности вашего предприятия разоблачила экономического разведчика (промышленного шпиона), внедренного конкурентами. Можно ли перевербовать его и заставить работать на себя, и если да — как это сделать?

Для перевербовки разоблаченных шпионов существует два основных рычага влияния: *запугивание* и *подкуп*.

В первом случае можно пригрозить, что ваших возможностей вполне достаточно для того, чтобы этого человека никто больше

не взял на работу на должность выше дворника, что вы расскажете о нем всем кадровым агентствам, что его можно привлечь к уголовной ответственности за несанкционированный шпионаж, что его деструктивные действия привели к огромным убыткам компании, и вы подадите на него в суд, и т. д.

Однако перед беседой как следует подумайте, чего наверняка испугается вражеский агент, а на что просто не обратит внимания. Многие сразу идут на попятную, как только речь заходит о компрометации в глазах супруги. Может, вы вспомните, что на корпоративный праздник ваш агент пришел с дамой по имени Марина, хотя имя его законной жены — Ольга? Тогда припугните его тем, что вы намерены пригласить в офис его супругу, и упомянутый факт при ней наверняка подтвердят сотрудники, присутствующие на этом празднике.

Но есть люди, которые не поддаются шантажу; запугать удается, как правило, в основном малоопытных и слабохарактерных людей. Если же говорить об опытных экономических разведчиках, то они практически не допускают ошибок, которые могут быть использованы для шантажа, а если что-то подобное все же случается — то они, как правило, будут готовы к любым последствиям.

Поэтому если запугать «засланного казачка» не удалось, используйте другой и самый верный метод — деньги.

Заранее определитесь с тем, каким максимальным количеством денег вы согласны пожертвовать, и поделите эту сумму пополам. Полученную «половину» предлагайте четко, решительно и конкретно: почти всегда экономический разведчик — человек деловой, любит определенность и ясность. Если вам удалось перевербовать агента за необременительную сумму денег — считайте, что полдела сделано.

Почему полдела? А потому, что, начиная с данного момента, за «перебежчиком» должна быть установлена постоянная слежка: очень может быть, что ему захочется в течение какого-то времени поработать и на вас, и на свое прежнее руководство. Обязательно просматривайте его электронную корреспонденцию, установите на его компьютер модули слежения и шпионское про-

граммное обеспечение (более подробно о подобных программных продуктах рассказывается ниже), а также предпримите иные необходимые меры безопасности (или просто поставьте соответствующую задачу службе собственной безопасности вашего предприятия, если таковая имеется).

Что же делать, если перевербовать вражеского агента не удалось? Бывает же так, что человека и шантажировать нечем (опытный разведчик не дает поводов для шантажа), и деньгами его переманить не получится (конкурент платит ему на несколько порядков больше, чем вы можете предложить).

В данном случае просто сделайте вид, что вы ничего не знаете. Но вместе с этим — предупредите о разведчике службу собственной безопасности и сотрудников предприятия, оградите его от реальной информации и всячески «сливайте» ему побольше дезинформации: пусть ее и отсылает своему куратору. Это введет вашего конкурента в заблуждение и обеспечит принятие ошибочных решений с его стороны. При грамотной постановке дезинформационных мероприятий это может привести к фатальным ошибкам конкурента даже на стратегическом уровне.

Компромат как неотъемлемый инструмент контрразведки

Компромат в современной России является одним из наиболее популярных и эффективных средств ведения любой борьбы: конкурентной, политической, экономической, поэтому было бы странно, если бы подразделения экономической контрразведки субъектов хозяйствования не использовали его в своих целях.

Что же представляет собой компромат? Чтобы ответить на этот вопрос, достаточно вспомнить, что слово «компромат» — это сокращенное словосочетание «компрометирующий материал».

Если же говорить подробнее, то компромат обычно представляет собой различного рода документы и материалы (фото- и видеозаписи, бумаги, электронные документы, материалы аудиопрослушивания и др.), содержащие такие сведения о физическом

или юридическом лице, которые оно старалось держать в тайне от общественности. Причем чем выше общественный, политический либо иной статус человека, чем более видное положение в обществе он занимает — тем более отрицательное воздействие может оказать на него любой компромат. В первую очередь люди боятся компромата, раскрывающего тайны их личной жизни, а также доказывающий наличие связей с криминальными структурами.

Компромат на того или иного человека может «всплывать» одним из следующих способов:

- случайное обнаружение;
- целенаправленная слежка;
- провокация человека на совершение компрометирующих его действий.

В первом случае компрометирующие материалы совершенно случайно попадают в руки заинтересованным лицам — например, в результате утери их владельцем, либо обнаруживаются в процессе разговора с общими знакомыми и т. п.

При целенаправленной слежке заинтересованные лица отлично знают, что рано или поздно человек совершит неблаговидный поступок, и постараются его зафиксировать. Это может быть, например, момент дачи/получения взятки или свидание женатого человека с посторонней женщиной и т. д.

Если же никак не удается найти на человека компромат, можно попытаться его спровоцировать на совершение компрометирующих действий. Например — во время корпоративной вечеринки подсыпать в бокал с вином усыпляющее средство и сфотографировать «мертвецки пьяного» известного человека в разных позах, для пущей убедительности облив ему брюки и измазав лицо губной помадой. Еще один распространенный вариант компрометации — организация семейному человеку (неважно — мужчине или женщине) свидания с противоположным полом и фиксирование всех «подробностей происходящего» на фото или видео.

Важно!

В настоящее время многие российские детективные агентства активно работают в сфере получения компромата на кого угодно — начиная от известных личностей и заканчивая рядовыми обывателями.

Характерной особенностью компромата является то, что он способен не только поставить жирный крест на будущей карьере и планах человека, но и полностью сломать ему жизнь, а в особо трагических случаях — и довести до самоубийства. Но иногда компромат имеет прямо противоположный эффект, оборачиваясь неожиданной и полезной рекламой.

Одним из направлений использования компромата является склонение к сотрудничеству лиц, имеющих доступ к важной информации либо занимающих ответственные должности. Например, часто с помощью компромата осуществляется перевербовка вражеских агентов (экономических разведчиков и промышленных шпионов, засланных конкурентами).

Однако перед тем как использовать компромат в отношении кого бы то ни было, необходимо оценить возможную ответную реакцию человека и попытаться предугадать его действия.

Например, вы планируете шантажировать человека с сильным характером и устойчивой психикой. Компромат у вас, что называется, «железный», и оппонент никуда не денется — ему придется сотрудничать с вами помимо своей воли. Однако учтите: сильный и волевой человек, скорее всего, всеми доступными средствами попытается вам отомстить, и не факт, что вы будете довольны таким сотрудничеством. Возможно, он также постарается добыть на вас компрометирующие материалы — и поверьте, месть его будет намного более жесткой (если не сказать — жестокой), нежели ваши действия в отношении него.

Однако не стоит впадать в другую крайность, т. е. шантажировать с помощью компромата слабохарактерных и безвольных людей. Такие люди в подобных случаях не всегда способны адекватно оценить ситуацию и принять здравое решение, а напротив — могут руководствоваться эмоциями, впасть в панику и наделать массу глупостей. Например, результатом авантюрного и непродуманного шантажа иногда является самоубийство.

В настоящее время существуют разные приемы и методы, с помощью которых человека вынуждают идти на сотрудничество под давлением компрометирующих материалов. Как правило, все они основаны на том, что человек из-за компромата боится утратить тот или иной статус или опасается привлечения к уголовной ответственности. Однако нужно понимать, что в любом случае рассчитывать на долгосрочное эффективное сотрудничество с подобными агентами не следует: со временем страх может притупиться, а также возможно появление вариантов, при которых человек перестанет бояться компромата (например, ему угрожали, что расскажут жене о наличии любовницы и покажут ей соответствующие фото, а он через некоторое время развелся по собственной инициативе). Энтузиазм агента неуклонно снижается и со временем сходит «на нет», в результате чего он начинает поставлять малоинтересную и почти бесполезную информацию.

Однако компромат можно использовать не только как средство вербовки, но и как инструмент дискредитации противников. Причем в данном случае совершенно необязательно располагать реальными компрометирующими материалами — вполне можно использовать вымышленные факты.

Например, в профилактических мерах, направленных на борьбу с экономической разведкой конкурирующих предприятий, часто применяется такой способ. В средствах массовой информации появляются статьи о том, что на таком-то предприятии разоблачен экономический разведчик или промышленный шпион, более того — не просто разоблачен, а тайно перевербован. Если на вашем предприятии действительно есть «засланные казачки», наверняка подобная информация в прессе заставит понервничать их хозяев: им придется ломать голову над тем, соответствует ли эта информация действительности, и если да — кто именно из работников экономической разведки оказался перевербован. При удачном стечении обстоятельств это может привести к ненужным «резким движениям» со стороны конкурента, и если у вас внезапно уволился один или несколько сотрудников — возможно, это просто срочно отозванные промышленные шпионы.

Глава 6

Сравнительно честный отъем: рейдерство, или насильственный захват предприятий

В последние годы все чаще можно услышать такой термин, как «недружественное поглощение», который, по сути, означает насильственный захват предприятия. В современной России от насильственного захвата не застрахован ни один субъект хозяйствования: поглощаются не только отдельные предприятия и организации, но и крупные финансово-промышленные и иные холдинги, под контролем которых находится если не целая экономическая отрасль, то ее преимущественная часть.

Недружественное поглощение — это процесс, который протекает не моментально, а в течение определенного периода времени. Иногда ход данного процесса сопровождается громкими преступными событиями: перестрелками, устранением или дискредитацией неугодных и т. п. Хотя в последние годы наметилась тенденция к более «цивилизованному» (если можно так сказать) решению вопросов, с применением таких методов, как подкуп, шантаж, должностной подлог, подделка документов, злоупотребление служебным положением и т. д. Некоторые независимые исследователи высказывают мнение, что в России в настоящее время проходит нечто вроде «национализации», только она проводится не силами государства, а крупными олигархическими кланами, умеющими изымать принадлежащие законным собственникам ценные бумаги и предприятия.

За последние несколько лет в России произошло несколько тысяч поглощений одних предприятий другими, причем почти в трех четвертях случаев они носили характер недружественных, т. е. представляли собой насильственный захват субъекта хозяйствования. Именно поэтому с каждым днем увеличивается число руководителей, которые одной из приоритетных задач, стоящих перед службой безопасности предприятия, называют борьбу с недружественным поглощением и распознавание подобных попыток на самых ранних этапах.

