Охрана предприятия

№4 (26), 2012

Оглавление

Broker, Trader, Law¬yer, Spy: The Secret World of Corporate Espionage
By Eamon Javers. HarperCollins, 320 pages

Исследования

В. Шарлот
Графология безопасности. *Графологическая экспертиза почерка и ее использование в службе безопасности компании*

Безответственность частного бизнеса угрожает национальной безопасности

О негативных аспектах слияния коммерческих и государственных интересов в стратегически важных инфраструктурных секторах экономики США рассуждает эксперт и консультант по вопросам безопасности Син Мартин («Network World», May 04, 2012).

Согласно официальной американской статистики 85% стратегической национальной инфраструктуры США управляется частным бизнесом. Проблема в том, что в целях экономии средств многие компании объединяют в единое целое производственную компьютерную сеть (призванную обеспечивать и контролировать работу инфраструктурного объекта) и коммерческую сеть. Тем самым хакеру предоставляется возможность проникнуть в систему управления объекта, взломав хранилище коммерческих данных.

Кроме того, важно иметь в виду, что компании нередко связаны через Интернет с корпоративными сетями своих партнеров и поставщиков, что также облегчает злоумышленникам задачу вторжения в «святая святых» национально-стратегических объектов.

Все последние тенденции, связанные с развитием и распространением Интернет-технологий, позволяют, по мнению автора, сделать однозначный вывод о растущих рисках для национальных инфраструктур. Ведь прежде, в до-интернетовскую эпоху, системы контроля и управления жизненно важными объектами имели замкнутую конфигурацию, изолированную от внешнего мира. С середины 90 – х годов прошлого века бурно развивающиеся Интернет технологии охватили буквально все сферы экономической жизни. Интеграция физической охраны с интернет технологиями объективно порождает новые уязвимости и риски с непредсказуемо тяжкими последствиями. К примеру, нарушение нормальной работы крупного энергетического объекта способно погрузить в темноту города и целые регионы, лишить население воды и других необходимых средств поддержания жизни. Достаточно вспомнить последствия аварии на электросетях 2003 года, нарушившей нормальную жизнь 55 миллионов жителей США и Канады.

Особо следует сказать об уязвимостях современных систем управления нефтяных и газовых сетей. Не так давно компьютерная сеть министерства нефти Ирана подверглась успешной атаке хакеров и вынудила чиновников срочно отключить

основной терминал экспорта нефти от сети Интернета.

Успех хакеров обусловлен не столько их талантом, совершенством используемой ими технологии, сколько невниманием компаний к элементарным основам компьютерной и информационной безопасности. В числе наиболее распространенных ошибок:

- Недостаточная защищенность программных приложений от внешних проникновений.

- Слабая политика паролей. Статистика информационных утечек показывает, что из 10 миллионов материалов, подвергшихся информационной утечке в последние годы, примерно 8 миллионов содержат электронные адреса и пароли, при этом большинство паролей принадлежат не частным лицам, а компаниям.

- Либеральный подход к наделению сотрудников привилегированными правами доступа к секретной и конфиденциальной информации.

- Тенденция разрешать персоналу приносить на работу и пользоваться личными девайсами.

Во второй части статьи автор говорит о методах и способах минимизировать риски. Изложение читайте в следующем номере нашего журнала.

(по материалам сайта networkworld.com)

Сканеры безопасности

В Соединенных Штатах Америки разрешено применять в аэропортах два вида технологии сканирования пассажиров – backscatter (обратное рассеивание с использованием рентген-лучей) и радиочастотные миллиметровые волны. Первая технология используется компанией Rapiscan, вторая – L-3 Communications. Их плюсы и минусы анализируются в статье М. Харвуда в июньском номере журнала Security Management за этот год.

До недавнего времени обе технологии «догола раздевали» проходящих контроль людей: дистанционно удаленный оператор изучал изображение на мониторе и сообщал контролеру, находящемуся рядом со сканером, представляет или нет угрозу осматриваемый пассажир. Несмотря на то, что оператор с монитором находится в закрытом помещении и не может вживую видеть людей, перспектива оказаться «голым», пусть даже на экране, вызывает раздражение и недовольство пассажиров.

Идя навстречу пожеланиям, компания L-3 Communications внедрила в свои машины технологию ATR (automated target recognition), убирающую с экрана изображение человеческого тела. На мониторе фиксируются только материальные предметы. Тем самым и отпала необходимость держать оператора в удаленном месте, закрытом помещении.

Но остается другая проблема – озабоченность угрозой здоровью от использования рентген-лучей. В странах Евросоюза, например, использование технологии backscatter (которая, кстати, широко применяется в радиолокационных станциях) просто запрещено.

Зато технология миллиметровых волн получила широкое распространение и за пределами США, в частности, в России. Но и к ней есть вопросы. Германия и Франция решили отказаться от этой технологии из-за большого процента (от 25 до 54%) ложных сигналов, спровоцированных такими деталями одежды как пуговицы, молнии, накладные карманы, и даже глубокие складки одежды. Вице-президент L-3 Communications Уильям Фрейн объясняет этот недостаток «устаревшим программным обеспечением» и уверен, что его замена на более совершенную программу «вернет машины в строй в Германии и во Франции».

Надо также упомянуть и о скептиках, полагающих, что террористы способны обмануть сегодняшние технологии сканирования. При этом обычно ссылаются на статью в Journal of Transportation Security, March 2011, авторы которой продемонстрировали возможность безнаказанно пронести через контроль backscatter взрывчатое вещество PETN, используемое террористами.

