

18+

КРП

Дмитрий
Глазунов

Ренат
Мамбетов



БЕЗОПАСНОСТЬ БИЗНЕСА



NDA



Ренат Мамбетов

Безопасность бизнеса

«Издательские решения»

Мамбетов Р.

Безопасность бизнеса / Р. Мамбетов — «Издательские решения»,

ISBN 978-5-00-607046-2

Незащищенный бизнес долго не живет. В принципе он и существовать-то сегодня не может без реализации полного цикла безопасности. Посмотрите на брюнетку, весело болтающую со своей подружкой в центре Москвы. Что они там обсуждают, попивая кофе? Любовницу генерального директора и ее СПА-салон, открытый на «откатные» деньги? Ну-ну... Этот текст будет полезен руководителям крупных организаций, сотрудникам СБ, и просто увлеченным корпоративной жизнью людям.

ISBN 978-5-00-607046-2

© Мамбетов Р.
© Издательские решения

Содержание

Предисловие, которое необходимо прочесть	6
Введение	9
Глава 1.	12
Глава 2.	20
Конец ознакомительного фрагмента.	25

Безопасность бизнеса

Дмитрий Глазунов

Ренат Мамбетов

*Написано с уважением к сильным, инициативным, уверенным,
системным и умным людям.*

Друзья, коллеги, без вас этот труд не состоялся бы.

Корректор Елена Кормильцева

Дизайнер обложки Вера Филатова

© Дмитрий Глазунов, 2023

© Ренат Мамбетов, 2023

© Вера Филатова, дизайн обложки, 2023

ISBN 978-5-0060-7046-2

Создано в интеллектуальной издательской системе Ridero

Предисловие, которое необходимо прочесть

Мы прежде всего люди, а уже потом специалисты по безопасности и управлению рисками. И именно поэтому мы знаем, насколько тесно связана жизнь человека и жизнь бизнеса. Любая мелочь, происходящая ежедневно в вашей жизни, влияет на ее качество. Заболел ребенок, нервничает супруга, случилось небольшое ДТП? Каждый из этих факторов повлияет на дальнейшую судьбу семьи, где-то меньше, а где-то больше. Так и в организации – любое малозначительное, на первый взгляд, происшествие может и будет влиять на общую обстановку. На производственные процессы, на настроение коллектива, на личные провалы в графике руководителя. И в итоге повлияет на показатели финансовой прибыли. Грамотно настроенная система безопасности нивелирует большинство крупных проблем и мелких неурядиц. Такая система может заранее спрогнозировать проблемы, а при их внезапном проявлении помогает справиться с ними максимально оперативно и безболезненно.

Так вот, немного об авторах этой книги, об их опыте и о том, почему безопасность предприятия должна быть именно системной. А также несколько слов о том, кому эта книга пригодится и как ее читать. И ответ на душещипательный вопрос про рекламу.

Об авторах

Не будем расплываться и размазывать заслуги и неудачи авторов на много строк. Скажем коротко, тезисно и по фактам. Оба автора имеют длительный опыт работы в правоохранительных органах. Причем не на должностях, предполагающих выполнение палочной системы, а в различных подразделениях с «творческим» характером работы. В их деятельность входили и процессуальные, и оперативные направления. Надзор, проверки, раскрытие и расследование преступлений всех видов и характеров. Опыт деятельности в органах сформировал понимание системности работы. Знания, полученные в масштабных федеральных компаниях, способствовали пониманию бизнес-процессов, корпоративной культуры и передовых технологий в крупных предприятиях. В общей сложности стаж работы в сфере безопасности и правоохранительной деятельности на двоих – более 30 лет. Сферы деятельности авторов «на гражданке» – крупные сельскохозяйственные холдинги, предприятия перерабатывающего цикла, торговые центры федерального уровня, аудит и ревизионная деятельность.

Круг общения авторов составляют специалисты и руководители в сфере безопасности по всей стране и ближнему зарубежью. Консультации при написании книги оказывали более 10 действующих сотрудников из разных сфер предпринимательства, в том числе сыроделия, животноводства, казино, аудита, ритейла, общепита, недвижимости, издательской и типографской деятельности, автомобильного бизнеса и других.

Нашими партнерами являются две компании международного уровня по экспертизе контрагентов, анализу конкурентов и всевозможным проверкам на «чистоту рук» и одна организация из сферы инноваций и GPS-навигации. Об этих партнерах мы расскажем в соответствующих главах, где и укажем их названия (все они вам, несомненно, известны).

Об авторах все. Впрочем, стоит еще сказать, что они не сторонники «палочной» системы работы и привыкли (чего и всем советуем) думать головой и не мыслить узко.

Кратко про системность в работе

Мы настаиваем, что безопасность на предприятиях должна быть системной и затрагивать все сферы деятельности. Но при этом «безопасность» не должна мешать работе и тормозить процессы. Она не вызывает негативные эмоции у сотрудников и не вставляет палки в колеса бизнесу. Безопасность обязана, как и все подразделения компании, существовать во благо прибыли и для нивелирования убытков. **Soft Power**, мягкая сила – вот наш стиль

работы. Эффект от деятельности СБ, по нашему мнению, должен быть **конкретизирован, подтвержден и измерим**. Мы не сторонники пустой болтовни и построения воздушных замков. Не теоретики, а практики. И именно поэтому считаем, что понятия «**экономический эффект**» и «**профилактический эффект**» – величины измеримые. Служба безопасности должна приносить осязаемый результат, а не просто «существовать» за деньги собственника.

Кому пригодится эта книга?

Руководителям крупных предприятий. Управляющим всех уровней, в том числе топ-менеджерам и директорам. Сотрудникам служб безопасности, ревизионных и аудиторских подразделений. Собственникам среднего и малого бизнеса, которые только планируют создать СБ или не могут наладить ее работу. Кризис-менеджерам, привыкшим решать проблемы здесь и сейчас. Сотрудникам всевозможных силовых структур, которые, листая материалы очередного уголовного дела, мечтают о жизни вне системы и ждут пенсии.

