

Гладкий Алексей

**Бизнес-безопасность в современной России:
что угрожает вашему бизнесу и как его
защитить**

Оглавление

Введение	6
Глава 1. Понятие бизнес-безопасности	7
Что представляет собой безопасность предприятия?	8
Задачи системы бизнес-безопасности	8
Когда следует подумать о безопасности?	10
Основные правила системы безопасности предприятия	12
Чего больше всего боятся российские бизнесмены?	13
Кто может проявить «нездоровый интерес» к вашему бизнесу?	15
Интерес со стороны государства	15
Интерес со стороны конкурентов	16
Интерес со стороны криминальных структур	19
Отрицательное влияние криминала на бизнес.....	19
Государственный бандитизм как часть российской экономики	20
Есть ли польза бизнесу от криминала?	22
Интерес к бизнесу со стороны собственных работников	22
Внутренний аудит и индикаторы злоупотреблений	23
Глава 2. Что угрожает вашему бизнесу?	26
Что говорит наука, или Энтропия и ее влияние на состояние бизнеса	26
Коррупция и ее место в современной российской экономике	28
Экономическая сущность коррупции.....	29
«Курс молодого взяточдателя», или Как правильно давать взятку	31
Бывает ли «некриминальная» коррупция?	34
Мошенничество и аферы как спутники бизнеса	35
Использование поддельных документов, печатей и штампов	36
Искусственное занижение цен, или Бесплатный сыр — в мышеловке	38
Использование фирм-однодневок.....	38
Недобросовестная конкуренция как вид современного мошенничества	40
Проблемы с дебиторской задолженностью	44
Почему не платят должники?	44
Распространенные уловки безнадёжных дебиторов	45
Форс-мажор и связанные с ним опасности	46

Виды и проявления форс-мажорных обстоятельств	46
Как минимизировать потери от форс-мажора	49
Агрессия — направленная и организованная угроза	51
Медиация как метод разрешения корпоративных конфликтов	55
Что такое «медиация»?	55
Пример применения медиации для разрешения конфликта	58
Глава 3. «Офисные оборотни», или Опасайся собственных сотрудников	60
Особенности внутренней коррупции	60
Объемы ущерба, причиняемого «офисными оборотнями»	61
Некоторые распространенные виды злоупотреблений и мошенничества	63
Внутренний коррупционер: кто он?	66
«Моральный облик строителя коммунизма», или Портрет честного работника	69
«Удар в спину», или Бухгалтерские злоупотребления	70
«Бухгалтерские» откаты	70
Прочие «злодеяния» бухгалтеров	73
Меняется бухгалтер? Будь начеку!	75
Как мошенничают кассиры	77
Воровство складских работников	78
«Естественная убыль» ТМЦ	78
Махинации с нормами расхода ТМЦ	79
«Передергивание» учетных и отпускных единиц измерения	80
Инвентаризация как средство контроля	81
Бывает и такое: сговор бухгалтера и программиста	82
Ошибки в подборе кадров и как их избежать	82
Что такое хед-хантинг?	85
Глава 4. К вам пришла проверка	87
Виды проверок	87
Как вести себя при проверке?	89
Подумай о безопасности заранее	93
Опасность использования «скользких» схем ухода от налогов	95
«Липовое» приобретение ТМЦ	96
Минимизация НДС через штрафы и неустойки	96

Уменьшение налога на прибыль с помощью мнимых расходов	97
Оформление нелегально проданного товара	98
Легализация активов через вклады учредителей	98
Угрозы со стороны «неналоговых» проверок.....	100
Проверки санстанции.....	100
Проверки пожарных служб	102
Проверки природоохранных служб	104
Глава 4. Рейдерство, или Что такое недружественное поглощение?	105
Современный рейдер: кто он?.....	106
Какие предприятия наиболее подвержены насильственному захвату?	107
Основные способы недружественного поглощения предприятий	108
Кто может выступать в роли захватчика?	110
Характерные признаки недружественного поглощения предприятия	111
Превентивная защита от недружественного поглощения	114
Как защититься, если процесс недружественного поглощения уже начался?	116
«Особенности национального захвата»	118
Глава 5. Информационная безопасность предприятия	119
Экономическая разведка и промышленный шпионаж	119
Цели экономической разведки	120
Сведения, интересующие экономических разведчиков и промышленных шпионов	120
Источники конфиденциальных сведений	123
Распространенные методы получения информации	124
Инструментарий промышленного шпионажа	126
«Империя наносит ответный удар», или Экономическая контрразведка	127
Цели и задачи службы экономической контрразведки.....	128
Планирование работы службы контрразведки	129
Дезинформация как эффективный инструмент экономической контрразведки	131
Планирование и реализация дезинформационных мероприятий	133
Можно ли перевербовать экономического разведчика?	136
Компромат как средство контрразведки	137
Берегись инсайдера!	140
Хакеры и их мишени	142

