

А У ВАС В КОМПАНИИ ЕСТЬ МОШЕННИКИ?



Беседовала **ЕКАТЕРИНА ЗОЛОТАРЕВА**

20 января 2017 г. в Минске состоялась бизнес-встреча для руководителей «БЕЗОПАСНОСТЬ БИЗНЕСА И БУДУЩЕЕ ВЫЖИВАНИЕ ОРГАНИЗАЦИИ». На встрече присутствовали руководители, количество подчиненных которых достигает от сотен до нескольких тысяч человек. В таких больших коллективах сложно заметить мошенничество сотрудников.

Спикер из Латвии – вице-президент по стратегическому маркетингу консалтинговой компании «ПЕРФОРМИЯ СНГ» **Ярослав КАПЛАН** показал 3 кейса на примерах компаний мирового уровня о том, как один сотрудник способен нанести непоправимый ущерб организации (и даже полностью уничтожить «непотопляемую», казалось бы, корпорацию). Редактор журнала задала спикеру вопросы, актуальные для всех руководителей предприятий.

– Ярослав, поделитесь с нашими читателями своим видением, что такое «кадровая безопасность» и каковы основные методы ее диагностики.

– Кадровая безопасность предприятия представляет собой постоянную и целенаправленную деятельность собственников бизнеса и руководства компании по предотвращению рисков и угроз, хоть как-то связанных с сотрудниками, которые работают в данной компании.

Сегодня персонал – главная сила предприятия, определяющая эффективность всех других факторов, влияющих на развитие бизнеса. С другой стороны, персонал является источником основных угроз экономической безопасности предприятия. В соответствии с данными статистики до 80% совокупного ущерба организации происходит от собственного персонала. Когда мы подходим к диагностике кадровой безопасности пред-

**СЕГОДНЯ ПЕРСОНАЛ –
ГЛАВНАЯ СИЛА ПРЕДПРИЯТИЯ,
ОПРЕДЕЛЯЮЩАЯ ЭФФЕКТИВНОСТЬ
ВСЕХ ДРУГИХ ФАКТОРОВ,
ВЛИЯЮЩИХ НА РАЗВИТИЕ
БИЗНЕСА. С ДРУГОЙ СТОРОНЫ,
ПЕРСОНАЛ ЯВЛЯЕТСЯ
ИСТОЧНИКОМ ОСНОВНЫХ УГРОЗ
ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ
ПРЕДПРИЯТИЯ.**

приятия, то, как правило, мы можем наблюдать в большинстве организаций отсутствие эффективной системы мониторинга, которая бы включала в себя целый комплекс мероприятий с персоналом организации.

– Какие самые распространенные ошибки руководителя приводят к утечкам информации и финансовым потерям?

– Первая ошибка заключается в том, что на предприятии нет эффективной системы оценки кандидата на этапе его трудоустройства в компанию. Такая система могла бы включать анализ личностных качеств кандидата, его достижений на предыдущих местах работы, рекомендаций его коллег и непосредственных руководителей и т.д.

Вторая причина заключается в том, что на постсоветском пространстве нет целостных систем профилактики и предотвращения мошенничества со стороны собственного персонала. Как показывает опыт, подразделения, которые имеют к этому непосредственное отношение, – департаменты по персоналу, службы безопасности, службы внутреннего аудита и пр. – работают сами по себе. И порой они не только не сотрудничают, но и открыто конфликтуют и соперничают между собой. Поэтому очень часто все течет само по себе до тех пор, пока уже сам факт мошенничества не открывается сам по себе. И тогда начинается: «Почему это произошло? Кто куда смотрел?»

– По статистике около 80% ущерба материальным активам компаний наносится их собственным персоналом. В чем корень зла – в человеческой природе и желании взять то, что плохо лежит, в неправильной работе с персоналом, в личности руководителя?

– В криминалистике существует т.н. треугольник мошенничества, который описывает необходимые условия для того, чтобы сотрудник пошел на должностное преступление и мошеннические действия. Этот треугольник состоит из трех вершин: давление, возможность, оправдание. Чтобы человек пошел на совершение преступления, необходимы все три элемента этого треугольника. У человека в жизни в какой-то момент может возникнуть высокое давление внешних обстоятельств, когда ему срочно будут нужны деньги (погасить кредит банку, вернуть долг, заплатить за дорогостоящее лечение и т.д.). Но одного этого



Справка

Ярослав КАПЛАН – предприниматель с 20-летним опытом, консультант по управлению (обучался и практиковался в Дании, США, России и Латвии), вице-президент по стратегическому маркетингу компании «ПЕРФОРМИЯ СНГ», которая специализируется на эффективных решениях для найма сотрудников.

НАШИ ГОСТИ

фактора самого по себе недостаточно, чтобы человек пошел на преступление. В этот момент времени ему также нужно иметь такую возможность. Например, бесконтрольный доступ к расчетному счету предприятия, наличным средствам, материальным ценностям, оборудованию и т.д. Когда у сотрудника есть оба эти фактора – давление внешних обстоятельств и возможность что-то украсть, то тогда ему остается только придумать себе оправдание своим действиям, чтобы чувствовать, что он все равно остается правым, даже когда совершает преступление. Например, сотрудник может так оправдывать свои действия: «Я заслуживаю этого, мой вклад в компанию больше того, что я получаю», или «Я честный человек, а то мог бы взять намного больше», или «Кто-то на моем месте взял бы намного больше»...