Как читать книгу?

Книга сделана и как пособие для практического применения, и как интересный материал для понимания реальных ситуаций.

Главы представляют собой тандем из двух разделов. В каждой главе есть невыдуманная история из жизни и тезисная формулировка с описанием функционала разбираемого материала. Например, в главе про служебные расследования первая часть представляет собой короткий рассказ из жизни менеджера, который обманул сам себя, а вторая – разбор структуры проведения служебных расследований.

В конце каждой главы вы найдете несколько чистых листов, они для заметок. Используйте для памяток и собственных комментариев.

Про рекламу в книге

Ее здесь нет. От слова совсем. Мы называем ряд известных организаций по проверке контрагентов, описываем свойства систем видеонаблюдения, плюсы и минусы различных баз данных. Разные компании мы называем «Партнерами», но ни одну из них не рекламируем. Мы подходим непредвзято и объективно. И наша задача – дать читателю понимание о плюсах и минусах работы разного программного обеспечения и оборудования. И да, мы сами пользовались всеми этими «системами», отсюда и мнение. Иногда это мнение будет восторженным, а иногда негативным. Зато оно объективно.

Чтобы быть окончательно честными

Вы всегда можете обратиться к авторам этой книги за советом и помощью. Совет может потребоваться тем, кто только собирается строить собственную СБ или сомневается в «чистоте рук» своих сотрудников. Помощь – предпринимателю, чей бизнес спикировал в кризис, и кризис этот связан с проблемами в безопасности.

Для остальных эта книжка – интересное прикладное пособие, на конец 2023 – начало 2024 года не имеющее аналогов в стране.

И последнее

Мы не составляли энциклопедию или учебник. Мы писали интересную (надемся) и полезную книгу на стыке жанров. В ней есть пробелы и недосказанности, она охватывает далеко не весь спектр направлений комплаенса и безопасности. Некоторые темы проработаны не очень глубоко, другие более досконально. Относитесь к чтению этого текста по-дружески, а мы всегда на связи – проконсультируем и подскажем, если что-то непонятно.



Схема взаимодействия СБ и бизнеса

P.S. Для нормального понимания и усваивания информации из книги необходимо минимальное знание законодательства и голова на плечах.

P.P.S. В книге присутствует много современных корпоративных терминов и аббревиатур (OSINT, KPI, NDA, DLP и т.д.) – лучше подтянуть «матчасть» перед прочтением, чтобы было понятно, о чем речь. В самом конце есть словарь современных корпоративных терминов (естественно, он не полный, но достаточный для работы СБ) с комментариями от авторов – обратите внимание.

Введение

Скорее всего вы прочитали аннотацию этой книжки. Помните упомянутую там брюнетку? Она реальна. И она вполне реально развалила компанию. Не потому, что она была промышленной шпионкой или сливала информацию конкурентам. Просто у нее маргарин в голове, а у ее руководителя нет времени разбираться в содержимом ее черепной коробки. Максимум, на что способен ее шеф – разбираться в других элементах ее тела.

Миловидная черноволосая девушка в кофейне в центре Москвы. Все атрибуты успешной секретарши при ней – сумочка от «Луи», яблочный смартфон, накачанные губы и хищный маникюр. Она постукивает ногтями по столику, листает меню и одновременно с ленцой, но нагло, смотрит на официанта. Официант, в свою очередь, смотрит на нее весьма дерзким взглядом, чтобы не сказать похотливо. Девушка дожидается подружку, и они в течение десяти минут обсуждают своих боссов. Хихикают, многозначительно закатывают глаза и расходятся. За эти несколько минут происходит два незначительных события, которые на первый взгляд ни при каких обстоятельствах не могут привести к краху организации.

Первое событие могло бы не случиться, если бы брюнетка была более воспитанна, но увы... В какой-то момент, поймав взгляд молодого официанта, она надменно спрашивает: «Чего уставился? Счет неси», – и не слишком понижая голос уже подруге: «Понабрали баранов...» (это в ней проснулось ее провинциальное прошлое).

И действительно, чего это он уставился на твое декольте? Скромнее нужно быть или соблюдать дресс-код. Официант, конечно, тоже неправ, но это уже совсем другая история. Важно то, что молодой парень почувствовал себя оскорбленным. Ему указали на «его место», да еще и такая красotka в самом центре столицы. Обидно.

И по-прежнему ничего страшного для босса и организации пока не наблюдается. Разве что в следующий раз брюнетке плюнут в кофе.

Но случается еще одна роковая случайность. Эта особо одаренная мадам, расплатившись, выронила из папки листик А4 и не заметила. Они с подружкой весело зашагали в сторону офисов. Листик медленно опустился на пол прямо под столиком и мог бы почить в утробе мусорного бака, но судьба распорядилась иначе...

Лист этот содержал самую малость конфиденциальной информации. Номер личного зарубежного счета директора организации. С упором на слове «личного». Не бог весть что за важные данные. Может быть, директору не стоило открывать счет в банке на Кипре, может быть, не стоило выводить туда часть прибыли, может быть, не стоило поручать своей секретарше сверить реквизиты и взять распечатку из банка. Но факт в том, что она уронила именно этот документ с реквизитами и это послужило точкой отсчета.

И до сих пор ничего проблемного не случилось. Ну, ксерокопия с данными человека, наименованием банка и несколькими цифрами. Подумаешь, проблема... Попади такой документ в руки 99,99% людей – они его выкинут в ближайшую урну. Но тут в игру вступает его величество случай. За соседним столиком сидит один из топ-менеджеров конкурентов, который пару раз бывал в офисе и видел брюнетку. И этот топ-менеджер знает, что его руководитель любит получать информацию о «противнике».