Еще одна проблема – пропускная способность. В американских аэропортах она составляет сейчас 149 пассажиров в час (до трагедии 9/11 достигала 350 пассажиров в час). Между тем, нагрузки возрастают. По данным экспертов, в ближайшие три года 700 миллионов людей в мире предпримут первый в своей жизни авиа перелет. А к середине столетия услугами авиакомпаний будут ежегодно пользоваться 16 миллиардов пассажиров.

Над всеми этими проблемами ломают голову в лабораториях ведущих мировых лидеров – упомянутых компаниях Rapiscan и L-3 Communications. Стоящая перед ними задача – сделать свои машины более быстрыми, меньшими по габаритам, более эффективными, способными справляться с существующими и потенциально новыми угрозами. Им в затылок дышат конкуренты – компании Morpho Detection (американский филиал французской фирмы Safran) и Microsemi. О них читайте в следующем номере нашего журнала.

Оптические турникеты

В последнее время в сфере СКУД все большую популярность начинают приобретать оптические турникеты. Они представляют собой компонент системы контроля доступа, которая состоит из программного обеспечения, считывателей карт-пропусков, а также предполагает наличие «контролера доступа» (охранника). В отличие от обычных механических устройств оптические турникеты действуют с помощью электронных (инфракрасных) лучей, аудио-визуальных интерфейсов. В них используются не физические средства воспрепятствования несанкционированному проникновению, а звуковые и световые сенсорные устройства. Они контролируют прохождение одного человека по одной карте. Если по одной и той же карте пытаются пройти через турникет двое и более людей, система немедленно подает сигнал тревоги. Оптические турникеты, пишет Синди Дубин в мартовском номере журнала Security Magazine, особенно хороши для зданий с высокой интенсивностью потока входящих и выходящих людей. Они также весьма полезны для отслеживания числа людей, находящихся в здании в каждый отдельный момент.

Некоммерческая организация Pechham Inc., занимающаяся вопросами профессионального обучения и переобучения людей с ограниченными возможностями

(штат Мичиган), занимает здание, которое ежедневно посещают более тысячи человек. Учитывая особенности контингента (много инвалидов), обычные механические турникеты создавали массу неудобств. Компания приобрела трехдорожечный оптический турникет, представляющий собой систему дверей из стекла. Две дорожки (прохода) – стандартные, третья – для колясочников. Посетители, подходя к стеклянным дверям, прикладывают к считывателю закодированную карту, двери открываются на время, достаточное для прохода одного человека. Если же кто-то пытается «прилепиться» сзади, пройти по чужому пропуску, система резким противным звуком сигнализирует об этом оператору (охраннику). Как уверяют в Pechham Inc., с установкой оптического турникета, число попыток несанкционированного проникновения сократилось на 80%.

В кризисном 2009 году небоскреб Mid-Atlantic опустел на три четверти – арендаторы не могли платить высокую ставку за помещения люкс. Владельцы высотки решили воспользоваться моментом, чтобы модернизировать и отремонтировать помещения, повысить уровень безопасности. Частью этого плана стала установка 12 оптических турникетов, контролирующих подход к двум лифтовым холлам. Их ширина значительно меньше, чем механических турникетов, что позволило увеличить число проходов, следовательно, и пропускную способность. Кроме того, не последнюю роль сыграла и эстетика – оптические турникеты выглядят куда элегантнее и современнее своих механических предшественников.

Австралийская компания 321 Exhibition Street в городе Мельбурн переоборудовало одно из своих зданий для сдачи в аренду за хорошие деньги богатым фирмам. Была приобретена и установлена система СКУД, включая использование оптических турникетов с двойными стеклянными барьерами. Первый барьер открывается при прикладывании к считывателю кодированной карты-пропуска и немедленно закрывается, как только посетитель оказывает в своеобразном шлюзе между двумя рядами дверей. Инфракрасный сенсор проверяет, нет в этом пространстве кого-либо еще, кроме обладателя пропуска. Если все в порядке, открывается второй барьер. Все это занимает доли секунды.

Оптические турникеты особенно хорошо зарекомендовали себя как надежное средство отличия служащих, имеющих постоянные карты-пропуска, от посетителей – гостей, которые обязаны предъявить документы, идентифицирующие личность и разъясняющие цель визита.

Социальные сети на вооружении частных детективов

Частные детективы, впрочем, равно как и правоохранительные органы, все чаще обращаются к социальным сетям в проведении расследований. Преимущество социальных сетей в том, что они помогают довольно быстро устанавливать контакты интересующих личностей. Поль Парлон, детектив в администрации Массачусетского университета в Бостоне, благодаря использованию социальных сетей обнаружил пропавшего студента, а в другом случае идентифицировал студента с серьезными психическими расстройствами. Традиционные методы расследования, говорит Парлон, требуют значительно большего времени и средств.

Вместе с тем, признается детектив, некоторые расследования невозможны без использования уловок и хитростей на грани закона. Так, в частности, ему приходилось создавать в Интернете фальшивые профили, которые служили приманкой для искомого объекта и его контактов.

Тактика расследования предполагает посещение чатов, подписку на ряд онлайновых публикаций. Один из приемов – завязать дружеские отношения с контактами интересующей детектива персоны. Конечно, для этого требуется время, зато можно получить «эффект снежного кома: пользователи принимают вас в свою компанию и вы по нарастающей траектории обрастаете полезными для расследования контактами» (журнал Security Management, June, 2012).

