Охрана предприятия

№4, 2010 (№14)

Оглавление

Охрана небольших помещений

Рекомендации специалиста

Безопасность в командировках: что брать с собой на случай стихийных бедствий?

Охрана предприятия за рубежом

Индия: полно охранников, но кто их обучает?

Пожары в Австралии: уроки 2009 года

2009 год выдался в Австралии самым жарким и сухим за всю историю наблюдений. Пожары охватили огромные территории, унесли почти 200 человеческих жизней, включая детей и целые семьи. Впервые в истории огонь подступил непосредственно к многомиллионному, второму по численности городу Мельбурну. В окрестностях мегаполиса огнем уничтожено более 750 домов. 5 000 жителей лишились своих жилищ.

Власти вынуждены признать, что не обладают ресурсами, гарантирующими защиту каждого дома и призывают проживающее в сельской местности население действовать самостоятельно, по обстановке, учиться распознавать поведение огня, но, в первую очередь, вести себя осмотрительно, ведь более половины всех пожаров (а их число в Австралии ежегодно достигает цифры 60 000) вызваны человеческим фактором.

Надо отметить, что последнее десятилетие на этом континенте отмечено небывалым повышением температуры – почти на градус по Цельсию в сравнении с предшествующими годами. Засуха охватила значительную часть территории, где месяцами не выпадало ни капли дождя, а температура не опускалась ниже 40 градусов.

Большинство людей, гибнущих в пожарах, ждут до последней минуты, затем пытаются спастись бегством, но не успевают. Многих обнаружили сгоревшими прямо в своих автомобилях, придавленных падающими деревьями в огненном кольце. Повезло некоторым из тех, кто пережидал в подвалах или вырытых наспех земляных убежищах. При сильном ветре пожары распространяются с такой быстротой, что люди просто не успевают ни эвакуироваться, ни защититься. Иногда скорость достигает 40 км/час. При этом система связи дает сбои: мобильные операторы не справляются с перегрузками, ведь количество звонков возрастает в десятки раз!

Власти страны признают, что во многих случаях «спасение утопающих – дело рук самих утопающих», и проводят через средства массовой информации разъяснительную кампанию о мерах, которые сельские жители должны предпринимать для своего спасения. Вот некоторые рекомендации, опубликованные на страницах национальной прессы:

1. Не пытаться самостоятельно противостоять огню, если лесной пожар подступает к жилищу, а немедленно эвакуироваться. Проживая в пожароопасном районе, в период летней (для Австралии правильнее сказать - «зимней») засухи, необходимо заранее составить план эвакуации, заблаговременно подготовиться (транспортные средства, маршруты, собрать документы и вещи первой необходимости), а также при возможности вывезти на это время детей, больных и стариков в более безопасные места.

2. Научиться распознавать поведение огня (направление, скорость и т.п.). Изучить местную топографию: наличие и расположение прудов, озер, болот, холмов. Важно, например, знать, что огонь быстрее распространяется по склону вверх. Чем круче склон холма, тем быстрее распространяется огонь.

3. В пожароопасных зонах желательно не насаждать растения вблизи строений.

4. Избегать паники. Попытки спастись в последнюю минуту часто оборачиваются трагедией.

5. В периоды повышенного риска организовать (совместно с соседями или в семье) круглосуточное дежурство по наблюдению за обстановкой.

6. Рыть пожарные пруды. Позаботиться о подъездных путях для пожарных машин. Оказывать помощь и поддержку командам профессиональных пожарников.

7. При строительстве домов использовать наиболее пожароустойчивые материалы. Особенно это касается кровли.

8. Установить в жилых и подсобных помещениях детекторы дыма, противопожарную сигнализацию. Регулярно проверять их исправность, менять батарейки (подзаряжать аккумуляторы). Везде, в первую очередь, в гараже и на кухне, поставить огнетушители.

(по материалам австралийских онлайновых изданий)

Лесные пожары – благо или беда?

Лесные пожары случаются в Северной Америке практически ежегодно. Только в Канаде они охватывают в среднем порядка 25 000 квадратных километров. В битве с огнем участвуют сотни специально натренированных пожарников. Привлекаются и студенты колледжей, университетов, нуждающиеся в заработке во время летних каникул. Команды огнеборцев забрасываются вертолетами и парашютными десантами с самолетов в «горячие точки».

Наблюдательные вышки, установленные еще сто лет назад, исправно продолжают службу. За последнее время к ним добавились более совершенные инструменты мониторинга – компьютерные системы космической связи, не только фиксирующие очаги возгорания, но и определяющие уровень влажности в этих местах, скорость горения и передвижения огня, направление ветров и т.п.

Эксперты уверены, что большинство возгораний вызвано человеческим фактором: 58% пожаров в Канаде, как низовых, так и верховых, возникают по небрежности людей. Остальные, как правило, обусловлены ударами молний. С 30-х годов прошлого столетия в школах проводятся специальные занятия по предотвращению и недопущению лесных пожаров. На автострадах размещены предупреждающие и напоминающие о пожарной безопасности щиты.

И в Канаде, и в США развернулась борьба между лесопромышленными компаниями и экологическим организациями, которые в этой части земного шара как нигде влиятельны и мощны. Лесопромышленники, осуществляющие коммерческие вырубки леса, выступают за минимизацию причиняемого пожарами ущерба для их бизнеса. Они исходят из тезиса, что чем меньше лесов, тем меньше пожаров. Такая позиция понятна. Их бизнес – это быстрые деньги. Они лоббируют свои интересы в правительстве, пропагандируют позицию в средствах массовой информации.

Однако, в последние годы все большее влияние в обществе завоевывает противоположная точка зрения. Она сводится к тому, что вызванные природными факторами лесные пожары идут во благо, а не во вред.

Так, в статье на сайте democraticunderground.com (October 30, 2003) под названием «В охвативших Калифорнию пожарах виноваты лесопромышленные компании» утверждается, что природные пожары (wildfires) необходимы для поддержания здоровой экосистемы. Огонь уничтожает гниющие остатки умерших деревьев, скопления листвы и иголок, расчищает место для нового поколения растений. Некоторые виды сосен (lodgepole pines) могут размножаться исключительно в условиях высокой температуры, которая раскрывает закупоренные смолой шишки и дает выход семенам. По данным науки, природные пожары происходят в Америке регулярно многие тысячи лет. Опустошенные огнем районы зарастают свежим лесом, более здоровым и мощным, чем их сгоревший «предок».