Каким же образом на практике осуществляется столь сложный процесс, как недружественное поглощение одного предприятия другим?

В настоящее время основным средством недружественного поглощения является использование в этих целях административного и силового ресурсов, а также судебной власти. Иначе говоря, те, кто желает произвести насильственный захват предприятия, имеют мощную поддержку в структурах государственной власти, в правоохранительных и налоговых органах и в судебной системе. Более того — уже довольно давно (несколько лет назад) сложился и успешно действует сегодня своеобразный рынок услуг, на котором за определенную (и, само собой — весьма немалую) плату захватчикам окажут содействие правоохранительные, судебные и иные органы государственной власти.

Конкретнее? Вот примерный «прейскурант» действующих на 2012 год цен (получен из неофициальных источников, расценки могут варьироваться в зависимости от региона).

- Заведение «заказного» дела работниками прокуратуры — от $50 000.
- Выемка реестра акционеров органами прокуратуры — от $20 000.
- Силовой захват офиса работниками МВД — от $20 000.
- Выигрыш безнадежного дела в Арбитражном суде — в среднем от $10 000 до 100 000, но может быть и значительно выше.
- Наложение ареста на имущество — от $5 000 до 15 000.
- Депутатский запрос — от $3 000 до 10 000.

- Принятие «нужного» постановления правительственных структур — от $300 000 до «плюс бесконечности», иногда применяется тариф в размере 2% от общей «цены вопроса».

Чтобы защитить предприятие от недружественного поглощения, сотрудники службы безопасности должны не только уметь своевременно распознавать и ликвидировать возможные угрозы еще на ранних стадиях подготовки, но и применять превентивные и тактические меры, а также обеспечить надежную защиту предприятия от насильственного захвата в условиях начавшейся атаки.

Какие предприятия больше всего рискуют стать жертвами рейдеров?

Безусловным лидером по степени привлекательности для захватчиков являются любые предприятия и организации, которые осуществляют свою деятельность в сфере добычи либо обработки природных ресурсов: нефтегазовые компании, предприятия металлургической и горнорудной отрасли, лесной и рыбной промышленности и т. д. Это неудивительно: на добыче, переработке и продаже природного сырья делаются миллиардные (в долларовом исчислении) состояния, здесь постоянно крутятся огромные деньги, а по рентабельности с такими предприятиями могут сравниться очень немногие.

Также потенциальных захватчиков весьма привлекают субъекты хозяйствования, занимающиеся производством и торговлей спиртными напитками и табачными изделиями. Сюда входят ликероводочные и табачные заводы и фабрики, предприятия оптовой и розничной торговли и т. п. Не секрет, что торговля человеческими пороками (к числу которых, помимо прочего, относятся спиртные напитки и табачные изделия) — одно из наиболее выгодных направлений деятельности, поэтому подобные предприятия подвержены серьезному риску в плане недружественного поглощения.

Активно интересуются потенциальные захватчики предприятиями мясной промышленности, в первую очередь — мясокомбинатами. При грамотной постановке дела такие предприятия

могут приносить очень и очень большой доход, поэтому по степени своей востребованности они следуют сразу после предприятий ликероводочной и табачной промышленности.

Ну а далее интерес к тому или иному предприятию зависит от его особенностей. Например, всегда интересно захватить компанию, которая располагает дорогостоящими зданиями либо земельными участками, да еще находящимися неподалеку от станций метрополитена. Да и вообще — для потенциальных захватчиков будет представлять интерес любое предприятие, владеющее ценными и привлекательными активами и имеющее положительное денежное сальдо.

Следует, однако, помнить и такой немаловажный нюанс: в настоящее время недружественное поглощение предприятий происходит, как правило, в тех отраслях, в которых еще не определились стратегические инвесторы, попросту говоря — где еще не все поделено между политико-олигархическими и иными группировками. Например, если взять угольную либо алюминиевую промышленность — то здесь захватчикам уже, как говорится, «ловить нечего»: все давно и надежно поделено, чужаков пускать в этот бизнес никто не намерен, а слишком настойчивым могут весьма основательно «прищемить нос». А вот что касается недостаточно развитых рынков, в которых можно рассчитывать на рентабельность выше, чем в данный момент, то здесь процессы насильственного захвата процветают.

Основные методы рейдерского захвата

Сегодня в России наиболее распространенными являются три варианта недружественного поглощения предприятий. Рассмотрим подробнее каждый из них.

Сущность первого способа заключается в *организации двойного менеджмента и создании двойного реестра акционеров*. Примерная схема действий может выглядеть так: предприятие-захватчик, владеющее крупным (но — не контрольным) пакетом акций, созывает внеочередное собрание акционеров, не ставя при

этом в известность основного акционера. Иначе говоря, основной акционер попросту игнорируется, и собрание проводится в тайне от него.

На данном собрании все привилегированные акции переоформляются в основные, а также избирается и утверждается новый совет директоров и генеральный директор (президент). Это и есть то, что называется «двойным менеджментом».

А что же настоящий собственник предприятия? Он действует наиболее очевидным и логическим путем — через суд старается доказать незаконность действий предприятия-захватчика. При этом он и не подозревает, что представители компании захватчика заранее позаботились о благополучном для себя исходе дела, оплатив «правильное» судебное решение согласно действующему «прейскуранту».

Отметим, что в некоторых случаях компании-захватчики оплачивают не судебное решение, а только максимально возможное затягивание дела. Так обычно поступают в ситуациях, когда денег не хватает (не секрет, что искусственное затягивание дела стоит дешевле, чем принятие «нужного» судебного решения).

Далее может последовать попытка силового захвата предприятия с помощью силовых структур (эта «услуга» также оплачена заранее), в первую очередь это касается производственных мощностей, финансовых потоков, а также складских помещений.

При этом законный собственник захватываемой компании может подвергаться и другим «мерам воздействия»: наложение ареста на банковские счета, принятие судебных решений о прекращении поставок сырья и материалов, запрете экспорта продукции предприятия и т. д.

Сущность второго распространенного способа недружественного поглощения предприятий заключается в *применении судебных исков миноритарных акционеров*. В данном случае рядовой акционер, являющийся держателем небольшого количества акций (он их приобрел накануне), подает иск по месту прописки (жительства), которое не совпадает с месторасположением предприятия. При этом он предъявляет обвинения держателю контрольного пакета акций в нарушении своих прав как акционера предприятия, утверждая, что они были нарушены либо в процес-

се проведения приватизации, либо по причине невыполнения инвестиционных обязательств.

Стоит ли говорить, что необходимое судебное решение было предварительно проплачено, поэтому исход дела уже предрешен! Ну а затем — арестовываются акции законного владельца компании, которые немедленно продаются какому-нибудь подставному юридическому лицу (вроде известного «Рога и копыта»). Эта подставная фирма быстро перепродает акции компании-агрессору. Смысл операции в том, что в данном случае компания-агрессор в соответствии с действующим законодательством однозначно является добросовестным приобретателем акций. Самое интересное, что законный хозяин компании может узнать обо всем происшедшем только тогда, когда на его предприятии появится новый владелец и сообщит ему о свершившемся факте.

Еще один распространенный способ недружественного поглощения основан на *применении механизма банкротства*. В данном случае предприятие-захватчик может просто выкупить все долги поглощаемой компании. Еще один вариант — когда в судебном порядке возбуждается процедура банкротства, причем инициатором этого является какое-нибудь предприятие-кредитор поглощаемой компании из числа государственных организаций.

Таковы наиболее распространенные способы «сравнительно честного отъема субъектов хозяйствования» у их законных владельцев. Помимо них, для насильственного захвата предприятий могут использоваться и более примитивные способы, например, откровенный разбой, насилие и захват силовым путем, безо всяких «лишних бумажных процедур» (юридически переоформление захваченного предприятия осуществляется чуть позже, когда прежний владелец поймет бесполезность и опасность любого сопротивления).

Рейдеры и агрессоры: кто они?

Всех потенциальных агрессоров можно условно разделить на три категории. Первая категория — это *крупные промышленные холдинги и финансово-промышленные группы*. Они, как правило, осуществляют недружественные поглощения с целью дальней-

шего развития и диверсификации собственных субъектов хозяйствования.

Следует учитывать, что представители данной категории являются наиболее опасными агрессорами. Почему? В первую очередь потому, что они обладают практически неограниченными административными, силовыми и судебными, а самое главное — финансовыми ресурсами. У них везде «все схвачено», давно и надежно куплены самые опытные и квалифицированные судьи, имеется мощная поддержка в силовых структурах, а также в государственных органах (разумеется, все это достигается путем щедрых денежных и иных подношений «нужным людям» либо тем, кому они укажут). Бороться с такими захватчиками чаще всего является безнадежным и даже опасным занятием: предприятие все равно отберут, а бывшего владельца, оказавшего упорное сопротивление — еще и всячески дискредитируют (например, осудят за несовершенное преступление и растиражируют это в «карманных» СМИ), либо — применят к нему физическое насилие. Кстати, не стоит забывать: какие бы абсурдные, противоречащие закону и здравому смыслу положения не содержал судебный документ, он в любом случае имеет юридическую силу и обязателен для исполнения. Поэтому поддаваться эмоциям, спорить и доказывать, что «эта бумажка для меня ничего не значит» — совершенно бесполезно.

Ко второй категории захватчиков относятся *инвестиционные компании, которые избрали недружественное поглощение своим основным видом деятельности*. В данном случае захватываемое предприятие интересует их лишь с точки зрения выгодной последующей перепродажи. Иначе говоря, купив предприятие, они не планируют использовать его по назначению в соответствии с имеющимся профилем (производство, торговля, грузоперевозки, строительство и т. д.): их оно интересует лишь как товар, предназначенный для дальнейшей продажи с целью получения максимальной прибыли.

Отметим, что представители данной категории захватчиков стремятся поглотить и впоследствии перепродать захваченное предприятие как можно быстрее. Именно по этой причине они,

как правило, не заинтересованы в долгих и нудных судебных разбирательствах, затягивании принятия судебных решений, масштабных кампаниях в средствах массовой информации и т. п. Почему? В первую очередь потому, что это приводит к быстрому и существенному снижению стоимости захваченного предприятия: не секрет, что активы «с проблемами» котируются, прямо скажем, невысоко. Еще одной причиной является то, что захватчики данного вида действуют на собственные средства, которые бывают весьма ограничены.

