ФИЛОСОФИЯ ЗАЩИТЫ

Безопасность – это бизнес-партнер

БЕЗОПАСНОСТЬ – ОБЛАСТЬ ЗАКРЫТАЯ. На то, конечно, есть объективные причины, хотя, в целом, отрасль только проигрывает от недостатка профессионального общения. В любом случае, коллеги не спешат делиться секретами профессиональной кухни. Поэтому, когда такое все-таки происходит, мы с удовольствием пользуемся представившейся возможностью. Сегодня с нами своим взглядом на современное состояние коммерческой безопасности делится СЕРГЕЙ МАТВЕЕВ, действительный член ACFE и директор по безопасности крупной компании.

Безопасность – понятие разноплановое. Что для вас значит безопасность бизнеса, с чего она начинается и в чем ее основное предназначение?

Вопрос неоднозначный, тут нет какого-то определенного ответа «как в учебнике», но попробую ответить. На мой взгляд, безопасность начинается с ее незаметности для бизнеса. Это значит, что в процессе развития бизнеса, движения к его стратегической цели безопасность ни коим образом не мешает ему своими процедурами или иными активностями. Бизнес не замечает и не ощущает на себе действия безопасности по пути вперед, и со стороны внешнего наблюдателя все складывается само собой. Система безопасности нейтрализует внешние и внутренние угрозы, которые мешают достижению бизнесом той или иной цели. Вот с этого, наверное, и начинается «безопасность бизнеса»: с ее незаметности и одновременно эффективности.

Вы говорите, как должно быть, но последние 20 лет мы видим абсолютно противоположную картину. В понятии обывателя руководитель службы безопасности – этакий «серый кардинал», самый влиятельный человек в компании для решения подковерных вопросов. И проблема даже не в том, что так происходит, а в том, что это считается нормой. В чем причина?

На самом деле ответ достаточно простой. Безопасность бизнеса – как отрасль, как институт в России, довольно молодая структура. Только в последние годы в крупных компаниях появились устойчивые бизнес-модели защиты бизнеса. Руководители таких компаний на примере западного опыта, стажировок и новых знаний успешно выстраивают превентивную модель безопасности. В годы перестройки появились первые охранные предприятия, которые и занимались безопасностью – ЧОПы. Я не могу сказать что ЧОПы тех времен занимались безопасностью бизнеса, они скорее продавали услугу защиты конкретных людей или решали какие то проблемы точечно. Ведь ЧОП – это тоже бизнес. По большей части, модели безопасности, похожие на эту, нацелены на решение уже возникших проблем, на то, что уже случилось. Они не предполагают системное прогнозирование или профилактику.

То, о чем вы говорите, наверное, как раз относится к тому периоду – 90-е, начало «нулевых». Тогда т. н. безопасность была маленькой

карманной армией собственника компании и руководитель безопасности был неким полководцем, который решал проблемы, не важно чьи. В настоящее время происходит модернизация, если хотите, трансформация самого понятия «безопасность бизнеса». По сути службы безопасности из «решальщика» проблем превращаются в структуры, которыя помогают бизнесу не допустить тех самых проблем, и не привлекать в дальнейшем дополнительные инвестиции компании для их решения.

То есть, если раньше, из-за специфики рисков безопасность была «на виду», то сегодня, в силу того, что бизнес принимает все более цивилизованные формы, безопасность становится незаметной, скрытой

Мысль правильная по сути, но с одной поправкой. Безопасность не то чтобы уходит в тень. Можно сказать, она становится неотъемлемой частью бизнес-процессов компании, внутри самого бизнеса как его составляющая. То есть безопасность перестает быть исключительным «решателем» проблем, перестает культивировать свою исключительность для бизнеса, и начинает управлять рисками мошенничества или хищения внутри бизнеса на всех этапах. Будь это какая-то техническая составляющая, вопросы коррупции, анализ бизнес-процесса или сделок, потери активов.

