**Сотрудники воруют**

Оглавление

[Как защитить ваш бизнес от коррупции 1](#_Toc16247650)

[В российских компаниях чаще всего воруют топ-менеджеры 5](#_Toc16247651)

[Почему в компаниях с жестким управлением больше воруют 7](#_Toc16247652)

[Как бороться с воровством на предприятии 9](#_Toc16247653)

[Сотрудники иногда мухлюют, получив оплату от клиентов 12](#_Toc16247654)

[Законно ли видеонаблюдение на рабочем месте? 14](#_Toc16247655)

[Кто из сотрудников и соискателей лжет 16](#_Toc16247656)

[Начинаем слежку: контроль за Интернетом, видеонаблюдение. 22](#_Toc16247657)

[Новый руководитель IT-отдела будет иметь доступ к важной информации. 28](#_Toc16247658)

[Никак не избавиться от воровства 29](#_Toc16247659)

[Сотрудники всегда крадут 32](#_Toc16247660)

[Ваши сотрудники крадут? 34](#_Toc16247661)

[Воровство – как избавиться 36](#_Toc16247662)

[Как правильно ввести систему видеонаблюдения в организации? 38](#_Toc16247663)

[60% российских компаний ловят увольняемых сотрудников на краже информации. Как не попасть в их число? 40](#_Toc16247664)

[Что делать, чтобы сотрудники не воровали 43](#_Toc16247665)

[Как спасти клиентскую базу от кражи со стороны сотрудников 45](#_Toc16247666)

[Почему воюют учредители и их «генералы» 47](#_Toc16247667)

[**Вернуться в каталог сборников по управлению персоналом**](http://учебники.информ2000.рф/personal2/personal3.shtml)

[**НАПИСАНИЕ на ЗАКАЗ: дипломы и диссертации, курсовые и рефераты. Переводы с языков, он-лайн-консультации. Все отрасли знаний**](http://учебники.информ2000.рф/napisat-diplom.shtml)

# Как защитить ваш бизнес от коррупции

Андрей Айвазов 07 декабря 2017

Контроль за коррупционными нарушениями в бизнесе в последнее время существенно ужесточился. Появляются новые требования по борьбе с отмыванием денег и финансированием терроризма, вводятся международные стандарты контроля за финансовыми потоками, требования к профилактике коррупции в компаниях. При этом антикоррупционный комплаенс, то есть система контроля за соответствием действий компании антикоррупционным нормам — пожалуй, одна из самых сложных для выстраивания. Чтобы эффективно защитить себя от рисков, бизнесу стоит учитывать ряд важных моментов.

**1. Комплаенс — это не только документы.** К числу классических заблуждений относится приравнивание комплаенс-процессов к формальным требованиям о совершении определенных действий, предусмотренных локальными нормативными актами компании. Комплаенс представляет собой более комплексный инструмент. Даже если вы сможете построить «отдаленную» от коммерции систему комплаенса и сделать ее эффективной, что крайне сложно, такой контроль будет тормозить и затруднять работу. Не стоит забывать, что противодействие коррупции не должно становиться самоцелью: ключевая задача комплаенса — обеспечивать бесперебойное и безопасное участие компании в коммерческих проектах.

В своей практике я неоднократно видел примеры, когда компании принимали десятки антикоррупционных документов, однако нарушений меньше не становилось. Лишь при комплексном подходе к комплаенсу, учитывающем как нормативную, так и организационную, психологическую, управленческую, кадровую часть, удается создать эффективный механизм предотвращения коррупции.

**2. Задумайтесь об уровне интеграции в бизнес-процессы.** Антикоррупционный комплаенс, как и многие другие поддерживающие функции (например, стратегическое планирование или HR), можно делить на «поколения» развития. Каждый такой этап предусматривает определенный набор выполняемых функций, и чем более продвинутое «поколение» антикоррупционного комплаенса внедряет компания, тем выше требования к временным, человеческим и финансовым ресурсам. Принято выделять **три поколения** антикоррупционного комплаенса. В первом поколении устанавливается лишь ряд ключевых процедур, общеобязательных требований. Во втором поколении существуют регламентированные бизнес-процессы для каждой зоны риска, однако нет «единого механизма» работы. В третьем — антикоррупционная политика интегрируется в ценности и каждый элемент бизнес-процессов.

У военных есть понятие overkill, чрезмерная огневая мощь, которая не требуется в таком объеме для уничтожения противника. Можно использовать эту аналогию и для комплаенса: бизнесу с понятными зонами риска не нужно разрабатывать сверхсложную систему противодействия коррупции по всем направлениям работы. Позаботьтесь о нормативных документах, базовом обучении всех сотрудников, а затем переместите фокус на зоны риска – это могут быть закупки, финансы, GR или иные области в зависимости от направления бизнеса.

Одна российская торговая компания решила после ряда коррупционных случаев внедрить крайне жесткий контроль в сфере платежной дисциплины. Специальную антикоррупционную процедуру проходил любой платеж компании за ее пределы на сумму более 1000 рублей, а сама процедура занимала не менее дня. Так как компании по роду деятельности требовалось платить много и часто, новый инструмент стал тормозить бизнес-процессы. Но во время антикоррупционного аудита выяснилось, что все случаи коррупции произошли в одной зоне риска — валютных закупках у поставщиков из нескольких стран, которая была эффективно зарегулирована, а с остальных платежей после проведения обучения сотрудников столь значительные ограничения были сняты.

**3. Помните, что комплаенс — всегда часть корпоративной системы ценностей.** Тому, кто регулярно сталкивается с правовыми системами разных государств, нетрудно заметить весьма интересную тенденцию. Зачастую в странах с невысоким уровнем коррупции о ней почти не говорят. А в договорах с контрагентами из юрисдикций, где коррупция процветает, содержатся пятистраничные антикоррупционные оговорки. Поэтому ключевым моментом является не регламентация, а правильная система корпоративных ценностей.

Практика показывает, что жесткие санкции сами по себе абсолютно недостаточны для предотвращения нарушений. Неоднократно различные страны для борьбы с преступностью значительно усиливали ответственность, но нужного эффекта такие меры не приносили. Если сотрудник совершает коррупционное преступление, за которое грозит уголовная ответственность, испугает ли его «увольнение с позором» из компании?

Необходимо сделать принцип нулевой толерантности к коррупции безусловной частью корпоративных ценностей и поддерживать его на всех уровнях, демонстрируя, что компания внедряет антикоррупционный комплаенс не потому, что «надо» или «рынок диктует», а потому что руководство принципиально против любых проявлений коррупции, потому что коррупция вредит бизнесу и потому что его рост через коррупционные действия в долгосрочной перспективе невозможен.

**4. Выявите зоны риска.** Важно сформировать понимание, в каких областях деятельности и в каких бизнес-процессах появляется наибольший риск возникновения коррупции. Особенно следует обращать внимание на возможность проявления «некорыстной» коррупции, когда сотрудник решает помочь своей фирме не совсем честными методами. Именно этот вид коррупционных правонарушений несет наибольшую угрозу компании и ее руководству, так как следователи в случае выявления преступления будут иметь основания полагать, что организация в этом замешана. Кроме того, в отличие от «корыстной» коррупции, «некорыстную» действительно возможно свести практически к нулю.

Классическими зонами риска являются получение разрешений и государственное оформление, закупки и продажи, финансовые операции и вообще все те подразделения, от работы которых напрямую зависит текущая коммерческая деятельность и, как следствие, прибыль компании. К сожалению, на практике общими представлениями о зонах риска обойтись не получится: данный вопрос крайне специфичен и привязан к конкретным бизнес-процессам. Выявление «опасных зон» — одно из самых сложных и комплексных действий при проведении антикоррупционного аудита и определении стратегии противодействия коррупции в бизнесе.

Сложно выявить риск там, где бизнес-процессы не являются до конца прозрачными или скрыты от большинства сотрудников. Например, для компании с большим количеством иностранных поставщиков зоной риска будет процесс их отбора, способы оплаты и условия контракта. Грамотный комплаенс призван урегулировать «опасные» зоны, не затрудняя работу соответствующим сотрудникам.

**5. Назначьте ответственных.** Линейные руководители хорошо знают свою работу и своих подчиненных, однако им зачастую не хватает видения, присущего топ-менеджерам. Из их числа и следует выбирать ответственных за антикоррупционный комплаенс. Вне зависимости от типа корпоративной культуры лучше всего функцию руководства антикоррупционным комплаенсом выполняют люди с «демократическим» складом ума и хорошими навыками влияния на коллег. Не ставьте во главу антикоррупционного комплаенса жестких лидеров военного типа: задача ответственных — мягкими способами донести ценности до нужных людей, а не вести их за собой на войну с коррупцией.

**6. Определитесь, что делать в кризисной ситуации.** Инструментов, которые гарантировали бы абсолютную безопасность и полное отсутствие рисков, не существует. Даже в компаниях с эффективными антикоррупционными механизмами коррупционное событие все равно рано или поздно может произойти. Комплаенс обязательно должен включать в себя подробный план реагирования с понятными мерами для решения проблемы. То, как вы будете действовать в кризисной ситуации, во многом определит и истинную ценность разработанного вами антикоррупционного комплаенса.

Екатерина Великая дала нам оставшийся в веках совет для руководства: «Хвалите громко, обвиняйте тихо». В случае с антикоррупционным комплаенсом ему стоит следовать только если речь идет о высших руководителях, и нет еще больших рисков репутации компании, а их при грамотно выстроенном антикоррупционном комплаенсе не должно возникнуть.Если риски все же существуют, я советую позаботиться в первую очередь о репутации, а затем оперативно модернизировать комплаенс-систему. При этом до полного подтверждения совершения правонарушения все расследования следует вести конфиденциально во избежание ущерба репутации компании и из уважения к собственным коллегам. При выявлении факта коррупции со стороны сотрудников о нем уже имеет смысл сообщать открыто.

Кризисные ситуации, конечно, бывают совершенно непредсказуемые. Вот пример: представитель поставщика звонит сотруднику компании, предлагая встретиться в его машине и «обсудить более эффективные возможности взаимодействия». Сотрудник, не задумываясь, принимает предложение. В машине представитель поставщика передает ему пакет. Сотрудник, не открывая пакет, выходит из машины. Через несколько минут, «почуяв неладное», он выбрасывает полученный пакет в пруд и звонит в полицию, сообщая, что представитель поставщика угрожал ему. Однако о произошедшем руководству компании сотрудник сообщает лишь на следующий день, предварительно проинформировав около десятка коллег об инциденте.

Стоит ли говорить, что топ-менеджменту пришлось приложить немало усилий, чтобы решить возникшие сложности с государственными органами и внутри компании? После этого инцидента, кстати, компания решила значительно модернизировать комплаенс-систему и провести дополнительное обучение персонала.

**7. Периодически тестируйте уровень восприятия коррупции.** Эффективность антикоррупционного комплаенсабазируется на уровне знаний ваших сотрудников. Большинство нарушений случаются в сложных ситуациях, когда более опытный контрагент, партнер или коллега провоцируют коррупцию, а молодой специалист в силу отсутствия как необходимых знаний, так и в силу низкой степени понимания сущности и угроз коррупции участвует в действиях, которые не совершил бы осознанно.

Уровень восприятия коррупции — это совокупность знаний об этом предмете, понимание того, как выражается коррупция в конкретных бизнес-процессах, как ее выявлять и предотвращать. Сотрудник может идеально знать регламенты комплаенса, но он не сообщит об угрозе коррупции, если не будет ее даже подозревать.

Методик оценки уровня восприятия коррупции много (как правило, они все включают оценку понимания коррупции, знания способов ее обнаружения, понимания наиболее рискованных проявлений коррупции), однако компании следует разработать свою, учитывающую ее ключевое направление работы. Желательно, чтобы в этом участвовал человек, ранее проводивший антикоррупционный аудит или же имеющий глубокие знания в вопросах противодействия коррупции в бизнесе.

Делая вывод из вышесказанного, отмечу, что в первую очередь при внедрении комплаенс-процессов необходимо учитывать особенности компании. «Абстрактный» комплаенс не работает: его просто не будут учитывать рядовые сотрудники, невзирая на потенциальную ответственность. Важным и сложным этапом будет выявление зон риска – тех направлений работы, где вероятность коррупционного правонарушения наиболее велика. Но без этого правовая безопасность бизнеса всегда будет под угрозой.

**Об авторе.** **Андрей Айвазов** —руководитель направления международного права компании «Альянс Консалтинг».

# В российских компаниях чаще всего воруют топ-менеджеры

Оксана Гончарова / «Ведомости»

Исполнительные директора и члены советов директоров российских компаний воруют более чем в половине случаев (56%), а функциональные менеджеры на втором месте по корпоративным злоупотреблениям (24% случаев), показало недавнее исследование аудиторской компании KPMG. Авторы опросили специалистов из различных подразделений KPMG, занимающихся расследованиями экономических злоупотреблений сотрудников. Исследование охватило 85 стран мира, включая Россию, Украину, Казахстан и Азербайджан. Как пишут авторы опроса, за рубежом топ-менеджеры и функциональные менеджеры воруют примерно одинаково (31 и 32% случаев соответственно).

Чаще всего корпоративные злоумышленники присваивают доходы и активы компании (46%), искажают финансовую отчетность (11%) и получают взятки от поставщиков и подрядчиков (11%). Каждая четвертая отечественная компания за последние два года потеряла из-за злоупотреблений более $1 млн, говорит партнер практики расследований мошенничеств PwC в России Инна Фокина. По данным KPMG, в 71% случаев мошенничеству способствует слабость внутреннего контроля в российских компаниях. За рубежом этот показатель ниже – 60%. Сотрудники любого уровня признают в опросах, что участвуют в хищениях, потому что у них просто есть такая возможность, поясняет руководитель отдела расследований KPMG в России и СНГ Иван Тягун. Но российские работодатели в отличие от их коллег за рубежом не спешат подавать в суд на вороватых сотрудников. Больше половины компаний предпочитают их увольнять без шума, а каждый шестой работодатель (15%), узнав о мошенничестве, вообще ничего не делает, рассказывает Фокина.

**Директора**

По данным KPMG, типичными мошенниками являются мужчины в возрасте от 36 до 45 лет, имеющие высшее образование и проработавшие на руководящей позиции более шести лет. Высокая должность, доверие со стороны работодателя и многолетний опыт работы позволяют им обходить контрольные процедуры и долгое время оставаться нераскрытыми.

Основатель консалтинговой компании PrECA Зелимхан Сулейманов говорит, что директора иногда мошенничают столь грубо, что не заметить этого может только слепой, особенно если речь идет о правлении региональных «дочек». Так, технический директор завода сам выбирал поставщиков и закупал дорогостоящее оборудование, но предприятие никаких документов, кроме накладных и счетов-фактур, не получало. Директор по дешевке закупал старое оборудование и велел его перекрашивать, чтобы оно выглядело как новое. Сумма за якобы новые станки делилась между поставщиком, техническим директором и сотрудниками технической поддержки, обслуживавшими оборудование. Технический директор за пять лет успел купить две квартиры в Москве. А разоблачил его откомандированный из штаб-квартиры руководитель проекта, который случайно заметил под свежей краской «недавно купленные» ржавые насосы. Проворовавшегося директора уволили, но он сейчас трудится на другом предприятии, рассказывает эксперт.

**Снабженцы**

Лидерами по числу злоупотреблений являются отделы закупок (22% случаев), отделы финансов и бухгалтерия (20%), а также служба сбыта (14%), говорится в исследовании KPMG. Тем не менее во многих компаниях в этих отделах отсутствуют даже базовые процедуры контроля – разделение полномочий, документально оформленные правила закупок, контроль за инвестициями, говорит Тягун. Сулейманов 12 лет руководил различными проектами по оптимизации закупок – в X5 Retail Group, Inventive Retail Group, Knauf Insulation, Moet Hennessy и др. Очень распространены простые схемы, которые нетрудно обнаружить, рассказывает он. Например, организатор закупок (начальник отдела снабжения или профильного подразделения) договаривается с одним или несколькими доверенными поставщиками (или даже сам создает подставных поставщиков). Он договаривается с ними о своем вознаграждении, а затем начинает закупать товары по завышенным ценам или манипулирует условиями тендеров так, чтобы выиграть смог только доверенный поставщик.

**IT-отделы**

Некоторые компании закладывают в смету проектов на закупку сложных IT-систем ненужные расходы: на построение команды, укрепление корпоративной культуры и пиар проекта. В практике Сулейманова был случай, когда крупный производитель потребительских товаров по просьбе IT-директора заложил в бюджет на внедрение IT-системы 270 млн руб., из них 20 млн руб. – на формирование проектной команды. «Нам удалось убедить работодателя, что 20 млн руб. – это слишком много для мероприятий по сплочению коллектива», – рассказывает он.

**Профилактика**

Шесть лет назад Сбербанк публично вывешивал списки сотрудников, уволенных в связи с утратой доверия (ст. 81 п. 7 Трудового кодекса), но потом списки публиковать перестал. Пресс-служба Сбербанка пояснила, что сейчас акцент делается на профилактике и предотвращении преступлений, а не на публичном порицании виновных. За последние годы банк разработал много предупредительных мер, например специальных математических алгоритмов, выявляющих признаки корпоративных хищений, утвердил политику проведения служебных расследований и составил перечень должностей, занимая которые сотрудники могут быть уволены в связи с утратой доверия. Последняя мера касается не только работников, которые несут материальную ответственность, но и тех, кто имеет доступ к клиентским счетам и совершает операции с электронными деньгами, рассказали представители банка.

