

## **ОХРАНА ПРЕДПРИЯТИЯ**

**№2, 2008**

### Общие проблемы

**Выбираем охранную фирму**

**В.Рибизов**

**Развитие рынка услуг телохранителей в России**

### Новые технологии, методологии

**Метод психозондирования (MindReader) - новая технология безопасности предприятия**

### Риски и угрозы безопасности бизнеса

**Ю. Козлов**

**Личная безопасность руководителя - каким должен быть телохранитель**

**Планируем аудит по безопасности**

**Быть готовым к ЧП на предприятии**

**Принтеры - уязвимое звено безопасности предприятия**

**Когда начальник читает вашу почту**

### Системы контроля и управления доступом

**Когда двери вращаются...(из опыта охраны зданий одной американской компании)**

**Часть 2**

**Ответственный за безопасность по этажу - зачем он нужен?**

### Охрана малого предприятия

**Выбираем фирму для установки и эксплуатации системы охраны**

**Охрана предприятия быстрого питания**

### книжное обозрение

**«Конвергенция охраны. Управление рисками безопасности предприятия»**

**В. Светозаров**

**Как в Америке выбирают охранное предприятие для обеспечения безопасности школ**

© "АМУЛЕТ" 2003 г. Тел/Факс.(495) 614-40-60, 614-41-60, E-mail:[info@amulet-group.ru](mailto:info@amulet-group.ru)

## Выбираем охранную фирму

Если вам надо найти фирму и заключить контракт по охране вашего предприятия, то, возможно, окажутся полезными советы западных специалистов по вопросам безопасности и охраны. Некоторые рекомендации по безопасности и охране опубликованы на сайте [bizsecurity.about.com](http://bizsecurity.about.com):

Главное – не спешить заключать контракт с первой попавшейся компанией по охране. Пусть вас не завораживает бравый вид «Охраны», красивая униформа и сверкающие бляхи. Не жалейте время на выбор достойного партнера по охране, с хорошей репутацией и безупречным бэкграундом.

Прежде всего, необходимо тщательно проверить лицензию на охрану, другие разрешительные документы по охране, обусловленные местным законодательством. Нелишне обратиться в организацию, выдавшую лицензию на охрану, и поинтересоваться, были ли жалобы от клиентов данной компании по охране.

Особенно важно обратить внимание на репутацию фирмы по охране. Надо просмотреть СМИ и заглянуть в специализированные базы данных на предмет, не было ли судебных исков против нее со стороны клиентов и собственных сотрудников охраны.

Обязательно надо обратиться с запросом к бывшим (или настоящим) клиентам фирмы охраны, спросить их мнение. В первую очередь, к тем, чья деятельность совпадает или схожа с вашей компанией.

Заслуживает внимание такой показатель как текучесть кадров охраны на оперативном уровне. В предприятиях по охране, бывает, она достигает 100 и выше процентов в год. Одновременно посмотреть, сколько лет работают в фирме охраны ее руководители.

Фирма предпочтительна, если она обеспечивает своим сотрудникам повышение квалификации, проводит обучение и тренинги по охране.

Еще до подписания контракта надо заблаговременно обговорить и отразить в контракте разные вопросы охраны, например:

- как руководство фирмы охраны будет осуществлять контроль за своими сотрудниками (охранниками);

- какое будет наказание, вплоть до замены, тех охранников, которые себя плохо зарекомендуют по охране объекта;
- порядок предоставления фирме-клиенту копий отчетов охранников (своему начальству). Последнее требование нужно для того, чтобы своевременно вскрывать и предотвращать угрозы, снижать риски, планировать собственную работу по безопасности и охране предприятия.

Внимательно проанализируйте предложенный предприятием по охране проект контракта.

Он должен полностью соответствовать законодательству и официальным инструкциям по безопасности и охране, а также отражать специфику вашей организации, особенности и требования.

О некоторых нюансах составления контракта и его финансовых аспектах – в следующем номере журнала.

## **Развитие рынка услуг телохранителей в России**

**В.Ребизов**

Принято считать, что телохранители в России появились в начале 90-х годов прошлого века. На самом деле их появлению предшествовал спрос на услуги крепких парней за рулем автомобиля во времена появления в августе 1988 года «Закона о кооперации». Теневые деньги уверенно выходили «в свет». В обиходе российских кооператоров и правоохранительных органов появилось заграничное слово «бизнес». Именно бизнес как деятельность, связанная с риском не только для денег, но, как показало развитие событий, для жизни и здоровья, стал генератором появления спроса на телохранителей – по образцу и подобию западных рынков

Спрос на телохранителей рос прямо пропорционально накоплениям «первоначального» капитала. Услуга стала особенно востребованной после громкой череды резонансных убийств, прокатившихся по стране. Телохранители становились престижными и модными, часто выступая со стороны заказчика как атрибут важности и достатка. Бизнес становился все больше рискованным, и личная охрана прочно завоевывала свою рыночную нишу. В нее, как в водоворот, включалось все больше и больше энергичных и авантюрных участников игры, правила которой тогда практически никто не знал. Последствия были достаточно печальными для многих.

В то время для того, чтобы носить с собой пистолет, достаточно было зарегистрировать ЧОП. Быстро и недорого. Пистолеты с «телохранителями» путешествовали городским транспортом и ночевали в местах, далеких от оружейных комнат. Услуги по «защите жизни и здоровья» оказывались мгновенно, спрос превышал предложения. Самым решающим аргументом качества становилось простое слово «профессионал». Этим статусом называли себя практически все, кто выходил на улицу за спиной «охраняемого тела». Отсутствие навыков, опыта, не говоря об умении, никого не смущало. Ни телохранителей, ни их работодателей.

Подобная ситуация была характерна на рынке телохранителей в 90-х. Зачастую

телохранители нанимались на время, для защиты своих клиентов во время сделок или перевозки ценных вещей, а то и просто для защиты от пуль во время выяснения отношений вне правового поля.

Следующим существенным событием в те годы был приток на рынок специалистов из правоохранительных органов после событий 1993 года. Медленно, но верно начал меняться подход к подбору, расстановке и обучению личной охраны. Офицеры моментально находили свое место в потоке спроса на высококлассных специалистов. Старшие офицеры уходили на руководящие посты в корпорации и компании, младшие - на пост к нарождающимся олигархам. Последние твердо знали стоимость своего здоровья и благополучия. Профессионалы получали достаточно, чтобы не искать заработка в сфере тренировок и обучения. Их заработная плата становилась своеобразным ориентиром для формирования ценовых категорий на рынке того времени. В то время она составляла около 1 800 – 2 000 долларов в месяц. Однако, по мере развития рынка проявилась устойчивая тенденция к ее снижению.