Безопасность вовлекается и встраивается, как полноправный участник, во все рискоемкие процессы и работает наравне с юристами, бухгалтерией и с другими подразделениями. Уже нет смысла выделять СБ как какое-то особенное подразделение, к которому все бегут как к главному «решальщику» внутри компании, а относятся как к бизнес-партнеру с соответствующими задачами и полномочиями. Безусловно, есть определенные особенности у подразделений безопасности – это специальные уставные задачи, такие как, например, взаимодействие с правоохранительными органами, выявление мошенников и проведение служебных проверок в их отношении, управление иными рисками где необходим т. н. творческий подход. И при такой модели безопасности ее руководитель – это уже, скорее, менеджер, который управляет этим процессом внутри бизнеса и несет ответственность за предотвращение потерь/хищений/проблем, а не за их «решение», что намного ценнее для бизнеса.

Безопасность перестает быть «решателем» проблем, перестает культивировать свою исключительность и начинает управлять рисками мошенничества или хищения внутри бизнеса на всех этапах

Это значит, что нельзя сейчас говорить о безопасности бизнеса как о службе охраны компании – ее функция уже давно намного шире. Многие не до конца осознают значение безопасности в бизнесе и когда слышат слово «безопасность», ассоциируют его с физической охраной, ЧОПами. С одной стороны это понятно, с другой – людей надо образовывать. Как известно, большая часть айсберга всегда под водой, а не на поверхности. В моей деятельности охрана занимает всего лишь 10–15 %. Основа работы – это управление рисками, экономическая безопасность, управление сохранностью активов.

Давайте раскроем этот вопрос. Итак, хозяин компании, генеральный директор подписывает контракт. Перед тем как принять решение, он оценивает риски. Для оценки этих рисков служба безопасности проводит проверку контрагентов

Конечно, ведь при подписании контракта, при совершении любой сделки всегда есть вторая сторона – партнер. А у партнера есть какие-то свои намерения. Что-то продать, что-то сделать совместно или что-то иное. Собственник или генеральный директор не понимает, насколько эти намерения соответствуют тому, что представляет из себя партнер, насколько он благонадежен и можно ли ему доверить эти работы. Конечно, к данному процессу подключается безопасность компании. Первое, что делается – это проверка на благонадежность: кто он, что он, какова его история, насколько этот партнер сможет исполнить предмет контракта. Дальше проверяется благонадежность самих по себе людей внутри этой компании, насколько эти люди в предмете бизнеса, нет ли у них криминального прошлого и не мошенники ли они. В целом происходит оценка рисков контракта, сделки или какого-то процесса. В ходе оценки рисков дается максимально полная картина для принятия взвешенного решения.

Какими источниками информации вы пользуетесь для этого?

Во-первых, есть открытые источники информации для проверки людей. Например: ресурсы судов, ФССП, соцсети. И много других.

Соцсети помогают?

На самом деле, соцсети помогают сильно. Люди выкладывают туда массу информации. С другой стороны я рекомендую очень аккуратно заниматься публикацией личной информации в соцсетях, поскольку, например, квартирные воры очень просто вычисляют образ жизни, точки передвижения и время передвижения владельцев квартир. Затем дело техники вычислить, когда квартира пустая, и обчистить ее в период длительного отсутствия владельцев

Используете ли вы какие-то закрытые базы для проверки людей?

Существуют информационные каналы, через которые можно получить сведения о наличии или отсутствии у человека судимости, или привлечения его к уголовной или административной ответственности. Также можно выяснить кредитную историю человека или компании и понять, насколько благонадежны эти люди или компании, платят ли они по кредиту и насколько их много. Может быть, компания погрязла в долгах в судебных исках и тут же просит дать предоплату в миллион долларов, с комментарием «а потом я выполню все свои обязательства». Конечно, такая компания потом пропадает вместе с деньгами.

Как происходит оценка рисков?