Консультант по вопросам работы в социальных сетях Джонни Ли специализируется на мониторинге интернет активности определенных людей или групп с целью обнаружения признаков потенциальной криминальной опасности. Он, в частности, пользуется поисковыми функциями Google, базирующимися на применении ключевых слов и выражений, что помогает ему выходить на определенные чаты, новостные сайты, форумы. Это избавляет от необходимости тратить время на самостоятельный поиск нужных сайтов, говорит Ли.

Прибегая к инструментарию социальных сетей, необходимо проявлять осторожность, предупреждает адвокат Бенджамин Райт. Прежде чем приступать к созданию в Интернете вымышленных образов, надо посоветоваться с юристами.

С другой стороны, подчеркивает Райт, судьи нередко отказываются принимать свидетельства, почерпнутые из Интернета, в качестве документа, ссылаясь на неопределенность источника, на невозможность перепроверки, на сомнительность методов получения информации.

По этой причине частные детективы обычно используют социальные сети для овладения первичной информацией, которая служит основой для дальнейшего, более глубокого и тщательного расследования.

Семь непростительных ошибок в организации охраны здания

Тим Джилес, в недавнем прошлом директор по безопасности корпорации IBM в США и Канаде, сегодня консультирует по вопросам планирования охраны зданий. В онлайновом журнале Chief Security Officer он отмечает наиболее распространенные ошибки:

1. Размещение охранных постов без предварительного анализа.

В большинстве компаний нет своего специалиста по охране зданий и помещений. Для охраны они приглашают соответствующую фирму, которая приходит со своими устоявшимися стандартами, размещает охрану без серьезного анализа особенностей, специфики охраняемого объекта. Специфика во многом определяется теми, кто владеет или арендует помещения. У одних арендаторов мощный поток посетителей. У других – наличие проблем с уволенными служащими. Ну, и так далее. Именно эти

особенности и должны диктовать, как надо организовать охрану.

2. Эстетика выше безопасности.

Этот недостаток уходит корнями в проектирование здания, в архитектурный дизайн, когда на первом плане эстетика, требующая, чтобы не было видно камер слежения, а красивый кустарник окаймлял здание по периметру. На этапе строительства мало кто задумывается о том, почему надо устанавливать камеры на самых видных местах, и как могут использовать пышную растительность злоумышленники.

3. Недооценка жесткого контроля при входе в здание .

В принципе, чем меньше дверей у здания, тем лучше для безопасности. Хотя, с другой стороны, в многоэтажных зданиях обязательно надо предусматривать возможность экстренной эвакуации, запасные выходы. Значение надежной охраны на входе нередко недооценивается. Джилес полагает абсолютно обязательным иметь систему СКУД с тревожной сигнализацией и электронными пропусками, а также обучать работающий в здании персонал бдительности, умению быстро и правильно реагировать, если замечен подозрительный посетитель.

4. Игнорирование менеджментом правил безопасности.

В таких случаях Джилес без обиняков заявляет руководителям компании: либо все работающие в здании в обязательном порядке носят персональные бэджики, либо можно закрывать программу безопасности.

5. Непонимание или игнорирование новейшей технологии безопасности.

Например, система записи видеонаблюдения оказывается бесполезной, если в случае происшествия персонал здания не знает, как ею пользоваться, как найти нужный кадр. Компании приглашают фирмы устанавливать дорогостоящие системы видеонаблюдения и часто совсем не заботятся о том, чтобы научиться ею управлять.

6. Отсутствие охраны отдельных важных помещений внутри здания.

Например, комнаты совещаний топ-менеджмента, куда не всякому вход разрешен. Джилес рекомендует использовать как особые электронные пропуска, выдаваемые строго ограниченному числу лиц, так и камеры внутреннего слежения.

7. Перебор с охраной.

Это другая крайность, считает Джилес, которая ведет к пустой трате средств. Каждому объекту должна соответствовать особая конфигурация охраны, отвечающая реальным потребностям и задачам. Но для выбора правильной конфигурации как раз и необходим предварительный анализ, о чем идет речь в пункте 1.

Информационно-аналитические центры как «система раннего

предупреждения» против терроризма и криминала

Информационно-аналитические центры как «система раннего предупреждения» против терроризма и криминала

окончание, начало см. журнал № 25

Весной 2003 года президент США Джордж Буш анонсировал создание Центра сбора информации о террористической угрозе. Одновременно во всех штатах стали формироваться Информационно-аналитические центры с задачей собирать информацию о возможно готовящихся террористических актах и иных тяжких преступлений. О деятельности одного из таких центров – в штате Колорадо рассказывается в пространной публикации онлайнового журнала Security Magazine, April, 2012.

Серьезное внимание уделяется соблюдению федерального и местного законодательства, особенно в той части, которая касается личных свобод и неприкосновенности частной жизни. В штатном расписании выделена должность офицера по вопросам privacy. Офицер обязан следить, чтобы информация, часто конфиденциальная, полученная о том или ином человеке, имела достаточно оснований для ее включения в официальные донесения, для установления наблюдения. Сотрудники Центра, конечно, знают либо догадываются, что многие простые американцы с подозрением относятся к деятельности Информационно-аналитических центров, считают, что их права на частную жизнь нарушаются. Масло в огонь подлили аналогичные центры в некоторых других штатах страны, установив слежку за участниками мирных протестных демонстраций и диссидентами. Такая практика официально осуждена, и в обязанности офицера по вопросам privacy входит предотвращение подобных ошибок.