Между тем в банках придумано много схем злоупотреблений. Например, кредитные специалисты берут откаты с заемщиков, которые не подходят банку, – с людей с плохой кредитной историей, предприятий без залогового обеспечения, а также мошенников, которые вовсе не намерены возвращать ссуды. Отдельная категория мошенников – специалисты по залогам. Эти сотрудники при оформлении кредита за откат могут завысить стоимость залогового имущества, увеличив таким образом сумму займа. А в случае невозврата кредита – продать залог по заниженной цене, получив с дружественного покупателя процент за выгодную сделку. Попадаются такие сотрудники, как правило, на контрольных закупках, говорит Руслан Шатохин, бывший управляющий директор крупного банка.

**Тест на порядочность**

Работодатели с особой бдительностью должны относиться к кандидатам на позиции топ-менеджеров, закупщиков, специалистов по продажам, руководителей географически отдаленных филиалов, замечает Тягун. Как рассказывает основатель кадрового агентства Rabotarestoran Нина Макогон, показательна частота смены мест работы кандидатом. Если менеджер нигде не задерживается больше года, это тревожный сигнал, за которым должно последовать дополнительное наведение справок.

В некоторых компаниях используются довольно жесткие методы профилактики злоупотреблений, например проверка на полиграфе. К примеру, «Северсталь» применяет полиграф на протяжении 12 лет. Как следует из презентации компании, все сотрудники Череповецкого меткомбината – от рабочих до топ-менеджеров – проходят проверку на полиграфе один раз в 1,5–2 года. Зато есть результат: в 2014 г., согласно презентации, через детектор лжи прошло 45 сотрудников, занимающихся закупками одного из видов сырья на Череповецком меткомбинате. В 2013 г. в коррупционную деятельность было вовлечено 75% закупщиков, а в 2014 г. – лишь 22% благодаря комплексному проекту по борьбе с хищениями персонала в «Северстали», говорится в презентации компании.

# Почему в компаниях с жестким управлением больше воруют

[Андрей Айвазов Руководитель, Москва](https://www.e-xecutive.ru/users/1757050-andrei-aivazov)

Пять проблем, которые губят антикоррупционный комплаенс – борьбу с коррупцией в российском бизнесе.

Комплаенс за последние годы стал очень популярным инструментом, призванным как укрепить безопасность бизнеса, так и повысить его статус на рынке. Однако, принимая локальные акты и регламентируя процессы, компании часто забывают, что, во-первых, все процессы должны быть грамотно интегрированы и взаимосвязаны. А, во-вторых, комплаенс – это гораздо более сложный механизм, нежели совокупность инструментов.

Так что же губит антикоррупционный комплаенс в российских компаниях?

**1. Нет эффективной коммуникации между людьми различного уровня**

Важный [вопрос противодействия коррупции в бизнесе](https://www.e-xecutive.ru/management/practices/1970744-kak-vympelkom-protivostoit-korruptsii-vnutri-kompanii-i-za-ee-predelami) – наличие взаимопонимания между сотрудниками разного уровня. Во внимание следует принимать не столько иерархию должностей, сколько личностный уровень сотрудников. Два этих статуса часто, но не всегда совпадают.

Классическая проблема, с которой сталкивается компания на уровне второго поколения антикоррупционного комплаенса – это различное понимание задач по противодействию коррупции, его целей и своей роли в соответствующих процессах в зависимости от уровня сотрудников. Эту проблему нужно решать, постоянно налаживая контакт между людьми. Подход «это правильно, потому что так сказали топы» на определенном уровне развития комплаенса просто перестает работать.

**2. Нет простого ответа на вопрос, почему коррупция – это плохо**

Цитата из общения с комплаенс-офицером крупной российской торговой компании: «Это же очевидный вопрос! Даже ребенок это знает! Коррупция недопустима, поскольку…» Дальше последовали тридцать секунд молчания. Отмечу: автор цитаты – один из лучших специалистов в области комплаенса, которых я знаю.

Это ярко свидетельствует о том, что дать точный ответ, почему коррупция – это плохо, весьма сложно, если опустить такие общие понятия, как «незаконно» и «аморально».

Для одних сотрудников коррупция плоха, потому что снижает эффективность компании в целом и мешает работе бизнеса. Для других – потому что подрывает доверие и мешает командной работе. Объяснений бесчисленное множество, как и вариантов поведения, вытекающих из понимания негативной составляющей коррупции. Грамотная система комплаенса должна быть готова обработать и переварить их все.

**3. Нет оценки уровня восприятия коррупции**

Не зная, насколько сотрудники понимают негативные последствия коррупции и как оценивают коррупционные риски, нельзя определить, какие инструменты fine tuning будут оправдывать ресурсы на их создание и функционирование.

На уровне зрелого второго поколения комплаенса и выше компания не сможет найти мгновенные меры, которые окажут значительное влияние на работу комплаенс-системы. Как следствие, требуется глубокая и специализированная отладка деталей и использование out-of-the-box-методов. Столь тонкая хирургия невозможна без всестороннего понимания, где прокалывается мидл- и линейный менеджмент, как будут действовать работники в различных обстоятельствах, в каких ситуациях коррупция представляется им наиболее опасной и почему.

**4. Нет разделения корыстной и некорыстной коррупции**

Корыстная коррупция была, есть и в обозримом будущем будет везде. Стремление нанимать на работу только честных и бескорыстных людей бессмысленно: сделать это просто невозможно. Лично я не знаю рабочих примеров такой кадровой системы, которая позволяла бы отбирать «идеальных граждан».

Путь к неприятию коррупции сотрудниками лежит не через этические обоснования, а через невыгодность ее для человека: риск должен быть выше преимуществ, которые может дать коррупция.

На Западе коррупция невысока в первую очередь по той причине, что у людей есть понятные перспективы на будущее и определенная стабильность, которой большинство не хочет жертвовать ради кратковременной выгоды. Человек, привыкая к оценивающему риск- мышлению, со временем начинает отрицательно относиться к коррупции в целом, поскольку понимает, что во всех своих проявлениях она угрожает будущему общества, способного обеспечить высокий уровень жизни, и подрывает те демократические ценности, на которых основывается социально ответственное государство.

Если корыстную коррупцию комплаенс полностью победить не в состоянии, то с некорыстной правильно выстроенная система может справиться полностью. Негативные исключения следует рассматривать оперативно и в соответствии с законом и внутренними процессами, чтобы не подрывать доверие к комплаенс-системе. Необходимо дать понять сотрудникам, что даже если их «коррупционная авантюра» в пользу компании увенчается успехом, компания примет все меры, чтобы наказать нарушителя.

**5. Чрезмерно жесткое управление**

В продолжение тезисов о причинах коррупции я бы хотел привести контрпример: в странах с жестким политическим режимом коррупция практически всегда очень высока, и история показывает, что уровень взяточничества в таких государствах [не зависит от уровня развития страны](https://www.e-xecutive.ru/management/practices/1820116-pobedit-korruptsiu-kak-eto-bylo-v-gonkonge-i-singapure). Аналогичная ситуация наблюдается и в компаниях, внедряющих антикоррупционный комплаенс: система, управляемая слишком жестко, просто разваливается изнутри.

Драконовское управление применимо в том случае, если необходимо добиться краткосрочных результатов имеющимися средствами. Комплаенс же ни в коем случае не может быть временной задачей, он должен формировать уважение к антикоррупционным ценностям, а не страх перед проверкой.

Диктаторский вариант не только дает обратный эффект в части антикоррупционного регулирования, но и лишает комплаенс-службу ее основной функции – советника, которому доверяют. Именно такую роль должен играть хороший комплаенс-офицер, настраивая ключевых сотрудников компании на [восприятие корпоративных ценностей](https://www.e-xecutive.ru/management/practices/1985112-kompas-dlya-biznesa-kak-vnedryat-korporativnye-tsennosti).

Это лишь самые распространенные ошибки, которые совершает бизнес при внедрении антикоррупционного комплаенса. На практике необходимо учитывать многие детали, которые носят индивидуальный характер, и в которых, как известно, кроется дьявол.

Но если топ-менеджмент допустит хотя бы некоторые из этих ошибок, система антикоррупционного комплаенса не заработает в полной мере эффективно. И все те ресурсы, которые вы потратили на ее создание, можно смело списать в убытки. Более того, неэффективно настроенный антикоррупционный комплаенс едва ли лучше, чем его полное отсутствие.

# Как бороться с воровством на предприятии

[Максим Вальпа Директор по развитию, Екатеринбург 9 апреля 2018](https://www.e-xecutive.ru/users/477479-maksim-valpa)

Мелкие кражи, средние или крупные хищения – все это на самом деле явления одного порядка, над искоренением и предотвращением которых нужно работать постоянно.

В начале этого разговора будет не лишним привести рассуждения уральского предпринимателя и инвестора, **Тимура Горяева**, которыми он делится в своей книге «Шпаргалки для боссов. Жесткие и честные уроки управления, которые лучше выучить на чужом опыте»:

*«Люди в России меньше привязаны к своему рабочему месту. Во-первых, им плевать на то, что их ценят, плевать на то время, что они потратили на компанию, плевать на все то, что компания сделала для них. Во-вторых, весь мир за забором каждый вечер им говорит, что воровать – это хорошо, воруй давай. Люди, строго говоря, и не жили никогда во времена, когда кто-то у нас на родине считал по-другому».*

Возможно, кому-то эти рассуждения могут показаться узкоотраслевыми, тем более что автор действительно опирается на свой «фабрично-заводской» опыт работы. Но наша российская специфика рабочего класса такова, что отношение к собственности работодателя зачастую везде оставляет желать лучшего. И не важно, чем именно занимается компания.

Но распространенное мнение о том, что человеческую природу не изменить, не должно сдерживать решившихся на борьбу с воровством. В этой же книге Тимур Горяев продолжает свою мысль следующим образом:

*«Убеждение "Воровать – это нормально" – первое, с чем вам придется бороться, выветрить его из голов очень сложно, но, повторю, возможно. Достаточно объявить в компании нулевую толерантность к вранью и воровству, четко транслировать это каждому сотруднику и неукоснительно, последовательно и, самое главное, без исключений соблюдать это правило. Неудивительно, кстати, что далеко не каждый человек может получить удовлетворение, работая в такой компании».*

Изменить в своей компании можно все, и «нездоровое» отношение к собственности предприятия тоже.

**Варианты воровства и методы борьбы с ними**

Давайте рассмотрим некоторые из видов противоправных действий персонала, попутно поняв, что позволяет им существовать, к каким последствиям это приводит и как с этим бороться.

Начнем с вида воровства, знакомого многим не понаслышке – это мелкие кражи, которые совершаются бессистемно и без особой подготовки. Как правило, жертвами любителей всего, что плохо лежит, становятся свои же коллеги или мелкое имущество компании. Совет тут простой. Главное не отмахивайтесь: «Сами разберитесь! Что как дети малые?» и не закрывайте на эти проблемы глаза.

А вот прямая угроза материальным активам компании возникает, когда начинают происходить систематические, продуманные хищения. Обычно нечистые на руку сотрудники – по одиночке или в сговоре – воруют небольшими «порциями». И обнаружить факты хищения порой удается только по прошествии недель, а то и месяцев, когда урон становится явным.

Но хуже всего то, что во многих компаниях руководство знает о подобной «деятельности» сотрудников, но не предпринимает никаких мер для предотвращения хищений, потому что «так заведено». Ситуация, когда компания закрывает глаза на хищения, покуда они происходят в «разумных» пределах, приводит к самым пагубным последствиям. Воровство остается не только безнаказанным, но и становится само собой разумеющемся. Более того, в России это неотъемлемый признак некоторых сфер легальной экономики.

Например, показательна в этом плане сфера транспортных услуг. До сих пор во многих компаниях, занимающихся грузоперевозками, считается нормальным, если водители сливают топливо, продавая его на стороне. Эта практика, устоявшаяся с советских времен, часто не встречает сопротивления – ведь это негласный источник заработка водителя, можно сказать, закрепленная надбавка. А если даже руководитель компании против, то он не всегда готов идти наперекор традициям, потому что велик риск вызвать недовольство сотрудников и спровоцировать саботаж.

Главная опасность такого положения дел состоит в том, что для сотрудника – с молчаливого согласия руководства – это становится так называемым KPI его работы. Он каждый месяц обдумывает, как еще можно увеличить объем краденного. В итоге половина затрат компании на топливо может оседать в карманах работников.

**Живейший пример из нашего недавнего опыта**

На одном предприятии сливали топливо на 500 тыс. рублей ежемесячно. Без оглядки на укоренившуюся практику руководство все же внедрило [систему контроля](https://goo.gl/QC3V2A). В итоге за счет ликвидации воровства и повышения дисциплины персонала компании удалось сократить топливные расходы на 50%.

Боязнь растерять кадры и вызвать простои в работе компании зачастую делает невозможной и борьбу с более изощренными, «беловоротничковыми» видами воровства, которые распространены практически везде. Например, с откатами и проведением сделок через подконтрольные фирмы, когда есть место манипуляциям с финансовой отчетностью и выводу огромных средств. Здесь руководство так же может быть в курсе происходящего, а нередко и в сговоре, искренне полагая, что всё это происходит в русле общепринятых норм.

Частично отследить такие махинации может помочь специальное программное обеспечение SIEM-класса *(SIEM – это объединение двух терминов, обозначающих область применения ПО: SIM – управление информационной безопасностью и SEM – управление событиями безопасности. Технология SIEM обеспечивает анализ в реальном времени событий безопасности, исходящих от сетевых устройств и приложений)*.

**Как полностью оградить бизнес от воровства**

Для того, чтобы избежать повторения перечисленных ситуаций или же пресечь на корню их появление там, где подобное, к счастью, еще не происходило, требуется основывать свою работу на следующих принципах и правилах:

* Независимо от характера и степени хищений, воровство остается воровством. Всем сотрудникам должно быть сказано о нетерпимости к любым кражам и махинациям. Нельзя даже допускать мысли о том, что это в том или ином виде возможно. Иначе воровство станет постепенно частью системы.
* Собственники и руководители не должны бояться устанавливать жесткие правила игры в своих компаниях. Несмотря на возможное противодействие со стороны персонала, необходимо развивать кадровую и экономическую безопасность, внедрять системы учета и контроля, в том числе для удаленного мониторинга рабочих процессов. Например, для контроля корпоративного автопарка стоит установить систему мониторинга транспорта и контроля расхода топлива.
* Противодействие воровству должно стать частью корпоративной культуры компаний. Стремление работать честно без корыстных побуждений нужно доносить до коллектива в качестве одной из главных ценностей.

Если вы поставите себе целью ликвидировать воровство как данность и будете постоянно напоминать об этом себе и своим сотрудникам, то вы с высокой вероятностью сможете сформировать команду, где каждый думает о том, как увеличить зарплату с помощью своего труда, а не как изобрести новый способ поживиться.

# Сотрудники иногда мухлюют, получив оплату от клиентов

**Сотрудники иногда мухлюют, получив оплату от клиентов. Как это зафиксировать и расстаться с ненадежными**

Сеть ресторанов присоединила компанию, которая владеет несколькими кафе. Вскоре новое руководство заметило, что в кафе низкая выручка. Замерили посещаемость. Она высокая. Стали проводить внеплановые проверки и установили, что у официантов и барменов иногда открыты кассовые счета, хотя посетители уже ушли. Значит, не исключены махинации. Нужно расставаться с такими работниками. Но как это сделать, чтобы было основание и без юридических огрехов?

**Шаг 1. Установите камеры видеонаблюдения в залах кафе и там, где расположены кассы**

Настройте видеокамеры так, чтобы на записях **стояли дата и время**. Это нужно для того, чтобы фиксировать, в какое конкретное время в зале есть люди, а когда нет, а также как проходят расчеты – наличными или пластиковой картой.

**Шаг 2. Выявив нарушения, сопоставляйте видеозапись с кассовыми чеками**

Посмотрите отметки времени. Если окажется, что согласно видеозаписи в зале в это время никого не было, а кассовые чеки закрыты именно в этот час и минуты, считайте, что **у Вас есть доказательство**: официанты и бармены нарушают правила ведения кассовых операций.

**ПРИМЕР**

Просматривая видеозаписи из зала одного из кафе, региональный руководитель подметил, что часто бывает так: посетители расплачиваются наличными и уходят, а бармен не выдает им кассовые чеки. Кроме того, официанты часто открывают счета для посетителей сразу после того, как они занимали столики. В результате возникает несоответствие: к примеру, посетители, сделавшие заказы, занимают 10 столиков, а счетов открыто – 14. Когда кадры видеозаписи с датой и временем сопоставили с кассовыми чеками, то убедились, что официанты и бармены несвоевременно открывали и закрывали счета. Все это руководство сети ресторанов посчитало грубым нарушением финансовой дисциплины, а также сигналом о возможных мошеннических действиях.

Записи видеокамеры и копии чеков и счетов Вы сможете предъявить сотрудникам кафе, если будете проводить с ними профилактические беседы и предлагать им расстаться.

