Охрана предприятия

№2, 2010 (№12)

Оглавление

Охрана торгового центра: пример успешной работы с кадрами

Охрана предприятия за рубежом

Как набирали и обучали охранников на Олимпиаду в Ванкувере

Как охраняется метро в Нью-Йорке

Недавние взрывы в московском метро вновь привлекли внимание СМИ к проблемам безопасности подземки в других городах мира.

Агентство АП распространило материал, посвященный охране нью-йоркского метро, которое имеет 468 станций, работает круглосуточно, перевозит в среднем 5 миллионов человек в день.

Метро в США входит в число наиболее приоритетных объектов, охраняемых от террористов. Этим занимается специально созданное после 9 сентября 2001 года антитеррористическое подразделение. Там внимательно изучают уроки террористических актов или их попыток в метро Мадрида, Лондона, Бомбея, Москвы.

В самые последние годы предприняты дополнительные меры безопасности: организация мобильной патрульной службы с оружием и специально тренированными собаками, оснащение сотрудников подразделения специальными приборами обнаружения вещества для использования «грязной ядерной бомбы», проведение ежегодно десятков тысяч проверок (наудачу) багажа пассажиров, специальные тренинги для выявления в толпе и задержания подозрительных лиц.

Кроме того, перед каждым входом (въездом) в туннель установлена небольшая будка с полицейским, там же - монитор, на экран которого передается изображение от видеокамер внутри тоннелей.

Каждый час полицейские проходят по вагонам, сопровождают поезда в водительской кабине. Как только обнаружится подозрительный предмет, немедленно сообщается начальству по специальной связи, но не по радиосвязи, используемой обычно полицией, – из-за риска, что радиосигнал может привести в действие предполагаемое взрывное устройство.

Важно отметить, что все сотрудники подразделения по охране метро проходят интенсивное обучение, дабы свободно ориентироваться в разветвленной сети платформ и туннелей, хорошо знать все входы и выходы, в том числе и предназначенные для использования в чрезвычайных ситуациях.

Опрятное трехэтажное здание в районе Бруклина ничем не выделяется в квартале. Между тем, в нем скрывается секретный вход в самое чрево нью-йоркской подземки. Журналисту агентства АП разрешили пройти туда при условии неразглашения адреса и увиденных деталей. Корреспондент пишет, что вход перекрывает мощная,

укрепленная болтами дверь, оснащенная тревожной сигнализацией и детекторами движения. Проникнуть незамеченным совершенно невозможно.

Владелец и арендаторы офисных помещений: кто из них и как отвечает за охрану

Есть такая американская поговорка: «хорошие соседи - все равно, что хороший забор». Она справедлива и применительно к вопросу об охране здания, где офисы арендуют разные компании. Ведь проблема с безопасностью у соседа легко может стать и вашей головной болью.

Обычно ни одна из фирм, арендующих помещения, не берет на себя полностью заботу о безопасности и охране всего здания. Вы ошибетесь, посчитав, что это исключительная обязанность владельца здания.

Тим Бартковьяк одновременно и владелец, и арендатор. Он директор службы безопасности крупной розничной сети Spartan Stores, которая управляет 54 супермаркетами, 21 магазинами и тремя автозаправочными станциями на Среднем Западе. Корпорация владеет рядом торговых помещений, другие она арендует.

Бартковьяк уверен, что основная тяжесть по обеспечению безопасности должна ложиться на плечи арендатора. В статусе владельца зданий его корпорация устанавливает металлические двери, надежные запоры, прочные оконные рамы. Но что касается оборудования и эксплуатации системы видеонаблюдения, патрулирования охранниками территории паркинга по вечерам, то за это, по его мнению, отвечают арендаторы. Мотивация такова: чем больше берешь на себя, тем выше ответственность, если что-то случается. А отвечать за все возможные преступления в отношении арендаторов владелец не хочет. «Спасение утопающих – дело рук самих утопающих».

Там, где Spartan Stores арендует помещения, Бартковьяк предпочитает сам организовывать охрану служащих и имущества компании, нежели полагаться на владельцев: «Мы вносим необходимые изменения в организацию безопасности, руководствуясь конкретной ситуацией и потенциальными угрозами. Если надо, устанавливаем систему видеомониторинга, меняем двери, организуем охрану служебных и транспортных подъездов» (Csoonline.com, April 1, 2005).

Он считает, что заниматься охраной помещений должен тот, кто там повседневно работает. Разделение полномочий по безопасности между владельцем и арендатором оформляется в арендном договоре или отдельным документом. Каких-либо универсальных правил, стандартов здесь нет. Тем более, если речь идет о здании, в котором работают разные фирмы-арендаторы. Обычно обязанности владельца не распространяются дальше установки прочных дверей и надежных замков.