Кто такие хакеры и что им нужно?.....	142
Распространенные хакерские приемы.....	143
Технические средства защиты и контроля.....	147
Системы контроля доступа	147
Охранная сигнализация	148
Системы видеонаблюдения.....	149
Антижучок, или Средства обнаружения шпионской аппаратуры	150
Заключение	151

Аннотация

Не секрет, что в современной России предпринимательство — это опасная профессия, 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 угрозы появляются извне и непосредственно связаны с конфликтными ситуациями, рейдерством, недобросовестной конкуренцией, или просто привычной коррупцией чиновников. Однако не меньше угроз скрыто и внутри бизнеса: это могут быть корыстные побуждения, воровство или просто халатность персонала, и т.п.

Бизнес всегда в той или иной степени связан с риском, но зачем же при этом допускать лишние неприятности?

Данная книга представляет собой своеобразное «Руководство по технике безопасности для предпринимателей». Она поможет вам избежать многих неприятностей, угрожающих вашему бизнесу, сэкономив тем самым немало ваших денег и нервов.

Введение

Что представляет собой безопасность вообще и политика безопасности бизнеса — в частности?

Каждый человек имеет собственное индивидуальное представление о том, что означает понятие «безопасность». В реальности же безопасность — понятие весьма абстрактное и во многом относительное. Однако при этом существует также чувство безопасности, которое все мы воспринимаем примерно одинаково.

Человек чувствует себя в безопасности, когда пребывает в знакомой и комфортной обстановке, вокруг все «свое и родное», когда рядом нет новых или неприятных людей с малопонятными психологическими и иными индивидуальными особенностями, когда нет беспокойных и вообще — неожиданных вестей (так или иначе касающихся этого человека), а также вовремя поступают те известия, которые мы ожидаем и от которых не ждем ничего плохого.

Иначе говоря, человек испытывает ощущение безопасности, когда целиком держит на контроле или хотя бы искренне полагает, что держит на контроле то, что происходит вокруг.

Помимо ощущения безопасности всем нам хорошо известно противоположное чувство — волнения, беспокойства и опасности, пусть даже на первый взгляд совершенно безосновательной. То, что мы не знаем о наличии каких-то обстоятельств или событий, еще вовсе не свидетельствует о том, что этих обстоятельств действительно нет. Поэтому подобное беспричинное ощущение опасности — это нередко сигнал имеющегося жизненного опыта, трансформировавшегося в интуицию, который напоминает нам о том, что все хорошее когда-нибудь если не заканчивается, то, по крайней мере — на время прерывается.

Ощущение беспокойства и опасности, если только оно не имеет навязчивого и постоянного характера, может принести ощутимую пользу, особенно если говорить о бизнес-безопасности. Здесь распространенное правило «Меньше знаешь — крепче спишь» совершенно неактуально. Человек не в состоянии быть в курсе всех событий и проверять абсолютно все. Что касается группы людей, в частности — акционеров или руководителей компании, то «держать руку на пульсе» еще труднее, даже если это строго структурированная общность (что, заметим, очень редко имеет место быть в бизнес-практике). В любом случае будут присутствовать некие обстоятельства, о которых либо вообще никто из коллектива не осведомлен, либо, даже зная о них — не уделил достаточно внимания или специально утаил их наличие от других людей. Поэтому ощущение опасности — это, по сути, проявление инстинкта самосохранения, которое напоминает нам о непременном наличии неучтенных обстоятельств и призывает нас еще раз все взвесить и произвести изменения, как в текущее функционирование бизнеса, так и в общий механизм организации его безопасности.

Планировать систему бизнес-безопасности — это вовсе не значит, что нужно «шарахаться от каждого куста» и подозревать всех и каждого. Любой коммерсант или бизнесмен скажет — для любой компании такой подход неприемлем в принципе: несмотря на то, что бизнес базируется во многом на знаниях и расчете, в нем также

всегда имеется место нормальному доверию, или хотя бы — адекватному планированию рисков. Слишком твердая и всеобъемлющая система безопасности в компании может нанести ущерб бизнесу, поскольку парализует его динамику и рост сводя «на нет» всякое позитивное начало.