**Помните: без согласия сотрудников видеонаблюдение установить нельзя**

Информация, которую работодатель будет получать с помощью видеонаблюдения, относится к персональным данным. Соблюдайте требования, установленные законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (п. [1](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=420380853&anchor=XA00M2O2MP#XA00M2O2MP), [3](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=420380853&anchor=XA00M2U2M0#XA00M2U2M0) ст. 3):  
**1.** Устанавливайте только открытое видеонаблюдение. За скрытое предусмотрена уголовная ответственность.  
**2.** Разработайте Положение о системе видеонаблюдения.  
**3.** Получите согласие сотрудников, ознакомьте каждого с положением под роспись ([п. 8 ст. 86 ТК РФ](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=420306731&anchor=XA00M9I2NE#XA00M9I2NE)).  
**4.** Для третьих лиц, имеющих доступ в помещение, разместите табличку: «Ведется видеонаблюдение».  
**5.** Не устанавливайте камеры видеонаблюдения в душе, туалете, раздевалках в целях защиты чести и достоинства граждан.

**Шаг 3. Пропишите порядок работы с кассовой техникой в ЛНА, составьте должностную инструкцию официанта/бармена**

Обязательно составьте локальный нормативный акт, в котором пропишите все правила работы с кассовой техникой, укажите, когда официанты и бармены открывают счет для клиента, когда закрывают, в какой момент должны выдать посетителям кассовый чек. Словом, обозначьте **все требования по соблюдению финансовой дисциплины**. Более детально порядок работы с ККМ установите в должностной инструкции официантов и барменов. Прямо напишите, что официанты и бармены **обязуются учитывать наличные денежные средства правильно** – в порядке, установленном законодательством и ЛНА компании.

С локальным нормативным актом и должностными инструкциями ознакомьте каждого сотрудника под роспись. Это будет подтверждением того, что официанты и бармены знают, каким правилам и нормам должны следовать на работе. Иначе работники смогут утверждать, что порядок работы с кассовой техникой и наличностью в компании не установлен либо этот порядок до них не довели. В случае нарушения положений должностной инструкции фиксируйте это в письменном виде, составляя акт.

**Шаг 4. Разработайте Положение о внутренних проверках, укажите, кто может их проводить**

В этом положении Вы вправе установить порядок проведения как плановых, так и внеплановых проверок в ресторанах и кафе сети. В данном случае Вам важны прежде всего внеплановые проверки, о которых сотрудники не знают заранее и к которым не готовятся. Цель в том, чтобы, во-первых, узаконить сам факт таких проверок, во-вторых, прописать правила, по которым они могут проводиться. Обязательно укажите в положении, что проверяющие от компании вправе просматривать видеозаписи камер наблюдения, сопоставлять данные видеозаписей с кассовыми чеками, фиксировать, когда счета для клиентов открываются и закрываются.

Обязательно перечислите в Положении о проверках и **лиц, которые уполномочены проводить проверку**, иначе впоследствии сотрудники смогут добиваться (в том числе в суде) отмены ее результатов.

**Если не запросили объяснительную записку, не вправе применять дисциплинарное взыскание**

Обязанность работодателя затребовать от работника письменное объяснение по факту совершенного дисциплинарного проступка – неотъемлемая составная часть процедуры привлечения работника к дисциплинарной ответственности. Эта обязанность установлена частью первой [статьи 193](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=420306731&anchor=ZAP1RLU3C4#ZAP1RLU3C4)Трудового кодекса. Сотрудник обязан предоставить объяснение в конкретный срок – два рабочих дня. Чтобы документально зафиксировать дату, когда работодатель потребовал, чтобы работник предоставил объяснение, лучше оформить это требование письменно – на бланке за подписью лица, наделенного правом налагать дисциплинарные взыскания. Но вообще законодательство не обязывает работодателя запрашивать объяснительную записку письменно.

**Шаг 5. Составьте докладную записку, у провинившегося запросите объяснительную**

Будет лучше, если докладную записку о факте нарушения кассовой дисциплины и работы с наличностью, а также порядка расчета с клиентами напишет либо непосредственный руководитель того, кто провинился, либо дежурный менеджер. На основании докладной записки попросите сотрудника дать письменные объяснения, почему он допустил нарушение. Если сотрудник в течение двух рабочих дней не предоставит объяснительную записку, Вы должны составить акт, в котором зафиксируете отказ. Акт подписывают не менее трех свидетелей из числа сотрудников компании.

**Шаг 6. Увольняйте в связи с утратой доверия. Проводить инвентаризацию и фиксировать ущерб не обязательно**

Нет, Вы, конечно, можете провести проверку в форме инвентаризации, а также организовать расследование и установить факт, что официант или бармен, нарушив порядок кассовой работы, причинил работодателю материальный ущерб ([ст. 274 ТК РФ](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=420306731&anchor=ZA00M0S2M0#ZA00M0S2M0)). А затем определить и размер ущерба. Если с работником заключен договор о полной материальной ответственности и наличие недостачи у этого работника доказано, то именно он должен доказать отсутствие своей вины в причинении ущерба ([п. 4 постановления Пленума ВС РФ от 16 ноября 2006 г. № 52](https://e.hr-director.ru/npd-doc.aspx?npmid=96&npid=902015687&anchor=XA00LUO2M6#XA00LUO2M6)).

Но в данном случае это вовсе не обязательно. Факт причинения материального ущерба компании либо хищения или растраты средств вовсе **не является обязательным условием для увольнения** по [пункту 7](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=420306731&anchor=XA00M8M2NC#XA00M8M2NC) части первой статьи 81 Трудового кодекса (утрата доверия). Скажите сотрудникам: сам факт нарушения ими финансовой дисциплины и порядка работы с кассовой техникой является грубым нарушением, за которое работодатель вправе наложить на них взыскание в виде увольнения. Правильность такого подхода подтверждается решением Тверского районного суда г. Москвы от 8 июня 2011 г. по делу № 2-3126/2011, [определением Московского городского суда от 12 октября 2011 г. № 33-32689](https://e.hr-director.ru/npd-doc.aspx?npmid=98&npid=1426255).

# Законно ли видеонаблюдение на рабочем месте?

26 октября 2018

У каждого человека есть свои секреты и тайны, личные и семейные отношения, которые по своей юридической природе имеют неприкосновенный характер. Рукописные (почтовые) и электронные сообщения, разговоры по телефону являются исключительно конфиденциальной информацией, принадлежащей только одному физическому лицу и охраняются статьей 23 Конституции РФ. Право на ограничение переписок, переговоров и отправки сообщений может дать лишь только судебный документ. В соответствии с законом «Об оперативно-розыскной деятельности», от 12.08.1995 г. №144-ФЗ, в целях проведения следственных мероприятий, расследования, раскрытия и пресечения преступлений, технические средства могут использоваться уполномоченными лицами, относящимися к структурам МВД, ОВД, ФСБ, Следственным комитетом и другими государственными структурами, включающими в себя отдел с оперативным подразделением.

Ограничения при сборе информации на работников для работодателя

Для работодателя права на такие полномочия вышеуказанными законами не предусмотрены. Трудовой кодекс РФ не включает в себя подробный перечень диспозитивных и императивных норм, регулирующих доступные способы осуществления контроля за сотрудниками компаний. Более того, на стороне неприкосновенности человека выступает и Кодекс практики МОТ, регулирующий на международном уровне защиту данных конфиденциального характера работников. Запрещено использовать слежку и вести звукозапись при помощи диктофонов, камер, специальных компьютерных программ и мобильных телефонов. Однако законодательство в суверенном государстве на национальном уровне может разработать альтернативный вариант законопроекта, позволяющее осуществлять данный вид мероприятий на рабочих местах. Разрешена ли скрытая слежка в офисах? Разрешено ли использовать в офисных и служебных помещениях (с целью обезопасить от преступлений компанию, работодателя и работников) аудио-и видеоаппаратуру скрытой записи и слежки? Этот вопрос не дает однозначного ответа, и не имеет развернутых юридических комментариев, ссылающихся на конкретные нормативные источники. Если же сослаться на акты Совета Европы, то можно получить общие разъяснения на возможность работодателя применить технические средства отслеживания, не нарушая прав работника. Международное законодательство допускает применение работодателем на предприятии видео-и аудиоустройств лишь при письменном согласии работников. Возможно, Государственная Дума вскоре разработает аналог подобного законопроекта на федеральном уровне, в котором будет черным по белому написано: что работодатель делать может, а что – нет. Письменное согласие на обработку данных

В каких случаях работодатель обязан взять письменное согласие работника на видеосъемку? Обработка персональных данных конкретного работника возможна с точки зрения действующей нормативной базы лишь с его разрешения. Следовательно, работник имеет полное право в соответствии со статьей 21 части первой ТК РФ узнать, с какой целью осуществляется аудио и видеосъемка. В соответствии со ст. 74 ТК РФ, внедрение на рабочем месте аудио-и видеоаппаратуры – это изменения условий труда работника, и он должен быть извещен о них не позднее, чем за 2 календарных месяца. При приеме нового работника, с условиями о видеонаблюдении он должен быть ознакомлен в локальном положении (которое компания в обязательном порядке должна разработать) и дать свое письменное согласие на видеосъемку и обработку персональных данных.

Ст. 9 (Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) «О персональных данных» Работодатель при этом не имеет права заниматься сбором и хранением информации, являющейся конфиденциальной (личной). Например, если целью контроля действий работника является регулирование и отслеживание производительности труда, предотвращение кражи и сохранность имущества работодателя и сотрудников предприятия, то обработка персональных данных возможна лишь по согласию работников. Данный вопрос регулируется статьей 86 ТК РФ. Перед получением согласия у работников на обработку персональных данных, стоит учитывать места, в которых установлены, или будут устанавливаться технические средства контроля. Если речь идет об общественных местах, например, таких как актовый зал, коридор и иные проходные места и помещения, то в письменном согласии сотрудников предприятия нет никакой необходимости (ст. 152.1 ГК РФ). Но все же во избежание возникновения конфликтных ситуаций, связанных с аудио и видеосъемкой на предприятии, работодателю рекомендуется разработать локально-нормативный акт или положение, описывающее цели внедрения на рабочих местах технические средства контроля и указать, сколько хранятся данные записи. Также желательно с юридической точки зрения перечислить нормы права, регламентирующие возможность работодателя осуществлять видеосъемку на территории предприятия.

В случае нарушения прав работника, касаемо вторжения в личную жизнь без его согласия, и использование работодателем конфиденциальной информации работника в корыстных целях, данное лицо будет нести административную, гражданскую и, возможно, уголовную ответственность – в зависимости от тяжести проступка.

# Кто из сотрудников и соискателей лжет

**Кто из сотрудников и соискателей лжет, подделывает документы и ворует? Чтобы выявлять это, применяйте профайлинг. Обучите подчиненных**

**Алла Пискунова**

**В одном промышленно-торговом холдинге падали продажи. Исследование показало: слишком высоки цены на продукцию и услуги. Руководство снизило цены на 20%! Однако продажи практически не выросли. Тогда опросили клиентов и были шокированы: половина из них не знают о снижении цены и платят, как и прежде. А по документам, поступающим в бухгалтерию, – полный порядок, всюду значится новая низкая цена. HR-директору поручили выявить мошенников, не прибегая к детектору лжи.**

Кроме того, руководство попросило уволить вредителей, а вместо них набрать таких сотрудников, которые не склонны к подобным махинациям. По сути, в рамках одной задачи Директору по персоналу нужно решить две. И обе очень сложные. Так как детектор лжи исключается из-за своей дурной славы и способности ухудшить имидж компании на рынке труда\*, нужно использовать другие инструменты и методы. HR-директор решил применить профайлинг (с английского profile – профиль, профилирование) и обучить этому методу своих подчиненных. Под этим термином понимается группа психологических приемов и методик оценки и прогнозирования поведения человека. Эти приемы несложные. Вы проводите собеседование с человеком и во время разговора наблюдаете за его вербальными и невербальными проявлениями, подмечаете непроизвольные и неконтролируемые телодвижения, жесты, мимику, интонации в голосе, манеру одеваться. Благодаря этому Вы распознаете истинные мотивы и намерения сотрудника, составляете его психологический портрет (профиль).

Невербальные проявления в поведении человека даже важнее словесных. Исследования ученых-психологов показывают: более 70% информации передается невербально. Ведь за вербальным сообщением «Уволился с прежнего места работы по собственному желанию» может скрываться что угодно: от воровства до банальной профнепригодности. И только если уметь улавливать невербальную информацию, можно понять, лжет человек или нет (различные исследования показывают: большинство людей лгут три раза за 10 минут), скрывает ли какие-либо неприглядные факты о себе (склонность к алкоголизму или наркомании, азартным играм), имеет ли нечистоплотные замыслы (скажем, присвоить часть прибыли компании).

Профайлинг применяется в самых разных сферах (более 10), но для нас интересны кадровый профайлинг и бизнес-профайлинг. Первый помогает определить, соответствует ли кандидат требованиям, предъявляемым компанией к вакансии (это нужно и менеджеру по подбору персонала), а также оценить уже работающих сотрудников (пригодится менеджеру по оценке). А второй вид поможет Директору по персоналу быть верным помощником руководства компании на деловых переговорах – подмечать, правду ли говорит человек, стоит ли верить его обещаниям.

**Профайлинг появился благодаря Джеку ПОТРОШИТЕЛЮ**

Это не преувеличение. Английский хирург Томас БОНД в 1888 году впервые попытался составить психологический портрет серийного убийцы Джека ПОТРОШИТЕЛЯ на основе свидетельских показаний и имевшихся в деле улик. И на первых порах профайлинг использовался именно для этого – выявления психологических характеристик неизвестных преступников по следам, оставшимся на месте преступления. Затем сфера применения этой методики расширилась. В последние десятилетия она стала HR-инструментом для проверки информации, получаемой от кандидатов и сотрудников, клиентов и деловых партнеров компаний.

**Пример**

Обучившись на курсах профайлингу, HR-директор сумел выяснить, кто и как продавал клиентам продукцию и услуги компании по старой высокой цене (см. начало статьи). Он побеседовал со всеми менеджерами по продажам, которые имели доступ к печати компании и оформляли финансовые документы клиентам. Двоих менеджеров-мошенников выдала их левая рука. В отличие от более развитой и подчиненной рассудку правой руки, левая хуже контролируется человеком. И всякий раз, когда менеджеры что-то скрывали, лгали, она подергивалась, пальцы делали непроизвольные движения. Поработав с двумя мошенниками получше, HR-директор понял их схему действий: они говорили клиентам, что в компании введена новая система оплаты товаров и услуг. Одна часть якобы платится в безналичном порядке (это и есть новая более низкая цена), а вторая часть (разница между новой и старой стоимостью) вносится наличными. Все документы оформлялись на ту часть, что перечислялась безналично. А на наличную часть менеджеры выдавали покупателям лишь приходный кассовый ордер, ставили на него печать, но в бухгалтерию эти ордера не сдавали. Наличность брали себе.

А теперь рассмотрим, как применять методики профайлинга.

Ольга БАКЛАГИНА,

руководитель мастерской практического психолога «Счастье», специалист-профайлер

Наше правое полушарие мозга считывает информацию об окружающих

Причем обрабатывает оно эту информацию очень быстро, и все проявления стресса у окружающих не остаются незамеченными. Вспотевшие руки, просьба подать стакан воды, попытки ослабить галстук, прикосновения к шее однозначно свидетельствуют о проявлении стресса. Но отчего? Может быть, в помещении просто жарко? Дотронулся до кончика носа – врет или простужен и боится чихнуть? Глаза покраснели – признак сильного волнения либо конъюнктивита или бессонной ночи? Не исключайте влияния внешних факторов и раздражителей! И еще постарайтесь быть понятным человеку. Стать своим не всегда получается, да и не всегда нужно. Но можно утверждать наверняка своим, как правило, не лгут. Видимо, поэтому в качестве экспертов, ведущих опросную беседу (собеседование), сейчас все чаще стали приглашать специалистов-профайлеров и психологов.

**Проведите калибровку – замерьте реакции человека в комфортной обстановке**

Для этого задайте несколько безобидных вопросов на отвлеченные темы, которые не поставят человека в ситуацию, когда ему надо лгать и лицемерить. Например: «Любите ли Вы свою семью?», «Помогаете ли жене (мужу) по хозяйству», «У Вас есть автомобиль? Давно ли Вы его купили?» Предложите собеседнику кофе, спросите о погоде или о пробках на дорогах – в общем постарайтесь его разговорить. А сами в это время не анализируйте ответы, а наблюдайте за тем, как человек будет держать корпус, ноги, руки, голову, какое у него будет выражение лица, куда он будет смотреть, как говорить.

**Задавайте более четкие и острые вопросы и наблюдайте за поведением сотрудника**

Ваша задача – подметить, в какой момент поведение кандидата или сотрудника меняется и проявляются новые, не свойственные ему черты. Когда человек лжет, у него нарушается внутреннее равновесие, он испытывает сильную эмоцию, начинает контролировать себя и «плывет» по сравнению с нормальным состоянием, которое мы зафиксировали в начале беседы. Например, если человек рад, что надул босса, то о краже будет говорить с улыбкой. Либо, если хорошо себя контролирует, эмоция радости едва уловимо проявится в мимике. В любом случае он подсознательно чувствует угрозу быть уличенным в обмане и понести за это наказание. Внутреннее напряжение непременно проявится в мимике, взглядах, жестах, речевых особенностях. Если Вы видите, что человек отошел от своей привычной модели поведения, то высока вероятность, что это вызвано попыткой солгать или скрыть от Вас информацию.

