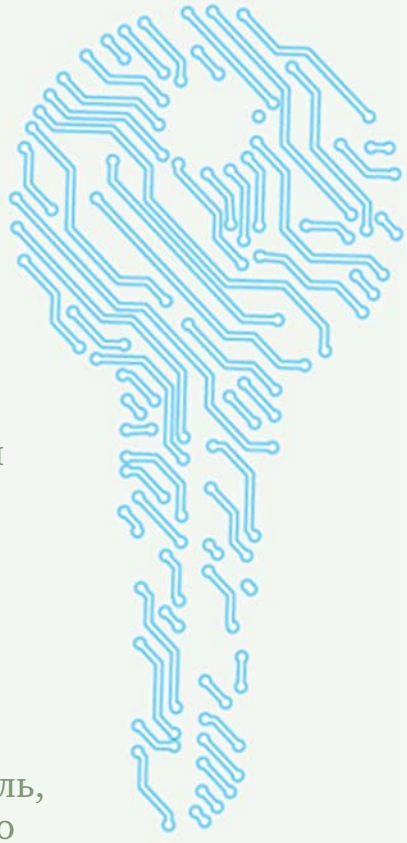
АНДРЕЙ ГЛЕБОВСКИЙ,
учебный центр «Информзащита»

Повышение эффективности работы СЭБ на стратегических направлениях



SHUTTERSTOCK.COM/EPIFANTSEV

Перед большинством собственников и представителей топ-менеджмента компаний сегодня стоит непростая задача: как путем относительно небольших затрат обеспечить наибольшую эффективность деятельности компании на различных бизнес-направлениях. Особую актуальность эта проблема приобретает, когда речь заходит об обеспечении надлежащего уровня комплексной корпоративной безопасности. Задача-максимум здесь выглядит очень привлекательной: мы вкладываем в развитие собственной системы корпоративной безопасности (экономическую, информационную и кадровую ее составляющие) рубль, а в результате получаем многократную эффективную отдачу. И эти мечтания не являются несбыточными, большинство экспертов в области корпоративной безопасности единодушны в том, что затраты на поддержание приемлемого уровня безопасности компании как минимум окупаются, а зачастую – окупаются многократно.

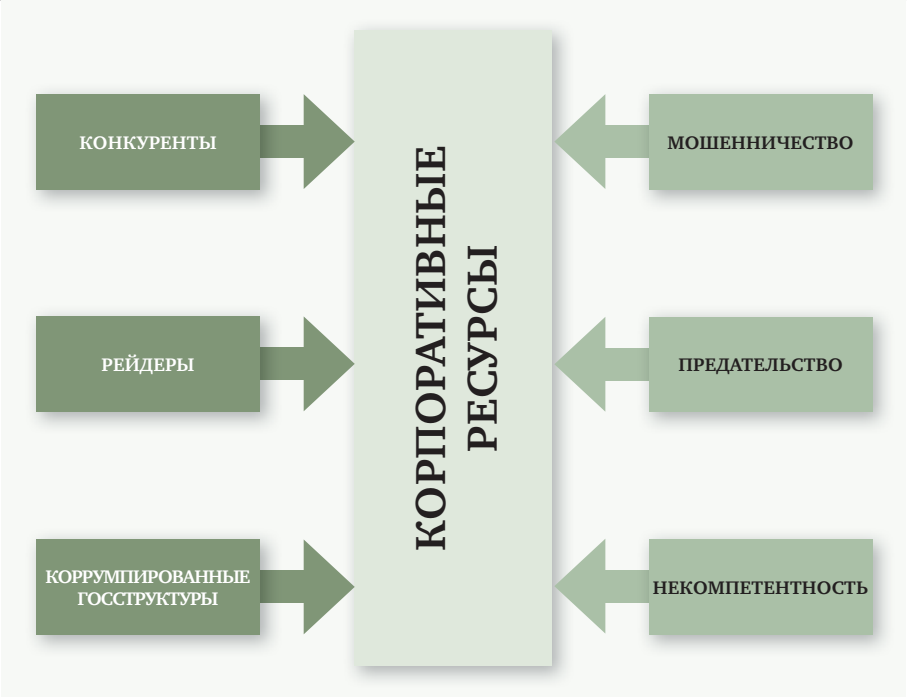
Но как только речь заходит о направлениях инвестиций в безопасность, то сразу возникает дилемма, сущность которой состоит в правильности определения адресности этих вложений. Если провести аналогию с военной наукой, то суть проблемы состоит в следующем: мы должны определиться распределить ли нам выделенные на обеспечение безопасности ресурсы равномерно по всем направлениям, т. е. распылить свои силы, или же сосредоточить эти ресурсы на наиболее важных направлениях, сформировать своего рода «ударный кулак», которым мы нанесем сокрушительное поражение нашему противнику? Ответ очевиден и вся история великих мировых сражений основана на том, что победитель смог сформировать решительный перевес в силах и средствах на главном направлении атаки и потому выиграл битву.

