

ОХРАНА ПРЕДПРИЯТИЯ

№1, 2008

Оглавление

Общие проблемы

Философия охранной деятельности

Rick Kaun, "Industrial Security"

Новые технологии, методологии

Конвергенция физической охраны и информзащиты предприятия

Экономика и финансы

Н.Миронов,

Формируем финансовый план СБ предприятия

Риски и угрозы

Ю. Козлов,

Личная безопасность руководителя - угрозы и риски

Системы контроля и управления допуском

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

Борьба с преступлениями среди персонала

Хищения на производстве - проблема и для Америки

Охрана малого предприятия

Выбираем средства защиты помещения

Профессиональное обучение

Профессионализм - не знания, а умение их применять

Профессиональная этика

Кодекс профессиональной этики Ассоциации индустрии безопасности Австралии (по материалам сайта www.asial.com.au)

Охрана предприятия за рубежом

Что заставляет американских бизнесменов раскошелиться на охрану предприятия?

Исследования

США: женщины увеличивают свое влияние в индустрии безопасности

Бум на мировых рынках охранного видеонаблюдения. Исследование американской маркетинговой компании

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

Философия охранной деятельности

Рик Каун, руководитель группы экспертов в американском охранном предприятии (корпорации) Matrikon, специалист в сфере управления рисками с акцентом на проблемы охраны предприятия, любезно дал разрешение на перепечатку некоторых фрагментов своей публикации на сайте упомянутой компании.

«Прежде чем приступить к осуществлению проекта по **охране** предприятия, необходимо сформулировать своего рода «философию безопасности», пишет автор. Каждый раз она будет звучать по-разному для каждой компании, каждой отдельно взятой отрасли, каждого региона. Но вместе с тем имеются и общие, базовые принципы, об охране о которых пойдет речь ниже.

1. Охрана предприятия – это серьезно и важно

Первый постулат достаточно простой. Он означает, что первые лица - владельцы компании, менеджеры и консультанты, продавцы и рекламщики, короче, все до последнего должны понимать, что поддержание на уровне безопасности предприятия в интересах всех и каждого. Это также важно, как и **охрана** труда. В большинстве случаев история предприятия – это история попыток повысить безопасность и охрану труда, объяснять персоналу, что и как надо делать, чтобы избежать травм и увечий. Каждый работник предприятия обязан иметь правильное представление о безопасности и охране труда. То же самое относится и к охране предприятия, к его безопасности. Суровый, но простой факт – даже самые лояльные работники предприятия объективно располагают возможностями нанести колоссальный ущерб компании – осознанно или нет. Другими словами, эффективность программы по охране предприятия напрямую зависит от осведомленности и подготовки всего персонала.

2. Охрана есть перманентный процесс

Многие организации обычно рассматривают программу по охране своего предприятия как проект, имеющий начало и конец, а также определенную стоимость. Такой подход может быть верным лишь в отношении какого-то отдельного компонента программы, но последняя в целом есть постоянный, непрерывный процесс. Это подтверждается хотя бы тем, что охранные технологии постоянно совершенствуются и требуют своевременной замены. К примеру, интернет-технологии, широко применяемые в охранной деятельности. То, что вчера было полезно и эффективно, сегодня обнаруживает бреши и требует более совершенной технологии. Система безопасности предприятия действенна только тогда, когда она отвечает самым современным требованиям охраны.

3. Охрана – дело каждого

Это главный постулат, на котором зиждется философия безопасности и охраны. Как упоминалось выше, самое слабое звено, откуда грозит наибольшая опасность – это персонал. Программы по безопасности, минимизации управленческих рисков, поддержанию конкурентноспособного бизнеса или планы реагирования на чрезвычайные ситуации регулярно требуют внесения тех или иных изменений в охрану. Важно разъяснять работникам предприятия, почему такие изменения происходят, почему к ним надо быть готовым. К сожалению, на практике очень часто действия по охране предприятия предпринимаются без учета подготовленности персонала, без четких планов обучения и переподготовки. В конечном счете, эти системы охраны живут или умирают в зависимости от того, как они воспринимаются и поддерживаются работниками предприятия.

4. Охрана – это баланс потребностей и возможностей

Последний и, возможно, самый важный постулат. Прежде чем начинать разработку и осуществление программ по безопасности, необходимо решить, какой уровень рисков приемлем для компании. Ведь любое нововведение в системе охраны требует затрат времени и средств. Это все надо просчитывать заранее. В конце концов, адекватность системы безопасности и охраны проверяется тем, насколько надежно она сопротивляется попыткам ее преодолеть, сколь быстро она восстанавливается, как хорошо охраняется, насколько мы сами готовы учиться и извлекать уроки.

Конвергенция физической охраны и информзащиты предприятия

О проблеме совмещения средств охраны и информационной защиты в единую систему безопасности предприятия и охраны говорят все последние годы. Интерес к этой проблеме вызван растущими угрозами скоординированной атаки на предприятие, когда попытки вывести из строя информационные средства контроля и управления сопровождаются действиями по преодолению систем физической охраны.

Плюсы конвергенции очевидны. Это и удешевление безопасности и охраны (управлять единой системой выгоднее, чем несколькими), и повышение уровня координации между всеми видами охраны (видеонаблюдение, физический контроль, безопасность

сетей, охрана и т.п.), и новые возможности для удаленного контроля и управления охраной из единого центра.

В теории все звучит хорошо. Реализовать конвергенцию практически – вещь сложная. И здесь могут пригодиться некоторые рекомендации специалиста.