**Пример**

В крупную косметическую компанию на должность арт-директора приняли молодого мужчину 32 лет, который представил потрясающее портфолио. И не пожалели: все его работы на ура принимались руководством компании. Но приблизительно через год случилось непонятное: арт-директор завалил подряд пять важных проектов. HR-директору поручили выяснить, в чем дело. Он поговорил с арт-директором, внимательно наблюдая за тем, как он реагирует на его вопросы. И заметил: все, что касалось выработки идей, вызывало беспокойство у сотрудника. Он начинал теребить пуговицы на одежде или хватал ручку и нервозно вращал ею. Директор по персоналу задавал все больше и больше вопросов на эту тему и постепенно вывел арт-директора на чистую воду. Оказалось, что на собеседование год назад он принес 90% не своих работ, а других дизайнеров. Когда его приняли на работу, он нашел стороннего дизайнера и передавал все свои задания ему, платил деньги из своей зарплаты. Когда подпольный дизайнер заболел и стал недоступен, арт-директор потерпел фиаско. В итоге с арт-директором расстались, а дизайнера, который действительно разрабатывал макеты, взяли на работу.

**Пять главных признаков того, что человек лжет**

Группа ученых из Калифорнийского университета в Лос-Анджелесе провела эксперимент, в ходе которого выявила ряд закономерностей. Во-первых, рассказывая придуманную историю, люди склонны повторять вопросы, которые им задают, прежде чем отвечать на них. Во-вторых, они периодически выдают фразы, оправдывающие их придуманные поступки, даже если в этом нет необходимости. В-третьих, они внимательно следят за реакциями собеседников, пытаясь определить, поверили им или нет. В-четвертых, нередко они сначала замедляют речь, чтобы дать себе время подумать, но как только появляется возможность, сразу же ускоряют темп. В-пятых, услышав сложный вопрос, лжецы бросают в сторону лишь короткий взгляд, в то время как люди, не стремящиеся солгать, надолго отводят глаза, чтобы сосредоточиться.

**Переформулируйте болезненный для человека вопрос и задайте снова**

Либо попросите уточнить детали той ситуации, о которой идет речь. Посмотрите, как сотрудник или соискатель отреагирует на этот раз. Все это необходимо сделать для того, чтобы убедиться, что Ваши подозрения верны и человек действительно может лгать. Это исключит неверную интерпретацию поведения собеседника. Если после Ваших дополнительных вопросов поведение человека вновь изменится, Вы получите дополнительное доказательство лжи.

**Еще раз проверьте, правильно ли Вы провели калибровку**

То есть убедитесь, что в момент предполагаемого обмана он действительно вел себя необычно. Для этого во время беседы вновь затроньте отвлеченную тему, чтобы собеседник немного расслабился. И если он снова станет себя вести спокойно, как в начале собеседования, значит Ваши наблюдения были верны и ему действительно есть что скрывать.

**Убедитесь, что смена поведения человека объясняется ложью**

Например, иногда реакции некомфортности проявляются просто из-за волнения человека по поводу самого собеседования или из-за формулировок, которые сами по себе вызывают чувство стыда или смущения у собеседника. Или, к примеру, улыбка человека может показаться Вам фальшивой. Но это не всегда означает, что человек лжет. Это может быть маской неуверенного в себе человека.

**Пример**

Девушка, претендовавшая на вакансию специалиста казначейства, во время собеседования время от времени словно прикрывала рот и говорила сквозь пальцы (само по себе это свидетельствует о стремлении скрыть неправду), положила ногу на ногу, скрестила руки (говорит о закрытости). Менеджер по подбору, естественно, заподозрила попытку обмана. Чтобы убедиться в этом, перевела разговор на нейтральную тему, но поведение девушки не вернулось к норме. Тогда HR-менеджер прямо спросила, почему соискательница зажата. Она объяснила – боится простудиться от кондиционера, слегка замерзла. Кондиционер выключили, и все подозрения по отношению к девушке исчезли.

**Постарайтесь фиксировать микровыражения эмоций**

Это один из так называемых маркеров (индикаторов) лжи. Эмоция может либо соответствовать словам человека, либо противоречить им. И если окажется, что противоречие есть, то именно микровыражение, а не слова, будет отражать его истинное мнение об объекте высказывания\*\*.

Микровыражение может буквально промелькнуть, заняв какие-то доли секунды, после чего черты лица собеседника примут прежнее выражение. Так что внимательно наблюдайте за человеком.

Но обратите внимание: есть **два признака неискренности мимики**. **Первый признак:** выражение задерживается на лице дольше 6–10 секунд. Если это происходит, то, скорее всего, на лице маска, то есть человек Вас обманывает, пытаясь продемонстрировать чувство, которое он не испытывает. **Второй признак:** эмоция проявляется на лице несимметрично. Например, если Вы видите, что человек улыбается лишь одной стороной (как правило, левой), это значит, что улыбка его фальшивая и она прикрывает собой какую-то другую эмоцию, которую он переживает на самом деле. Вполне возможно, что истинной эмоцией является вовсе не радость, а страх, который естественен для человека в моменты, когда он лжет.

Артем ПАВЛОВ,

руководитель агентства экономической и кадровой безопасности «D.I.»

Вглядитесь в черты лица - перед Вами карта человеческой личности

Допустим, перед Вами лицо с длинным носом и открытыми ноздрями. Интуитивно Вы начнете воспринимать такого человека как инфантильного и любопытного. А короткий и вздернутый носик, скорее всего, заставит Вас усомниться в аналитических способностях его обладателя. И это не случайно: именно так, согласно физиогномике, на лице человека отражаются особенности его личности. На самом деле каждый из нас является прирожденным профайлером и умеет не только читать людей по лицам, но и распознавать ложь по невербальному поведению. Например, если мы испытываем недоверие человеку, с которым только что познакомились, но не понимаем почему, – это срабатывает наш внутренний профайлер, который уже сделал свои выводы. Профайлинг – это, по сути, искусство перевода информации «с русского на русский», то есть из области неосознанного в осознанное.

**Не теребит ли человек кончик носа, не потирает ли веки? Наблюдайте за жестами**

Можно предположить, что человек хочет Вас обмануть, если он:

– дотрагивается до кончика носа. Но именно до кончика! Если он, например, начинает усиленно тереть спинку носа, то этот жест будет иметь другое значение – а именно что Вы сильно задели самолюбие собеседника и тем самым разозлили его;

– совершает другие рефлекторные, непродуманные движения рук возле лица (потирает веко, проводит пальцем над верхней губой, поглаживает ладонью губы, лоб, виски, подбородок, прикрывает рот);

– дистанцируется от собеседника (наклоняет туловище назад или отступает на шаг, принимает закрытую позу, скрещивая руки на груди или ноги под стулом);

– поджимает под себя ноги либо начинает постукивать ими о пол;

– быстро потирает руки (если же медленно, то это не признак обмана, а предвкушение взаимной выгоды).

**Но обратите внимание:** во-первых, ложь всегда проявляется не единичным жестом, а **цепочками из нескольких разных жестов**. Поэтому, например, по одному только дотрагиванию до кончика носа нельзя делать вывод о том, что Вы имеете дело с лжецом. Для этого нужно, чтобы он совершил еще какие-то телодвижения, подтверждающие Ваши догадки.

**Делает ли человек безапелляционные заявления, использует ли речевые клише**

Стремясь исказить информацию или преподнести ее однобоко, намеренно умалчивая о существенных деталях, человек обычно делает обобщения («все», «каждый», «всегда», «ни один», «никто»). Также стоит поставить под сомнение объективность слов собеседника, если он:

– начинает строить короткие предложения, в которых используется мало прилагательных. Лаконичность речи у обманщика объясняется тем, что он **боится не запомнить всего, что придумывает**, и подстраховывается, чтобы не запутаться в деталях;

– уклоняется от прямых ответов. Например, вместо четкого «нет» отвечает что-то в духе «я не такой человек, чтобы позволять себе…»;

– делает безапелляционные заявления («я никогда…», «я ни за что…», «я никому…»);

– изменяет темп речи, начинает говорить быстро или, наоборот, прерывается на длинные паузы, запинается;

– постоянно повторяет одни и те же фразы – речевые клише. Скорее всего, он их заранее разработал и заучил для самопрезентации.

**Анализируйте почерк человека. Это один из инструментов профайлинга!**

Давно подмечено, что мелкий, убористый почерк с небольшими расстояниями между буквами присущ людям экономным и скупым, а крупно, размашисто пишут люди широкой натуры, склонные к демонстративности. Если кто-то стремится занять на бумаге как можно больше места, то, скорее всего, он и в жизни не ограничивает себя в желаниях. Кроме того, установлено, что, когда человек волнуется (что может быть связано с необходимостью лгать), у него меняется характер почерка: неравномерно увеличиваются расстояния между буквами и их расстановка, наклон становится неустойчивым.

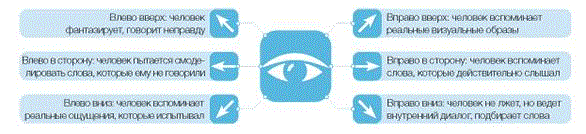
**Есть ли то, что не скроешь и не проконтролируешь, – страх и волнение?**

Такие эмоции – спутники лжи. Они проявляются в том, что человек начинает часто проглатывать слюну, покашливать, учащенно дышать. У него может появиться дрожь в голосе, пересохнуть в горле, измениться цвет лица (он бледнеет или краснеет). Человек начинает чаще моргать, иногда становится заметным нервный тик. Могут вспотеть руки. Но учтите: кашлять человек может из-за простуды, а голос у него может быть сам по себе дрожащим.

**Следите за движением глаз собеседника. Они выдают попытку солгать**

Направление, в котором неосознанно движутся глаза человека во время разговора, может свидетельствовать об истинных мыслях человека. Это утверждают специалисты по невербальным жестам Ричард БРАНДЛЕР и Джон ГРИНДЕР. Например, признаками лжи считаются взгляды влево вверх и влево в сторону (так это выглядит со стороны наблюдателя – см. схему ниже). Например, если, отвечая на вопрос, может ли человек работать в команде, он смотрит влево, высока вероятность, что ответ просто придуман. Если глаза движутся вправо, собеседник вспоминает свой прошлый опыт и, скорее всего, более правдив.

**Схема. Что означает направление взгляда человека**



\*О том, как проводить проверки на полиграфе, чтобы не сомневаться в их результатах, читайте в [№ 4, 2011](https://e.hr-director.ru/default.aspx?mid=9636&ut=s)  
\*\*Подробнее о том, как проявляют себя различные эмоции на лице человека, рассказывается в книге американского психолога Пола ЭКМАНА «Узнай лжеца по выражению лица».

# Начинаем слежку: контроль за Интернетом, видеонаблюдение.

**Начинаем слежку: контроль за Интернетом, видеонаблюдение. Как минимизировать негативные последствия**

**Александр ПЛЯСКИН,**руководитель проектов «Агентства стратегических инициатив по продвижению новых проектов»

**Руководители отделов все чаще говорят о том, что сотрудники стали опаздывать, много времени проводят в курилке и в буфете. На одном из совещаний у гендиректора решили, что надо установить электронную систему доступа, фиксирующую время прихода и ухода. Но это помогло лишь отчасти: сотрудники стали приходить вовремя, но по-прежнему работают, мягко говоря, с прохладцей. Уже и клиенты жалуются, что дозвониться трудно. И руководство решилось на непопулярную меру.**

Топ-менеджеры высказались за то, чтобы следить, чем занимаются сотрудники на работе, – установить видеокамеры в офисе и контролировать пребывание в Интернете, а также переписку с корпоративной электронной почты (это помогает понять, сколько сотрудники работают и много ли времени тратят на посторонние дела). Отъявленных лодырей выявить и уволить. На других сотрудников система наблюдения может подействовать как профилактическая мера: узнав про слежку, они прекратят подолгу сидеть в Интернете или болтать по телефону.

Но не исключены негативные последствия – кадровые и юридические. И Вам вместе с подчиненными предстоит нивелировать их. К примеру, есть риск, что большинство сотрудников воспримет установку видеокамер и просмотр переписки как ущемление свободы и чувства личного достоинства. А значит, начнет думать об уходе из компании. Причем в первую очередь такая мысль может возникнуть именно у самых добросовестных и ценных сотрудников: «Я и так работаю по полной, а тут еще слежка!»

Кроме того, необходимо соблюсти некоторые юридические формальности. Дело в том, что законодательство запрещает вести наблюдение за сотрудниками, не уведомив их об этом. Иначе могут возникнуть трения с правоохранительными органами.

**Пример**

В офисе компании установили камеры видеонаблюдения не только в коридорах, но и в рабочих помещениях, в курилках, на кухнях и в столовой. Сделали это тихо, ничего не говоря работникам. Один из специалистов, у которого были трения с руководителем и который собирался увольняться, заметил камеры. Чтобы сделать неприятность работодателю, специалист написал и подал в отдел внутренних дел заявление о нарушении своих прав. В компанию нагрянули вооруженные представители охраны правопорядка с проверкой. Они наложили штраф на организацию и на генерального директора, а также обязали прекратить наблюдение за сотрудниками, убрать видеокамеры и системы слежения, установленные на компьютеры.

Ваша задача – правильно преподнести новость о введении мониторинга, обосновать эту меру и, по сути, психологически подготовить коллектив, и предпринять действия, оберегающие от упреков в нарушении законодательства.

Совет

Объявляя о введении наблюдения в компании, не употребляйте слово «следить». Оно носит негативный оттенок и сразу переводит одних в ранг «надсмотрщиков», других представляет в виде заключенных, отбывающих восьмичасовой срок. Лучше говорить об учете рабочего времени персонала либо о мониторинге. Ведь работник продает свое рабочее время, а работодатель покупает этот ресурс, необходимый для функционирования бизнеса. Рабочее время тоже подлежит учету. Как и на что оно тратится? Какие результаты приносит? Сколько времени требуется в норме для достижения тех или иных результатов? Донесите до сотрудников мысль: учет рабочего времени становится просто частью общей системы управленческого учета компании.

**Объясните сотрудникам, что наблюдение – не против них, а для них**

Прямо объявите всем работникам компании о том, что будет установлена система наблюдения. Но затем приведите аргументы в поддержку этого шага. Намекните, что сознательным сотрудникам нечего бояться. Более того, у них, наконец, появится надежда, что они перестанут выполнять работу чуть ли не за весь отдел, в то время как лодыри ничего не делают. Также обязательно подчеркните, что главная цель системы не наказание, а возможность принять справедливое решение в сложных ситуациях. И для сотрудников может быть выгодно, что в офисе есть такая система.

**Комментирует Алексей ПЕРВЕНЦЕВ, HR-директор компании «Иннова»:**

**У видеонаблюдения могут быть цели, не связанные со слежкой**

В офисе нашей компании установлены камеры и действует пропускная система. Об этом знают все. Мы не используем видеонаблюдение для контроля за сотрудниками. Мы решаем другие задачи. Например, обеспечиваем безопасность, выявляем, какие зоны в офисе наиболее посещаемые, и изменяем офисное пространство в лучшую сторону, оцениваем результаты некоторых инициатив компании. К примеру, на одном из этажей офиса мы сделали библиотеку. Она расположена рядом с ресепшн, поэтому доступ к книгам имеют не только сотрудники, но и посетители офиса. Мы проанализировали видеозаписи и увидели, кто и как пользуется книгами, что мешает сотрудникам. Благодаря этому мы, не докучая работникам опросниками, сделали библиотеку более удобной.

**Пример**

В ресторане в зоне приема посетителей (там поставлен стол и выставлены спиртные напитки – на посошок) решили организовать видеонаблюдение. Сотрудники были резко против. Но их отношение полностью изменилось после одного инцидента. Как-то вечером в ресторан зашли молодые люди и нагло потребовали, чтобы официант бесплатно напоил их спиртным. Официант, конечно же, отказался. Тогда они пообещали оставить в книге для посетителей такой отзыв, который точно приведет к увольнению! Отзыв оставили. Но, просмотрев видеозапись, официанта не уволили, а премировали. Теперь против наблюдения никто не возражает.

Еще один аргумент в пользу системы наблюдения с точки зрения сотрудников – сохранность личных вещей.

**Пример**

В отделе продаж установили камеры видеонаблюдения. А перед тем как это сделать, руководство объяснило коллективу, что в офис часто приходят посторонние люди – курьеры, экспедиторы и водители клиентов. Некоторые не прочь прибрать к рукам все, что плохо лежит. Эти аргументы подкрепили недавней пропажей мобильного телефона одной из сотрудниц. После этого попросили работников подписать Положение о политике безопасности, где среди прочего был пункт о мерах по предотвращению хищений, краж и других противоправных действий в офисе компании. Большая часть персонала восприняла установку видеонаблюдения как вполне обоснованное мероприятие.

**Не говорите, что вся электронная почта будет просматриваться**

Объясните персоналу, что руководство может контролировать входящие и исходящие сообщения, чтобы препятствовать утечке конфиденциальной информации. Или, скажем, объявите, что мониторинг исходящих сообщений возможен лишь тогда, когда компания будет готовиться к тендеру. А в Положение о мониторинге включите следующий пункт: «Руководство компании имеет право отслеживать почту на предмет соответствия проводимой политике компании» или «Мониторинг проводится в целях предотвращения распространения неподобающего или незаконного контента».