Ситуация стала немного меняться после атаки террористов 9/11. В ходе переговоров об аренде помещений больше внимания уделяется вопросам безопасности. Если раньше в вестибюлях высотных, многоэтажных зданий обычно охраны не было, то в последние годы такое положение стало редкостью. Задачу обеспечения контроля за

доступом теперь, как правило, берут на себя владельцы строений. Как замечает Фил Бэнкс, директор консалтинговой фирмы Banks Group в Ванкувере, «все чаще арендаторы офисных помещений требуют от владельцев отчета, какая часть от вносимой ими арендной платы идет на охрану» (там же). Обычно она составляет 1%-6% от аренды.

Будущие арендаторы, обеспокоенные безопасностью, перед подписанием соглашения досконально проверяют наличие тревожной, пожарной сигнализации, запасных выходов, лестниц для экстренной эвакуации, выдвигают дополнительные требования, которые фиксируются в соглашении.

(продолжение в следующем номере)

Паркинги и гаражи: факторы безопасности

Многие, возможно, не помнят или не знают, что первая попытка взорвать Международный торговый центр в Нью-Йорке произошла еще в феврале 1993 года. Тогда сработавшая бомба была заложена в подземном гараже. Небоскреб не пострадал, но были человеческие жертвы.

К счастью взрывы гремят в подземных гаражах крайне редко. Преступления там обычно связаны с кражами вещей из автомобилей, реже - с фактами насилия. «Мы ни разу не сталкивались с грабежами и нападениями на людей», - говорит руководитель службы безопасности компании E-Trade, снимающей офис в высотке, Боб Лука, - «как правило, преступники разбивают окна авто, крадут магнитолы и забытые в машинах вещи. Служащие нашей фирмы этим очень обеспокоены» (itworld.com, March 10, 2010).

Естественно, что, ставя утром машину в гараж, владельцы хотят спокойно работать, не тревожась, что кто-то в нее залезет. И это дело охраны обеспечить надежную защиту. Какие для этого есть средства и пути? «Наличие обзора и постоянное наблюдение – вот два главных фактора, предупреждающих преступность», - утверждает Поль Дюбуа, исполнительный директор компании Tomasi-Dubois and Associates, консультирующий по вопросам охраны паркингов.

В больших зданиях подземные гаражи и паркинги обычно используются не одной компанией. Именно с этим обстоятельством сталкивается служба охраны упомянутой выше E-Trade. Компания хотела бы, но не может установить в подземном гараже, который ей не принадлежит, камеры слежения – вступает в силу закон privacy. Не имеет права и возвести вокруг здания высокий забор, чтобы предотвратить проникновение злоумышленников. Однако компания добилась разрешения установить видеокамеры на самом здании, чтобы отслеживать зону въезда и выезда. Она также заставила владельцев здания обеспечить освещение паркинга в темное время суток в соответствии со стандартами, которые требуют федеральные установления о борьбе с преступностью.

В дополнение к этому служба безопасности компании E-Trade разработала и вывесила во внутренней корпоративной сети (Интранете) инструкцию по безопасности в паркинге. Ничего необычного, рекомендации, продиктованные здравым смыслом: «не

забывайте в машине вещи, притягивающие внимание потенциальных преступников», и все в таком духе. Перед большими праздниками, например, Рождеством, всем служащим компании постоянно напоминают, чтобы забирали из своих машин свертки с подарками.

Руководитель СБ компании Лука регулярно направляет подчиненных посмотреть, все ли в порядке в паркинге, нет ли там чего или кого подозрительного. Поздними вечерами там постоянно дежурят двое охранников компании, обеспечивая безопасной подход заработавшихся служащих к своим машинам. Кроме того, налажен контакт с местным отделением муниципальной полиции. Когда получили информацию, что в районе объявилась банда подростков, Лука добился, чтобы дважды в сутки полицейский патруль объезжал квартал, где находится офис.

Благодаря этим мерам удается избежать нападений на работников фирмы. Между тем, разбойные нападения, изнасилования и даже убийства нередко случаются в больших подземных гаражах и паркингах при казино и крупных торговых центрах.

(окончание в следующем номере)

Когда бизнесу угрожают информационные «хищники»

Часть 2

(начало см. в журнале №11, «Когда бизнесу угрожают «черные лебеди»)

Растущую озабоченность руководителей СБ вызывают проблемы с информационной защитой. Они, может быть, не столь очевидны, как угрозы физической безопасности, но потенциальный ущерб для компании, а, следовательно, и для всей цепочки бизнес-процессов, несопоставимо выше по сравнению с банальными кражами и вооруженными ограблениями.