Представители третьей категории несколько напоминают своих «коллег», относящихся ко второй категории. Ими являются *инвестиционные компании, которые работают по конкретным заказам*. Да-да — оказывается, бывает и такое! Характерной особенностью захватчиков данного вида является то, что их возможности четко ограничены заказчиком. Очень редко представители этой категории имеют более-менее существенный административный, судебный или силовой ресурс — в первую очередь, по причине ограниченности собственных финансовых и иных средств (попросту говоря, для них это слишком дорого).

По оценкам независимых экспертов, относящиеся к третьей категории захватчики представляют собой наименьшую опасность. Им можно относительно легко и эффективно противодействовать, как говорится, даже «малой кровью».

Наиболее важными условиями построения грамотной и эффективной системы бизнес-безопасности являются знание службой безопасности предприятия типологии потенциальных захватчиков и адекватная оценка их возможностей.

Типичные признаки начавшегося захвата

Одним из наиболее явных симптомов начавшегося процесса недружественного поглощения является факт неожиданного и совершенно необоснованного проявления интереса к деятельности предприятия со стороны миноритарных акционеров. С их стороны поступают неожиданные вопросы, они требуют предос-

тавить копии тех либо иных документов и т. д. Причем в большинстве случаев эти действия не предпринимаются самими миноритарными акционерами, а исходят от их представителей, которые в совершенстве владеют акционерным правом. Это очень тревожный звонок: профессионалы знают свое дело и сумеют подготовить почву для максимально безболезненного и беспроблемного поглощения вашего бизнеса — если, конечно, вы (а точнее — служба безопасности вашей компании) не предпримете адекватных, решительных и эффективных мер.

Следующий характерный симптом — предприятие испытывает серьезные проблемы правового характера, возникающие из-за судебных обращений, направленных на защиту прав миноритарных акционеров. Отметим, что нередко данные иски с точки зрения здравого смысла являются полностью абсурдными и «высосанными из пальца», но в целом данное явление свидетельствует о начавшемся процессе насильственного захвата предприятия. Кстати, подобные исковые заявления часто подаются одновременно в нескольких разных регионах — а это уже свидетельствует о том, что действиями миноритарных акционеров руководит чья-то умелая рука, координируя и направляя процесс в нужное русло.

Характерным признаком начавшейся кампании по недружественному поглощению предприятия является нездоровый и активный интерес к нему со стороны средств массовой информации, причем интерес однобокий и носящий явно тенденциозный и деструктивный характер. В газетах, журналах и Интернете появляются явно заказные статьи о том, что в данной компании неоднократно и существенно нарушаются права акционеров, менеджмент уже давно является неэффективным, используются устаревшие приемы и методы работы, предприятие практически перестало выполнять свои инвестиционные обязательства и т. д. и т. п. С помощью таких материалов осуществляется подготовка общественного мнения (и не только) к предстоящей смене собственника (собственников) предприятия.

Однако нездоровый интерес к компании может проявляться и с точностью до наоборот, и это тоже является характерным

признаком начавшегося недружественного поглощения. На предприятие начинают наведываться какие-то посторонние и непонятно откуда взявшиеся эксперты, консультанты, исследователи, которые полагают, что фирма является очень успешной, высокорентабельной, работает эффективно и прибыльно, и желают выяснить причины столь ошеломительного успеха.

Явный симптом начавшегося насильственного захвата — это резкое и существенное ухудшение взаимоотношений предприятия с местными органами власти, особенно если до этого оно не испытывало никаких проблем с государством и фискальными органами. Местная администрация может по надуманной причине лишить предприятие лицензии на право осуществления основного вида деятельности, отказать в аренде офисных помещений либо производственных площадей, ограничить подачу электроэнергии. Стоит ли говорить, что эти действия полностью пропла-чены компанией-захватчиком (размеры взяток за подобное «содействие» могут достигать астрономических величин) и являются началом тщательно спланированной акции по недружественному поглощению вашего бизнеса!

Одновременно с этим предприятие начинают тщательно проверять все, кому не лень. Чуть ли не впервые за все время функционирования предприятия появляются представители пожарной службы и начинают осматривать каждый закуток, выдав в конечном итоге предписание о наличии существенных нарушений противопожарной обороны и запрете в связи с этим эксплуатации помещений. Также приходит санстанция, само собой — тоже находит нарушения и выписывает соответствующее предписание. Вполне могут посетить вас представители какого-нибудь природоохранного ведомства и сообщить, что складские помещения вашей компании, расположенные за городом, оказывают самое негативное воздействие на окружающую среду, и поэтому в ближайшее время будет принято постановление об их сносе.

Из налоговой инспекции являются самодовольные и наглые проверяющие, всем своим видом показывающие, что они настроены самым серьезным образом и никакой речи о «полюбовном» решении вопроса быть не может.

Как уже было отмечено, налоговая проверка при желании может поставить большой жирный крест на дальнейшем функционировании предприятия: никаких проблем не составляет найти нарушения, за которые на фирму будут наложены астрономические санкции, не исключено — с одновременным наложением ареста на расчетный счет и помещения компании.

Еще более серьезно — если на ваше предприятие заявятся представители отдела по борьбе с экономическими преступлениями либо работники налоговой полиции. Они могут не просто прекратить деятельность предприятия, но и привлечь его должностных лиц к уголовной ответственности — например, за неуплату налогов в особо крупном размере либо за злоупотребление служебным положением. Кстати, не секрет, что эти и другие подобные формулировки в современной России чаще всего используются не для реальной борьбы с преступниками, а для расправы с неугодными оппонентами.

Учтите, что при планируемом захвате предприятия проверяющих в первую очередь интересует следующее: реестры акционеров, наиболее существенные контракты снабжения и реализации, дебиторская и кредиторская задолженность предприятия.

Предельно четко на планирующийся насильственный захват предприятия указывает тот факт, что какой-нибудь неприметный владелец 1–2% акций компании просит предоставить ему на ознакомление список лиц, имеющих право на участие в общем собрании акционеров. Это же лицо наверняка потребует у регистратора сведения из системы ведения реестра, включающие в себя следующую информацию:

- имена владельцев (держателей) акций;
- количество акций, находящихся на руках у каждого держателя;
- категория и номинальная стоимость акций, находящихся на руках у каждого держателя.

Почему требуются именно эти сведения? Потому, что данная информация необходима для созыва внеочередного собрания акционеров в тайне от основного держателя акций. Кроме этого, подобные действия предпринимаются при целенаправленной скупке акций компании.

Нередко при попытке недружественного поглощения предприятия владельцам основного пакета акций поступает предложение об их продаже со стороны неизвестной инвестиционной компании. Этот симптом свидетельствует о том, что на ваш бизнес «положили глаз» и попытаются его захватить.

Помимо перечисленных, о готовящемся недружественном поглощении предприятия могут свидетельствовать и другие признаки — ведь многое зависит от специфики поглощаемого предприятия, от предпринимаемых захватчиками действий и т. д. Однако любой из указанных симптомов однозначно свидетельствует о приближающейся опасности и требует незамедлительного принятия соответствующих мер по защите компании.

Необходимо учитывать еще и следующий немаловажный нюанс. Очень часто осуществлением процесса недружественного поглощения занимаются бывшие работники силовых структур, и в первую очередь — спецслужб. Они психологически, тактически и практически рассматривают каждый новый проект недружественного поглощения как свое очередное спецзадание, проявляя при этом недюжинную смекалку и изобретательность. При этом они почти всегда используют пробелы и противоречия в российском законодательстве, которых, как известно — «воз и маленькая тележка». Кроме этого, используя имеющийся опыт, они заранее собирают о захватываемом предприятии максимум необходимой информации, как то: сведения об основных деловых партнерах, компромат на руководителей и должностных лиц компании, а также на мажоритарных акционеров, личная и деловая переписка руководителей и владельцев предприятия и т. д. Бороться с бывшими работниками спецслужб рядовому бизнесмену очень непросто, а зачастую — просто невозможно и даже опасно.

Как предотвратить захват предприятия с помощью превентивных мер

Система превентивной защиты от захватчиков должна включать несколько составных элементов.

Вначале необходимо сформировать защищенную корпоративную структуру. Суть здесь заключается в том, чтобы максималь-

но рассредоточить наиболее существенные активы предприятия по нескольким более мелким фирмам. Чтобы было понятнее, рассмотрим такой пример.

Допустим, предприятие занимается производством и реализацией какой-то продукции и имеет лицензию на право осуществления данного вида деятельности. Оно открывает три дочерние фирмы, на одну из них регистрируются складские помещения, на другую — офисные, на третью — производственная площадка со всем необходимым оборудованием. Весь персонал принимается на работу на головное предприятие, на «дочках» же числится минимум сотрудников (по принципу «директор-бухгалтер-шофер»). Головная фирма арендует у одной «дочки» склад, у второй — офис, у третьей — производственное оборудование и место под производственные помещения. Все основные финансовые потоки идут через головную фирму, она же заключает контракты на поставку и сбыт, в общем — осуществляет полноценную финансово-хозяйственную деятельность. Правда, иногда бывает целесообразно часть сбыта переложить на какую-нибудь «дочку» (например, вся продукция отгружается «дочке», а уже та продает ее непосредственным покупателям): ведь производимая продукция — это тоже активы. При такой постановке дела головное предприятие не имеет практически никакого имущества и более-менее серьезных активов (за исключением пары-тройки компьютеров).

Совет

Дочерние предприятия в подобных ситуациях следует регистрировать как закрытые акционерные общества.

Далее путем дополнительной эмиссии акций доля головного предприятия в уставном капитале дочерних фирм доводится до менее 25%. С помощью подобной схемы вы сможете создать систему перекрестного владения акциями дочерними предприятиями, поскольку все дополнительные акции будут размещаться между «дочками».

Это позволит вам решить две актуальнейшие задачи: равномерно распределить операционные и финансовые риски вашего бизнеса и обеспечить сохранность и конфиденциальность информации о том, кто реально владеет бизнесом.

На этом же этапе рекомендуется внести некоторые изменения в уставные и учредительные документы. Одна из популярных мер — это включение в учредительные документы пункта о том, что годовое собрание акционеров компании будет происходить не в офисе предприятия, а где-нибудь за границей, либо в ином строго определенном месте. Также можно закрепить в учредительных документах положение о том, что изменение состава совета директоров допускается не чаще одного раза в год, причем только на определенное количество человек.