Но упавший листик по-прежнему покоится под столом, а лезть туда прилично одетый мужчина не собирается. По закону жанра, на сцене появляется оскорбленный официант, он ныряет под стол и извлекает документ.

Если бы десять минут назад брюнетка просто ответила на его взгляд улыбкой и не умничала, то парень банально дождался бы ее следующего прихода и торжественно вручил ей находку. Но увы, он оскорблен и зол. А тут еще и мужчина за соседним столиком (кото-

рый, между прочим, всегда оставляет чаевые), тянет руку с фразой: «Давайте я ей передам... И номерок для вас возьму, она не такая бяка, как кажется».

Официант расцветает и с улыбкой передает листок учтивому мужчине.

Конец истории. Топ-менеджер передал документ своему начальнику, тот другу из налоговой. В итоге в отношении директора брюнетки возбудили уголовное дело, организация обанкротилась, а брюнетка уехала жить в Волгоградскую область (шутка, куда делась брюнетка, никто не знает).

Конечно, опытный человек скажет – дело не в «косяке» брюнетки, дело в том, что не нужно баловаться с финансовыми операциями за рубежом. Но кто знает, сколько бы существовала фирма, если бы секретарша не допустила оплошность. Может быть, неделю, а может, и десять лет.

Этот пример не о том, что нужно хорошо скрывать свои «скользкие» моменты. Это аналогия того, что любая мелочь может привести к краху. Это заверение в том, что Москва не такой уж и большой город. Особенно пределы Садового кольца, где топы крупных холдингов обедают в одних и тех же заведениях. Это убеждение, что **большое количество негативных случайностей опасно.**



А зарабатывать деньги нужно исключительно честно и прозрачно, к чему мы и призываем.

У руководителя фигуристой брюнетки не было времени выстроить в компании систему конфиденциальности и безопасности.

У руководителей вообще бывает мало времени разбираться в чем-либо. Коммерческая и финансовая деятельность занимает большую часть рабочего дня. Операционные ежедневные проблемы оттягивают любые временные «окна», о них болит голова за завтраком, обедом и ужином.

Поэтому, не имея должной сформированной системы работы безопасности, из небольшой проблемы можно запросто вырастить слона. Этот слон сначала растопчет какую-то часть бизнеса, а потом и остальное.

Построить такую систему вам поможет эта книга.

Надеемся, мы не сильно затянули предисловия, введения и прочую полемику. Приступаем к реальным кейсам.

Глава 1.

Почему для каждого бизнеса нужна индивидуальная система безопасности. Категории рисков. Уровни рисков. Немного сказок

Многовато для одной главы? Нормально. Мы просто кристаллизируем информацию и отсекаем лишние мысли.

Завод по производству пельменей, региональный торгово-развлекательный центр, салон сотовой связи, сельскохозяйственный холдинг и казино – это разные предприятия по извлечению финансовой прибыли.

И строительство системы безопасности для них тоже будет разным. Потому что риски разные. Принципиально отличные друг от друга схемы хищений, откатов и всевозможных вариаций нанесения убытков компаниям. А также плюс-минус разные проблемы при не должном соблюдении пожарной и инженерной безопасности, охране труда, бухгалтерии, кадровой работе и взаимодействии с надзорными органами.

Система безопасности создается исходя из рисков – это одна из главных аксиом создания безубыточной среды.

Всегда изначально определяется круг возможных рисков и уточняется степень их значимости. Карту рисков и степени значимости мы приведем в конце главы, а пока продемонстрируем живые примеры из практики.

Какие «исключительные», т. е. наиболее обширные зоны рисков у вышеперечисленных организаций?

У пельменного завода – в основном проблемы непосредственно на линиях производств и в цехах. Поставки некачественного сырья, хищения, случайная порча продукции, несоблюдение ГОСТов и, как следствие, нарушение производственных процессов, влекущее потерю качества пельменей. Пример мелкого хищения на таком предприятии – это когда рабочий банально выносит кусок мяса с производства. Понятно, что обычно в «теме» задействован и мастер цеха, и охранник. Но ущерб от такого «риска» минимальный, если не закрывать глаза на очевидные вещи. Пример более масштабной проблемы на таком предприятии – руководитель коммерческого отдела за откат закупает некачественное сырье, например муку не того сорта. По документам, естественно, мука будет вполне себе нормальной. По факту – «разбодяженная» ерунда. В этом случае могут капитально просесть продажи, уйдут любители именно этой продукции. Просто муж скажет на кухне жене: *«Испохабились и эти пельмени. Раньше хоть „Октавиан Август“ были нормальные, а теперь дерьмо»*. Жена обсудит с подружкой, подружка со своей мамой, а на общем пикнике обменяются мнениями несколько семей. Потеря даже 10—15% постоянных покупателей будет значить финансовый кризис как минимум в полугодии, а то и за год. В динамике это повлечет невосполнимый объем потерь.

А теперь ответьте честно. Чем предпочтет заняться среднестатистический начальник СБ? Выявить страшную преступную группу, состоящую из рабочего, мастера и охранника, которые на троих украли 438 килограммов свинины за полгода и нанесли ущерб предприятию в 100 000 рублей? Следом гордо направить материал проверки в ближайший отдел полиции для возбуждения уголовного дела по ст. 158 УК РФ и доложить об успехе начальству. Или выстроить систему безопасности так, чтобы коммерческий отдел не имел возможности покупать сырье у своих знакомых по завышенным ценам? То-то же.

Кражи пресекать нужно, но лучше их профилактировать.

А какие самые очевидные риски у торгово-развлекательного центра?

Другие. Нет, конечно, сотрудники тоже воруют. Уборщица «Доместос», например, домой таскает в целлофановом пакете. И в закупках проблем масса – начальник эксплуатационной службы специальные перчатки для электриков у друга-ипэшника приобретает, а девочке-закупщице шоколадки дарит за закрытые глаза.

