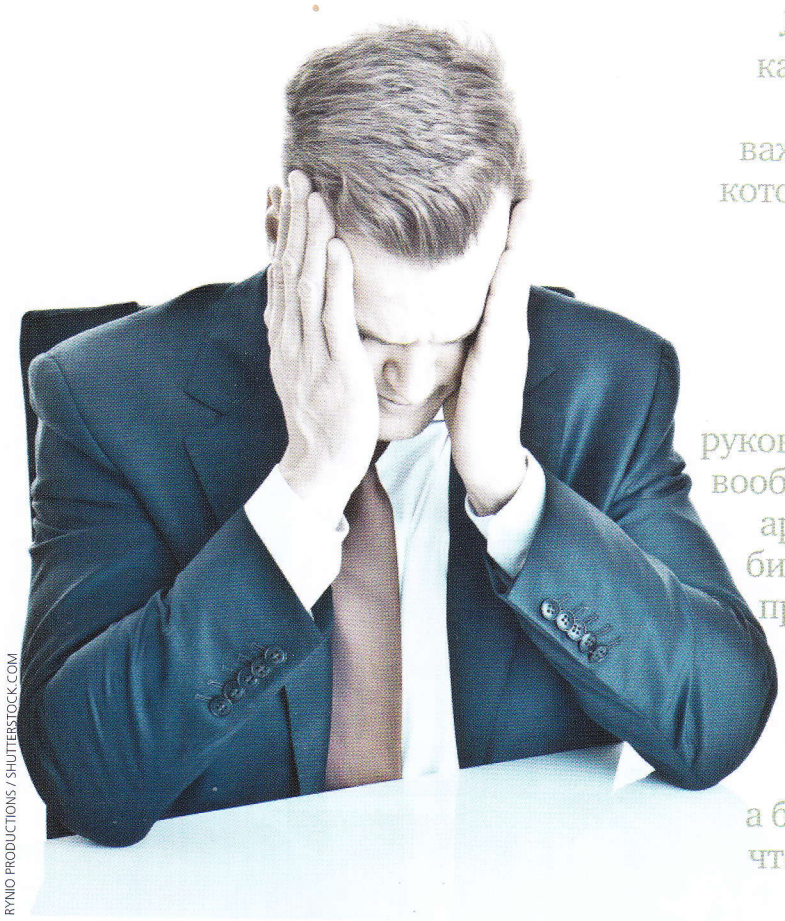
АНДРЕЙ ГЛЕБОВСКИЙ,
разработчик и преподаватель курсов по экономической и кадровой безопасности
Учебного центра «Информзащита»

Как минимизировать риски, связанные с внезапным увольнением ключевых сотрудников



RYNIO PRODUCTIONS / SHUTTERSTOCK.COM

Любой читатель согласится с тем, что каждый случай увольнения ключевого сотрудника, на котором завязаны важные бизнес-процессы, контрагенты, который обладает «критической массой» конфиденциальной информации, а тем более – если он в курсе «проделок» руководства компании в области налогового, таможенного и т. д. законодательства, – стресс для руководства и компании в целом. Богатое воображение моментально рисует целую армаду рисков, готовых разнести ваш бизнес в клочья. А если это увольнение происходит внезапно… А если еще и в конфликтной обстановке… Тут уже и подумать страшно! Не очень умный руководитель будет гнать от себя эти черные мысли, а более прозорливый – озаботится тем, чтобы заранее минимизировать риски такого варианта развития событий.

Превентивная деятельность должна иметь два аспекта: организационный и оперативный (информационный)

Организационный аспект включает в себя:

- готовность руководства компании к тому, что подобная ситуация может возникнуть;
- готовность осуществить кадровые перестановки, с тем чтобы оголившийся участок не оставался безнадзорным, готовность к замещению вакантной должности;
- построение такого уровня взаимодействия между структурными элементами системы внутреннего контроля (служба безопасности, кадровое подразделение, линейный менеджмент), при котором малейшие признаки того, что ключевой сотрудник норовит «навострить лыжи», немедленно осмысливается и ложится в основу проведения комплекса мероприятий по минимизации возможного ущерба.