Тогда же проявилась еще одна реальия телохранительства в России. И она была связана с оружием. МВД России с каждым годом становилось все сложнее контролировать оборот табельного оружия выданного на основании частных охранных лицензий. В то же время дипломы по специальности «охранник-телохранитель» можно было просто купить, цена доходила до 150 долларов за штуку. Практически каждый заинтересованный мог его получить и носить «Макаров», ссылаясь на статью закона о «защите жизни и здоровья». Критическая масса правонарушений в этой сфере достигла своего предела в конце 1995 года. Из терминологии частного охранного рынка волевым решением МВД исключило слово «телохранитель». В соответствии со стратегией организации, телохранители были четко разделены с охранниками, которые представляли рыночную категорию.

Изъятие из рыночного пространства упоминание о телохранителях никакого эффекта на спрос ровным счетом не оказало. Напротив, на конференциях уже набравшего уважение Международного форума «Технологии безопасности», а также на страницах профильной прессы стали чаще звучать призывы о внесении поправок в текущее законодательство, предусматривающих статус телохранителей. Эти призывы подхлестывала жестокая реальность – количество резонансных покушений не уменьшалось, имена жертв не сходили с первых полос газет и программ телевидения.

Отметим, что средний стаж работы телохранителя составлял уже 4-5 лет и это были люди, которые достаточно хорошо разбирались в рыночных хитросплетениях. Клиенты к ним привыкали, а сами телохранители чувствовали себя на высоте, их уверенность в собственном профессионализме крепла с каждым рабочим днем. Проблемы ношения оружия оставались проблемами охранных предприятий, и предметом более чем пристального внимания МВД.

Дефолт августа 1998 года стал для телохранителей своеобразной датой рождения нового взгляда на рыночную действительность. Существенно сократился спрос на личную охрану вследствие финансового краха многих предпринимательских структур. Клиенты стали гораздо разборчивее в выборе своей личной охраны. Предложение, наконец, превысило спрос. Средняя зарплата телохранителей покатилась вниз. Рынок отреагировал массовой атакой на имидж этой услуги, где основную роль играло слово «профессионал». Но далеко не все на этом рынке могли понять, что это такое. Профессионалом- телохранителем себя величал любой, кто желал получать деньги за свои былые достижения: служба в правоохранительных органах, «горячие точки»,

спортивные регалии и т.д. Но логика диктует: если все профессионалы, то никто не профессионал.

Профессионал отличается от ремесленника тем, что у последнего нет определенного уровня соответствия требованиям профессии, а у первого есть. Следующий вопрос заключается в том, кто определяет эти требования и насколько они реальны? Именно с этим столкнулись телохранители в канун нового тысячелетия. Началось очень жесткое и бескомпромиссное деление на телохранителей и профессиональных телохранителей. Сам процесс достаточно латентен, он скрыт от постороннего глаза. Чтобы в нем разобраться, нужно иметь причины. Но пока нет правового поля для телохранителей, это дело самих телохранителей. Процесс качественного деления телохранителей на вышеуказанные категории начался с наступлением нового века. Символично. Но закономерно.

С 2000 года российская школа личной охраны практически отказалась от концепций и доктрин западных коллег в области обеспечения личной безопасности по причине их малоэффективности в правовом и социальном пространстве России. Сформированы и предложены профессиональные принципы работы, требования и мораль. Практически все концептуальные положения подтверждаются практикой: профессиональный аудит, стандарты, квалификационные требования. Профессиональный подход стремительно набирает обороты, особенно после 2003 года, когда определилось региональное единство, рынок отреагировал повышением средней заработной платы телохранителям, которые сделали выбор в сторону профессионального развития. С 2004 года наблюдается постепенное выравнивание средней заработной платы в регионах и ее невысокий, но стабильный рост. Она перестала падать.

Сегодня средняя зарплата телохранителей в Москве в эквиваленте составляет порядка 1000 евро. Средняя зарплата телохранителя в России варьируется в зависимости от региона от 500 до 850 евро. Телохранителей можно смело отнести к развивающемуся среднему классу российского общества.

Согласно статистике в России средний возраст российского телохранителя – 28 лет, в 70 случаях из 100 – это бывший военнослужащий, он женат, имеет ребенка, его образование в 40% – высшее. Среднестатистический «профессиональный возраст» телохранителя начинается в 25 лет и оканчивается в 35-40 лет. В возрасте старше 40 лет телохранителю получить работу крайне сложно. По завершении профессиональной карьеры телохранитель может начать свое собственное дело.

Одним из мифов профессионального рынка остаются женщины-телохранители. Они есть, но оценить профессиональный уровень достаточно сложно в силу нежелания последних. Достаточно высоким спросом пользуются на рынке бывшие сотрудники ФСО, в меньшей степени других правоохранительных органов. На рынке личной охраны достаточно развит институт личных рекомендаций. С удовлетворением можно констатировать, что за последние пять лет наблюдается устойчивая тенденция к нивелированию ценности иностранных дипломов, выданных после прохождения различных профильных курсов за пределами страны.

Динамика роста охранных предприятий практически не повлияла на количество телохранителей. Рынок имеет достаточные кадровые ресурсы для удовлетворения спроса на эту услугу. Сегодня на рынке больше клиентов, готовых платить выше, но за качественный товар (т.е. за умение). Эта ситуация определяет перспективы дальнейшего развития профессионального сообщества телохранителей. Мониторинг

цитируемости телохранителей в СМИ также подтверждает этот тезис. Можно отметить понижение витальной (смертной) статистики с участием телохранителей в сравнении с девяностыми годами. Однако, реалии рыночной деятельности телохранителей сегодня не сильно отличаются от реалий десятилетней давности: телохранители продолжают переоценивать собственные способности и недооценивать возможности проявления угрозы в адрес своих охраняемых лиц. Опираясь на свежие статистические данные, можно сказать, что самым слабым звеном группы охраны по-прежнему продолжают оставаться водители автомобилей, причем как основных, так и прикрытия. Следующим моментом, отмечаемым специалистами, является слабость, а порой элементарное игнорирование телохранителями постовой дисциплины. Телохранители в принципе умеют стрелять, оказывать силовое противодействие нападению, знают, где идти, как открывать любые двери, как решаются хотя бы элементарные тактические задачи, они научились рассуждать на данную тему, но на посту они почему-то этого не делают. Вопросы психологического тренинга и мониторинга групп личной охраны будут приоритетными направлениями развития науки обеспечения личной безопасности.