Тони Лаполито, вице-президент IT компании VidSys, советует:

1. Делать все необходимое, чтобы первые лица компании реально осознавали потенциальные угрозы и поддерживали создание единой системы безопасности и охраны.
2. Не ломать, но сохранять существующую инфраструктуру безопасности и охраны, дополняя ее новыми технологиями, процессами и политиками.
3. Интегрировать систему видеонаблюдения с другими средствами охранной сигнализации (тревожные кнопки, видеоаналитика, сенсорные устройства, средства идентификации и пр.)
4. Совмещать цифровые и аналоговые электронные средства охраны. Замена аналоговых систем охраны на более современные цифровые требует не одного года и значительных средств. На переходный период, который может длиться и 5, и даже 10 лет (в зависимости от масштабов предприятия), важно добиваться максимального совмещения обеих систем.
5. Выбирать поставщика новых технологий среди компаний, с которыми уже имели успешный опыт в прошлом, которые хорошо изучили вашу инфраструктуру, а главное – знают «дорожную карту» перспективного развития компании.
6. Коррелировать информацию из всех источников. Отдельно взятая информация может ничего не говорить. Совмещенная с другой информацией – может сказать многое.
7. Использовать достижения в коммуникационных технологиях. Имеется в виду, в частности, интеграция систем охраны с мобильными телефонами, видеоконференциями, чатами, другими источниками получения и средствами передачи критически важной информации в нужный момент.

(по материалам сайта esj.com)

Формируем финансовый план СБ предприятия

Н.Миронов,

Одним из важных аспектов создания и совершенствования службы безопасности предприятия является обоснование его экономической целесообразности.

Для такой оценки абсолютно необходимо понимать, какие финансовые затраты будут

произведены на организацию СБ. Поскольку фактор времени является одним из решающих, важно понять как предстоящие затраты будут распределены во времени. Это особенно важно для небольших организаций, не обладающих серьезными финансовыми возможностями. Поэтапное развитие СБ в этом случае зависит от экономической эффективности бизнеса. Стремление руководителя предприятия к последней любой ценой, в том числе и за счет становления и совершенствования СБ, чревато серьезными негативными последствиями для всего бизнеса. Конечно, здесь возможны и компромиссные варианты. Например, страхование. Но, как известно, застраховаться на все случаи жизни при ведении хозяйственной деятельности в нашей стране невозможно.

Но и там, где есть необходимые средства для развития бизнеса, включая расходы на **охрану** предприятия, эти траты должны быть оправданы наличием угроз, степенью их вероятности, потенциальным ущербом.

Финансовый план СБ имеет две составляющие – переменную и постоянную.

Переменная составляющая включает расходы на обустройство помещений, приобретение оборудования, технических средств **охраны**, оружия (в том числе траты на их регистрацию), а также на программное обеспечение, информационные базы данных.

Постоянная составляющая связана с обслуживанием технических средств, обновлением информационных ресурсов, зарплатой, соцобеспечением и страхованием сотрудников СБ.

Ниже следует таблица расходов на организацию и развитие СБ, которая практически используется в торгово-производственной фирме «Заря».

ЭТАП		1	2	3	4	5
		1.12..2005	23.01.2006	01.02.2006	5.04.2006	1.06.2006
Дата начала и окончания этапа развития СБ		23.01.2006	01.02.2006	5.04.2006	1.06.2006	31.12.06
Расходы [т ы с . р у б .]		[Т ы с . р у б .]				
Транспорт	Переменные					300
	Постоянные		30	30	30	50
Связь	Переменные	5		60	45	18
	Постоянные	3		17	35	40
Вооружение	Переменные			45	50	55
	Постоянные					
Спецсредства	Переменные			12	12	6
	Постоянные					
Помещение для подразделения	Переменные			20	20	0
	Постоянные			3	6	6
Помещение для хранения оружия и спецсредств	Переменные					180
	Постоянные					6
Форма и снаряжение	Переменные			42	45	9
	Постоянные				3	3

Спортивно- тренировочная база	Переменные					
	Постоянные					30
Охранно-пожарный комплекс и СКУД	Переменные			450	450	
	Постоянные			9	18	18
Информационно-аналитические системы	Переменные					350
	Постоянные					10
Фонд заработной платы и расходы на страхование	Переменные			75	75	20
	Постоянные	30	40	330	650	800
Непредвиденные расходы	Переменные	10	10	50	50	90
	Постоянные	6	6	10	10	15

Для дальнейшей проработки финансового обеспечения службы безопасности предприятия следует составить помесячный план финансового обеспечения службы безопасности. В этом плане следует отразить суммарные расходы на реализацию мер технического и организационного характера, как по месяцам, так и по итогам года.

В нашем примере ожидаемая прибыль от реализации продукции торгово-производственной фирмы «Заря» на порядок превышает финансовые затраты на реорганизацию СБ. Это приемлемое соотношение. Тем не менее существует возможность оптимизации затрат по распределению их во времени.

Расходы на создание СБ имеют неравномерный характер. В нашем случае это связано с приобретением дорогостоящих технических средств. Например, пересмотреть сроки закупки дорогостоящего оборудования, либо приобрести его в лизинг или на условиях отсрочки платежей с определенным графиком погашения задолженностей

Следует отметить, что обычно на начальном этапе развития бизнеса основная часть прибыли от деятельности идет на развитие бизнеса или покрытие расходов, связанных с привлечением заемных средств и не каждому предприятию по силам активное развитие собственного подразделения безопасности. Тем не менее, как это отмечалось выше не стоит пренебрегать вопросами безопасности. Можно привлекать сторонние организации (ЧОП и т.п.) разумно подходя к выбору выполняемых ими функций. Это позволит сократить бюджет СБ на этапе становления бизнеса.

Об авторе: Миронов Николай Николаевич. Начиная трудовую карьеру на малом предприятии "Техномедика", а в последние годы работает на предприятии "Торговый дом "Горсия"", которое оказывает услуги для торговых и выставочных организаций по поставке и установке необходимого оборудования и мебели. В 2006 году закончил вечернее обучение в Институте Безопасности Бизнеса МЭИ (ТУ).

Личная безопасность руководителя - угрозы и риски

Ю. Козлов,

О компании «ХХХ». Ведет коммерческую деятельность с 1993 года. Основная деятельность – производство и реализация приборов бытового назначения. Основное производство продукции находится в Юго-восточной Азии. Ежегодный оборот продаж составляет порядка 11 500 000\$. Обеспечением комплексной безопасности компании занимается собственная служба безопасности, в задачу которой входит в основном экономическая безопасность, деловая разведка, защита коммерческой тайны, обеспечение защиты от внутренних угроз. В структуру Службы Безопасности входят: отдел защиты информации; отдел деловой разведки; отдел инкассации и охраны; оперативно – технический отдел.