Периодически нам приходится оценивать различные сделки или бизнес-процессы, новые или действующие, на наличие в них рисков мошенничества или утраты актива. В ходе такой оценки мы выявляем тонкие места, или, по-другому, факторы риска, которые в дальнейшем могут реализоваться и превратиться уже в угрозу и в худшем случае в утрату актива компании или совершение того или иного преступления. Эта оценка дает бизнесу возможность здраво оценивать ситуацию и принимать вполне эфективные и успешные решения.

Кто он, современный директор по безопасности, по-вашему? Традиционно, выходец из силовых структур?

Этот вопрос мне очень часто задают. На него нет однозначного ответа. Часто руководитель по безопасности – это действительно выходец из силовых структур – ФСБ, МВД, армии, но мое персональное мнение: директор по безопасности любого предприятия в первую очередь – это грамотный и хороший управленец, с качественным образованием – юридическим или финансовым и с хорошим опытом по выстраиванию различных систем или моделей безопасности коммерческих компаний. Если нужен в структуре безопасности кто то из бывших высокопоставленных представителей силового блока для взаимодействия с силовыми органами или органами власти, то его можно взять в штат в статусе советника для решения узкопрофильных задач. В настоящее время очень важным становится такое качество руководителя, как способность выстраивать коммуникации внутри компании и создавать свой профессиональный круг общения.

А вы сами в каких силовых структурах работали в каком звании? У вас юридическое образование?

Я начал работать в безопасности в 1999 году в период зарождения самого термина «безопасность бизнеса» и, конечно, до этого я работал в правоохранительных органах, следственных подразделениях МВД в офицерском звании. Юридическое образование я получил до начала работы в следственных органах. Но как только занялся изучением нового для себя блока под названием «безопасность бизнеса», я осознал, что для успешной карьеры необходимо экономическое образование. И в итоге я получил диплом экономиста. Я был офицером, но, проработав уже почти 18 лет в структурах безопасности, я понял, что наличие офицерских погон в прошлом это и не плохо и не хорошо. Есть свои и плюсы и минусы.

Вы занимаете довольно высокий пост для своей профессиональной области. Насколько в вашей текущей работе помогает опыт работы в силовых структурах?

Безусловно, это помогает. Во-первых, правила дисциплины и субординации. Во-вторых, понимание специфики уголовного права, уголовного процесса, различных норм, с которыми приходится сталкиваться на ежедневной основе. Кроме того, есть четкая картина процедуры проведения служебных проверок или расследований. Но, в целом, это все можно наработать и получить знания за довольно короткий промежуток времени. Главное – правильно понять потребность бизнеса в той или иной модели безопасности, под стратегию бизнеса настроить систему безопасности, собрать необходимую для этого команду и расставить правильные приоритеты. И не важно, каких силовых служб ты бывший сотрудник, какие погоны ты носил, если у тебя в голове есть четкое понимание собственной роли в структуре компании и четкая картина того, как организовать эффективное направление безопасности, остальные вопросы –дело техники.

Получается, что образ «сотрудника безопасности» который сформировался 20 лет назад, достаточно сильно трансформировался. Сегодня директор по безопасности – это современный молодой человек с хорошим образованием, владеющий навыками психологии, бизнеса. Это

не закостенелый отставник, пришедший «в монастырь со своим уставом»

Термин начался трансформироваться несколько лет назад. Я не скажу, что все компании к этому пришли. Конечно, есть такие компании, где нужен руководитель безопасности в единственном числе, самостоятельно решающий все возникшие проблемы. Например, небольшая компания со скромной структурой безопасности. Если мы говорим о крупных компаниях со штатом безопасности в несколько сотен человек, то, конечно, здесь нужен управленец для построения системной работы, в меньшей степени зависящей от человеческого фактора. При таком подходе у руководителя безопасности нет даже возможности погружаться в микро-менеджмент и самому решать проблемы. Задача руководителя – настраивать и управлять процессами внутри этой большой компании. Но, повторюсь, все очень индивидуально. Во всех компаниях, даже в похожих, может быть различная модель безопасности и различные подходы к ее обеспечению. Все зависит от стратегии бизнеса, желания и требований собственников бизнеса и топ-менеджмента.