Одно из несомненных достижений Информационно-аналитического центра в Колорадо – создание широкой сети горизонтального обмена информацией (помимо служебного взаимодействия с местными правоохранительными органами) с общественными организациями и крупными коммерческими компаниями. В каждой из таких организаций, входящих в сеть, выделен специальный сотрудник для поддержания постоянных информационных связей. Сюда входят, к примеру, пожарные команды, местные американские МЧС, а также жизненно важные инфраструктурные объекты и частный бизнес, обычно на уровне руководителей служб безопасности компаний и фирм. При этом сигналы, поступающие от негосударственных организаций, рассматриваются не менее серьезно, чем данные, передаваемые правоохранительными органами.

Для «гражданских» участников информационной сети проводятся специальные занятия, которые занимают три полных рабочих дня. Обучение проводится по следующим темам: ситуационный анализ, анализ и передача информации, источники опасности, домашний и международный терроризм, гражданские права и свободы.

На счету колорадского центра скопилось немало успешных историй о предотвращении преступлений и поимке бандитов. Вот одна из них. Неизвестный проник ночью в книжный магазин и заложил три самодельные бомбы, которые, впрочем, не сработали.

Наружные видеокамеры зафиксировали грузовик, на котором злоумышленник отъехал. Аналитики смогли правильно идентифицировать марку и модель автомашины. Данные были немедленно переданы в информационную сеть, и спустя считанные часы преступника задержали.

С приобретением опыта Центр проявляет все больше амбиций, претендуя на охват всего спектра криминальной сферы. В конце концов было решено помимо основной задачи – антитеррористической – сконцентрироваться на борьбе с угонами автомобилей. За последние 5 лет в штате Колорадо было угнано более 30 000 машин. При этом в 75% случаев угоны сопровождались (сочетались) с другими преступлениями – наркоторговлей, убийствами, изнасилованиями, грабежами...После того, как Центр подключился к этой проблематике, уже в течение первого года число угонов сократилось на 9%.

Когда случается непредвиденное

Прошло пять лет со дня выхода книги Н. Талеба «Черный лебедь». Ее автор представил концепцию событий, которые трудно (или невозможно) предугадать, так как они 1) происходят очень редко; 2) очень значительны (разрушительны) по последствиям; 3) нередко обусловлены человеческим фактором. (О термине «черный лебедь» см. журнал «Охрана предприятия» № 11, материал «Когда бизнесу угрожают «черные лебеди»).

Старший редактор в исследовательской и консалтинговой организации Security Executive Council М. Блейдс опубликовал в июньском выпуске журнала Security Magazine за этот год статью, посвященную концепции Талеба. Он пишет, что непредсказуемость всегда вызывает головную боль у руководителей служб безопасности. За неготовность к тем или иным поворотам, событиям начальство в лице первых лиц компании по головке не погладит.

Вместе с тем, концепцию «черного лебедя», по мнению Блейдса, сегодня можно «интегрировать» в целостную картину и политику безопасности бизнеса, использовать в процессах анализа и управления рисками. Каким образом? Ответ на этот вопрос частично дает организованная в апреле 2012 года организацией Security Executive Council конференция на тему «Будущее поколение руководителей безопасности бизнеса». Большинство выступавших на конференции категорически отвергли даже теоретическую возможность быть всегда и ко всему готовыми. Диссонансом общему настроению прозвучала презентация вице-президента компании Assets Protection for Target Б. Брекке, который ознакомил участников конференции с некоторыми практическими методами подготовки и действий в непредсказуемо экстремальных условиях. Собственно, речь идет о двух методах.

Первое. Важно готовится не к самим событиям, а к возможным последствиям. Весной 2011 года по южным штатам США пронеслись несколько торнадо, унесшие жизни более 300 человек и нанесшие ущерб в миллиарды долларов. 20 сотрудников корпорации Target в штате Алабама лишились своих жилищ, один погиб. Кроме того, из-за проблем в подаче электроэнергии нарушилась работа розничных магазинов, принадлежащих компании.

В соответствии с планом действий в экстремальных обстоятельствах были предприняты меры по обеспечению безопасности персонала компании. Одновременно запущены резервные генераторы, давшие ток в магазины. Между тем, подвозить продукты было неоткуда – оптовая база, питающаяся из федеральной электросети, была полностью обесточена. Компания, конечно, готовилась встретить разрушительные последствия торнадо, но не предусматривала вариант, при котором магазины готовы работать, но лишены снабжения товарами. Пришлось в срочном порядке искать и свозить на оптовую базу мощные генераторы, что и позволило в конце концов возобновить подвоз в магазины продуктов и воды, в которых отчаянно нуждалось местное население.

Второй урок: необходимость заранее устанавливать партнерские взаимоотношения с другими компаниями и организациями, как частными, так и государственными, в каждом отдельном районе. Как выразился один из участников конференции Рэд Джонс, «когда загорелся дом, уже нет времени договариваться с соседями, кто что должен делать». Вопросы взаимодействия надо проговаривать заблаговременно и включать достигнутые результаты в свои планы.

Профессиональный тренинг как средство снятия стресса у операторов СКУД

Бернард Скальоне, имеющий 30-летний стаж работы в сфере охранной индустрии, выступил автором статьи в журнале Seciruty Magazine (April, 2012), где он пытается доказать необходимость специальных занятий с охранниками, которым приходится вступать в конфликты с неуравновешенными посетителями. Он вспоминает два эпизода из собственного опыта работы в качестве директора по безопасности в крупном медицинском центре.

Эпизод первый. Один из сотрудников больницы забыл дома удостоверение, служившее пропуском в центр, и устроил большой скандал с женщиной-охранником. Начав с ругани, этот сотрудник завершил разборку смачным плевком в лицо женщины.