Эд Аморозо, глава СБ компании AT&T, видит основную проблему для бизнеса в чрезмерной сложности новых информационных технологий: «Компьютеры и сети слишком сложны для управления и контроля….Люди не знают, как остановить эпидемию спама на индивидуальном и корпоративном уровнях».

Джунхо Ли, вице-президент Федерального резервного банка США говорит о головной боли, вызываемой DOS атаками, способными парализовать всю корпоративную компьютерную сеть: «У нас в банке есть всевозможные средства защиты от DOS. Но я настроен скептически. Удар мощностью 10 гигабайт в секунду может вывести из строя как корпоративную сеть, так и провайдеров».

Партнер по безопасности компании Deloitte & Touche Рена Мирс убеждена, что кибер-преступность приближается к своему пику: «Еще 10 лет назад злоумышленники просто хулиганили в Интернете, так сказать, «разминали мозги». Сегодня происходит «монетизация» преступлений – фишинг и спам. Последующие шаги еще более опасны, так как кибер-преступники все время совершенствуют свое оружие». По ее мнению, в настоящее время кибер-преступность предпочитает не громкие атаки, а малозаметную работу, подобно паразитам, которые заводятся в здоровом теле: «не

создавая видимых проблем, они стремятся потихоньку подворовывать интеллектуальную собственность, прибирать к рукам информацию кредитных карт».

Ни Аморозо, ни ЛИ не верят, что средства защиты, используемые провайдерами, могут эффективно предотвратить ущерб, который могут нанести бизнесу все более совершенные и изощренные инструменты кибер-преступности.

Из истории промышленного шпионажа в современной Америке

(начало см. №№-9-11)

Промышленный шпионаж как государственная политика

Во многих странах власти поддерживают и сами участвуют в технологическом и промышленном шпионаже. Зачем они это делают? Прежде всего, для приобретения технологии, годной в военных целях. А также для усиления конкурентоспособности отечественного бизнеса, повышения ВВП.

Участие государства в этой сфере многолико. Привлекаются спецслужбы, подкупаются и переманиваются иностранные специалисты, внедряются инсайдеры. Поддерживаемый государством экономический шпионаж – проблема глобального масштаба. Он более изощренный и искусный, нежели разведка, осуществляемая силами отдельных частных компаний. А потому и более опасный по своим последствиям для интересов страны, потенциальной жертвы шпионажа.

Нередко финансируемые государством шпионские организации маскируются под безобидные гражданские институты. К их числу принадлежит японский Институт физико-химических исследований. В мае 2001 года власти США обвинили двух японцев в попытках овладеть интеллектуальной собственностью, принадлежащей медицинскому научно- исследовательскому центру имени Лернера. Один из них занимал там видное положение. В течение 1998-1999 гг. он и его соотечественник предприняли действия, связанные с хищением результатов генетических исследований по лечению от болезни Альцгеймера. Украденные материалы они переправляли в Институт физико-химических исследований, содержащийся за счет госбюджета и принадлежащий правительству Японии. При этом надо заметить, что по указанию японского министерства науки и технологий упомянутый институт открыл и руководил исследованиями в этой же области медицины.

Следователи установили, что японцы не только пытались похитить научные секреты и нанести физический урон конкуренту, но и уничтожить реагенты и другие физические материалы, полученные в результате лабораторных исследований и испытаний. Главный подозреваемый сбежал домой, но экстрадирован в США не был. Правительство Японии заявило, что оно здесь «не при чем» и вообще «не в курсе дела».

Некоторые вопросы остались без ответа. Был ли японец, работавший в американском центре, специально внедрен туда, или он, будучи принят на работу, по собственной

инициативе решил подзаработать на хищении секретов?. И почему власти Японии отказались выдать его США для завершения следствия?.

Десять недооцененных аспектов охраны предприятия

Десять недооцененных аспектов охраны предприятия

Завершаем изложение материала, опубликованного 29 ноября 2006 года под этим названием на сайте www.darkreading.com

10. Интеграция систем безопасности с программным обеспечением

Можно сколько угодно ругать производителей программного обеспечения, но это дело охранных предприятий - оказывать ни них давление, принуждая к выпуску более надежных и отвечающих требованиям безопасности программных продуктов. Даже мельчайший изъян в программе, интегрированной с системами охраны, простая ошибка в кодировании, могут стать причиной большой головной боли.

К сожалению, компании, выпускающие программное обеспечение, не всегда в состоянии обеспечить надежную идентификацию дефектов, возникающих в интегрированных системах охраны.

