

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

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	<i>Екатерина Кондукова</i>
Зам. главного редактора	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Екатерина Капалыгина</i>
Редактор	<i>Елена Васильева</i>
Компьютерная верстка	<i>Людмилы Чесноковой</i>
Корректор	<i>Зинаида Дмитриева</i>
Дизайн обложки	<i>Марины Дамбиевой</i>

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

© Гладкий А. А., 2013

© Оформление, издательство «БХВ-Петербург», 2013

Оглавление

Введение	7
Глава 1. Чего больше всего опасаются мелкие и средние бизнесмены?	8
Агрессия как элемент современного российского бизнеса	10
Государственный бандитизм: шантаж со стороны госструктур и силовых органов	14
Грязные методы конкурентной борьбы	16
Нездоровый интерес со стороны собственных работников	22
«Наезды» со стороны криминалитета	24
Глава 2. Изохренные методы мошенничества и обмана, используемые «офисным планктоном»	27
Примерные объемы ущерба, причиняемого «оборотнями в офисе»	28
Типичный портрет сотрудника-мошенника	30
Типичный портрет честного работника	33
Как ворует и злоупотребляет бухгалтер	34
Получение бухгалтером «откатов» от сторонних структур	34
Примеры других бухгалтерских злоупотреблений	40
Важные нюансы, которые нужно учитывать при смене бухгалтеров	42
Хитрые приемы мошенничества, используемые кассирами	46
Обман и воровство на складе	47
Списание естественной убыли	48
Махинации с нормами расхода ценностей	48
Несоответствие отпускных и учетных единиц измерения	50
Инвентаризация как средство контроля	51

Злоупотребления снабженцев и сбытовиков	53
Попытка выкупа предприятия собственным менеджментом	54
«Подводные камни» при покупке программного обеспечения	55
Откаты товароведам	57
Глава 3. Проверка, провокация или шантаж?	60
Классификация современных проверок	60
Как действовать во время проверки	63
Превентивные меры, позволяющие предотвратить возможные неприятности	70
Если вы виноваты. Как незаметно для контролеров устранить некоторые нарушения	73
Оформление неучтенной реализации товара	73
Легализация активов через вклады собственников и учредителей предприятия	75
Уменьшение налогооблагаемой базы	76
Минимизация НДС через штрафы и неустойки	78
Специфика «неналоговых» проверок	78
Проверки санстанции	79
Проверки пожарных служб	82
Проверки природоохранных служб	85
Глава 4. Коррупция, мошенничество, аферы, подставы	87
Коррупция в современной России	87
Как бизнесменов провоцируют и ловят на взятках	89
Как распознать провокацию	90
Как грамотно противостоять провокатору?	93
Поддельные документы, печати и штампы	94
Искусственное занижение цен с целью обмана	97
Манипуляции с «фирмами-однодневками»	98
Неплатежеспособность должников и хитрости безнадежных дебиторов	100

Форс-мажор и его «подводные камни»	103
Виды и специфика форс-мажора	103
Минимизация потерь от форс-мажора	108
Обман с доверительным управлением финансами на валютных и фондовых рынках	111

Глава 5. Экономическая разведка и промышленный шпионаж 113

Какая информация интересует шпионов?	113
Источники информации, которыми пользуются разведчики и шпионы	117
Способы добычи интересующих сведений	119
Техническое обеспечение современного промышленного шпионажа	123
Инсайд как причина многих неприятностей	124
Противостояние шпионажу: экономическая контрразведка	128
Как должна функционировать служба экономической контрразведки	130
Дезинформация как один из самых эффективных элементов контрразведки	133
Практическое применение дезинформации	137
Как перевербовать экономического разведчика	141
Компромат как неотъемлемый инструмент контрразведки	143

Глава 6. Сравнительно честный отъем: рейдерство, или насильственный захват предприятий 147

Какие предприятия больше всего рискуют стать жертвами рейдеров?	149
Основные методы рейдерского захвата	150
Рейдеры и агрессоры: кто они?	152
Типичные признаки начавшегося захвата	154
Как предотвратить захват предприятия с помощью превентивных мер	158

Если поглощение уже идет, или	
Как остановить начавшийся рейдерский захват.....	162

Глава 7. Мошенничество, шантаж и вымогательство с применением IT-технологий.....166

Хакеры и основные объекты их «охоты».....	166
Некоторые методы и приемы, используемые хакерами.....	167
Использование мошенниками шпионского ПО	170
Общие сведения о шпионских программах — SpyWare	170
Чем опасны клавиатурные шпионы?.....	171
Как самостоятельно распознать наличие в компьютере программ-шпионов	173
Характерные признаки наличия в компьютере SpyWare	173
Краткий обзор антишпионских программ	174
Фишинг	176
Удаленное шифрование данных	178
DOS-атака на сайт с последующим вымогательством денег	179
«Реклама и продвижение» корпоративных сайтов.....	179

Глава 8. Технические средства защиты и контроля ...182

Системы контроля доступа	182
Охранная сигнализация	183
Системы видеонаблюдения.....	185
Антижучок, или Средства обнаружения шпионской аппаратуры	187
Заключение	189

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 совершаются возвратно-поступательные движения товаров, 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 острстки 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 сдерживать 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 несовершенно 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. Программшпионы 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 X 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 сногшибательным 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-

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

Иногда изначально могут запугивать не учредителя или ответственного лица 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 тельца»);
- ❑ 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-