Лесопромышленные компании несут большую долю вины за возникновение пожаров, угрожающих жизни и имуществу людей. Они обычно вырубают и утилизируют крепкие, здоровые деревья, оставляя на месте больные растения, опилки, кустарники, хвою, листья и прочий легко возгораемый мусор. Тактика «прореживания лесов», восхваляемая лесопромышленниками, также, по мнению многих специалистов, не выдерживает критики. То, что они называют «прореживанием», на практике сводится

к удалению наиболее крупных, сильных и здоровых деревьев. Чем лес старше и гуще, тем он более пожароустойчив. И, напротив, прореженный лес пропускает больше солнечного тепла и ветра, что обуславливает уменьшение влажности, а, значит, усиление риска возгораний.

Экологи и многие эксперты выступают против искусственных насаждений – своего рода лесных плантаций, разводимых лесниками и лесопромышленниками. Монокультура, к тому же одного возраста, считают они, ведет к деградации экосистемы, распространению болезней и эрозии почвы.

Частные охранные услуги по версии Конфедерации европейских служб безопасности

Частные охранные услуги по версии Конфедерации европейских служб безопасности

Комментарий А.Куражова

Перевод В. Светозарова

Конфедерация европейских служб безопасности (Confederation of European Security Services - CoESS) в мае текущего года опубликовала документ, содержащий перечень видов деятельности, осуществляемых частными охранными структурами и другими предприятиями, работающими в сфере безопасности. Данный документ представляется интересным для ознакомления с негосударственными структурами безопасности в странах Европы.

CoESS была основана в 1989 году по совместной инициативе нескольких национальных ассоциаций частных охранных предприятий в странах – членах ЕС. С самого начала она носит статус европейской организации, объединяющей национальные ассоциации негосударственного сектора безопасности. Целью CoESS провозглашается «обеспечение в Европе защиты интересов организаций и национальных компаний, предоставляющих услуги безопасности во всех их формах и представительство совместных интересов частных охранных сообществ – членов CoESS посредством участия в многогранной работе, направленной на гармонизацию национального законодательства в сфере частного охранного бизнеса». CoESS осуществляет профессиональные, экономические, коммерческие, юридические, социальные и другие исследования, касающихся деятельности своих членов; собирает и распространяет среди них информацию; представляет и обеспечивает защиту своих членов в европейских и международных организациях; формирует и отстаивает совместные позиции в отношении к Европейскому сообществу в целом и к любым другим национальным или международным организациям.

Название документа, о котором ниже идет речь, – Definition of Private Security Services - можно перевести как «Определение частных охранных услуг». Вот его перевод:

Definition of Private Security Services

Основное внимание в этой таблице фокусируется на услугах, оказываемых охранными предприятиями. Не берутся в расчет: пенитенциарная система, пожарная охрана, медицинская скорая помощь, а также производство, установка и эксплуатация охранного оборудования. Однако, в общий портфель охранных услуг, оказываемых клиенту, нередко включаются: противопожарная безопасность (соблюдение противопожарной безопасности и меры по тушению возникших очагов огня) и медицинская помощь, электронные системы охраны (установка тревожной сигнализации), противопожарная сигнализация. Приведенные ниже охранные услуги/продукты не исчерпывают все содержание охранной деятельности, но демонстрируют взаимосвязь между ними.

<table>
<tr><td colspan="8">Виды частных охранных услуг</td><td>Охрана общественного порядка[1]</td><td>Частные военно-охранные услуги[2]</td></tr>
<tr><td>Консалтинг по безопасности
- Управление рисками
- Деловая разведка (бизнес-разведка, конкурентная разведка – ред.)
- Планирование охранной деятельности
- Осуществление (проектов по безопасности)</td><td>Частные расследования[3]
(необходимо отличать от частных расследований преступлений)</td><td>Управление толпой (или контроль над толпой)[4]
- Безопасность на массовых мероприятиях
- Контроль за входом-выходом</td><td>Охрана
- Стационарная охрана
- Мобильная охрана
- Проверки
- Непосредственная защита (в т.ч. персональная охрана?)
- Реагирование на сигналы тревоги
- Контроль за доступом
- Контроль ключей к запорам и замкам</td><td>Системы электронной охраны[5]
- Тревожные кнопки
- Контроль за доступом
- Блоки доступа
- Видеонаблюдение</td><td rowspan="3">Физические/механические средства охраны[6]
- Замки
- Барьеры[9]
- Печати, пломбы
- Освещение
- Сейфы
- Спецпомещения (подвалы и т.п.)</td><td rowspan="3">Охраняемые перевозки ценностей[7]
- Инкассация
- Работа с наличными средствами
- Банкоматы и терминалы по оплате за услуги</td><td rowspan="3">Информационная безопасность[8]
- Внутренние коммуникации и сети
- Безопасность хранимых документов
- Хранение персональных данных</td><td rowspan="3">- Наблюдения за порядком в местах скопления людей
- Частные криминальные расследования
- Контроль за автостоянками
- Контроль за транспортом</td><td rowspan="3">- Вооруженная охрана
- Армейские функции</td></tr>
<tr><td colspan="3">Обучение и тренинг охранной деятельности[10]</td><td colspan="2" rowspan="2">Мониторинг и контроль за сигнализацией[12]
- Система подачи сигнала (распределения)
- Электронное наблюдение и регулирование
- Операционная система дистанционного контроля
- Контроль за обеспечением безопасности
- дистанционный контроль охраняемых перевозок</td></tr>
<tr><td colspan="3">Охрана национальных стратегических инфраструктур[11]</td></tr>
</table>

Примечания

1. Включены действия, к которым нередко применяется термин "частная полиция», - т.е. в традиционном, классическом понимании полицейские функции, выполняемые частными охранными предприятиями в случае обращения к ним государственных правоохранительных организаций. Это характерно для крупных торговых центров, спортивных мероприятий, концертов под открытым небом и т.д.

2. Речь идет, прежде всего, о вспомогательных функциях персонала, имеющего военные навыки, для государственных организаций, неправительственных организаций, частных компаний в районах вооруженных конфликтов, повышенной опасности, для спасения людей. Тех, кто выполняет такие функции, обычно именуют «частно-военные компании» Деятельность наемников исключена.

3. Этот термин в некоторых случаях, когда речь идет о расширении зоны действий и проблемах расследования, заменяется определением «частные разведуслуги»

4. Также называется иногда – «борьба с массовыми беспорядками».

5. Планирование, установка и эксплуатация систем B2B (Business-to-Business), B2C (Business-to-Consumer).

6. Обычно рассматриваются как часть проекта, часто применяются в сочетании с другими охранными услугами

7. В расширительном смысле – перевозка всего, что представляет ценность: кровь для госпиталей, произведения искусства, документов и т.п. Но чаще всего, это охрана перевозимых денег, откуда и появление данного термина «инкассация».