Второй эпизод связан с посетителем, которому не разрешили войти в здание, поскольку не смогли найти на рабочем месте пригласившего его служащего организации. Разбушевавшийся посетитель вытащил пистолет и стал угрожать всем, кто находился в лобби. Правда, затем он ушел, не приведя в исполнение свои угрозы, а позднее был опознан и арестован. Но охранник, вступивший с ним в конфликт, и подвергшийся большому риску, обратился к своему начальству с просьбой более не ставить его на контроль у входных дверей.

Как пишет Скальоне, он не раз убеждался на протяжении всей своей карьеры, что место на контроле доступа – самое тяжелое с точки зрения стресса, так как приходится сталкиваться с оскорблениями, агрессией, риском потерять здоровье, а то и жизнь. Он утверждает, что, принимая во внимание это обстоятельство, необходимо проводить с охранниками специальные занятия, помогающие снимать стресс. Тренинги должны помогать овладевать особой методикой контроля и проверки людей

на пункте СКУД. Учебные пособия, как напечатанные, так и компьютерные курсы, для данного дела мало подходят. Занятия должны проходить в классе, с использованием интерактивных методов.

Особенно важно проигрывать «вживую» возможные сценарии, связанные с потенциальными конфликтами. Групповое обсуждение сценариев помогает слушателям глубоко вникать в реальные ситуации, могущие произойти в их работе, разобраться в них, чтобы в дальнейшем правильно, с наименьшим стрессом, справляться с самыми сложными ситуациями на своем рабочем месте.

Скальоне подчеркивает, что тренинги, за которые он ратует – не просто изложение инструкций, но, прежде всего, овладение практическими навыками работы охранника. Впрочем, в компании должны быть все необходимые документы, формулирующие политику и процедуры в области охраны и безопасности.

Автор статьи считает, что надо также проводить разъяснительную работу с персоналом компании, с арендаторами, если речь идет о здании, где размещены разные фирмы и организации. Конечно, было бы неплохо их тоже приглашать на занятия. По меньшей мере, расклеить в лобби, при входе в здание, напоминания о необходимости соблюдения правил прохода через систему контроля и идентификации личности.

Как добиться приемлемого бюджета для службы безопасности в компании

окончание, начало см. журнал № 25

Журналист издания Chief Security Officer Мэри Брандел взяла интервью у ряда американских специалистов-практиков в сфере безопасности бизнеса на тему финансирования этой функции в компаниях США.

Необходимо прямо указывать на персональную ответственность руководящих менеджеров за реализацию в компании проектов по безопасности. Дж. Кларк, руководитель СБ в компании Websense, составил диаграмму выполнения плана конкретных мер по безопасности в отделах и управлениях компании, где четко указано, в каких подразделениях план выполняется по графику, а в каких тормозится. Представленная генеральному директору диаграмма возымела действие. Отстающие подтянулись.

Еще до официального представления начальству нового проекта под финансирование неплохо бы его предварительно неформально «обкатать» с участием топ-менеджеров. Говорит Р. Гюнтнер, директор по безопасности корпорации Mastercard Worldwide: «Прежде чем выставить «на продажу» новую инициативу, я внимательно взвешиваю три вопроса: стоит ли этот проект финансовых затрат, почему он необходим для бизнеса компании, отвечает ли проект стратегии бизнеса. Все эти вопросы я неформально прорабатываю с руководителями разных управлений компании. Поэтому для них не является сюрпризом, когда проект официально вносится на рассмотрение. Более того, в их лице я могу рассчитывать на поддержку».

Надо учитывать профессиональный менталитет руководителей. Скажем, в поле зрения заведующего отделом кадров - имеющиеся проблемы в отношениях между сотрудниками компании, в то время как заведующего хозяйственным отделом, возможно, беспокоит, что часть имущества компании содержится не там, где полагается. Знать эти особенности, находить особый подход к каждому менеджеру – значит, создавать благоприятные условия для продвижения своего проекта.

Не менее важно учитывать меняющееся настроение тех, от кого зависит окончательное решение. Если начальник чем-то раздражен, то лучше не торопиться со своими идеями. Гюнтнер: «Если вы сумели выбрать верный момент, чтобы предложить проект, тогда вперед, вы повышаете свои шансы на успех».

Лучше показывать, чем рассказывать. Представляя проект, надо иметь в виду, что визуальный ряд быстрее и убедительнее слов донесет до аудитории ваши мысли. Дж. Кларк в ходе одной презентации изобразил на экране наплывающие на город грозовые тучи. И когда генеральный директор спросил его о гарантиях безопасности, докладчик ответил: «Посмотрите на приближающуюся грозу. Мы не можем гарантированно ее избежать, но можем подготовиться и минимизировать ущерб». Кларк верит в эффективность красноречия и даже взял одним из своих помощников в СБ человека, отличающегося особым искусством в этом деле. Блестящий коммуникатор, на совещаниях и в неформальных встречах он умело убеждает менеджеров компании в их заинтересованности поддержать проекты по безопасности.

Как правильно выбирать фирму для физической охраны предприятия

Один из руководителей компании Alliedbarton Security Services Рэндал Дорн предлагает методологию выбора фирмы в сфере индустрии безопасности для заключения контракта по физической охране.

Сформировать команду внутри компании, которая будет заниматься контрактным процессом. Обычно в нее включают руководителей (представителей) собственной службы безопасности, юридического, финансового и кадрового отделов, а также управления по закупкам.