**Информировав сотрудников о наблюдении за ними, получите их роспись**

В [Конституции Российской Федерации](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=499075091) закреплено право каждого гражданина на неприкосновенность частной жизни, на тайну переписки, телефонных переговоров и почтовых сообщений. А согласно [статье 21](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=902304710&anchor=ZA01Q0G38O#ZA01Q0G38O) Трудового кодекса, каждый работник имеет право на полную достоверную информацию об условиях труда и требованиях охраны труда на рабочем месте. О том, что устанавливаются камеры видеонаблюдения, записываются телефонные переговоры и проводится перлюстрация писем, работодатель обязан предупредить сотрудников, получив их роспись.

В Правилах внутреннего распорядка нужно указать, что в компании существует конкретная система слежения (например, система видеонаблюдения, мониторинга интернет-трафика, адресов электронной почты). Кроме того, приведите обоснование производственной необходимости в их установке. В здании офиса разместите специальные таблички, извещающие о том, что ведется наблюдение. Новым сотрудникам говорите о внутреннем мониторинге на собеседовании до заключения трудового договора.

**Пример**

Сотрудник торговой компании установил на свой компьютер программу, которая способна обнаружить агента слежения. Программа обнаружила агента, и работник понял, что за ним следят, хотя не предупреждали и не давали соответствующих документов на подпись. Сотрудник пришел в службу управления персоналом и пригрозил обратиться в правоохранительные органы и в трудовую инспекцию. Его удалось отговорить, а за понимание и неразглашение информации выплатили вознаграждение. Но через некоторое время он все равно уволился. А позже заявления об увольнении принесли еще несколько работников.

**Порой достаточно муляжей видеокамер**

Сама новость об установке систем наблюдения за сотрудниками может стать хорошей профилактической мерой. **Работники начинают работать более эффективно**, придерживаются трудового распорядка, ведут себя в коллективе вежливо и доброжелательно относятся к клиентам. И самое главное – практически полностью исключается вероятность мошенничества, краж и других противоправных деяний. В некоторых компаниях вместо камер ставят муляжи, предупреждают сотрудников о том, что их телефонные разговоры записываются, хотя на самом деле этого не делается. А эффект все равно ощутимый.

**Пример**

В одном провинциальном городе власти поставили чиновников перед фактом: каждая минута их рабочего времени будет под контролем, а все их хамские выходки запишут на пленку и покажут по местному телевидению. На сотрудников благотворно подействовала уже сама эта новость: на работу не опаздывают, с посетителями вежливы.

**Комментирует Оксана МОРОЗОВА, HR-директор RosLogistics:**

**Сделайте так, чтобы сотрудники проявляли свои лучшие качества**

Негативные эмоции возникают у персонала, если разрушаются его ожидания. Еще во время собеседования с кандидатом говорите о том, что в компании ведется мониторинг работы сотрудников. Подчеркивайте, что это несправедливо, мкогда недобросовестных сотрудников не наказывают, в то время как большинство честно и эффективно трудятся.

По статистике, 10 % работников всегда злоупотребляют безнаказанностью, 10 % – никогда не используют служебное положение в личных целях. А вот поведение 80 % сотрудников формируется в зависимости от того, какая рабочая атмосфера царит в компании. Создайте условия, в которых сотрудники будут проявлять свои лучшие как профессиональные, так и человеческие качества. Например, с помощью грамотной политики безопасности и корпоративной культуры. Люди стараются не совершать те поступки, которые осуждаются большинством.

**Когда можно обойтись видеокамерой, а когда нужна программа-шпион для компьютера**

Видеонаблюдение оправдано в тех случаях, когда нужно проверять, как трудятся рабочие в производственных цехах, продавцы в магазине, менеджеры по продажам, официанты. Но как с помощью камеры понять, чем занимается сотрудник, с серьезным видом часами сидящий за компьютером, – занимается делом или ходит по интернет-сайтам? Чтобы получить ответ на этот вопрос, установите специальную программу на компьютер, которая будет собирать информацию обо всех действиях работника.

**Пример**

В московском офисе крупного производственного холдинга установили так называемый агент слежения, который собирал информацию обо всех действиях человека за компьютером. Например, программа фиксировала время включения и выключения компьютера, все операции с файлами (создание, копирование, удаление), какие программы и сайты человек открывал и на какое время, что писал в ICQ, MSN, какие письма отправлял в Mail.ru-агенте, в Yahoo Messenger. Кроме того, агент слежения периодически делает снимки с экрана монитора, показывает, какие файлы распечатаны и многое другое. IT-служба могла в режиме реального времени просматривать данные о каждом пользователе, а также создавать статистические отчеты для руководства компании. Сначала система слежения была установлена так, что пользователи не могли ее видеть. Но после того как выяснилось, что около 80 % сотрудников больше половины рабочего времени тратят на личные дела, Директор по персоналу посоветовал руководителю компании предупредить персонал и сделать программу видимой. Правда, руководство объяснило, что мониторинг будет проводиться только с 9 до 18. В итоге большая часть сотрудников вообще перестала заходить в социальные сети и сидеть в чатах в рабочее время.

**Прослушка стационарных и мобильных телефонов, система радиометок с Wi-Fi**

Система прослушивания и регистрации телефонных звонков необходима, если Вы хотите контролировать сотрудников, которые по работе должны часто звонить. Это в основном персонал колл-центров, секретари, иногда менеджеры по продажам.

Не самый этичный вариант – прослушка мобильных телефонов – подходит в том случае, если необходимо контролировать специалистов, которые часто ездят. Посоветуйте генеральному директору предоставить таким сотрудникам бесплатную мобильную связь, в которую уже вшиты подслушивающие устройства. Компания убьет двух зайцев – и лояльность повысит, и мониторинг обеспечит.

Если Ваше предприятие занимает огромную площадь, и важно, чтобы каждый сотрудник находился на своем месте, покидая его лишь в определенное время, можно воспользоваться системой на основе Wi-Fi, разработанной компанией Hitachi. В одежду персонала (например, в униформу) вшиваются радиометки, и система следит за ними, сообщая обо всех перемещениях сотрудника. Это особенно важно, если работа специалистов связана с материальной ответственностью (например, в огромных складах) и в определенных помещениях некоторым работникам вообще не рекомендуется находиться. Если сотрудники службы безопасности вашей компании сообщат, что кто-то из работников слишком часто бывает там, где ему не нужно, это повод внимательнее понаблюдать за таким сотрудником.

**Комментарий Наталья ЦВЕТКОВА, исполнительный директор издательской группы «ЕЖЕ»:**

**Всегда можно найти альтернативу слежке**

Естественно, система слежения не может быть востребована абсолютно во всех организациях. Во-первых, многие люди в принципе не согласятся работать в компании, где за ними так жестко следят, и их можно понять. Во-вторых, многие (особенно люди творческих профессий) работают «на результат» и никого не волнует, как они этого результата добиваются. Так что каждый руководитель для себя должен решить сам – стоит ли таким образом контролировать сотрудника. Или, может, лучше работать над повышением лояльности и качеством подбора персонала?

**За топ-менеджером – особый контроль**

Это необходимо в том случае, если есть существенные подозрения, что топ-менеджер, к примеру, передает конфиденциальную информацию или замечен во взаимосвязях с рейдерами. Тогда стоит проводить тотальный мониторинг: видеонаблюдение, прослушку телефона, контроль за активностью в Интернете. Не лишним будет приставить к такому руководителю «своего человека». Причем делать все это нужно незамедлительно! Игра стоит свеч.

**Если видеокамера зафиксировала преступление**

Предположим, сотрудники службы безопасности информировали Вас о краже, мошенничестве, умышленном уничтожении или повреждении имущества, либо о другом уголовно наказуемом преступлении. Посоветуйте руководству компании обратиться с заявлением в правоохранительные органы. Не стоит пытаться действовать самостоятельно, так как ваша компания не имеет права вести скрытое наблюдение в офисе, даже если речь идет о криминале. На это есть право только у оперативных подразделений госорганов ([ст. 13](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=902313805&anchor=ZA023LG3GO#ZA023LG3GO) и [ч. 5 ст. 6](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=902313805&anchor=ZA01HGE337#ZA01HGE337) ФЗ от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»). Но даже если Вы представите запись, сделанную скрытой камерой, она не будет принята правоохранительными органами или судом как доказательство. Ведь они получены с нарушением требований законодательства. Правда, не всегда дело доходит до суда. Как рассказала Оксана МОРОЗОВА, HR-директор RosLogistics, нередко записи, уличающие сотрудника в преступлении, используются неофициально, чтобы побеседовать с вредителем и расстаться.

**Если сотрудник постоянно нарушает дисциплину**

На основании только материалов системы слежения уволить нарушителя нельзя. Причина та же – записи не признаются доказательствами. Судебная практика тому подтверждение.

**Пример**

В рамках судебного разбирательства работодатель предъявил видеозапись, из которой явно следовало, что официант грубо общался с клиентом, не оказал ему услуги. Это означает, что официант не выполнил свои служебные обязанности, совершил дисциплинарный проступок. При этом представитель работодателя отметил, что устройства видеозаписи установлены в зале ресторана, то есть в месте общего пользования, где не предполагается частной жизни работника. Однако суд встал на сторону работника и восстановил его на работе. Судья мотивировал такое решение тем, что доказательства, представленные работодателем, были получены с нарушением закона. Поэтому они не имеют юридической силы ([ст. 60 ГПК РФ](https://e.hr-director.ru/npd-doc.aspx?npmid=99&npid=902314342&anchor=ZA01RSA3FD#ZA01RSA3FD)) и не могут являться основанием для наложения дисциплинарной ответственности на работника – увольнения. А иных доказательств у работодателя не было.

Чтобы уволить сотрудника, действуйте традиционно: составляйте акты о нарушении, требуйте объяснительные записки у работника, делайте замечания, выносите выговоры.

**Чтобы не было произвола со стороны службы безопасности**

Сотрудники этой службы, получив функции контроля над остальными работниками, попадают в некую «привилегированную касту». Чтобы они действовали тактично и в правовом русле, во-первых, в обязательном порядке ознакомьте их под роспись с положением о защите персональных данных. Во-вторых, четко регламентируйте функции сотрудников службы безопасности. Важно определить перечень лиц, имеющих право собирать информацию, обрабатывать ее, просматривать и распространять. К примеру, установите, что просматривать видеозапись может только генеральный директор и непосредственный руководитель. В-третьих, работу тех, «чья служба и опасна и трудна», тоже контролируйте, в том числе с помощью мониторинга. И пусть они об этом не забывают!

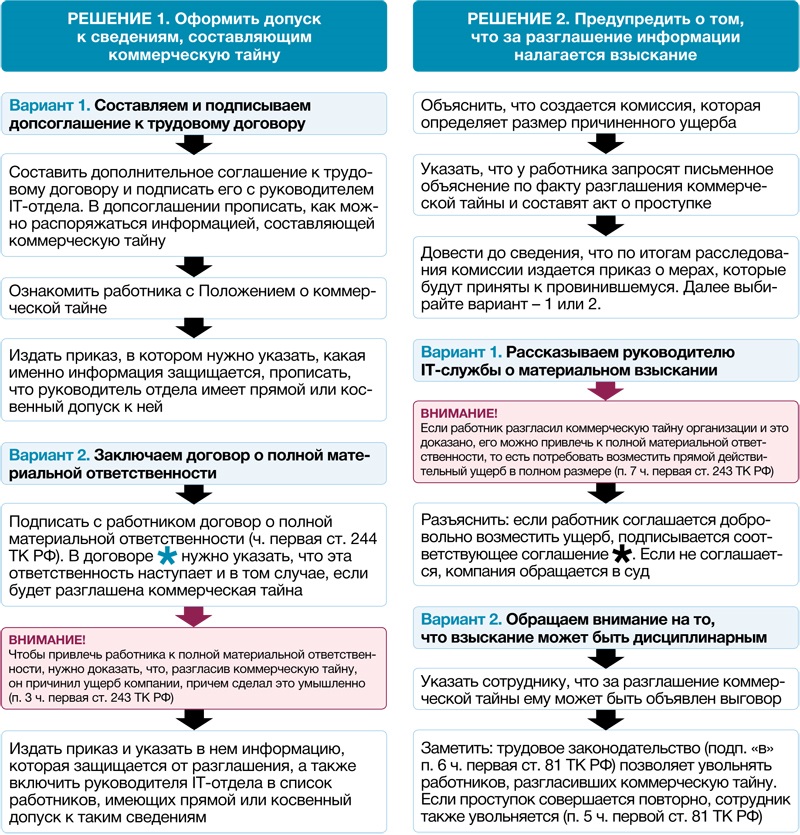
**Если Вы решили следить за персоналом**

Обратите внимание на следующие советы:

1. Взвесьте еще раз все за и против наблюдений за сотрудниками: возможные негативные последствия и позитивный эффект. Как они соотносятся? Если перевешивает негатив, подумайте об альтернативных методах.  
2. Стоит ли овчинка выделки в финансовом смысле: покроют ли выгоды от введения системы наблюдения затраты на нее?  
3. Объясните сотрудникам, чем вызвана необходимость наблюдения (не раскрывая всех секретов, например необходимости понять, кто ворует).  
4. Не проводите наблюдение там, где сотрудники должны быть в интимной уединенной обстановке, например в туалете, раздевалке, сауне (если, конечно, нет оснований подозревать кого-то в серьезном уголовном преступлении).  
5. Выделите помещение без системы слежения, чтобы там сотрудники могли решить без лишних глаз и ушей срочные личные проблемы (поставьте телефон, компьютер с доступом в Интернет).

# Новый руководитель IT-отдела будет иметь доступ к важной информации.

**Как не допустить утечки**



\* Договор о полной материальной ответственности заключается не произвольно, а по форме, утвержденной Постановлением Минтруда России от 31 декабря 2002 г. № 85.  
\* Если работник отказывается возмещать ущерб, работодатель вправе удержать его, но в размере, не превышающем средний месячный заработок сотрудника (ч. первая ст. 248 ТК РФ).

# Никак не избавиться от воровства

14.06.2017

Почему в вашей компании незаметно растет число воров, и как с этим можно по-настоящему серьезно бороться — истории из практики от Олега Щербатых, президента «Уральской ассоциации полиграфологов».

[**Олег Щербатых**](http://ekb.dk.ru/wiki/scherbatyh-oleg#binding)**, президент «**[**Уральской ассоциации полиграфологов**](http://ekb.dk.ru/wiki/uralskaya-assotsiatsiya-poligrafologov#binding)**»:**

— У одного крупного российского банка была в свое время рекламная кампания под девизом «Честным быть выгодно». Серия рекламных роликов этого банка строилась вокруг того, чтобы показать зрителям жизненные ситуации, в которых сами зрители наверняка бы соврали, в которых соврать кажется всеми принимаемым выходом. А герой ролика неожиданно говорил правду и получал бонус. К сожалению, кампания была и прошла, а вот проблема осталась.

В подавляющем числе корпоративных культур в российском бизнесе ложь — нормальная, и часто даже поощряемая, практика.

Руководители компании не понимают, что, поощряя маленькую ложь, допуская такую ложь, они взращивают катастрофическую культуру — культуру воровства и безразличия. А это уже имеет не моральные, а очень и очень материальные последствия.

Я профессионально занимаюсь расследованием и предотвращением преступлений в бизнесе, и меня все больше и больше интересует проблема — как в головах людей формируется и крепнет уверенность, что красть можно? Почему они решают, что рассказывать о преступлении другого — сомнительное решение, и лучше не лезть не в свое дело?

Возьмем, к примеру, случай из практики. Продуктовый магазин, сотрудники которого считали, что, раз они работают без обеда, можно взять себе бесплатно продуктов, выбрать колбаску подороже или рыбку копченую, а может, и маленькую бутылочку коньяка в конце рабочей смены коллективом выпить. И никто из пяти продавцов не считал это зазорным, и даже вопросы про воровство их особо не волновали, каждый из них считал это мелочью, недостойной внимания. Никто из них, съедая продуктов на 100-150 руб. в день, не считал себя вором, а на вопрос: «Как же недостача?» отвечали, глядя честными глазами: «А мы ее перекрываем — где-то покупателю поменьше завесим, где-то товар подороже продадим».

Как это отражается на имидже магазина, никого особо не волновало, но бизнес начинал нести убытки гораздо более серьезные, чем кажется. Потому что клиенты, постеснявшиеся поднимать скандал, больше в этот магазин не ходили и своим знакомым не советовали. Соответственно, выручка падала, магазин нес не только прямые убытки, но и репутационные. И главное — никто из работников не считал, что делает что-то плохое.

А бывает, люди чем-то обижены, считают, что им мало платят или что они перерабатывают, но боятся сказать об этом руководству: лучше они соврут, лишний раз улыбнутся, ведь правда не приветствуется. И тогда они начинают из собственных эгоистичных соображений добирать деньги, продукты, излишки товара, оправдывая себя тем, что это руководство им не доплачивает или много с них требует. Такие и называют причины: мало платят или плохо относятся. А на вопрос — почему же вы тогда здесь работаете, почему бы вам не поискать работу с более высокой мотивацией — отвечают, что везде так.

В лживой культуре существует уверенность, что руководитель — всегда самодур или жадина, мол, все начальники хотят, чтобы работник много работал и мало получал.

