



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

# Предотвращение сговора сотрудников службы безопасности и склада

В НЫНЕШНИЕ КРАЙНЕ СЛОЖНЫЕ В ЭКОНОМИЧЕСКОМ ПЛАНЕ ВРЕМЕНА особую актуальность приобретают вопросы деструктивности вектора устремлений различных категорий работников компаний. Это очевидно: в условиях, когда корабль компании нещадно бросает по волнам штормящего бизнес-моря, крайне важна слаженность работы всей команды. А если кто-то из матросов нашей компании начинает прорубать дыры в борту, то живучесть нашего условного бизнес-судна становится весьма проблематичной. ДРУГИМИ СЛОВАМИ, корпоративное мошенничество является существенной угрозой компании в любые времена, а в кризисной ситуации НЕГАТИВНЫЕ РИСКИ ВНУТРИКОРПОРАТИВНОГО «КРЫСЯТНИЧЕСТВА» многократно усиливаются.



**П**ри этом мошенник мошеннику рознь. Одно дело, когда рядовой работник ликеро-водочного завода выносит через проходную спрятанную за пазухой четвертинку, и совсем другое – когда менеджер этого завода, подделав документы, мошенническим путем похищает целую фуру элитной алкогольной продукции. Следовательно, в кризисных условиях собственникам бизнеса необходимо выделить группы наиболее подверженных риску внутрикорпоративного мошенничества сотрудников.

Применим для этого сформулированный Дональдом Кресси «треугольник мошенничества», вершинами которого являются три основных фактора:

- возможность совершения мошенничества;
- давление внешних обстоятельств;
- самооправдание.

Рассмотрим подробнее фактор возможности. Как известно, «кто что охраняет, тот то и кушает». Наиболее широкий спектр возможностей для совершения хищений имеют те сотрудники компании, в функционал которых входит совершение тех или иных операций с активами (денежные средства, товарно-материальные ценности и т.д.), – назовем их условно логистами. Но много ли наворуешь в одиночку, под бдительным оком недремлющей и высокопрофессиональной службы экономической безопасности (СЭБ)? Следовательно, следующий вывод: чтобы воровать много, долго и безнаказанно, надо привлечь в соучастники сотрудника СЭБ. И вот тут уже можно говорить о формировании устойчивой преступной группы, которая будет действовать активно и безнаказанно.

Как предотвратить формирование такого криминального альянса? Дать исчерпывающий ответ на этот вопрос весьма непросто, но попробуем определиться с основными направлениями этой работы. Нам видится два стратегических вектора:

- предотвращение **самой возможности** сговора сотрудника СЭБ и логиста;
- предотвращение **последствий** такого сговора.

Естественно, что наиболее перспективным является предупреждение возможности криминального сговора. Конечно же, мы не доводим ситуацию до абсурда и не призываем исключить возможность общения безопасника и логиста. Речь идет о другом: степень лояльности этих групп сотрудников должна исключать саму возможность

изучения личности кандидатов в эти службы. Это весьма и весьма непросто в силу архиважности проблемы. Вопросы приема на работу материально ответственных лиц – тема отдельного большого разговора.

И эти проблемы многократно усиливаются, если вам требуется получить информацию о предшествующем

## Чтобы воровать много, долго и безнаказанно, надо привлечь в соучастники сотрудника СЭБ. И вот тут уже можно говорить о формировании устойчивой преступной группы

возникновения у них преступных замыслов. Причем это должно происходить не от того, что эти люди просто не понимают, где и что можно украсть. Если этой специфической группой познаний не обладает ни логист, ни безопасник, то они просто непрофессионалы: плох тот сторож, который не имеет представления о том, где находится дыра в заборе, и о том, как могут украсть охраняемое им имущество.

Напротив, эти сотрудники должны уметь предвидеть все ухищрения потенциальных мошенников, знать способы совершения хищений и методы их выявления. Но высокий уровень корпоративной лояльности не позволит им использовать свой профессиональный инструментарий для совершения хищений. И вот здесь мы вплотную упираемся в вопросы кадровой безопасности и проверки кандидатов на потенциально криминогенные должности.

