Грани риска, или Кто с тобой работает?

Анна Кулик
Руководитель Исследовательского Центра Корпоративной Безопасности

Константин Митрошин
Исполнительный директор Исследовательского Центра Корпоративной Безопасности

Современный бизнес — многоуровневая система, которая включает в себя не только обеспечение процессов роста, увеличение прибыли, создание репутации, поддержание качества и прочее, но и крепость, где необходимо иметь и надежный тыл, и сторожевые башни. Предприниматели сталкиваются со многими проблемами, как коренящимися внутри компании (сотрудники, партнеры), так и приходящими извне (конкуренты, недоброжелатели). Шпионаж, передача информации конкурентам или другим заинтересованным лицам, похищение денежных средств или дорогостоящего оборудования, злоупотребление служебным положением, использование «откатных» схем, информационные войны и хакерские атаки — вот далеко не весь список опасностей, подстерегающих любой бизнес. Готовиться к противодействию возможным проблемам необходимо заранее, ведь грамотно выстроенная система безопасности компании обеспечит снижение рисков от различных противоправных действий.

В целях подробного рассмотрения вопросов борьбы с вышеперечисленными опасностями разделим риски на два блока. А примеры из реальной практики помогут соединить теорию с реальностью и предложат возможные пути выхода из сложных ситуаций.

Внешние риски

Те проблемы, которые подстерегают бизнес, в свою очередь подразделяются на несколько вариантов по степени мотивации, лиц, несущих угрозу.

1. ***Шпионы*** или, как иногда говорят, «засланные казачки». Лица, проникающие в компанию с целью изъятия важной информации или ресурсов, обычно засылаются конкурентами, недобросовестными партнерами или просто недоброжелателями. Рассмотрим реальный случай из нашей практики.

Руководитель одной из компаний осознал, что конфиденциальная информация неизвестным образом уходит на сторону. Естественно, чтобы минимизировать ущерб и найти виновников, он начал искать источник проблем. Было выявлено несколько подозреваемых, в том числе мужчина и женщина, которые с интервалом в три месяца были приняты на работу в компанию.

Когда круг лиц, которые потенциально были способны совершать данное коммерческое преступление, был определен, встал вопрос, не проверить ли всех сотрудников тестированием с помощью профайлинга (безинструментальный метод прогнозирования поведения и выявления лжи) и детектора лжи. Но явные доказательства «слива» отсутствовали (были только догадки со стороны руководства), и существовала возможность, что информация просто теряется из-за халатности служащих. В таких условиях вышеупомянутые мероприятия могли спугнуть виновных, а также нарушить внутренний климат в коллективе.

В итоге было принято решение провести проверку тайно, так чтобы никто ничего не заметил, провести первичный отсев людей, и уже далее инициировать беседу с лицами, вызывающими наибольшее подозрение. Такой формат проверок называется «легендированными». Их суть заключается в том, что проверяющие отыгрывают какую-то заранее подготовленную историю в условиях спокойной обстановки и использования эффекта неожиданности. В данном случае был организован корпоратив по поводу 8 марта, а проверяющих экспертов пригласили как организаторов увеселительных мероприятий: прове-

дение деловой игры, тимбилдинг и демонстрация фокусов с картами.

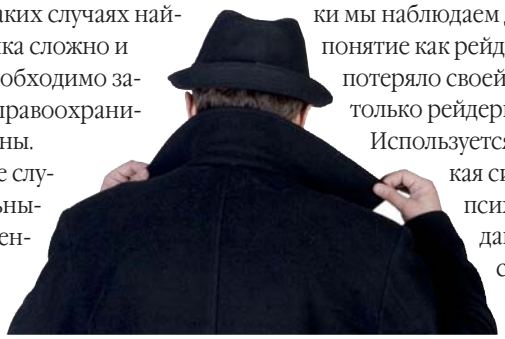
На протяжении вечера за подозреваемыми скрытно наблюдали, анализировали поведение и коммуникацию. Отметим, что с такой задачей компания может справиться и без привлечения сторонних экспертов, используя обычную наблюдательность и психологически комфортную обстановку. В итоге было замечено, что отношения между двумя изначально выделенными персонами весьма близкие, несмотря на демонстрацию личностной неприязни друг другу на глазах коллектива в рабочее время. В какой-то момент женщина в процессе увеселительных мероприятий, когда внимание всего коллектива было занято, подошла к мужчине и как будто невзначай коснулась рукой его затылка, жест был мимолетен.