Чего сегодня больше в защите бизнеса – расследований внутренних и внешних инцидентов или аналитики и профилактики? Чего больше нападения или защиты?

Повторюсь, что безопасность, занимающаяся анализом big data, профилактикой и управлением рисками намного эффективней и дешевле для бизнеса, нежели безопасность, которая «бьет по хвостам» и решает уже случившиеся проблемы. Поэтому я стараюсь выстраивать именно такие системы, которые занимаются в большей части прогнозированием и управлением рисками.

Если мы говорим, что в 90-е годы основой безопасности бизнеса была защита от внешней агрессивной среды, в том числе и физическая, то сегодня внешние угрозы снизились?

Я не могу сказать, что внешние угрозы канули в лету, они скорее трансформировались в другую форму. Мы живем в ситуации экономического кризиса, более того, мирового уровня. И в этой ситуации бизнес уже не пытается больше зарабатывать обычным увеличением стоимости продаваемого товара или услуги, так как при сегодняшней конкуренции сделать это

Директор по безопасности любого предприятия в первую очередь – это грамотный и хороший управленец, с качественным образованием

достаточно сложно, а порой и невозможно. Бизнес пытается найти дополнительную эффективность в сокращении расходов, тем самым улучшая EBITDA компании и размер ее прибыли для владельцев. Вот как раз в сокращении расходов безопасность и помогает бизнесу. Например, управляя сохранностью активов компании, безопасность регулирует уровень потерь, а потери компании напрямую связаны с ее финансовым результатом. Другой пример, когда безопасность занимается борьбой с коррупцией в компании, тем самым вычищая коррупционную составляющую из закупочных цен товара. Это означает меньшую закупочную стоимость единицы товара, и, соответственно, меньшую розничную стоимость на полке. И таких примеров можно привести сотни, где безопасность оказывает реальную помощь бизнесу в его развитии и достижении стратегических целей.

Не могу не отметить, что безопасность, конечно, защищает бизнес и от внешних агрессий, будь то внешняя преступная среда, защита от конкурентной разведки или защита от различного рода чрезвычайных ситуаций.

Очень важно, анализируя исторический опыт случившихся ситуаций, анализируя бизнес-процессы компании с точки зрения их прозрачности и наличия риск-факторов, прогнозировать наступление каких-то угроз и заниматься профилактикой.

Бизнесу интереснее инвестировать в модели безопасности, которые не допускают совершения мошенничества или любой иной потери актива, нежели иметь непрогнозируемые инвестиции в постоянное решение образовавшихся проблем. Потому как собственника бизнеса и бизнес в целом интересует только сохранность активов и их преумножение, а не то количество преступников, которое будет разоблачено или уволено. Если

хищение уже совершено, то фактически актив или его часть уже утеряны и для собственника или бизнеса, это уже негативный эффект.

Должно ли подразделение безопасности иметь в штате собственных хакеров, сотрудников IT, работающих на службу безопасности?

Все зависит от уровня и размера компании, насколько она готова инвестировать в тот или иной вопрос. Если мы берем большую компанию, то в таких компаниях безопасность имеет в структуре подразделение информационной безопасности. Это те самые люди, которые и создают барьеры для того, чтобы внешние злоумышленники не пробились в информационную систему компании. Офицеры информационной безопасности, используя свою экспертизу, своевременно обнаруживают и блокируют внешние попытки взлома системы и затем проводят работу по определению источников угроз. Конечно, внутри отделов информационной безопасности есть специалисты с узкими задачами, которые обладают экспертными знаниями в области информационных технологий и, наверное, которых можно назвать «хакерами» по характеру их деятельности.

