www.securityinfowatch.ru
№8 октябрь 2013

БЕЗОПАСНОСТЬ

информационное обозрение

Тема номера

Кадровая безопасность компании

18+

БЕЗОПАСНОСТЬ:
информационное обозрение
№ 8 октябрь 2013 г.

Учредитель
ООО «Центр Компьютерного Моделирования»

Генеральный директор
Баранов А.В
a.baranov@csc.ru

Исполнительный директор
Рязанкина Н.И.
n.ryazankina@csc.ru

Главный редактор
Соколова А.Н.
a.sokolova@csc.ru

Дизайн и верстка
Летина А.М.
a.letina@csc.ru

Фотограф
Летина А.М.
a.letina@csc.ru

Корректор
Анохина Т.Н.

Отдел рекламы
Криницын П.С.
p.krinitsyn@csc.ru

Адрес редакции
109316, Москва, Волгоградский пр-т, 47
Телефон +7 926 011 6754

Мнение авторов не всегда отражает точку зрения редакции.

За содержание рекламных публикаций и объявлений редакция ответственности не несет.

Все права на материалы, опубликованные в издании, принадлежат журналу «Безопасность: Информационное обозрение».

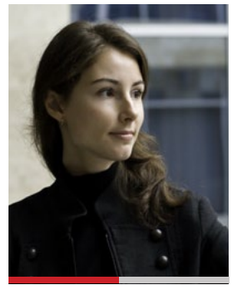
Любое использование материалов журнала допускается только с письменного разрешения редакции и со ссылкой на журнал.

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Свидетельство о регистрации
Эл № ФС77-48486 от 31 января 2012 года.

Учредитель - ООО «Центр Компьютерного Моделирования».
Издатель - ООО «Центр Компьютерного Моделирования».

От редакции



Осень – горячая пора подбора кадров

Осень – период деловой активности. Время важных встреч и решений, демонстрации собственных достижений, подбора нового персонала. Неслучайно большое число профильных мероприятий традиционно проходят именно осенью. «InfoSecurity Russia» и «Interpolitex» в Москве, «ИнфоБЕРЕГ-2013» в Сочи, «Комплексная безопасность» в Ижевске, «Охрана и безопасность» в Челябинске… Разные города России готовятся принимать экспертов и представителей бизнеса, решающих вопросы обеспечения безопасности на предприятии. А мы снова готовимся держать руку на пульсе событий и рассказывать вам о самых важных тенденциях в мире безопасности.

Широкая и многогранная тема кадровой безопасности в компании вполне заслуженно стала одной из ключевых в нашем журнале. И это, на мой взгляд, правильно: большинство руководителей и специалистов, отвечающих за безопасность на предприятии, полагают, что кадровая безопасность – центральная часть любой системы, которую организация формирует для своей защиты.

Среди проблем, рассмотренных нашими авторами и героями, такие важные проблемы, как правила построения кадровой и информационной безопасности компании, выявление рисков корпоративного мошенничества, подбор частного охранного предприятия. Последняя тема представляется одной из самых актуальных, ведь безопасность любого объекта начинается с защиты его периметра, а первое впечатление об организации во многом складывается благодаря охране, встречающей посетителей на проходной.

Адель Соколова

Кадровая безопасность компании: правила построения.

Moscow Business School
Leadership Energy

подробная информация
по тел. +7 (495) 646-75-17
на сайтах: www.mbs-seminar.ru, www.mba.ru

Бизнес-образование, позволяющее всегда быть на шаг впереди!

Семинары, тренинги и программы MBA для специалистов и руководителей, стремящихся к профессионализму в своей отрасли.

НОВОСТИ

Воровство и грабеж вышли из моды

Число криминальных преступлений в Великобритании в 2012 г. снизилось на 9% и достигло самого низкого уровня с 1981 г. Это связано с тем, что большинство преступлений сегодня совершаются в Интернете, ставшем куда более привлекательной мишенью для злоумышленников, чем темные улицы и иные небезопасные места, пишет газета «Daily Mail».

По сообщениям полиции, современные преступники реже идут на разбой, вооруженное нападение и т.п., зато с легкостью берутся за схемы мошенничества с кредитными картами, организацию фиктивных аукционов онлайн и афер, связанных со знакомствами в сети Интернет. Существуют опасения, что официальные данные недостаточно четко отражают реальную обстановку, связанную с виртуальной преступностью, поскольку значительная часть подобных махинаций нигде не документируется. Люди, столкнувшиеся с интернет-мошенничеством, далеко не всегда обращаются за помощью в официальные службы.

Согласно статистике ежедневно около 3 британцев (примерно 1 212 человек в год) становятся жертвами преступлений, связанных с сайтами знакомств. На них злоумышленники создают себе аккаунты для того, чтобы завести дружбу с состоятельными людьми, входят к ним в доверие, а затем сообщают своим френдам вымышленную причину, по которой им срочно требуется собрать крупную сумму денег. Получив от пользователей средства, аферисты исчезают. Жулики, орудующие за рубежом, могут попросить своих друзей-англичан перевести на их счет сумму для покупки билета на самолет до Великобритании. Однако они никогда не приезжают к своим знакомым и возлюбленным, найденным в интернете.

Еще одним способом обмана пользователей является проведение аукционов онлайн, а также продажа через интернет товаров по заниженным ценам. В минувшем году было зарегистрировано 22 694 подобных преступления. Для сравнения стоит отметить, что жертвами хакеров и вирусных атак стали 11 048 пользователей. Примерно столько же человек пострадали от преступников, работающих с пластиковыми картами.

Роскомнадзор обнародовал утечки данных в 2012 году

Роскомнадзор сообщает о росте административных правонарушений в сфере защиты персональных данных. По сведениям ведомства, за минувший год было составлено 5359 соответствующих протоколов, в то время как в 2011 г. – 4901, а в 2010 г. – 2996. Подробная информация появилась в отчете о деятельности организации в 2012 г. в качестве Уполномоченного органа по защите прав субъектов персональных данных в Российской Федерации.

«Мировыми судьями по результатам рассмотрения 4786 направленных материалов были приняты постановления о привлечении операторов к административной ответственности в форме штрафа на общую сумму 8 млн 680 тыс. 150 рублей», – отмечается в отчете Роскомнадзора. Известно, что из всех инцидентов с персональными данными только 62% относятся непосредственно к утечкам, связанным с несоблюдением операторами требований по обеспечению конфиденциальности и безопасности. Остальные случаи утечек связаны с передачей персональных данных без соответствующего согласия людей. В качестве примера можно привести несогласованную передачу данных коллекторам для взыскания задолженности.

«В большинстве своем факты утечек были связаны с несанкционированным распространением персональной информации, содержащейся на бумажных носителях, допущенным, в том числе учреждениями здравоохранения, осуществляющими обработку специальных категорий персональных данных», – говорится в материалах ведомства. В числе положительных тенденций эксперты Роскомнадзора отмечают рост гражданской активности среди населения в вопросах защиты персональных данных.

Угроза видеонаблюдению: «противоохранная» одежда

На рынке верхней одежды появились товары, позволяющие нарушителям быть незаметными для видеокамер. Одним из первых создателей так называемой стелс-одежды стал художник и профессор дизайна нью-йоркской Школы визуальных искусств Адам Харви. Его коллекция одежды StealthWear словно создана для того, чтобы подразнить современное общество, находящееся под наблюдением десятков тысяч видеокамер.

Для создания «противоохранной» одежды Харви использовал отражающие металлизированные ткани. Из них дизайнер изготовил куртки и плащи с капюшонами вроде тех, что используются пожарными, призванными свести к минимуму теплоизлучение человеческого тела. Подобная амуниция способна сделать человека невидимым для дронов, использующих тепловизоры для отслеживания перемещений граждан на открытых пространствах.

Пока новинки от Харви еще не прошли серьезных испытаний экспертами в области охраны и разведывательными структурами. Однако сам дизайнер убежден, что в современном мире, в условиях тотальной слежки за гражданами, подобный «камуфляж» будет весьма востребованным.

Большинство мобильных «зловредов» предназначены для Android

За минувший год число вредоносных приложений для мобильных операционных систем выросло на 614% – до 276 259 штук. При этом 92% программ предназначены для проникновения в устройства, работающие на базе ОС Android. Эксперты отмечают, что большинство опасных приложений распространяются через неофициальные магазины и направлены на получение мошенниками мгновенной прибыли. Серьезная угроза по-прежнему висит над корпоративными сетями, на которые осуществляют целевые атаки посредством ботнетов.

По данным исследования Mobile Threats Report, за последние 3 года количество вредоносных программ для мобильной ОС Android выросло с ошеломляющей скоростью. Авторы работы из компании Juniper Networks отмечают, что если в 2010 г. доля вредоносов, ориентированных на данную операционную систему, составляла 24%, то в 2012 г. она увеличилась до 47%, а к марту 2013 г. уже достигла 92%. «Разработчики вредоносных программ осознали широкие возможности того, что Android лидирует на рынке мобильных операционных систем», – заключают эксперты.

Три из пяти всех сторонних магазинов приложений для Android создавались как китайские и российские площадки, отмечают в Juniper Networks. Именно они служат для распространения вредоносного ПО. 73% таких программ составляют «лжеустановщики» и SMS-трояны, предназначенные для несанкционированной отсылки SMS с пораженных мобильных устройств на дорогостоящие платные номера. Каждая успешная атака может принести злоумышленнику прибыль до $10.

Аэропорты США хотят упростить досмотр пассажиров

Администрация транспортной безопасности США (TSA) стремится снизить число факторов, мешающих комфортному перемещению путешественников пишет «The New York Times». Так, недавно было объявлено о расширении списка граждан, имеющих право пользоваться программой TSA PreCheck. Запущенная в 2011 г. PreCheck («Предпроверка») была разработана для ускорения процесса досмотра пассажиров, заранее предоставивших о себе максимально полные сведения.

Ожидается, что в скором времени проходить процедуру проверки заблаговременно смогут все граждане США. Для этого им будет необходимо оставить онлайн-заявку на сайте, пройти предварительную проверку, предоставить свои отпечатки пальцев и заплатить 85 долл. Повторная процедура будет проводиться только через 5 лет. Граждане, воспользовавшиеся программой PreCheck, смогут проходить контроль в аэропорту по упрощенной системе – не снимать обувь и ремни, перевозить жидкости. Эксперты полагают, что облегчение процедуры прохождения контроля в аэропорту никак не снизит уровень обеспечения безопасности пассажиров.

Большинство специалистов сходятся во мнении, что изматывающие процедуры предполетного контроля отнюдь не гарантируют безопасность пассажиров. Например, одним из наиболее действенных нововведений после трагедии 11 сентября стало укрепление дверей в кабину пилота – это никак не отразилось на скорости перемещения путешественников в аэропорту, зато сделало невозможным угон самолета.

СОБЫТИЯ

Всероссийская специализированная выставка 5 ЛЕТ
Комплексная безопасность

1. V Всероссийская специализированная выставка «Комплексная безопасность», 18–20 сентября 2013 г.

Место проведения: : Россия, Удмуртская республика, г. Ижевск, ул. Кооперативная, 9.
Сайт: www.vcudmurtia.ru/events/safe

VВсероссийская специализированная выставка «Комплексная безопасность» в Ижевске организуется пятый раз. С 2009 г. в выставке приняли участие 258 предприятий из 21 региона России, было проведено 46 деловых мероприятий. Ежегодную ижевскую выставку «Комплексная безопасность» отличает солидный состав участников, среди которых ведущие предприятия отрасли.

Ежегодно выставку посещают представители федеральных и республиканских органов власти, местного самоуправления, социальных структур, образовательных и лечебных учреждений, руководители промышленных, монтажных и многих других предприятий республики. Среди почетных гостей выставки 2012 года были Президент Удмуртской Республики А.А. Волков, заместитель министра РФ делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий А.П. Чуприян, руководитель Приволжского регионального центра МЧС России И.В. Паньшин, директор департамента промышленности обычных вооружений, боеприпасов и спецхимии Министерства промышленности и торговли РФ А.В. Потапов. Впервые выставку посетили начальники Главных управлений МЧС России 83 субъектов Российской Федерации.