В феврале 2007 года в результате разлада в компании, один из ее бывших руководителей привлек к сотрудничеству криминальные структуры и ряд недобросовестных сотрудников милиции. На региональных представителей оказывалось психологическое давление, звучали угрозы физической расправы. В марте 2007 года на руководителя компании предположительно готовилось покушение, в частности, было выявлено наружное наблюдение. Выяснилось, что люди, осуществляющие наблюдение, принадлежат к одной из столичных ОПГ.

Были проанализированы и систематизированы потенциальные угрозы. Они изложены в прилагаемой таблице, которая в принципе универсальна и может служить отправной точкой для анализа угроз в любой возможной ситуации.

№ п/п	Ситуации	Угрозы	Меры организационного характера	Меры технического характера
1	Отдых - дома	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица и близких ему людей - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица и близких ему людей - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - поджоги - шантаж, угрозы физического насилия или убийства - кража личного имущества Непредвиденного характера: - нежелательные посетители - пожар	- организация собственной Службы безопасности - организация подразделений охраны - разработка обязанностей, инструкций сотрудникам охраны - обеспечение охраны загородного дома - обеспечение подразделений охраны оружием, связью, спецсредствами, форменной одеждой - организация видеонаблюдения, средств сигнализации, пожаротушения - организация стрельб в тире, систематических занятий по подготовки сотрудников охраны	- регистрация собственной Службы безопасности - лицензирование сотрудников охраны - обустройство помещения для сотрудников охраны - закупка оружия, спецсредств, технических средств, форменной одежды сотрудникам охраны загородного дома - получение разрешения на использование радиочастоты - закупка и монтаж средств связи - устройство надежного забора по периметру, въездных ворот - просчет, закупка и установка оптимального количества камер видеонаблюдения, монитора, средств сигнализации и пожаротушения - заключение договора со спортивным залом, тиром

	- на территории РФ	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица и близких ему людей - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица и близких ему людей - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - шантаж, угрозы физического насилия или убийства - ограбление - кража личного имущества Непредвиденного характера: - нежелательные посетители - пожар - болезнь охраняемого лица - потеря документов, денег - случайные знакомства - мошенничество - стихийные бедствия	- организация собственной Службы безопасности - организация подразделения выездной охраны - разработка обязанностей, инструкций сотрудникам выездной охраны - обеспечение охраны места пребывания - обеспечение подразделения выездной охраны оружием, радио и мобильной связью, спецсредствами - техническими средствами - возможность наличия у охраны денег, для нужд охраняемого лица - организация стрельб в тире, систематических занятий по подготовки сотрудников охраны, в том числе медицинской	- регистрация собственной Службы безопасности - лицензирование сотрудников выездной охраны - закупка оружия, спецсредств, технических средств, одежды сотрудникам выездной охраны - получение разрешения на использование радиочастоты - закупка радиостанций - закупка мобильных телефонов, Sim карт с роумингом - обустройство помещения для сотрудников выездной охраны - наличие у сотрудников выездной охраны пластиковых денежных карт «Виза», «Мастеркарт» - наличие у сотрудников выездной охраны медицинской аптечки - заключение договора со спортивным залом, тиром
--	--------------------	---	--	---

	- за границей	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица и близких ему людей - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица и близких ему людей - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - шантаж, угрозы физического насилия или убийства - ограбление - кража личного имущества Непредвиденного характера: - нежелательные посетители - пожар - болезнь охраняемого лица - потеря документов, денег - случайные знакомства - мошенничество - стихийные бедствия	- организация собственной Службы безопасности - организация подразделения выездной охраны - разработка обязанностей, инструкций сотрудникам выездной охраны - обеспечение сотрудников выездной охраны заграничными паспортами - обеспечение охраны места пребывания - обеспечение подразделения выездной охраны мобильной связью, техническими средствами - возможность наличия у охраны денег, для нужд охраняемого лица - организация занятий по подготовки сотрудников охраны, в том числе медицинской	- регистрация собственной Службы безопасности - подбор и обучение сотрудников выездной охраны иностранным языкам - получение сотрудниками выездной охраны заграничных паспортов - закупка технических средств, одежды сотрудникам охраны - закупка мобильных телефонов, Sim карт с роумингом - обустройство помещения для сотрудников выездной охраны - наличие у сотрудников выездной охраны пластиковых денежных карт «Виза», «Мастеркарт» - наличие у сотрудников выездной охраны медицинской аптечки - заключение договора со спортивным залом
--	---------------	---	--	--

2	Работа (офис)	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица и близких ему людей - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - поджоги - шантаж, угрозы физического насилия или убийства - кража личного имущества Непредвиденного характера: - нежелательные посетители - посещение офиса сотрудниками правоохранительных органов - болезнь - пожар	- организация собственной Службы безопасности - организация подразделения охраны офиса - разработка обязанностей, инструкций сотрудникам охраны офиса - обеспечение охраны офиса - организация должного пропускного режима - обеспечение подразделения охраны офиса оружием, связью, спецсредствами, техническими средствами, форменной одеждой - организация видеонаблюдения, средств сигнализации, пожаротушения - организация стрельб в тире, систематических занятий по подготовки сотрудников охраны	- регистрация собственной Службы безопасности - лицензирование сотрудников охраны офиса - обустройство помещения для сотрудников охраны офиса - обустройство КХО - закупка оружия, спецсредств, технических средств, форменной одежды сотрудникам охраны офиса - получение разрешения на использование радиочастоты - закупка радиостанций - закупка и монтаж средств связи - устройство надежного входа в помещение офиса - просчет, закупка и установка оптимального количества камер видеонаблюдения, монитора, средств сигнализации и пожаротушения - заключение договора со спортивным залом, тиром
---	---------------	---	--	--