Но масштаб этих проблем в ТРЦ совсем иной, они незначительные. Максимальные риски в региональных ТРЦ – это когда директор за благодарность заводит на самые проходные и ценные места не международных мастодонтов бизнеса, а мелких предпринимателей. Которые не соблюдают требования пожарной безопасности, продают некачественный товар и расторгают договор спустя год. Директор разводит руками, пожимает плечами, а убытки несет собственник. И да, если у любителей продавать одежду и обувь на вес в огромных торговых залах что-то загорится, то в тюрьму в итоге сядут все. И директор, и собственник, и начальник СБ, и уборщица.

Головная боль и основные риски любого **сельскохозяйственного холдинга** – хищения десятков тонн зерна во время уборочной компании в полях. Сливы топлива. Списание годных запчастей. Закупки плохих удобрений. Проблемы с арендой земельных участков.

В салоне сотовой связи риски абсолютно другие – мошеннические схемы по гарантийным случаям с фиктивными поломками смартфонов, например. **В казино** – целенаправленное «опускание» финансовой прибыли, подставные клиенты, фальшивые подкупы должностных лиц (взятки давать нельзя ни в каком виде и никому, но находятся уникалы, которые якобы «решают» вопросы, а в итоге кладут деньги себе в карман).

Риски на каждом предприятии свои. Несмотря на их кажущуюся «одинаковость».

Определим категории рисков и их уровень.

Категории рисков:

1. Финансовые.

Это одна из самых нелюбимых сфер контроля для подразделений безопасности. Налоговая отчетность, инвестиции, основные средства, бухгалтерский учет, кредиты, движение наличных средств, закупки, тендеры, продажи, дебиторская задолженность, деинвестиционные активы.

Безопаснику предстоит вникать в бухгалтерский учет, учиться видеть финансовые потоки и согласовывать платежи между организациями.

Для собственника сфера отчетностей и финансов тоже своеобразный Рубикон, перейти который не всякому дано.

Отсюда и риски – опытный бухгалтер и финансист могут или быть хорошим подспорьем, или наоборот, манипулировать и директором, и предприятием. Гениальный руководитель управления закупок способен разорить компанию за сезон или принести хорошую прибыль и сократить расходы за тот же срок.

В этой сфере разбираться надо, нужно в нее вникать и контролировать. Как правильно и ненавязчиво нивелировать финансовые риски, мы рассмотрим в отдельной главе.

2. Кадровые.

Кадры – наше все. Непросто сейчас подобрать хорошего специалиста. Даже тракторист в 2023 году должен иметь высокую квалификацию – управлять голландским трактором за 50 млн нужно уметь. Специалист по пожарной безопасности обязан знать все виды огнетушителей и уметь составлять схемы зданий. Бухгалтер не может быть судим за мошенничество, присвоение или растрату. Директора желательно брать с опытом работы руководителем. И так далее, и так далее. У каждой должности своя специфика.

Как искать «чистых» сотрудников, если большая часть претендентов по уши в кредитах и долгах? Где взять не судимых рабочих? Как проверять кадры строго в рамках законного поля? Что такое NDA?

Категория кадровых рисков тоже полна «головняков» для руководства и службы безопасности. Аналогично, подробную информацию мы рассмотрим в отдельной главе.

3. Техничко-технологические.

Инженерные войска в деле. В эту сферу входит пожарная безопасность, экология, охрана труда. Кроме того, именно эта сфера одна из наиболее проблемных по документированию и выявлению краж. Зачастую инженерные подразделения очень «качественно» воруют запчасти, осуществляют фиктивные ремонты (почти как настоящие) и организуют стабильный слив ГСМ.

Как профилировать кражи запчастей, как не получить штраф за пожарную безопасность, как нивелировать риски при травмах на производстве, мы, естественно, расскажем в нескольких отдельных главах.

Пока просто помните – хороший эсбэшник разбирается во всем.

4. Периметр и охрана.

И тут некоторые бывалые сотрудники служб безопасности выдохнули. Наконец-то знакомая сфера. Но не думайте, что организация периметров, видеонаблюдение, подготовка графиков несения службы ЧОО и выявление мелких краж при выходе сотрудников с КПП это все.

Риски, связанные с несением службы охранниками, тоже являются составной частью глобальной сферы безопасности. Погрузимся мы в эту сферу ближе к концу книги.

5. Правовые.

В эти риски, по мнению авторов, стоит поместить договорную работу. Проверку контрагентов (хотя она и пересекается с другими сферами). Регламенты, должностные инструкции, взаимодействие с надзорными органами и прочие действия, связанные с организацией системы работы.

Будет несколько глав, отдельно охватывающих правовые риски во всем их многообразии.

Риски – наше все.

От банальных краж расходников, гаечных ключей и ручек до миллионных махинаций и офшоров. Риски являются альфой и омегой безопасности. Они проникают во все остальные сферы жизнедеятельности. Именно о пресечении рисков и минимизации убытков написана эта книжка. В каждой главе, будь то кадровая безопасность или организация охраны, мы упрямся именно в риски.

Данные **5 видов рисков** определяют первую часть карты рисков. Вторая ее сторона – **уровни рисков**. Их тоже всего 5.

Абсолютный – его никто не видел, но мы все о нем слышали. Это когда «придраться» в организации не к чему от слова «вообще». Когда инспектор МЧС приходит в торговый центр и плачет. Когда маржа +1000%. Когда за последние 10 лет на предприятии не было ни одной кражи. Такого не бывает. Даже у Илона Маска.

Стабильный — хорошая, рабочая обстановка в выбранной сфере. Есть свои небольшие проблемы, но они быстро решаются, в том числе благодаря качественно выстроенной системе безопасности.

Нестабильный — есть значимые проблемы, их можно решить, но для этого потребуется задействование времени и ресурсов.

Критический — проблемы усугубились, потому что кто-то забил на них или просто не обращал внимания. Их уже не решить простыми мерами. Причем решать критические проблемы нужно быстро. Скорее всего сегодня.