Организаторы: правительство Удмуртской Республики, администрация города Ижевска, Министерство внутренних дел по УР, Главное управление МЧС России по Удмуртской Республике, Удмуртская торгово-промышленная палата, Выставочный центр «УДМУРТИЯ».

Тематика выставки: безопасность в ЧС, пожарная безопасность, системы общественной безопасности, безопасность дорожного движения, системы охраны, информационная безопасность, экологическая и промышленная безопасность, безопасность труда, медицина катастроф, защита дома и офиса.

infosecurity RUSSIA

2. InfoSecurity Russia–2013, 25–27 сентября 2013 г.

Место проведения: Россия, Москва, «Крокус Экспо».
Сайт: www.infosecurityrussia.ru

InfoSecurity Russia–2013 – место встречи экспертов со всего мира, возможность обменяться опытом и прослушать лекции исследователей ведущих международных университетов. Тематические акценты выставки и наибольшее количество мероприятий соответствуют ключевым трендам развития ИТ и ИБ – облачные вычисления, мобильная коммерция, DLP, непрерывность бизнеса, кибервойны.

В рамках деловой программы X Юбилейной выставки InfoSecurity Russia 2013 пройдут:
• Конференция «Персональные данные».
• Конференция «IT-инфраструктура современного предприятия».
• Конференция «Защита АСУ ТП».
• Конференция «Противодействие мошенничеству».

Впервые на выставке InfoSecurity Russia будет работать демонстрационная зона для функционального тестирования Межсетевых экранов. Также в 2013 г. на InfoSecurity Russia–2013 будет представлен новый кластер, посвященный исследованиям всего спектра киберпреступности, киберкультуры и кибертерроризма, информационных войн и защиты критической инфраструктуры, теоретическим основам и практическим примерам последних разработок цифровой криминалистики.

XVII МЕЖДУНАРОДНАЯ ВЫСТАВКА
INTERPOLITEX
СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА

3. XVII Международная выставка Interpolitex, 22–25 октября 2013 г.

Место проведения: Россия, Москва, ВВЦ, павильон 75.
Сайт: www.interpolitex.ru

Экспозиция Международной выставки средств обеспечения безопасности государства «ИНТЕРПОЛИТЕХ 2013» разместится на площади 25 500 кв.м. в трех экспозиционных залах павильона №75 на ВВЦ и представляет собой выверенное сочетание взаимосвязанных выставок и специализированных тематических экспозиций, взаимодополняющих друг друга:
• Выставка полицейской техники.
• Военно-технический салон.
• Выставка «Граница-2013».
• Выставка «Беспилотные многоцелевые комплексы – «UVS TECH 2013».

Деловая программа Interpolitex включает следующие мероприятия:
• Научно-практическая конференция МВД России «Перспективы создания образцов вооружения и специальной техники нового поколения».
• Конференция «Законодательные, организационные и технические вопросы эффективного применения беспилотных авиационных комплексов в воздушном пространстве РФ при решении задач МЧС, МВД и других ведомств».
• IX Международная научно-практическая конференция «Промышленная утилизация БП-2013».
• Научно-практическая конференция «Традиции и перспективы оснащения российского бойца» и др.

Также в рамках Interpolitex–2013 пройдут демонстрационный показ эксплуатационных и боевых возможностей вооружения и техники промышленных предприятий и показные учения специальных подразделений ВВ МВД России.

HI-TECH BUILDING

4. XII Международная выставка-форум HI-TECH BUILDING 2013, 29–31 октября 2013 г.

Место проведения: Россия, Москва, Экспоцентр, павильоны 1 и «Форум».
Сайт: www.midexpo.ru

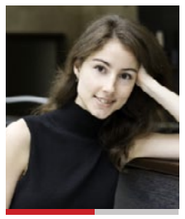
Единственная выставка в России и СНГ в области автоматизации зданий и систем «Умный дом».

Тематика мероприятия:
• автоматизация и диспетчеризация;
• интегрированные системы безопасности;
• системы управления освещением;
• системы управления климатом;
• электротехнические системы управления;
• ИТ-системы;
• энергоэффективные системы.

Ваше мнение и комментарии присылайте по адресу
info@csc.ru

Частное охранное предприятие: правила выбора

Анатолий Брединский



Интервью подготовила и провела Адель Соколова

Ранок охранных предприятий в России изобилует различными предложениями. Многочисленные ЧОП обещают качественное и гарантирование оказание самых разных услуг – от перевозки ценных грузов и обеспечения безопасности сложных объектов до присмотра за малолетними детьми. Неверное решение при выборе подрядчика может стоить заказчику весьма дорого. О том, с чего начать поиски подходящего ЧОП, и как не допустить роковых ошибок, мы поговорили с руководителем проекта «Безопасность для всех», старшим преподавателем кафедры Защиты, Охраны и Безопасности ГУФиС РМ Анатолием Брединским.

Безопасная школа

Забота о детях - наша работа

Комплекс “Безопасная школа” создан для обеспечения безопасности школьников. Это надёжный и экономичный способ контролировать вход и выход на основе бесконтактных карт-ключей.

Как работает система:

- **Именная карта-ключ** выдаётся каждому школьнику и всем сотрудникам.
- Для того чтобы пройти через турникет, на входе и выходе необходимо **поднести карту к считывающему устройству**.
- Проход школьника через турникет сопровождается отправкой **SMS-сообщения на телефон родителей** (услуга sms-информирования).
- Информация о проходе через турникет фиксируется в базе данных, доступ к которой можно получить на сайте **Безопасной школы**.

Стоимость установки, подключения и обслуживания комплекса “Безопасная школа”:

- Установка оборудования - **БЕСПЛАТНО!**
- Подключение и обслуживание - **БЕСПЛАТНО**
- Комплект карт-ключей - **БЕСПЛАТНО**
- Услуга “**SMS-информирование**” только для родителей, желающих получать SMS-сообщения о своих детях - 250 рублей в месяц.

Дополнительная услуга - оплата обедов в школьной столовой при помощи карточки-ключа.

Каждый сам решает, необходимо ли заботиться о безопасности своих детей, но не многие понимают, что безопасность жизни и своего будущего зависит во многом именно от нас. Задумайтесь об этом сейчас, ведь так сложно быть в безопасности в наше непростое время.

www.safeschool.ru

- Анатолий, что нужно сделать первым делом, когда компания решила обратиться к услугам частного охранного предприятия – проверить справочники, поспрашивать у знакомых, поискать в Интернете, побывать в офисе понравившихся ЧОП, посетить охраняемые ими объекты?

- Идеально, когда все это делается вместе, так как каждый из вариантов позволяет получить полезную информацию. Например, с помощью поисковых систем появляется возможность увидеть, в каком контексте упоминается ЧОП в Интернете, не является ли участником скандалов или криминальных историй, как о нем отзываются на форумах и т.п. Визит на охраняемые организацией объекты также может дать очень много полезной информации. Появляется возможность увидеть ваших будущих охранников на рабочем месте, проследить, как они себя ведут, как выглядят, как разговаривают с людьми. Сходите в головной офис компании, поскольку важно знать, где он расположен, какая там атмосфера. Нелишним будет поспрашивать знакомых по бизнесу: наверняка кто-то уже пользовался услугами ЧОП. Или, может, отыщутся знакомые, родственники, работающие на конкретном предприятии, которые будут готовы поделиться интересной информацией о нем. Только не надо заранее говорить, с какой целью вы интересуетесь, так как это может повлиять на искренность ответов. Постарайтесь также узнать, сколько зарабатывают сотрудники охраны и имеют ли они социальный пакет. Это очень важный показатель для определения эффективности их дальнейшей деятельности.

- Чем нужно руководствоваться при выборе ЧОП?

- Наиболее важными показателями, на мой взгляд, являются возраст ЧОП, наличие у него хорошей репутации на рынке, положительных отзывов и рекомендаций, а также серьезных и крупных клиентов (желательно из той же сферы деятельности, что и ваше). Также стоит обратить внимание на количество сотрудников, работающих в приглянувшейся вам компании, их оснащенность и подготовленность. Изучая комплекс предоставляемых услуг и, конечно, цены на них, помните: низкая стоимость должна настораживать, ведь качественная работа не может стоить дешево. Но все это при условии, что вы не хотите сэкономить на своей безопасности.

- Что является показателем надежности охранного агентства?

- Объективных показателей надежности и профессионализма пока нет, так как до сих пор нет единых стандартов на услуги по безопасности, таких как, например международные стандарты ISO. Поэтому относительным показателем надежности является срок, в течение которого компания действует на рынке, ее клиенты, наличие филиалов в регионах и других городах, предоставление всего комплекса услуг в области безопасности, а не только физической охраны. Ну и, пожалуй, самым важным показателем является количество и состав ее персонала. Только надежная компания может позволить себе иметь в штате квалифицированных профессионалов.

- Что необходимо запросить у выбранного ЧОП для того, чтобы убедиться в правильности своего решения?

- Проверить документы, безусловно, не будет лишним, но гарантией это, увы, не является. Лучше обратите внимание на то, как с вами выстраивают отношения: насколько серьезно подходят к составлению договора на охрану, как много внимания уделяют изучению вашего объекта, как отвечают на вопросы и т.п.

- Что должно настораживать заказчика при разговоре с представителем агентства?

- Нечеткие, слишком обтекаемые ответы на поставленные вопросы, нежелание отвечать на «неудобные вопросы» или даже раздражительность, когда вы хотите узнать слишком много подробностей. Плохим знаком является отсутствие системного подхода к работе с клиентом, предварительного тщательного изучения объекта и причин, которые побудили вас обратиться за помощью ЧОП. Чрезмерное упоминание «солидности» и «крутизны» ЧОП, «козыряние» высокопоставленными связями, демонстративно уничижительные высказывания о конкурентах, грубая или агрессивная манера ведения переговоров, затягивание с оформлением договора или сведение его к формальностям, нежелание рассматривать ваши предложения, пожелания, слишком низкая цена на услуги в сравнении с другими компаниями – все это должно настораживать вас.

- Какие пункты в договоре с ЧОП следует изучать с особой тщательностью?

- Прежде всего, это сам объект охраны. Например, бывали ситуации, когда на предприятии причинялся вред работникам, а сотрудники ЧОП утверждали, что забота о жизни и здоровье персонала не входит в их обязанности, так как договор заключен только на обеспечение безопасности имущества компании. Во-вторых, рассмотрите права и обязанности сторон. Особенно это касается случаев, исключающих ответственность исполнителя. Уделите внимание условиям оплаты, в которых должно быть четко указано, за что и сколько следует платить. Стоит помнить, что в договоре на охрану наиболее важной бывает информация, которая содержится в его приложениях. Именно в них прописывается план охраны объекта, численность охранников, их экипировка, график работы и т.п.

- Какие мероприятия следует провести после составления договора?

- Нужно подготовить свой объект к охране, произвести необходимые действия по его укреплению и модернизации (обычно эти рекомендации предоставляют представители ЧОП после изучения объекта), по возможности выделить на предприятии отдельное помещение для сотрудников охраны, провести инструктаж своих работников. В случае когда на объекте есть технические средства охраны (например видеонаблюдение), решить вопрос о возможности их дальнейшего использования и обслуживания сотрудниками ЧОП.

- Выполнения каких обязанностей можно требовать от охранного агентства?

- Только исполнения обязательств по договору согласно действующему законодательству. Сотрудники охраны не могут быть втянуты в имущественные или хозяйственные споры, они не обладают правами представителей правоохранительных органов, не могут проводить оперативно-розыскные мероприятия. Иными словами, сотрудники охраны не могут привлекаться для выбивания долгов, захвата спорного имущества, запугивания других лиц и тем более применения физической силы к ним, они не имеют права взимать штрафы, обыскивать клиентов или персонал. Поэтому прежде чем требовать от них исполнения какой-либо дополнительной работы, надо удостовериться, что ваши требования не противоречат действующему законодательству.