Можно с определенной долей оптимизма сказать, что российский рынок телохранителей обрел определенные очертания, но заявить о том, что он сложился, было бы преждевременно. Найти телохранителя достаточно просто, но нанять профессионального телохранителя для клиентов составляет достаточно сложную задачу. Парадоксальная ситуация на рынке личной охраны особенно характерна для больших российских городов с населением около миллиона человек или более: тех, кто готов заплатить за услуги профессионального телохранителя, больше, чем тех, кто соответствует этим требованиям. Клиент начинает включаться в маркетинговые стратегии. Он начинает понимать роль и место телохранителя. Ему становится не все равно, кто находится рядом с ним и за что он платит деньги.

## **Метод психозондирования (Mindreader) - новая технология безопасности предприятия**

(по материалам сайта [www.mindreader.ru](http://www.mindreader.ru))

Неправомерные действия, халатность, саботаж, утечка конфиденциальной информации со стороны сотрудников организаций приносят колоссальный ущерб компаниям. Некоторые руководители понимают опасность, которую таят в себе эти угрозы, многие руководители даже не представляют, что причиняет им ущерб, и в каком объеме, поскольку многие инциденты тщательно скрываются и не контролируются, поэтому организации часто оказываются не в курсе, что они подвергаются атаке изнутри.

В настоящее время основное внимание уделяется в основном техническим средствам безопасности (контроль доступа, тотальное видеонаблюдение и т.п.) и не всегда учитывается "человеческий фактор" когда, либо кандидат на вакансию имеет "человеческие слабости" (алкоголь, наркотики, игровая зависимость), либо работающий сотрудник имеет твердые намерения воспользоваться служебным положением в личных целях и знает как "обойти" существующие системы

безопасности.

Широко применяются два метода решения поставленных задач, это полиграф (детектор лжи) и аппаратно-программный комплекс MindReader (разработка НИИ психотехнологий). Единственное сходство данных методов заключается в том, что они во многом решают одинаковые задачи, хотя возможности АПК MindReader, как в сфере кадровых вопросов, проблем безопасности, так и в других сферах гораздо шире. О полиграфе накоплена обширная литература. О разработке НИИ психотехнологий известно меньше.

Основатель НИИ психотехнологий, И.В. Смирнов, начинал свою карьеру в должности заведующего лабораторией психокоррекции в Московском медицинском институте им. И.М. Сеченова (ныне - Московская медицинская академия им. И.М. Сеченова), в которой в восьмидесятах и начале девяностых годов прошлого века проводились исследования, в том числе, и по заказу правительства СССР. В научно-исследовательских работах были получены результаты, показавшие, что действительно можно получать достоверный вывод об обладании человеком конкретным знанием, минуя его сознание.

Технология, о которой идет речь, зарождалась в лаборатории психокоррекции - одновременно с развитием доступной компьютерной техники - как диагностическое средство, способное помочь психотерапевту в максимально короткие сроки определить у пациента вытесненные причины неврозов, и вообще - у человека - сознательно или неосознанно скрываемую им информацию. С 2003 года метод внедряется на территории России в коммерческих и государственных организациях, в основном в целях обеспечения кадровой безопасности. Обследуются принимаемые на работу и действующие сотрудники на предмет выявления у них рисков, которые могут нанести организации ущерб. К этим рискам относятся, например, разного рода зависимости, намерения получить конфиденциальную информацию в интересах конкурента и пр. Метод психозондирования на Всемирной выставке научных достижений в Брюсселе (1998 г.) удостоен Большой золотой медали. Дважды отмечен медалью Международного форума "Технологии безопасности", проходящего ежегодно в Москве.

Программно-аппаратная реализация данного метода позволяет сотруднику службы безопасности или сотруднику кадровой службы самостоятельно разрабатывать тесты под определенные существующие проблемы и задачи.

Тест полностью автоматизирован и не требует специальных знаний от оператора АПК.

Кроме этого, при проведении регулярных проверок действующих и рекрутируемых в организацию сотрудников, с помощью АПК MindReader руководителям становится доступной, причем с минимальными временными затратами, следующая информация:

- \* принадлежность кандидатов к определенным криминальным кругам;
- \* наличие или отсутствие недозволенных связей с конкурентами;
- \* намерения кражи и передачи информации;
- \* степень лояльности к организации и руководству;
- \* наличие фактов использования служебного положения в корыстных целях, сговора с клиентом ("откат") или аналогичные намерения; патологические мотивы (алкоголизация, наркомания, игровая зависимость, стремление к мести, склонность к неоправданному риску и т.п.);
- \* наличие личных проблем (неадекватное отношение к охраняемому лицу, долги,

неадекватное отношение к оружию, проблемы с законом, семейные проблемы и т.п.);

- \* криминальные намерения кандидата

- \* оценка морально-психологического климата внутри коллектива.

По результатам комплекса тестов появляется возможность отследить:

- \* формирование и развитие у сотрудников моральных основ честной и ответственной работы;

- \* мотивацию сотрудников на самоотверженные действия при решении ответственных задач;

- \* психологическую совместимость сотрудников;

- \* степень авторитета руководителей;

- \* негативные факторы, влияющие на психическое состояние сотрудников.

- \* взаимоотношения в коллективе.

По оценкам аналитиков служб безопасности ведущих банков России АПК MindReader позволяет заблаговременно вскрыть следующие нарушения:

- \* Злоумышленный сговор внештатных сотрудников отделов потребительского кредитования.

- \* Криминальный вывод активов банка топ-менеджерами.

- \* Кража баз данных.

- \* Внедрение "казачков" засланных.

- \* Сговор сотрудников служб инкассации.

- \* Невозврат кредитов.

- \* А также оценить риск при приеме кандидатов на работу.