Как обстоят дела с перлюстрацией корпоративных почтовых ящиков сотрудников?

Если это почта корпоративная, то она принадлежит компании, а не сотрудникам. И сотрудникам об этом сообщается. В каждой крупной компании существует система DLP (Data Leak Prevention), которая контролирует утечку информации из компании путем пересылки сообщений в почте или переноса данных через внешние накопители. Данный инструмент отслеживает информационные потоки и своевременно информирует отделы информационной безопасности

ГЛАВНОЕ – ПРАВИЛЬНО ПОНЯТЬ ПОТРЕБНОСТЬ БИЗНЕСА, ПОД СТРАТЕГИЮ БИЗНЕСА НАСТРОИТЬ СИСТЕМУ БЕЗОПАСНОСТИ, СОБРАТЬ НЕОБХОДИМУЮ ДЛЯ ЭТОГО КОМАНДУ И РАССТАВИТЬ ПРАВИЛЬНЫЕ ПРИОРИТЕТЫ

о произошедшей утечке информации, составляющей коммерческую тайну компании, для реагирования.

Сколько компания должна тратить на безопасность, есть ли какая-то формула?

Ее не существует. Все зависит от отрасли бизнеса, его размера, задач. Безопасности не должно быть слишком много и не должно быть слишком мало, она должна быть достаточной для решения поставленных задач. Задача директора по безопасности определить уровень достаточности. Не нужно из бизнеса делать тюрьму с закрытыми клетками, решетками, нет такой задачи. Есть задача определить уровень риск-аппетита в различных направлениях бизнеса, который компания допускает, и работать уже с отклонениями свыше этого установленного уровня.

Не нужно забывать, что желание заниматься всем и свести к нулю все возможные нарушения или отклонения – это задача практически невыполнимая, которая в первую очередь влечет за собой слишком большое инвестирование в безопасность и может стоить чересчур дорого для компании. Если сформулировать более правильно, задача директора по безопасности определить уровень затрат на безопасность относительно выручки компании, который позволит все затраты на безопасность окупать за счет ее положительного эффекта на финансовые показатели компании.

Давайте перейдем к той части, которая касается непосредственно ритейла. Поговорим сначала о внутренней безопасности. Почему люди крадут?

Это хороший вопрос. Ответ на этот вопрос – ключевая тема безопасности в бизнесе. Многие владельцы бизнесов, топ-менеджеры, директора по безопасности пытаются бороться со следствием, то есть с самой утратой актива или потерей товара. Вынос продукции домой – это следствие. А необходимо найти причину, почему люди это выносят, что позволяет делать им это так просто, и другие важные вопросы, которые следует для начала задать в каждом конкретном случае. Необходимо определить факторы, которые влияют на это, порождают это и затем работать уже с факторами, потому как бороться со следствием абсолютно бесполезно и ситуация с выносом товара не изменится.

Хорошо, такой вопрос. В крупных супермаркетах, например прилавки с конфетами расположены так, что вы провоцируете людей

Я всегда стремлюсь к тому, чтобы человек в своей работе начал думать вместе со мной

на то, чтобы украсть, взять хотя бы одну конфету

Если мы берем тему воровства товара в магазинах, то внешнее воровство, так назовем покупателей, из всех хищений составляет примерно 15%, остальные 85% – воровство сотрудников магазинов. К тому же у компании нет задачи свести воровство к нулю. Задача компании, в частности безопасности, держать приемлемый или допустимый уровень потерь в магазинах. Иначе инвестиции в безопасность будут колоссальными и сами магазины превратятся в крепости с невысоким товарооборотом и слабой привлекательностью для клиента.

Тогда почему происходят случаи неадекватно грубого обращения с покупателями, в основном из низкообеспеченых слоев населения – пенсионерами, ветеранами, которых подозревают в воровстве в магазинах? Не проще ли их отпустить, если это практически не влияет на уровень потерь?