3	Передвижение охраняемого лица на авто-транспорте	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица - применение взрывчатых веществ в различной форме, различными методами - использование радиоактивных и химически вредных веществ - создание аварийной ситуации Непредвиденного характера: - авария - болезнь	- организация собственной Службы безопасности - организация подразделения выездной охраны - организация группы контрнаблюдения и предварительного осмотра - разработка обязанностей, инструкций сотрудникам выездной охраны и группы контрнаблюдения - обеспечение охраны в период передвижения - обеспечение подготовленным и оснащенным автотранспортом - обеспечение подразделения выездной охраны оружием, радио и мобильной связью, спецсредствами, техническими средствами - возможность наличия у охраны денег для нужд охраняемого лица - организация стрельб в тире, систематических занятий по подготовки сотрудников охраны, водителей, в том числе медицинской	- регистрация собственной Службы безопасности - закупка, бронирование, оснащение автотранспортных средств - лицензирование сотрудников выездной охраны - закупка оружия, спецсредств, технических средств, одежды сотрудникам выездной охраны, группы контрнаблюдения - получение разрешения на использование радиочастоты - закупка радиостанций - закупка мобильных телефонов, Sim карт с роумингом - наличие у сотрудников выездной охраны пластиковых денежных карт «Виза», «Мастеркарт» - наличие у сотрудников выездной охраны медицинской аптечки - заключение договора со спортивным залом, тиром, авто полигоном
	- поездом, самолетом	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица - похищение охраняемого лица - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - шантаж, угрозы физического насилия или убийства - ограбление - кража личного имущества Непредвиденного характера: - авария - пожар - болезнь охраняемого лица - потеря документов, денег - случайные знакомства - мошенничество - стихийные бедствия	- организация собственной Службы безопасности - организация подразделения выездной охраны - разработка обязанностей, инструкций сотрудникам выездной охраны - обеспечение охраны места передвижения - обеспечение подразделения выездной охраны оружием, радио и мобильной связью, спецсредствами, техническими средствами - возможность наличия у охраны денег для нужд охраняемого лица - организация систематических занятий по подготовки сотрудников охраны, в том числе медицинской	- регистрация собственной Службы безопасности - лицензирование сотрудников выездной охраны - закупка оружия, спецсредств, технических средств, одежды сотрудникам выездной охраны - получение разрешения на использование радиочастоты - закупка радиостанций - закупка мобильных телефонов, Sim карт с роумингом - наличие у сотрудников выездной охраны пластиковых денежных карт «Виза», «Мастеркарт» - наличие у сотрудников выездной охраны медицинской аптечки
4	Нахождение охраняемого лица в командировке	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - шантаж, угрозы физического насилия или убийства - ограбление - кража личного имущества Непредвиденного характера: - нежелательные посетители - пожар - болезнь охраняемого лица - потеря документов, денег - случайные знакомства - мошенничество - стихийные бедствия	- организация собственной Службы безопасности - организация подразделения выездной охраны - разработка обязанностей, инструкций сотрудникам выездной охраны - обеспечение охраны места пребывания - обеспечение подразделения выездной охраны оружием, радио и мобильной связью, спецсредствами, техническими средствами - возможность наличия у охраны денег для нужд охраняемого лица - организация стрельб в тире, систематических занятий по подготовке сотрудников охраны, в том числе медицинской	- регистрация собственной Службы безопасности - лицензирование сотрудников выездной охраны - закупка оружия, спецсредств, технических средств, одежды сотрудникам выездной охраны - получение разрешения на использование радиочастоты - закупка радиостанций - закупка мобильных телефонов, Sim карт с роумингом - обустройство помещения для сотрудников выездной охраны - наличие у сотрудников выездной охраны пластиковых денежных карт «Виза», «Мастеркарт» - наличие у сотрудников выездной охраны медицинской аптечки - заключение договора со спортивным залом, тиром
5	Деловые встречи вне офиса	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - шантаж, угрозы физического насилия или убийства - ограбление - кража личного имущества Непредвиденного характера: - мошенничество - болезнь	- организация собственной Службы безопасности - организация подразделения выездной охраны - организация группы контрнаблюдения и предварительного осмотра - разработка обязанностей, инструкций сотрудникам выездной охраны, группы контрнаблюдения - обеспечение охраны места пребывания - обеспечение подразделения выездной охраны оружием, радио и мобильной связью, спецсредствами, техническими средствами - возможность наличия у охраны денег для нужд охраняемого лица - организация стрельб в тире, систематических занятий по подготовки сотрудников охраны, группы контрнаблюдения, в том числе медицинской	- регистрация собственной Службы безопасности - лицензирование сотрудников выездной охраны - закупка оружия, спецсредств, технических средств, одежды сотрудникам выездной охраны и группы контрнаблюдения - получение разрешения на использование радиочастоты - закупка радиостанций - закупка мобильных телефонов, Sim карт с роумингом - наличие у сотрудников выездной охраны пластиковых денежных карт «Виза», «Мастеркарт» - наличие у сотрудников выездной охраны медицинской аптечки - заключение договора со спортивным залом, тиром