- Что, в свою очередь, должна предоставить фирма охранному агентству – план здания, точную информацию о проблемах?

- Прежде всего, юридическое подтверждение прав на имущество, подлежащее охране. Сотрудники охраны должны быть уверенны, что правомерно охраняют ваше, а не чужое имущество. Они должны быть в курсе, какие материальные ценности необходимо охранять, где они хранятся, и как защищены, кто будет курировать вопросы взаимодействия с ЧОП от предприятия. Следует также сообщить свои пожелания к охранникам (например владение иностранными языками, высокий рост, отсутствие татуировок на видимых частях тела, соблюдение дресс-кода и т.п.)

- Как проверить, хорошо ли работают сотрудники охранного агентства?

- Вечная проблема заказчика: если охрана работает хорошо, и на предприятии ничего плохого не происходит, ему начинает казаться, что сотрудники ЧОП даром получают свои зарплаты. На самом деле эффективность охраны можно выявить по следующим показателям: на объекте не происходит никаких инцидентов, а те, что происходят, быстро и эффективно решаются представителями агентства; клиенты и сотрудники не жалуются на их действия, не возрастают потери от краж и порчи имущества. Если в вашей компании все так, значит, ЧОП работает хорошо. Но если у вас все равно есть сомнения, попросите кого-то из знакомых посетить охраняемый объект под видом обычного клиента и попытаться, например затеять конфликт. Сами понаблюдаете и их расспросите, как действовала ваша охрана, узнаете, насколько профессиональными и корректными были их меры. Только не переусердствуете, чтобы потом не пришлось выручать знакомых из полиции.

- Какими качествами и навыками должен обладать профессиональный охранник?

- Сначала он должен пройти обязательное обучение. После этого проводится аттестация. В ходе прохождения специальных курсов изучаются правовые основы, техника рукопашного боя и огневой подготовки, правила оказания первой помощи, психология и тактика охранной деятельности. К сожалению, практика показывает, что иногда такого обучения оказывается недостаточно, и поэтому некоторые профессиональные агентства организуют собственную дополнительную подготовку. Не углубляясь в этот

вопрос, отмечу, что, по моему мнению, охранник должен иметь хорошую правовую и физическую подготовку, уметь предотвращать критические ситуации и выбирать тактически верное поведение. Одним из самых главных качеств является умение корректно общаться с людьми, не давая развиваться возможным конфликтным ситуациям. Главная задача сотрудника охраны – предотвратить возможные проблемы, а не демонстрировать свою «крутизну» в их решении.

Если к сотрудникам ЧОП есть объективные претензии, то можно попросить об их замене. Однако это не должно зависеть от капризов работников охраняемого предприятия, которым не понравился тот или иной представитель охраны, проявляющий строгость. Кстати, умение найти общий язык с клиентом и удовлетворить его пожелания является одним из признаков профессионализма охранного предприятия.

- В каких случаях можно прервать контракт с охранным агентством?

- Условия расторжения договора обычно указываются в его соответствующих разделах. Если есть сомнения по поводу выбора агентства, можно заключить договор на менее длительные сроки, например на полгода. Тогда по истечении этого периода можно будет принять окончательное решение, стоит ли продолжать пользоваться услугами конкретной компании. По собственному опыту могу сказать, что если изначально было верно выбрано профессиональное охранное предприятие, поводов для расторжения договора с ним возникнуть не должно, так как серьезные компании дорожат своими клиентами.

- Как не переплатить за услуги ЧОП?

- Есть такое выражение: безопасность стоит дорого, но она того стоит. Не надо гнаться за дешевизной, это всегда вредит качеству. Естественно, перед тем как заключить договор, изучите предложения от различных охранных организаций при условии, что все они равны по уровню оказания услуг. Не стоит выбирать самое дешевое или самое дорогое предложение. Серьезное охранное предприятие всегда гибко подходит к вопросу ценообразования и наверняка сможет предложить вам какие-то индивидуальные бонусы.

- На что еще стоит обратить внимание?

- Не забывайте, что сотрудники охраны – это в первую очередь люди. Относитесь к ним с уважением и вниманием, и они ответят вам взаимностью. Однако воздержитесь от панибратства, отношения должны быть корректными, но при этом клиент имеет право предъявлять разумные требования и контролировать работу охраны. Объясните своему персоналу, что работа сотрудников охраны очень важна для вашей компании, и что они должны помогать представителям ЧОП. Понятно, что мало кому нравится контроль со стороны третьих лиц, но это необходимость, а не прихоть конкретного охранника. И еще один важный момент: если театр начинается с вешалки, то для многих предприятие начинается с охраны. От того, насколько у вас профессиональные охранники, зависит не только сохранность материальных ценностей, жизнь и здоровье сотрудников. От этого зависит и мнение партнеров и посетителей о вас. Грубость и некомпетентность сотрудников охраны нередко способна оттолкнуть значительную часть клиентов. Поэтому выбирайте правильное охранное предприятие.

Ваше мнение и комментарии присылайте по адресу
info@csc.ru

www.ekeyRus.ru

ekey

Просто Удобно Безопасно

№1 в Европе по системам доступа по отпечаткам пальцев

- Сделано в Австрии
- Температурный режим от - 40 до + 85 С°
- Подключение до 3-х дверей к одному сканеру
- Вероятность распознавания FAR 1x10^{-6}
- Сетевые решения для малых и больших офисов
- Совместимы с любыми электронными замками
- 24 месяца гарантии от производителя

Решение для дома, офиса, корпоративной сети

Приглашаем производителей дверей




Ваш палец - это ключ!

ekeyRus.ru БИОМЕТРИЧЕСКИЕ СИСТЕМЫ

Будущее уже наступило!

www.ekeyrus.ru (495) 739-34-99

г. Москва, 1-й Волконский пер., д. 15

«Салон умных дверей» - гипермаркет «Стройдом» (D12), ТЦ «ЮНИМОЛЛ», Новорижское шоссе.

г. Санкт-Петербург (812) 458-71-13

Кадровая безопасность компании: правила построения

Алла Поспелова

Специалист по управлению, командообразованию и конфликтологии, консультант по корпоративной культуре.
Профессиональный преподаватель, общий стаж преподавания — 18 лет.
Имеет три высших образования.
Автор более 200 публикаций по рекламе, маркетингу и управлению.
Школа Делового и личностного развития, возглавляемая Аллой Поспеловой, существует с 2006 г. За этот период компания успела сделать себе имя в сфере коучинга и смежных услуг – консалтинга, брендинга, тренингов для персонала.
Как коуч специализируется на персональном карьерном росте с нуля в рамках крупных трейдинговых компаний Екатеринбурга и Москвы, а также консультирует владельцев бизнеса.
Основной деловой интерес — стратегическое развитие предприятия; нематериальные принципы мотивирования сотрудников, выстраивание команды и использование энергии конфликта в эффективном командообразовании. Готовится к печати книга по эффективному управлению персоналом «Управление без давления».

Кадровая безопасность на предприятии должна учитывать все аспекты его функционирования. Это система мер, правил и инструментов, подвижная во времени и пространстве, т.е. настолько гибкая, чтобы работать эффективно в разных отделах и сферах производства, будь то охранное предприятие или же компания по изготовлению молочных продуктов. О том, как грамотно управлять персоналом, нанимать сотрудников, выстраивать систему безопасности при работе на производстве, где задействованы человеческие ресурсы, и многом другом журналу «Безопасность: Информационное обозрение» рассказал один из лучших бизнес-тренеров России, директор Школы делового и личностного развития «Фабрика роста» Алла Поспелова.

- Алла Николаевна, как Вы определяете понятие «кадровая безопасность на предприятии»? Какова ее сущность и цели?

- Кадровая безопасность на предприятии – это, на мой взгляд, умение защитить организацию в целом от различных проблем, связанных с кадрами. Это могут быть неприятности, связанные с нанесением юридического и финансового вреда, например, воровство или ненадлежащее выполнение своих обязанностей. Второй момент – это юридическая кадровая безопасность. На многих предприятиях важна компетентность специалистов, наличие у них настоящих, а не поддельных дипломов. Не стоит забывать и о мотивации персонала, формировании у сотрудников желания выполнять свои обязанности честно. По этому поводу можно рассказать анекдот: «ГИБДД России выразило озабоченность в связи с новой политической инициативой Всероссийского общества автомобилистов. «Призыв "Выпил, вызови такси, чтобы заработал водитель, а не гаишник!" обладает всеми признаками недобросовестной конкуренции, а сравнение тарифов таксистов и гаишников – это вообще явный демпинг...», – сообщили в пресс-центре ГИБДД». Таких анекдотов не может быть, если люди настроены честно работать и честно выполнять свои обязанности.

«Во всем мире работа с персоналом стоит на трех китах: сотрудник должен быть управляемым, обучаемым и адекватным. Четвертый кит – компетентность. Этого вполне достаточно, чтобы обезопасить себя от неприятностей».

- Каким образом мы можем оценить кадровую безопасность на предприятии и предотвратить возникновение негативных факторов, связанных с персоналом?

- Способов предотвращения не очень много. Все они могут быть применены на этапе найма людей на работу. Когда мы нанимаем персонал, тут не нужно никакое волшебство, необходимо лишь следовать простому алгоритму:

1. Берем резюме и сравниваем обозначенные в нем компетенции с компетенциями, которые нам требуются.

2. Приглашаем на собеседование только тех кандидатов, чьи компетенции нас полностью устроили.

3. Приглашаем человека на собеседование и задаем вопросы, которые помогут нам установить действительное наличие компетенций.

4. Проверяем то, что человек написал о себе, например подлинность его диплома о высшем образовании.

5. Не стоит думать, что рекомендации с предыдущих мест работы гарантируют правдивое представление о соискателе, это не всегда так. Личная встреча и беседа – лучший способ проверить, не завышена ли у кандидата самооценка.

6. Я также считаю, что не следует полностью полагаться на психологические тесты. Большинство из них строятся на каких-либо физиологических реакциях. Например, у человека пересыхает во рту не только, когда он врет, но и из-за определенных проблем со здоровьем. В результате вы сочтете опасным человека, максимальный «вред» от которого – слишком частое пользование кулером. Люди, у которых аллергия, чешут носы, а грязная обувь может стать причиной того, что человек примет закрытую позу. На мой взгляд, никто не способен выглядеть более честно, чем профессиональный лжец, который знает все тонкости психологических проверок. Он не начнет крутить волосы, не будет прикрывать рот или садиться в закрытую позу, а также ответит верно на все письменные вопросы, поскольку имеет опыт поиска работы и знает, как производить впечатление.

Если вы все же прибегнете к тесту, советую задавать вопросы «по кругу» – т.е. по нескольку раз переформулировать одни и те же пункты и внимательно следить за тем, совпадают ли ответы, и насколько они совпадают.

- Как можно избежать утечки информации на предприятии?

- Это одна из главных задач системы кадровой безопасности. Промышленный шпионаж, кражи баз данных, откаты – серьезнейшие проблемы, которые могут возникнуть при несоблюдении элементарных правил. При проведении аудита бизнеса, в частности аудита персонала, нередко можно столкнуться с ситуацией, когда откатная составляющая насчитывает 50% от цены услуги. Причем этим не брезгуют не только люди, которые сидят на маленьких зарплатах. Неправы руководители, которые считают, что их топ-менеджеры слишком хорошо зарабатывают, чтобы брать еще и взятки. Однажды, проводя аудит бизнеса и персонала в одной из крупнейших инжиниринговых компаний, я столкнулась с ситуацией, когда соучредитель, член совета директоров умудрялся воровать 20–30% от стоимости каждой поездки подчиненных за рубеж, наживаясь на изготовлении сувенирной продукции, заказе билетов, оплате гостиницы и многом другом.

Очень важно поощрять честных сотрудников, а также тех, кто сумел сэкономить средства предприятия. В противном случае когда-нибудь и честный человек задумается: «Я вижу, как коллега рядом со мной ворует и получает такой

же годовой бонус, как и я, несмотря на то, что я сэкономил предприятию деньги».