По словам эксперта Келли из компании Consilium1, «производители не испытывают достаточного давления со стороны пользователей, чтобы стремиться выпускать продукты с надежными, безопасными кодировками».

Аналитик компании CERT Сиакорд утверждает: «Если покупатели начнут отдавать явное предпочтение более безопасным продуктам перед продуктами с множеством функциональных возможностей, тогда производители начнут делать ставку на надежность и безопасность».

Проблема баланса между функциональными возможностями программных продуктов, которые действительно необходимы, и рисками с точки зрения безопасности – ключевая. Сиакорд считает, что «кибер-преступники выбирают самые легкие и доступные пути, и если атакуемый ими вектор защиты оказывается уязвимым, то летит к черту вся защита. Глупо тратить деньги на защиту одного какого-то вектора, оставляя уязвимыми остальные». Это то же самое, что крепко запирать двери, оставляя открытыми окна.

СКУД без просчетов и ошибок

Часть 2. Закупаем оборудование

Джейсон Коулинг разработал и осуществил множество проектов СКУД для государственных и частных организаций. На страницах онлайнового журнала csoonline.com он выступил с развернутой статьей – руководством по созданию и эксплуатации системы контроля и управления доступом.

Автор выделяет четыре этапа проекта СКУД:

1. Планирование

2. Закупки оборудования (прокьюрмент)

3. Установка, отработка и запуск СКУД

4. Эксплуатация и тренинг персонала

В прошлом номере журнала (№11) были рассмотрены вопросы планирования. Сейчас в фокусе внимания второй этап проекта – закупка оборудования.

Итак, мы определили, кто и за что отвечает в ходе реализации проекта, посоветовались с администрацией здания и коммунальными службами. Пришло время обратиться к поставщикам.

Нужных продавцов найти нелегко. Их много на рынке, предлагающих всевозможные варианты оборудования для СКУД. Но вычислить именно того, кто вам нужен, довольно сложно.

Для начала отберем как минимум три фирмы. Желательно, чтобы они торговали однотипными системами. В противном случае сравнивать, анализировать достоинства и недостатки тех и других просто невозможно. Попросите, чтобы они прислали расценки, характеристики и прочие данные. Но этого мало. Надо, чтобы все они ответили на следующие ваши вопросы:

1. Сколько СКУД и каких характеристик поставили за последний год (или два – три года)? Кому конкретно реализовали? Надо связаться с этими компаниями и собрать отзывы.

2. Является ли предлагаемая вам СКУД оригинальным, запатентованным оборудованием, или она стандартна, совместима и взаимозаменяема с системами ряда других фирм? Это ваше решение – иметь систему, монопольно выпускаемую одной компанией, или распространенную на рынке версию, предлагаемую разными фирмами.

3. Сколько времени потребуется для начала работ по установке после дня подписания контракта? Обычно подготовка к работе занимает 6-8 недель, но у некоторых фирм – дольше, так как они не имеют каких-то комплектующих частей и вынуждены их заказывать.

4. Может ли поставщик в гарантированное время (идеально в течение 24 часов) прибыть для срочного ремонта, если оборудование выйдет из строя? Поинтересуйтесь также, к кому обращаться в этом случае – к местному дистрибьютеру или непосредственно в компанию? Обратите внимание, насколько быстро и адекватно поставщик отвечает на ваши запросы. Если он проявляет медлительность в ходе продажи, то также будет себя вести и в обслуживании.

5. Финансовые условия. Поищите фирму, которая готова продавать, сдавать в аренду, или на условиях лизинга. Попросите предоставить условия по каждому из вариантов и внимательно их изучите с участием финансового директора (бухгалтера).

6. Обязательной узнайте, на все ли оборудование распространяется гарантийный срок. Это должно быть зафиксировано документально. Предпочтителен поставщик, который готов будет в течение гарантийного срока не только возмещать стоимость заменяемого оборудования, но и оплачивать работу техников, осуществляющих замену и ремонт.

Готовим заблаговременно «план реагирования» для системы тревожной сигнализации

На предприятии сработала тревожная сигнализация. Надо реагировать. Но будет ли ваш ответ адекватным? Достигнет ли он ожидаемых целей?

Эти вопросы необходимо задавать еще до установки тревожной сигнализации. И здесь есть, о чем поломать голову.

Джеки Гримм, директор отдела программных решений по безопасности компании Diedbold Security, предлагает ряд рекомендаций по разработке т.н. «плана реагирования» (response plan), который должен минимизировать риски ошибочных действий при срабатывании сигнализации.