Кризисный – решать поздно. Нужно переделывать систему. Пример – сотрудники УЭБ и ПК изъяли все компьютеры и документацию, а директора арестовали по ст. 91 УПК РФ.

Или более лайтовый пример (но тоже кризисный) – поле с посевами уже сгорело. Вместе с двумя комбайнами. Слава богу, все живы, но комбайнов в КФХ было всего два. Можно уволить директора и ответственного за пожарную безопасность, но, поверьте, проблема не в этом. Проблема в организации системы работы.

Каждый сотрудник СБ или руководитель должен следовать аксиоме – **строить свою работу от рисков**. Поэтому, организовав с нуля службу безопасности, ревизионный отдел или аналогичное обособленное подразделение, лучше визуализировать проблемы. Например, как в нашей таблице – «карте рисков».

Таблица №1

		Виды рисков				
		Финансовые	Кадровые	Технико-технологические	Периметр и охрана	Правовые
Уровни рисков	Абсолютный	х				
	Стабильный			х		
	Нестабильный		х			
	Критический				х	
	Кризисный					х

Надеемся, всем понятно, что работу нужно начинать с тех проблем, которые находятся справа от центра таблицы – с нестабильными, критическими и кризисными рисками. Но так как человек – существо многозадачное, то не стоит забывать и о тех сферах, где уровень «нормальный». А то он быстро превратится в критический.



Сказка первая.

Надежный старый дуб

Монитор мигнул, и на экране появилось множество ячеек. Ежегодная видеоконференция по подведению итогов началась. Основной инвестор и создатель холдинга улыбнулся присутствующим. На фоне волевого лица за окном виднелся Биг-Бен. Мужчина не стал тратить время на вступительное слово и перешел к делу:

– Для начала заслушаем руководителя службы безопасности.

Одна из ячеек на экране никак не хотела оживать, на ней красовалась надпись «Камера отключена». Послышался тугий густой голос:

– Уважаемый Марк Борисович, коллеги...

Его сразу же перебила секретарша босса:

– Николай Иванович, у вас камера отключена.

Голос сбился с повествования и пробурчал:

– Да, секунду, извините. Никак не подружусь с техникой. У вас каждый раз конференции в разных мессенджерах.

Последнее слово он проговорил с нажимом.

Наконец ячейка моргнула, и в ней появилась массивная голова с седым ежиком волос, гладковыбритыми щеками и волевым подбородком. Мужчина продолжил:

– Службой безопасности ООО «Рога и копыта» за год выявлено 17 фактов хищения ГСМ, что на 3 факта выше аналогичного периода прошлого года. За данные хищения уволено четверо сотрудников (в прошлом году трое). Совместно с правоохранительными органами задержана группа лиц, осуществлявших хищение ТМЦ, возбуждено уголовное дело по ч. 2 ст. 158. Один из участников приговорен к реальному лишению свободы. 187 сотрудников наказаны за нарушение дисциплины. К участию в торгах не допущены 23 организации. В настоящий момент службой безопасности углублены, усилены методики...

Николай Иванович открыл массивную бархатную папку (в которой он, между прочим, еще документы на подпись к начальнику полиции в 2007 году носил), достал оттуда несколько листов и намерился зачитать предложение о введении штрафной сетки на предприятии. По его

замыслу, собственник должен был оценить старание и умение. Но собственник, видимо устав от цифр, задал вопрос:

– Николай Иванович, скажите, пожалуйста, сколько составил общий объем по этим 17 фактам краж ГСМ?

– Секундочку, – начальник СБ зарылся в бумаги, – всего 253 литра, товарищ... в смысле Марк Борисович.

– Хм-м, – собственник неопределенно кивнул, – а вот эта кража групповая, там что? Какие ТМЦ похитили?

– Один бензогенератор, три картриджа для принтеров и комплект рабочей формы одежды.

– Угу. А 23 организации, которые вы не допустили к торгам? Там были аффилированные с нашими топ-менеджерами коммерческие структуры из Европы?

– Эммм... Да нет. В основном мелкие ипэшники, местные паразиты, хотели залезть к нам в торги...

– Понятно, – собственник вздохнул, но не очень тяжело. – Николай Иванович, помните, в прошлом году я вам говорил, что необходимо увеличить показатель по экономии ГСМ?

– Так точно! – начальник СБ занервничал, – так вот же, Марк Борисович, плюс три факта, АППГ...

– Николай Иванович, я имел в виду в процентном соотношении по всему холдингу. Не 17 фактов на 253 литра. Нужно было построить систему профилактики хищений, добиться, например, – собственник заглянул к себе в блокнот, – как у наших конкурентов ООО «Доски и гвозди». Сокращение на 8% расхода ГСМ. Экономия налицо, 8% – это сколько? По нашим объемам вышло бы миллионов семьдесят... Да, Маргарита Петровна?

Строгая женщина в очках в одном из окошек видеоконференции кивнула:

– 73 миллиона 457 тысяч рублей.

– Вот видите, Николай Иванович, как работает служба безопасности у ООО «Доски и гвозди». Наверное, вам пора на пенсию.

Начальник СБ вскинулся, едва не опрокинув ноутбук:

– Да я, верой и правдой. Как преданный пес...

Вот и сказке конец.

Сказка вторая.

Молодой и перспективный

Сергея бодро шагал по длинному коридору в сторону кабинета начальника департамента безопасности и корпоративной защиты. За спиной дробно постукивали каблук блондинки из канцелярии. Сергей обернулся.

– Уфф, Маринка. Ты огонь!

Блондинка качнула бедрами в облегающей юбке и хохотнула. Одарив Сергея многозначительным взглядом, девушка скрылась за одной из дверей.

«Нужно будет вечером набрать, она вроде не замужем», – сверкнула мысль в голове Сереги.