Метод психозондирования, разработанный И.В.Смирновым, внедряется в работу служб безопасности и охранных предприятий России. Получает он известность и за рубежом. *В следующем номере журнала читайте обзор западных СМИ об этом изобретении.*

## **Личная безопасность руководителя - каким должен быть телохранитель**

**Ю. Козлов**

В предыдущем (№1) нашего журнала мы опубликовали статью Юрия Козлова «Личная безопасность руководителя – угрозы и риски (на примере компании «XXX»)». В текущем номере предлагаем вашему вниманию вторую статью автора, посвященную созданию в рамках службы безопасности компании группы телохранителей на примере конкретной крупной компании «XXX» (о компании см. №1 журнала).

Первый шаг – формирование штатного расписания подразделений, обеспечивающих личную безопасность Руководителя Компании «XXX».

В нашем случае штатное расписание выглядит так:

После утверждения штатного расписания приходит очередь кадрового вопроса. Подбор сотрудников - ключевой этап обеспечения безопасности предпринимателя.

На сегодняшний день рынок вакансий в сфере охранных услуг насыщен соискателями. Согласно статистики, львиную долю (60%) составляют отставники силовых ведомств и

министерств (армия, милиция, ФСБ, отслужившие в «спецназе», или в «горячих» точках). И еще выпускники специализированных школ по подготовке частных охранников и детективов. На втором месте (30%)- только что вернувшиеся из армии «дембели», «срочники». И на третьем месте - все остальные граждане, как правило, никакого отношения к охранной службе ранее не имевшие. Это и пенсионеры, и молодежь, не определившаяся со своим призванием в жизни, и желающие подзаработать студенты, наивно полагающие, что в охране особых знаний и умений требуется. Во всем этом многообразии работодателю приходится вести селекционную работу по «отделению зерен от плевел».

Попытаемся проанализировать возможности, способности приведенных выше категорий соискателей применительно к разным должностям в системе безопасности организации.

Заместитель начальника Службы безопасности - начальник личной охраны

Большой удачей для предпринимателя было бы «заполучить» представителя Федеральной службы охраны- продолжательницы дела 9-го управления КГБ СССР. Общеизвестно, что лучшие профессионалы - те, кто занимался охраной высокопоставленных лиц государства. Высококласная школа, пройденная на прежней службе, научила таких «спецов» практически всему, чему должен отвечать современный телохранитель и его руководитель. Они могут многое: просчитать действия вероятного противника, учесть все мелочи, и неотступно надзирать за тем, чтобы их подчиненные этими самыми мелочами не пренебрегали.

#### Сотрудники подразделения выездной охраны

##### *Телохранитель*

Телохранитель высшей квалификации в идеале - разносторонний профессионал с натренированной способностью к молниеносной ориентацией, с отработанной до уровня звериного чутья интуицией и безусловной мышечной памятью. Опытный «спец», который в критической ситуации не мыслит, а действует «на автомате». Его стиль жизни и мышления - поиск и оценка опасности, способов защиты от нее в любой обстановке. Это человек железной дисциплины, мастер выкручиваться из нестандартных ситуаций. То, что для всех стресс, кошмар и ужас, для него - норма.

Зачастую при выборе телохранителя бизнесмены руководствуются довольно распространенными ошибочными критериями: телохранитель, значит, обязательно широкоплечий атлет высокого роста, с тяжелыми кулаками. В личной охране чаще всего ценятся те, кто не выделяется ни внешностью, ни одеждой, ни поведением. Главная задача телохранителя не столько прикрыть клиента своим телом, сколько предотвратить угрозу в экстремальной ситуации благодаря молниеносным, целесообразным, грамотным действиям.

Телохранитель не обязательно должен обладать «черным поясом» по каратэ или быть чемпионом по боксу. Кулаки и мускулы не спасают от пули, а спортивная техника далеко не всегда пригодна для реальной жизненной ситуации. Плох тот телохранитель, который стремится довести дело до рукопашной схватки. Он должен так строить свое поведение, чтобы у потенциального агрессора пропадало желание подвергаться риску, чтобы ограничить его возможности для покушения. В этом заключается суть работы телохранителя, основная задача. Конечно, я не отрицаю пользу регулярных тренировок по рукопашному бою, но надо различать спорт и

прикладной уличный бой.

Часто считают, что за плечами телохранителя обязательно должна быть служба в «горячих» точках, на худой конец- служба в спецназе. Те, кто так думает, не понимают, что всякий опыт специфичен. Телохранителю не требуется умение устраивать засады в горах, или прыгать ночью с парашютом. К тому же, далеко не все возвращаются с войны с психологической закалкой. Кое-кто скорее может стать профессиональным киллером, а не телохранителем. .

Отдельно хотелось бы отметить телохранителей- женщин. Они, как правило, ценятся за интуицию и «алогичное», с точки зрения мужчин, поведение. Кроме того, женщина успокаивающе воздействует на недоброжелателя: большинство мужчин не воспринимают их как серьезных противников. Женщин- телохранителей можно видеть в окружении сильных мира всего.

#### *Водитель-охранник*

При выборе водителя- телохранителя следует учитывать следующие моменты. Водитель не может эффективно делать свое дело, если одновременно с управлением транспортного средства он обязан охранять жизнь клиента от возможных посягательств вне машины, в машине, в движении или на месте. Только в тех нечастых случаях, когда покушение происходит во время движения машины, от водителя зависит все или почти все. Во всех иных ситуациях совмещать функции водителя и телохранителя практически невозможно. Поэтому на эту должность надо выбирать именно водителя, способного, если надо, оставить руль и выполнять функций телохранителя.

#### *Сотрудник группы контрнаблюдения*

Здесь лучше подходят сотрудники оперативно- поисковых подразделений силовых министерств. За десятилетия существования службы наружного наблюдения, бывшие оперативники- «топтуны» обладают всеми необходимыми навыками для осуществления контрнаблюдательных мероприятий.

#### *Охранник*

На должность охранника можно пригласить отставников Министерства обороны и неоперативных подразделений милиции. Меньше подходят вчерашние военнослужащие - «срочники», так как они не могут похвастаться тем, чем овладели за годы своей службы представители вышеперечисленных категорий соискателей - житейским опытом, выдержкой и самодисциплиной. Пенсионеры силовых структур, как правило, не старые люди (минимальный срок для получения выслуги- 20 лет), могут полноценно нести службу охранника на новом месте работы.