Моя хата с краю: работая над расследованием преступлений, приходилось сталкиваться с людьми, которые сами не принимали участия в преступлении, но знали, кто его совершил или кто причастен. Но получить от них помощь в расследовании никак не получалось. Они считали: «раз я преступления не совершал, то я и непричастен, а помогать я никому не обязан». Мотивация этих людей простая: я — не стукач. Это можно понять, когда работаешь с рецидивистами или людьми, которые отбывали наказания в местах лишения свободы. Мол, им «по статусу» не положено помогать сотрудникам полиции или администрации (если они это делают, то только тайком). Но невозможно понять, почему так поступает работник, который получает зарплату на предприятии, и почему он так наплевательски относится к материальным ценностям компании.

Я в случаях желания отсидеться, не рассказывать о преступлениях других, всегда напоминаю людям: первой начинают гореть те хаты, которые с краю.

Иногда люди боятся сказать правду, потому что им кажется, что воруют все вокруг. На предприятии, производящем молочную продукцию, группа людей в сговоре специально понижали жирность молока, которое шло в продажу, а излишки продукции сбывали по «серым» схемам. Недостач на предприятии не было, все выглядело нормальным, были ли претензии от покупателей по поводу качества молока, мне доподлинно неизвестно. И все бы это продолжалось еще долгие годы, если бы однажды ко мне не попала бывшая сотрудница этого предприятия, которая и рассказала об этих схемах. Она уже не работала в компании, и, устраиваясь в другую организацию, поделилась со мной, что и как происходило на заводе. Я спросил у нее, почему она не сказала об этом руководству или службе безопасности компании. Ее ответ был следующий: она боялась этих людей, прямого доступа к директору у нее не было, она не знала точно, была ли служба безопасности «в доле», кто именно получал с этого прибыль. В итоге она решила для себя, что ей проще уволиться, чем поднимать это вопрос.

Таких случаев в моей практике десятки, если не сотни, и везде одно и то же. Я, конечно, понимаю, что выгляжу несколько наивно с призывами бороться с ложью, но ведь я говорю не про абстрактную честность.

Я говорю о том, что, если вы как руководитель приложите усилия для формирования в своем бизнесе корпоративной культуры, укрепляющей роль открытости, честности, вы сможете избежать гигантского количества реальных и потенциальных рисков.

Сможете сэкономить миллионы рублей. Задумайтесь над этим вопросом, проанализируйте, как и что стоит изменить в корпоративной культуре компании, и для вас лозунг «честным быть выгодно» обретет всю полноту его материального смысла.

# Сотрудники всегда крадут

09.03.2016

Как воруют у работодателей Екатеринбурга те, кого никто не подозревает? ОПЫТ борьбы с «честными» воришками специально для DK.RU от Олега Щербатых, президента «Уральской ассоциации полиграфологов».

[Олег Щербатых](http://ekb.dk.ru/wiki/scherbatyh-oleg#binding), президент «[Уральской ассоциации полиграфологов](http://ekb.dk.ru/wiki/uralskaya-assotsiatsiya-poligrafologov#binding)»:

— В моей работе есть особая категория случаев — ситуации, когда у работодателей воруют самые, казалось бы, надежные сотрудники или те, кто должен охранять ценности компании. Я долго пытался понять, что же все эти случаи объединяет.

К примеру, мы недавно проводили проверку отдела логистики крупного предприятия на предмет сговора логистов с перевозчиками. В отделе есть парень, трудится в компании не первый год на должности с невысокой зарплатой. Уже «пересидел» многих начальников. Те, кто пришел в одно время с ним, успели стать ведущими специалистами, руководителями проектов и т.д. А он вроде бы ни к чему не стремился, карьеры не делал, повышения зарплаты не просил.

Работал парень точно, стабильно, аккуратно. Идеальный сотрудник!

Только что-то мне показалось подозрительным в этой идеальности. Вскоре я узнал, что он курит дорогие сигареты, у него айфон последней модели, дорогая одежда. И еще почему-то за все время работы он ни разу не уходил в отпуск или на больничный. Стали разбираться. В его задачи входило, в том числе, выставление претензий поставщикам по пропавшим и порченым грузам. Что делал парень? Он просто договорился с поставщиками и регулярно менял цифры в претензиях, отправлял их не по адресу, а иногда, например, запятую переставлял не туда. Конечно же, в ущерб интересам нанимателя. **Такие «безобидные» махинации приносили ему каждый месяц доход, в несколько раз превышавший зарплату.**

А вот еще история про правильного, старательного сотрудника.

Очень добросовестный и ответственный начальник склада в магазине электроники так «оберегал» товар, что по всякому поводу и без отправлял хорошую, исправную технику в сервисный отдел.

Там ее проверяли, давали подтверждение, что все работает хорошо, претензий нет. После этого ставили штамм сервисного отдела и отправляли обратно в магазин. В чем подвох? А в том, что по правилам компании на такую технику делалась скидка 80% от цены продажи, ведь [фирма](http://www.dk.ru/wiki/solomon-yuridicheskaya-firma#binding) была заинтересована в освобождении склада от того, что по документам числилось как «хлам». Начальник же склада в это время звонил знакомым перекупщикам и продавал им технику с солидным дисконтом, забирая себе разницу. За время такой «добросовестной» работы он купил квартиру сыну, каждый год раза по два летал за границу отдыхать — в общем, ни в чем себе не отказывал.

**Не меньше, чем «честняки», стараются в свою пользу и сотрудники охраны.**

Вот казалось бы невинный процесс — продажа попкорна в кинотеатре. Не каждый из нас берет чеки при такой покупке. В то же время прибыль от продажи попкорна может исчисляться сотнями процентов. Провести учет попкорна можно только контролируя тару, которая используется в кинотеатре. В одном из кинотеатров Екатеринбурга продавцы вступили в сговор с охраной предприятия и стали приносить на работу продукцию, реализуя ее через бар. А охранники предприятия не просто «закрывали на это глаза», но еще и помогали проносить продукцию. И началось все с любовной истории между охранником и сотрудницей бара. При проверке выяснилось, что в выходной или праздничный день незаконный доход составлял около 10 тыс. рублей.

И уже на следующие выходные после ликвидации такой схемы прибыль владельца кинотеатра по продажам попкорна увеличилась на 20%.

Еще «веселее» бывает, когда охрана начинает особо старательно «бороться» с воровством. Например, в большинстве компаний для борьбы с нечистоплотностью при проведении закупок составляется конкурентный лист предложений по поставкам. В нем сравнивают предложения поставщиков, отсрочки, платежи и т.п. Для того чтобы исключить сговор, всю эту информацию должна проверять служба безопасности.

Но в случае с товарами, которые массово закупаются для самой борьбы с воровством (противокражные ворота, противокражные этикетки на товар и т.п.), служба безопасности – сама и закупщик, и проверяющий.

Что в результате? Конечно, массовые откаты. К примеру, по недавнему опыту одной из компаний суммы откатов при приобретении противокражного оборудования составляли до 300 тыс. рублей в месяц.

И таких случаев в моей практике очень и очень много. Присмотритесь к самым лучшим своим сотрудникам. За их «идеальностью» может скрываться немало интересного. Поверьте —  если украсть можно, рано или поздно воровать начнут. Анализируя такие случаи, я сделал для себя простой вывод: система контроля должна быть многоуровневой и максимально скрытой. И даже тогда нужно периодически перетрясать кадры. Вы скажете, что так и до паранойи недалеко, а я отвечу:

Легкая паранойя – неизбежный удел каждого собственника.

Если он, конечно, хочет таковым остаться. Можно сколько угодно говорить про честность людей, про их порядочность, но это всегда будут счастливые исключения, а конфликт труда и капитала никто не отменял. Тот, кто работает, всегда стремится взять у того, кто владеет, чуточку больше. Только кто-то пачку бумаги выносит из офиса, а кто-то товара на миллионы в свою пользу списывает.

# Ваши сотрудники крадут?

09.03.2016

Как воруют у работодателей Екатеринбурга те, кого никто не подозревает? ОПЫТ борьбы с «честными» воришками специально для DK.RU от Олега Щербатых, президента «Уральской ассоциации полиграфологов».

[Олег Щербатых](http://ekb.dk.ru/wiki/scherbatyh-oleg#binding), президент «[Уральской ассоциации полиграфологов](http://ekb.dk.ru/wiki/uralskaya-assotsiatsiya-poligrafologov#binding)»:

— В моей работе есть особая категория случаев — ситуации, когда у работодателей воруют самые, казалось бы, надежные сотрудники или те, кто должен охранять ценности компании. Я долго пытался понять, что же все эти случаи объединяет.

К примеру, мы недавно проводили проверку отдела логистики крупного предприятия на предмет сговора логистов с перевозчиками. В отделе есть парень, трудится в компании не первый год на должности с невысокой зарплатой. Уже «пересидел» многих начальников. Те, кто пришел в одно время с ним, успели стать ведущими специалистами, руководителями проектов и т.д. А он вроде бы ни к чему не стремился, карьеры не делал, повышения зарплаты не просил.

Работал парень точно, стабильно, аккуратно. Идеальный сотрудник!

Только что-то мне показалось подозрительным в этой идеальности. Вскоре я узнал, что он курит дорогие сигареты, у него айфон последней модели, дорогая одежда. И еще почему-то за все время работы он ни разу не уходил в отпуск или на больничный. Стали разбираться. В его задачи входило, в том числе, выставление претензий поставщикам по пропавшим и порченым грузам. Что делал парень? Он просто договорился с поставщиками и регулярно менял цифры в претензиях, отправлял их не по адресу, а иногда, например, запятую переставлял не туда. Конечно же, в ущерб интересам нанимателя. **Такие «безобидные» махинации приносили ему каждый месяц доход, в несколько раз превышавший зарплату.**

А вот еще история про правильного, старательного сотрудника.

Очень добросовестный и ответственный начальник склада в магазине электроники так «оберегал» товар, что по всякому поводу и без отправлял хорошую, исправную технику в сервисный отдел.

Там ее проверяли, давали подтверждение, что все работает хорошо, претензий нет. После этого ставили штамм сервисного отдела и отправляли обратно в магазин. В чем подвох? А в том, что по правилам компании на такую технику делалась скидка 80% от цены продажи, ведь [фирма](http://www.dk.ru/wiki/solomon-yuridicheskaya-firma#binding) была заинтересована в освобождении склада от того, что по документам числилось как «хлам». Начальник же склада в это время звонил знакомым перекупщикам и продавал им технику с солидным дисконтом, забирая себе разницу. За время такой «добросовестной» работы он купил квартиру сыну, каждый год раза по два летал за границу отдыхать — в общем, ни в чем себе не отказывал.

**Не меньше, чем «честняки», стараются в свою пользу и сотрудники охраны.**

Вот казалось бы невинный процесс — продажа попкорна в кинотеатре. Не каждый из нас берет чеки при такой покупке. В то же время прибыль от продажи попкорна может исчисляться сотнями процентов. Провести учет попкорна можно только контролируя тару, которая используется в кинотеатре. В одном из кинотеатров Екатеринбурга продавцы вступили в сговор с охраной предприятия и стали приносить на работу продукцию, реализуя ее через бар. А охранники предприятия не просто «закрывали на это глаза», но еще и помогали проносить продукцию. И началось все с любовной истории между охранником и сотрудницей бара. При проверке выяснилось, что в выходной или праздничный день незаконный доход составлял около 10 тыс. рублей.

И уже на следующие выходные после ликвидации такой схемы прибыль владельца кинотеатра по продажам попкорна увеличилась на 20%.

Еще «веселее» бывает, когда охрана начинает особо старательно «бороться» с воровством. Например, в большинстве компаний для борьбы с нечистоплотностью при проведении закупок составляется конкурентный лист предложений по поставкам. В нем сравнивают предложения поставщиков, отсрочки, платежи и т.п. Для того чтобы исключить сговор, всю эту информацию должна проверять служба безопасности.

Но в случае с товарами, которые массово закупаются для самой борьбы с воровством (противокражные ворота, противокражные этикетки на товар и т.п.), служба безопасности – сама и закупщик, и проверяющий.

Что в результате? Конечно, массовые откаты. К примеру, по недавнему опыту одной из компаний суммы откатов при приобретении противокражного оборудования составляли до 300 тыс. рублей в месяц.

И таких случаев в моей практике очень и очень много. Присмотритесь к самым лучшим своим сотрудникам. За их «идеальностью» может скрываться немало интересного. Поверьте —  если украсть можно, рано или поздно воровать начнут. Анализируя такие случаи, я сделал для себя простой вывод: система контроля должна быть многоуровневой и максимально скрытой. И даже тогда нужно периодически перетрясать кадры. Вы скажете, что так и до паранойи недалеко, а я отвечу:

Легкая паранойя – неизбежный удел каждого собственника.

Если он, конечно, хочет таковым остаться. Можно сколько угодно говорить про честность людей, про их порядочность, но это всегда будут счастливые исключения, а конфликт труда и капитала никто не отменял. Тот, кто работает, всегда стремится взять у того, кто владеет, чуточку больше. Только кто-то пачку бумаги выносит из офиса, а кто-то товара на миллионы в свою пользу списывает.

# Воровство – как избавиться

14.06.2017

Почему в вашей компании незаметно растет число воров, и как с этим можно по-настоящему серьезно бороться — истории из практики от Олега Щербатых, президента «Уральской ассоциации полиграфологов».

[**Олег Щербатых**](http://ekb.dk.ru/wiki/scherbatyh-oleg#binding)**, президент «**[**Уральской ассоциации полиграфологов**](http://ekb.dk.ru/wiki/uralskaya-assotsiatsiya-poligrafologov#binding)**»:**

— У одного крупного российского банка была в свое время рекламная кампания под девизом «Честным быть выгодно». Серия рекламных роликов этого банка строилась вокруг того, чтобы показать зрителям жизненные ситуации, в которых сами зрители наверняка бы соврали, в которых соврать кажется всеми принимаемым выходом. А герой ролика неожиданно говорил правду и получал бонус. К сожалению, кампания была и прошла, а вот проблема осталась.

В подавляющем числе корпоративных культур в российском бизнесе ложь — нормальная, и часто даже поощряемая, практика.

Руководители компании не понимают, что, поощряя маленькую ложь, допуская такую ложь, они взращивают катастрофическую культуру — культуру воровства и безразличия. А это уже имеет не моральные, а очень и очень материальные последствия.

Я профессионально занимаюсь расследованием и предотвращением преступлений в бизнесе, и меня все больше и больше интересует проблема — как в головах людей формируется и крепнет уверенность, что красть можно? Почему они решают, что рассказывать о преступлении другого — сомнительное решение, и лучше не лезть не в свое дело?

Возьмем, к примеру, случай из практики. Продуктовый магазин, сотрудники которого считали, что, раз они работают без обеда, можно взять себе бесплатно продуктов, выбрать колбаску подороже или рыбку копченую, а может, и маленькую бутылочку коньяка в конце рабочей смены коллективом выпить. И никто из пяти продавцов не считал это зазорным, и даже вопросы про воровство их особо не волновали, каждый из них считал это мелочью, недостойной внимания. Никто из них, съедая продуктов на 100-150 руб. в день, не считал себя вором, а на вопрос: «Как же недостача?» отвечали, глядя честными глазами: «А мы ее перекрываем — где-то покупателю поменьше завесим, где-то товар подороже продадим».

Как это отражается на имидже магазина, никого особо не волновало, но бизнес начинал нести убытки гораздо более серьезные, чем кажется. Потому что клиенты, постеснявшиеся поднимать скандал, больше в этот магазин не ходили и своим знакомым не советовали. Соответственно, выручка падала, магазин нес не только прямые убытки, но и репутационные. И главное — никто из работников не считал, что делает что-то плохое.

А бывает, люди чем-то обижены, считают, что им мало платят или что они перерабатывают, но боятся сказать об этом руководству: лучше они соврут, лишний раз улыбнутся, ведь правда не приветствуется. И тогда они начинают из собственных эгоистичных соображений добирать деньги, продукты, излишки товара, оправдывая себя тем, что это руководство им не доплачивает или много с них требует. Такие и называют причины: мало платят или плохо относятся. А на вопрос — почему же вы тогда здесь работаете, почему бы вам не поискать работу с более высокой мотивацией — отвечают, что везде так.

В лживой культуре существует уверенность, что руководитель — всегда самодур или жадина, мол, все начальники хотят, чтобы работник много работал и мало получал.

Моя хата с краю: работая над расследованием преступлений, приходилось сталкиваться с людьми, которые сами не принимали участия в преступлении, но знали, кто его совершил или кто причастен. Но получить от них помощь в расследовании никак не получалось. Они считали: «раз я преступления не совершал, то я и непричастен, а помогать я никому не обязан». Мотивация этих людей простая: я — не стукач. Это можно понять, когда работаешь с рецидивистами или людьми, которые отбывали наказания в местах лишения свободы. Мол, им «по статусу» не положено помогать сотрудникам полиции или администрации (если они это делают, то только тайком). Но невозможно понять, почему так поступает работник, который получает зарплату на предприятии, и почему он так наплевательски относится к материальным ценностям компании.

Я в случаях желания отсидеться, не рассказывать о преступлениях других, всегда напоминаю людям: первой начинают гореть те хаты, которые с краю.