Это положение нашло свое воплощение в так называемом «законе Парето», согласно которому 20 % наших усилий, сосредоточенных на правильно выбранных направлениях, дадут нам 80 % желаемого результата, а остальные 80 % усилий, которые распределятся по менее важным направлениям, будут иметь КПД лишь 20 %. Следовательно, крайне важным для нас является правильность определения основных, «стратегических» направлений приложения усилий по обеспечению эффективного функционирования системы корпоративной безопасности компании.

Вопрос о том, какие именно направления корпоративной безопасности являются «стратегическими», является дискуссионным и тут могут высказываться различные мнения. Личный опыт автора говорит о том, что такими направлениями являются:

- Кадровый отбор сотрудников СБ.

Рисунок 1.



- Работа с персоналом компании на всех этапах его производственного функционирования.
- Создание эффективно действующей сети информаторов.
- Инструментальный контроль индивидуальной лояльности.
- Работа с контрагентами.

Кратко, насколько позволяют размеры журнальной статьи, остановимся на каждом из рекомендуемых нами направлений.

Кадровый отбор сотрудников СБ

Это направление мы не просто так поставили на первое место. Вопросы профессионализма и наивысшего уровня корпоративной лояльности сотрудников СБ являются ключевыми. Если собственник будет вкладывать в безопасность компании значительные средства, но распоряжаться этими средствами будут некомпетентные сотрудники или так называемые «имитаторы кипучей деятельности», а еще хуже – склонные к совершению мошеннических действий сотрудники СБ, то тут «закон Парето» действовать не будет.

Но сказать легко, а как реально обеспечить эффективность отбора соискателей на должность сотрудника СБ? Буквальное толкование Федерального закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ существенно затрудняет наши попытки получить объективную информацию о соискателе. Если речь идет о выходце из системы правоохранительных органов, то узнать, на каких должностях он служил и как себя зарекомендовал практически невозможно – эта информация имеет гриф «секретно».

Но даже в таких непростых условиях расписываться в собственном бессилии было бы неправильным. Проведение собеседования с кандидатом опытным сотрудником СБ, использование широкого спектра инструментальных методов контроля существенно повышает результативность выявления нежелательного контингента будущих сотрудников подразделения безопасности.

Типичной ошибкой сотрудников СБ и кадровых служб является следующее: тщательно проверив кандидата на стадии приема его на работу, про него забывают до того момента, пока он не совершит что-то из ряда вон выходящее или пока не возникнет необходимость его уволить

Работа с персоналом компании на всех этапах производственного функционирования

Типичной ошибкой сотрудников СБ и кадровых служб является следующее: тщательно проверив кандидата на стадии приема его на работу, про него забывают до того момента, пока он не совершит что-то из ряда вон выходящее или пока не возникнет необходимость его уволить. До этого момента никто не интересуется, что представляет из себя данный сотрудник, каков уровень его персональной корпоративной лояльности. А ведь именно от этого и зависит, станет ли наш коллега расхищать активы компании, продавать на сторону нашу конфиденциальную информацию или творить другие гадости.