Также можно воспользоваться услугами частных школ охраны, которые выпускают уже готовых специалистов, но этот путь обойдется дороже.

## **Планируем аудит по безопасности**

Аудит по безопасности проводится с целью обеспечения надежной охраны предприятия. Серьезный аудит способен выявить потенциальные риски и угрозы,

определить меры по их предотвращению. Сайт eHow рекомендует придерживаться следующего плана при подготовке к аудиту:

Сформулировать цели аудита и сформировать список объектов (помещений, имущества и т.п.), которые надлежит охранять.

Определить физический и концептуальный периметры безопасности, внутри которого будет проводиться аудит. Физический периметр охватывает материальные объекты, подлежащие аудиту по безопасности. Это может быть здание, а может быть и комната. Концептуальный – то, что не поддается физическому измерению (компьютерные файлы, базы данных, телефонная, электронная и другие виды коммуникаций). При этом понятно, что все, что находится вне заранее определенной границы, аудитом не охватывается.

Продумать и создать список угроз отдельно для каждого из объектов аудита (компьютеры, сейфы, комната, цех, здание, территория). Это самый важный этап подготовки.

Определить, какие объекты наиболее уязвимы для проникновения извне.

Опираясь на список наиболее важных и уязвимых с точки зрения безопасности объектов охраны, сформулировать план защитных мер. При этом необходимо, чтобы на каждую потенциальную угрозу были проработаны и приняты разные меры защиты (например, установка эффективной системы видеонаблюдения и внедрение системы шифрования внутренней корреспонденции).

## **Быть готовым к ЧП на предприятии**

Чрезвычайные происшествия на предприятии, несущие угрозу сотрудникам, клиентам, местным жителям и экосреде, могут быть вызваны разными причинами – объективными или человеческим фактором. Обычно их нельзя заранее предупредить. Но быть готовым к ним необходимо.

Большинство западных компаний имеют специальные планы – на случай ЧП. Сначала создается группа по разработке такого плана. Эта группа изучает условия работы на предприятии (в организации), выделяет наиболее важные участки, оценивает потенциальные угрозы, определяют средства и возможности (в том числе человеческие) достойно справиться с ситуацией.

Естественно, конкретный план действий в условиях ЧП определяется спецификой предприятия, его местонахождением, климатическими и прочими условиями. Но есть минимальный набор предполагаемых средств и мер на случай ЧП, который, по мнению экспертов онлайн-журнала Industrial Security Service ([www.bestguards.com](http://www.bestguards.com)), должен включать:

Противопожарные средства (умение персонала с ними обращаться)

План эвакуации персонала с указанием конкретных маршрутов

Инструкции для тех, кто должен оставаться на рабочих местах во время общей

эвакуации, управлять рабочими процессами в период от возникновения ЧП до своей эвакуации

Инструкции для персонала после полной эвакуации

Обязанности облеченных соответствующими полномочиями сотрудников предприятия, которые должны принимать меры по ликвидации последствий ЧП, спасению персонала и оказанию медицинской помощи

Имена, должности, контактная информация о тех лицах в компании, которые отвечают за выполнение плана

Необходимо, чтобы принятый план действий в условиях ЧП был доведен до сведения всех сотрудников компании. Более того, желательно, чтобы он был обсужден в отделах предприятия/организации. План теряет всякий смысл, если сотрудники о нем не знают, не понимают, что должны делать при возникновении ЧП, если не проводятся учебные мероприятия, не вносятся в план коррективы, диктуемые обстановкой и временем. Реализация плана действий во время ЧП, отмечает в заключение упомянутое издание, не только защитит сотрудников предприятия, клиентов, помещения, но и поможет максимально сохранить работу компании.

## **Принтеры - уязвимое звено безопасности предприятия**

Когда речь заходит об охране предприятия, то о принтерах обычно не вспоминают. А напрасно. Принтеры должны входить в обязательный список возможных угроз безопасности бизнеса.

Принтеры могут быть носителями важной корпоративной информации, подчеркивает вице-президент Gartner Group Research Кен Вейлерстейн, - и нередко такая информация застревает в «памяти» принтера надолго после печати документа.

«Давно прошло время, когда принтеры представлялись не более чем «немой машиной», подчеркивает Микаел Ховард, менеджер по развитию международного бизнеса известной корпорации Hewlett-Packard. Современные принтеры обладают способностью запоминать и хранить отпечатанные материалы. Более того, наиболее совершенные модели приобретают характеристики компьютеров, взаимодействуя с корпоративными сетями и серверами. К тому же, продолжает Ховард, многие организации пренебрегают защитой своих сетей, редко меняют пароли принтеров, тем самым создавая благоприятные условия для атак хакеров. Очутившись в сети, хакер может поменять конфигурацию оперативной платы. В одном американском университете студенты, не выходя из общежития, преспокойно перехватили документы, отправленные для распечатки в принтер академического департамента университета, и ознакомились с материалами предстоящего им экзамена.

Другая слабость заключается в жестких дисках. Их легко украсть, прочесть хранимую информацию во время ремонта, в любой ситуации, когда принтер попадает в другие руки (например, передается в дар местной школе).

Определенную озабоченность вызывают многофункциональные принтеры, скажем, совмещенные с факсом – оставшиеся от времен, когда в Интернет заходили исключительно через телефонные кабели с помощью модемов. В федеральных агентствах США, например, категорически запрещено пользоваться такими принтерами.

Как защитить информацию, проходящую через принтер? Микаел Ховард советует регулярно, ежемесячно или лучше еженедельно чистить жесткие диски. Очень важно, чтобы менеджеры по закупкам внимательно знакомились с характеристиками принтеров, прежде чем их приобретать. Главное здесь в том, может ли компания извлекать и держать у себя жесткие диски перед ремонтом или очередным ТО.

Есть и другие способы обезопасить принтеры от кражи информации. В частности, шифрование данных во время передачи по корпоративным сетям. К этому прибегают в исключительных случаях.

(по материалам сайта [www.securitymanagement.com](http://www.securitymanagement.com), June 2008)

## Когда начальник читает вашу почту

Газета Wall Street Journal online (June 10, 2008) опубликовала результаты опроса, проведенного фирмой Proofpoint среди крупных американских компаний. Выяснилось, что почти каждая третья компания содержит в штате людей, в чьи функции входит контроль и анализ внешней электронной почты сотрудников. Конечно, замечает газета, надо делать поправку на специализацию Proofpoint (технологии по предотвращению информационных утечек) и, следовательно, ее заинтересованность в такого рода опросах.