6	Посещение массовых мероприятий (стадионов, концертных залов и т.д.)	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - шантаж, угрозы физического насилия или убийства - ограбление - кража личного имущества Непредвиденного характера: - мошенничество - болезнь - массовые беспорядки - случайные встречи, Знакомства	- организация собственной Службы безопасности - организация подразделения выездной охраны - организация группы контрнаблюдения и предварительного осмотра - разработка обязанностей, инструкций сотрудникам выездной охраны, группы контрнаблюдения - обеспечение охраны места пребывания - обеспечение подразделения выездной охраны оружием, радио и мобильной связью, спецсредствами, техническими средствами - возможность наличия у охраны денег для нужд охраняемого лица - организация систематических занятий по подготовке сотрудников охраны, группы контрнаблюдения, в том числе медицинской	- регистрация собственной Службы безопасности - лицензирование сотрудников выездной охраны - закупка оружия, спецсредств, технических средств, одежды сотрудникам выездной охраны и группы контрнаблюдения - получение разрешения на использование радиочастоты - закупка радиостанций - закупка мобильных телефонов, Sim карт с роумингом - наличие у сотрудников выездной охраны пластиковых денежных карт «Виза», «Мастеркарт» - наличие у сотрудников выездной охраны медицинской аптечки
7	Посещение охраняемым лицом родственников, знакомых, выезд в гости	Умышленного характера: - вооруженное нападение с целью покушения на жизнь и здоровье охраняемого лица и близких ему людей - обстрел из автоматического оружия, в том числе снайпером - похищение охраняемого лица и близких ему людей - применение взрывчатых веществ в различной форме - отравление - использование радиоактивных и химически вредных веществ - шантаж, угрозы физического насилия или убийства - ограбление - кража личного имущества Непредвиденного характера: - нежелательные посетители - болезнь охраняемого лица - случайные знакомства	- организация собственной Службы безопасности - организация подразделения выездной охраны - организация группы контрнаблюдения и предварительного осмотра - разработка обязанностей, инструкций сотрудникам выездной охраны, группы контрнаблюдения - обеспечение охраны места пребывания - обеспечение подразделения выездной охраны и группы контрнаблюдения оружием, радио и мобильной связью, спецсредствами, техническими средствами - возможность наличия у охраны денег для нужд охраняемого лица - организация стрельб в тире, систематических занятий по подготовке сотрудников охраны, в том числе медицинской	- регистрация собственной Службы безопасности - лицензирование сотрудников выездной охраны - закупка оружия, спецсредств, технических средств, одежды сотрудникам выездной охраны - получение разрешения на использование радиочастоты - закупка радиостанций - закупка мобильных телефонов, Sim карт с роумингом - наличие у сотрудников выездной охраны пластиковых денежных карт «Виза», «Мастеркарт» - наличие у сотрудников выездной охраны медицинской аптечки - заключение договора со спортивным залом, тиром

Об авторе. Козлов Юрий Валерьевич, начальник Службы выездной охраны Холдинга безопасности "Магнум-А" www.magnum-a

Когда двери возвращаются...

Из опыта охраны зданий одной американской компании

Проблема контроля и управления доступом продолжает оставаться головной болью для служб охраны предприятий и помещений. Решается она разными способами. От простейшего – хорошо укрепленной двери до применения сложных электронных систем идентификации входящих.

В число наиболее эффективных систем контроля и управления доступом (СКУД) – шлюзовые технологии, предполагающие наличие как минимум двух дверей и устройства идентификации личности. Иногда такие системы называют «ловушки» (mantraps), особенно если попавший в междверное пространство человек не может выйти обратно без вмешательства охраны.

Шлюзовые технологии исправно служат на тысячах предприятий по всему миру, в том числе и в зданиях завода Texas Instrumentas в Далласе. Система здесь включает следующие элементы:

Видеонаблюдение (CCTV),

Голосовая связь с охранным центром,

Двойные двери с промежутком, вмещающим 12 человек,

Кнопка вызова охраны в случае необходимости,

Операторы, осуществляющие проверку персонала, пропусков.

Но, как отмечает автор статьи на сайте www.hortondoors.com Роберт Пирсон, после нескольких лет эксплуатации выяснилось, что мантрапы не слишком эффективны. Необходимо держать целую группу охранников-операторов, которые явно не справляются с одновременным контролем за всеми 24 входами в здания предприятия. Обнаружились проблемы с опознаванием через видеонаблюдение. Массовый приход на работу (и уход) создавал толчею в «ловушках», замедляя процесс контроля и проверки. Потерянный или украденный пропуск (бэджик) позволял его новому владельцу беспрепятственно проходить в здания.

Служба безопасности предприятия долго ломало голову, как усовершенствовать СКУД. Решили не тратить деньги на дополнительные дорогостоящие электронные устройства, а просто заменить мантрапы на вращающиеся двери (revolving doors).

В порядке эксперимента установили 2 вращающиеся двери в одном из зданий, где трафик сравнительно небольшой. Их автоматизировали. Двери начинали вращение только после успешной проверки пропуска (бэджика) специальным считывателем. Дверь имела четыре пропускные секции с расчетом на одного человека каждая.

Через год эксперимента было решено установить вращающиеся двери на всех 24 входах. Но прежде чем принять окончательное решение, нужно было ответить на следующие вопросы:

- Надо ли обязательно автоматизировать вращающиеся двери?
- Сколько секций должна иметь каждая дверь – три или четыре?
- Какова будет ширина прохода (секции)?
- Как должны располагаться секции в режиме закрытой (неработающей) двери?
- Какая аппаратура должна контролировать и предотвращать попытки «протиснуться вдвоем» на один пропуск?
- Где должен располагаться считыватель, с какими визуальными индикаторами?

Несмотря на тщательное планирование, не все удалось предусмотреть в деталях. Возникли непредвиденные осложнения и проблемы. Но о них - в следующем номере журнала.

Хищения на производстве - проблема и для Америки

Кражи на предприятиях собственными сотрудниками стоят США 40 миллиардов долларов и ежегодно растут на 15%. Таких преступлений – масса, но только немногие

расследуются или предаются огласке, отчасти по репутационным мотивам, отчасти из-за сложности изобличения преступника. Раньше топ-менеджмент компаний если и не мирился с хищениями, то, во всяком случае, не уделял им серьезного внимания.

Однако экономические проблемы, с которыми сегодня сталкивается Америка, заставляют предпринимателей более серьезно относиться к этой проблеме. Тем более, что кражи становятся все изощреннее, все чаще применяются компьютерные технологии. Ситуация вынуждает предпринимателей усиливать контроль внутри предприятий, требовать от своих сотрудников повышения бдительности на рабочих местах.