Проанализировать текущее состояние охраны предприятия, определить приоритеты, слабые места. Какие есть возможности для исправления и улучшения? В чем заключаются цели, задачи программы по безопасности, насколько они отвечают сегодняшним реалиям?

Сформулировать задачи по улучшению физической охраны. Неплохо сравнить свои задачи с теми, которые ставят и решают ваши основные по бизнесу конкуренты в деле обеспечения своей безопасности. Важно узнать, какие зарплаты и бонусы получают охранники у конкурентов, какова их квалификация, натренированность…

Составить список из нескольких охранных фирм, которые имеются в регионах вашего бизнеса. Пригласите их представителей посетить объекты, которые предстоит охранять. Попутно проверьте, все ли нормально у них с лицензированием, сколько лет они на рынке безопасности, насколько стабилен персонал охранников и менеджмент,

имеется ли опыт оказания охранных услуг компаниям, которые занимаются схожим с вашим бизнесом…

Предложить подготовить и представить проект партнерства с описанием деятельности компании, а также целей и ожиданий от сотрудничества. Проект должен включать количество рабочих часов, обязанности, выбор формы одежды, вид страховок, финансовые условия и т.д.

Изучив поступившие предложения, сократите список до двух или трех фирм-претендентов, вступите с ними в прямые и конкретные переговоры. Вы должны удостовериться, что будущий партнер ясно понимает специфику вашей компании и готов полностью ее учитывать, предоставляя свои услуги.

10 рекомендаций, как добиться эффективности тренингов по безопасности

Президент компании Wombat Security Technologies Джо Феррара считает серьезным просчетом, когда обучение вопросам охраны предприятия зачастую доверяется профессионалам в сфере безопасности, не имеющим навыков и необходимых знаний для преподавания. Именно им в первую очередь он адресует свои рекомендации, изложенные на сайте csoonline.com, May 03, 2012. Он отмечает при этом, что ничего нового не изобрел, а просто использует опыт проведения учебных курсов по безопасности бизнеса, накопленный несколькими поколениями с середины прошлого века.

1. Дробите учебный материал. Слушатели лучше понимают и запоминают небольшие по объему информации.

2. Повторяйте и закрепляйте пройденный материал. Учебный процесс должен носить постоянный, непрерывный характер.

3. Контекст. Люди обычно лучше усваивают контекст, нежели контент. Поэтому важно вести занятия с учетом максимального приближения к действительности, связанной со спецификой их нынешней или предстоящей работы.

4. Варьируйте формы изложения концепции. Если одна и та же мысль доносится до слушателей неоднократно и всякий раз в разных контекстах, то она лучше понимается и усваивается.

5. Используйте интерактивные методы. Они весьма результативны, например, когда идет практическое обучение вопросам идентификации фишинговых схем или создания надежных паролей.

6. Проводите различные игры, максимально приближенные к реальности. Ошибки, сделанные в ходе учебных игр, едва ли повторятся в практической жизни.

7. Рассказывайте истории. Старайтесь избегать сухого перечисления фактов и данных, предлагайте учебный материал в виде интересных рассказов.

8. Понуждайте слушателей думать. Важно, чтобы слушатели сами могли самостоятельно переварить учебный материал, осознать его значение, сделать собственные умозаключения.

9. Учитывайте индивидуальные особенности слушателей, как ни банально это звучит.

10. Давайте как концептуальные, так и процедурные знания. Первые рисуют общую проблему, вторые – показывают пути и методы ее решения. Именно сочетание этих двух видов знаний дает наилучший результат.

Новый стандарт ASIS International для физической охраны

Международная организация охранной индустрии ASIS International установила новый стандарт для физической охраны, выпустив документ «Security Management Standard: Physical Assets Protection».

Подготовленный Техническим комитетом ASIS, который состоит из 80 членов, представляющих 17 стран, документ определяет основные подходы и требования к физической охране персонала, имущества, информации компаний и организаций. Речь идет об охране как измеряемых объектов (персонал, оборудование и т.п.), так и не поддающихся физическому измерению активов (бренд, репутация, информация). Документ предлагает рамочные стандарты установки, управления, мониторинга, содержания, модернизации систем физической охраны.

Говорит Аллисон Уайдл, член Технического комитета из London Business School: «Любая организация сталкивается в своей деятельности с рисками. Перед ней всегда стоит дилемма: как определить, какие риски можно себе позволить, а какие надо минимизировать с оптимальными затратами, чтобы достичь стоящих перед организацией стратегических и тактических целей. Принятый ASIS новый стандарт позволяет найти оптимальный баланс между этими двумя вызовами» (securitymanagement.com, May 29, 2012).

Physical Assets Protection Standard объединяет в единую систему менеджмента функцию безопасности организации и ее различные смежные направления – управление рисками, охрана здоровья, финансы, контроль качества товаров/услуг, соблюдение законов и принятых в индустрии правил и норм.

Эта система управления должна:

- обеспечивать неуклонное следование принципам и политике Physical Assets Protection Standard;

- помочь вырабатывать и реализовывать всеобъемлющую программу управления рисками, которая призвана обнаруживать, анализировать и оценивать риски,

угрожающие материальным и нематериальным ценностям;

- с учетом особенностей подлежащих охране ценностей содействовать созданию и работе системы физической охраны;

- интегрировать с этой целью человеческие ресурсы, процедуры, технологии, оборудование;

- постоянно отслеживать, оценивать и контролировать управление системой физической охраны.

