



КТО И КАК ОХРАНЯЕТ ТАЙНЫ БЕЛОРУССКОГО БИЗНЕСА

Проблема конфиденциальности и информационной безопасности бизнес-компании в ближайшее время станет одной из основных для руководителей и топ-менеджеров: многие в связи с наступившими тяжелыми временами собираются заняться «липосакцией бизнеса» или, проще говоря, сокращением и оптимизацией персонала, следовательно, будут увольняться люди, которые знают о фирме многое, если не все. Кроме того, ужесточится конкурентная борьба, а уж о том, что «кто владеет информацией, тот владеет миром» известно давно. Как сохранить коммерческую тайну компании и обезопасить свой бизнес от утечки информации? Корреспондент портала www.interfax.by попросил рассказать об этом эксперта по вопросам безопасности **Александра Радкевича**.

Подписка о неразглашении – формальность!

По мнению эксперта, каждый руководитель или владелец компании должен лично заботиться о сохранении конфиденциальной информации. Именно он, а не глава службы безопасности, должен оценить риски и необходимый уровень защиты.

«Информационная защита предприятия начинается с того, что главный человек в компании должен определить круг вопросов, которые действительно представляют коммерческую тайну данного предприятия. На каждом предприятии уровень этой информации, диапазон и степень секретности различны. Причем от размеров компании это не зависит - может быть фирма и из трех человек, но если она работает в жесткой конкурентной среде, то ее внутренняя информация ценится на вес золота. В понятие «секретная» может входить разная информация - все, что касается финансово-хозяйственной деятельности предприятия, подбора и расстановки кадров и многое другое», - утверждает А.Радкевич. И лишь после полной оценки начинается работа по защите этой информации.

«Все заботятся о защите информации по-разному. Одни идут по формальному пути, то есть в дополнительном к контракту соглашении работник подписывает обязательство о неразглашении служебной информации. Если руководитель компании думает, что это очень действенная мера безопасности и на этом останавливается, то совершает большую ошибку: это, в принципе, пустой документ, который рассчитан больше на психологическое воздействие на человека, которого берут на работу», - утверждает эксперт. По его словам, этот документ «рассчитан на честных людей и никаким образом не ограждает предприятие от утечки информации». «Человек, который пришел к вам устраиваться на работу со злым умыслом - все подпишет! Он знает, что рычага давления на него в этом плане нет. Законодательное поле и такие документы, о которых идет речь, не позволяют защитить конфиденциальную информацию предприятия», - предупреждает А.Радкевич. Естественно, речь не идет о подписании обязательства о неразглашении государственных тайн и т.п.

Доверяй, но ограждай

После определения границ той части информации, утечки которой руководитель предприятия хотел бы избежать, предпринимаются определенные организационные меры по защите информации. Как утверждает эксперт по безопасности, следующий шаг - определение круга людей, которые владеют этой информацией по должностным обязанностям. «Этот круг должен быть минимизирован. Кроме того, руководителю стоит позаботиться о том, чтобы текучесть кадров, владеющих конфиденциальной информацией, был минимальна. Для этого в компании должно быть сделано все, чтобы сотрудники, владеющие конфиденциальной информацией, были абсолютно лояльны и чувствовали себя комфортно. Другими словами, чтобы у них даже и мысли не возникало сменить работу», - советует А.Радкевич.

По его словам, недальновидные руководители, которые не заботятся о таких вопросах, в конце концов сталкиваются с тем, что на важных, связанных с коммерческой тайной, постах начинается текучка, а бывшие сотрудники (носители конфиденциальной информации) уходят «в поле». «Отследить их не представляется возможным - они вполне могут устроиться к вашим конкурентам, и коммерческая тайна вашей компании будет продана «за бочку варенья и корзину печенья». А может быть просто разглашена - большей частью во внешнюю среду информация уходит именно таким образом», - отмечает эксперт.

Ключевым моментом соблюдения информационной безопасности является ее «дозирование» - каждый сотрудник должен владеть именно тем объемом информации, который положен по его должности и соответствует его компетенции. И не больше! «Это - ключевой момент информационной безопасности компании. «Перетекания» информации из высших эшелонов в низшие и ее «брожения» в коллективе попросту



не должно быть. В противном случае получается базар: все знают всё, и руководитель компании является заложником ситуации и теряет над ней контроль», - предупреждает А.Радкевич.