Общеизвестно, что болезнь гораздо проще предупредить, чем потом долго и трудно лечить. Следовательно, сотрудники кадровых служб должны проявлять максимум усилий при

профессиональном опыте сотрудника СЭБ. Здесь возможны два варианта:

- соискатель на должность сотрудника СЭБ ранее работал в аналогичной структуре другой компании;
- соискатель не имеет такого опыта, он только что уволен из правоохранительных органов.

Рассмотрим первый вариант. Каждому, кто пытался получить объективную характеристику на соискателя с прежнего места работы, прекрасно известны все сложности этого процесса, обусловленные требованиями закона РФ «О персональных данных». Если мы ведем речь о получении характеризующих сведений на бывшего сотрудника СЭБ, то этот процесс многократно усложняется: деятельность по обеспечению экономической безопасности компании непременно подпадает под категорию коммерческой тайны, и бдительный кадровик не станет рисковать и информировать вас о каких-то прегрешениях бывшего безопасника, даже если такие имели место. Следовательно, остается довольствоваться лишь лаконичной записью в трудовой

книжке об увольнении «по собственному желанию». Но каковы были истинные причины этого увольнения? В любом случае следует иметь в виду, что безопасников просто так не увольняют: слишком уж много они знают.

Как определить набор компетенций соискателя-безопасника? В резюме, которое вывешивается на рекрутинговом сайте, все соискатели пишут о своем высоком профессионализме. Но тогда возникает вопрос: «Если ты такой уж “крутой профи”, то почему ты остался без

т. д. совсем не приходится: личное дело бывшего сотрудника имеет гриф «совершенно секретно». Основными источниками информации о прошлом опыте оперативной или следственной работы в такой ситуации являются его собственные рассказы о себе, любимом. Насколько они правдивы? Если кадровик ранее носил погоны, то он сможет распознать болтуна и вралю. А если у кадровика такого опыта нет? Остается только развесить уши и слушать байки бывшего опера или следователя о его «героическом»

старшего начальствующего состава в подразделениях БЭП, ОПУ, ГУСТМ (аналитическая разведка, проведение специальных технических мероприятий).

- Знание и навыки обращения со спецтехникой, системами информационной безопасности и контроля.
- Знание методов и специфики работы спецслужб.
- Разрешение на оружие.
- Установленные связи по взаимодействию с большинством правоохранительных, административных и иных структур».

Убаюканная рассказами мошенницы (бывшей рыночной торговки), некой Оксаны Петровны С-ко (она же По-ва), HR-директор способствовала ее назначению на должность руководителя информационно-аналитического подразделения СЭБ. Осмотревшись на новом месте, эта мошенница вместе со своим соучастником не только успешно развела руководство компании на крупные суммы, выделяемые для «решения вопросов в различных инстанциях» (см. последний пункт резюме), но и встала на путь прямого предательства корпоративных интересов: по своей инициативе установила контакты со службой безопасности компании-конкурента и в течение длительного времени передавала конфиденциальную информацию, тоже отнюдь не бесплатно.

Так каким же образом можно минимизировать риски трудоустройства на ключевые должности в СЭБ и логистическое подразделение подобного рода «Оксаны Петровны» и ей подобных? Видится один выход – применение различных инструментальных методов контроля. Подробный обзор этих методик дан в статьях Никитина М.Ю., преподавателя УЦ «Информзащита».

Мы не будем останавливаться на широком спектре возможностей этого высокоэффективного и весьма экономичного инструментария. Приведем лишь цитату из бессмертного произведения С. Михалкова «Дядя Степа – милиционер»: «Ведь недаром сторонится милицейского поста и милиции боится



© DEPOSITPHOTOS.COM/ELCIGASS

**В любом случае следует иметь в виду, что безопасников просто так не увольняют: слишком уж много они знают**

работы? Почему прежний работодатель не рекомендовал тебя своим знакомым?» Добиться внятного ответа на этот вопрос, как правило, бывает непросто.

Второй рассматриваемый нами вариант – наш кандидат только что уволился из правоохранительной системы. Здесь рассчитывать на помощь кадровиков из МВД-ФСБ-СК и

прошлом. А тут недалеко и до фатальных ошибок.