Казалось бы, что в этом особенного, да и как это может быть связано со сливом информации? Дело в том, что на вопрос начальника обоим подозреваемым «Хорошо ли они друг друга знают?», они пояснили, что видят друг друга на работе не часто, так как работают в разных отделах, знают друг друга только по имени, вне работы они никак не связаны. В то же время зона, которой якобы невзначай коснулась молодая женщина, является для каждого из нас весьма интимной. Пробуйте коснуться затылка малознакомого человека — это крайне неловко и неэтично. Эпизод позволил сделать вывод, что подозреваемые сотрудники как минимум близко знакомы и не испытывают неприязни друг к другу. Начав разбираться в деталях и проведя с ними уже личную беседу, эксперты выяснили, что они состояли в интимных отношениях и в сговоре, и действительно сливали информацию компании-конкуренту, каждый по направлению отдела, в котором трудился — именно для этого и трудоустроились.

Итог — люди найдены, деньги не потеряны, микроклимат в основной команде не нарушен, так как никто ничего не заметил. Вывод прост: наблюдайте за взаимоотношениями в коллективе, за невербальными сигналами в расслабленных обстановках, кто с кем дружит, выходит курить и — какие последствия это может иметь.

2. ***Гастролеры, мошенники.*** Это один человек или небольшая группа людей, целью которой становится быстрая нажива. Еще один реальный случай из практики. Украденные у одной женщины документы, куда входили паспорт и карточка пенсионного страхования (да еще и жертва была выбрана внешне похожей на одну из злоумышленниц), были использованы преступниками для устройства на работу в ресторан.

Спустя неделю после трудоустройства злоумышленница взяла в банке кредит по поддельным документам, спокойно пройдя этап проверки, и на следующий же день вынесла выручку из ресторана, куда устроилась работать. В таких случаях найти преступника сложно и долго, еще необходимо задействовать правоохранительные органы.



Подобные случаи с поддельными или украденными документами не редкость в различных сферах бизнеса. Но можно предотвратить и выявить потенциальную угрозу уже на этапе собеседования или принятия решения о выдаче денежных средств.

Один из вариантов диалога с субъектом, которого вы подозреваете в попытке под выдуманной биографией внедриться в компанию или взять кредит, займ и исчезнуть в неизвестном направлении выглядит следующим образом:

— Назовите вашу дату рождения? (Здесь, как правило, человек без запинки, не глядя в поддельные документы, дает ответ, заученный по легенде).

— А это какой знак зодиака?

Скорее всего, данный вопрос, носящий эзотерический характер, не будет рассматриваться в качестве обязательного момента при составлении фальшивой биографии персонажа. Длительную заминку, паузу или невозможность ответить на этот или подобный простой, но неожиданный вопрос, специалисты обычно используют в качестве маркера, указывающего на то, что с собеседником что-то не так. В реальном случае на этом вопросе злоумышленница запнулась, чем навлекла на себя подозрения, в результате проверки ее настоящая личность была установлена.

Старайтесь найти как можно больше уязвимых мест для проверки подлинности документов и направленно задавать вопросы.

3. ***Рейдеры.*** Рейдерский захват у многих ассоциируется с лихими 90-ми, криминальными личностями, вламывающимися в компанию, выкидывающими вон всех сотрудников, жестко захватывающими управление. Эти времена остались позади, но отголоски мы наблюдаем до сих пор. Такое понятие как рейдерский захват не потеряло своей актуальности, вот только рейдеры стали другими. Используется уже не физическая сила, а сила ума, психологического давления и иные скрытые манипулятивные инструменты. Многим компаниям приходится защищаться и отбиваться от организаций, занимающихся поглощением бизнесов для дальнейшей их перепродажи.

Различают 3 вида рейдерства:

«Белое» рейдерство (в рамках закона) — четко спланированное поглощение компании, происходящее хоть и против воли основного собственника, но в строгом соответствии с требованиями закона. Как правило, такой вид рейдерства применяется по отношению к компаниям с малоэффективным корпоративным управлением и финансовыми затруднениями.

«Серое» рейдерство — поглощение компании, осуществляемое внешне законными средствами, аналогичными методам «белого» рейдерства, но совокупность этих средств в целом составляет схему мошенничества, аналогичную методам «черного» рейдерства. Это весьма распространенный вид рейдерского захвата, так как

крайне сложно оспорим и практически недоказуем.

«Черное» рейдерство — незаконный захват собственности, основа которого базируется на применении криминальных методов: подделке документов, подкупе чиновников (судьи, работники правоохранительных ведомств и пр.), шантаже, мошенничестве и др. Такой вид рейдерства может быть применен к любой компании, но в первую очередь к компании непубличной.

Проблема рейдерских захватов волнует многих лиц, принимающих управленческие решения. Ей посвящены сотни конференций по безопасности ведения бизнеса во всех существующих отраслях. Самое верное действие — профилактика, предупреждение, предотвращение захвата, хотя оно же и самое сложное.