Очень важным средством превентивной защиты является ограничение возможностей (в первую очередь — в части управления акционерным капиталом) высших должностных лиц компании, которые нередко являются держателями крупных пакетов акций. Не стоит забывать, что всегда существует риск продажи топ-менеджером своего солидного пакета акций внешнему агрессору, желающему захватить предприятие. Заметно снизить такой риск можно следующим образом: в трудовом договоре (контракте) с высоким должностным лицом (тем же топ-менеджером) должен присутствовать пункт о том, что работник не имеет права продавать свои акции в течение указанного срока.

Однако наиболее действенной превентивной мерой является сбор всех акций высокопоставленных работников компании в один топ-менеджерский пакет — это можно сделать, в частности, с помощью создания некоммерческого партнерства либо закрытого акционерного общества.

Также эффективной является следующая мера: в трудовом договоре (контракте) с каждым высшим руководителем должен быть отражен пункт о том, что в случае смены собственника и досрочного прекращения трудовых отношений выплачивается компенсация в такой-то сумме (причем размер компенсации должен быть астрономическим, чтобы потенциальному захватчику заниматься недружественным поглощением вашей компании было заведомо невыгодно).

Рекомендуется ограничить (конечно, в пределах разумного) полномочия высших руководителей компании. Например, директора можно ограничить в заключении сделок, так или иначе связанных с имуществом предприятия.

Одним из важнейших превентивных средств защиты является четкий и надежный контроль кредиторской задолженности предприятия.

Важно!

Кредиторская задолженность компании — один из излюбленных инструментов предприятий-захватчиков, используемый для реализации процесса недружественного поглощения.

Контролировать кредиторскую задолженность предприятия должен как руководитель, так и служба безопасности. Особое внимание следует уделять просроченной кредиторской задолженности: нельзя допускать возникновения условий для давления на предприятие со стороны кредиторов, которым надоело ждать погашения долга.

Категорически не рекомендуется вступать в те или иные договорные отношения с неизвестными субъектами хозяйствования, которые в будущем могут внезапно исчезнуть. В любом договоре должен присутствовать пункт, предусматривающий обязательное информирование другой стороны об изменении основных реквизитов предприятия. В первую очередь к таким реквизитам относятся: юридический адрес субъекта хозяйствования, его банковские реквизиты, а также индивидуальный номер налогоплательщика.

Кстати, для отражения кредиторской задолженности иногда бывает целесообразно открыть отдельное юридическое лицо, которое будет находиться под полным контролем у собственников и высших должностных лиц предприятия. На такой фирме числится вся кредиторская задолженность головного предприятия, и тем самым внимание потенциальных захватчиков отвлекается на не имеющее никакой ценности юридическое лицо.

В качестве эффективной превентивной меры можно также предложить следующую схему. Предприятие, являющееся лакомым куском для потенциальных захватчиков, заключает договор на отгрузку своей продукции с крупнейшим потребителем. Этот договор включает важный пункт: при смене собственника (собственников) предприятия-поставщика, а также его органов управ-

ления компания-покупатель имеет полное право расторгнуть договор в одностороннем порядке.

Поскольку покупатель является крупнейшим потребителем данной продукции, то после расторжения данного договора у него возникает серьезнейшая проблема с поставками, и ему необходимо в срочном порядке подыскивать себе другого надежного поставщика. Стоит ли говорить, что в подобной ситуации компания-покупатель будет нести серьезные убытки! А компенсировать эти убытки должен прежний поставщик, т. е. фактически долг по ним, а также — по немалым штрафным санкциям ложится на компанию-захватчика. При составлении договора нужно учесть, что причитающаяся к возмещению в данном случае сумма должна быть астрономической, дабы отбить желание у агрессоров заниматься насильственным захватом предприятия.

Если поглощение уже идет, или Как остановить начавшийся рейдерский захват

Если вы обнаружили, что в отношении вашей компании уже начался процесс недружественного поглощения — помните: все методы и средства, которые использует против вашего бизнеса компания-захватчик, с успехом можно применить против самого агрессора. Причем для защиты, как правило, требуется намного меньше сил и средств, чем для нападения: как показывают результаты независимых исследований, если предприятие-жертва тратит 1 рубль на защиту, то это вынуждает агрессора тратить 10 рублей на дальнейшую атаку.

В качестве эффективной меры противодействия недружественному поглощению можно порекомендовать проведение контрскупки акций своего предприятия, а также — активную, целенаправленную и мощную скупку акций компании агрессора. Нередко этой не самой сложной меры бывает вполне достаточно для того, чтобы охладить пыл не в меру агрессивных захватчиков.

Если вы чувствуете, что агрессор настроен серьезно и решительно — срочно проводите реструктуризацию активов своей

компании. Иначе говоря, выводите все более-менее серьезные активы и оформляйте их на подставные дочерние фирмы: «распыляться» на несколько мелких фирм, дабы захватить активы каждой из них по отдельности, агрессору будет невыгодно ни экономически, ни с точки зрения здравого смысла.

Если агрессор уже скупил какую-то часть акций вашего предприятия — рекомендуется осуществить блокировку этого пакета акций с одновременным проведением дополнительной эмиссии акций: это позволит сделать бессмысленными все предыдущие действия агрессора.

Если в отношении вашего предприятия начат процесс недружественного поглощения — вспомните известное правило: лучшая защита — это нападение. Пишите соответствующее заявление в правоохранительные органы, обращайтесь с исковыми заявлениями в отношении компании-захватчика в судебные органы, ставьте в известность о происходящем местные органы власти. Даже если в вашем регионе агрессор имеет мощные административные, силовые, судебные и иные ресурсы, то в дальнейшем вы сможете обратиться в вышестоящие инстанции, приложив копии ответов из органов местной власти (а эти копии ответов вполне могут свидетельствовать о наличии в вашем регионе коррупции).

Также необходимо привлечь внимание широкой общественности к происходящему. Найдите хороших журналистов, пусть они опубликуют в газетах, журналах и Интернете несколько внушительных статей о том, как ваше преуспевающее предприятие подвергается попытке недружественного поглощения со стороны сомнительной структуры, возможно — имеющей криминальные корни. Можно упомянуть о том, что предприятие-захватчик оказалось не в состоянии вести собственный бизнес и пришло к полнейшему упадку по причине редкого непрофессионализма и дилетантизма со стороны как владельцев, так и высших должностных лиц и теперь пытается поправить свои дела, насильственно захватив преуспевающее предприятие.

Если у вас есть связи на телевидении — можно преподнести примерно такую же информацию в каком-нибудь новостном сю-

жете, сдобрив ее для верности краткими интервью со счастливыми работниками вашего преуспевающего предприятия, выступающими категорически против недружественного поглощения, а также любой смены собственников и управленческих кадров компании.

Кстати, человеческий ресурс может оказать мощную поддержку владельцу поглощаемого предприятия. Проведите общее собрание всех без исключения работников предприятия и объясните им ситуацию. Расскажите, что сейчас все они имеют работу, получают неплохую заработную плату, но ситуация складывается таким образом, что предприятие хотят насильственно захватить совершенно посторонние агрессоры. Поясните, что в случае смены собственника дела на предприятии заметно ухудшатся, начнутся проблемы с выплатой заработной платы (она заметно снизится, а выплачиваться будет с задержками), изменится в худшую сторону порядок предоставления отпусков и оплаты больничных листов. И вообще — социальная программа на предприятии будет практически свернута, о таком понятии, как «социальный пакет», лучше полностью забыть, то же самое касается медицинской страховки, и плюс ко всему — значительная часть работников попадет под сокращение штатов.

Стоит ли говорить, что подобные перспективы будут восприняты вашими работниками в штыки! Особенно если отношение к персоналу со стороны предприятия в данный момент вполне достойное, люди действительно получают вовремя неплохую заработную плату и т. д. Очень может быть, что, когда представители компании-захватчика приедут на предприятие предъявлять ультиматум руководству (либо — просто посмотреть, что здесь и как), их у дверей встретит толпа агрессивно настроенных работников и просто погонит прочь. При хорошей «предварительной подготовке» персонала с вашей стороны в ход вполне могут пойти гнилые помидоры, тухлые яйца, а из толпы прямо в лобовое стекло приехавшего с захватчиками 600-го «Мерседеса» полетит внушительных размеров булыжник.

Кроме этого, сотрудники собственного предприятия могут оказать и другую существенную помощь, если не лично, то через

какие-то имеющиеся связи. Например, у одного дядя является высокопоставленным чиновником в местной мэрии, у другого — брат работает в правоохранительных органах, у третьего папа является отставником ФСБ с мощными связями, и т. д. Приложив совместные усилия, вполне можно отстоять родное предприятие от недружественного поглощения, попутно хорошенько «прополоскав» агрессора в средствах массовой информации и по местному телевидению.

При разработке и реализации мер защиты не стоит забывать немаловажный нюанс: у захватываемого предприятия есть реальная стоимость, на которую рассчитывает компания-захватчик. Иначе говоря, агрессор заранее определяет максимально возможную цену, которую он согласен заплатить за осуществление операции недружественного поглощения. Обычно предельно допустимый размер «цены вопроса» находится в пределах годовой, реже — полуторагодовой прибыли захватываемого предприятия. Учтите, что в данном случае речь идет о реальной прибыли компании, а не о той, которая декларируется в налоговом органе и отображается в официальных бухгалтерских и налоговых отчетах.

Поэтому при защите своего предприятия от начавшегося недружественного поглощения исключительно важным является умение всеми доступными средствами затягивать время. Чем больше времени тянется процедура захвата (а точнее — борьба захватываемого предприятия с агрессором), тем больше возрастает «цена вопроса», т. е. величина затрат, которые приходится нести захватчику. Российская практика показывает, что злоумышленники отказываются от своих намерений после того, как стоимость операции по насильственному поглощению компании достигает двухгодичной (редко 2,5 года) реальной прибыли захватываемого предприятия.

Глава 7

Мошенничество, шантаж и вымогательство с применением IT-технологий

В наш век бурного развития IT-технологий невозможно представить, чтобы злоумышленники разных мастей оставили эту сферу без своего внимания. В частности, они могут не только воровать конфиденциальную информацию и даже «держать руку на пульсе» вашего предприятия, но и заниматься откровенным шантажом и вымогательством. В этой главе речь пойдет о том, какие опасности их деятельность может нести для бизнесменов и деловых людей.

Хакеры и основные объекты их «охоты»

Хакер в общепринятом понимании этого слова — это мошенник, осуществляющий противоправную и деструктивную деятельность в Интернете и сфере IT-технологий.