– Можно ли распознать нечестного человека уже на первом собеседовании? Следует ли каждого кандидата на вакансию рассматривать как потенциальную угрозу?

– Я противник того, чтобы устраивать в компании «охоту на ведьм». Тем не менее в компании должны быть эффективная система оценки кандидата на стадии трудоустройства, наблюдения за поведением уже работающих сотрудников, анализ общих и персональных рисков персонала, оптимизация систем вознаграждения и т.д. Правильная проверка кандидата на работу – это не конец, а только начало функционирования системы кадровой безопасности предприятия. Проходит время, и сотрудник может начать мыслить и совершать поступки в соответствии с новыми жизненными обстоятельствами.

– Какие службы в первую очередь в ответе за кадровую безопасность?

– Говоря о кадровой безопасности, нужно помнить, что это система, включающая целый комплекс мероприятий. Разработка и контроль этой системы должны лежать на собственниках организации и высшем руководстве компании. В качестве исполнительской части требуется скоординированная деятельность практически всех подразделений компании, включая департамент по персоналу, службы внутренней безопасности, службы внутреннего аудита и т.д.



ПРАВИЛЬНАЯ ПРОВЕРКА КАНДИДАТА НА РАБОТУ – ЭТО НЕ КОНЕЦ, А ТОЛЬКО НАЧАЛО ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ КАДРОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ.

– Ущерб организации может быть нанесен сотрудником непреднамеренно. Казнить или помиловать в таком случае, если сотрудник в целом эффективен и это его первый промах?

– Нужно признать, что в большинстве случаев, когда речь идет о кадровой безопасности, сотрудник идет на должностное преступление и мошенничество совершенно осознанно и заранее планирует это преступление, чтобы «замести следы». Часто он вовлекает в эту схему и других сотрудников, формируя круговую поруку в этом

коллективе, что осложняет обнаружение фактов мошенничества и увеличивает размер причиненного ущерба. Если говорить о непреднамеренном ущербе, то в случае его обнаружения имело бы смысл провести с сотрудником дополнительное обучение требованиям безопасности на предприятии и позволить сотруднику добровольно компенсировать причиненный ущерб.

– Как вычислить преднамеренного мошенника?

– Это совсем не простой вопрос, и на него нет однозначного ответа. Конечно, существует целый набор признаков, по которым можно сделать те или иные выводы. Но эти выводы руководство компании сможет сделать только в том случае, если на предприятии существует целая система мониторинга кадровой безопасности.

– Известно, что лучшее лечение – профилактика. Какие профилактические меры нужно использовать, чтобы не допустить мошенничества?

– Лучшей профилактикой против мошенничества могло бы стать создание в организации такой корпоративной культуры, в которой бы все сотрудники были заинтересованы в достижении целей организации и относились бы к бизнесу компании, как к своему собственному. В такой организации мошенникам будет неуютно, и многие из них предпочтут найти себе другого работодателя-жертву.

– Расскажите о самом грандиозном случае мошенничества в вашей карьере.

– На меня наибольшее впечатление произвел «творческий» подход сотрудников ИТ на складе одного крупного оптового предприятия. Имея доступ к коду программы, программист перепрограммировал формулу расчета остатков на складе. Стандартная (бухгалтерская) формула расчета остатков такая: Остаток на начало периода + Приход – Расход.

Программист «усовершенствовал» эту формулу следующим образом: Остаток на начало периода + Приход – Расход – 5 штук. Таким образом, он мог бесплатно брать со склада каждый месяц по 5 единиц любого товара, и при этом не возникало «минусов» при ежемесячных инвентаризациях. Учитывая, что ассортимент в этой фирме

был около 3000 единиц товара при средней стоимости единицы 10-30 долл., мы можем посчитать нанесенный ущерб.

– Как управлять кадровой безопасностью в период массовых сокращений? Увольнение сотрудника по инициативе нанимателя может стать и поводом для мести. Как обезопасить компанию и предотвратить нежелательные последствия?

– Тут все будет зависеть от того, как именно будет проходить сокращение затрат. Например, вместо простого сокращения штата, допустим, на 25%, можно перевести какое-то количество сотрудников на неполную ставку, в т.ч. 0,1-0,25 ставки, и по мере улучшения ситуации постепенно возвращать полную ставку, можно создавать рабочие группы из «временно непрофильных» сотрудников» и решать острые проблемы в кризисный период, можно по-



Фото Валерий Шайгар

могать уволенным сотрудникам в поиске работы, можно сохранить премирование за сверхрезультат и т.д. Все эти действия могут значительно повлиять на то, как сотрудники будут интерпретировать происходящее в компании. Лучшим способом обезопасить компанию и предотвратить нежелательные последствия будет разработка продуманного антикризисного плана, в котором следует заранее предусмотреть все действия, которые компания должна будет произвести, если наступит кризисная ситуация. Этот план нужно разработать до того как такая ситуация может наступить. В этом случае есть возможность выиграть время и заранее продумать наилучшие «пути выхода» и предусмотреть различные сценарии. ■