Одно из ключевых решений в предупреждении возможного акта рейдерства — улучшение качества и охраны работы бизнес-процессов, а также использование квалифицированных помощников.

Предпочтительным для рейдеров является такой критерий, как присутствие в компании нескольких учредителей или акционеров. Ведь всегда можно попытаться найти слабое звено, а затем с помощью шантажа и постороннего воздействия склонить кого-либо из акционеров продать свой пакет акций. Важно чтобы среди дольщиков сохранялись здоровые отношения, потому что конфликт — это серьезная трещина, которую рейдеры могут расширить до пропасти.

Главный совет управленцам: внимательно отслеживать свой круг общения и «читать людей» , проверять искренность деловых партнеров, поставщиков, клиентов, сотрудников и соискателей.

4. ***Психопат.*** Антисоциальная личность, которая не имеет определенной цели, но вносит деструктивность во взаимоотношения в коллективе. Результатом порой является порча репутации компании, внесение раздора между учредителями и коллективом. Более того, данный человек, являющийся абсолютно вменяемым и расчетливым, не имеет определенной итоговой точки в своих действиях, он получает удовольствие от разрушения и психологического давления на других. Иногда такие люди разыскивают «скелеты в шкафу» у ключевых лиц в компании и занимаются шантажом. Тут совет один: внимательно анализировать кандидата на должность, потенциального партнера или поставщика. Психопатическая личность умеет производить приятное впечатление на окружающих, но его действия имеют эксплуататорский характер и несут разрушение.

Чем более тщательно изучен кандидат на должность в компании и работающий сотрудник с позиций корпоративной безопасности, тем меньше вероятность проникновения в компанию лиц с различными деструктивными намерениями, влекущими за собой и внешние угрозы.

Теперь ознакомимся со следующим блоком угроз, которые исходят изнутри, они наиболее часто встречаются как в крупном, так и малом бизнесе, вне зависимости от сферы деятельности организации.

Внутренние риски

1. ***Вор, мошенник.*** Сотрудники часто воруют рабочую канцелярию. Но когда речь идет о секретной информации, деньгах или дорогостоящем оборудовании, такое поведение может повлечь очень существенные репутационные риски и огромные финансовые потери.

Всех соискателей и сотрудников можно разделить на рисковые категории (данные усредненные), что следует принимать во внимание как при подборе персонала, так и при оценке уже работающего.

1) 10% будут совершать противоправные действия в любой ситуации, потому что по воспитанию, складу характера, жизненным принципам они ищут наживы и не ладят с совестью. Необязательно этот человек имеет внешние признаки неблагополучия.

2) 10% ни при каких обстоятельствах не нанесут вреда компании и вообще никому, потому что обладают высокими моральными качествами, и испытывают уважение к окружающим и чужому имуществу.

3) 80% будут действовать в зависимости от обстоятельств. Если система безопасности позволит совершать кражи или передавать информацию без видимых рисков и последствий — это произойдет. Если образовались долги, что повышает мотивацию на получение выгоды, дверца сейфа открыта, и никто не узнает о краже, такой человек может пойти на противоправное действие.

Поэтому важно построить работу таким образом, что самые неблагонадежные 10% вообще не попадут в компанию, а 80% не будут иметь ни желания, ни возможности что-либо совершить.

При приеме на работу можно предупредить, что периодически служба безопасности будет проводить проверки на полиграфе. На деле их проводить не обязательно, однако это станет дополнительным психологическим барьером для совершения противоправных действий. Тем более что использование полиграфа в России в настоящее время законом не запрещено, получения лицензии на приобретение и использование не требуется. Важно учитывать, что этот совет не панацея и подойдет не всем, но уже на этапе приема людей стоит продемонстрировать, что уровень контроля за безопасностью в компании высок. Это избавит неустойчивую личность от деструктивных мыслей.

При найме на работу можно собрать информацию о человеке по базам данных, которые в большинстве своем есть в арсенале служб безопасности компаний, а также провести сбор данных посредством анализа открытых интернет-источников. Тут важно обратить внимание на показатели возможной неблагонадежности: долги по кредитам, увольнения по статье, уголовные дела и другую информацию, раскрывающую трудовую деятельность.

Часть рисков можно сократить за счет четко выстроенной системы фильтров при приеме на работы. Тщательное изучение кандидата с позиции корпоративной безопасности

позволит снизить риск проникновения злоумышленников.