Легче всего, замечает газета, обвинить американских бизнесменов - участников опроса - в паранойе. Но результаты исследования многое объясняют и оправдывают:

23% опрошенных заявили о фактах утечки конфиденциальной информации.

44% имеют основания подозревать, что служебная информация просачивается наружу через электронную почту.

34% крупных компаний отметили, что ловили сотрудников на использовании внутренней информации в неслужебной переписке.

Не удивительно, что в половине американских компаний наказывали сотрудников за нарушение внутренней политики в отношении e-mail. А в каждой четвертой за такие проступки увольняли.

При этом электронная почта – не единственный источник беспокойства. 21% опрошенных признали, что сталкивались с фактами размещения служебной информации на открытых веб-блогах (при этом 14% заявили, что эта информация касалась весьма чувствительных финансовых аспектов). 12% опрошенных сказали, что им пришлось расследовать случаи утечек по каналам онлайн-видео или аудио на таких сайтах как YouTube.

На публикацию Wall Street Journal online на сайте [blogs.wsj.com](http://blogs.wsj.com) пришли отклики и комментарии. Вот некоторые из них:

- «контроль за содержанием электронной переписки сотрудников помогает выявлять, предупреждать утечки служебной информации. Понимая, чем чреваты последствия для репутации компании, руководитель может эффективно минимизировать риски, повысить уровень безопасности своей организации» (Джим Келтон);

- «конечно, плохо, когда менеджеры следят за своими коллегами. Но поскольку злоупотребление информационной инфраструктурой компаний происходит регулярно, другого выхода нет. Нельзя же безнаказанно паразитировать на доверии начальства» (Джеф Виллиамс);

- «на рабочем месте для входа в электронную почту и Интернет в личных целях я использую собственный ноутбук и сотовую беспроводную карту. Конечно, это мне обходится в \$60 ежемесячно, зато я могу в Интернете делать все, что хочу, не опасаясь слежки» (анонимный автор).

## Когда двери вращаются...

### Часть 2

В предыдущем номере журнала мы схематично описали работу системы вращающихся дверей, которую приняла на вооружение служба безопасности одной крупной американской компании вместо традиционной технологии двухдверного шлюза («мантрапа») – последний требовал большого числа охранников, в час пик создавал толчею, давал сбои.

Хотя все, казалось, было просчитано и спланировано, при установке опытного образца в одном из 24 подъездов принадлежащих компании зданий выявились проблемы. В компании работает огромное число сотрудников. Неожиданная для них смена пропускного режима могла породить нервозность и бестолковщину, особенно в часы пик. Кроме того, надо было проверить, подойдут ли электронные пропуска (бэджики) к новым считывателям, учитывая, что многие сотрудники ранее ими вовсе не пользовались. Обнаружилось, что в компьютерной базе данных отмечены не все пропуска, что некоторые бэджики пришли в негодность. Прежде чем запускать новую систему контроля и управления допуском, было решено предоставить работникам компании возможность опробовать ее, заодно и проверить свои пропуска.

Для этого в нескольких подъездах были установлены специальные тестеры – считыватель и две лампочки, зеленая и красная. Кроме того, каждому работнику была вручена краткая инструкция, как пользоваться новым режимом:

Пропустить бэджик через считыватель.

Убедиться, что зажегся зеленый.

Встать на темный коврик между считывающим устройством и дверями.

Дверь начнет вращаться.

Было подсчитано, какое число людей будут проходить в разное время дня. Расчет показал, что 5 секунд достаточно на проход одного человека. Это

среднестатистический интервал включал также время на непредвиденные задержки (бэджик упал, его неправильно приложили к считывателю, и т.д.). В часы пик работали резервные двери. Практика показала, что утром и вечером небольшая очередь возникает, но не более чем на 10 минут. С этим вполне можно мириться.

Несмотря на тщательную подготовку, первые дни ознаменовались настоящим хаосом. Кто-то забыл свой пропуск дома, у кого-то бэджик неисправен, но, главное, многие не смогли сразу понять очередность действий.

Чтобы приноровиться, ушло три дня. На вторую неделю дело пошло еще лучше. Пропускная способность новой технологии СКУД оказалась высокой. Поскольку считыватели установлены по обе стороны дверей, одновременно ими пользоваться могут входящий и выходящий. Значительную часть времени двери вращаются практически безостановочно, позволяя уменьшить среднестатистическое время на проход до 2.5 секунд.

Рядом со считывающим устройством кроме зеленой и красной ламп в панель вмонтирована кнопка связи с постом контроля СКУД. Камеры слежения помогают контролировать работу системы. Дверной проем настолько узок, что позволяет проносить с собой только небольшой сверток, сумку или портфель. Для проноса громоздких вещей, например, оборудования, а также для гостей, не имеющих пропуска, равно как и для людей с ограниченными возможностями в каждом здании имеется отдельное лобби.

Внедрение системы вращающихся дверей позволило более чем вдвое, сократить персонал **охраны**, и одновременно повысить безопасность.

*В следующем номере журнала читайте, как данная система СКУД работает в аэропортах США.*

## **Ответственный за безопасность по этажу - зачем он нужен?**

На сайте [bizsecurity.about.com](http://bizsecurity.about.com) опубликован материал Райана Грума, озаглавленный "Floor Marshal" (то означает в переводе лицо, ответственное за безопасность на этаже здания). Автор провел: эксперимент: заходил в учреждения и офисы, садился за свободный рабочий стол и ждал, пока кто-нибудь не спросит, а что он, собственно говоря, здесь делает. Иногда ему удавалось провести таким образом целый рабочий день. Его вывод: нужна система ответственных за безопасность по каждому этажу из числа персонала фирмы (но не профессиональных охранников, обеспечивающих охрану по периметру здания!).

«Многие компании, - отмечает Грум, - слишком большие, чтобы все знали друг друга в лицо, но достаточно компактные, чтобы обратить внимание на празднующегося по офису незнакомца. А между тем, нахождение посторонних чревато кражами и даже угрозой здоровью и жизни сотрудников».

Для компании, которая размещается на нескольких этажах здания, он предлагает создать комитет ответственных за безопасность из числа сотрудников, который бы

собирался регулярно, не реже раза в месяц. В этот комитет должны входить ответственные по этажу, главный по безопасности компании, начальник охраны здания.