8. Включает системы информационной и коммуникационной безопасности; охрану документов – их подготовку, содержание и хранение, транспортировку; идентификацию личности, в том числе – обеспечение и охрану средств ID

9. Т.е. заборы, ворота, двери, окна, блокеры, турникеты и т.п.

10. Вспомогательные, часто лицензируемые услуги, нацеленные на повышение квалификации охранного персонала до уровня установленных требований. Эти услуги предоставляются частными охранными предприятиями, органами власти (полицией), или независимыми институтами.

11. Новая, важная, увеличивающаяся в объеме специфическая услуга, которая включает также антитеррористический элемент. Она не имеет отдельной категории в данной схеме и, возможно, должна быть отнесена к категории «частные военно-охранные услуги».

12. Сегодня мониторинг позиционируется в серой зоне между категориями «охрана» и «системы электронной безопасности».

Комментарий

Как видно, спектр того, чем на Западе занимаются негосударственные (частные) структуры безопасности, чрезвычайно широк и имеет тенденцию к дальнейшему расширению. Следует иметь в виду, что перечисленные виды деятельности не являются исключительной прерогативой негосударственных структур. Подобными вещами заняты и некоторые государственные службы: армия, полиция, ведомственные образования. В данном перечне представлено то, к чему «допущены» негосударственные структуры безопасности наравне с другими участниками этого рынка.

Данный документ коренным образом отличается от перечня видов охранных услуг, содержащихся в ст.3 Федеральный закон Российской Федерации от 22 декабря 2008 г. N 272-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием государственного контроля в сфере частной охранной и детективной деятельности".

Стоит обратить внимание на то, как прочно в Европе функции безопасности укоренились в бизнесе. Сколько разнообразных задач относится к сфере безопасности и как участвуют в их решении негосударственные структуры!

Эти функции «бытуют» и в нашей жизни. Развивающаяся инфраструктура деловых отношений делает их востребованными практически повсеместно. Вот только решаются они у нас по-другому. Часть из них, образующая специально лицензированные виды деятельности, жестко регламентируется законом, а часть – реализуется вне этих жестких рамок. В настоящее время в связи с несовершенством и явной тенденциозностью ФЗ № 272, направленного на уменьшение роли частного сектора на рынке безопасности, вместо «контролируемого развития» происходит свертывание этого рынка. При возрастающей (особенно - в условиях кризиса) потребности в охранных и других услугах безопасности, количество частных охранных предприятий и сопутствующих их деятельности фирм сокращается, объем легальных, с позиции нового закона услуг - также. Государственные структуры в лице МВД, Минобороны не имеют возможности занять образующиеся ниши, в том числе и в силу их собственного сокращения. Ведомственная охрана развивается крайне медленно и не имеет той гибкости, которая присуща частной.

Европейский документ ценен тем, что он объективен в показе всего того, что мы именуем «негосударственным сектором безопасности». Все, что в нем перечислено, не исчезает в силу нововведений того или иного закона – оно есть. Только осуществляется все это уже вне сферы специального законодательного регулирования. Там, где раньше стоял частный охранник, теперь стоит контролер (офис-менеджер, администратор, консьерж, вахтер, сторож). Охрана ценностей в процессе их транспортировки уступает место экспедиционному контролю. Консультирование по вопросам правомерной защиты от противоправных посягательств заменяется услугами адвокатского бюро, работой подразделений риск-менеджмента, внутреннего контроля, информационно-аналитическими услугами и т.п. Место систем видеонаблюдения занимают системы промышленного (офисного) телевидения и т.д. Ранее бывший довольно прозрачным и внятным рынок услуг безопасности в нашей стране все больше «затеняется», сужается в своей «официальной» части, но не перестает существовать, совершенствоваться и даже развиваться в зоне, свободной от навязанного государством чрезвычайно жесткого и неэффективного контроля. Не случаен в этой связи ажиотажный спрос на пакет учредительных документов предприятия с условным наименованием САВОК – «Служба администраторов, вахтёров, операторов, консьержей». Объективно существующие и необходимые бизнесу функции остались. А вот каким образом их осуществлять, что «оставить» в зоне контроля регуляторов, а что вывести из этой зоны, можно понять, проанализировав представленный выше документ.

Новые задачи для служб безопасности предприятия

В последнее время за рубежом заметна тенденция к расширению круга задач, выполняемых службами безопасности предприятий. Помимо собственно охранной деятельности в их прямые обязанности все чаще включаются вопросы, относящиеся к управлению рисками (в том числе страхование, защита от стихийных бедствий и восстановление производства). Соответственно меняются и требования, предъявляемые к руководителям и сотрудникам СБ, что четко отражается в расписании должностных обязанностей.

Сэм Виникур, президент компании Total Search Solutions, рассказал автору публикации в журнале «The Security Magazine», June 1, 2010 Марку МакКурту, что «опыт и навыки в сфере управления рисками, обеспечения стабильной работы предприятия постепенно вытесняют такие требования как опыт армейской службы или работы в правоохранительных организациях». Все более востребованными становятся знания в сфере защиты информации.

Рост преступлений, совершаемых работниками предприятий (от фактов насилия до кражи офисного имущества), объясняет рост числа объявлений о найме на рынке безопасности. Боб Хейес, директор Security Executive Council, отмечает, что впервые за последние 18 месяцев в кадровом сегменте индустрии безопасности заметно оживление: значительно больше увольнений и приглашений на работу. «Рост числа увольнений служит знаком оздоровления в нашей индустрии. Главное – в изменении подхода первых лиц компаний к задачам и роли службы безопасности в компании. Они начинают понимать, что СБ должны занимать более значимое место в управлении рисками».

Джефф Снайдер, президент рекрутинговой фирмы Securityrecruiter.com, рассказал о том, как он помогал крупной корпорации найти руководителя службы безопасности. После процесса отбора он представил клиенту трех финальных кандидатов, все - с большим опытом работы в правоохранительных органах. «Победил тот из них, кто во время собеседования фокусировал внимание на особенностях и результатах работы корпорации, спрашивал о стоящих перед корпорацией производственных целях и о том, как служба безопасности может наилучшим образом способствовать их достижению».

«Когда я узнаю от соискателя, что руководители организации, где он в настоящее время работает, регулярно приглашают его/ее на производственные совещания для участия в обсуждении вопросов планирования и стратегии, то мне понятно, что передо мной – элитный специалист в области безопасности», подчеркивает Снайдер. Он добавляет: «В настоящее время компании переписывают должностные обязанности руководителя по безопасности. Они в поисках новой роли для СБ, которая бы адекватно отвечала нынешним и грядущим вызовам компании в целом. И они спрашивают, есть ли у нас на примете такой специалист, который бы мог по-новому построить работу СБ? Они готовы согласиться принять бывшего офицера из правоохранительных органов при условии, что он имеет опыт и навыки бизнес менеджера».