Он ускорил шаг – не терпелось рассказать начальнику о своей победе сегодня. Парень был в восторге от новой работы. Должность звучала внушительно, зарплата была достойная, график ненапряжный.

Раньше он о таком мог только мечтать. Три года в патрульно-постовой службе, потом год в участковых, потом еще два года опером в уголовном розыске. Ни дня отдыха, ни дня без нервотрепки. То ли дело теперь – лови глуповатых колхозников на «хищах», да и уходи домой в 18.00. Сказка.

Он для порядка стукнул пару раз и толкнул дверь в кабинет начальника.

– Разрешите? – бодро спросил Серега.

– Заходи, Сергей, заходи.

Молодой мужчина, немногим старше Сереги, приподнялся из-за стола и протянул руку. «Сколько ему все-таки лет? Тридцать три, тридцать пять?» Серегу давно интересовал возраст начальника. Молодой мужик на такой должности. Да еще и, говорят, сам попал в кресло, без «толкача». Умный, наверное.

– У меня хорошие новости, шеф, – немного фамильярно произнес Серега, – показатель на неделю закрыт.

– Каким образом? – посмотрел в лицо Сереге мужчина.

– Получается...

– Да, и... – перебил его начальник, – забудь ты про эти показатели. Нет у нас такого понятия.

– Я по старой памяти, – ухмыльнулся Серега и продолжил. – Получается, еду я по трассе. Вижу, на нашем поле, ну, которое прямо за Новоалександровкой. Ну, соя на котором растет.

Начальник кивнул, он не нуждался в пояснениях, где и что у них растет.

– А там трактор наш «Нью Холланд» стоит, – продолжал Серега, – подхожу, значит. Водитель, урод, в кабине дрыхнет. А рядом, сечете, открытая бутылка пива.

Опять кивок.

– Он хоть и спит, но за рулем? Правильно? – продолжал весело вещать Серега. – Что это значит? Выпивший за рулем. Статья 12.8 Кодекса об административных правонарушениях. Ну, попал ты, друг, думаю.

Шеф наморщил лоб, а Серега продолжил:

– Я гайцов вызвал, оформили. Копию протокола привез. Вот и результат – сделали палку.

– Ты не подумал, что штраф теперь заплатит компания? Что трактористов и так нет, а сейчас в сезон вообще не найдешь? Вы идиот, Сергей?! – рассердился шеф. – Ты не «палку» сделал, а ущерб нанес. Дверь закрой с той стороны.

И этой сказке конец.

Понятно, что обе истории доведены до квинтэссенции идиотизма. Вряд ли есть настолько архаичный начальник СБ, как Николай Иванович, и настолько глупый сотрудник, как Серега. Но сказки наглядно показывают, как делать не надо. А как надо? А надо минимизировать убытки, не строить палочную систему работы и **действовать по принципу «не навреди», а не по принципу «заработай баллы».**

Думать, анализировать, планировать и выстраивать максимально прозрачную и работоспособную систему. Систему, которая будет экономить миллионы и профилировать проблемы.

Надеемся, никто из читателей не узнал себя в сказках.

Итог главы и применение на практике

Система безопасности в любой организации создается от рисков. Для понимания и визуализации проблем создайте карту рисков.

Категории рисков:

- финансовые;
- кадровые;
- технико-технологические;
- периметр и охрана;
- правовые.

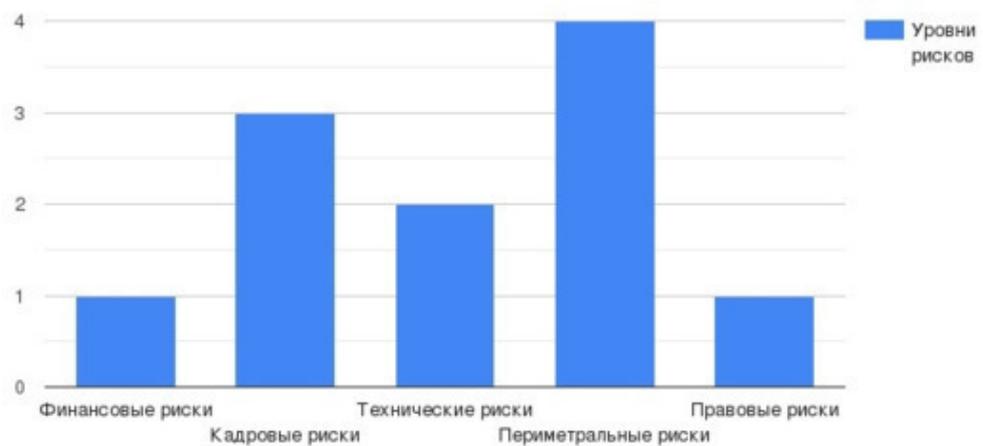
Уровни рисков:

- абсолютный;
- стабильный;

- нестабильный;
- критический;
- кризисный.

Не обязательно делать таблицу. Можно сделать диаграмму или вообще борд с наложением на карту предприятий. Для этого, правда, нужно совладать с программами для визуализации, но выглядеть будет наглядно.

В общем, любым удобным способом определяем и визуализируем риски, и шагаем дальше.



Для качественных и подробных заметок
Для качественных и подробных заметок

Глава 2. Основы построения безопасности. Конфиденциальность

В 2022 году к одному из авторов обратилась собственница консалтингового агентства из Объединенных Арабских Эмиратов (ОАЭ). Задача предстояла следующая – построить систему конфиденциальности в компании с нуля.

При первоначальном общении с заказчиком ничего сложного в вопросе создания такой системы автор не увидел. Банальный кейс для однополярной организации, хоть и с большим финансовым оборотом. По сути, в фирме всего несколько десятков сотрудников и один офис в Дубае. Не металлургический завод, и даже не сеть торговых точек регионального уровня. Просто консалтинговое агентство.