К оперативному (информационному) аспекту мы относим:

- наличие юридической базы, позволяющей СЭБ контролировать действия увольняемого и предупреждать попытки причинения вреда компании;
- способность СЭБ обеспечить «информационное прикрытие» увольняемого, когда его деструктивные действия будут находиться в поле зрения лиц, информирующих СЭБ о происходящем в секторе их наблюдения;
- способность и готовность руководства компании и СЭБ противостоять попыткам шантажа и вымогательства со стороны увольняющегося ключевого сотрудника.

Давайте попытаемся, насколько позволяют рамки статьи, рассмотреть этот сложнейший и актуальнейший вопрос по превентивной деятельности.

Начнем с того, что в регламенте взаимодействия структурных подразделений должно быть четко прописано: любая информация о подозрениях на то, что какой-то ключевой сотрудник намеревается уволиться, должна поступать в СЭБ или от службы персонала, или от руководителя подразделения. От своевременности получения службой безопасности такой информации зависит, удастся ли предпринять какие-то меры по предупреждению рисков наступления неблагоприятных последствий от такого увольнения, насколько эти меры будут эффективны.

Не нужно быть семи пядей во лбу, чтобы сделать следующий вывод: чем выше служебное положение сотрудника в компании, тем выше риски наступления негативных для фирмы последствий его нелояльности и, как крайнего проявления нелояльности, прямого предательства интересов компании. Следовательно, контролю лояльности именно таких сотрудников на всех этапах их функционирования в компании СЭБ должна уделять максимально возможное внимание.

В развитие этой мысли проведем такую аналогию. Согласно кодексу Бусидо каждый самурай должен просыпаться утром с мыслью о том, что он сегодня умрет. Это помогает самураю жить праведно (у него не будет времени на замаливание грехов) и умереть достойно (он заранее психологически готов к этому событию).

Любая информация о подозрениях на то, что какой-то ключевой сотрудник намеревается уволиться, должна поступать в СЭБ

Так же и каждый начальник СЭБ должен просыпаться с мыслью о том, что именно сегодня любой из ключевых сотрудников компании может подать заявление об увольнении с неясными (но подозрительными) последующими намерениями. Разумеется, эта «головная боль» должна касаться не только сотрудников СЭБ, но и руководителя компании, и HR-директора. Поэтому, если вопрос касается высшего звена ключевых сотрудников – представителей топ-менеджмента, то в компании должна быть разработана система эффективного замещения. Создание такой организационной структуры дает нам следующие преимущества:

- во-первых, мы никогда не знаем достоверно, кто из наших работников в какой момент окажется «слабым звеном», и потому должны быть готовы к любому варианту развития событий;
- во-вторых, осознание топ-менеджером факта, что он может быть без проблем замещен, дисциплинирует и не позволяет возомнить себя незаменимыми.

Разумеется, речь не идет о полноценном дублировании, как в экипажах космических кораблей, – это слишком накладно. Но на первое время, до поиска новой кандидатуры, без ощутимого ущерба предприятию финансового директора может заменить главный бухгалтер или аудитор, HR-директора – начальник отдела кадров и т. д.

Рассмотрим самую проблемную ситуацию – увольнение ключевого сотрудника в конфликтной ситуации. Здесь возможно два варианта:

- конфликт вызревал давно, предположения о предстоящем увольнении этого работника существовали и ситуация не стала ни для кого неожиданностью;
- решение об увольнении стало неожиданным для руководства компании. Если решение топ-менеджера об увольнении принято им спонтанно, например, в результате нелицеприятного разговора с учредителем, то такое увольнение следует рассматривать как форс-мажорное обстоятельство. В такой ситуации СЭБ изначально была лишена возможности предпринять какие-либо предупредительные меры и никаких претензий к ней предъявлено быть не может. Но и сам топ-менеджер, еще вчера не помышлявший об увольнении, не имел реальной возможности подготовиться и умыкнуть конфиденциальную информацию.

Если же ключевой работник заранее готовился к увольнению, но до официального объявления им о своих намерениях руководство компании об этом не знало, то такая ситуация свидетельствует о том, что ни начальник СЭБ, ни руководитель службы персонала, ни руководитель подразделения не справляются со своими обязанностями по контролю лояльности персонала. За такую халатность вполне заслуженным будет строгое взыскание.