Компания Diversified Risk Management, оказывающая услуги по охране предприятия, рекомендует на своем сайте (diversifiedriskmanagement.com) некоторые общие предупредительные меры по минимизации краж. В частности, обращать внимание на признаки возможного воровства со стороны персонала. Такими признаками могут быть, как считают в этой компании:

- появление у работника больших наличных средств;
- новая дорогая одежда или драгоценности;
- новая дорогая машина;
- обеды в ресторанах;
- выражаемое недовольство зарплатой, начальством, условиями труда;
- не входящие в служебные обязанности контакты с водителями транспорта, торговцами.

Среди рекомендаций – совет следить за частными объявлениями в местной прессе (местных сетях Интернета), где вполне могут встретиться предложения о продаже краденной продукции.

Выбираем средства защиты помещения

Crime Prevention Fact Sheet. Reducing Criminal Opportunity. March, 2005

Для многих малых предприятий, небольших коммерческих организаций, таких как турбюро, редакция журнала, нет возможности держать в штате охранников или, тем более, нанимать охранные предприятия для защиты своих помещений, нередко представляющих 1-2 комнаты с отдельным выходом.

Таким предприятиям остается уповать на технические средства защиты, сигнализации, оповещения, охраны. Их сегодня предлагается множество. Прежде чем идти на рынок и выбирать, полезно ознакомиться с некоторыми советами специалиста, изложенными в публикации «Знакомимся с системами предупреждения и сигнализации, [охраны](#)» на сайте ...

Системы предупреждения, говорится в этой статье, предназначены для [охраны](#) от

злоумышленников, сигнализации в полицию, и вообще для вашего спокойствия в свободное от работы время.

Для начала надо понять, насколько уязвимо помещение для несанкционированного проникновения. Если входная дверь и окна слабы, то одни лишь системы сигнализации и охраны не спасут. Первым делом надо позаботиться о замене двери на металлическую или прочную деревянную, установив систему сигнализации и охраны (с использованием мобильного телефона, телефонной линии, радиоустройства). То же самое касается и окон. Прочные двери и окна совершенно необходимы для эффективной работы систем охраны.

Любая охранная стратегия включает в себе три D:

- Detering (отпугивание, т.е. уведомление потенциального вора, что помещение на охране).

- Detecting (обнаружение).

- Delaying (здесь: создание помех для быстрого проникновения в помещение).

Все три D воплощаются в системе двух дверей - внешней и внутренней. Внешняя дверь оснащена системой сигнализации (оповещения), а внутренняя должна быть особенно сильно укреплена и охраняться. Представим, что преступнику удалось справиться с первой, внешней дверью. Тотчас же срабатывает сигнализация и охрана, может быть, специальная сирена. Преступнику еще предстоит преодолеть запоры второй двери, на что требуется время. И он неизбежно сталкивается с дилеммой: что делать, охрана? Или рисковать, ожидая каждую секунду появления полиции, соседей, хозяина помещения, или убраться восвояси.

Еще одна важная вещь, которую надо принять во внимание - защита средств охраны. Последние достаточно уязвимы. Они зависят от работы телефона (телефонной линии), от питания. Поэтому надо подумать, что будет с техникой, если внезапно вырубится электричество и перестанет работать телефонная линия (например, в результате урагана или иного природного бедствия). Поэтому многие системы охраны снабжаются альтернативными источниками питания (батареи, аккумуляторы), которые позволяют продолжать работу в автономном режиме от нескольких часов до нескольких дней. Все это учитывается при выборе охранных устройств. Поставьте перед продавцом вопросы, такие, например, как: «на сколько часов работы без внешнего питания рассчитан предлагаемый продукт охраны?», «достаточен ли собственный ресурс для громкого звукового сигнала сирены и охраны?» и т.п.

Специалисты советуют по возможности сочетать аудио и визуальные средства охраны. Это наиболее эффективный путь не допустить преступника в помещение, с охраной. Даже если ему удастся вывести из строя систему аудиосигнализации, то риск засветиться на видеопленке наверняка отпугнет.

Профессионализм - не знания, а умение их применять

Ускоряющийся процесс глобализация мировой экономики сопровождается

изменениями в сфере криминала. Преступники используют все более изощренные методы и все более совершенные технические средства, представляющие возрастающую угрозу безопасности бизнеса. Правоохранительные государственные организации не в состоянии противостоять криминалу в бизнесе, не отвлекаясь при этом от своих прямых задач и функций по поддержанию общественного порядка. Именно частные охранные предприятия обладают наилучшими возможностями удовлетворить потребности бизнеса и людей в защите от криминала. Также все более очевидно значение профессиональной подготовки охранников с учетом быстро развивающихся инновационных технологий, новых коммуникаций и, как уже говорилось, «возрастающей квалификацией криминальных групп».

Вопросам подготовки и переподготовки работников охранных предприятий и служб безопасности посвящена публикация в журнале The Security Online (www.thesecurityonline.com). Ее автор, доктор Хоук, считает конечной целью системы подготовки «изменение отношения и поведения в нужном направлении как тренеров, так и тех, кого они тренируют».

Профессиональный уровень охранников, пишет он, особенно в странах с развивающейся экономикой, всегда отстает от практики и требований времени. Поэтому «курс по ориентации» составляет важную часть профессиональной карьеры охранника. При этом сами преподаватели (тренеры) должны постоянно учиться, чтобы соответствовать постоянно возникающим новым требованиям времени.

Охранная деятельность сродни любой другой, но с одним важным отличием – она требует скрупулезного соблюдения законодательства. Профессия охранника сопряжена с риском балансирования на грани дозволенного, поэтому первоочередная задача профессиональной подготовки – внушить понимание, что достигать поставленных целей можно и следует исключительно на основе принципа «закон и порядок».

Среди других знаний и квалификаций, приобретаемых во время подготовки и переподготовки:

- Понимание, что профессионализм выражается не столько в знании, сколько в умении их применять на практике;
- приверженность дисциплине в выполнении служебных обязанностей;
- умение действовать самостоятельно и инициативно;
- чувствовать моральную ответственность за общий успех, работать в команде;
- понимать, что нужно клиенту и максимально соответствовать его ожиданиям;
- демонстрировать отличную коммуникабельность – дипломатично разрешать сложные ситуации с клиентами, сохраняя лояльность, дружественный настрой, внушая им уверенность;
- ощущать гордость за свою работу, за обеспечение безопасности клиента и его бизнеса;
- проявлять позитивное отношение к возникающим проблемам, сохраняя спокойствие, хладнокровие, выдержку;

- вести правильный образ жизни, как на работе, так и вне ее, поддерживая на должном уровне профессиональную готовность – интеллектуальную, социальную, психологическую и физическую.