В настоящее время опытные хакеры обладают целым арсеналом «продвинутых» средств, которые позволяют им без проблем проникнуть в любой компьютер или корпоративную сеть. Например, иногда для того, чтобы заполучить в свой компьютер программу-шпиона, достаточно просто зайти на определенный сайт. Адрес этого сайта вы можете получить в спамерском электронном письме, причем ссылка вполне может сопровождаться заманчивым пояснением, вроде: «Лучшие девушки Рунета» или

«Читай компромат на президента» и т. д. Кроме этого, программы-шпионы могут распространяться в виде вложений к почтовым сообщениям, да и вообще теми же способами, что и компьютерные вирусы.

Какие же сведения интересуют хакеров?

В большинстве случаев — никакие, поскольку они действуют по наводке определенных лиц (конкурентов, недоброжелателей и т. п.). А вот тех уже интересовать может очень и очень многое: реальные (а не те, которые подаются в налоговую инспекцию) отчетные данные, деловая переписка, сведения с онлайн-конференций и совещаний, коды доступа, логины и пароли и т. д. Кстати, пин-кодами, логинами, паролями и иными подобными сведениями могут интересоваться и сами хакеры — например, с целью мошенничества.

Не стоит забывать и о таком явлении, как хакерские атаки, в результате которых, например, может «упасть» корпоративный сайт, прекратить работу корпоративный почтовый сервер, полностью оборваться выход в Интернет и т. д. Конечно, через некоторое время работоспособность поврежденных ресурсов будет восстановлена, но это потребует немало усилий, времени и средств.

Некоторые методы и приемы, используемые хакерами

Распространенный хакерский прием — это Denial of Service, по-русски — «Отказ от обслуживания». Он реализуется с помощью хакерской атаки и приводит к выводу из строя операционной системы либо отдельных приложений. Достигается это за счет того, что хакер хитрым способом формирует особый запрос к тому или иному приложению, в результате чего оно перестает работать. Обычно для возврата приложения в рабочее состояние приходится перезагружать компьютер.

С целью блокировки электронной почты могут организовываться так называемые «почтовые бомбежки» (Mail Bombing). Сущность приема заключается в следующем: на компьютер, имеющий почтовый сервер, посылается огромное количество

почтовых сообщений, в результате чего тот просто «виснет» и выходит из строя. Если эти письма будут содержать вложения, то при их проверке может «зависнуть» и антивирусное программное обеспечение. Иногда письма присылаются в таком немыслимом количестве, что переполняют жесткий диск компьютера и полностью блокируют его работу.

Для защиты от «почтовых бомбежек» в большинстве случаев достаточно выполнить грамотную настройку почтового сервера.

Довольно эффективным хакерским методом является снифинг (прослушивание сети). Если в корпоративной локальной сети вместо коммутаторов установлены концентраторы, то полученные пакеты доставляются всем машинам в сети, а уже каждый компьютер самостоятельно определяет, к нему или нет относится данный пакет. Если хакер сумеет проникнуть в компьютер, который является участником такой сети, или получит доступ непосредственно к корпоративной сети, то ему будет доступна абсолютна вся имеющаяся в сети информация (включая совсем уж секретные данные вроде логинов, паролей и т. п.). В данном случае дальнейшие действия злоумышленника предельно просты: он с помощью сетевой карты, настроенной на режим прослушивания, будет легко принимать все пакеты, кому бы они ни адресовались.

Для защиты от подобного проникновения рекомендуется вместо концентраторов использовать коммутаторы, а также шифровать весь трафик.

Если никаким программным методом у злоумышленника не получается проникнуть в компьютер либо корпоративную сеть, то он может сделать это физически. Например, характерной особенностью клавиатурных шпионов (кейлоггеров — подробнее о них речь пойдет ниже) является то, что они могут выступать не только в виде внедренного в компьютер вредоносного программного обеспечения, но и в виде отдельных устройств. Такие устройства обычно устанавливаются между клавиатурой и системным блоком и, поскольку имеют весьма небольшие размеры, могут долго оставаться незамеченными. Однако чтобы установить такое устройство, необходим доступ к компьютеру в отсут-

ствие пользователя. Чтобы своевременно обнаружить такой «сюрприз», рекомендуется почаще обращать внимание на то, не появилось ли новое устройство между клавиатурой и системным блоком.

Еще один вариант — это так называемый «ip-хайджек». В данном случае хакер просто физически внедряет устройство в сетевой кабель, выступая как бы в виде посредника при передаче пакетов. Это позволяет ему овладевать всей передаваемой информацией. Правда, это не самый лучший прием ввиду относительно легкого обнаружения.

Для защиты от подобного «врезания» необходимо постоянно отслеживать состояние сетевых кабелей, а еще лучше — использовать специально предназначенные защитные кабельные короба. Ну и, конечно, обязательно нужно шифровать весь трафик.

Часто для достижения своих целей хакеры используют метод «ложного DNS-сервера» — правда, его применение возможно только в том случае, если сетевые настройки установлены в автоматический режим. В таком случае при подключении компьютера к сети он выдает запрос (иначе говоря — отправляет широковещательный пакет) относительно того, кто будет являться его DNS-сервером, к которому в последующем будут отправляться DNS-запросы. Если злоумышленник имеет физический доступ к сети, то он вполне может перехватить подобный широковещательный запрос и ответить, что именно его компьютер будет являться DNS-сервером.

Это один из наиболее опасных хакерских приемов, поскольку он позволяет манипулировать захваченным компьютером, как марионеткой. Например, если пользователь захочет зайти на сайт банка и осуществить перечисление куда-либо денежных средств, то мошенник вполне может отправить его на свой компьютер и предоставить для заполнения фальшивую банковскую форму ввода учетных данных (например, логина и пароля). В конечном итоге эти учетные записи будут в распоряжении злоумышленника.

Для защиты от подобного мошенничества рекомендуется максимально ограничить возможности физического доступа к корпоративной сети посторонних лиц.

Использование мошенниками шпионского ПО

Для реализации своих преступных замыслов мошенники активно используют специальное программное обеспечение — так называемые программы-шпионы (SpyWare). Далее речь пойдет о том, что они собой представляют, какие виды SpyWare наиболее распространены и чего следует опасаться в первую очередь.

Общие сведения о шпионских программах — SpyWare

В настоящее время существует несколько видов шпионского ПО. Например, у многих злоумышленников пользуются популярностью сканеры жесткого диска. Этот шпион тщательно изучает все содержимое жесткого диска вашего компьютера (какие программы установлены, какие файлы и папки хранятся, и др.) и отсылает собранные сведения своему хозяину. Таким образом, злоумышленник получает сведения о том, где хранятся файлы ключей WebMoney, в каком каталоге установлен WebMoney Keeper, а также прочие секретные сведения.

Информацию о том, чем вы занимаетесь на компьютере, может собирать экранный шпион. Сущность его состоит в том, что он периодически через определенные промежутки времени (которые заданы злоумышленником) делает снимки экрана (на компьютерном сленге — скриншоты) и отсылает их хозяину. Подобные сведения могут представлять интерес, например, для шантажистов и вымогателей.

Также немалой популярностью у злоумышленников пользуются так называемые «прокси-шпионы». После того как такой SpyWare проникает в компьютер, этот компьютер будет выполнять роль прокси-сервера. На практике это означает, что злоумышленник при работе в Интернете сможет прикрываться именем (точнее — IP-адресом) ничего не подозревающего пользователя, и если его действия будут носить деструктивный или противозаконный характер — отвечать придется безвинному

человеку. В частности, это может обернуться не только внушительными штрафами, но даже привлечением к уголовной ответственности.

Еще один популярный у злоумышленников вид SpyWare — это почтовые шпионы. Их главная задача — сбор сведений об адресах электронной почты, хранящихся в данном компьютере, и отсылка этой информации хозяину. Сведения собираются обычно в почтовых программах и адресных книгах, а также органайзерах. Такая информация имеет высокую ценность для тех, кто занимается рассылкой спама. Кроме этого, почтовые шпионы могут вести откровенно деструктивную деятельность: редактировать содержимое писем, менять пароль доступа и т. д., а это уже широкое поле деятельности для шантажистов и вымогателей.

Для борьбы со шпионским программным обеспечением предназначены специальные программные средства — защитные утилиты и программы категории AntiSpyWare.

Есть еще один опасный тип шпионских программ — клавиатурные шпионы, или кейлоггеры. О них речь пойдет в следующем разделе.

Чем опасны клавиатурные шпионы?

Клавиатурный шпион — это программа либо устройство, с помощью которого осуществляется постоянное наблюдение за всеми нажатиями клавиш на клавиатуре (а во многих случаях — и за всеми щелчками мыши) с целью получения информации обо всех набираемых пользователем текстах. Зачем это нужно? Ответ на данный вопрос у каждого злоумышленника свой: одному нужно перехватывать чужие почтовые сообщения, другому — получить номера кредитных карт, третьему — взломать пароли, четвертому — украсть у разработчика исходные тексты еще не вышедшей программы, а пятому — все вместе взятое и еще что-нибудь.

Важно!

С помощью клавиатурного шпиона злоумышленник может в кратчайшие сроки опустошить все кредитные карты и электронные кошельки жертвы.

Характерной особенностью клавиатурных шпионов является то, что они могут выступать не только в виде внедренного в компьютер вредоносного программного обеспечения, но и в виде отдельных устройств. Такие устройства обычно устанавливаются между клавиатурой и системным блоком, и, поскольку имеют весьма небольшие размеры, могут долго оставаться незамеченными. Однако, чтобы установить такое устройство, необходим доступ к компьютеру в отсутствие пользователя. Поэтому на домашних компьютерах такой вид клавиатурных шпионов встречается редко, чаще — на офисных и рабочих, а также на компьютерах «общественного пользования»: в студенческих аудиториях, на почте, в интернет-клубах и др. Чтобы своевременно обнаружить такой «сюрприз», рекомендуется почаще обращать внимание на то, не появилось ли новое устройство между клавиатурой и системным блоком.

Достаточно широко распространены в настоящее время так называемые перехватывающие клавиатурные шпионы. Такие шпионы в большинстве случаев представляют собой программу, состоящую из исполняемого файла с расширением *.exe, и dll-библиотеки, с помощью которой осуществляется управление процессами записи информации. Перехватывающий клавиатурный шпион без проблем запоминает практически любой набранный текст: документы, письма, исходные коды программ (данная возможность нередко используется для кражи исходников еще не вышедших программ), номера кредитных карт, пароли (в том числе и самозаполняющиеся) и т. д.