Ответственный по этажу – это работник, добровольно согласившийся взять на себя функции присматривать за посторонними в помещении. Желательно, чтобы у него был помощник (заместитель), особенно на случай отсутствия первого.

Всякий раз, когда ответственный замечает в помещении постороннее лицо, он должен подойти и спросить документы, разрешающие ему здесь находиться. Те, кто пришел по приглашению конкретного сотрудника, удостоверяются последним. Выдается пропуск, если таковой отсутствует. Если же постороннее лицо не может внятно объяснить и доказать, что он приглашен и кем приглашен, его немедленно выдворяют. В случае сопротивления немедленно вызывается охрана, а в некоторых случаях и полиция.

Такая система «добровольной охраны», уверяет Грум, «помогает обеспечивать безопасность сотрудников, компьютеров и их содержимого».

## **Выбираем фирму для установки и эксплуатации системы охраны**

В прошлом номере журнала мы уже говорили, что для многих небольших организаций нет возможности держать в штате охрану, тем более пользоваться услугами предприятий по охране. Выход – устанавливать системы **охраны** - сигнализации и защиты. Читатели ознакомились с советами американского специалиста, какие средства охраны и как выбирать. Сейчас речь пойдет о не менее важных вопросах – как выбирать фирму по охране, которая будет устанавливать системы охраны, предупреждения и защиты.

Прежде чем приглашать компании по установке средств охраны к себе, проверьте их профпригодность. Для начала поищите в Интернете возможные упоминания потенциальных партнеров. Изучите их сайт. Если там есть список клиентов, обязательно постарайтесь с кем-нибудь из них переговорить, еще лучше подъехать и осмотреть результаты работы **охраны** на месте. Если такого списка на сайте компании нет, попросите. Уверенная в себе фирма по охране не откажет и даже поможет установить контакт с их клиентами.

Если дело дошло до переговоров, то нелишне будет попросить разъяснений по следующим вопросам охраны:

- система охраны, которую вам предлагают, - стандартная или будет адаптирована к конкретным условиям помещения? Если ответ следует: «как всем», спросите, способна ли стандартная система охраны обеспечить надежную охрану вашего помещения. Если специалист по охране не уверен, лучше обратиться в другую компанию по охране или проконсультироваться у независимого эксперта.

- Как часто предлагаемая система охраны нуждается в текущем обслуживании (ремонте)?

Регулярная чистка контактов, подзарядка батарей и иная работа по ТО систем охраны необходима не только для того, чтобы в нужный момент сигнализация сработала, но и для предупреждения ложных сигналов. Неплохо поинтересоваться, готова ли фирма по охране проводить работы по обслуживанию и будет ли эта услуга включена в общую стоимость работ по охране или оплачиваться отдельно по каждому выполненному ТО.

- И, может быть, самый важный вопрос: сколько времени потребуется профессиональному вору, чтобы преодолеть защиту помещения после подачи тревожного сигнала? Если представители фирмы по охране не могут вам ответить на такой вопрос, то лучше поискать других специалистов.

*(по материалам периодического издания "Crime Prevention Fact Sheet", March, 2005)*

## **02-14 Охрана предприятия быстрого питания**

Сетевые рестораны быстрого питания, получающие все большее распространение в России, представляют собой специфический бизнес, который характеризуется круглосуточной работой, преобладанием молодежи среди клиентов, местонахождением – как правило, на оживленных городских перекрестках. Услуги быстрого питания удобны для клиентов, но и весьма уязвимы для криминала, потому что не редко пренебрегают охраной.

О проблеме обеспечения безопасности ресторанов быстрого питания рассуждает на сайте [www.crimedoctor.com](http://www.crimedoctor.com) Крис МакГои. Он изучал надежность охраны тысяч ресторанов быстрого питания в США, и в каждом случае владельцы и менеджеры были вынуждены соглашаться, когда им указывали на слабости и уязвимости охраны. В двух вещах они проявляют скептицизм и неуверенность – что делать для улучшения безопасности, и в какую сумму им это станет. Между тем, в большинстве штатов местные законы прямо обязывают их заботиться о безопасности и охране клиентов и персонала, возлагая на них ответственность за последствия ограблений и другие криминальных происшествий в случаях неадекватной охраны.

Что такое «адекватная охрана» в данном контексте? Это порог необходимой и разумной охраны, указывает автор, который напрямую зависит от того, где находится конкретный объект. Например, ресторан расположен в квартале, где рядом работают ночные бары и прочие увеселительные заведения. Или, напротив, вдали от населенных пунктов, вдоль междугородних трасс, что делает его особенно привлекательным для грабителей, когда нет охраны. Другой ресторан находится в месте, где часто встречаются враждующие группы подростков, и тоже нет охраны. И так далее...

В принципе для каждой сети ресторанов быстрого питания в США разработан стандарт защиты и охраны, который обязательно включает систему видеонаблюдения,

тревожные кнопки, надежные сейфы. Что касается дополнительных мер – они зависят от криминогенной ситуации. Если она достаточно высока, рекомендуется чаще проводить проверку надежности **охраны**. Обычно такие проверки, осуществляемые специалистами в области охранной деятельности, обнаруживают серьезные недочеты – неисправные замки, неработающие видеокамеры, мертвые системы звуковой сигнализации. Автор неоднократно сталкивался с явным пренебрежением владельцев и менеджеров к требованиям безопасности и охраны. В одних случаях проверки систем охраны вообще никогда не проводились. В других – просто сэкономили на охране клиентов и работников.

Особенно важно контролировать, чтобы персонал ресторанов в районах повышенного риска регулярно проходил обучение по вопросам безопасности и охраны. Естественно, серьезные требования должны предъявляться к приему на работу. Автор статьи утверждает, что огромное количество преступлений так или иначе связано с сомнительным прошлым собственных сотрудников.

## **«Конвергенция охраны. Управление рисками безопасности предприятия»**

*Dave Tyson, Security Convergence: Managing Enterprise Security Risk, 232 pages*

*Published by Elsevier/Butterworth-Heinemann, \$50*

Приобретение: [www.asisonline.org](http://www.asisonline.org)

«Эта книга станет открытием для всех профессионалов охранного дела, кто не занимался сравнительным изучением двух видов охраны – физической и цифровой», отмечает в рецензии на книгу Карим Веллани ([www.securitymanagement.com](http://www.securitymanagement.com), June 2008). Книга показывает, где сегодня находятся в своем развитии оба вида **охраны**, в каком направлении совершенствуются, и что особенно важно – как специалисты физической охраны должны готовиться к тому дню, когда эти системы сольются в единую структуру корпоративной безопасности.