Такой план должен учитывать особенности предприятия, объектов мониторинга, и, что особенно важно, – к каким угрозам и опасностям надо быть готовым. Например, противопожарная сигнализация требует немедленных действий, когда каждая минута дорога. Но система (при ее соответствующей настройке) может подать сигнал и на понижение температурного режима хранения продуктов на складе. И в этом случае реагирование будет совсем иным. Все разнообразные, потенциально возможные ситуации необходимо учитывать при подготовке такого плана.

Еще один пример. Отказала одна из камер видеонаблюдения. Если это произошло днем, то, скорее всего, она просто вышла из строя и нуждается в ремонте или замене. Но если она отказала ночью, во внерабочее время – сигнал для серьезной проверки, не дело ли это рук злоумышленников.

Прежде чем окончательно утверждать «план реагирования», его надо проверить после установки системы сигнализации. Инсценируйте одно, два нарушения, чтобы на деле испытать, как будет действовать охрана.

Реакция на сигнал тревоги должна быть незамедлительной, даже если он ложный, вызван, скажем, работой уборщиков в зоне системы сигнализации.

План реагирования - не Священное Писание. Всякий раз, когда появляются новые угрозы, он должен корректироваться. Например, обычно правила предписывают обращение в полицейский участок только после второго, подтверждающего сигнала. Но если в районе расположения предприятия участились ограбления, в план вносится изменение: звонок в полицию после первого же сигнала.

И еще раз надо отметить, что план составляется заблаговременно, до, а не после

установки системы тревожной сигнализации.

(по материалам журнала «The Security Magazine»)

Базовые принципы внутрикорпоративных расследований

Онлайновый журнал CSO от 25 января 2010 года поместил обширную статью о фундаментальных основах подготовки и осуществления расследований преступлений, совершаемых сотрудниками. Начинаем в текущем номере публикацию материала в изложении.

Какие шаги необходимо сделать по планированию расследования?

Адвокат Джон Томпсон, автор ряда книг по этой теме, предлагает использовать для планирования и проведения внутренних расследований следующий перечень обязательных тем и вопросов:

Разработать (если нет в компании) всем понятную, четкую политику в отношении внутренних расследований. Она должна предусматривать все необходимые для расследований процедуры, которые бы соответствовали правовым нормам и существующему законодательству.

Документировать политику компании и предстоящее расследование. Важно письменно зафиксировать, что предпринимаемое расследование будет проводиться в точном соответствии с законодательством страны и политикой компании в этом вопросе. Это нужно на тот случай, если подозреваемый подаст иск на компанию, обвиняя ее в нарушении законов. Другой письменный документ – т.н. «подтверждающий меморандум» (confirmatory memorandum), который фиксирует, что все вовлеченные в расследование стороны, включая подозреваемых лиц, поставлены в известность и дают на это свое согласие.

Минимизировать давление на свидетелей. Давление могут оказывать подозреваемые лица, находясь в офисе. Поэтому Томпсон советует в таких случаях отстранять их временно от работы. Либо проводить расследование конфиденциально, не ставя в известность объект расследования.

Сформировать команду для интервью и разделить задачи. Нежелательно беседовать «один на один» с подозреваемыми в ходе расследования, так как они могут впоследствии опровергнуть собственные же показания. Должны присутствовать не менее двух членов комиссии. Один задает вопросы, другой записывает в блокнот или фиксирует на диктофон.

Собрать все документы и улики: личные файлы, записи телефонных разговоров, расходные счета, расписания деловых встреч, данные о времени прихода-ухода подозреваемых, их компьютерные файлы, перехваты электронной почты.

Предусмотреть возможность и необходимость применения специальных методов

расследования. Речь идет о методах, рискованных с точки зрения их легальности и законности: взятие отпечатков пальцев, обыск, использование подслушивающих и видео-устройств, и т.п. Если есть сомнения, надо заручиться квалифицированной рекомендацией юриста компании и согласием руководства.

Заранее подготовить список вопросов для интервью. Это не означает, что разговор надо вести по бумажке. Но вопросник поможет что-то важное не забыть, в целом повысит качество информации. Важно, чтобы вопросник был приложен к другим документам расследования (записям ответов).

Добиваться письменных заявлений подозреваемых и свидетелей. Это поможет впоследствии, если опрашиваемые лица откажутся от своих первоначальных показаний.

Секрет хранения коммерческих секретов

Все знают в теории, что такое коммерческая тайна, но в реальной практике многие менеджеры и управленцы слабо представляют себе, что именно относится в их компании к секретам, и еще меньше понимают, как их охранять. Между тем, раскрытие коммерческой тайны чревато катастрофическими последствиями для бизнеса. Что стало бы с транснациональной корпорацией Кока-Кола, если бы формула напитка была бы вывешена в Интернете? Разорение.