Кодекс профессиональной этики Ассоциации индустрии безопасности Австралии

По материалам сайта www.asial.com.au

Ассоциация индустрии безопасности Австралии (Australian Security Industry Association Limited – ASIAL) основана в 1969 году. Представляя поначалу небольшую группу охранных предприятий, ассоциация сегодня объединяет компании, занимающие 85% рынка безопасности в этой стране. Этот рынок развивается динамично. Он приносит ежегодный доход 4.5 миллиарда долларов США и обеспечивает занятость 150 тысяч человек, что для малонаселенной страны совсем неплохо.

В Ассоциации состоят как корпоративные, так и индивидуальные (менеджеры, оперативники) члены. В Ассоциации также состоят некоторые крупные потребители услуг безопасности.

Необходимым условием для принятия в члены Ассоциации является согласие с Кодексом профессиональной этики (Code of Professional Conduct), который провозглашает следующие принципы и требования:

- Вести профессиональную деятельность в соответствии с общественными интересами.
- Проявлять порядочность и честность в отношении клиентов или сотрудников, как бывших, так и настоящих, со своими коллегами и в целом с людьми.
- Не распространять заведомо лживую информацию в любом ее виде, не скрывать правду и факты. Придерживаться правды, точности и хорошего вкуса в рекламных кампаниях.
- Избегать конфликта интересов, за исключением случаев, когда получено согласие всех затронутых сторон при условии их полного информирования.
- Держаться в стороне от компаний, ведущих нелегальный или неэтичный бизнес.
- Не наносить умышленный ущерб профессиональной репутации и делу других компаний.
- Если член Ассоциации обнаружит, что другой член организации использует нарушающие этические нормы методы, он обязан сообщить об этом в Ассоциацию.

- Поднимать профессиональный уровень и знания путем обмена информацией и опытом с другими членами Ассоциации, использования достигнутой квалификации в интересах других.
- Не злоупотреблять членством в Ассоциации вне установленных Ассоциацией целей, правил и политики.
- Сотрудничать с коллегами в развитии и укреплении принципов, декларируемых данным Кодексом.

Кодекс профессиональной этики Ассоциации индустрии безопасности Австралии

По материалам сайта www.asial.com.au

Ассоциация индустрии безопасности Австралии (Australian Security Industry Association Limited – ASIAL) основана в 1969 году. Представляя поначалу небольшую группу охранных предприятий, ассоциация сегодня объединяет компании, занимающие 85% рынка безопасности в этой стране. Этот рынок развивается динамично. Он приносит ежегодный доход 4.5 миллиарда долларов США и обеспечивает занятость 150 тысяч человек, что для малонаселенной страны совсем неплохо.

В Ассоциации состоят как корпоративные, так и индивидуальные (менеджеры, оперативники) члены. В Ассоциации также состоят некоторые крупные потребители услуг безопасности.

Необходимым условием для принятия в члены Ассоциации является согласие с Кодексом профессиональной этики (Code of Professional Conduct), который провозглашает следующие принципы и требования:

- Вести профессиональную деятельность в соответствии с общественными интересами.
- Проявлять порядочность и честность в отношении клиентов или сотрудников, как бывших, так и настоящих, со своими коллегами и в целом с людьми.
- Не распространять заведомо лживую информацию в любом ее виде, не скрывать правду и факты. Придерживаться правды, точности и хорошего вкуса в рекламных кампаниях.
- Избегать конфликта интересов, за исключением случаев, когда получено согласие всех затронутых сторон при условии их полного информирования.
- Держаться в стороне от компаний, ведущих нелегальный или неэтичный бизнес.
- Не наносить умышленный ущерб профессиональной репутации и делу других компаний.
- Если член Ассоциации обнаружит, что другой член организации использует

нарушающие этические нормы методы, он обязан сообщить об этом в Ассоциацию.

- Поднимать профессиональный уровень и знания путем обмена информацией и опытом с другими членами Ассоциации, использования достигнутой квалификации в интересах других.
- Не злоупотреблять членством в Ассоциации вне установленных Ассоциацией целей, правил и политики.
- Сотрудничать с коллегами в развитии и укреплении принципов, декларируемых данным Кодексом.

Что заставляет американских бизнесменов раскошелиться на охрану предприятия?

Более 200 миллиардов долларов в год тратят американские предприниматели на охрану своих предприятий. Эти данные приводятся в исследовании, проведенном журналом "The Security Magazine" в конце 2006 года. Эта сумма не включает расходы специализированных организаций, профессионально занимающихся вопросами безопасности и охраны бизнеса, равно как и государственную поддержку со стороны Министерства внутренних дел США.

Еще 10 лет назад большинство компаний не выделяли **охрану** как приоритетное направление своей деятельности. Ситуация поменялась после 11 сентября 2001 года. Вопросы безопасности и охраны бизнеса выдвинулись на первый план и расходы по этой статье бюджета резко возросли. Что в первую очередь заставляет американских предпринимателей раскошелиться на безопасность и охрану? Эксперты журнала выделяют основные факторы:

1. Защита материальной и интеллектуальной собственности.
2. Репутация/бренд.
3. Защита людей (персонала, клиентов).
4. Законодательство, требования властей.

Подмечена интересная, новая для Америки тенденция: все чаще предприниматели включают охрану как составную часть бизнес-проектов, и соответственно интегрируют расходы на безопасность в общие статьи бюджета. Например, **охрана** может функционально рассматриваться (и осуществляться) как часть экологической охраны в энергетических компаниях, или как одна из функций по обеспечению безопасности пациентов в клиниках и больницах.