Клавиатурный шпион (имеется в виду программа, а не устройство) может проникнуть в компьютер разными способами: например, как и любой другой шпионский модуль — в составе какой-либо устанавливаемой на компьютер бесплатной программы (как правило — от неизвестного либо сомнительного разработчика), либо через программу обмена сообщениями, и т. д. В последнее время нередки случаи, когда для «получения» в свой компьютер клавиатурного шпиона достаточно было просто зайти на определенный сайт.

Стопроцентной защиты от клавиатурных шпионов, как и от других вредоносных программ, в настоящее время не существу-

ет — ведь известно, что на каждое противоядие можно найти новый яд. Однако при соблюдении мер предосторожности можно свести к минимуму вероятность их появления на компьютере.

Как самостоятельно распознать наличие в компьютере программ-шпионов

Отличительной чертой SpyWare является то, что их трудно распознать с помощью штатных антивирусных программ. Для борьбы с ними предназначены специальные утилиты, которые можно скачать в Интернете. Но помните: многие шпионские программы маскируются именно под утилиты для борьбы с ними. В результате, установив на свой компьютер утилиту для борьбы со SpyWare, можно вместо нее заполучить сам шпионский модуль. Поэтому рекомендуется либо использовать утилиты известных разработчиков, либо воспользоваться рекомендациями других пользователей, уже столкнувшихся с подобной проблемой ранее.

Характерные признаки наличия в компьютере SpyWare

В некоторых случаях пользователь может самостоятельно, без применения специальных программ категории AntiSpyWare распознать присутствие в компьютере шпионского ПО. Вот его характерные признаки:

- при запуске браузера по умолчанию начинает открываться совершенно незнакомая веб-страница (а не пустая страница или не та, что была ранее определена пользователем как домашняя);
- значительно увеличивается исходящий трафик;
- наблюдаются сбои в работе операционной системы;

- появление неоправданно высоких счетов за телефонную связь (наверняка в компьютер проник шпионский модуль автоматического дозвона);
- в браузере появились незнакомые элементы управления (кнопка, пункт контекстного меню, инструментальная панель и т. п.);
- появились незнакомые элементы в списке Избранное, причем удаление их невозможно;
- в окне **Диспетчер задач** на вкладке **Процессы** видно, что какой-то новый процесс использует ресурсы компьютера почти полностью;
- на экране монитора периодически произвольно появляются рекламные окна, причем даже при отсутствии действующего подключения к Интернету;
- на рабочем столе появляются незнакомые иконки либо значки, при активизации которых осуществляется автоматический переход на незнакомую веб-страницу.

Кроме этого, для обнаружения SpyWare можно провести небольшую «ревизию» содержимого компьютера. В частности, следует проверить содержимое папки **Program Files**, каталога автозагрузки, а также раздела **Установка и удаление программ** в **Панели управления**. Некоторые шпионские программы помещают свой значок в правую часть панели задач (рядом с часами), поэтому при возникновении подозрений нужно посмотреть — не появился ли в панели задач неизвестный значок? Также нужно проверить содержимое подменю **Пуск – Все программы** — некоторые шпионские модули могут проявиться здесь. В браузере следует проверить страницу, открываемую по умолчанию, а также папку **Избранное**.

Краткий обзор антишпионских программ

Одним из эффективных антишпионских средств по праву считается программа SpyWareBlaster, разработчиком которой является фирма JavaCoolSoftWare. Она предназначена для использо-

вания в операционных системах Windows любой версии, начиная с Windows 95.

Программа отличается эргономичным и в то же время простым и интуитивно понятным пользовательским интерфейсом, в котором большинство параметров настраиваются путем установки/снятия соответствующих флажков либо переключателей. Среди всего многообразия параметров работы программы особо следует отметить возможность блокировки настроек домашней страницы (в результате чего уже ни один шпионский модуль не сможет изменить, например, адрес страницы, загружаемой по умолчанию).

Также в программе реализована возможность создания «отката» для настроек интернет-обозревателя — достаточно зафиксировать текущие настройки браузера (причем можно сохранить несколько различных конфигураций настроек) и при необходимости вернуться к ним в любой момент (обычно — при возникновении подозрений, что в настройки интернет-обозревателя без участия пользователя были внесены нежелательные изменения).

Кроме упомянутых выше, программа SpyWareBlaster имеет ряд других интересных возможностей.

Еще одна полезная утилита для борьбы со шпионскими модулями — программа AVZ, которая распространяется бесплатно. Многие пользователи считают ее одной из лучших программ для поиска и удаления не только программ-шпионов, но и рекламных модулей. Кстати, помимо борьбы со шпионскими и рекламными модулями, эта программа успешно борется и с некоторыми вирусами. В определенном смысле она является аналогом знаменитой Ad-Aware.

Русскоязычный интерфейс программы удобен и понятен пользователю. Предварительная настройка AVZ проста, причем во многих случаях параметры, предложенные по умолчанию, являются оптимальными. Для каждого типа вредоносного объекта, который был обнаружен в процессе сканирования (вирус, программа-шпион и др.), можно указать, каким образом с ним поступить: удалять, выдать только отчет и др. Кроме этого, можно настроить сканирование на выборочный поиск вредоносных про-

грамм — например, искать и удалять только шпионские модули, а все остальное игнорировать.

В программе автоматически ведется протоколирование процесса сканирования. Полученный протокол при необходимости можно сохранить в отдельном файле для последующего изучения.

Для борьбы с клавиатурными шпионами можно использовать программы, предназначенные для борьбы и с другими SpyWare (две из них рассмотрены выше), а также специализированные программы, которые называются «анти-кейлоггеры». Одной из таких программ является Anti-keylogger, которую разработали российские специалисты.

К ее достоинствам можно отнести многоязычность (поддерживает, в том числе, и русский язык), а также удобство в эксплуатации. Программа обладает простым и дружественным интерфейсом. В разделе **Опции** предусмотрена возможность настройки параметров работы программы. Кроме этого, в разделе **Лист исключений** реализована возможность ведения списка исключений, куда можно включать программы, которые не должны распознаваться как клавиатурные шпионы.

Фишинг

Вид мошенничества, который мы рассмотрим в данном разделе, используется для кражи данных кредитных карт (номера кредитной карты, пароля, пин-кода и т. д.) с целью последующего присвоения чужих денежных средств.

Первые попытки фишинга были зафиксированы в конце 90-х годов прошлого столетия, и с тех пор популярность этого вида мошенничества постоянно растет. При этом мошенники могут действовать следующим образом.

Пользователь получает электронное письмо от лица своего банка с просьбой (а точнее — с требованием) срочно перейти по указанной в письме ссылке и подтвердить свои регистрационные данные. Ссылка приводит пользователя на поддельный сайт, который является точной копией сайта банка. Разумеется, ничего не подозревающий пользователь спокойно вводит свои конфиден-

циальные данные в форму на этом сайте, и тут же данные попадают к злоумышленникам.

Здесь возможны различные варианты. Например, мошенники могут потребовать ввести регистрационные данные либо для их подтверждения, либо для подтверждения якобы полученного крупного денежного перевода.

Каким же образом можно распознать, что полученное от имени банка письмо — фальшивка?

В большинстве случаев подобные письма могут иметь следующие признаки:

- к пользователю обращаются не лично по имени и фамилии, а общим приветствием — вроде «Уважаемый клиент»;
- в письме обязательно будет присутствовать гиперссылка на сайт и предложение туда перейти;
- требования подтвердить свои конфиденциальные данные весьма настойчивы;
- в письме возможно наличие угроз (заблокировать счет, прекратить сотрудничество и т. п.) в случае отказа от выполнения требований;
- не исключено наличие в письме грамматических и иных ошибок.

Также для заманивания пользователя на фальшивый сайт может использоваться внедренная в его компьютер вредоносная программа. Ее задача заключается в том, чтобы автоматически перенаправить пользователя на фальшивый сайт, как только он наберет в интернет-обозревателе определенный веб-адрес (как правило — адрес своего банка). Ну а дальше — обычная схема: ввод конфиденциальных данных в предложенную форму, после чего они попадут в руки мошенников.

Иногда для фишинга используются специальные клавиатурные шпионы. Их отличие от обычных клавиатурных шпионов (кейлоггеров) заключается в том, что они активизируются только после входа пользователя на определенный сайт (например — сайт банка). В результате все выполненные на этом сайте действия (в том числе и ввод данных кредитной карты) становятся известны злоумышленникам.

Удаленное шифрование данных

Описываемый в этом разделе способ интернет-мошенничества относится к разряду «продвинутых» и требует от злоумышленника определенной квалификации.

Речь идет об удаленном шифровании данных. Смысл этого способа заключается в том, что злоумышленник, получив доступ к удаленному компьютеру, шифрует в нем определенные файлы, документы и т. п. таким образом, что пользователь не может их самостоятельно расшифровать. Через определенное время пользователь зараженного компьютера получает электронное письмо с требованием перевести определенную сумму денег (это может быть и 100, и 10 000 долларов, и любая другая сумма) по указанным реквизитам — за это ему будет выслан ключ для расшифровки информации. Разумеется, пользователь в большинстве случаев готов отдать требуемую сумму, лишь бы вернуть свои данные.

Этот прием в настоящее время набирает все большую популярность. Следует отметить, что злоумышленники сейчас предпочитают шифровать данные не у какого-то домашнего пользователя (хотя такие случаи тоже нередки), а на корпоративных компьютерах и серверах — ведь домашний пользователь при всем желании не сможет заплатить столько же, сколько какая-нибудь даже небольшого размера фирма.

При возникновении подобной ситуации можно считать удачей, если злоумышленник требует перевести деньги банковским переводом — в этом случае его относительно легко вычислить (разумеется, своевременно обратившись в соответствующие органы). Но если в качестве платежных реквизитов указывается кошелек WebMoney, Яндекс.Деньги либо аналогичной интернет-системы, то здесь шансы обнаружить злоумышленника невелики. В данном случае хорошо, если после получения денег он не поленится выслать ключ для расшифровки данных.

Можно сказать, что удаленное шифрование данных является одним из самых изощренных и опасных видов интернет-мошенничества.

DOS-атака на сайт с последующим вымогательством денег

Многим наверняка знакомо такое понятие, как DOS-атака. Сущность заключается в том, что какой-либо веб-ресурс подвергается мощной программной «бомбежке», в результате чего сайт или начинает очень сильно «тормозить», или попросту «падает». Долгие годы этот метод использовался преимущественно для того, чтобы вывести из строя сайты конкурентов или просто отомстить той или иной организации.