Иногда люди боятся сказать правду, потому что им кажется, что воруют все вокруг. На предприятии, производящем молочную продукцию, группа людей в сговоре специально понижали жирность молока, которое шло в продажу, а излишки продукции сбывали по «серым» схемам. Недостач на предприятии не было, все выглядело нормальным, были ли претензии от покупателей по поводу качества молока, мне доподлинно неизвестно. И все бы это продолжалось еще долгие годы, если бы однажды ко мне не попала бывшая сотрудница этого предприятия, которая и рассказала об этих схемах. Она уже не работала в компании, и, устраиваясь в другую организацию, поделилась со мной, что и как происходило на заводе. Я спросил у нее, почему она не сказала об этом руководству или службе безопасности компании. Ее ответ был следующий: она боялась этих людей, прямого доступа к директору у нее не было, она не знала точно, была ли служба безопасности «в доле», кто именно получал с этого прибыль. В итоге она решила для себя, что ей проще уволиться, чем поднимать это вопрос.

Таких случаев в моей практике десятки, если не сотни, и везде одно и то же. Я, конечно, понимаю, что выгляжу несколько наивно с призывами бороться с ложью, но ведь я говорю не про абстрактную честность.

Я говорю о том, что, если вы как руководитель приложите усилия для формирования в своем бизнесе корпоративной культуры, укрепляющей роль открытости, честности, вы сможете избежать гигантского количества реальных и потенциальных рисков.

Сможете сэкономить миллионы рублей. Задумайтесь над этим вопросом, проанализируйте, как и что стоит изменить в корпоративной культуре компании, и для вас лозунг «честным быть выгодно» обретет всю полноту его материального смысла.

# Как правильно ввести систему видеонаблюдения в организации?

Видеонаблюдение в организациях – обычная вещь.

Введение системы видеонаблюдения помогает работодателю контролировать и безопасность в помещениях, и продуктивность использования работниками своего рабочего времени, и даже в определенных случаях может стать основанием для привлечения работника к дисциплинарной ответственности. Однако вводить видеонаблюдение в организации необходимо, учитывая определенные нюансы.

Главным образом, важно учитывать, что видеоизображение работника относится к его персональным данным, что по общему правилу требует согласия на обработку персональных данных.

В то же время, это не значит, что если работник отказывается давать такое согласие, то работодатель автоматически лишается возможности ввести в своей компании систему видеонаблюдения.

Так, на практике превалирует следующая позиция: даже при отсутствии согласия на обработку биометрических персональных данных всех работников организации работодатель все равно может ввести систему видеонаблюдения. Правда, в случае спора с работником работодателю нужно будет подтвердить, что видеозапись использовалась исключительно в таких целях, как проверка эффективности производственного, контроль и учет рабочего времени работников, рациональное использование работниками рабочего времени, повышение производительности труда. Указанное подтверждается судебной практикой (см., например, Апелляционное определение Волгоградского областного суда от 29.08.2014 по делу №33-8937/2014).

В данном случае судами признается, что ведение видео- и аудиофиксации не нарушают основные конституционные права работников, так как видеозапись рабочего процесса не является раскрытием персональных данных работника и не используется для того, чтобы установить обстоятельства его частной жизни либо его личную и семейную тайну (см., например, Апелляционное определение Оренбургского областного суда от 3 декабря 2014 г. по делу №33-7039/2014, Апелляционное определение Московского городского суда от 08.12.2016 №33-49698/2016, Апелляционное определение Саратовского областного суда от 18 октября 2012 г. по делу №33-5946/2012).

Вместе с тем, советуем обратить внимание на Разъяснения Роскомнадзора «О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки» (которые, тем не менее, не являются нормативным правовым актом), согласно которым при ведении видеонаблюдения в рабочих помещениях оператора с целью фиксации возможных действий противоправного характера согласно ст. 74 Трудового кодекса Российской Федерации работники должны быть уведомлены об изменении условий трудового договора по причинам, связанным с изменением организационных или технологических условий труда (введением видеонаблюдения), под роспись.

Кроме того, если в целях охраны безопасности в организации работодатель нанимает стороннюю охранную организацию, следует учитывать еще и часть третью статьи 12 Закона РФ от 11.03.1992 №2487-1 «О частной детективной и охранной деятельности в Российской Федерации» согласно которой в случае оказания охранных услуг с использованием видеонаблюдения, а также оказания охранных услуг в виде обеспечения внутриобъектового и (или) пропускного режимов персонал и посетители объекта охраны должны быть проинформированы об этом посредством размещения соответствующей информации в местах, обеспечивающих гарантированную видимость в дневное и ночное время, до входа на охраняемую территорию. Такая информация должна содержать сведения об условиях внутриобъектового и пропускного режимов.

При этом видеонаблюдение в помещениях организации следует осуществлять только для конкретных и заранее определенных целей. Эти цели должны быть обусловлены соответствующими нормативными правовыми актами, устанавливающими правовые основания видеонаблюдения. Например, у нас в офисе Института Профессионального Кадровика установлены камеры,

Автор: Мария Финатова, Юрист-партнер группы компаний Валентины Митрофановой

# 60% российских компаний ловят увольняемых сотрудников на краже информации. Как не попасть в их число?

Сергей Ожегов, Генеральный Директор компании «СерчИнформ», Москва

Справка

Сергей Ожегов окончил механико-математический факультет БГУ. В компании, которой сейчас руководит, начал работать сразу после окончания вуза. Первая должность – менеджер по продажам, затем вырос до коммерческого директора. С 2015 года работает в нынешней должности. Постоянный спикер конференций в сфере информационной безопасности.

ООО «СерчИнформ»

Сфера деятельности: разработка средств информационной безопасности

Численность персонала: 250

Территория: головной офис – в Москве; дополнительные офисы – в Екатеринбурге, Казани, Новосибирске, Санкт-Петербурге, Хабаровске, Алма-Ате (Казахстан), Киеве (Украина), Минске (Белоруссия)

Общая выручка от продажи продуктов и услуг по направлению DLP: 856 млрд руб. (в 2015 году)

Более 60% российских компаний ловят увольняемых сотрудников на краже информации. Люди совершают такие преступления из-за обиды или чтобы получить преимущество в поиске работы у конкурентов.

Ситуация 1. Сотрудник удаляет ценные документы. Бухгалтера рекламного агентства попросили уволиться по собственному желанию. Предложение попрощаться было мирным, сотруднице дали время на поиск новой работы, но от ее мести компанию это не спасло. Перед увольнением бухгалтер удалила документы, на восстановление которых у фирмы ушло больше двух месяцев. Далее выяснилось, что новым работодателем обиженной стал крупный клиент агентства. Вскоре он отказался от услуг рекламодателя, наслушавшись фальшивой «подноготной» агентства от новой сотрудницы.

Ситуация 2. Сотрудник крадет данные для трудоустройства на новое место. Работницу автоцентра поймали на пересылке закрытых данных с корпоративной почты на личную. Среди прочего письмо содержало персональные данные коллег и клиентов. В объяснительной нарушительница указала, что информация нужна ей для написания диплома на тему «Влияние политики руководства компании на настроения в коллективе». А через пару дней служба безопасности перехватила письмо, из которого следовало, что сотрудница ведет переговоры о трудоустройстве на новое место – в страховую компанию. И база персональных данных – ее «пропуск» в эту фирму. Мошенницу уволили.

Ситуация 3. Сотрудник блокирует работу организации. Логистическая компания попрощалась с системным администратором: тот требовал увеличения зарплаты, хотя оснований для этого не было. Расставание прошло гладко, но вскоре система компании «легла». Уходя, «недооцененный» сотрудник загрузил в систему файл-бомбу – программу с отложенным запуском. Через две недели она активировалась и стерла конфигурации сетевого оборудования: сотрудники не могли получить почту, распечатать документы и выйти в интернет, а все звонки клиентов переадресовывались директору. На полноценное восстановление работы компании ушел месяц.

Также читайте

«Какая мотивация нужна Вашим сотрудникам? Есть точный ответ»

Как защитить данные: самые доступные способы

Я начинаю защиту информации еще на стадии подбора сотрудников.

Анализирую мотивы и опыт соискателя. Менеджер по продажам на собеседовании предлагает клиентскую базу с прошлой работы? Следующему работодателю он предложит моих клиентов. Специалист по закупкам нигде не задерживался больше года? Среди таких есть люди, которые увольняются, чтобы их не успели поймать на воровстве. Кандидатов, которые вызывают у меня подобные подозрения, на работу не беру.

Также читайте

«"Сотрудники страшнее конкурентов": пять секретов управления Майкла Делла»

Фиксирую в трудовом договоре согласие сотрудников нести ответственность за защиту конфиденциальной информации. По данным нашего исследования, так поступают в 86% компаний. Обязательства сотрудника выглядят так:

не разглашать сведения, составляющие коммерческую тайну, которые будут доверены или станут известны в ходе выполнения должностных обязанностей;

не передавать третьим лицам и не раскрывать публично сведения, составляющие коммерческую тайну, без согласия компании;

выполнять требования приказов, инструкций и положений по обеспечению сохранности коммерческой тайны;

в случае попытки посторонних лиц получить сведения о коммерческой тайне сообщить об этом руководству компании;

сохранять коммерческую тайну тех предприятий, с которыми организация имеет деловые отношения;

не использовать знание коммерческой тайны для занятий любой деятельностью, которая может нанести ущерб компании;

в случае увольнения передать руководству компании все носители коммерческой тайны;

немедленно сообщать руководству компании об утере носителей коммерческой тайны, удостоверений, пропусков, ключей от режимных помещений, хранилищ и т. д., которые могут привести к ее разглашению.

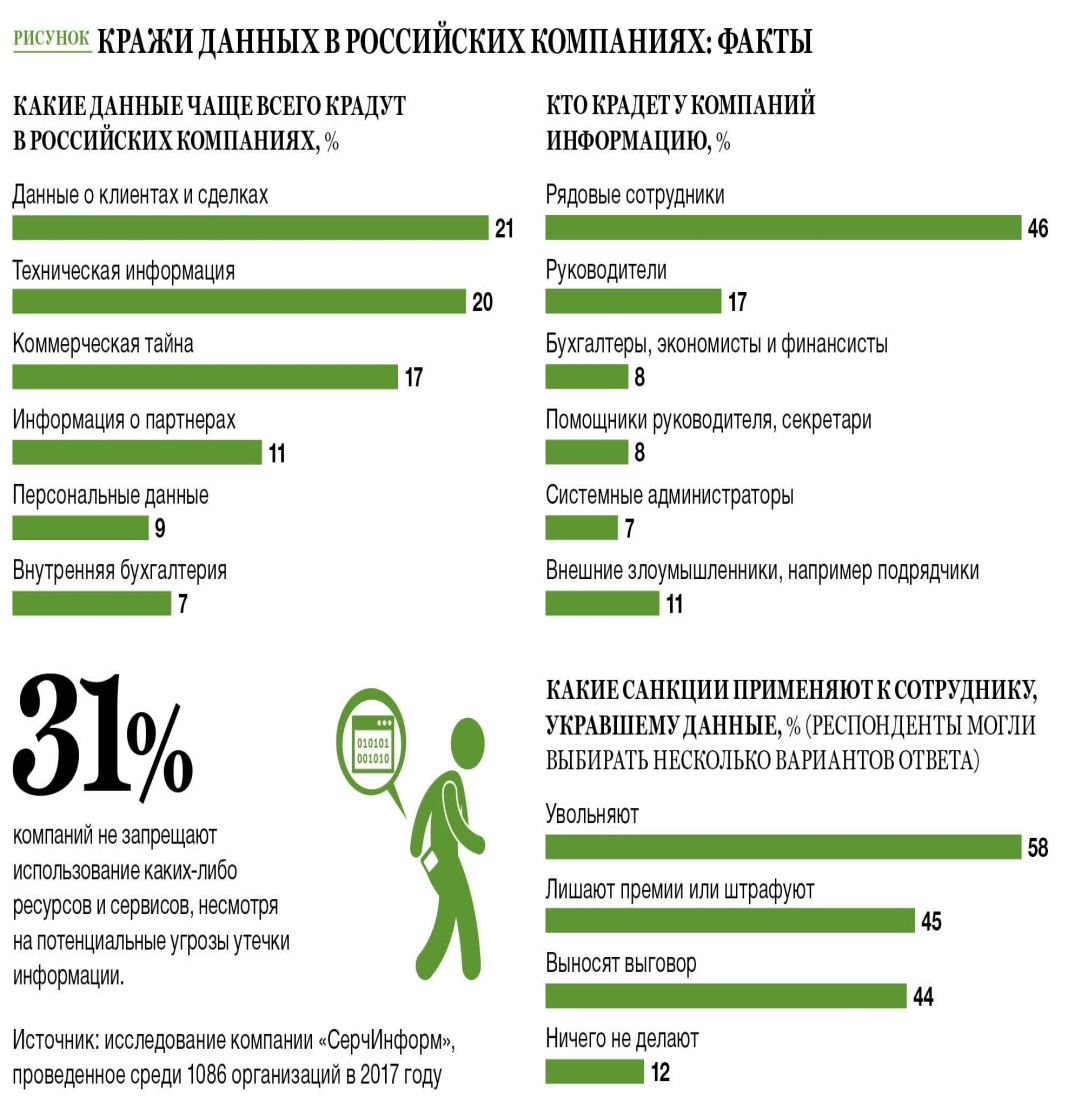
Также читайте

«Хотите выявить скрытый потенциал бизнеса?»

Распределяю сотрудников по группам риска. Есть люди, потенциально опасные для компании. Азартные игроки могут украсть, чтобы вложиться в игру, должники – чтобы отдать долг. «Пропуском» в группу риска становится дружба с экс-сотрудниками и конкурентами, негативное мнение о руководстве или недовольство зарплатой. Наша кадровая служба и служба безопасности анализируют страницы сотрудников в соцсетях, контролируют, на какие сайты заходят люди с рабочих компьютеров. Отслеживаем все действия сотрудников из групп риска с документами: что пересылают по почте, что распечатывают.

Разделяю права доступа. Человек, одержимый местью, предсказуем: он посягнет на самое ценное из того, к чему имеет доступ. Поэтому я разграничиваю права доступа. Управлять доступом к ресурсам можно стандартными средствами Microsoft, например Active Directory. С помощью настроек доступа к документам и папкам даю права чтения или редактирования только отдельным сотрудникам или отделам. Права пользователей также можно задавать для сетевых хранилищ, к примеру для FTP-сервера. Даже облачные сервисы позволяют разграничивать права пользователей. Вероятность утечки информации снижается, когда доступ к ней имеет ограниченный круг людей.

Перечисленные меры работают только в комплексе. Судите сами: режим коммерческой тайны не спасет, если обиженный линейный сотрудник будет иметь доступ к документам топ-менеджеров.



# Что делать, чтобы сотрудники не воровали

*Все более-менее крупные компании* [*сталкиваются с воровством*](https://www.vedomosti.ru/management/articles/2016/12/14/669476-samie-opasnie-moshenniki)*. Но одно дело, когда речь идет о «фантиках» — сотрудник распечатал книгу на корпоративной бумаге или взял для друзей пару комплектов презентационки. И совсем другое — если это происходит систематически и оставляет заметные дыры в бюджете. На мелочи собственники закрывают глаза, это постоянная статья расходов. Но вместе с тем допускают и крупные кражи.*

Салон авто с разветвлённой сетью дилерских центров по всей стране получил жалобу от клиента. Тот утверждал, что во время техосмотра новые детали его автомобиля заменили на старые. Расследование показало, что клиент прав, а сотрудники давно наживаются на заказчиках. Если бы не жалоба клиента и помощь специалиста-профайлера, компания могла бы узнать о мошенничестве своих из прессы и поплатиться репутацией.

Более изощренную схему придумали сотрудники другого нашего клиента. Рабочие ночной смены распечатывали две накладные на вывоз труб: в одной 4 единицы, в другой 3. Грузили в машины четыре трубы, на проходной предъявляли соответствующую накладную. По дороге одну трубу сбрасывали и позже «реализовывали», а остальные доставляли адресату по другой накладной. Стоимость одной украденной трубы составляла 1,5 миллиона рублей, так что в месяц компания теряла 6-7,5 миллионов. Обнаружить схему удалось в Skype, где мошенники обсуждали детали предстоящей операции.

Люди воруют по разным причинам: из обиды, из желания восстановить справедливость или потому что крадут всё, стремясь отомстить руководству или под давлением. Но что интересно, в 2016 году более 90% случаев мошеннических действий со стороны сотрудников российских компаний было обусловлено либо полным отсутствием внутреннего контроля, либо «дырами» в системе. Еще 37% работников, которых удалось уличить в мошенничестве, говорили, что у них для этого просто [была подходящая возможность](https://home.kpmg.com/ru/ru/home/insights/2016/12/profiles-of-the-fraudster-russia-and-the-cis-report.html).

*В управлении компанией так: либо обеспечиваешь безопасность, либо создаешь условия для мошенничества. Третьего не дано*

Если поощрять воровство не ваш план, вот ряд мер, которые работают в комплексе.

**Введите регламент**

Чётко и ясно объясните сотрудникам, что нельзя. И не бойтесь быть банальными, ведь один собственник считает присвоенную пачку чая и распечатанные документы постоянной статьей расхода, а другой готов проводить инвентаризацию и вычитать деньги из зарплаты служащих. Как людям понимать границы, если вы их не очертили?