Помимо финансовых потерь есть едва ли не более важная для некоторых сфер деятельности угроза – слив информации и выгрузка контактов. Это сулит очень серьезные проблемы, особенно если контакты выгружает менеджер по продажам.

Помните и о возможности слива информации конкурирующим предприятиям. Приведу один печальный пример. В развивающуюся компанию «Страховой брокер» на должность заместителя директора устроился идеально подходящий по всем параметрам молодой человек. Через полгода руководитель предприятия увидел, что, несмотря на рекламу, активные продажи и т.д., у компании практически пропали крупные и индивидуальные заказчики. В результате расследования выяснилось, что замдиректора являлся ближайшим родственником начальника конкурирующего предприятия, и все крупные заказы уходили именно ему. В процессе работы шел перехват контактов и информации.

- Какие методы противодействия сливу информации Вы порекомендуете?

- Во-первых, после каждого мероприятия необходимо отслеживать, чтобы все контакты были выгружены в общую систему. Если у одного менеджера выгружается в систему 40 контактов, а у другого один-два, то налицо воровство. Бывает и так, что менеджер организовал мероприятие, на котором не было вашей целевой аудитории, тогда его можно уличить в профнепригодности. Все эти ситуации возникают в результате несоблюдения кадровой безопасности.

Выгрузка информации может быть разной: контакты, персональные данные клиентов или сотрудников, адреса, характеристики, формулы, выгрузка коммерческих тайн и т.п. Специальные программы, отслеживающие внутрисетевой трафик, позволяют просматривать динамику действий каждого компьютера любого сотрудника. Сколько входящей информации, сколько выходящей, с какими документами работал человек и тому подобное. Например, если он выгрузил много контактов или превысил лимит Интернета, у него автоматически заблокируется сеть, до тех пор пока в деле лично не разберется директор компании. После официального приказа запрет снимается. Это элементарный контроль трафика внутри сети.

При этом важно помнить, что забор не должен быть дороже дома. Перед покупкой программы руководителю следует просчитать минимальный и максимальный ущерб своего предприятия в случае потери контактов. Если максимальная потеря будет составлять 500 тыс., а программа стоит один миллион, решение о ее приобретении нельзя считать логичным. Если потери могут составить пять млн, а программа стоит один миллион, то на нее однозначно следует потратиться.

- Расскажите о кадровой безопасности как об инструменте разрешения межличностных деструктивных конфликтов.

- Несовместимость работников может обернуться серьезным ущербом для предприятия. Когда секретарь не сработался с ключевым сотрудником, но установил дружественные отношения с владельцем фирмы, компания может потерять лучшего специалиста. Конфликт – это почти всегда плохо. Но и полное отсутствие разногласий в организации должно настораживать, ведь неравнодушные к успеху предприятия сотрудники могут и должны иметь разные точки зрения и отстаивать их. Но конфликт должен быть конструктивным.

Деструктивный конфликт – это неразрешимые межличностные противоречия. Приведу пример такого конфликта. В крупной айтишной компании, где очень хорошо были подобраны сотрудники, между руководителями двух подразделений постоянно шел конфликт, очень сложный конфликт, вплоть до саботажа, а работать подразделения должны были вместе. Руководитель одного подразделения принципиально отказывался выполнять требования другого. Почему? Дело в том, что один был по типу «мачо», считал нормальным иметь любовниц и выказывать полное неуважение к женщинам, а второй – хороший семьянин и отец двух дочерей. При этом оба были профессионалами высокого уровня. В результате была принята вынужденная мера – взаимодействие между ними было решено осуществлять исключительно через ведомство директора.

- Какие тренинги могут помочь сотруднику отдела кадров принять правильные решения при приеме людей на работу?

- Тренингов по найму персонала достаточно много. Процесс трудоустройства должен быть доведен до автоматизма, а не проходить по принципу «понравился – не понравился». В последнем случае неизбежны конфликты и иные негативные последствия. Также хорошо периодически проводить тренинги по конфликтологии. На личном опыте могу сказать, что это, к сожалению, одни из самых редко покупаемых тренингов, но одни из самых полезных. Качественно проведенный тренинг помогает не только преодолеть разногласия, но и использовать энергию конфликта с пользой. Игнорируя конфликты, руководители оказывают себе медвежью услугу.

Помимо посещения тренингов я советую периодически проводить в компании ассесмент и аудит персонала.

- Какие основные советы Вы могли бы дать начальнику службы персонала?

- Всегда держать руку на пульсе. И никогда не забывать, что кадры решают все.

Риски корпоративного мошенничества: предупреждение, выявление и пресечение

Андрей Глебовский,
Учебный центр
«Информзащита».

Культивирование позиции «воруй, воруй, Россия, всего не украдешь» на всех уровнях и во всех формах (наследие истории, случаи из современной жизни, факты воровства в собственной компании, информационный фон массмедиа и др.) – все это формирует в обществе тренд «нет времени ждать, все хочется взять». В итоге в результате мошеннических действий в России ежегодно пропадает более 2 трлн рублей. Типичные оправдания нарушителей: «А что, так все поступают» или «Ты бы на моем месте не взял?» Вот и текут рекою в звеньях одной цепи под названием корпоративное мошенничество махинации с финансовой отчетностью, которые вводят в заблуждение инвесторов, сокрытие компаниями данных об убытках, картельные сговоры и т.д. Не помогают ни законы, ни наказания. Остается одно – предупредить, выявить и пресечь.

Мошенничество в бизнесе

«Разве нет более насущной проблемы для бизнеса, чем противодействие мошенничеству?» – спросите вы. И будете правы. Самый важный вопрос для акционеров - успехи компании. А они, как известно, напрямую зависят от степени доверия к менеджменту. Основная масса экономических преступлений в российских компаниях выявляется корпоративными службами безопасности и подразделениями внутреннего аудита (28 и 20% соответственно), об остальных становится известно из других источников (например правоохранительных органов).

Это яркий пример того, что никто не задумывается над вопросом: «А какая ситуация у нас с воровством в компании?» Вроде бы все знают, что оно есть, но никто не догадывается, в каких масштабах, а иногда и вовсе не придают этому значения. Мероприятия по линии служб экономической безопасности, даже если они проводятся высококвалифицированными профессионалами, являются лишь одним из столпов, на которых должен базироваться весь арсенал в борьбе с корпоративными мошенничествами. По данным материалов исследований таких авторитетных аудиторских компаний, как PWS и Ernst&Yang, в 70–80% российских компаний СЭБ отсутствует либо только имитирует свою работу. И здесь, по мнению экспертов УЦ «Информзащита», важную роль играет создание эффективно действующей системы внутреннего контроля и включение в нее таких направлений, как управленческий учет и предварительный анализ операций. Кроме того, во многих компаниях присутствует политика «правил тушения, а не предотвращения пожара», т.е. чаще думают над тем, как восстановить status quo после случая мошенничества, и можно ли вернуть утраченное.

Приведем характерный пример. Однажды топ-менеджеры крупного московского предприятия обнаружили недостачу товара на сумму свыше 10 млн рублей. Продукция была отгружена получателям на условиях отсрочки платежа, но, когда подошли сроки оплаты, расположенные в разных регионах России контрагенты с возмущением заявили, что никакой продукции не заказывали, в глаза ее не видели и, соответственно, оплачивать ничего не собираются. Необходимо заметить, что на период этих криминальных отгрузок на предприятии фактически отсутствовала служба экономической безопасности.

После приглашения специалистов, имеющих соответствующие знания и опыт, была выявлена следующая схема: менеджеры отдела сбыта, используя ранее заключенные договоры с покупателями из регионов, изготовили подложные печати этих организаций, систематически подделывали доверенности на получение товарно-материальных ценностей и целыми фурами вывозили продукцию, которую впоследствии сбывали через сеть торговых точек своих соучастников в московском регионе. Вновь созданная СЭБ не только выявила систему хищения, но и полностью отработала всю преступную цепочку. Материалы были переданы в УВД ЗАО г. Москвы, возбуждено восемь уголовных дел.

Деформация корпоративных отношений

Как показало исследование Pricewaterhouse Coopers, более половины инцидентов, в том числе связанных с негативными экономическими последствиями для компаний, совершаются собственными сотрудниками. Аналитики утверждают, что такая проблема как «чужой среди своих» возникает из-за отсутствия согласованности между действиями кадровых служб и СЭБ. По мнению специалистов УЦ «Информзащита», можно выделить несколько ключевых тезисов, характеризующих ситуацию с мошенничеством в компаниях:

КАК ПОКАЗАЛО ИССЛЕДОВАНИЕ PRICEWATERHOUSE COOPERS, БОЛЕЕ ПОЛОВИНЫ ИНЦИДЕНТОВ, В ТОМ ЧИСЛЕ СВЯЗАННЫХ С НЕГАТИВНЫМИ ЭКОНОМИЧЕСКИМИ ПОСЛЕДСТВИЯМИ ДЛЯ КОМПАНИЙ, СОВЕРШАЮТСЯ СОБСТВЕННЫМИ СОТРУДНИКАМИ.

- Персонал может совершать мошеннические действия, чувствуя себя обманутым топ-менеджментом компании. Многие проблемы следует решать «изнутри», а не «снаружи».
- Наибольшее число преступлений на предприятии совершают люди, находящиеся в родственных связях (72% случаев). Как говорится, «тут кому-то он кум, там кому-то он зять, человек он такой – он не может не взять».
- Руководство и топ-менеджмент не обладают полной и объективной информацией о ситуации с мошенничеством в компании, четким пониманием портрета корпоративного мошенника и основных мотиваций к совершению преступных действий.

Наиболее типичными видами мошенничества, совершаемыми наемными работниками, остаются:

- использование откатов и взяток;
- проведение сделок с подконтрольными компаниями;
- подделка или фальсификация документов с целью совершения хищений.

Что же делать в этом случае руководителю и безопаснику? Руководителю – как минимум знать эти вопросы. Безопаснику – представлять себе план и алгоритм действий, направленных на предотвращение мошенничества. И вот тут часто сотрудникам компаний не хватает знаний и профессиональных навыков. Невозможно, да и не нужно делать из руководителя и аудитора, и финансиста, и безопасника одновременно, однако следует обеспечить ему понимание принимаемых СБ стратегических мер. Важно осознавать, что воровство рядового персонала – это только часть проблем для руководства компании, тем более если подобные нарушения остаются без внимания. В 22% случаев воровство в незначительных масштабах может продолжаться в компании более 10 лет.

Царь Горох воровал, царь Иван воровал...

Аферы, совершаемые топ-менеджментом предприятия, представляют собой один из наиболее сложных типов корпоративного мошенничества. «Все во имя денег» и «после меня хоть потоп» здесь выступают основными принципами, да и близость к «большим деньгам» приводит к соблазну украсть. По данным Pricewaterhouse Coopers, если во всем мире основную массу хищений совершает средний менеджерский состав и линейный персонал (77% случаев), то в России это является прерогативой топ-менеджмента (50%). Причем у нас наиболее часто встречающийся тип экономических правонарушений (62%) – это использование служебного положения в личных целях, а 10% махинаторов являются членами советов директоров. Как не вспомнить фразу «в России лучше воровать вагонами – не заметят». Ну а если заметили? В 80% случаев разоблачение мошенника такого уровня совсем не означает его изгнание из компании. Нередко владельцы бизнеса дорожат ценными сотрудниками, даже если те воруют.

В случае увольнения проворовавшегося руководителя не следует ждать от него раскаяния и чистосердечного признания. Совсем наоборот: эти проворные и сметливые ребята, как правило, предвидят возможность такого развития событий и заранее страхуются – накапливают материалы, компрометирующие компанию и ее директора, а при увольнении выдвигают требование выплатить им солидное вознаграждение и предоставить положительные рекомендации для трудоустройства на новом месте.

Получается, в такой ситуации остается только одно – выдать вору «золотой парашют» и под пение корпоративного гимна с почестями проводить его до проходной? Но и эта процедура требует знаний и особого подхода, ибо на кону оказывается репутация компании. Тактика общения с шантажистами, эффективное противодействие вымогательству и принятие законных контрмер – важнейшие знания, которыми должен обладать сотрудник службы безопасности.