Журнал «The Security Magazine» приводит пример, когда директор по безопасности в

одной транснациональной корпорации провел серию встреч и совещаний с руководителями ведущих подразделений и владельцами ассоциированных компаний, стремясь понять проблемы, стоящие перед ними, и стратегию выхода на более высокий уровень. В ходе встреч он спрашивал и выяснял, чем может возглавляемая им служба безопасности помочь в решении их задач, например, путем распространения и дальнейшего использования информации, которой обладает СБ. В результате ему удалось выстроить новую, более эффективную модель взаимодействия СБ с бизнес структурами внутри корпорации.

А. Куражов, Новые «роли» телефона

На прошедшей недавно в Москве 16-й Международной выставке «Охрана, безопасность и противопожарная защита» MIPS 2010, во множестве технических решений различных аспектов безопасности, представленных в экспозиции, вновь с особой актуальностью заявили о себе системы контроля телефонных переговоров (СКТП).

Не будем говорить об их негласном использовании – это прерогатива специальных служб и сфера, ограниченная законодательством. Сегодня «в ходу» телефонная «гласность» - когда системы контроля телефонных переговоров устанавливаются и используются легально, как часть «производственного процесса». Первенство в подобном использовании принадлежит государственным инстанциям. МЧС, ФСБ, МВД, РЖД, Минздравсоцразвития и др. уже давно имеют call - центры, оборудованные СКТП. Большое количество государственных и частных компаний в сфере транспорта, связи, торговли, разнообразных услуг реально и гласно контролируют телефонные переговоры своих сотрудников. Область полезного применения означенных систем чрезвычайно разнообразна.
Они распространяются и в банковской сфере. Перечислим лишь несколько задач, решению которых способствует внедрение СКТП в банках.

Повышение уровня трудовой дисциплины. Как показывает опыт, установка СКТП оказывает "тонизирующее" воздействие на сотрудников. Телефоны используются более «производительно» - в большей степени для делового общения. Сокращается количество звонков, время телефонных переговоров. Из обихода исчезает ненормативная лексика, постепенно повышается культура делового общения: телефонные контакты становятся более содержательными, корректными. Привычка контролировать себя сказывается на внутриколлективных отношениях и на работе с документами заметным повышением аккуратности сотрудников в выполнении своих непосредственных обязанностей, а в итоге – увеличением общей результативности работы.

Сокращение расходов на телефонную, в особенности – междугороднюю связь, что особенно актуально для банков с широкой филиальной сетью. Снижение доли «неслужебных» разговоров, устранение излишнего многословия в телефонных контактах дает ощутимую экономию в расходах на стационарную телефонную связь, в особенности – на IP трафик. Справедливости ради надо отметить, что при этом

возможны колебания в затратах на трафик электронной почты, мобильной телефонной связи. Но это – временные явления и они могут быть скорректированы контрольными мерами, предназначенными для этих систем.

Наличие в банке СКТП и надлежащая работа с получаемой при этом информацией вносят новые ритмы в управление: это – и *двойной контроль за подчиненными*, заряженными на решение особенно важных задач; и *более детальная проработка сделок* – прослушивание фрагментов записей совещаний, переговоров помогает продумывать ответы на «непростые» вопросы и принимать более взвешенные решения. Это – *возможность восстановления истории сделки, ее деталей*, утраченных в связи с увольнением ведущего сотрудника, и подтверждение достигнутых договоренностей, и *средство корректировки взаимоотношений руководителя с подчиненными*, и многое другое.

Традиционно данные регистрации телефонных переговоров используются *в разрешении конфликтов: начальника с подчиненным, сотрудника с клиентом, подразделения с подразделением.* Все чаще зафиксированные телефонные переговоры становятся частью доказательственной базы в судопроизводстве, в особенности – в процессах, инициированных сотрудниками против компаний, в которых они работали.

Еще одной сферой использования регистрации телефонных переговоров является *обучение сотрудников*, как новых, так и постоянных. Что может быть нагляднее конкретных примеров из профессиональной деятельности компании? Прослушивание специально отобранных фрагментов записей помогает быстрее привить новичку корпоративные правила поведения, сформировать надлежащую манеру общения с клиентом, скорректировать имеющиеся стереотипы, исправить недостатки. Возможность прослушивать телефонные разговоры сотрудника через определенное время и сравнивать результаты позволяет руководителю отследить рост его профессионализма. Это может помочь и самому сотруднику (если он добивается профессионального роста) и его руководителю, решающему текущие кадровые вопросы, такие как поощрение, взыскание, перестановка, продвижение и т.п.

Сама по себе легализация фиксации телефонных переговоров, будучи даже просто формальной частью офисной работы, становится *мощным барьером, препятствующим утечке коммерческой информации*. Определенное количество таких барьеров должно быть в каждой компании. В последнее время, в связи с введением в действие Федерального Закона № 152 – ФЗ «О персональных данных», такие барьеры становятся особенно необходимыми.

Чрезвычайно велика роль регистрации телефонных переговоров в *профилактике различного рода правонарушений*, еще встречающихся в деятельности кредитных организаций, таких как мошенничества, халатность, подлоги, хищения и др. В организациях, где такие системы установлены и грамотно эксплуатируются, значительно меньше нарушений внутрикорпоративных правил, предписанных норм поведения.

Стоит заметить, что внедрить в деятельность банка подобную систему не просто. Помимо технических сложностей, вполне преодолимых, есть сложности этического и психологического порядка. По отзывам людей, работающих с указанными системами, главная трудность заключается в воспитании лояльного отношения коллектива к наличию и функционированию систем контроля телефонных переговоров и в «правильном» использовании получаемой информации. Успех наступает тогда, когда весь коллектив компании (или, по крайней мере, большая его часть) уверен в том, что данные СКТП используются корректно, в соответствии с принятыми и оглашенными правилами, с соблюдением конфиденциальности там, где это необходимо, и с уважением к общепринятым этическим нормам.

Большое значение имеет подбор специалистов для работы с СКТП. Распространенное мнение о том, что с реализацией этой весьма деликатной функции лучше всего справляются люди, прошедшие школу оперативной работы, например – в спецслужбах, правоохранительных органах и им подобных, на практике не всегда оправдано. При всех прочих преимуществах выходцев из вышеперечисленных инстанций, следует обращать внимание не на их прошлые заслуги, а на реальные личностные качества: аккуратность; педантичность; хороший слух, память; аналитические способности; дисциплинированность, чувство долга. Это объяснимо: ведь они выполняют весьма специфичную работу, выдерживая пресс ее «непопулярности». Данную категорию сотрудников целесообразно выделить в автономную группу с подчинением одному из руководителей высшего эшелона.