Деньги, вкладываемые в безопасность бизнеса, учитываются при планировании следующих бюджетов:

- инвестиции в новые проекты;
- охрана труда (программы по обучению персонала и его защите);

- контроль качества продукции;
- охрана авторских прав и интеллектуальной собственности;
- офис-менеджмент (сюда обычно включают деньги на обеспечение противопожарной безопасности).

США: женщины увеличивают свое влияние в индустрии безопасности

США известны мощными феминистскими движениями, которым удалось многого добиться в уравнивании фактических прав женщин с мужчинами. Женщины играют все большую роль в политике и бизнесе. Но еще остается немало сфер общественной деятельности, которые по традиции считаются «мужскими». К ним относится и индустрия безопасности.

Гендерная проблема хорошо просматривается на примере выставок и форумов, проводимых в России и за рубежом национальными и международными организациями и ассоциациями в области охранной деятельности, в целом безопасности бизнеса. Женщины преобладают среди персонала, организующего и обслуживающего такие мероприятия. Их можно встретить у стендов компаний, распространяющих рекламные материалы, проспекты и брошюры. Но совещания, конференции, круглые столы в более узком, профессиональном составе фактически представляют собой «собрание мужского клуба». Так сложилось исторически. США здесь – не исключение. И все же в Америке, как показывает проведенное недавно исследование на эту тему, женщины начинают проникать на руководящие посты в этой, традиционно закрытой в прошлом для них области деятельности.

В марте 2008 года американская компания Security Sales & Integration опубликовала на сайте www.securitysales.com статью своего сотрудника, в прошлом известного журналиста Роднея Боша «Пробивая стеклянную стену: женщины в индустрии безопасности». Публикация основана на исследовании с участием многочисленных представителей разных сегментов индустрии безопасности. Это было не первое подобное исследование, проведенное SSI. Последний раз проблема рассматривалась в 2005 году и было установлено, что женщины в индустрии безопасности составляли тогда всего 5% от общего числа занятых в среднем и высшем эшелонах менеджмента. Сравнение полученных в этом году результатов с теми, трехлетней давности, показывают определенный прогресс. Число женщин достигло 8%. Прирост за три года – 40%.

Исследование опиралось на членские списки (директории) крупнейших организаций в индустрии безопасности США: Security Industry Association (SIA), American Society for Industrial Security (ASIS), National Burglar and Fire Alarm Association (NBFAA), Central Station Alarm Association (CSAA). Изучались списки владельцев компаний, входящих в эти организации, высшего и среднего звена управленцев.

При этом отмечено, что женщин практически не видно среди руководителей охранных предприятий, организаций, имеющих дело с системами охраны и сигнализации. В то же время немало женщин руководят относительно небольшими, посредническими,

торговыми фирмами, действующими в сфере промышленной безопасности. Это прежде всего касается семейных компаний, где мужчина, как правило, инженер, технический специалист, занимающийся установкой и обслуживанием систем охраны, видеонаблюдения, а его жена – фактический руководитель фирмы, организатор. Хотя формально мужчины обычно возглавляют (по документам) семейные фирмы.

Ситуация немного начинает меняться и в более крупных компаниях. Шендон Харбор, не так давно выбранная президентом фирмы SDA Security в городе Сан-Диего, говорит, что «ее вдохновляет пример других женщин, достигших больших высот в индустрии безопасности». Она приводит имена Нэнси Чизхольм, вице-президента ADT Security Services, Ивонны Хао, вице-президента по Северной Америке компании ADI, Пэм Петров, вице-президента Vector Security,.....

Многие участники исследования сходятся во мнении, что слабое присутствие женщин на руководящих постах в охранных предприятиях не в пользу развития этой индустрии. Как заметила одна из опрошенных в ходе исследования, «к сожалению, возможности привлечения женщин к управлению, особенно к обсуждению и выработке свежих идей и инициатив, сегодня весьма ограничены. И этот наносит ущерб индустрии безопасности».

Бум на мировых рынках охранного видеонаблюдения

Исследование американской маркетинговой компании

Американская маркетинговая компания ABI Research специализируется на изучении влияния новых технологий на мировые рынки. Одно из последних исследований компании посвящено системам видеонаблюдения.

На основе полученных данных аналитики вывели прогноз: мировые продажи оборудования для видеонаблюдения в ближайшие 6 лет возрастут втрое, достигнув почти 50 млрд.долларов в 2013 году (www.securityinfowatch.com). Имеются в виду камеры, компьютеры, кабели и т.п., а также затраты труда на установку и обслуживание.

Вице-президент компании Стан Чат прокомментировал: «Мы находимся на пике крупных изменений, происходящих на рынке охранного наблюдения. Происходит переход от аналоговых к цифровым технологиям. Как говорится, «волна поднимает все лодки». В результате умножаются возможности для продавцов и расширяется выбор охраны для пользователей».

В ходе исследования его авторы отметили, что сегодня слова «**охрана**», «безопасность» у всех на устах. Видеонаблюдение пользуется спросом не только у охранных предприятий и служб безопасности и охраны. Оно находит широкое применение в вертикальных рыночных структурах, таких как образование, розничные сети, транспорт, финансы, охрана. Причем не обязательно речь идет об **охране**. К примеру, камеры слежения и технологии распознавания, расположенные в магазинах, позволяют анализировать поведение посетителей, их мимику, реакцию на предлагаемые товары....

Исследование показало, что Европа сегодня – наиболее насыщена системами охранного видеонаблюдения. Только Великобритания с ее более чем 4 миллионами камер слежения охраны представляет собой общество, подвергаемое самому мощному в мире мониторингу.

Второе и третье место по емкости занимают рынки Северной Америки и Китая. Последний особенно интенсивно развивается в виду приближающейся летней Олимпиады.

Аналитики ABI Research полагают, что хотя цифровые технологии видеонаблюдения обладают неоспоримыми преимуществами, многие из традиционных пользователей и реселлеров чувствуют себя не вполне комфортно с новыми технологиями охраны. А потому, следует вывод, возрастающее значение приобретает профессиональная переподготовка тех и других.