Как обычно все решается

В России борьба с корпоративным мошенничеством ведется тремя стереотипными способами, каждый из которых имеет свои недостатки.

Стереотип 1. Зачисление в штат СЭБ представителя силовых ведомств (вне зависимости от сегмента рынка и отрасли) для:

- попытки проверки лояльности сотрудников;
- отлова явных корпоративных мошенников (часто постфактум) с использованием имеющихся связей в правоохранительных органах.

Данная мера подразумевает открытое решение проблем и не позволяет обнаруживать скрытые угрозы.

Стереотип 2. Ошибочный подход к противодействию корпоративным мошенничествам – направленность на «ликвидацию» и «искоренение» угроз, а не минимизацию риска их появления. Еще одна ошибка – прием на работу в СЭБ команды, которая умело имитирует деятельность по обеспечению экономической безопасности компании. В результате предприятие будет обречено на уничтожение рейдерами, конкурентами и собственными внутренними расхитителями.

Стереотип 3. Не замечать проблем, связанных с корпоративными мошенничествами, закладывая «убыточный процент» на воровство. Этот подход представляется абсурдным, поскольку типы, масштабы мошенничества и объемы убытков предсказать невозможно. Да и забывается принцип «из мелочей складывается крупное».

Перечисленные подходы порождают 100-процентную вероятность возникновения рисков корпоративного мошенничества. Как показало исследование британской аудиторской компании Ernst & Young, проведенное в России в 2011 г.,

- только 19% сотрудников считают, что их компания в течение последних нескольких лет наращивала свои усилия по борьбе с корпоративным мошенничеством;
- только 43% российских респондентов указали на наличие антикоррупционной политики и кодекса корпоративной этики в их компаниях;
- только 32% отметили существование четких штрафных санкций за нарушение этих политик;
- только 18% российских респондентов участвовали в тренингах по антикоррупционной политике.

Риски стереотипных подходов

С актуальностью угрозы разворовывания собственным персоналом всего, что плохо лежит, вряд ли решится поспорить кто-либо из «капитанов бизнеса». Однако на деле руководители компаний отнюдь не всегда прилагают должные усилия к тому, чтобы минимизировать актуальные риски. Или просто не знают, как это сделать.

Другой враг – типичность мышления. Самовнушение руководства, что в их компании не существует угрозы корпоративного мошен-

АТК СПб
ассоциация тренинговых компаний
www.atkspb.ru
info@atkspb.ru

Санкт-Петербург: +7 (812) 642-77-78
Москва: +7 (495) 720-92-78
Бесплатно по России: +7 (800) 555-07-78

Ассоциация тренинговых компаний Санкт-Петербурга приглашает специалистов по обеспечению безопасности предприятий на актуальный специализированный семинар:

Служба экономической безопасности на предприятии. Оценка и предупреждение потенциальных угроз. Внеплановые проверки бизнеса.

Создание и внедрение службы экономической безопасности на предприятии. Постановка задач, связанных с защитой и предупреждением угроз экономической безопасности компании. Организация проведения профилактических мероприятий по защите экономической безопасности компании и физической охране объектов с применением современных технологий.

Предотвращение недружественных поглощений, практический опыт противостояния регистраторов рейдерским атакам, бизнес-разведка, конкурентная разведка и промышленный шпионаж, контрольно-ревизионная работа, проверки бизнеса государственными органами, современные системы охраны объектов, информационная безопасность предприятия.

За более подробной информацией обращайтесь по телефону:
+7 (812) 642-777-8

ничества, – обманчивая позиция. Однако это распространенная ситуация в бизнесе, которая подтверждает полное отсутствие аудита самой СЭБ, руководитель которой подчас выступает в роли успокаивающего «психолога» генерального директора. Между тем вера руководства компании в 100-процентную компетентность собственной СЭБ недопустима. Как говорится, доверяй, но проверяй.

Проверка эффективности работы СЭБ проводится далеко не во всех компаниях и часто представляет собой набор формальных процедур. Следствием такого подхода является случайность в раскрытии корпоративных мошенничеств. Согласно статистике большинство фактов КМ – это неожиданность для бизнесмена. Причинами того, что число нарушений в компании перевалива-ет за допустимый предел, могут быть: текучка кадров (когда меняются менеджеры, администраторы и т.д.), размер компании, отсутствие понимания у СЭБ бизнес-процессов и внутрикорпоративной ситуации в организации. Подобное положение дел – предпосылка для проведения комплексного аудита.

Как восстановить status quo?

Это самый важный вопрос для бизнеса после выявленного факта корпоративного мошенничества. По мнению преподавателей УЦ «Информзащита», для успешного расследования инцидентов необходимо знание теоретических и стратегических аспектов, норм уголовного права и методик выявления нарушений. Принципиальным в этом смысле становится рассмотрение проблемы КМ с уголовно-правовой и криминалистической точек зрения.

Практика показывает, что наиболее часто встречающимися и опасными являются следующие уголовно наказуемые деяния корпоративных расхитителей: собственно мошенничество (ст. 159 УК РФ), присвоение и растрата (ст. 160 УК РФ), кража (ст. 158 УК РФ), коммерческий подкуп (ст. 254 УК РФ), кражи конфиденциальной информации (ст. 183 УК РФ). Подробный юридический анализ каждой из указанных норм уголовного права с учетом руководящих разъяснений пленумов Верховного суда РФ помогает правильно формировать доказательственную базу и своевременно инициировать судебные и уголовные процедуры, а это, в свою очередь, позволяет законными способами возместить утраченное.

В настоящее время существует множество эффективных способов возврата украденных активов, в том числе и из-за рубежа. Однако полностью вернуть похищенное практически невозможно. Сложнее ситуация обстоит с ущербом репутации, когда, например, факт коррупции становится достоянием общественности.

По мнению специалистов УЦ «Информзащита», для эффективной работы сотрудники СЭБ должны знать ответы на следующие вопросы:

- Что мотивирует работников на совершение корпоративного мошенничества?
- Чем обусловлена возможность совершать мошенничество?
- Каковы признаки мошенничества со стороны наемных работников, менеджеров, руководителей?
- Каковы внешние признаки корпоративного мошенничества?
- Каковы внешние признаки мошенничества с финансовыми документами?
- Что такое аналитические симптомы мошенничества?
- Как осуществляются проверки в целях вычисления корпоративного мошенничества?
- Каковы основные способы устранения рисков мошенничества?
- Как проводятся расследования корпоративного мошенничества?

Обучение специалистов службы экономической безопасности поможет найти способы решения давно назревших проблем компании, переосмыслить подходы к совершенствованию борьбы с корпоративными мошенничествами, создать систему безопасности без «узких мест» и искоренить желание сотрудников нанести ущерб работодателю. Конечно, обучение персонала не является гарантией избавления от всех бед, но и при его отсутствии позитивных тенденций ожидать не следует.

Ваше мнение и комментарии присылайте по адресу

info@csc.ru

NOMITEK

Системы безопасности

- Видеонаблюдение
- Видеодомофоны
- Системы контроля доступа
- Системы учета рабочего времени

Почему выгодно работать с нами?

- Мы уже 5 лет на рынке и рекомендуем оборудование проверенное временем и соответствующее всем современным требованиям
- Гарантия на работы и оборудование составляет 2 года. В гарантийном случае мы бесплатно демонтируем оборудование, произведем ремонт и последующий монтаж (устранение неисправности в течение 36 часов)
- Гибкая система скидок при повторном обращении
- Техническая поддержка - наши специалисты всегда готовы ответить на все интересующие Вас вопросы по пользованию установленным оборудованием
- Мы ведем бухгалтерский учет по общей системе налогообложения - работая с нами вы экономите НДС (18%)

Нам уже доверились

Телефон: +7 (495) 646-88-21

E-mail: nomitek@bk.ru URL: www.nomitek.ru

Игра в другого человека

Наталья Литова

Кристофер Роканкурт – один из самых известных в мире мошенников-«актеров». Подделывая документы и выдавая себя за других людей, он проворачивал финансовые аферы, грабил ювелирные магазины и представлялся потомком Рокфеллера. «Работая» таким образом во Франции, Швейцарии и США, преступник нанес им ущерб, оценивающийся в 40 млн долл.

Роканкурт родился в небольшом французском городке в 1967 г. Биография мистификатора полна пробелов и недомолвок. По некоторым данным мать будущего мошенника была проституткой, а отец – бедняком, любившим приложиться к бутылке. В пять лет мальчик и вовсе лишился родителей: мать якобы умерла от туберкулеза, отец напился и утонул в море, после чего сирота был отправлен в приют. Возможно, именно там, терпя лишения и унижения, Кристофер раз и навсегда решил, что его жизнь будет яркой и благополучной. К сожалению, способы, которыми Роканкурт принялся обеспечивать себе безбедное существование, были не достойны законопослушного гражданина.

Повзрослев, юноша тайно покинул приют и отправился прямиком в столицу – Париж, где и начался его мошеннический путь. Свой первый заработок – 1,4 млн долл. – он получил, подделав документы на чужую недвижимость и продав ее. Позже, в 1980–1990-е годы XX в., он не раз проделывал подобные манипуляции с целью получения легкой и крупной наживы.

Было у Роканкурта еще одно любимое и прибыльное занятие – ограбление ювелирных магазинов. Впервые обогатиться таким образом ему удалось в Швейцарии в 1991 г. И, хотя вина афериста-грабителя так и не была доказана, въезд в альпийскую страну ему отныне был запрещен. Говорят, сообщник грабителя взял всю вину на себя, а затем умер в тюрьме. Избежав расплаты за содеянное, Роканкурт несколько лет не давал о себе знать, выжидая, пока забудутся его женевские делишки. А затем продолжил совершать преступления уже на территории США.

В середине 1990-х годов предприимчивый француз принялся выдавать себя за родственника то одной, то другой знаменитости, чтобы втираться в доверие к одиноким богатым женщинам и обворовывать их. В разное время он представлялся племянником знаменитого кинопродюсера Дино де Лаурентиса, сыном итальянской актрисы Софи Лорен и даже родным братом Доди аль-Файеда – продюсера, сына египетского миллиардера Мохаммеда Аль-Файеда и последнего возлюбленного принцессы Уэльской Дианы.

Но и подобное «родство» казалось мошеннику недостаточно блестящим. Сняв роскошный особняк в самом богатом районе Лос-Анджелеса Беверли-Хиллз, он стал передвигаться исключительно на вертолете (в крайних случаях – на лимузине) и взял себе новое имя – Кристофер Рокфеллер, заявив таким образом о своей принадлежности к знаменитому роду американского предпринимателя, первого долларового миллиардера в истории человечества Джона Рокфеллера. Появляясь в ресторанах, аферист окружал себя эффектными женщинами и угощал своих жертв дорогим алкоголем и изысканными блюдами. В списке знакомых Кристофера оказались такие звезды как Микки Рурк, Жан-Клод Ван Дамм и Наоми Кэмпбелл. Впрочем, поговаривают, что их интерес к новоиспеченному продолжателю рода Рокфеллеров зиждился исключительно на финансовой выгоде. Так, мошенник пообещал Ван Дамму, карьера которого на тот момент катилась вниз, выделить солидные средства на съемки нового боевика. В обмен каратист-киноактер демонстрировал свою дружбу со спонсором, способствуя поддержанию его имиджа богатого и знаменитого.

Подобная шумиха была на руку Роканкурту. В мире о нем говорили как об удачливом финансисте, не пропускающем ни одного светского мероприятия и разгоняющем скуку благодаря гонкам «Формулы-1». «Наверное, я не так хорош, как Михаэль Шумахер, но мы с ним из одной конюшни "Ferrari"», – небрежно бросил Роканкурт в одном из интервью.

Действуя напористо и уверенно, мошенник только в одной из частей Лос-Анджелеса смог заполучить у доверчивых кредиторов почти 1 млн долларов. Нити преступной паутины, созданной Роканкуртом, тянулись в Майами, Сан-Франциско и Гонконг, а о размерах его афер даже спустя десятилетия можно только догадываться. По мнению Джорджа Мюллера, расследовавшего это громкое дело, речь идет о миллионах долларов.