Практическое освоение навыков работы с СКТП особых трудностей не представляет, поскольку разработчики систем ориентируются на пользователя упрощенного уровня компьютерной грамотности. Включить систему и настроить ее на решение заданных задач может практически любой человек, когда-либо имевший дело с компьютером. Гораздо труднее «включить» и «настроить» административно-режимные механизмы функционирования этих систем в повседневной жизни организации.

В первую очередь следует проработать юридические аспекты наличия СКТП: зафиксировать в документах, регламентирующих деятельность организации, данное обстоятельство и под роспись уведомить о нем всех работающих. Работодатель вправе ограничить ведение телефонных переговоров в личных целях в рабочее время, а если тем или иным работником эти требования нарушаются, к нему может быть применено дисциплинарное взыскание. Являясь собственником телефонных аппаратов, а также официальным пользователем телефонных линий, работодатель может ограничивать возможность использования принадлежащего ему имущества, а также устанавливать любую аппаратуру на принадлежащие ему средства коллективного доступа к телефонной связи.

Телефонная связь предоставляется работнику на основании трудового договора, в соответствии с этим договором должна определяться и ответственность работника за нарушение условий, на которых она предоставлялась. Если же своими действиями работник причинил работодателю те или иные убытки (например, работодатель оплатил личные междугородные переговоры работника), то он обязан возместить причиненный материальный ущерб в соответствии с порядком, определенным трудовым законодательством.

Упоминание об использовании СКТП необходимо в Положении об организации, Правилах внутреннего трудового распорядка, трудовых договорах, инструкциях, соглашениях.

Что касается технического исполнения, то, анализируя рынок, нетрудно убедиться в том, что выбор среди продуктов данного направления есть: основными в числе прочих являются системы записи телефонных разговоров «Phobos», «Фантом», «Незабудка». Будучи схожими в решаемых задачах, они отличаются программным обеспечением, интерфейсом.

Примечательны критерии выбора, наиболее часто используемые отечественными специалистами. В отличие от зарубежных продуктов, которые в первую очередь оценивают надежность, совместимость с другими программами, используемыми в компании, в нашей стране превалируют, к сожалению, цена и субъективное предпочтение заказчика, основанное либо на профессионализации (ранее работал с подобной системой и хорошо ее изучил), либо на меркантильном интересе (выбирается та система, покупка которой приносит выгоду и карману заказывающего её сотрудника).

При всех прочих достоинствах, для банков в наибольшей степени подходит СКТП «Фантом», разработанная компанией «МД системы». Высокая надежность в работе, основывающаяся на том, что данная система изначально разрабатывалась под телефонию; возможность использования вместе с IP-технологиями делают именно эту СКТП наиболее востребованной в банковской сфере. Сегодня в банках наиболее распространено телефонное оборудование компаний Panasonic, Siemens, LG, Samsung, NEC, Ericson, Definity. Разработчики СКТП «Фантом» ориентировали свой продукт на сочетаемость именно с этими брендами.

В настоящее время, в силу самых различных причин, банки ощущают усиление конкурентной борьбы. К этой борьбе добавляется проблема кадров: исследования рынка специалистов банковского дела показывают ограниченность ресурса высококвалифицированных кадров и высокую динамику переходов (банки «перекупают» друг у друга менеджеров среднего и высшего звена). В этой ситуации вопросы сохранения лояльности персонала к банку, предотвращения утечки информации, рассекречивания технологий банковской деятельности и им подобные приобретают особенную остроту. Правильно выстроенная работа с СКТП может стать действенным инструментом решения этих вопросов.

Финансовое мошенничество в компании: роль службы безопасности

Бред МакФарланд почти 20 лет занимается расследованием внутрикорпоративных финансовых преступлений, возглавляет в настоящее время службу безопасности холдинга The South Financial Group. В интервью для сайта csoonline.com (April, 10, 2010)

он рассказал о специфических особенностях работы по выявлению и предотвращению внутрикорпоративных преступлений в финансово-кредитных организациях.

Прежде всего, он отметил изменение отношения финансовых компаний к жульничеству своих сотрудников. В прошлом многие компании не занимались такого рода расследованиями, воспринимая попытки мошенничества как неизбежное зло, которым приходится расплачиваться, занимаясь финансовым бизнесом. Сейчас все изменилось. В эпоху информационных технологий угрозы, которые таят в себе информационные утечки, заставляют компании борьбу с мошенничеством внутри персонала выдвинуть в число первоочередных приоритетов. К тому же влияют как репутационные издержки, так и ужесточающиеся законодательные требования, нормы, регламентации.

МакФарланд подчеркнул, что программа возглавляемой им СБ включает такие вопросы как предотвращение воровства, обеспечение безопасности сотрудников, защита корпоративной информации и информации клиентов. Руководители и ведущие сотрудники СБ в кредитно-финансовых организациях должны, по его мнению, отвечать следующим требованиям:

- обладать базовым знанием основ бухгалтерского дела;

- разбираться в правовых аспектах, касающихся сферы финансов;

- обладать высокой коммуникабельностью - способностью поддерживать тесные контакты со всеми заинтересованными подразделениями компании;

- уметь проводить внутренние расследования: опрашивать свидетелей, анализировать документы и т.п.

Отвечая на вопрос о наиболее распространенных видах преступлений, с которыми сталкивается СБ, он на первое место поставил махинации с платежными документами (чеками). Затем идут: кредитное мошенничество, воровство персональных данных, фальсификация кредитных карт и т.д. Всеми этими вопросами занимается служба безопасности с тесной связи с другими подразделениями и правоохранительными органами.

Особую опасность представляют попытки использования недобросовестными служащими доступной им клиентской информации: подделка кредитных документов, манипуляции с персональными данными, увод средств с клиентских счетов...

В чем отличие расследований преступлений, совершаемых внутри и извне компании? Принципиальных различий нет, утверждает МакФарланд. Просто когда речь идет о внутрикорпоративных расследованиях, то к ним привлекаются многие службы и управления: отдел, где совершено преступление, подразделения, пострадавшие от мошенника, отдел кадров...

Важнейшее значение имеет взаимодействие СБ и отдела, который вплотную занимается информационными технологиями, поскольку постоянный контроль и анализ потоков данных представляет собой главное средство противодействия мошенничеству. «Четкий контроль данных в сочетании со знанием схем, которые применяют преступники, позволяет минимизировать риски».

Для лучшей координации в холдинге The South Financial Group создана специальная

группа (Risk Team), куда входят представители всех направлений, отвечающих за безопасность и охрану предприятия, включая специалистов по информационной защите, а также отдела по управлению рисками (Risk Management), юридической службы и тех подразделений, которые наиболее уязвимы и подвержены преступлениям.