Ну это совсем другая тема. Человеческий фактор существует везде. Те инциденты, которые происходили в разных городах с покупателями, были инициированы обычными людьми, теми самыми охранниками, которые стоят небольших денег. И это не вопрос общей настройки безопасности внутри компании, это вопрос настроек конкретных людей на ту или иную ситуацию, работающих в конкретном магазине. Это вопрос их морального состояния и общего развития.

То есть это не установка компании?

Конечно нет, это настройки конкретных людей, их возможная озлобленность на мир, на людей, возможно, на компанию или вообще плохое самочувствие или настроение, которые тоже не появляются из ниоткуда. Опять же возвращаемся к факторному анализу – а почему сотрудник, охранник, накинулся на покупателя? Это необходимо проанализировать и сделать выводы для внесения каких-то корректировок либо в систему мотивации, либо в систему подбора сотрудников или управления ими.

Тогда почему вы берете такого человека, вы не видите риски?

Если мы говорим о сотрудниках компании, то, конечно же, невозможно «отсканировать мозг» и предугадать его действия в будущем. Тем более, если количество набираемых на работу людей исчисляется тысячами в месяц. Если мы говорим про сотрудников ЧОП, то эта проблема должна заинтересовать в первую очередь наше государство с точки зрения внимания к этой отрасли, стандартизации, создания обучающей и профессиональной базы, минимального уровня заработной платы, различных грейдов сотрудников, для того, чтобы не попадали в охрану неблагополучные, неблагонадежные и несостоявшиеся граждане. И тогда есть шанс минимизировать подобные случаи.

Возвращаясь ко внутренним хищениям. Как с ними бороться, если это 85 % всего воровства в компании?

Сейчас очень важно не просто ловить за руку сотрудников, которые совершают хищения, очень важно подходить аналитически к управлению этими процессами и рисками. Что это значит? Есть теоретическая база, на которой основываются методики управления потерями или хищениями.

Первый столп – это «10 % сотрудников никогда ничего не воруют, потому что они идеологически правильные и принципиально честные, 10% людей постоянно что-то крадут и основная масса людей (80%) находится на грани. Они могут совершить хищение при наличии тех или иных условий».

Возвращаясь к 80-ти процентам мы подходим ко второму теоретическому столпу – треугольник хищения. Первый угол треугольника – это наличие возможности совершить хищение. Второй угол – это самооправдание человека, который совершил хищение. Третий угол – это потребность в деньгах. И вот когда все эти три угла сходятся в голове одного человека и реализуются, человек совершает хищение.

Задача безопасности – удержать эти 80% людей от совершения хищения, убрать хотя бы один из углов в этом треугольнике. Либо мы работаем с потребностью в деньгах – это система мотивации, которая должна быть эффективной и правильной. Либо работаем с возможностью совершить хищение, то есть настраиваем определенные контрольные процедуры или систему сдержек и противовесов так, чтобы, например, кассир не смог пробить определенный товар при определенных условиях, либо невозможно было в системе украсть денег, потому что технически это закрыто, невозможно. Самооправдание – это самое сложное, потому что, как правило, люди, пользующиеся самооправданием говорят: «А почему вот

кто-то берет товар домой, а мне нельзя?» Или: «Почему мой начальник ездит на шикарной машине, а мне нельзя?» Это крайне сложно – вычистить у человека из головы такого рода настройки и это уже идеологическая работа в долгом временном горизонте.

В общем, если говорить о проблеме потерь в любой ритейл компании, мы должны в первую очередь бороться не с потерями самими по себе, потому что потери – это уже следствие, эффект от неправильно построенной мотивации сотрудников, либо от неправильно построенных бизнес-процессов компании и так далее. В этом и задача безопасности по управлению этим процессом – разложить всю ситуацию на факторы и работать уже с первопричиной (факторами), а не со следствием.