Данный документ представляет собой инструкцию для руководителей служб безопасности, подчеркивает вице-президент компании Securitas Security Services USA Бернард Гринауолт: «стандарт призван помочь практикам определить уровень приемлемых рисков и размеры инвестиций в управление ими».

Документ можно скачать на сайте www.asisonline.org

Рецензия

Broker, Trader, Law¬yer, Spy: The Secret World of Corporate Espionage
By Eamon Javers. HarperCollins, 320 pages

Книга посвящена вопросам промышленного (корпоративного) шпионажа. Она интересна широкому кругу читателей, и, прежде всего, тем, отмечает рецензент книги Джеймс Данн, что рассказывает о «специалистах» этой сферы. Большинство из них получили навыки шпионажа на государственной службе, а затем пришли их применять в частный сектор экономики.

Одна из таких легендарных фигур – Хал Липсет, послуживший немало лет в армии, а затем нашедший применение своим шпионским способностям в бизнесе. Он получил широкую известность несколько десятилетий назад, когда, вынужденный предстать перед комиссией Конгресса США, он продемонстрировал стакан мартини с передатчиком, встроенным в маслину, и антенну виде зубочистки.

У автора книги, пишет в своей рецензии Данн, по крайней мере, три задачи: поднять проблему конфликта интересов, морально-этических аспектов шпионажа, продемонстрировать наращивание технологической базы этой деятельности, просто развлечь читателей увлекательными сюжетами.

Рассказывая о самых разных историях промышленного шпионажа, автор книги подводит читателей к мысли о том, что морально-этических издержек можно было бы избежать, внеся определенные поправки в действующее законодательство с целью придания этому промыслу ограниченного правового характера, фактически - частичной легализации. Рецензент с иронией прокомментировал данный посыл, отметив, что едва ли найдется кто-либо, кто решится променять все, что дает ему эта работа – деньги, влияние, азарт, интеллектуальное удовлетворение, престиж – на официальную регистрацию своих занятий.

Графология безопасности

Графология безопасности
Графологическая экспертиза почерка и ее использование в службе безопасности компании (сокращенный вариант исследования)

Автор: Шарлот Всеволод – Клуб Сотрудников Информационных Служб (Клуб СИС) http://club-sis.net.

Сотрудник компании – один из основных источников ее успеха и он же – один из основных причин ее неудач. Предотвратить прием на работу в компанию неподходящих сотрудников – одна из важнейших задач кадрового подбора. Кадровые службы обычно отсекают некомпетентных, неопытных, неэффективных, несоответствующих должности или корпоративной культуре соискателей.

Со своей стороны, выявить недобросовестных и ненадежных кандидатов помогает Служба безопасности (СБ) компании. Для решения этой задачи СБ использует различные методы, такие как проверка по базам данных (БД), по учетам, по предыдущим местам работы, по открытым источниками, а также собеседование, установка по месту жительства и наружное наблюдение, проверка на полиграфе.

Отечественные СБ практически никогда не используют психологическое тестирование. В случае отсутствия или слабости кадровой службы психологический портрет кандидата вообще не составляется, либо составляется на основании мнений представителей других организаций и субъективных представлений интервьюера. СБ, как и служба по подбору персонала, нуждается в инструменте выявления психологических рисков, связанных с кандидатами - доступном, но эффективном методе, позволяющем оценить не только комплексный психологический портрет личности, но и получить информацию о потенциальной благонадежности кандидата. Методом, отвечающим этим запросам, может стать графологический анализ личности (анализ почерка кандидата).

Графология представляет собой психодиагностическую методику, основанную на научном подходе, предполагающую исследование психомоторной подоплеки графических явлений с целью изучения психологических характеристик пишущего.

На сегодняшний день во многих странах анализ почерка является одним из средств психодиагностики личности. Графологическое тестирование применяется в странах Европы (Франция, Испания, Венгрия и др.). По мнению экспертов, во Франции данный метод оценки на регулярной основе практикуют 85% компаний, а в Израиле это вообще наиболее часто употребляемая процедура по оценке личности при приеме на работу. Меньше графология распространена в США и Канаде.

Графологическая экспертиза почерка при проверке персонала и контрагентов.

Использование графологической экспертизы при отборе кандидатов на вакантные должности позволяет путем создания целостного психологического портрета кандидата выявить опасные категории сотрудников:

- недобросовестных (склонных к обману, мошенничеству и манипулированию другими людьми, индивидов, с ослабленным моральным ограничителем);

- ненадежных (халатных, пускающих «пыль в глаза», склонных к саботажу, слабо предсказуемых, зависимых, патологически жадных индивидов);

- неэффективных (ленивых, с низким уровнем развития, которого не хватает для выполнения рабочего функционала, как их противоположность – чрезмерно амбициозных, излишне независимых).

- деструктивных (конфликтных, т.е. создающих конфликтные ситуации с коллегами и/или руководством, интриганов, карьеристов в плохом смысле, не вписывающихся в корпоративную культуру, эгоистов, авантюристов)

Перед СБ компании также стоит задача не допустить заключения договора с мошеннической, ненадежной и неэффективной компанией. Для решения этой задачи используются те же методы, что и для проверки соискателей, персонала. Необходим комплексный анализ всей доступной информации, и важнейшей составляющей для анализа является психологический портрет потенциального контрагента. В коротком собеседовании сложно создать целостное представление о личности человека, особенно с учетом необходимости выявить его надежность.