Паркинги и гаражи: факторы безопасности

(начало см. журнал №№ 12,13)

Материальное обеспечение охраны паркингов составляют: СКУД, видеокамеры, электронные считыватели пропусков, наличие двусторонней связи с офицером охраны, система тревожной сигнализации. Желательно не устанавливать дополнительных перегородок, т.к. за ними легко прятаться. Злоумышленники также любят скрываться, используя внутренние лестницы в многоэтажных паркингах, поэтому желательно застеклить лестницы таким образом, чтобы они просматривались насквозь. Подходы к лифтам и коридоры также должны быть достаточно открыты и хорошо просматриваться. Дизайнер Аларкон любит повторять, что, проектируя гаражи, он всегда думает, будет ли он спокоен за своего сына, ставящего там машину.

Легкое ограждение помогает охранять наземный или многоэтажный паркинг, вынуждая людей входить и выходить через предназначенные для этого ворота. Там, где требуется повышенный уровень безопасности, следует воздвигнуть забор, непреодолимый для злоумышленников.

Для особо охраняемых объектов, таких, как, например, больницы, паркинг надо размещать таким образом, чтобы взрыв начиненной тротилом машины нанес минимальный ущерб зданию и персоналу. Паркинг должен быть на приличном удалении от помещений больницы, либо обнесен высокой и прочной стеной. Конечно, никакая стена не выдержит мощного взрыва, что продемонстрировал теракт в торговом центре Оклахомы, поэтому от охранников требуется внимательный и строгий контроль. В тех многоэтажных паркингах, которыми пользуются разные фирмы и лица, можно по договоренности с владельцами выделить отдельные этажи для определенных компаний.

Самую большую головную боль с точки зрения безопасности представляют подземные гаражи. После взрыва бомбы в подземном паркинге Международного торгового центра в 1993 году (Нью-Йорк), этой проблеме стали уделять несравненно больше внимания. Обычно в таких гаражах мало свободного, хорошо просматриваемого пространства, включая лестницы, много внутренних перегородок и стен, что требует установки огромного числа камер слежения, представляет сложности для мониторинга всего пространства. Однако в городских, уплотненных районах подземные гаражи - единственный способ поставить машину. Для подземных гаражей в принципе действуют те же самые правила безопасности, как и для наземных, многоэтажных паркингов, о которых рассказано выше и в предыдущих номерах журнала.

СКУД без просчетов и ошибок

Часть 4, заключительная

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 прошлых номерах журнала (№№ 11, 12, 13) изложены первые три этапа. В завершающей публикации говорим об эксплуатации оборудования и тренинге персонала.

1. Если возможно, начинайте обучение персонала уже на стадии программировании и формировании баз данных. К сожалению, нередко на это не обращают внимания. Программа для СКУД довольно сложна. И надо заранее готовить сотрудников к управлению программой, учитывая постоянно меняющиеся условия (персонал компании, рабочее расписание, различные мероприятия, которые необходимо учитывать, постоянно внося коррективы в программное обеспечение).

2. Научите сотрудников архивации данных. Большинство программ по контролю за доступом способны сохранять данные на определенный срок. Бывают обстоятельства, требующие обращения к прошлому, и здесь архивы могут оказать неоценимую помощь.

3. Для управления программой назначьте компетентного сотрудника. Ошибочно рассчитывать, что все работает в автоматическом режиме, и нет необходимости вмешиваться в процесс. На практике почти ежедневно требуется взаимодействие системы и ответственного за нее: пропуска для новых сотрудников, ликвидация карт для увольняемых, изменение рабочего расписания и тому подобное.

4. Добивайтесь приобретения достаточно мощного, современного компьютера для СКУД. Компьютер, способный обеспечить лишь минимум спецификаций программного обеспечения, не будет работать надежно. Большинство продаваемых на рынке платформ для СКУД предполагают предварительно сконфигурированные (preconfigured) компьютеры. Их преимущество в том, что операционная система идеально подходит для программного обеспечения СКУД и очень надежна в работе. К тому же «железки» этой системы унифицированы и легко заменяются во время ремонта.

СКУД без просчетов и ошибок

Часть 4, заключительная

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 прошлых номерах журнала (№№ 11, 12, 13) изложены первые три этапа. В завершающей публикации говорим об эксплуатации оборудования и тренинге персонала.

1. Если возможно, начинайте обучение персонала уже на стадии программировании и формировании баз данных. К сожалению, нередко на это не обращают внимания. Программа для СКУД довольно сложна. И надо заранее готовить сотрудников к управлению программой, учитывая постоянно меняющиеся условия (персонал компании, рабочее расписание, различные мероприятия, которые необходимо учитывать, постоянно внося коррективы в программное обеспечение).

2. Научите сотрудников архивации данных. Большинство программ по контролю за доступом способны сохранять данные на определенный срок. Бывают обстоятельства, требующие обращения к прошлому, и здесь архивы могут оказать неоценимую помощь.

3. Для управления программой назначьте компетентного сотрудника. Ошибочно рассчитывать, что все работает в автоматическом режиме, и нет необходимости вмешиваться в процесс. На практике почти ежедневно требуется взаимодействие системы и ответственного за нее: пропуска для новых сотрудников, ликвидация карт для увольняемых, изменение рабочего расписания и тому подобное.

4. Добивайтесь приобретения достаточно мощного, современного компьютера для СКУД. Компьютер, способный обеспечить лишь минимум спецификаций программного обеспечения, не будет работать надежно. Большинство продаваемых на рынке платформ для СКУД предполагают предварительно сконфигурированные (preconfigured) компьютеры. Их преимущество в том, что операционная система идеально подходит для программного обеспечения СКУД и очень надежна в работе. К тому же «железки» этой системы унифицированы и легко заменяются во время ремонта.

Электронная СКУД: время выбрасывать механические замки?

С распространением электронных карт доступа встает вопрос: что делать с

традиционными, механическими замками? Выбрасывать? Ни в коем случае, говорят американские профессионалы по охране предприятия в статье М. Фитцжеральда (онлайновый журнал csoonline, March 22, 2010).

И те, и другие средства имеют свои плюсы и минусы. Использование электронных пропусков предполагает определенную гибкость: их можно запрограммировать на доступ в четко обозначенные помещения, например в подземный паркинг, главный служебный вход и рабочую комнату (но не в бухгалтерию и другие службы компании). Ими также легче управлять, меняя в зависимости от необходимости комбинацию мест доступа. Но есть и недостатки. Электронная СКУД перестает работать из-за внезапного отключения электричества. Компьютеры могут дать сбой и парализовать всю систему. Наконец, установка и эксплуатация электронной СКУД намного дороже использования традиционных замков, что немаловажно для фирм, вынужденных на всем экономить.