«Закат» карьеры легендарного афериста начался в тот момент, когда его поведение вызвало подозрения у одного из «клиентов». Слухи о неблагонадежности потомка Рокфеллера поползли по всей Америке и привели к началу полномасштабного расследования. Роканкурт был арестован и обвинен в мошенничестве. Впрочем, вскоре Кристоферу удалось выйти на свободу благодаря залогу в 200 тыс. долларов, внесенному его официальной женой звездой «Плэйбоя» Марией Пиа Райс. Едва выйдя из заключения, Роканкурт по поддельным документам покинул США. По разной информации он жил в Венесуэле, а затем Гонконге, где, не теряя времени даром, увеличил свой незаконно нажитый капитал еще на несколько миллионов долларов.

Скучая по Северной Америке, Роканкурт поехал в Канаду, ведь в США после лос-анджелесского скандала ему путь был заказан. Остановившись в фешенебельном отеле одного из самых дорогих горнолыжных курортов, преступник представился знаменитым автогонщиком и боксером, путешествующим под вымышленным именем, дабы избежать внимания поклонников. От легенды о родственных связях с Рокфеллером по понятным причинам пришлось отказаться. Для убедительности мошенник переезжал с места на место в компании жены и ребенка. В Канаде Кристофер завел дружбу с крупным бизнесменом Робертом Болдоком и уговорил его инвестировать порядка 5 млн долларов в оформленную на него компанию Heartlink Canada, а затем продал «товарищу» дом стоимостью около 10 млн долларов, на поверку оказавшийся недостроенной рухлядью. На этот раз справедливость взяла верх: злоумышленника удалось поймать, осудить и в 2002 г. отправить на несколько лет за решетку. В тюрьме деятельный лжебизнесмен написал книгу, в которой рассказал обо всех своих приключениях и махинациях.

В 2005 г. преступник вышел на свободу, нашел новую роскошную пассию – мисс Францию-2000 Соню Роллан – и вернулся к привычной жизни. Хотя у пары родилась дочь, через некоторое время супруги расстались. О Кристофере Роканкурте с тех пор ничего не было слышно. Кто знает, быть может, знаменитый мошенник возводит новую финансовую пирамиду или втирается в доверие к очередному миллионеру? Судя по тому, как легко ему каждый раз удается заводить знакомых и возвращаться к беспечной светской жизни, «клиенты» Роканкурта недостаточно внимательно читали его книгу, значительная часть которой посвящена описанию «доверчивых богачей», искренне считавших его своих другом.

Как остановить грабителя за пять секунд?

Ольга Подолина

Согласно официальной статистике только в 2013 г. число банкоматов, пострадавших от действий преступников, выросло на 40%. Эта цифра неуклонно растет, заставляя экспертов неустанно работать над изобретением новых, более совершенных решений для защиты от злоумышленников. По словам специалистов, одна из основных проблем физической защиты банкоматов состоит в том, что всего за 1–2 минуты грабители успевают выполнить всю запланированную работу и скрыться до приезда сил реагирования. Вот пример такого преступления: банкомат прикрепляется тросом к автомобилю, вырывается с корнем, а затем в специально оборудованном месте производится его вскрытие и извлечение ценностей. Существуют и другие способы быстрого ограбления банков. Частота подобных случаев говорит о том, насколько важно в сложившихся обстоятельствах вовремя остановить преступников.

Функция Anti-Raid (мощный первый выброс дыма) создана специально для эффективной борьбы с дневными вооруженными ограблениями и введена в обновленную линейку Smoke Screen в 2013 г.

Научно-исследовательский центр «Охрана» МВД предложил решение, которое в 2014 г. будет включено в список рекомендаций по защите банкоматов по всей России. Главное преимущество системы активной защиты под названием CONCEPT Smoke Screen или «Туман безопасности» – возможность максимально быстро дать отпор злоумышленникам, смешав их планы и выбив почву из-под ног.

Результаты атомно-силовой микроскопии не выявили никаких остатков дыма Smoke Screen на тестовых образцах.
Производитель предоставляет международную гарантию в размере эквивалентном 10 млн фунтов стерлингов – дым Smoke Screen не повреждает имущество.

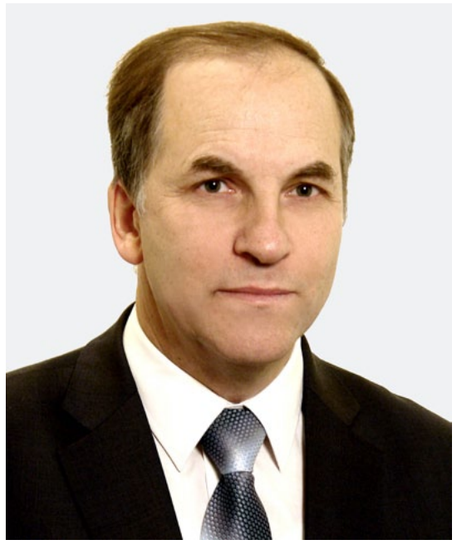
Изобретение включает в себя специальный дымогенератор, ультразвуковой барьер и ксеноновый стробоскоп. По заявлению разработчиков, в случае тревоги, получив сигнал от охранного извещателя или тревожной кнопки, установленных в помещении или охраняемом банкомате, система начнет вырабатывать в большом количестве густой белый дым/туман, который за несколько секунд полностью заполнит все помещение. Вместе с дымогенератором сработает громкая высокочастотная сирена, генерирующая так называемый «белый шум»: преступники не смогут пользоваться рацией и испытают нечто вроде «морской болезни». Специалисты сообщают, что у грабителей заложит уши, возникнет головокружение и подташнивание. Вслед за сиреной включится мощный ксеноновый стробоскоп, благодаря чему густая завеса тумана в помещении, в котором не видно собственную вытянутую руку, начнет мерцать.

В НИЦ МВД отмечают, что подобные условия помешают нарушителю ориентироваться в помещении и пространстве и не позволят ему контролировать ситуацию и совершать противоправные действия. Система начинает полноценно функционировать через 10–20 сек. после объявления тревоги и безопасна для здоровья человека. «Как показали испытания, обеспечивается эффективное противодействие попыткам совершения краж и ограблений на охраняемых объектах, в том числе попыткам взлома и хищения банкоматов и платежных терминалов», – рассказал представитель НИЦ МВД.

«Smoke Screen не сообщает об ограблении, не дает возможности его увидеть, не вызывает полицию. Smoke Screen просто останавливает это ограбление. Мгновенно», – говорится на сайте разработчика. Еще одно важное преимущество новинки – ее безопасность для человека и техники. Как отмечает компания-производитель систем, дым совершенно не оставляет осадка благодаря мельчайшему размеру генерируемых частиц и его «сухости» и не портит имущество. Кроме того, дым состоит из раствора глицерина, безопасен для контакта с электроникой, пищей, для астматиков и не имеет никаких противопоказаний при рекомендованном использовании.

Благодаря своим характеристикам новая система может найти применение не только в банкоматах, но и для защиты депозитариев и клиентской зоны при дневных вооруженных ограблениях офисов банка, в салонах ювелирных брендов, музеях, бутиках, сейфовых и кабинетах, в зонах риска (витрины, экспонаты, дисплеи, прикассовая зона) тысяч организаций, коттеджах, квартирах и гаражах, лабораториях и многих других местах.

«Безопасность не может быть дешевой»



Сергей Гордеев

Сергей Гордеев отвечает за продажи HID Global в России и странах СНГ с 2011 г.

До этого Сергей на протяжении 13 лет работал в сфере систем технической безопасности, занимал пост исполнительного директора одной из компаний.

В 1996 г. защитил диссертацию в Московском энергетическом институте, имеет ученую степень кандидата технических наук. Автор более 20 научных статей и пяти патентов.

В системах идентификации и контроля доступа безопасность стоит на первом месте. О новых концепциях и подходах к защите данных мы поговорили с Сергеем Гордеевым – региональным менеджером по продажам компании HID Global, которая стала «пионером» в области систем безопасной идентификации.

– Сергей, компания HID Global существует с 1991 года. Назовите, пожалуйста, несколько главных «прорывов» компании, произошедших в области за последние годы.

– Для начала немного истории. Компания HID Global пришла на российский рынок в 1994-1995 гг., представив новый индустриальный стандарт технологий контроля доступа HID prox 125 кГц. Фактически это тот стандарт, на котором строились и продолжают строиться в настоящее время системы контроля управления доступом. Главными преимуществами HID prox 125 кГц, способствовавшими быстрому росту популярности этой технологии на российском рынке, были высокая безопасность, приемлемая стоимость и удобство использования. Но рынок развивался и, чтобы соответствовать современным тенденциям и идти в ногу со временем, спустя несколько лет мы предложили новую, более защищенную линейку карт и считывателей iCLASS 13,56 МГц. Карты, выпущенные по этой технологии, не только обладают высоким уровнем защиты от копирования, но также могут использоваться для других приложений (доступ к компьютеру, различным корпоративным приложениям, платежи).

Однако жизнь не стоит на месте, требования к защите постоянно повышаются, и любая технология рано или поздно может устареть. Соответственно необходимо думать над тем, какие решения будут востребованы в будущем и какие будут наиболее безопасны, поскольку в ID-идентификации безопасность стоит на первом месте. Являясь «пионером» в области систем безопасной идентификации, компания HID Global разработала новую концепцию безопасности в СКУД, реализовав ее в технологии iCLASS SE. Концепция идентификации iCLASS SE обладает тремя основными преимуществами. Во-первых, информация, помещенная на карту, защищена несколькими слоями безопасности: шифрование данных, цифровая подпись и привязывание этих данных к определенному носителю (смарт-карте, NFC-телефону, USB-токену и т.д.). Второй важный момент – это возможность осуществления апгрейда систем безопасности на месте, т.е. без замены карт и считывателей. Подобный подход используется в информационных технологиях. Если раньше, когда технология устаревала, необходимо было менять само оборудование, то сегодня, используя iCLASS SE, можно осуществлять апгрейд непосредственно в процессе эксплуатации, создавая дополнительные уровни безопасности удаленно, через интернет. В-третьих, безусловно, это мобильность. Мы живем в мире, где телефон является незаменимым средством коммуникаций, и сегодня он получает очень широкие возможности. Современные смартфоны с технологией NFC могут использоваться в качестве идентификаторов для доступа в помещение или к корпоративным базам данных. Например, используя технологию iCLASS SE, в телефон можно безопасно записать информацию о разрешении или запрете доступа пользователя к тем или иным объектам. В случае утери устройства все цифровые ключи удаляются из телефона с помощью мобильного оператора. В целом можно сказать, что iCLASS SE обладает большим потенциалом в применении в системах контроля и управления доступом, являясь на сегодняшний день главным прорывом в технологиях СКУД.

– Все ли задачи, стоящие перед разработчиками решений безопасной идентификации, выполнены на сегодняшний день?

– Безусловно, все задачи, связанные с развитием решений безопасной идентификации, сразу решить невозможно. Более того, мир меняется, и нужно быть готовым к изменениям технологий, появлению новых разработок. К примеру, у HID Global весь потенциал новой линейки считывателей iCLASS SE еще не реализован до конца. Прежде всего, в iCLASS SE заложена возможность работы с устройствами, поддерживающими технологию NFC, но пройдет еще немало времени, прежде чем будут осуществлены все договоренности с производителями телефонов и операторами мобильных услуг для обеспечения возможности записи данных о доступе либо непосредственно на телефон, либо на sim-карту. Кроме того, необходимо создать также определенный портал сервисных услуг, позволяющий управлять цифровыми ключами, передавать и удалять их при необходимости.

– HID Global является поставщиком решений безопасной идентификации для миллионов заказчиков по всему миру, занимаясь разработкой систем управления физическим и логическим доступом, решений для персонализации карт, защищенных государственных удостоверений личности, технологий, используемых в устройствах для идентификации животных, а также в промышленных и логистических приложениях. Есть ли у компании приоритетное направление деятельности?