Сфера деятельности заказчицы – помощь в организации бизнеса на территории Эмиратов. Образно говоря, есть в одной из стран СНГ предприниматель, который хочет открыть филиал или вообще переехать в ОАЭ. Предприниматель этот, естественно, не имеет времени разбираться в тонкостях законодательства страны и не желает заниматься бумажной волокитой.

Консалтинговое агентство помогает ему собрать пакет документов для регистрации бизнеса на территории Эмиратов, открывает банковские счета, способствует в получении вида на жительство. В зависимости от заказа может подобрать недвижимость для аренды, сделать обзор рынка и выявить конкурентов. Клиенты агентства – собственники крупного и среднего бизнеса. Но в основном крупного. С оборотами от миллиарда рублей.



Естественно, коммерсанты и топ-менеджеры компаний такого уровня не любят публичности и распространения подробностей своей деятельности. Поэтому конфиденциальность в работе агентства необходима прежде всего.

Собственницей агентства в режиме короткой конференции в «зуме» была поставлена задача – создать такую систему конфиденциальности, которая полностью исключит утечку информации из компании. Рабочая встреча имела сжатый характер, женщина коротко и пылко (пока пила чашечку кофе перед рейсом в международном аэропорту Рима) обозначила лишь общее направление. Первоначально задача показалась совсем не сложной, планировалось создать **«Положение о конфиденциальной информации», штрафную сетку и ряд должностных инструкций**. Автор даже посоветовал клиентке обратиться к среднестатистическому кадровику. Но уже на следующей конференции оказалось, что все далеко не так банально.

Короткая ремарка от авторов. Она же одна из аксиом безопасности.

Конфиденциальность – это один из элементов системы безопасности.

На крупном предприятии конфиденциальность затрагивает все сферы деятельности. И кадровую политику, и финансовые операции, и механики производства, и сферу закупок, и ИТ. На законодательном уровне закреплён запрет на разглашение личных данных сотрудников, в уголовном праве существует понятие промышленного шпионажа. Любые крупные сделки обеспечиваются подписанием NDA (соглашение о неразглашении сути сделки между организациями).

В примере про консалтинговое агентство из ОАЭ важно то, что заказ был не на построение системы безопасности. Собственница хотела только полностью закрыть вопрос по конфиденциальности. Оно и понятно. Сокращать расходы в консалтинговом агентстве практически негде. Хищения отсутствуют как класс. Тендеров, закупок не проводится. Периметра, камер и прочих элементов физической охраны тоже нет. Из материальных ценностей – только обстановка офиса и минимум наличности в сейфе. Ценностью являлась исключительно **информация**.

*Сложно спорить (да и не нужно) о том, что **информация** сегодня одна из главных золотоносных жил бизнеса. Кто владеет информацией, тот владеет сделками, контрактами, громким брендом. И в итоге своим сегментом рынка.*

Когда задача по созданию системы конфиденциальности в ОАЭ развернулась во всей своей красе, автор тяжело вздохнул. Предстояла долгая и плодотворная работа.

Вместе с хозяйкой агентства **определили круг рисков. И в дальнейшем отталкивались от каждого риска индивидуально** (надеюсь, вы внимательно читали первую главу).

Как думаете, какие риски при оказании услуг консалтинга в Эмиратах для состоятельных бизнесменов?

Нет, это не шпионаж собственных сотрудников в пользу конкурентов. И не попытки сотрудниц завести роман с клиентами. Это безалаберность, длинные языки, глупость работников и расслабленность в коллективе.

Коллектив, в основном состоящий из молодых клерков, айтишников, незамужних женщин и бывших студентов, просто не мог сохранять в тайне подробности бизнеса своих клиентов. Почему и как собственница собрала именно такую команду – не наше дело. Думаем, глав-

ным преимуществом при рассмотрении кандидата было знание 2—3 языков на разговорном уровне. Но это не важно. Важно было создать систему конфиденциальности, исходя из имеющегося положения. А не воспитывать заказчицу и не указывать ей, кого брать, а кого не брать на работу. В коммерческой сфере лучше вообще никого не воспитывать. Это вам не правоохранительные органы.

Забегая вперед, скажем, что система для компании из ОАЭ удалась и работает и поныне. Далее речь пойдет именно про эту систему. Но авторы рекомендуют применять такую формацию для большинства организаций. Поэтому при построении элемента структуры безопасности и **конфиденциальности** вы можете взять ее.

Расширенная универсальная **«Система конфиденциальности»**.

Данный комплекс документов включает в себя два типа документов.

Первый тип – официальные положения и регламенты.

Сухие, юридически выверенные:

1. Положение о коммерческой информации (тайне).
2. Перечень сведений, составляющих коммерческую тайну.
3. Штрафная сетка.
4. NDA.

Первый тип документов, как видите, представляет собой стандартный набор, который должен быть в любой организации. Фундамент сохранения конфиденциальной информации. Данные документы подписываются каждым сотрудником вне зависимости от занимаемой должности.

О том, где их взять, мы скажем после краткого описания.

Положение о коммерческой тайне предполагает информацию о том, в соответствии с какими нормативно-правовыми актами разработано понятие конфиденциальности, понятие коммерческой тайны, ответственность за разглашение, порядок предоставления информации в государственные органы и так далее.

Это максимально «высушенный» документ, который хоть и хочет быть понятным для всех, но оставляет желать лучшего в ясности. Положение будет стандартным для большинства организаций.

Перечень сведений, составляющих коммерческую тайну, содержит широкий список сведений для конкретной организации.

Сокращенно может выглядеть так:

1. Сведения по вопросам управления, кадровым, штатным, правовым вопросам и вопросам региональной политики, сведения о клиентах организации в любой форме, сведения о партнерах организации в любой форме, сведения о контрагентах организации в любой форме.
2. Сведения об экономической, финансовой и бухгалтерской деятельности.
3. Сведения о коммерческой деятельности на внутреннем рынке.
4. Сведения по вопросам внешнеэкономической деятельности.
5. Сведения об ИТ-архитектуре организации.