Однако с недавних пор этот технический прием стал активно использоваться мошенниками. Алгоритм их действий прост: на сайт-жертву организуется мощная DOS-атака. После того как сайт успешно «ляжет», злоумышленники связываются с его владельцем или администрацией и диктуют свои условия: мол, платите такую-то сумму денег — и сайт «оживет». Чтобы «подтолкнуть» жертву к принятию «правильного» решения, мошенники могут добавить, что в случае оплаты они гарантируют сайту защиту от подобных атак в будущем. В случае отказа атаки будут продолжаться, причем их мощность будет с каждым разом увеличиваться.

Стоит ли говорить, что после перечисления денег мошенникам никакая защита сайту от DOS-атак обеспечиваться не будет! Более того — выманив деньги один раз и «почуяв слабину», мошенники наверняка повторят свои действия.

В подобных ситуациях настоятельно рекомендуется не идти на поводу у мошенников, а объединить свои действия с владельцем хостинга и обратиться с соответствующим заявлением в правоохранительные органы.

«Реклама и продвижение» корпоративных сайтов

Каждый владелец корпоративного сайта желает, чтобы у него было много посетителей. Посещаемый ресурс способен привлекать клиентов, приносить прибыль, способствовать появле-

нию выгодных деловых партнеров, дальнейшему развитию бизнеса и т. д.

Учет числа посещений ведется с помощью специальных счетчиков. Сегодня абсолютно бесплатно можно получить счетчики, например, на следующих сервисах: www.hotlog.ru, www.mail.ru или www.bigmir.net.

В настоящее время развелось немало мошенников, которые делают вид, что занимаются продвижением сайтов. В реальности они лишь пускают пыль в глаза, однако их «услуги» по «раскрутке и оптимизации сайта» стоят недешево.

> ***Важно!***
>
> Многие мошенники подкупают тем, что за свои услуги они могут не требовать предоплаты.

В общем случае обман происходит примерно следующим образом. Человек вводит в поисковую систему запрос «услуги по продвижению сайтов» и в предложенном списке выбирает какую-нибудь организацию.

Связавшись с ней, он объясняет ситуацию (мол, такой-то сайт нужно раскрутить и т. п.), после чего стороны оговаривают стоимость услуг и сроки окончания работ.

Мошенники могут предложить клиенту, чтобы он наблюдал за тем, как растет число посетителей его сайта. Человек реально видит: вчера было столько-то посещений, сегодня их стало намного больше, а на следующий день счетчик вообще показал цифры, о которых и мечтать не приходилось. Когда наступает срок сдачи работ, заказчик с чистой совестью рассчитывается с «исполнителями», поскольку результат налицо.

Сразу после расчета ситуация кардинально меняется. Человек видит, что число посещений вновь резко снизилось, более того — вернулось практически на начальный уровень. Следовательно, деньги за раскрутку и продвижение сайта были потрачены зря.

А секрет состоит в том, что никто и не занимался оптимизацией, продвижением и раскруткой веб-ресурса. Вся «работа» мошенников заключалась в том, чтобы с помощью нехитрых манипуляций искусственно «накрутить» показания счетчика. Как

только они получили деньги от заказчика — они прекратили его «накручивать», следовательно — данные о посещаемости вернулись на прежний уровень.

Примечание

Сегодня в Интернете можно найти утилиты, предназначенные как раз для искусственной накрутки установленных на веб-ресурсах счетчиков. Если вас устроит такая «псевдопосещаемость» — вы можете накрутить показания счетчиков и самостоятельно, и вовсе не обязательно обращаться для этого к мошенникам.

Если вы намереваетесь заказать раскрутку и продвижение корпоративного сайта у профессионалов — постарайтесь найти их по рекомендации людей, которым доверяете. В крайнем случае, если такой возможности нет, хотя бы не поленитесь навести справки в Интернете об организации, к которой вы хотите обратиться.

Глава 8

Технические средства защиты и контроля

В настоящее время существует множество самых разнообразных технических средств защиты и контроля, активно используемых многими российскими субъектами хозяйствования. Далее будут рассмотрены некоторые из них.

Системы контроля доступа

Системы контроля доступа предназначены для предотвращения несанкционированного проникновения на территорию предприятия посторонних и нежелательных посетителей, а нередко и для фиксирования всех посещений. Самым распространенным средством контроля доступа является домофон, который устанавливается уже не только во многих офисах, но и в большинстве новых жилых домов и иных зданий и сооружений.

Принцип работы традиционного домофона прост: посетитель не может проникнуть в помещение, пока не сообщит по переговорному устройству, расположенному у запертой входной двери, о своем прибытии. Если человека согласны принять — ему откроют дверь, в противном случае — разумеется, нет. Одной из разновидностей домофонов являются видеофоны — приборы, с помощью которых можно не только переговариваться со стоящим у входа посетителем, но и видеть его.

При этом сотрудники компании открывают запертую дверь специальным ключом или карточкой, подносимой к считывателю: если код карточки или ключа имеется в памяти контроллера, куда считыватель передает информацию — дверь будет открыта.

Примечание

В настоящее время существуют домофонные и иные подобные системы, которые в качестве «ключей доступа» используют отпечаток пальца человека.

Кстати, при желании руководитель предприятия может постоянно получать информацию о том, в какое время сотрудники компании приходят на работу и уходят с нее: для этого достаточно установить сетевой либо автономный контроллер с возможностью вывода информации на экран монитора или записи ее на жесткий диск компьютера. Да и вообще — современные системы позволяют фиксировать абсолютно все посещения и любые передвижения людей в пределах офиса и сохранять эту информацию в видеофайлах либо иным способом.

Среди прочих систем контроля доступа можно отметить самые разные замки, турникеты, шлагбаумы и т. п. Кое-где контроль доступа осуществляется с помощью внушительных охранников, пропускающих и выпускающих посетителей и сотрудников только по соответствующим документам (пропускам и т. п.).

Охранная сигнализация

Охранная сигнализация применяется уже довольно давно и является одним из наиболее эффективных инструментов защиты помещений компании от несанкционированного проникновения посторонних в нерабочее время. По данным статистики, каждый второй субъект хозяйствования оборудовал свои помещения охранной сигнализацией.

Принцип работы типовой охранной сигнализации выглядит примерно следующим образом. Вначале представители организации, занимающейся монтажом и установкой сигнализации, внимательно изучают помещение на предмет выявления мест, наиболее удобных для несанкционированного проникновения (окна, двери и т. п.). Все такие места оснащаются специальными охранными датчиками. Затем в комнате охраны устанавливается прибор сигнализации, к которому подключены все охранные датчики. При любом открытии двери или окна либо при разбитии

оконного или дверного стекла, а также при любом несанкционированном проникновении в помещение соответствующие датчики передают сигнал на прибор охранной сигнализации. Работник охраны с помощью этого прибора сразу определяет, где и в каком месте совершено проникновение в помещение. Кстати, в месте проникновения при этом включается звуковая и (или) световая сигнализация.

Возможно, у читателя возникнет вопрос: поскольку далеко не все предприятия и организации имеют комнату охраны, где в таком случае устанавливается прибор охранной сигнализации и куда датчики отправляют сигналы?

В данном случае по желанию заказчика могут использоваться следующие варианты:

- передача сигнала на пульт вневедомственной охраны;
- передача сигнала по радиоканалу на пульт охраны организации, которая устанавливала охранную сигнализацию (некоторые поставщики охранных систем предлагают такую услугу);
- передача сигнала тревоги на введенные номера телефонов;
- передача тревожных SMS-сообщений на введенные ранее номера телефонов.

В современных охранных сигнализациях наиболее часто используются датчики трех типов: *инфракрасные датчики*, *датчики разбития стекла* и *герконы*. Кратко рассмотрим каждый из них.

Инфракрасные датчики реагируют на каждое движение объекта в охраняемом помещении; они бывают настенные и потолочные.

Название *датчика разбития стекла* говорит само за себя: он срабатывает при звуке бьющегося стекла (оконного, дверного, стеклянных перегородок и т. п.).

Датчики типа *«геркон»* состоят из двух элементов: собственно геркона (расшифровывается как «герметизированный контакт») и обыкновенного магнита. В рабочем состоянии эти элементы должны располагаться рядом друг с другом, причем магнит обычно монтируется на подвижную часть. Датчики этого типа могут устанавливаться на окна, двери, в иные раздвигающиеся

или открывающиеся места. Причем герконы бывают невидимые и накладные (в первом случае они являются врезными, во втором — монтируются прямо на поверхности). Герконы могут предназначаться специально для деревянных либо металлических поверхностей.

Системы видеонаблюдения

В современной России большинство более-менее крупных субъектов хозяйствования оборудовали свои помещения системами видеонаблюдения. Использование подобных систем позволяет решить следующие задачи:

- заметное облегчение и повышение эффективности работы службы безопасности предприятия;
- заметное расширение возможностей для деятельности подразделения экономической контрразведки;
- фиксирование и учет всех посетителей предприятия;
- информирование руководства компании о том, чем занимаются сотрудники в рабочее (а иногда — и в нерабочее) время.

Кроме этого, использование системы видеонаблюдения — это престижно, модно, солидно и эффективно.

В настоящее время различают три типа видеонаблюдения: уличное (внешнее), внутреннее и скрытое (последнее, как правило, наиболее эффективно).

Отметим, что для подбора оборудования, которое необходимо включить в состав системы видеонаблюдения на вашем предприятии, настоятельно рекомендуется пригласить специалиста из организации, у которой вы предполагаете его приобретать. Дело в том, что имеется множество нюансов, разобраться в которых может только специалист. Вместе с этим стоимость разных элементов оборудования может существенно различаться, а зачем вам переплачивать?

Конкретнее? — Черно-белая видеокамера стоит примерно вдвое дешевле, чем аналогичная цветная. Камера уличного наблюдения с АРД (автоматическая регулировка диафрагмы) где-то

в полтора раза дороже камеры без АРД. Стоимость камеры повышенной четкости (560–600 ТВЛ) примерно на 25–50% может быть выше, чем у камеры обычной четкости (420 ТВЛ).

Если вы не разбираетесь в подобной технике, то сами не сможете определить, какое именно оборудование вам требуется с учетом специфики расположения офиса, его внутренней планировки, наличия и состояния уличного освещения, и т. д. Можем лишь отметить, что для организации видеонаблюдения в стандартном офисе требуется в среднем от 4 до 10 камер, и всего один монитор (при условии, что между видеокамерами и монитором установлено специальное устройство — квадратор или мультиплексор).