Автор книги начинает с определения понятия «конвергенция» для специалистов физической охраны. Затем указывает на «культурные отличия» физической и цифровой видов охраны. Но не ограничивается выявлением различий, уделяя внимание и тому, что их сближает, объединяет перед лицом потенциальных угроз.

Далее рассматриваются технические достижения в индустрии физической охраны, как они благоприятствуют процессам конвергенции, каковы выгоды приносит конвергенция, включая объединение ресурсов и выстраивание единой вертикали службы **охраны**. Несколько разделов посвящены вопросам обучения сотрудников служб безопасности, новым веяниям и технологиям.

С первой до последней страницы автор книги убеждает читателей в преимуществах конвергенции и готовит их к этому.

# **Ох 02-16 Как в Америке выбирают охранное предприятие для обеспечения безопасности школ**

**В. Светозаров**

В конце июля агентство Ассошиэйтед Пресс распространило сообщение, что в муниципальном колледже американского города Финикс, штат Аризона, неизвестный открыл огонь, три человека ранены. По информации агентства, состояние двоих из пострадавших оценивается как критическое. Перестрелка произошла около 16.00 по местному времени.

США прочно занимают лидирующее в мире место по таким преступлениям, совершаемым в школах. Понятно, что проблема охраны школьных учебных заведений стоит в центре внимания властей, общественности и прессы. На охрану школ выделяются немалые средства. Бизнес по-своему реагирует на эту ситуацию. Огромное количество охранных компаний предлагают свои услуги в обеспечении безопасности учеников и преподавателей. При этом, как водится, на рынок охранных услуг для школ выходят и сомнительные фирмы, откуда-то появляются самозванные «эксперты по безопасности», которые, не обладая ни опытом, ни профессионализмом, спешат заработать на болевой проблеме американского общества.

«Берегитесь шарлатанов» - предупреждает Национальная ассоциация директоров средних школ США и предлагает развернутые рекомендации, как, по каким критериям отбирать охранное предприятие. Они могут быть полезными и в наших, российских условиях. Вот некоторые требования, опубликованные еще 9 лет назад в журнале The High School Magazine (vol. 6, No.7, May/June 1999):

Специализированный охранный опыт. Компания может занимать видное место в сфере охрannого бизнеса, но это еще не значит, что там есть специалисты по охране школ. Школьным администраторам не стоит обольщаться титулами и званиями тех, кто предлагает свои услуги. Смотрите на имеющийся практический опыт, навыки, приобретенные в достаточно специфической области обеспечения безопасности школьных учебных заведений.

Знание реалий. Исследования, теории и прочие науки необходимы для пополнения наших знаний о безопасности в школах. Но обладание этими знаниями еще не гарантия их успешного применения в жизни, на практике. Проверяйте, насколько фирмы, предлагающие услуги по охране, знают реальную среду, особенности школьной жизни.

Проверка квалификации, надежности, репутации фирмы. Изучая информацию, представленную фирмой (на сайте, в проспекте, в предложении услуги), не принимайте на веру заявления, например, о том, что фирма «имеет многолетний опыт охрannой деятельности». Добивайтесь конкретных данных, где, в какой области фирма приобрела практический опыт. Не стесняйтесь требовать список клиентов для контакта с ними. Проявляйте осторожность относительно т.н. «некоммерческих», «общественных», «исследовательских» организаций, предлагающих аналогичные услуги. Бывает, что такими ширмами пользуются вполне коммерческие фирмы, чтобы

прибавить внешней солидности, респектабельности, внушить доверие. Главный критерий – практика и опыт именно в этой сфере.

Проверка надежности специалистов, охранников. Необходимо убедиться, что предлагаемые вам специалисты (включая, охранников) все свое время и энергию отдадут делу охраны вашей школы, что для них это дело не второстепенное, не хобби, не что-то «нагрузочное» в дополнение к основным интересам и занятиям. Если специалисты позиционируют себя как «универсальные эксперты», знающие все, что относится к охранной деятельности, то это повод насторожиться – на самом деле очень немногие люди, действительно разбирающихся одинаково глубоко во всех аспектах этой отрасли индустрии.

Требования к охранникам в школе, изложенные в последнем абзаце, можно дополнить такими человеческими качествами как психологическая устойчивость, толерантность, коммуникабельность. Одно дело – охранять завод, имея дело с взрослыми людьми, другое – учебное учреждение, контактируя с детьми, подростками, молодежью. Увы, конфликты между охранниками и учениками (и, соответственно, администрацией школы) – не редкость в американских школах. Об одном таком инциденте, случившемся осенью прошлого года в обычной нью-йоркской школе, рассказывает онлайн-журнал The Moderate Voice ([www.themoderatevoice.com](http://www.themoderatevoice.com), October 14th, 2007, by Joe Gandelman, Editor-in-Chief).

Директор школы, Марк Федерман, был арестован полицией после того, как вступился за ученицу, задержанную охранниками школы. Школьница опоздала на уроки и охранники ее не пустили. Она попыталась прорваться силой и, по версии охранников, затеяла драку. На ее стороне вмешался директор. Результат: директор и двое охранников получили незначительные увечья. Директор арестован. Союз гражданских свобод Нью-Йорка и некоторые другие общественные организации выступили в поддержку администрации школы, заявляя, что данный случай подтверждает обеспокоенность директоров школ поведением охраны: «это школы, а не тюрьмы, необходимо остановить криминализацию молодежи».

В свою очередь, Союз охранников школьных учреждений Нью-Йорка (есть и такой!) через своего представителя опроверг обвинения. Продемонстрировав клочок волос, выданный школьницей из шевелюры охранника, он сказал следующее: «Служащих охраны несправедливо обвиняют в криминализации школ. Именно к ним и относятся как к преступникам».

Тема отношений охраны и администрации – одна из многих, обсуждаемых в Америке в контексте безопасности учебных учреждений. В следующем номере журнала мы расскажем о некоторых технологиях и технических средствах, используемых в охране американских школ.