– Выделить приоритетное направление непросто, потому что все составляющие безопасной идентификации в одинаковой степени важны. Я могу сказать, что во всех сферах деятельности мы постоянно работаем над обновлениями линейки, чтобы наши решения отвечали требованиям сегодняшнего дня. Бóльший акцент делается на физический доступ, тем не менее персонализация карт также значима. HID Global активно развивает это направление, представляя принтеры для персонализации карт. В первую очередь, это серия Fargo, где можно выделить новый индустриальный принтер HDP8500, предназначенный для использования в интенсивном режиме и печати большого количества карт. Принтер HDP5000 также был обновлен в этом году: теперь он обладает более высокой скоростью печати, и гарантия на него действует в течение трех лет. HID Global также ведет разработки и в направлении логического доступа: доступа к персональным данным, к компьютеру. Разработана новая линейка считывателей OMNIKEY® для чтения смарт-карт и организации системы логического доступа.

– Какие критерии определяют направленность новых разработок Вашей компании?

– Прежде всего, наши разработки связаны с изучением рынка, и предоставляемые решения направлены на удовлетворение потребностей клиента. Поскольку сфера деятельности HID Global – это ID-идентификация, то критерием номер один, определяющим все разработки компании, является обеспечение максимальной безопасности технологий. Решения, которые мы предлагаем рынку, должны предотвращать возможные угрозы, существующие на сегодняшний день, и предвосхищать появление угроз в будущем.

– Какими Вы видите системы управления доступом в недалеком будущем?

– Несмотря на то что сфера систем управления доступом достаточно консервативна и технологические прорывы здесь происходят редко, хочу отметить несколько тенденций, которые будут определять развитие этой области в ближайшем будущем. Прежде всего, это мобильность систем идентификации, возможность помещения данных для безопасного доступа не только на карты, но и на любой другой носитель. Как я уже упоминал, это может быть и телефон, и USB-токен, и любое другое устройство. Самое главное – чтобы данные на этом носителе были надежно защищены. Второй важный момент – это возможность быстрой и безопасной передачи цифровых ключей, а также управления ими с помощью сервисного портала. Полагаю, что облачные технологии, которые сейчас широко используются в ИТ, в ближайшее время будут востребованы и в области физического доступа.

– Оборудование, производимое компанией HID Global, широко распространено во многих странах мира. Насколько отличаются потребности клиентов и, соответственно, Ваши предложения для предприятий России и зарубежья?

– Некоторые различия в предпочтениях российских и иностранных клиентов, конечно, есть. К сожалению, во многих случаях российский рынок очень чувствителен к цене. Зачастую конечные пользователи не задумываются над тем, какую технологию они закладывают в свою систему безопасности. Они действуют по остаточному принципу, стараясь уложиться в бюджет, который у них имеется. Соответственно довольно часто небольшие организации выбирают недорогую и не обеспечивающую необходимого уровня защиты технологию EM Marin. Крупные же корпорации, которые заботятся о безопасности, заинтересованы в долгосрочных инвестициях, чтобы выбранная технология не устаревала и не нужно было дополнительно платить за смену оборудования. Они более вдумчиво подходят к вопросам выбора системы и отдают предпочтение современным технологиям идентификации, понимая, что безопасность не может быть дешевой. Что касается иностранных клиентов, то на Западе общепринята система страхования имущества, и страховые компании всегда обращают внимание, насколько надежно защищены информационные и материальные ценности организации от внешних угроз. В России пока такая система не развита, поэтому часто клиент выбирает ту технологию, которая обойдется ему дешевле. Хотя в целом ситуация меняется, и общая тенденция смещается в сторону более защищенных технологий.

– Опишите типичного потребителя Вашей продукции.

– Сложно описать типичного покупателя, потому что система безопасности нужна всем так же, как пожарная или охранная сигнализация. Среди наших клиентов есть и малые организации, использующие, например, контроллеры EDGE для открытия всего одной двери, и крупные корпорации, устанавливающие более сложные системы. Так, например, все аэропорты столицы оборудованы считывателями HID Global. Новейшие технологии используются и заводами, и театрами, и крупными банками, поэтому здесь нельзя сформировать портрет типичного потребителя – это может быть любая компания, которая заботится о защите своих активов.

– Насколько мне известно, HID Global занимается реализацией заказов государственных органов разных стран мира. В чем основные отличия этих разработок от проектов, направленных на удовлетворение нужд коммерческих предприятий?

– В компании HID Global есть подразделение, которое непосредственно занимается взаимодействием с государственными структурами в различных странах. Это прежде всего работа, связанная с выпуском удостоверений государственного образца: паспорта, водительские лицензии и прочие документы. Что касается других направлений деятельности, в частности физического и логического доступа, принтеров, то с госструктурами мы работаем через наших партнеров, дилеров. Нужно сказать, что требования государственных структур несколько выше требований коммерческих организаций. Государственные учреждения проверяют наличие всех необходимых сертификатов, соответствие характеристик оборудования государственным стандартам, требованиям указов, законов и других регулирующих актов.

ON -- LINE

Прима Информ

информационный провайдинг

«Прима-Информ» - масштабный интернет-проект прямого доступа к данным ФНС, ГМЦ Росстата, ФАС, ФССП и иных ведомств. Портал позволяет пользователям оперативно получать сведения о юридических и физических лицах для проверки достоверности данных, представленных потенциальными контрагентами, деловыми партнерами, кандидатами для приема на работу, а также для решения иных информационных и аналитических задач, стоящих перед организацией.

Через портал ***www.prima-inform.ru*** Вы получаете прямой он-лайн доступ к следующим основным источникам:

- **ГМЦ Росстата РФ:** “Предприятия России”,“Балансы предприятий 2005-2010 гг.”, “Аффилированные лица: юридические и физические”, “Индивидуальные предприниматели России”, “Адреса массовой регистрации”;
- **Федеральная Налоговая Служба:** выписки из ЕГРЮЛ, ЕГРИП, “Юридические лица, в состав исполнительных органов которых входят дисквалифицированные лица”, “Адреса массовой регистрации”;

- **Федеральная Служба Судебных Приставов:** “Реестр должников - юридических лиц”, “Розыск должников - физических лиц в рамках исполнительных производств”;
- **Верховный Суд РФ:** “Справочная информация по делам”;
- **Высший Арбитражный Суд РФ:** “Картотека арбитражных дел;
- **“КоммерсантЪ” (издательский дом):** “Объявления о несостоятельности (банкротствах);
- **Правоохранительный портал “112.ru”:** проверка лиц, находящихся в розыске;
- **Федеральная Антимонопольная Служба:** “Реестр недобросовестных поставщиков”;
- **Услуга “Поиск абонента”** по номерам мобильных телефонов всех операторов мобильной связи.

Специальная партнёрская программа:

Абсолютно новое решение на рынке информационных услуг.
Интеграция сервиса информационного провайдинга на Вашем сайте.

- отсутствие переходов на сторонний сайт - это Ваш и только Ваш клиент;
- отсутствие упоминаний об источнике информации - Ваш ресурс - главный источник информации для Вашего клиента;
- вся информация о партнере - в личном кабинете Вашего клиента!

Что означает прямой доступ к ресурсам для пользователей системы:

- **оперативный доступ** - любые изменения по компании видны сразу;
- **достоверность** - информация не модерируется, не изменяется и не подвергается никакой обработке - предоставляется “как есть” от информационных источников.

Сайт: **http://www.prima-inform.ru**
e-mail: **online@prima-inform.ru**
Skype: **Prima-Inform**
тел: **+7(495) 646-34-80**

Есть тестовый доступ!

– В последнее время заметно увеличился интерес к теме биометрической идентификации, дающей дополнительные возможности по защите персональных данных. Ведет ли компания HID Global разработки в данной области?

– После того как случились печальные события, связанные с терактами, по всему миру произошел всплеск интереса к биометрии. Действительно, биометрические признаки уникальны и неповторимы. Но биометрическая идентификация имеет ряд сложностей, которые пока сдерживают активное развитие этого направления. Прежде всего, это относительная дороговизна оборудования. Второй момент – невозможность быстрого прохождения процесса идентификации: как правило, идентификация по отпечатку пальца или сетчатке глаза занимает гораздо больше времени, чем идентификация по обычной карте. Кроме того, могут возникать ошибки первого и второго рода, когда система может пропустить чужого или, наоборот, не пропустить своего. Поэтому оптимальный вариант, который мы рекомендуем, - это идентификация по двум составляющим: по карте и биометрическому признаку, который может быть помещен непосредственно в сектор памяти карты. Среди разработок HID Global есть биометрический считыватель модели bioCLASS. Это считыватель отпечатков пальцев, совмещенный со считывателем бесконтактных смарт-карт iCLASS, клавиатурой и ЖК-дисплеем, благодаря чему возможна трехфакторная аутентификация пользователя. Подобные решения широко используются нашими клиентами. В данный момент мы работаем над выпуском обновленного считывателя, который появится в продаже во второй половине этого года.

– В последние годы наметилась устойчивая тенденция к конвергенции (сближению) физического и логического доступа. Какие шаги HID Global осуществляет в этом направлении?

– Сближение физического и логического доступа является одним из главных трендов в безопасности на сегодняшний день. У HID Global существуют решения, позволяющие одновременно получать доступ и в определенные помещения, и к внутренней сети организации, используя для этого всего одну карту. Речь идет о картах Crescendo, которые имеют контактный чип и бесконтактный чип iCLASS SE для физического доступа. Это решение очень удобно и востребовано, на его основе реализовано достаточно много проектов на Западе. В России темпы пока не столь высоки: мы начали осуществлять первые проекты на базе Crescendo начиная с прошлого года, но в будущем, полагаю, эта тенденция только продолжит свое развитие.



тел. +7 (495) 507-82-80

mail@detector-online.ru

г. Москва, Мясницкий проезд, 4/3
(30 метров от метро «Красные Ворота»)

Ассоциация полиграфологов

СТОЛИЧНАЯ ЭКСПЕРТНАЯ ГРУППА

- Служебное расследование (кражи на производстве, хищения, утечка информации и т.д.)
- Проверка кандидата при приёме на работу (наркотическая, алкогольная, игровая зависимость, воровство на прошлом месте работы, проблемы с законом и т.д.)
- Периодические проверки сотрудников (лояльность фирме и руководству, нанесение ущерба организации, корыстная связь с конкурентами и т.д.)
- Проверка «супружеской верности»

Детектор лжи – для тех, кто хочет знать истину

Исследование Searchinform: Компании стали больше думать о защите данных

Максим Кикеня,
аналитик компании SearchInform

Начало 2013 года запомнилось многим россиянам инцидентом, связанным с потерей значительной суммы денег одним из банковских гигантов России и Европы – «Сбербанком». Преступной группировке, в которую, как известно, входили бывшие и действующие сотрудники финансовой организации, удалось заполучить более 50 млн рублей путем хищения средств с зарплатных карт клиентов. Данная возможность у злоумышленников появилась благодаря доступу к паспортным сведениям, информации о банковских счетах клиентов и т.д. Преступники совершили ряд незаконных финансовых операций, оформляя фальшивые доверенности. Позже злоумышленники были задержаны, однако факт уязвимости системы информационной безопасности «Сбербанка» вновь всплыл наружу. Напомним, что подобный инцидент имел место не в первый раз.

Однако не будем ограничиваться только данным примером. Давайте взглянем на ситуацию, связанную с информационной защищенностью российских компаний, более комплексно.

Как показали результаты опроса, проведенного компанией Searchinform более чем в 150 государственных и коммерческих организациях Москвы, в целом предприятия стали более ответственно относиться к своей информационной безопасности. Так, согласно статистике, число компаний, которые проводят инструктаж сотрудников для разъяснения политик информационной безопасности, увеличилось на 46% по сравнению с прошлым годом. Причинами данного скачка могли стать как ужесточение правил соблюдения безопасности информации высшими регулирующими органами, так и желание самих руководителей обезопасить себя на этом уровне.