Все полученные видеоизображения можно записывать как на видеокассету (хотя их век уже заканчивается), так и на жесткий диск. Отметим, что в стандартном офисе видеокамеры обычно монтируются на входе в помещение, в его коридорах, реже — в отдельных комнатах, кабинетах и вспомогательных помещениях.

Что касается видеокамер, предназначенных для скрытого наблюдения, то они могут маскироваться в стенах, датчиках пожарной или охранной сигнализации, вентиляционных отверстиях и иных укромных местах. При этом предназначенное для объектива отверстие по размеру не должно превышать 2 мм.

Если необходимо замаскировать камеру в стене, то она в нее попросту замуровывается. При этом снаружи остается лишь небольшой конец объектива диаметром пару миллиметров. Положительным качеством такой маскировки является то, что камеру скрытого наблюдения будет практически невозможно обнаружить. Однако подобный монтаж видеокамеры является довольно трудоемким, и его необходимо выполнять в отсутствие посторонних: в любом современном офисе любая новость (и уж тем более касающаяся установки камеры скрытого видеонаблюдения) разносится практически моментально.

А вот скрытые камеры, которые устанавливаются в датчиках охранной или пожарной сигнализации, можно монтировать в любое время: сотрудники наверняка будут думать, что устанавливается действительно сигнализация.

Кроме этого, камеры скрытого видеонаблюдения можно устанавливать под подвесным потолком, за картинами, плакатами, в имеющихся кабельканалах, в гнездах светильников и галогенных ламп, и т. д. В любом случае, скрытое видеонаблюдение поможет вам узнать много интересного о жизни вашего предприятия, а также о его сотрудниках.

Антижучок, или Средства обнаружения шпионской аппаратуры

Как уже отмечалось, в настоящее время на российском рынке представлено великое множество самых разных шпионских устройств и разведывательной аппаратуры: скрытые микрофоны, жучки, системы скрытого видеонаблюдения, аппаратура для съема и перехвата информации и т. д. Чтобы не допустить утечки конфиденциальной информации, подобные средства необходимо обнаруживать и обезвреживать.

Для обнаружения шпионской аппаратуры существуют специально предназначенные технические средства, объединенные под емким и конкретным названием «антижучок».

Например, некоторые категории антижучков работают путем выявления и подавления радиосигналов, исходящих от жучков, камер скрытого видеонаблюдения. Более того — они позволяют обнаружить подобные устройства, чтобы их можно было демонтировать и утилизировать (либо использовать против того, кто их установил). Причем нередко они оформляются в виде брелоков, часов, зажигалок и тому подобных не вызывающих подозрения предметов, что позволяет с их помощью чувствовать себя в безопасности не только в собственном офисе, но и в любых иных помещениях (на переговорах, на презентации, в ресторане...).

Что касается принципа действия небольших портативных антижучков, то в большинстве случаев он примерно таков: при обнаружении в непосредственной близости шпионской аппаратуры на антижучке загорается соответствующий световой индикатор либо он подает звуковой сигнал тревоги. Получив подобный сигнал, следует прекратить обсуждение конфиденциальных тем в данном помещении.

Также с помощью антижучка можно найти жучок или другую шпионскую аппаратуру: для этого нужно нажать кнопку «Поиск» и поднести антижучок к подозрительному месту (к вентиляционному отверстию, рабочему столу, за батарею, к щели между плинтусом и стеной и т. п.); при положительном результате поиска будет подан соответствующий сигнал. Наиболее часто используются следующие световые индикаторы:

- желтый — в обследуемом месте, а также в непосредственной близости от него шпионская аппаратура не обнаружена;
- оранжевый — антижучок обнаружил наличие радиоизлучения;
- красный — шпионская аппаратура находится в пределах метра от нахождения антижучка;
- красный мигающий (иногда сопровождается звуковым сигналом) — шпионская аппаратура находится на расстоянии нескольких сантиметров.

Некоторые из антижучков способны функционировать в режиме постоянного мониторинга, некоторые нужно включать и выключать.

Следует отметить, что кроме небольших и компактных антижучков в настоящее время существуют мощные профессиональные системы обнаружения шпионской и разведывательной аппаратуры. Их основной недостаток — громоздкость и невозможность незаметного применения, хотя, конечно, по функциональности, мощности и иным техническим характеристикам они намного лучше.

Заключение

Хочется верить, что эта книга дала вам много новой информации, касающейся безопасности бизнеса и его защищенности от внешних и внутренних угроз. Ее несомненным достоинством является то, что значительная часть представленного материала основана на рассказах практикующих бизнесменов, работников государственных органов (в том числе представителей налоговой инспекции, сотрудников ОБЭП, подразделений финансовых расследований), а также экономических разведчиков.

Автор выражает надежду, что предложенный материал был полезен и интересен читателям. Предложения и пожелания направляйте по адресу: arsen211@yandex.ru.

Гладкий Алексей Анатольевич

www.bhv.ru

Гладкий А.

Как обманывают при покупке автомобиля. Руководство для экономных

Магазин «Новая техническая книга»
СПб., Измайловский пр., д. 29, тел.: (812) 251-41-10

Отдел оптовых поставок
E-mail: opt@bhv.spb.su

Выбери самостоятельно хорошую машину без проблем!

- О чем нужно помнить, отправляясь на авторынок
- Как определиться с выбором автомобиля
- Малоизвестные секреты, уловки и хитрости продавцов
- Как определить истинный возраст подержанной машины
- Как обманывают в автомобильных салонах
- Самые коварные мошеннические приемы

Покупка автомобиля — сложный, ответственный, а иногда и опасный процесс. В сфере автомобильного бизнеса всегда хватало различного рода мошенников, для которых ничего не стоит оставить доверчивую жертву и без машины, и без денег. Рассказывается, где и на чем вас могут обмануть, а также как избежать обмана и что противопоставить мошенникам, о чем нужно помнить, отправляясь на авторынок, по каким признакам определяется истинный возраст подержанного автомобиля, на что обратить особое внимание при его внешнем осмотре, как маскируют дефекты двигателя и подвески, почему нельзя покупать машину по доверенности, как обманывают в автомобильных салонах (на валютных курсах, на укомплектованности машины, на продаже аксессуаров втридорога) и о многом другом. Практическую значимость приведенных советов и рекомендаций намного повышает тот факт, что они базируются на конфиденциальных рассказах лиц, непосредственно занятых в автобизнесе.

Гладкий Алексей Анатольевич, известный российский автор автомобильной, экономической и прикладной литературы. К настоящему времени из-под его пера вышло более 50 книг, большинство из которых за короткий срок выдержали несколько тиражей. Фирменный стиль А. А. Гладкого — простота и доступность изложения, легкость подачи материала, а также множество ценных советов и рекомендаций, основанных на реальных событиях. Все это во многом предопределяет популярность автора у читателей и обеспечивает стабильно высокий спрос на его книги.

www.bhv.ru

Гладкий А.

Особенности ПДД разных стран мира. Шпаргалка для тех, кто путешествует за рулем

Магазин «Новая техническая книга»
СПб., Измайловский пр., д. 29, тел.: (812) 251-41-10
Отдел оптовых поставок
E-mail: opt@bhv.spb.su

Почувствуй себя уверенно на зарубежных дорогах

- Что такое Международная конвенция о дорожном движении
- О чем нужно знать, въезжая в чужую страну
- Как избежать неприятностей при встрече с дорожной полицией
- Где внести дорожный сбор
- По какому графику работают АЗС в разных странах
- Какой скоростной режим действует на зарубежных дорогах
- За какие нарушения ПДД можно попасть в тюрьму

Книга представляет собой полезную шпаргалку для тех, кто планирует отправиться за границу за рулем автомобиля, и особенно — кто намеревается проехать транзитом несколько стран. Рассказывается, какой скоростной режим действует в той или иной стране, какие санкции полагаются за нарушение ПДД, каковы правила парковки, проезда нерегулируемых перекрестков, перевозки детей, использования ремней безопасности, зимних покрышек и т. д. Вы узнаете, чем в разных странах мира должен быть укомплектован автомобиль, какие документы обязан иметь при себе водитель, в каких странах права международного образца являются недействительными, в каком режиме работают автозаправочные станции, где внести дорожный сбор, что делать в случае ДТП, что такое Международная конвенция о дорожном движении, а также о многом другом.

Гладкий Алексей Анатольевич, известный российский автор автомобильной, экономической и прикладной литературы. К настоящему времени из-под его пера вышло более 60 книг, включая «Самоучитель безопасного вождения», «Готовимся к экзамену в ГИБДД. Комплексное руководство», «Как обманывают при покупке автомобиля. Руководство для экономных», выпущенных издательством «БХВ-Петербург». Большинство книг за короткий срок выдержали несколько тиражей. Фирменный стиль А. А. Гладкого — простота и доступность изложения, легкость подачи материала, а также множество ценных советов и рекомендаций, основанных на реальных событиях. Все это предопределяет популярность автора у читателей и обеспечивает стабильно высокий спрос на его книги.

www.bhv.ru

Магазин «Новая техническая книга»
СПб., Измайловский пр., д. 29, тел.: (812) 251-41-10

Отдел оптовых поставок
E-mail: opt@bhv.spb.su

Дубневич Ф.

Как построить дачу за полцены, 3-е изд.

- Планировка и строительство дома
- Столярные и плотничные работы
- Печи и камины

Если вы хотите своими руками и недорого построить уютный дом и благоустроить садовый участок, то эта книга, выдержавшая уже два издания и ставшая бестселлером, для вас. В ней вы найдете советы и рекомендации по выбору проекта дома, подготовке участка к строительству, фундаментным работам, возведению стен и перекрытий, по устройству крыши и кровельным работам, установке окон и дверей. Большое внимание уделено столярным и плотничным работам: внутренней отделке помещений, хозяйственным постройкам, ограждению участка и др. Подробно описана кладка печей и каминов. В новом издании рекомендованы современные строительные материалы и соответствующие им технологии.

Дубневич Федор Федорович, профессиональный строитель, специалист в области промышленного и гражданского строительства. Участвовал в проектировании жилых и общественных зданий в Санкт-Петербурге, высотных жилых и уникальных общественных зданий в Москве, а также в проектировании и строительстве малоэтажных домов в Подмосковье.