В этой ситуации СЭБ следует прогнозировать дальнейшее развитие событий. Многое тут зависит от причин конфликта, личностных качеств увольняющегося, от положения компании на рынке (входит в ограниченное чис-

ло участников рынка или рынок переполнен), от степени активности конкурентной борьбы, от специфики работы увольняющегося сотрудника и от множества других факторов.

Рассмотрим два примера:

- В конфликтной ситуации увольняется коммерческий директор средней по масштабам охвата рынка торговой фирмы, занимающейся розничной реализацией продуктов питания. Рынок, на котором работает эта фирма, огромен, и поэтому появление еще одного безработного как источника какой-то конфиденциальной информации о коммерческих тайнах этой торговой компании вряд ли у кого-либо вызовет ажиотажный интерес. На первоначальном этапе нового работодателя еще может заинтересовать клиентская база, но не более того.
- В аналогичной ситуации увольняется директор по производству компании, которая специализируется на производстве эксклюзивной продукции, например, оборудования для подводных работ. Таких компаний на всю Россию наберется не более десятка, конкуренция в борьбе за вожделенный госзаказ очень велика. Специалист обладает уникальными познаниями и навыками, которые он может реализовать только у конкурентов. Естественно, он не пожелает кардинально изменить свою профессиональную ориентацию, его опыт и навыки – отличный товар, который пользуется спросом. Этот топ-менеджер моментально будет принят на работу к конкурентам на еще более льготных условиях, чем имел прежде.

Очевидно, что во втором случае риски негативных последствий для компании от такого увольнения будут гораздо опаснее, чем в первом. Это заставляет нас сделать вывод о том, что СЭБ должна использовать все имеющиеся в ее распоряжении рычаги мониторинга корпоративной лояльности для контроля за ключевыми сотрудниками. Человеку, психологически не готовому следовать рекомендуемому нами кодексу «Бизнес-Бусидо», нелегко решиться на проведение подобных мероприятий при отсутствии признаков деструктивного поведения топ-менеджера, неловко подозревать хорошего и преданного интересам компании человека. Порядочным людям вообще свойственно считать и всех окружающих такими же порядочными людьми. Кроме того, прижимистый руководитель компании может считать, что не нужно тратить ресурсы там, где пока нет проблемы.

Возможно, убедить такого щепетильного руководителя в необходимости принятия превентивных мер помогут результаты исследования, проведенного Международной антивирусной компанией ESET (Словакия) в ходе совместного опроса с FutureToday, ведущим российским консультантом в области управления брендом работодателя:

«17 % респондентов признались, что им доводилось уничтожать ценные документы, переписку или программное обеспечение, чтобы навредить бывшему работодателю.

13 % опрошенных поступали более прагматично. Они уносили с собой рабочие материалы (например, базу клиентов, планы, отчеты и другие данные) для последующей продажи или использования на новом месте работы.

Около 4 % сотрудников после увольнения пользовались недоработками ИТ-специалистов прежней компании, в частности, заходили в рабочую почту или продолжали удаленно посещать корпоративные ресурсы.

Еще 4 % респондентов открыто мстили бывшему работодателю – публиковали корпоративную информацию (от финансовых документов до личных данных руководства) в Интернете.

В 25 % компаний принято ограничивать доступ увольняющегося сотрудника к корпоративной информации в последние дни работы. 22 % сразу же после ухода работника отключают удаленный доступ к почте, а 16 % меняют пароли от всех корпоративных ресурсов, которыми пользовался уволенный». http://www.esetnod32.ru/company/press/center/38-sotrudnikov-slivali-sekrety-eks-rabotodateley/

Работодатель имеет право контролировать целевой характер использования ресурсов

AFRICA STUDIO / SHUTTERSTOCK.COM

Задача СЭБ – убедить руководителя компании в том, что должна быть разработана соответствующая система превентивных мер по минимизации ущерба от деструктивных действий информированного сотрудника. Причем эта работа должна проводиться не тогда, когда он уже проявил свою недружественность по отношению к компании, а уже сейчас. И сами ключевые сотрудники должны знать о возможности осуществления за ними такого контроля и понимать его необходимость. Кого-то такая информированность, возможно, удержит от совершения действий в ущерб компании, а кого-то подтолкнет действовать изощренно и конспиративно. Но, как говорится, на то и щука, чтобы карась не дремал. Для того руководство компании и платит своим безопасникам, чтобы они успешно противодействовали ухищренным вредителям.