Тут же возникает вопрос: чья лояльность для нас наиболее актуальна? Должны ли мы в равной степени пристально интересоваться уровнем лояльности уборщицы и финансового директора? Для ответа необходимо оценить каждого сотрудника как потенциального носителя конкретных групп рисков, и тут далеко не все зависит от его формального статуса в компании. Так,

SHUTTERSTOCK.COM/SEAMARTINI

персональный водитель генерального директора может быть носителем весьма существенных рисков: он знает все маршруты передвижения первого лица компании, зачастую слышит его телефонные переговоры и т. д. То же можно сказать и об уборщице, которая наводит чистоту в комнате переговоров и может установить там «жучок». Для отнесения сотрудника к определенной группе риска рекомендуется использовать так называемый «треугольник мошенничества», так же именуемый как «гипотеза Дональда Кресси».

Но даже если мы верно определили круг объектов нашего пристального наблюдения, то возникает другой вопрос: каким образом контролировать их индивидуальную корпоративную лояльность? Ответу на этот вопрос посвящены два следующих раздела данной статьи.

Создание сети информаторов и обеспечение ее эффективного функционирования

Это наиболее дискуссионный и деликатный вопрос, который некоторыми оппонентами утрируется и толкуется как насаждение корпоративной политики всеобщего доносительства. При ответе возможным участникам дискуссии следует начать со статистических данных о КПД внутренних информаторов в деле борьбы с корпоративным мошенничеством. По данным издания «Директор по безопасности», из общего количества выявленных фактов корпоративного мошенничества на долю информаторов из числа сотрудников приходится более 25 %. Вопрос дискутирующим поборникам морали: вы готовы пожертвовать четвертью расхищенных корпоративными мошенниками активов компании ради сохранения своих белых одежд незапятнанными «позором сотрудничества» с современными «Павликами Морозовыми»? Вряд ли найдутся такие расточители среди собственников бизнеса. Да и чисто юридически точку в этом вопросе поставил законодатель, который в ст. 21 Трудового кодекса РФ четко прописал ОБЯЗАННОСТЬ работника «незамедлительно сообщить работодателю либо непосредственному руководителю о возникновении ситуации, представляющей угрозу… сохранности имущества работодателя». Остается лишь провести четкую грань между таким информированием, в морально-этической подоплеке которого заложен высокий уровень корпоративной лояльности, и омерзительным «стукачеством», совершаемым для сведения счетов, продвижения по карьерной лестнице и т. д. Но это – дело профессиональной подготовленности сотрудника СБ, о которой мы говорили ранее.

Как бы ни был хорошо подготовлен сотрудник СБ в профессиональном плане, его богатый опыт не может быть в полной мере реализован, если ему работодателем не предоставлен правовой (на уровне локальных нормативных актов компании) и технический инструментарий. Поэтому мы рекомендуем юридическому и кадровому подразделениям включать в содержание трудового договора с работником компании следующие положения:

- Работник ознакомлен и согласен с тем, что Работодателем в служебных 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.

Тем, кто склонен рассматривать эти положения как ущемление личных прав гражданина, ответил Европейский суд по правам человека, который, в частности, указал, что работодатели имеют право читать личные сообщения сотрудников в электронной почте или мессенджерах,

отправленные в рабочее время. Поэтому стенания по поводу неотчуждаемости конституционных прав гражданина и работника в данном случае представляются неуместными. Ведь никто в здравом уме не станет возражать против запрета водителю халтурить на заводской машине или против контроля несения службы полицейским на посту. А чем отличается от этого ситуация с контролем содержания работ, выполняемых на служебном компьютере в служебное время (за которое, кстати, работодатель платит работнику деньги)?

Определившись с легитимностью подобного контроля за действиями работника, остается лишь наметить круг лиц, представляющих повышенный интерес в плане обеспечения надлежащего уровня корпоративной безопасности, своевременно получать и правильно оценивать те объемы информации, которые станут доступны в результате работы информационного подразделения СБ.