Расширенная версия предполагает углубленное «расписывание» и обоснование каждого пункта.

В принципе, этот список может быть внесен в **«Положение о коммерческой тайне»**, но мы рекомендуем утвердить отдельный документ. Не ради бюрократии, а для практического

применения и донесения до сотрудников. Поверьте, его все равно придется в виде выписки «извлекать» из Положения. Ведь сотрудникам так нагляднее.

Штрафная сетка

Напомним, мы сейчас ведем разговор о конфиденциальности. Решать, какие наказания применять к сотрудникам за разглашение конфиденциальной информации, вам предстоит совместно с HR или с кадровой службой. В этом случае мы предлагаем не плодить бюрократию, а объединить все виды наказаний в одной таблице. И за разглашение конфиденциальных сведений, и за опоздание на работу, и за прочие проступки.

Штрафная сетка имеет простой табличный вариант, утвержденный руководителем предприятия.

Вообще разговор о штрафах – это отдельный геморрой. Фактически законодательство и так предполагает ответственность сотрудников за разглашение коммерческой тайны и сопутствующие правонарушения (ст. 183 Уголовного Кодекса РФ). Трудовой Кодекс регламентирует и опоздания, и прогулы, и прочие нарушения трудовой дисциплины. Наказания за кражи, коммерческие подкупы и мошенничества, естественно, предусмотрены УК РФ.

Штрафная сетка реально выполняет две функции – **профилактическую** и **наказания за мелкие нарушения**. С профилактикой все понятно (надеемся). С наказаниями за мелкие нарушения тоже более-менее понятно – нарушение формы одежды на производстве, грубость по отношению к клиенту в ритейле и прочие неприятные истории.

В любом случае приходится возвращаться к взаимодействию с кадровой службой. Штрафы в коммерческих организациях не назначаются просто так. Нельзя лишить человека премии на пустом месте. Любой штраф – это первоначально служебная проверка, объяснение, приказ. И только потом лишение части денег. И даже при этом все не так легко. Надеемся, ни для кого не новость, но штраф может взиматься только с премии. Либо от ежемесячной ее части, либо от годовой. Только KPI (ключевой показатель эффективности, или попросту говоря премия) является базой для уменьшения, а не окладная часть зарплаты.

Повторим третий раз – штрафные сетки создаются и вводятся в действие совместно с кадрами.

Впрочем, ваша задача сделать так, чтобы конфиденциальные сведения не ушли на сторону. И не были разглашены по случайности. А штрафы – крайняя и непопулярная мера.

NDA

Еще одна (наряду с KPI) относительно новая аббревиатура. Non-disclosure agreement – соглашение о неразглашении. Заключается между двумя организациями, когда сведения о коммерческой (или любой другой) деятельности становятся известны контрагенту. Например, вы вызываете специалиста для настройки «1С: Егр». В процессе работы специалист видит ваши финансовые показатели или поданную заявку на патент. Чтобы у временно нанятого сотрудника не возник соблазн проинформировать ваших конкурентов – необходимо заключить NDA.

Соглашение о неразглашении в 95% случаев типовое. Составляет его юрист, подписывает руководитель организации и контрагент.

Думаем, некоторые читатели уже задались вопросом – где взять образцы документов. Отвечаем – в конце книги вы найдете контакты авторов. Обратитесь к нам, и мы скинем вам на почту типовые версии Положения, Перечня, Штрафной сетки и NDA. Просто предложите нам свою дружбу. Шутим, отправим полностью безвозмездно. Дабы вы не искали ерунду в интернете.

Переходим ко **второму типу документов**, которые необходимы для корректной работы системы конфиденциальности. Их мы вам не предоставим. Для каждой организации такие документы индивидуальны, они верстаются с нуля. Можете обратиться к профессиональному специалисту, который вам их создаст. Либо попробуйте сделать сами. Да, и мы скажем правду, – второй пакет не обязателен, но лучше его сделать.

Политика конфиденциальности – глобальный документ в виде системы, которая объясняет сотрудникам всех уровней для чего нужна конфиденциальность. В отличие от **Положения**, составляется понятным языком с обращением к читателю. Тезисная простота и понятность соседствует со смешными примерами. В **Политике** руководство, обращаясь напрямую к сотруднику, рассказывает о компании, об общих целях по достижению прибыли. Максимально заботливо и ясно.

Если вы работали в крупных компаниях, то знаете, что у любой крупной сети продуктовых или строительных супермаркетов есть мотивационная система для сотрудников. Эдакий комплекс документов, написанный простым языком, – про историю компании, про устремления, про общие цели, поддержку друг друга. В этих же проспектах содержится и ненавязчивая информация о том, что в фирме не приветствуется. **Политика конфиденциальности** построена по такому же принципу – объяснить сотруднику, что и для чего.

Например, Политика для консалтинга из ОАЭ начинается со слов:

«Когда мы разговариваем с родителями по телефону – стараемся контролировать, что говорим. Не говорим о проблемах и кредитах, боимся „сболтнуть лишнее“. Общаясь со своими детьми – выбираем слова, думаем, прежде чем сказать. Дома не оставляем острые предметы в ящике с игрушками. Мы контролируем речь и действия в личной жизни, а когда контроль ослабевает – пожинаем негативные плоды. Обсуждая жизнь друзей и подруг, мы знаем, что они так же сплетничают о нас. Нам это неприятно. Это простые истины, правила „чистых рук“, их знают все».

В тексте даже есть пословица – про слово и воробья.

Понятно, что конкретно эта политика подстроена под среднестатистического сотрудника того агентства. Ориентирована на возраст, сферу общения и образ жизни. При создании аналогичного документа всегда необходимо учитывать, кто будет читать текст – среднестатистический менеджер, вчерашние студенты или сегодняшние эмигранты. Каждому свое.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.