Авторы публикации в «Business Week» М.Хэлиган и Д.Хаас предлагают свои рекомендации по охране коммерческой тайны. Прежде всего, советуют они, надо разобраться, что составляет коммерческую тайну в вашей фирме. Это могут быть и новые производственные технологии, и данные клиентов, и ценовая информация, и проводимые исследования и даже неудачные опыты. К примеру, формула жидкости WD-40, широко применяемой в мире, в том числе для предотвращения замерзания автомобильных замков и против ржавчины, появилась как результат сороковой попытки. Но засекречены все 40 формул, ибо знание предшествующих неудачных 39 попыток облегчает конкуренту поиск нужной формулы.

Затем важно определить, кто имеет доступ к секретам – в самой компании и извне. Служащие компании имеют определенные обязательства перед организацией, где они работают. Есть еще группа людей, не связанная формальными обязательствами хранить корпоративную тайну. Это поставщики, внештатные консультанты, временные служащие, наконец, потребители товаров. Конечно, невозможно полностью изолировать компанию от внешнего мира, да это и не надо. Существуют разные способы хранения секретов. Например, компания - правообладатель жидкости WD-40 держит написанную от руки формулу в специальном мощном сейфе, который весит 350 кг и находится в бетонном укрытии, охраняется с помощью круглосуточного видеонаблюдения, новейших систем тревожной сигнализации.

Естественно, не каждая компания может себе позволить бункер для хранения секретов. Но любая организация должна знать и придерживаться фундаментального правила: «охрана секретов – дело всех работников компании». Чтоб достичь этого,

необходимо формировать в организации соответствующую культуру внутренних взаимоотношений, чтобы каждый служащий, независимо от должностных обязанностей, понимал, в чем заключается коммерческая тайна компании, осознавал свою личную ответственность за ее сохранение.

Авторы публикации подчеркивают, что речь идет не просто о проведении учебы, тренингов, особенно с новыми работниками. Лекции быстро забываются. Культура – нечто большее, чем просто инструкция: «прочитай, подпиши и верни». Это, прежде всего, осознание каждым служащим, рабочим простого факта, что риск, связанный с утратой секрета, есть прямой риск для него самого – уменьшение зарплаты, социальных взносов, наконец, риск потерять работу. Поэтому охрана коммерческих секретов напрямую связана с его/ее благополучным настоящим и будущим.

Надо постоянно об этом говорить, напоминать, в том числе и о том, что коммерческой тайной может быть любая информация о фирме: данные о поставщиках, предстоящие изменения в ценовой политике, проводимые лабораторные исследования и испытания, практически все, что может быть использовано конкурентами против фирмы. В наше время высоких технологий служащие должны отдавать отчет в том, что открытая переписка по e-mail легко перехватывается, что телефонный разговор может быть подслушан, что информацию с экрана ноутбука в общественном месте можно подсмотреть.

(по материалам сайта bx.businessweek.com за 19 февраля 2010 года)

Шесть важных рекомендаций тем, кто отвечает за личную охрану

начало см. журнал №№ 9, 10, 11

Рекомендация 5. Поддерживать контакты с носителями информации

Информация – что кровеносная система для живого существа. Без нее не обойтись в личной охране. Желательно установить и поддерживать тесные связи с помощниками охраняемой персоны, персоналом отелей, где он останавливается, с организаторами мероприятий, которые он посещает. Если на мероприятии присутствуют и другие вип-персоны, то это хорошая возможность для установления контактов с коллегами, их охранниками. От них можно получить полезную информацию, если, конечно, они захотят ее предоставить.

Когда намечается поездка за рубеж или в незнакомый вам город, неплохо попытаться узнать, кто из ваших коллег там побывал и сможет дать вам полезные рекомендации.
Что касается компании, где работает охраняемый объект, что лучше всего наладить контакты с теми из секретариата, кто отвечает за расписание рабочего времени, планирует в деталях поездки, встречи и мероприятия, а также с представителями СБ и кадровиками.

Рекомендация 6. Не забывать о членах семьи

Наиболее уязвимыми для злоумышленников являются не тщательно охраняемые бизнесмены, а члены их семьи. Известно немало случаев киднеппинга и шантажа.

Служба безопасности должна позаботиться, чтобы супруга, дети и другие близкие родственники, проживающие вместе, имели представление о мерах безопасности и предосторожности, а жилые помещения были бы оснащены системами тревожной сигнализации. Хорошо предусмотреть в доме специальное помещение, где семья могла бы надежно укрыться в случае опасности и дожидаться прибытия полиции.