Организация эффективной работы с контрагентами

Все сказанное до сих пор относилось ко внутриорганизационным моментам. Но, осуществляя свою коммерческую деятельность, любая компания оказывается вовлеченной в определенного вида контрагентские отношения. А раз так, то у нас автоматически возникают риски быть обманутыми мошенниками (особенно актуально при работе с контрагентом на условиях товарного кредита или отсрочки платежа), а также риски непроявления нами должной налоговой осмотрительности при выборе контрагента или риск невольно быть втянутыми в такую цепочку взаимоотношений с другими фирмами, когда действия вашей компании могут быть истолкованы как соучастие в отмывании денежных средств, добытых преступным путем, или как финансирование экстремизма (терроризма). Другими словами, нам необходимо знать, с кем мы сотрудничаем и иметь у себя набор доказательств, подтверждающих проявление нами должной осмотрительности при принятии решения о сотрудничестве с тем или иным контрагентом (клиентом).

Неоценимую помощь здесь оказывают нам информационно-аналитические системы, в частности, наиболее популярные сейчас «СПАРК-Интерфакс» и «Контур.Фокус». Открывая стартовую страницу любой компании, мы сразу получаем целый комплекс информации о потенциальном контрагенте, его деловой репутации и отдельных характеристиках, указываемых регуляторами в качестве «тревожных симптомов» – адрес массовой регистрации, частое участие в судах в качестве ответчика по причине неисполнения договорных обязательств, количество исполнительных производств, скоринговые оценки и т. д. Кроме того, мы можем с помощью информационно-аналитических систем получить интереснейшую информацию о персоналиях – собственнике и руководителе нашего потенциального контрагента.

Например, нас интересуют сведения о бизнес-активности г-на Норкина Юрия Викторовича, ИНН 616823631887. Открываем его персональную страницу в любой информационно-аналитической системе, и что мы видим? Он является учредителем или генеральным директором в 97(!) компаний[1]. Посмотрим внимательнее перечень основных направлений деятельности возглавляемых им компаний и подивимся многофункциональности и бизнес-талантливости Юрия Викторовича:

- ООО «Боно-Трейд» – оптовая торговля металлами и металлическими рудами.
- ООО «Стрим-Плюс» – деятельность в области права и бухгалтерского учета.
- ООО «Креатив и внедрение» – деятельность, связанная с использованием вычислительной техники и информационных технологий.
- ООО «ХимТоргГарант» – торговля оптовая автомобильными деталями, узлами и принадлежностями.
- ООО «Волга Ойл» – торговля оптовая ювелирными изделиями.
- ООО «АналитЦентр» – исследование конъюнктуры рынка, и так – 97 раз!

Не будем давать юридической оценки деятельности уважаемого Юрия Викторовича, просто припомним требования, изложенные ФНС РФ в приказе от 30.05.2007 № ММ-3-06/333@ и в письме от 11.02.2010 № 3-7-07/84:

«Под фирмами-однодневками налоговыми органами признаются юридические лица, не обладающие фактической самостоятельностью, созданные без цели ведения деятельности, как правило, не представляющие налоговую отчетность, зарегистрированные по адресу массовой регистрации и т. д.»

Таким образом, используя возможности информационно-аналитических систем, в течение буквально нескольких минут мы можем получить огромные массивы информации как о потенциальном контрагенте, так и о физических лицах, возглавляющих эту компанию. Ну, а сможем ли мы сделать из этой информации правильные выводы – целиком и полностью зависит от того, насколько профессиональны сотрудники нашей СБ. Итак, круг замкнулся: все начинается с высоких требований к деловым и личностным качествам сотрудника СБ и этим же заканчивается.

Если взглянуть на предлагаемые здесь основные, «стратегические» направления приложения усилий, то очевидной становится отсутствие необходимости каких-то крупных денежных вливаний. Нельзя же рассматривать выделение компанией нескольких десятков тысяч рублей в год на подключение к информационно-аналитической системе как ощутимый удар по бюджету серьезной компании. Все остальные перечисленные здесь направления и вовсе носят организационно-управленческий, а не затратный характер.

Безусловно, предлагаемые здесь направления приложения усилий – не догма, а база для осмысления проблемы с учетом специфики конкретной компании. Остается пожелать нашим читателям успеха в этой работе и помнить, что для достижения успеха нам необходимо будет затратить минимум усилий. Главное – правильно определить точки приложения наших усилий! ●

[1] Эта информация согласно ст. 8 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» получена из общедоступного источника персональных данных.