Вернемся к кадровой проблеме в области безопасности. Вот если посмотреть на людей, работающих или устраивающихся на должность охранника, то чисто визуально кажется, что большинство из них как раз из тех 10%, которые постоянно совершают хищения. Как вам удастся отбирать качественных сотрудников и с ними работать?

Это важная тема, потому что в крупных компаниях подразделения безопасности большие по количеству, это тысячи человек. В таких больших подразделениях есть сотрудники с экспертными знаниями, которые штучные и собираются с рынка вручную, есть сотрудники, которых набирают путем массового набора. В случаях массового набора используется «профиль сотрудника» и далее проводится стандартная проверка кандидата. Конечно, невозможно залезть глубоко в голову человеку и понять его намерения на стадии подбора и конечно же случаются ошибки в подборе людей, приходится расставаться с некоторыми из них. В моей практике даже были случаи привлечения к уголовной ответственности сотрудников безопасности.

При наборе людей основной критерий для меня – это желание человека думать, двигаться совместно с идеями, заниматься творчеством и стойко отстаивать свои позиции и точки зрения. Я всегда стремлюсь к тому, чтобы человек в своей работе начал думать вместе со мной, идти вместе к нашей цели. Я стараюсь стать лидером для него, не просто руководителем или «боссом», который раздает команды, а заразить его своей идеей, стать для него проводником и помощником, чтобы ему самому хотелось делать свою работу, потому что он считает, что он причастен к чему-то важному и значимому.

У вас есть удивительная любовь к своей профессии и вы действительно хотите ее облагородить. Но вот готовы ли вы пойти в один из магазинов, встать и проработать вместе с рядовым сотрудником?

Я вам скажу больше, мы это делаем периодически. Весь наш менеджмент периодически выезжает в магазины нашей необъятной страны и вместе с сотрудниками смотрит проблемы на земле.

Скажите, а откуда у вас такие подходы и такой взгляд на безопасность бизнеса? Вы отличаетесь от большинства коллег

Скажем так, у меня были хорошие учителя. Они заложили мне в голову правильные принципы, правильные подходы и правильные модели. Дальше дело техники и времени оттачивать мастерство и нарабатывать практику. Я безмерно благодарен этим людям, с которыми, впрочем, мы до сих пор поддерживаем теплые, дружеские отношения и до сих пор отношусь к ним как к учителям, хотя сам уже давно учу других.

Последний вопрос. Вы генерируете какие-то идеи, они, наверное, как-то воспринимаются, видите ли вы огонек в глазах сотрудников или вы – белая ворона в этом бизнесе и сотрудники тяжело воспринимают что-то новое?

Все новое воспринимается очень тяжело, тем более в такой отрасли, как безопасность. Но лед однозначно тронулся.

Изначально есть три стадии жизни идеи :

Первая – это отрицание самой идеи и поиск оправдания, почему это не будет работать, вторая – это скептицизм, когда идея реализовывается, но сотрудник не верит в ее эффективность, а третья – это принятие уже этой идеи, убежденность в том что она работает и дает свои результаты.

Пример на практике. Новый процесс к управлению внутренними потерями. Изначально сотрудники относились к этому крайне негативно, потом был скептицизм и отсутствие веры в результат, а сейчас все подхватили эту идею и несут ее уже дальше с большим оптимизмом. Потому что людям важно видеть результат того, что они делают и понимать, как они лично могут оказывать влияние на ту или иную ситуацию. Нужно сотрудникам показать как можно зарабатывать, правильно выполняя свою работу, а когда каждый сотрудник начнет правильно выполнять свою работу, тогда вся система безопасности заработает правильно и эффективно.

В заключение хочу сказать, что моя идея – изменить отношение окружающих к безопасности, показать, что безопасность – это бизнес-партнер и в состоянии оказывать полезный эффект на финансовые показатели компании наравне с ключевыми функциями бизнеса, привлекать в безопасность молодых, амбициозных людей с хорошим образованием, которые готовы развиваться сами и развивать вместе с собой компанию. ●