Типичный кейс. HR-директор крупной московской компании занималась подбором кандидатур на должность безопасника-аналитика и прельстилась таким вот резюме «бывшего майора милиции»:

«1994–2003 г. Служба в органах внутренних дел на должностях среднего и



тот, чья совесть нечиста!» Перенесем эту мудрость на нашу тематику и прочно уясним себе: если кандидат на «криминогенную» должность в ответ на ваше предложение пройти обследование на полиграфе или с помощью других инструментальных методов контроля начинает громогласно стенать о нарушении его прав или пытаться обойти эту преграду – будьте уверены, на 100 % что-то здесь нечисто! Лучше откажитесь от услуг такого работника!

Подводя итог первой части рассматриваемой темы, можно сказать, что если вам удалось подобрать на должность сотрудника СЭБ и логиста людей с негибким внутренним стержнем порядочности, то стоящая перед вами задача обеспечения сохранности активов решена на 90 %. Еще 10 % мы оставляем на то, что изначально честный и порядочный человек, попав в обстановку корпоративной нелояльности, может деформироваться в плане личностных установок и быть вовлеченным в криминальную деятельность. Однако это – тема для другой статьи.

Но давайте допустим, что выполнить вышеописанные требования нам не удалось, и в компании сформировался криминальный тандем из логиста и сотрудника службы безопасности. Для достоверности картины сюда следует включить еще и сотрудника бухгалтерии, отвечающего за учет вверенных логисту товарно-материальных ценностей. Вот это уже крайне опасно, и тому есть весьма наглядные примеры.

«Прокуратура в Приморье направила в суд уголовное дело о хищении металлоконструкций более чем на 96 млн руб. при строительстве моста с материка на остров Русский во Владивостоке, возведенного к саммиту АТЭС-2012», – сообщает РИА «Новости» со ссылкой на краевое УМВД России.

По данным полиции, 32-летний бывший сотрудник службы безопасности компании «Мостовик» Рафаэль Джавадов наладил схему криминального вывоза и сбыта металлоконструкций.

Для этого подозреваемый создал организованную группу, в составе которой были работники контрольно-пропускного пункта, беспрепятственно пропускавшие определенный транспорт, и кладовщики, имеющие свободный доступ к металлу. Также он приобрел технику для перевозки металла, водителем которой назначил ранее судимого за похищение человека жителя города Находка.

«Похищенное со складов компании-застройщика подозреваемые сдавали в пункты приема металла во Владивостоке. Предварительный ущерб от их действий превышает 96 млн руб.», – сообщает УМВД.

«За один криминальный рейс вывозили со складов компании металлоконструкции на сумму более чем на полмиллиона рублей», – отмечает «Интерфакс» со ссылкой на пресс-секретаря полиции УМВД России по Приморскому краю Евгению Соковишину.

[www.kommersant.ru](http://www.kommersant.ru)

Г-н Джавадов и его поделники далеко не одиноки в своих криминальных устремлениях к чужим товарно-материальным ценностям. У думающего собственника бизнеса рано или поздно должны возникнуть взаимосвязанные вопросы.

- Не творится ли что-то подобное в моей компании?
- Кому в моей компании можно верить, если даже безопасникам не следует доверять на все 100 %?

Ответ содержится в народных мудростях о шиле в мешке и о том, что «сколько веревочке ни виться...». В подобной ситуации следует исходить из того, что все тайное рано или поздно становится явным. Чем выше уровень корпоративной лояльности основной массы работников, тем больше шансов на то, что информация о совершаемых хищениях поступит руководству компании по горячей линии или от информаторов службы экономической безопасности, не все же безопасники – воры!

Но в этом случае собственнику бизнеса придется иметь дело с материальными последствиями, то есть с реальным ущербом, который возместить весьма и весьма непросто, а зачастую – невозможно. Поэтому вряд ли можно предложить разумную альтернативу превентивным профилактическим мероприятиям, исключающим саму возможность криминального сговора между сотрудником СЭБ и работником логистического подразделения. ●