На этом этапе важно продуктивное взаимодействие между Службой безопасности (СБ) и кадрами (HR). Отсутствие четких регламентов и разделения сферы ответственности между этими службами создает ощутимые пробелы при оценке кандидата. Одна из частых проблем — кадровая служба имеет слабое представление о том, что может и должна сделать СБ для оценки персонала при приеме на работу. Процесс приема на работу слишком формален и быстротечен. Стоит подчеркнуть важность взаимодействия между СБ и HR и наладить работу по простой схеме:

- Отдел кадров собирает максимум исходной информации о кандидате (ФИО, дата рождения, паспортные данные) и передает ее Службе безопасности, которая уже детально рассматривает и ищет возможные риски.
- При собеседовании идет оценка профессиональных и личностных качеств кандидата.
- Кадровая служба оценивает кандидата на пригодность в своем направлении.
- Затем полученная информация вновь передается в СБ, где сотрудники начинают проводить проверку легальными и законными методами. Тут пригодится Интернет, характеристики с прошлых мест работы, рекомендации.
- После сбора всей информации Служба безопасности выдает свое заключение по данному кандидату. Данные сопоставляются с выводами HR и совместно выносится окончательное решение.

2. ***Инсайдер.*** Человек, располагающий конфиденциальными данными о делах фирмы. История знает множество примеров торговли инсайдерской информацией на самых различных уровнях, от рядовых сотрудников до ТОП-менеджеров. Иногда такого рода утечки происходят случайно, из-за болтливости сотрудников, что опять же можно предвидеть, составив подробный профиль человека. Однако основная мотивация в этом случае — финансовая выгода.

Технологии защиты от инсайдеров:

- Четкие инструкции и работа с персоналом, имеющим доступ к конфиденциальной безопасности (инструктаж, проверка знаний правил безопасности и их соблюдение).
- Регулярная проверка сотрудников, обладающих конфиденциальными данными о компании, на утечку сведений третьим лицам.
- Аудит всех операций в сети, совершаемых сотрудниками (особенно администраторами).
- Регулярное обучение Служб безопасности и HR новым методам и технологиям работы с персоналом.
- Контроль за соответствием уровня зарплаты с уровнем конфиденциальности информации.
- Оценка уровня благонадежности человека, получающего доступ к конфиденциальной информации, еще на этапе приема на работу.
- Контроль за электронными носителями информации.

Естественно, для сохранения комфортной психологической обстановки в коллективе все эти меры должны проводиться аккуратно и ненавязчиво.

3. ***Бездельники.*** Подбор сотрудника, который соответствует личностным и профессиональным критериям, требует большого труда. Но иногда только в рабочем процессе выясняется, что человек проводит время на работе, занимаясь чем угодно, только не продуктивным трудом. У него проблемы с дисциплиной, с качеством выполнения работы, что сказывается на всем коллективе. Он получает зарплату, временами внушительную, но при этом не приносит никакой пользы. Рецепт кажется простым: увольнение.

Но в такого сотрудника уже «вложились», он знаком со спецификой компании и, возможно, хорошо бы выполнял работу — но на другой должности.

Один из реальных примеров выхода из такой ситуации — рокировка кадров, которую последнее время, особенно с учетом кризиса, мы применяем в практике работы с компаниями.

Девушка без проблем прошла собеседование и вышла на новую работу помощником бухгалтера. Спустя два месяца в бухгалтерии стали возникать проблемы. Руководитель собирался уже уволить сотрудницу, однако вовремя воспользовался нестандартным советом.

По девушке было видно, что ей хочется общения и эмоций, ей не сидится на месте, что затрудняло деятельность бухгалтерии, где важно быть сосредоточенным и внимательным. Она получила предложение перейти в отдел продаж. При смене области деятельности девушка потеряла в зарплате, но приобрела то, чего так не хватало в бухгалтерии: общение, командировки, встречи, новые знакомства и — отсутствие монотонной работы. Уже в первый месяц сотрудница перевыполнила план

продаж, и благодаря бонусам заработала больше, чем на должности помощника бухгалтера. Она выразила руководителю огромную благодарность за предоставленную возможность.

Нужно использовать положительные стороны характера человека, что принесет гораздо больше плодов, нежели постоянная текучка кадров в связи с невыполнением своих обязанностей.

Мы перечислили далеко не все факторы риска и далеко не все способы их предотвращения. Наша цель — напомнить, что из самой сложной ситуации можно искать и находить выход, порой нестандартный. Важно при прогнозировании поведения людей, а соответственно и рисков, с ними связанными, использовать приемы правильного общения, умение задавать детальные вопросы и проводить анализ вербальных и невербальных сигналов. В процессе такой коммуникации можно выявить деструктивную личность, «засланца», бездельника и прочих уже на первичном этапе работы с кандидатом в сотрудники компании.