Даже если какие-то неблагоприятные обстоятельства существуют — это вовсе не говорит о том, что они содержат опасность. Однако на всякий случай рекомендуется помнить известный закон Мэрфи: «Если какая-нибудь неприятность теоретически может произойти — она обязательно произойдет».

Дело в том, что возможная опасность присутствует постоянно, и система бизнес-безопасности должна не только подозревать все и всех на предмет появления известных угроз, но еще и быть готовой адекватно воспринять и парировать любую угрозу.

Возможных неприятностей и опасностей для бизнеса существует очень много, поэтому 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 «прикинуть» в любой компании.

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

Адекватно оценивая вероятного противника, проще организовывать систему безопасности. Но его чрезвычайно опасно недооценивать, а уж тем более недопустима недооценка простых случайностей, поэтому политика безопасности — это не только политика постоянного отслеживания ситуации и определения невидимых угроз, а еще и политика постоянной готовности к трезвым и разумным действиям в возникшей проблемной ситуации.

ВНИМАНИЕ

При изучении данной книги следует учитывать, что все встречающиеся в ней совпадения, если таковые будут, являются случайными, а приведенные примеры носят условный характер.

Итак, что же представляет собой современная бизнес-безопасность? Об этом, а также о многом другом мы поговорим в первой главе книги.

Глава 1. Понятие бизнес-безопасности

Обеспечение собственной безопасности актуально для всех без исключения субъектов хозяйствования — независимо от вида деятельности, форм собственности и иных факторов. Разница может наблюдаться лишь в том, какие приемы и методы использует предприятие, дабы обезопасить себя от неприятностей.

Что представляет собой безопасность предприятия?

В общем случае под безопасностью субъекта хозяйствования подразумевается его защищенность от угрозы нанесения ущерба, а также от негативного влияния тех либо иных факторов. Для достижения безопасности используются меры организационного, правового, экономического, психологического, социального и технического характера.

Бытует мнение, что безопасность — это в первую очередь физическая защищенность предприятия. Однако это является распространенной ошибкой: прошло то время, когда предприниматели и бизнесмены чувствовали себя в безопасности, укрывшись в бронированном автомобиле или спрятавшись за спины могучих охранников. В настоящее время для достижения безопасности необходимо осуществлять всесторонний анализ потенциальных угроз, а иногда даже проводить математические вычисления с целью разработки эффективных средств защиты и минимизации возможных рисков. Угрозами для бизнеса является не только явления, имеющие физическую природу (рэккет, насилие, грабеж, порча или уничтожение имущества, и т.д.), но и целый ряд факторов некриминального характера: некомпетентность собственного персонала, мошенничество и воровство на предприятии, «наезды» налоговых и правоохранительных органов, непорядочность бизнес-партнеров, и т.д. и т.п.

Основная цель создания системы бизнес-безопасности — это обеспечение для предприятия возможности успешно осуществлять свою деятельность в условиях нестабильности (как внутренней, так и внешней), своевременно распознавать и предотвращать все потенциальные угрозы, защищать всеми законными способами свои интересы, охранять здоровье и жизнь работников предприятия. Также налаженная система безопасности позволяет пресекать различного рода злоупотребления (например, хищение денежных средств либо товарно-материальных ценностей, и др.), предотвращать порчу либо уничтожение активов субъекта хозяйствования, утечку конфиденциальной информации, а также попытки нанесения вреда либо получения секретных сведений с помощью IT-технологий.

Задачи системы бизнес-безопасности

Для достижения главной цели бизнес-безопасности, которая была сформулирована в предыдущем разделе, система бизнес-безопасности должна обеспечить решение перечисленных ниже задач.

- ❑ Своевременное выявление возможных угроз и оперативная разработка эффективных мер противодействия.
- ❑ Обеспечение защиты производственно-технологических процессов.
- ❑ Комплексная разработка и внедрение мероприятий, направленных на защиту конфиденциальной информации (коммерческой тайны, деловых секретов, и т.п.).
- ❑ Максимально подробное изучение деловых партнеров (как имеющих, так и потенциальных) и оперативное выявление фактов, которые должны вызвать