Время выбрасывать механические замки еще не пришло. Они используются даже там, где уже действуют электронные карты. Например, в подсобных, технических помещениях (отопление, вентиляция и кондиционирование воздуха, электрогенераторы, силовые щиты), медкабинетах, туалетных комнатах. По сравнению с уязвимой электроникой они сохраняют надежность при соответствующем внимании и контроле.

Бернард Скальоне, директор по безопасности в медицинском учреждении New-York-Presbyterian Hospital, держит в штате своей службы, насчитывающей 150 сотрудников, трех слесарей на полной ставке по ремонту замков. В текущем году он потратит на ремонт, приобретение и замену механических замков почти 20% денег, отпущенных по статье «расходы на средства охраны», отчасти по причине проводимого во многих зданиях и помещениях ремонта. Правда, 30-40% этой статьи бюджета уйдет на приобретение и установку новых систем электронного допуска.

Скальоне считает, что, внедряя электронные средства, совсем не обязательно отказываться от традиционных замков. Надо совершенствовать систему контроля. В New-York-Presbyterian Hospital ключи к механическим замкам хранятся в одном месте и контроль за их использованием осуществляется с помощью компьютеров. То есть, дежурному охраннику нет нужды записывать в тетрадь, кто и когда взял ключи, когда вернул. Все это за него делает компьютер, который следит, кто взял ключи и к каким дверям, когда и какие двери открыты/заперты. Все данные в автоматическом режиме фиксируются и хранятся в памяти компьютера.

По мнению Скальоне, необходимо идти к интеграции систем видеонаблюдения и управления механическими замками, когда камеры фиксируют изображение лиц, пользующихся дверными ключами. В New-York-Presbyterian Hospital это дело ближайшего будущего. В первую очередь такой интеграционной системой охраны будут обеспечены помещения, где хранятся и выдаются лекарства, и операционные, где установлено дорогостоящее оборудование.

Базовые принципы

внутрикорпоративных расследований

(начало см. журнал №№ 12,13)

Если возникает необходимость изъять у подозреваемого компьютер, содержащиеся в нем файлы, то такую акцию необходимо заранее планировать и запротоколировать специальным актом. Обычно компьютер изымается ночью или ранним утром, до начала работы.

Вот что рассказывает об этой операции руководитель службы безопасности на одном из американских предприятий (анонимно): «Обычно эту работу проделывают два сотрудника СБ. Один из них имеет при себе подробный перечень шагов, которые необходимо предпринять, протоколирует все действия, а другой отсоединяет компьютер от сети, разбирает его, снимает жесткий диск, закрывает и ставит машину на место. Однажды во время этой операции неожиданно в комнате появился служащий, работающий с этим компьютером. Пришлось ему сказать, что его машина «заражена вирусами и нуждается в чистке в отделе IT». Чтобы избежать подобной ситуации, надо все это проделать или ночью, или же лишить подозреваемого доступа в офис, изъяв пропуск».

Сложнее с мобильными гаджетами. Их также изымают под любым предлогом. Но, конечно, в таких случаях не удается скрыть от подозреваемого, что в отношении него ведется внутреннее расследование. После того как карты раскрыты, наступает время для беседы (допроса).

Существует специальная методология допроса, позволяющая установить степень вины (или невиновность) подозреваемого. Она разработана Н. Гордоном, основателем и директором The Academy for Scientific Investigative Training в Филадельфии.

Беседа начинается с темы, не имеющей отношения к содержанию, но призванной растопить ледок, создать непринужденную и откровенную атмосферу. Разговор на отвлеченные предметы дает возможность допрашивателю изучить стиль поведения собеседника: манеру говорить, смотреть в глаза или в сторону, жестикуляцию…

Беседуя, важно обращать внимание на жесты, характеризующие реакцию, настроение, отношение. Например, если собеседник часто подносит руку ко рту или глазам, то это может говорить о лживости его слов, о желании скрыть правду. Жестикуляция правдиво отвечающего на вопросы обычно как бы призвана помочь объяснить свою позицию. К примеру, он/она прикладывает руку к груди, смотрит прямо в глаза…

Формулируя вопросы, надо избегать их обличительного характера. Важно записывать и вопросы, и ответы. Желательно вести допрос вдвоем, когда один записывает, а другой беседует. Недопустимо, чтобы кто-то третий, скажем, присутствующий на беседе начальник отдела кадров, вмешивался в беседу. Его дело – слушать и не влезать.

Нередко приходится допрашивать сотрудников как свидетелей. В таких случаях Гордон советует обязательно уведомлять, что они – вне подозрений, но могут помочь расследованию.

В принципе можно использовать скрытые камеры для видеозаписи допроса, если это предусмотрено и разрешено документированной политикой безопасности в компании, если камеры давно установлены в общедоступных помещениях. Но с правовой точки зрения могут возникнуть проблемы. В любом случае лучше предварительно посоветоваться с юристом.

Каких ошибок надо избегать? Запугивания, представления под вымышленным именем, предъявления обвинений без достаточных доказательств, утечки информации, ведущей к распространению слухов, которые могут повредить как компании, так и проводящим расследование.

Воровство в компании: легка беда начало

«Это не был чек в полмиллиона долларов, - говорит г-жа Каттани, которой решением суда запрещено работать в общественных организациях, - сначала немного взяла здесь, немного – там. Так постепенно и происходило мое падение».

Ее криминальная история начиналась вполне невинно: турагент случайно снял деньги на оплату отпускной поездки Каттани не с ее частного счета, а со служебной кредитной карты. Каттани об этом никому не сказала. В компании не заметили. Тогда она стала понемногу использовать деньги компании для оплаты личных нужд.

Она никого не обвиняет в содеянном. Только себя. Движимая чувством вины, она ездит с лекциями, рассказывая, какой урон наносит бизнесу воровство в компаниях. Особенно там, где для этого созданы подходящие условия.

«То, что произошло со мной, может случиться с каждым, если этому благоприятствует обстановка, - говорит она, - А именно: слабый контроль в компании, личная острая нужда в средствах, склонность к «рационализации». Если эти три фактора совпадают – возникает соблазн, коварно и неизбежно». (abcnews.go.org).

Другой персонаж - Джюстин Паперни, в прошлом биржевой маклер, осужденный за уголовное преступление.

«Конечно, я знал, что мой клиент использует схему Понци (схема построения финансовой пирамиды, предполагающая, что доходы первых инвесторов обеспечиваются взносами новых участников; названа по имени итальянского эмигранта Чарльза Понци, впервые построившего подобную пирамиду в конце 1920-х гг.), - признается Паперни, который провел полтора года в тюрьме.