**Пропишите правила и ответственность сотрудников во внутренних документах компании**

Как и в каких целях могут использоваться компьютеры, инструменты для работы, интеллектуальная собственность и другие ресурсы фирмы, можно прописать во внутренних инструкциях, трудовом контракте и прочих бумагах. Например, в Правилах внутреннего распорядка может появиться пункт: «Предоставляемые работнику для выполнения трудовых обязанностей ЭВМ и другая оргтехника должны использоваться исключительно для решения рабочих задач».

Если компания заинтересована не допускать краж ценной информации, следует также ввести режим коммерческой тайны. Для этого — определить перечень данных, составляющих тайну, и ограничить доступ к ним; включить в трудовые и гражданско-правовые договоры пункты о порядке обращения с конфиденциальной информацией. А после — отслеживать, кто обращается к ней.

Но кроме простых и достаточных регламентов люди должны понимать и последствия несоблюдения. Например, угроза выплатить штраф в размере 1,5 млн рублей или получить семь лет тюрьмы за воровство данных (ст. 183 УК) отбивает у сотрудников желание воровать секреты фирмы накануне увольнения.

**Контролируйте**

Иначе как вы узнаете о том, что правила не соблюдаются? Кто-то задействует СКУД и устанавливает видеонаблюдение. Другие ужесточают процедуру инвентаризации и используют DLP-систему, чтобы не допустить утечки конфиденциальных данных. Будут это программно-аппаратные или процедурные средства — зависит от специфики бизнеса. Но важно понимать, что чем больше сотрудников и правил, тем больше инструментов контроля понадобится. Чтобы защитить бизнес со штатом в несколько сотен человек, кроме инструментов контроля понадобятся и специалисты, которые возьмут эту задачу на себя, — служба безопасности.

**Наказывайте за нарушения**

Демонстрация того, что правила записаны не просто так, — сильный мотиватор к их соблюдению. Обещали штрафы, выговоры и отстранения от дел — раздавайте их всем заслужившим независимо от статуса. Такой подход докажет, что гласные и негласные правила вашей корпоративной культуры не расходятся.

**Договаривайтесь на берегу и используйте правильное позиционирование**

Объясните персоналу цели и задачи контроля, заручитесь их письменным согласием. Чтобы не демотивировать людей, обсудите с HR-отделом так называемое «позиционирование контроля» внутри коллектива. Повернув эту новость нужной стороной, вы избавитесь от многих проблем. Например, расскажите коллективу, что их переработки также будут учитываться системой, «потерянный» из-за сбоя ПК файл можно будет легко восстановить, а в случае любой неразберихи система покажет, кто действительно виноват.

**Вместо итога**

В нашей компании работа сотрудников контролируется с помощью DLP-системы, СКУДа и внутренних инструментов типа тасктрекера и CRM. Я уверен, что бесконтрольность рождает хаос, а «отношения на доверии» возможны только в небольших коллективах. Поэтому, когда дело касается бизнеса, я предпочитаю придерживаться правила «доверяй, но проверяй».

# Как спасти клиентскую базу от кражи со стороны сотрудников

Вы сможете: предотвратить кражу клиентской базы, оптимизировать методы защиты.

Сергей Соловьев, Директор компании ICL Services, Казань

Клиентская база — одна из наиболее чувствительных зон любой компании. Мы пришли к мысли о необходимости защиты клиентской базы не сразу. К счастью, явных и крупных потерь у нас не было, но пара инцидентов заставила задуматься о защите данных. Вот что мы предприняли.

Обязали сотрудников хранить тайну

Подписали соглашение о неразглашении информации о клиентской базе с каждым сотрудником. За нарушение соглашения предусмотрены штрафы в размере понесенных компанией убытков. Разработали политику по работе с конфиденциальной информацией и обязали сотрудников проходить тестирование на знание этой политики.

Вопрос на знание политики конфиденциальности

Разграничили права доступа

Для защиты информации разграничили права доступа к данным о клиентах, подготовленным коммерческим предложениям и документации по проектам. В зависимости от исполняемой роли и должности сотрудник не видит того, что происходит у других. Полная картина доступна лишь руководителю. Это уменьшает соблазн использовать или украсть чужую информацию. А если данные пропали, у службы безопасности есть список тех, кто имел доступ к документам.

Предоставили права администратора только IT-службе

Учетные записи сотрудников не имеют прав администратора. Работники не могут самостоятельно устанавливать запрещенные программы и приложения. Так мы гарантируем, что сотрудник не отредактирует, не удалит и не перешлет важные файлы на сторонний источник. Этих мер требуют наши обязательства по контрактам с международными клиентами и партнерами.

Приучили сотрудников не пересылать рабочие файлы по почте

Правила обязывают сотрудников не работать с файлами локально и не пересылать их по почте. Например, работник выполнил задачу и ему нужно, чтобы руководитель проверил документ. В этом случае исполнитель присылает в письме ссылку на место хранения файла на корпоративном сервере.

Закрепили каждого клиента за несколькими сотрудниками

С каждым клиентом взаимодействуют несколько сотрудников разных уровней принятия решений. Например, помимо продавца с клиентами работает менеджер, ответственный за представление сервиса. Регулярные встречи с заказчиком проводит руководитель соответствующего региона. Он же решает возникшие проблемы. Так сотрудник не сможет увести клиента после увольнения.

Разработали матрицу рисков

У нас есть матрица рисков, которая оценивает возможные последствия, вероятность ущерба и его величину, дает возможность сопоставить потенциальный ущерб с затратами на его предотвращение. Оценка позволит применять простые решения, когда необязательно прибегать к дорогим и сложным методам. Ведь на рынке есть разные инструменты информационной защиты компании:

отключение USB;

удаление драйверов для сторонних носителей;

контроль печатных устройств;

внедрение систем автоматизированного слежения за компьютерами.

Наша матрица рисков оценивает:

уровни рисков;

вероятность их наступления;

категории влияния (финансовую, юридическую, репутационную).

Экономическая целесообразность. Средняя стоимость DLP-программ для компании из 250 человек варьируется в пределах 1,5–5 млн руб. Понадобится отдельный менеджер по информационной безопасности. Поскольку кто‑то должен мониторить выявленные программой отклонения и предпринимать по ним корректирующие действия. Для малого бизнеса такой вариант может быть дорогим решением проблемы. Поэтому надо соотносить затраты и риски.

Юридическая составляющая. Основные инструменты защиты — соглашение о конфиденциальности, ограничения прав доступа, управление контактами. Они не имеют юридических последствий. Вопрос вызывает только слежение за компьютерами сотрудников. С юридической точки зрения все правильно. Компьютер — средство труда, и работодатель вправе контролировать, как оно используется и в каких целях. Но во избежание двойных трактовок и юридических недоразумений внесите информацию о слежении в трудовой договор.

Моральная сторона вопроса. Осознание того, что все его действия контролируются, мобилизует сотрудника и уменьшает возможность злоупотреблений. Но отсутствие доверия негативно сказывается на лояльности. Инструменты защиты клиентской базы должны быть органично вписаны в корпоративную культуру компании.

# Почему воюют учредители и их «генералы»

Вячеслав Московский Аналитик, Москва

Пять ошибок в подборе и назначении генерального директора, которые могут поставить под угрозу всю деятельность компании.

Конфликтов в компании не избежать, и это совершенно нормально. Исключение – случаи, когда корпоративный конфликт ставит под угрозу деятельность всей организации как единого и неделимого организма. Противостояние между генеральным директором и учредителем создает именно такую угрозу. Разберем несколько типичных конфликтных ситуаций, возникающих между этими лидерами компании. Наиболее частые причины – это пять логических ошибок при подборе или назначении кандидата на должность CEO.

1. Эмоциональный выбор

Кандидат нравится учредителю, который видит в нем много общего. Мы все так устроены: совокупность схожих с нашими психологических качеств, умений, знаний и навыков нам по душе. Но если мы хотим вдохнуть новый импульс в деятельность своей компании, то разумнее искать в кандидате качества, которых нам самим не хватает. Для взаимного опыления и дополнения. Или, наоборот, для полной автономии генерального директора от мнения учредителя.

2. Переоценка опыта кандидата

В этом случае внимательно анализируется, что человек делал в прошлом, и недостаточно учитывается его индивидуальный мотивационный период. Мотивационные периоды длятся от полутора до пятнадцати лет, и у каждого человека эти периоды индивидуальны. Условно их можно поделить на три фазы: подъем, спад, стагнация.

Так, учредитель точно ошибся, если взял в стартап «генерала», который раньше руководил схожим направлением деятельности в компании, насчитывавшей 2000 человек. Даже если учредитель раньше много лет с таким менеджером работал, пословица «Старый друг – лучше новых двух» в этом случае совершенно не аксиома. Опыт достижений в большой компании практически невозможно полностью применить в строительстве нового бизнеса. Главным камнем преткновения станет системный и административный подход, который хорошо зарекомендовал себя в большой компании, но совершенно неадекватен для растущего коллектива 20+ человек. Такой подход может существенно снизить скорость выхода компании на динамично развивающийся рынок и демотивировать сотрудников затяжным принятием решений в условиях дефицита времени.

Опасно и то, что генеральный директор, перешедший в стартап из крупного бизнеса, находится в стагнационном мотивационном периоде, что гарантирует отсутствие «тяги» с его стороны. Это изначальная угроза для роста компании в условиях повышенной динамики на рынке. И если учредитель решит исправить свою ошибку, сам факт увольнения CEO послужит ускорению коммуникаций как внутри компании, так и в работе с клиентами. Это даст такой же эффект, как сброс балласта за борт корзины воздушного шара.

3. Непоследовательность в делегировании полномочий

В бизнесе, как в такси: если ты сел на заднее сиденье, предназначенное для пассажира, и сообщил водителю адрес назначения, неразумно перехватывать у него управление автомобилем или комментировать каждый маневр. Учредителю необходимо заранее принять для себя решение о делегировании генеральному директору оперативного управления и доверии к его деятельности.

Так, в одном из известных мне банков позиция председателя правления предполагает полную автономию в оперативном управлении. И менеджер, занимающий эту должность, принципиально действует в соответствии со своими полномочиями. Каждый раз, когда кто-то из учредителей настаивает на своем «повороте», он смело предлагает автору идеи взять управление банком на себя либо судить об эффективности текущих решений по итогам года. Нравится ли учредителям такая самостоятельность председателя банка? Далеко не всем, однако банк поднимается в различных рейтингах, обрастает клиентской базой, повышает качество сервиса, успешно выводит на рынок новые финансовые услуги и стабильно растет, принося учредителям прибыль. Следовательно, с поставленной задачей председатель правления справляется успешно.

4. Непродуманность решения о найме

«Я думал, он хороший парень», – разводят руками учредители, когда «генерал» вдруг преподносит шокирующий сюрприз. Но думать мало. Говорят: доверяй, но проверяй. Поэтому уже на первой стадии переговоров о приглашении в компанию нового руководителя как учредителю, так кандидату необходимо детально обсудить и облечь в договорную форму все моменты своего взаимодействия, все права и обязанности CEO именно в этой компании. Здесь не может быть банальных мелочей, каждый нюанс может сыграть решающую роль в перспективе. Поэтому во избежание финансовых и временных потерь не стоит экономить на предварительной подготовке к взаимодействию с новым «генералом». К разработке его контракта и оценке психологического потенциала рекомендуется подключать высококлассных юристов и экспертов-психологов.

Так, перекупив за большие деньги генерального директора одного известного завода, учредитель был уверен, что нашел мессию, который спасет и его завод. Субъективная оценка победоносного прошлого менеджера вселяла в учредителя уверенность в его продуктивности. Однако в характерологической справке на данного кандидата, которую мы подготовили, черным по белому было написано: «не надежен», «мотивация идет на спад», «в условиях давления со стороны демотивируется и забирает взятые на себя ранее обязательства». К сожалению, учредителя эти выводы не вразумили. Мы дали прогноз: на новом месте этот руководитель проработает не менее шести месяцев. Он ушел через четыре месяца: написал заявление сразу, как только встал вопрос о необходимости представления интересов завода в следственных органах. Дело о производстве контрафактной продукции было возбуждено еще при прошлом руководстве завода, и новый «генерал» об этом прекрасно знал. Более того, ввиду этого обстоятельства он договорился о двойном размере оплаты своего труда. Удивлению учредителя не было предела, когда при увольнении CEO потребовал выплатить ему компенсацию, равную годовой зарплате. Оказалось, что он прописал в трудовом договоре пункт, дающий ему право уйти с компенсацией при возникновении необходимости разгребать старые «грехи» завода. В общем, завод залихорадило после явления «спасителя» еще сильнее. А время было потеряно, как и деньги учредителя.

5. Неправильно поставленные задачи и требования

Пятую ошибку чаще всего совершают небольшие компании, которые часто меняют свою бизнес-тактику. Они нанимают генерального на одну деятельность, а затем концепция деятельности меняется – и требуется руководитель уже с совершенно иными индивидуально-личностными качествами и опытом.

Что делать, если «генерал» не на своем месте?

Неэффективных сотрудников не бывает. Бывают люди, занимающиеся не своим делом или не заинтересованные в своем развитии. В любом случае учредитель способен на это повлиять своей личностью, харизмой, примером, участием и поддержкой. И, конечно, когда человек не заинтересован в собственном развитии, выбор остается за учредителем: учить, лечить или «мочить» такого сотрудника. Пример удачной корректировки задач руководителя в такой ситуации – решение учредителя одной из строительных компаний, решившей перейти от строительства к обслуживанию объектов недвижимости. В сложившейся ситуации генеральный директор уступил свое место учредителю, а сам занял должность менеджера проектов, взяв в свое управление самый большой объект недвижимости из возможных. При этом, по договоренности с учредителем, он получил право стать его младшим партнером, если через год покажет успешные результаты на этом объекте.

Важную роль в конфликтных и спорных ситуациях в компании должен играть HR-директор или, если компания небольшая, HR-менеджер. Фактически эйчар – это главный доверенный человек учредителя как по вопросам формирования корпоративной культуры, так и по вопросам взаимодействия с сотрудниками. HR-директор должен разделять с учредителем ответственность за человека, которого он одобрил на должность CEO. Он должен быть первым, кто может рассказать собственникам компании, когда и чего следует ожидать от нового руководителя. А в спорных ситуациях он должен стать своего рода рефери.

Что бывает, когда мнение руководителя HR-службы игнорируется? Приведу еще один пример. В погоне за быстрыми антикризисными мерами, невзирая на предупреждения, учредитель назначил генеральным директором человека, обещавшего быстрые позитивные перемены. Действуя по принципу «цель оправдывает средства», новый «генерал» начал сокращать издержки компании, увольняя самых лояльных сотрудников. Быстрые перемены не заставили себя долго ждать. У CEO сразу же возник конфликт с HR-директором, формировавшим корпоративную среду и лично вставшим на защиту каждого из сокращаемых. Учредитель, скрипя зубами, ждал обещанные победные цифры. В итоге после серии «кадровых расстрелов» ушел и HR-директор. При этом масштабные сокращения лишь замедлили генерацию компанией долгов, они не решили ситуацию и загнали компанию в еще более крутое пике. Тогда учредитель уволил генерального директора как не оправдавшего надежды и решил срочно вернуть прежнего HR-директора, чтобы попытаться воссоздать хоть часть прежней корпоративной среды, культуры и штата. HR-директора вернуть в компанию удалось, но о дальнейшей судьбе этого бизнеса история умалчивает.

Мораль в том, что сегодня не цель оправдывает средства, а средства оправдывают цель. Эффективность и результат важны, но не менее важны способы достижения результата и последствия мер, принятых для повышения эффективности бизнеса. Бомба, конечно, эффективна в качестве оружия, но разрушения от нее могут превосходить полученную пользу и носить необратимый характер. Изменились технологии, изменилась скорость обмена информацией, однако, как и прежде, люди решают все.

Необходимо помнить, что мир сегодня совершенно не такой, как был вчера. Если вчера неграмотным считался тот, кто не умел читать, писать или считать, то сегодня неграмотный тот, кто не умеет быстро переучиваться, обрастать новыми актуальными знаниями. Учредитель и генеральный директор как субъекты управленческого труда находятся в равных условиях, требующих от каждого высокого уровня доверия, трудолюбия, ответственности и дисциплины.

[**Вернуться в каталог сборников по управлению персоналом**](http://учебники.информ2000.рф/personal2/personal3.shtml)

[**НАПИСАНИЕ на ЗАКАЗ: дипломы и диссертации, курсовые и рефераты. Переводы с языков, он-лайн-консультации. Все отрасли знаний**](http://учебники.информ2000.рф/napisat-diplom.shtml)

|  |  |
| --- | --- |
| [**КНИЖНЫЙ МАГАЗИН**](http://учебники.информ2000.рф/chitai.shtml) |  |

|  |  |
| --- | --- |
| [**ТОВАРЫ для ХУДОЖНИКОВ и ДИЗАЙНЕРОВ**](http://учебники.информ2000.рф/kar.shtml) |  |

|  |  |
| --- | --- |
| [**АУДИОЛЕКЦИИ**](http://учебники.информ2000.рф/lectr.shtml) |  |

|  |  |
| --- | --- |
| [**IT-специалисты: ПОВЫШЕНИЕ КВАЛИФИКАЦИИ**](http://учебники.информ2000.рф/otu.shtml) |  |

|  |  |
| --- | --- |
| [**ФИТНЕС на ДОМУ**](http://учебники.информ2000.рф/fit1.shtml) |  |