Иногда наиболее эффективными оказываются самые простые способы охраны. Например, можно до зубов вооружить охрану, но не позаботиться о проверке служащих, непосредственно соприкасающихся с охраняемой персоной по службе.

Охрана - это профессия или занятие, не требующее подготовки?

Такой вопрос поднимает и пытается ответить автор публикации в журнале «Canadian Security Magazine» (January, 2010) Глен Киттерингхэм, специалист по безопасности бизнеса.

«Я всегда удивляюсь и огорчаюсь, - пишет он, - когда встречаюсь с представителями индустрии безопасности, полагающими, что им нечему учиться для того, чтобы лучше выполнять свои обязанности и продвигаться по карьерной лестнице». Таких людей, увы, немало в этой сфере, подчеркивает автор статьи.

Многие, с кем ему приходится общаться, утверждают, что у них «не книжное, а уличное, практическое, подсказанное жизнью образование, и это лучшее, чему можно научиться». Любопытно, что эти же самые люди нередко выражают недовольство своим заработком, но ничего не желают делать, чтобы зарплата выросла.

Было бы полбеды, если бы так рассуждали работники безопасности младшего и среднего звеньев. Но очень разочаровывает, когда столь же пренебрежительно к тренингам, сертификации относятся так называемые «лидеры индустрии безопасности». Среди последних немало тех, кто охотно посещает отраслевые конференции и собрания, даже выступает на них, общается с капитанами бизнеса, но при этом не удосуживается подумать о собственном профессиональном образовании, подтвержденном соответствующими документами. Такие люди, по мнению Глена, дискредитируют понятие цехового профессионализма.

Верхом лицемерия называет он поведение начальников, требующих от подчиненных профессиональных сертификатов пригодности, но при этом не желающих учиться сами. Можно ли представить себе, чтобы компания наняла на ставку главного бухгалтера или инженера человека без документов, свидетельствующих о его квалификации? То же самое можно сказать о многих сферах деятельности – юриспруденции, медицине, машиностроении.

Глен далее пишет: «Перед кризисом, разразившимся осенью 2008 года, я каждую неделю получал звонки с просьбой порекомендовать их для работы охранником или

специалистом среднего звена по безопасности. Нужно признаться, что мне довольно часто приходилось отказывать в этой просьбе по той простой причине, что они просто не имели соответствующего образования и подготовки».

Такую ситуацию необходимо переломить, если «мы хотим, чтобы охрана стала действительно профессией, а не занятием для всех желающих».

Канада: зарплаты охранников и профессиональная учеба

Во многих провинциях Канады местные власти, требуя от охранников пройти обязательный курс обучения, утверждают, что полученный по окончании курсов сертификат гарантирует более высокую зарплату. Вполне логичное и разумное предположение, что более высокая квалификация, приобретаемая на тренингах, должна непосредственно влиять на вознаграждение. Во всяком случае, вернувшись с учебы, охранники вправе рассчитывать на повышение по службе и/или в денежном довольствии. Начальники также вправе ожидать, что их клиенты согласятся на дополнительные расходы с учетом более квалифицированной охраны. Клиентам же ничего не остается, как оплачивать по повышенной шкале услуги охранных предприятий. Такой вот приятный расклад...

Однако на практике все выглядит по иному, пишет эксперт Брайн Робертсон в журнале Canadian Security Magazine: «Уровень зарплат в заключаемых охранными предприятиями контрактах определяется рыночным соотношением спроса и предложения. Трудно встретить менеджера, который бы не хотел, чтобы его сотрудники получали более достойную зарплату, чем ту, которую они имеют. Но все ограничивается двумя непреодолимыми факторами: стремлением руководителей охранного предприятия к росту прибылей и острой конкуренцией на рынке охранных услуг».

В Канаде и США уровень оплаты охранников фиксируется в договорах между охранными предприятиями и клиентскими организациями. Нередко клиенты соглашаются вписать в договор цифру $30/час, понимая, что реально охранники будут получать $20/час. Однако немало и компаний, которые настаивают на буквальном исполнении всех пунктов договора, сознательно занижая уровень зарплат. В конечном счете, все определяет рынок. Если бы все охранные предприятия, присутствующие на конкретном рынке, согласованно подняли бы уровень оплаты охранников на $5, клиентам не оставалось бы ничего кроме как с этим примириться.

В провинциях Канады довольно много компаний, предлагающих курсы обучения охранному делу. Они конкурируют между собой и в принципе стоимость двухнедельных курсов не так уж велика - $500. Если иметь в виду, что минимальный уровень зарплаты, установленный в Канаде с марта 2010 года, составляет $10.25 в час, легко подсчитать, что личные расходы на обучение окупятся в первый же месяц после поступления на службу.