Не болтай!

Человек, покинувший компанию с «камнем за пазухой», безусловно, пойдет устраиваться на работу по профилю - скорее всего, к вашим конкурентам. Указав в анкете прошлое место работы, он проходит собеседование и уж там... «Когда во время собеседования начинаешь правильно задавать определенные вопросы, то получаешь нужные ответы и для себя начинаешь представлять, каким образом построена система финансово-хозяйственной деятельности на предприятии, где ранее работал соискатель рабочего места. Да, зачастую, обиженные сотрудники как на духу рассказывают все тайны со своего прошлого места работы, стараясь продемонстрировать лояльность потенциальному работодателю», - утверждает А.Радкевич.

Впрочем, палка о двух концах - «болтуна» могут просто не взять на работу. «Руководитель во время собеседования оценивает, какую информацию доводит до него соискатель и для себя принимает решение: либо взять человека на работу, но на ту должность, где он будет знать минимум и не доставит никаких проблем, либо вообще не возьмут на работу. Руководителю ведь становится понятно, что если с этим работником не сложатся отношения, то вся информация об его фирме станет всеобщим достоянием», - объясняет эксперт.

Кадровый вопрос

Каждый руководитель должен себе четко представлять - кого он хочет видеть на той или иной должности. И просчитывать, что за его решением последует. Например, хотите, чтобы все конкуренты узнали о вашей финансовой деятельности? Наймите заместителем главного бухгалтера молодого амбициозного человека!

«Главный бухгалтер в каждой компании - стабильный человек, который имеет очень высокую меру ответственности, достаточно высокую зарплату и т.д. и т.п. Как правило, главного бухгалтера всеми силами стараются удержать и вообще руководитель делает все возможное, чтобы на этой должности люди у него менялись как можно реже. Но есть такая позиция, как заместитель главного бухгалтера. Круг вопросов, которыми он занимается уже, чем у главбуха, однако последний и заболеть может, и в отпуск уйти. И тогда его заместитель получает доступ ко всей информации и решает все вопросы, которыми обычно занимается главбух! Но статус его ниже, как и заработная плата. В конце концов, а это может произойти уже через полгода, он сам захочет стать главным бухгалтером и... уйдет, унося с собой важнейшую информацию! Получается своеобразная кузница кадров, а это уже очень плохо», - объясняет эксперт.

Без провокаций!

«Многие говорят про воровство информации. В этом отношении самая главная защита - не создавать условий для воровства. Допустим, если у вас золотые слитки лежат прямо в коридоре, то рано или поздно у кого-то обязательно появится желание положить слиток в портфель. Получается, сам хозяин спровоцировал человека на воровство! То же самое касается и информации», - утверждает А.Радкевич.

По его словам, нельзя выкладывать на стол то, что не должны видеть работники, не обладающие должной компетенцией. Если это случилось - это уже провокация. Человек просто подумает: «А почему бы и нет? Я в «зачачку» положу - будет какой-то рычаг давления на администрацию. Или заработать на этом смогу». Каждый должен знать и оперировать тем объемом информации, который ему положен в соответствии с его компетенцией. Кроме того, в этом отношении важны элементы воспитательной работы и построения взаимоотношений с персоналом. Если работник чувствует себя в компании комфортно, уважает руководство, ощущает стабильность своего положения - воровать не будет.

Кроме того, по мнению А.Радкевича, руководители среднего и нижнего звена очень хорошо должны знать своих подчиненных, все их проблемы, запросы, чаяния и нужды. «Если ты сможешь сотруднику, то он у тебя по чисто моральным соображениям не сможет ничего взять! Это как раз тот аспект, который является очень сильным сдерживающим фактором», - подчеркнул эксперт.

Безусловно, из каждого правила бывают исключения. Однако главное, чтобы исключения не становились правилом. Если все ваши тайны будут известны конкурентам - успеха не видать. В бизнесе мелочей не бывает, а сохранность коммерческой тайны - совсем не мелочь...

**интервью Александра Радкевича
председателя правления ООО «Сэйф Бизнес Компани»
для Interfax.by**