«Но умения отличать правильное от неправильного недостаточно, - продолжает он, - Я ощущал собственное превосходство. Я оправдывал свое поведение большими комиссионными, которые получал. Если вы преступили закон в первый раз, то одна ложь переходит в другую и растет как снежный ком».

Любопытно, что Паперни обнаружил в тюрьме немало людей, таких же, как он, прохиндеев. Они тоже оправдываются тем, что просто использовали благоприятную

возможность нажиться. «Это обычные нормальные ребята. Среди них есть и брокеры, и бухгалтеры, и аудиторы. Лишь единицы носят на лбу печать врожденного преступника. Большинство – такие же люди, как вы и я».

Охрана небольших помещений

Если компания занимает немного площадей, скажем, всего несколько комнат, все равно она нуждается в надежной охране имущества, интеллектуальной собственности, сотрудников.

Джоки Бадаго на сайте realestateproarticles.com (1 марта 2010 г.) обращает внимание на некоторые шаги, которые следует предпринять в первую очередь для организации охраны.

Прежде всего, следует выяснить, какова криминогенная обстановка в районе расположения фирмы. В местном отделении полиции вам расскажут, какие преступления, связанные со взломами, грабежами, воровством, имели место в последнее время. Там же могут посоветовать, какую систему безопасности следовало бы выбрать.

Сегодня на рынке предлагается масса средств охраны. Многие из них подходят для малого бизнеса. Прежде чем выбрать, надо все хорошо продумать. Надо защитить двери и окна? Сначала посмотрите, насколько легко проникнуть в служебные помещения. Прикиньте, что бы вы сделали на месте злоумышленника, чтобы забраться в офис.

Следующий после подготовительной работы шаг – выбор средств охраны. На рынке есть и дорогие системы, и подешевле. Неверно считать, пишет автор, что недорогие средства защиты всегда уступают дорогим качественно. Вполне возможно подобрать оптимальную по соотношению «цена-качество» систему, которая будет надежно вам служить. Главное, чтобы эта тревожная сигнализация или другая выбранная вами система была установлена на всех внешних дверях и окнах.

Часто пренебрегают дверными замками. Если они обычные, то лучше заменить на современные замочные системы, надежно защищающие от взлома. Одновременно поставить железную дверь.

Надо подумать и о камерах видеонаблюдения. Это не дешевое удовольствие. Если бюджет напряжен и лишних средств нет, можно использовать для этих целей офисное оборудование – компьютер, веб-камеру, программное обеспечение видеонаблюдения.

Инвестиции в безопасность в любом случае необходимы и себя полностью оправдывают.

Безопасность в командировках: что брать с собой на случай стихийных бедствий?

Основатель и глава компании по безопасности и управлению рисками Insight Security Крис Фалкенберг утверждает, что руководители СБ, готовя командировки менеджеров, думают прежде всего об угрозах, обусловленных человеческим фактором, и часто не предусматривают опасности, генерируемые потенциальными стихийными бедствиями (землетрясения, торнадо, пожары, цунами и т.п.). Возможно, по той причине, что такие форс-мажоры случаются редко.

Фалкенберг настаивает: «если вы отвечаете за безопасность поездки, то вам надо обеспечить командированного всем необходимым для того, чтобы продержаться без помощи извне в течение, по крайней мере, 72 часов (CSO, March 2, 2010). Фалкенберг предлагает список вещей, которые обязательно надо иметь в чемодане:

Телефон спутниковой связи. В некоторых экстремальных ситуациях (например, при аварийном отключении местной электросети) обычные сотовые телефоны могут оказаться бесполезными. Либо не поступает энергия на вышки сотовой связи, либо просто не дозвониться, так как сети перегружены. В этих условиях телефоны космической связи незаменимы.

Вторая вещь, о которой надо позаботиться – это запас чистой воды. Во время землетрясения в Чили более всего востребованными оказались системы очистки воды. В поездку можно взять необременительный по весу и габаритам прибор по очистке воды, специальные йодированные таблетки, иные средства. Они особенно необходимы, когда речь идет о поездке в развивающиеся страны.

Фонарь на батарейках (сигнальная лампа). По мнению Фалкенберга,в экстремальной ситуации нет более ценного инструмента, чем flashlights.

Маски N-95. Они полезны на случай землетрясения, пожара, эпидемических заболеваний.

Наконец, хорошая медицинская аптечка. Она просто необходима там, где помощь врачей приходит не сразу.

Индия: полно охранников, но кто их обучает?

Глен Киттерингхем, специалист по безопасности, провел некоторое время в Дели, где читал курс лекций для преподавателей охранного дела (Certified Protection Officer Instructors). В онлайновом журнале canadiansecuritymag.com он поделился впечатлениями.

Глен спросил местного коллегу, сколько в Индии насчитывается охранников. Ему ответили, что никто не ведет официальный учет, но в стране насчитывается порядка 10 000 охранных предприятий. Эта цифра звучит правдоподобно для страны с населением 1 миллиард 200 миллионов жителей (в одном Дели – 30 миллионов). Во время своей поездки Глен встречал охранников повсюду. Зарплаты в Индии низкие, в среднем охранник зарабатывает в месяц около 100 долларов США.

В свой первый выходной он отправился в сопровождении коллеги из числа местных экспертов по безопасности в ближайший молл (мега-торговый центр). На въезде в подземный паркинг их машину встретили два охранника. Один из них с помощью специального приспособления на колесиках с зеркалом осмотрел днище. Второй попросил поднять багажник. Он несколько раз взмахнул ручным металло-детектором и затем разрешил закрыть багажник. Охранники ориентированы на поиск взрывчатых веществ, разъяснили Глену.

В паркинге он увидел еще несколько охранников, которые регулирование движение. Оставив машину на стоянке, они двинулись к лифту, зайти в который можно, только пройдя через стационарный, рамочный металло-детектор. Лифтом управлял еще один охранник.

Бродя по торговым помещениям, Глен заметил, что у входа в каждый магазин стоят один-два охранника, нанятые владельцем лавки. Хозяева молла имеют и собственную службу безопасности, сотрудников которых можно было видеть повсюду. Все эти охранные компании работают отдельно друг от друга, избегая кооперации, даже в случае каких-либо происшествий. По подсчетам Глена, в охране торгового центра занято свыше 200 человек. Все они, как правило, без оружия.

Живя и работая в Дели, Глен не раз сталкивался с металло-детекторами, особенно часто в торговых районах мегаполиса. Когда он проходил через них, раздавался сигнал тревоги, но никто не обращал на это внимания. Никому из охранников и в голову не могла придти мысль остановить его и обыскать.

Главная здесь проблема – низкий профессиональный уровень охраны. С охранниками, похоже, здесь никто серьезно не занимается.