Охрана торгового центра: пример успешной работы с кадрами

Mall Dufferin – один из крупнейших торговых центров Канады. Его площадь – 250 тыс кв. метров. Он включает 120 магазинов. Ежегодно молл посещают 12 миллионов человек.

Начальник службы безопасности центра Митч Бойл пришел сюда работать в 2004 году. В первые шесть месяцев он и его помощники собирали статистические данные о всех происшествиях в торговом центре. Обнаружили, что более половины конфликтов обусловлены слабой подготовкой охранников. Кроме того, было установлено, где и в какое время чаще всего совершаются кражи, в том числе автомобилей со стоянок.

По итогам исследования были предприняты серьезные меры по переподготовке и тренингу всех сотрудников СБ. Владельцы центра выделили для этого соответствующие средства. Если раньше учеба новичков занимала 4 дня, то теперь – 4 недели.

В целом роль безопасности в работе молла возросла. Установили дополнительно 40 камер видеонаблюдения внутри и снаружи центра, развернули еще один стационарный пункт охраны. Но главное внимание стали уделять улучшению кадрового состава охраны. Говорит Бойл: «Я стал подбирать людей по их моральным и интеллектуальным характеристикам. Некоторые из моих помощников прежде не работали в охране, но продемонстрировали готовность учиться, влиться в команду» (canadiansecuritymag.com, January, 2010). От сотрудников СБ теперь требуют умения общаться с посетителями центра, быть дипломатичными, владеть переговорными навыками.

Работа с кадрами дала положительные результаты. В 2009 году по сравнению с 2005 годом число преступлений уменьшилось на 29 процентов, кражи автомобилей – на 81 процент, все виды насилия – на 47 процентов.

Бойл убежден, что в основе достигнутого успеха – умение сотрудников находить общий язык с персоналом центра и покупателями. Безопасность стала важным компонентом бизнеса.

Как набирали и обучали охранников на Олимпиаду в Ванкувере

Международный олимпийский комитет и власти Канады пригласили компанию Australia Severson помочь обеспечить безопасность на Играх. Эта компания хорошо зарекомендовала себя в 2000 году на летней Олимпиаде в Сиднее, и с тех пор регулярно участвует в организации крупных спортивных состязаний, территориально располагаясь на австралийском континенте.

Основатель и владелец компании Северсон рассказал, как проводился набор охранников на последнюю зимнюю Олимпиаду. Всего надо было найти и отобрать 5 000 человек. Эту задачу необходимо было решить в течение 6 недель. Набор был анонсирован в Канаде и других странах Британского Содружества. Именно оттуда в первую очередь рекрутировались охранники для Олимпиады.

«Мы понимали, - говорит Северсон, - что найти достаточное число квалифицированных специалистов только за счет бывших работников спецслужб и правоохранительных органов за короткий срок невозможно. Поэтому сфокусировали внимание на поиск людей из разных сфер, отраслей и их интенсивное обучение».

В результате рекламной кампании было получено свыше 11 тысяч заявок. Отбор проводился тщательно. Все подвергались двойной проверке – компанией Severson и Олимпийским оргкомитетом, чтобы исключить проникновение террористов и преступников.

После проверки и отбора охранники прошли интенсивное обучение. «Мы разработали многоплановый учебный курс, - рассказывает Северсон, - для начала слушатели прослушали лекции общей ориентации, где их ознакомили с особенностями организации и проведения Игр, со спецификой функций, которые на них возлагалась. Затем они погрузились в практические вопросы своей работы, начались занятия с моделированием конкретных ситуаций, тренировки с использование специальной аппаратуры для сканирования и просвечивания. «В частности, занятия проводились в лаборатории, где слушатели проводили немало времени, обучаясь навыкам и умению обнаруживать предметы, запрещенные особым списком МОК к проносу на территорию спортсооружений и олимпийскую деревню».

Одновременно решались вопросы размещения и проживания армии охранников, прибывших сюда из разных концов Канады и из-за рубежа. Специально для них был возведен из готовых панелей и модулей временный жилой район: двухэтажные дома типа общежитий со всеми современными удобствами, включая ванные комнаты и прачечные помещения (после Игр дома разбираются).

Охранникам на Олимпийских Играх выплачивалось жалование в размере 10 долларов в час (для специалистов, работающих с контрольной X-ray аппаратурой – 16 долларов). Кроме того, все они обеспечивались полным комплектом теплой одежды, включая перчатки, шляпы, шарфы.