Существует относительно немного возможностей непосредственного получения информации о психологических качествах и истинных мотивах деятельности руководителя потенциального контрагента. Среди них: невербальное поведение, изменение температуры кожных покровов лица, поведение в момент собеседования, особенности ответов на поставленные вопросы и т.п. Однако, несмотря на кажущуюся простоту, подобную информацию сложно «считывать», еще сложнее ее использовать для анализа. Поэтому нельзя пренебрегать дополнительным источником информации - почерком, который может быть очень ценным для СБ. Экспертиза графолога позволяет дополнить картину, созданную объективными данными проверки и субъективным впечатлением от собеседования, проясняет многие недостающие звенья, а иногда серьезно корректирует первоначальные выводы.

Графологическая экспертиза почерка может быть использована не только в подборе персонала и проверке контрагентов, но и при назначении сотрудников на руководящие должности, с целью изучения потенциальной лояльности сотрудников, в служебных расследованиях и при изучении конкурентов.

В служебных расследованиях графологическая экспертиза может быть использована как совместно с проверкой на полиграфе, так и самостоятельно. Основная задача в данном случае - выявление психологических качеств, способствующих совершению служебного проступка, конструирование психологической модели произошедшего, выявление причин, по которым тот или иной человек мог совершить неблаговидный поступок.

Позитивный эффект дает совмещение графологической экспертизы с проверкой на полиграфе. Полиграфолог, имея на руках результаты графологического анализа, может более тонко и индивидуально задавать вопросы, «бить» по слабым точкам опрашиваемого.

Методы, применяемые для проверки персонала и контрагентов, их достоинства и недостатки.

	Достоинства	Недостатки
*Проверка по базам данных**	Доступность и оперативность	Устаревшая и неполная информация
*Проверка по учетам МВД***	Достоверность, актуальность информации	Неполнота
Проверка по открытым источникам	Доступность, оперативность, небольшие затраты	Неточная, недостоверная, не актуальная информация
Изучение финансовой информации	Объективная информация, позволяющая сделать вывод о финансовой устойчивости компании	Запаздывание информации Росстата. Не учитывается «черная» бухгалтерия
Проверка по предыдущим местам работы	Информация о надежности и добросовестности, опыте решения различных задач	Субъективность и неполнота отзывов
*Установка по месту жительства и наружное наблюдение****	Информация об образе жизни, привычках, пристрастиях, наклонностях, связях и т.п.	Затратность метода, сложность
Проведение «оперативного» эксперимента	Достоверность информации	Сложность метода
Полиграф	Получение информации по отдельным аспектам надежности кандидата	Затратность, сложность процедуры. Возможность подготовиться к проверке.
Собеседование со специалистом	Создание целостной картины личности кандидата	Субъективность выводов о надежности кандидата
*Традиционные психодиагностические методики*****	Получение информации о различных аспектах личности кандидата. Возможность автоматизировать процедуру. Возможность проведения дистанционного тестирования	Не дают ответ о надежности кандидата *(за исключением тестов на благонадежность)*
Графологическая экспертиза	Создание целостной картины личности кандидата. Получение информации о надежности личности в целом. Возможность проведения дистанционной экспертизы	Оценочный характер информация о надежности.

* - *адресно-справочные, телефонные, регистрационные, базы банков и государственных организаций*

** - *использование данного метода службами безопасности коммерческих структур находится вне правового поля*

*** - *метод, редко использующийся СБ, но его использование коммерческими структурами нельзя назвать правомерным*

**** - *СБ редко применяют этот метод при проверке персонала других подразделений*

Выводы графологической экспертизы почерка кандидата или руководителя контрагента в сочетании с информацией из других источников позволяют:

- построить модель потенциальной лояльности/нелояльности, надежности/ненадежности кандидата или работающего сотрудника;

- сформировать психологический портрет сотрудника, деятельность (или действия) которого попали под служебное расследование;

- создать психологический портрет руководителя возможного контрагента с целью выявления его потенциальной ненадежности, понять, в чем она будет выражаться;

- определить наиболее оптимальные условия взаимодействия с данным руководителем контрагента (например, для человека с рациональным, логическим подходом необходимо четко проработать процедуру взаимодействия, предоставить информацию в виде графиков, таблиц, показателей в процентах, а для человека эмоционального плана важен индивидуальный подход, неформальные отношения);

- построить психологический портрет руководителя конкурента (спрогнозировать его методы работы - предпочтение консервативной стратегии и традиционных методов конкуренции, либо внедрение чего-то нового, нестандартного, недобросовестного).

Таким образом, графологическая экспертиза может нести ценнейшую информацию о человеке, позволяющую понять его глубинные мотивы и важнейшие психологические и деловые качества. Однако при решении вопроса определения благонадежности кандидата или надежности контрагента необходимо понимать, что в силу сложности человеческой натуры и влияния целого ряда непредвиденных обстоятельств на него, ни одна психодиагностическая или проверочная методика не дает 100% уверенности. В каждом конкретном случае слишком много зависит от внешних условий и внутренних процессов и состояний. Поэтому для повышения точности прогноза необходимо использовать в комплексе несколько проверочных и психодиагностических методик.

Автор выражает глубокую благодарность эксперту-графологу, кандидату психологических наук, руководителю представительства в Москве Института Графоанализа Инессы Гольдберг Ларисе Евгеньевне Дрыгваль за неоценимую помощь в подготовке данной статьи.

В статье использовались материалы сайта Института Графоанализа Инессы Гольдберг ***http://inessa-goldberg.ru/*** *и сайта Графология МСК ру http://grafologia-msk.ru а также книга Гольдберг И.И. Графология шаг за шагом (в 8-и томах). – Екатеринбург: У-Фактория; М.: АСТ Москва, 2008.*