Вот с таким «конспираторами» и должна вести борьбу СЭБ. А тут уже «на войне – как на войне», кто кого. Основное оружие сотрудника СЭБ – работники вашей компании, которые творчески подходят к исполнению своих трудовых обязанностей, предусмотренных ст. 21 Трудового кодекса РФ – «Основные права и ОБЯЗАННОСТИ работника», в частности – «незамедлительно сообщить работодателю либо непосредственному руководителю о возникновении ситуации, представляющей угрозу… сохранности имущества работодателя…». Именно эти неравнодушные и лояльные компании лица и должны проинформировать представителей администрации о том, что увольняющийся задумал что-то недоброе в отношении активов или интеллектуальной собственности компании.

Однако кроме информационного потенциала людей с активной жизненной позицией сотрудникам СЭБ следует вооружиться и техническими средствами, применение которых будет правомерным лишь в том случае, если вы заранее обеспокоились этим вопросом, учитывая ряд юридических вопросов. В частности, рекомендуется внести в трудовой договор следующие положения:

17% УВОЛЕННЫХ СОТРУДНИКОВ ПРИЗНАЛИСЬ, ЧТО ИМ ДОВОДИЛОСЬ УНИЧТОЖАТЬ ЦЕННЫЕ ДОКУМЕНТЫ, ПЕРЕПИСКУ ИЛИ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ЧТОБЫ НАВРЕДИТЬ БЫВШЕМУ РАБОТОДАТЕЛЮ

- Работник ознакомлен и согласен с тем, что работодателем в служебных и подсобных помещениях компании ведется видеонаблюдение и видеозапись в целях обеспечения противопожарной, антитеррористической безопасности и контроля за соблюдением сотрудниками правил внутреннего распорядка, трудовой дисциплины и режима коммерческой тайны;
- Работник ознакомлен и согласен с тем, что корпоративная электронная почта используется им исключительно в служебных целях и работодатель может контролировать целевое использование корпоративной электронной почты.
- Работник ознакомлен и согласен с тем, что компьютерная техника представляется ему работодателем исключительно для решения служебных задач и не может использоваться в личных целях для хранения, изучения и передачи любой неслужебной информации. Работодатель имеет право контролировать целевой характер использования закрепленной за сотрудником компьютерной техники и выделенного ему интернет-трафика.

Естественно, что главная цель всех перечисленных здесь технических мероприятий – получение объективной информации о том, чем занят сотрудник (группа сотрудников) в рабочее время на рабочем месте. Особенно актуальны эти приемы и методы контроля на стадии увольнения работника, когда уровень его корпоративной лояльности стремится к нулю или имеет уже отрицательное значение.

Что может и должна предпринять СЭБ при получении информации о предстоящем увольнении сотрудника, имея в руках рекомендуемый инструментарий? Для ответа на этот вопрос следует исходить из того временного интервала, который мы имеем в своем распоряжении.

В любом случае предстоит осуществить следующие действия:

- Установить контроль за тем, какие именно работы сотрудник выполняет на своем компьютере.
- По возможности установить аудио- и видеоконтроль за его действиями на рабочем месте.
- Ориентировать доверенных лиц СБ из окружения увольняемого на контроль за его поведением – ксерокопированием каких-то документов, скачиванием информации на внешние носители, настораживающими факторами поведения.
- Согласовать с руководством компании и со службой персонала оптимальную дату последнего дня работы сотрудника. Тут интересы разных подразделений могут быть различны: руководитель цеха может настаивать на двухнедельной отработке, пока он подыщет замену, а для сотрудников СЭБ чем раньше он окажется за воротами – тем лучше, ведь у увольняемого будет меньше шансов навредить предприятию. Естественно, при этом должны четко соблюдаться требования Трудового кодекса РФ.
- Отключить пользователя от выхода в сеть Интернет и от локальной компьютерной сети.
- По возможности в наиболее сжатые сроки изъять у него служебный компьютер.

Изложенные в данной статье рекомендации – лишь примерный алгоритм универсальных и общеобязательных мероприятий, которые мы рекомендуем провести, чтобы избежать шока от увольнения ключевого сотрудника вашей компании. ●