На 80% по сравнению с прошлым годом вырос показатель предприятий, где руководители подписывают договор о неразглашении конфиденциальной информации со своими сотрудниками. В этом году об этом заявили 96% опрошенных. Данное явление можно объяснить участившимися случаями потери конфиденциальной информации в компаниях, а также нежеланием руководителей попадать в подобные ситуации. Кроме того, данные профилактические меры не требуют финансовых затрат, но в то же время служат сдерживающим фактором для недобросовестных сотрудников на психологическом уровне. Страх попасть под суд или расстаться с кругленькой суммой денег за хищение корпоративной информации может ощутимо повлиять на поведение человека.

Еще один шаг в сторону укрепления информационной безопасности руководители делают через оповещение сотрудников о наличии DLP-систем или других решений для защиты и контроля информационных потоков в компании. По данным статистики, число таких предприятий за прошедший год выросло с 17 до 43%. По мнению некоторых специалистов, подобные системы дают больше плодов, когда сотрудники не подозревают об их существовании на своих компьютерах, однако на самом деле ничто так не мотивирует не совершать глупостей, как осознание того, что за тобой пристально следят. Кроме того, работодатель, не оповестивший сотрудника о наличии подобной системы, нарушает закон, а именно права человека на неприкосновенность частной жизни, тайну переписки, телефонных разговоров и т.д., предусмотренных конституцией РФ в статье 23.

Подкрепляя вышесказанное данными статистики компании Searchinform, хочется отметить, что количество утечек информации за минувший год сократилось более чем на 20%, а число сотрудников, желающих насолить работодателю, похитив информацию, уменьшилось на треть.

Между тем можно с уверенностью сказать, что на данном этапе стремление компаний обезопасить себя от утечек информации еще не проявилось в полной мере. Случаи кражи данных по-прежнему не так уж и редки. Причем, согласно статистике, наиболее популярным объектом воровства становятся финансовые (50%), технические (31%) и персональные данные (19%). Такая информация является наиболее привлекательной для инсайдеров. Изменяется лишь процентное соотношение этих пунктов. Известно, например, что во время выборов учащаются случаи хищения персональной информации, когда ворованные паспортные данные неактивных или досрочно проголосовавших избирателей используются для подделки бюллетеней.

Кроме того, сегодня стремительный оборот набирает тенденция перевода информации в электронный вариант. Теперь, к примеру, нам не нужно стоять в длинных очередях, чтобы записаться на прием к врачу в поликлинике, достаточно предварительно зарегистрироваться в сети Интернет. Нам не нужно ехать на вокзал за билетом, мы можем приобрести его электронную версию. Доступ к информации и работа с ней становятся проще. И это, с одной стороны, облегчает нашу жизнь, а с другой – делает защиту данных более уязвимой для злоумышленников. В результате слишком стремительного внедрения электронных систем обслуживания в повседневную жизнь граждан многие из них так и остались недоработанными. Этим может воспользоваться любой злоумышленник. Как часто мы обращаемся к интернет-банкингу, чтобы оплатить коммунальные услуги или связь, оставляя в сервисах данные своих кредитных карт и другую персональную информацию? Что если завтра эти сведения станут доступны мошеннику, а наша честно заработанная зарплата превратится в ноль на пластиковой карточке? Да, ситуация неприятная.

Как показало исследование Searchinform, наиболее склонными к хищению корпоративной информации в минувшем году были представители управляющего звена. На долю менеджеров пришлось 33% краж данных. И это неудивительно, ведь термин «менеджер» стал так часто применяться к работникам управленческой сферы деятельности, что сегодня практически в каждой компании, если не во всех, есть представители данной профессии.

Второе «почетное» место занимают работники финансового сектора (22%). Стоит отметить, что понятие «инсайдер» пришло к ним именно из финансовой среды, а потому присутствие финансистов в тройке лидеров скорее укоренившаяся традиция, нежели что-то новенькое. Закрывают список самых «опасных» сотрудников IT-специалисты (11%), которые имеют широкий доступ к большому объему информации, а также могут осуществлять контроль над другими пользователями. Знания же технических аспектов компьютерных систем дает им возможность манипулировать информацией, что и является соблазном для многих представителей данной профессии.

Стоит отметить, что в последнее время возросла и степень ответственности, которую чувствуют руководители предприятий перед общественностью в случае утечки информации. Число компаний, которые в обязательном порядке сообщают своим клиентам о краже данных, выросло на 10%. Причиной этому мог послужить подъем российского бизнеса после кризиса и обостренная борьба за выбор потребителя. С приходом зарубежных инвесторов российский бизнес частично перенял западноевропейские черты, в основе которых лежит концепция заботы о потребителе.

Как бесплатно построить ИБ компании

Роман Идов,
аналитик компании SearchInform

Обеспечение безопасности данных сегодня является одной из приоритетных задач для многих коммерческих и государственных организаций. Даже одна утечка информации может принести серьезные финансовые убытки бизнесмену, а чиновника и вовсе лишить должности. Однако, осознавая ценность конфиденциальных данных и проблематику их утечки, не каждый может грамотно, а главное, эффективно выстроить барьер безопасности вокруг своей информации. Собственно о том, как защитить свои данные от утечки, и пойдет речь дальше.

Для решения проблем информационной безопасности существуют специализированные средства, например DLP-системы (от англ. Data Leak Prevention). Данные системы позволяют контролировать информационные потоки компании, передаваемые посредством электронной почты, веб-браузеров, интернет-мессенджеров, Skype, внешних носителей (USB/CD/DVD) и т.д. DLP-системы анализируют потоковые данные, выходящие за черту защищаемой информационной зоны. При обнаружении в информационном потоке конфиденциальных данных срабатывает компонентная система, и передача данных блокируется. Однако внедрение DLP-системы на предприятии – удовольствие недешевое, поэтому некоторые руководители вынуждены отказываться от него. Но что делать, если защищать корпоративные данные нужно, а средств на внедрение полноценной DLP-системы нет?

В этом случае многие компании предпочитают выстраивать информационную безопасность своими силами. Однако стоит понимать, что качество и эффективность собственноручно выстроенной системы ощутимо отличаются от того, что могут предложить специализированные средства. Тем не менее наличие хоть какой-нибудь системы защиты данных на предприятии лучше, чем ее полное отсутствие.

Давайте рассмотрим базовый комплекс мер, который необходим для обеспечения информационной безопасности в условиях, когда хочется сэкономить. Прежде всего, руководство должно задуматься о том, какая информация представляет наибольшую ценность для компании. Ведь защищать «то, не знаю что» крайне нерационально. Также может возникнуть банальное желание защищать все. Однако, как показывает практика, добиться этого крайне сложно даже крупным и обеспеченным организациям. В противном случае, взяв широкий размах, вашей компании просто не хватит средств, чтобы завершить начатое дело. Если же определить ценность документов для вас составляет трудность, попробуйте представить, что может случиться с компанией, если какие-либо из них будут похищены. Какая именно утечка способна нанести компании наибольший вред? Именно эти сведения и являются для вас наиболее ценными!

После того как перечень особо важных документов определен, стоит разработать политику информационной безопасности, разграничивающую права доступа к конфиденциальным данным между сотрудниками, а затем провести соответствующий инструктаж. В данном документе должен быть обозначен список конфиденциальных документов, сотрудники, имеющие право доступа к ним, уровень доступа, возможные варианты угроз и методы защиты от них. Сам процесс создания подобной «бумаги» не должен вызывать у вас трудностей: посмотрите аналоги в Интернете, примеры подобных документов не являются редкостью. Адаптировав найденную инструкцию под свои нужды, можно получить готовую политику информационной безопасности.

Следующий шаг – составление должностной инструкции на основе политики безопасности, которую в идеале должны подписать все сотрудники. Не лишним будет провести зачет среди персонала, тогда инструкция надолго останется в памяти людей. Для профилактики подобный инструктаж стоит повторять с определенной периодичностью, например раз в один-два месяца.

Следующим шагом на пути строительства информационной безопасности станет разграничение доступа персонала к документации. Настроив права доступа в любых штатных системах, используемых компанией (CRM, бухгалтерский учет, СЭД и пр.), выполнить поставленную задачу не составит труда. Однако стоит помнить, что подобное разграничение необходимо настроить для всех информационных систем, так как в противном случае созданная система безопасности будет недостаточно эффективной.

Еще одним важным этапом в обеспечении безопасности информации является защита корпоративной сети и рабочих станций сотрудников от угроз из внешнего мира. Можно, конечно, прибегнуть к использованию специализированных средств, но мы не будем отклоняться от темы и продолжим разговор о бесплатных методах. Удивительно, но очень многие предприятия страдают из-за утечек данных только потому, что не используют межсетевой экран или вовсе забывают установить пароль доступа к офисной сети Wi-Fi. Для начала стоит позаботиться хотя бы об этом. В противном случае даже малоопытному злоумышленнику хватит навыков в IT-сфере, чтобы похитить корпоративные секреты.

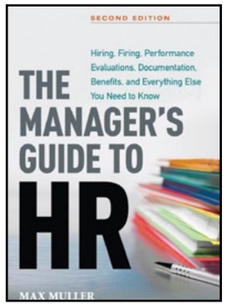
После того как офисная сеть будет защищена паролем, стоит задуматься о межсетевом экране – комплексе программных средств, осуществляющем контроль и фильтрацию проходящих через него сетевых пакетов по заданным правилам. Для нашей задачи можно использовать такие бесплатные версии межсетевых экранов, как Astero, ClarkConnect, ZoneAlarm Free Firewall и т.д. Однако данными примерами ограничиваться не стоит, так как существует масса других как бесплатных, так и платных вариантов.

Не менее важным этапом построения системы информационной зашиты на предприятии является разработка и внедрение правил кадровой безопасности. Не стоит принимать на работу тех сотрудников, которые уже были отмечены в инцидентах, связанных с утечкой информации. Нужно понимать, что переманивание сотрудников у конкурентов может дать не только положительный результат, но и привести к негативным последствиям. Так, например, в перспективе данному сотруднику могут предложить заработную плату больше, чем вы в состоянии ему платить, и тогда все ваши корпоративные секреты уйдут вместе с перебежчиком.

Кроме того, безопасность информации зависит не только от средств ее поддержания, но и от самого рабочего коллектива. Поэтому развивайте в компании культуру информационной безопасности, напоминайте сотрудникам о том, что их благосостояние зависит от успешного функционирования всей организации. И если компания теряет конфиденциальные данные, то это отражается на ее деятельности, а затем и на сотрудниках. Коллектив, проникшийся идеей важности обеспечения ИБ, будет работать внимательнее, а случайные инциденты (например отправка важного документа неверному адресату) сократятся.

Соблюдение вышеуказанных правил позволит снизить риск утечки конфиденциальных данных и защитить информацию от чужих рук. Конечно, стоит понимать, что данные методики не гарантируют полный контроль информационного трафика, но в качестве «фундамента» информационной безопасности подходят хорошо. В будущем же, конечно, стоит задуматься и о внедрении профессиональных систем информационной защиты.

КНИГИ



1. Макс Маллер. Руководство по управлению персоналом: наем, увольнение, оценка деятельности, документация, пенсии и многое другое (Max Muller. The Manager's Guide to HR: Hiring, Firing, Performance Evaluations, Documentation, Benefits, and Everything Else You Need to Know).

Язык: английский.

Дата выхода: 15 августа 2013 г.

Управление персоналом требует от менеджера мастерства и определенной сноровки. Умение разбираться в тонкостях кадровой политики – важное качество для руководителя предприятия. Первое издание этой книги, увидевшее свет несколько лет назад, подробно знакомит читателя с правилами найма, увольнения сотрудников, ведения документации и пр. Однако жизнь не стоит на месте. Предлагаемое издание учитывает произошедшие изменения и рассказывает:

- о влиянии, которое оказывают на процесс рекрутинга социальные медиа;
- об изменении трудовых стандартов за последнее время, включая премирование сотрудников и выплаты пенсий;
- о правилах обеспечения внутренней безопасности на предприятии;
- Законе о пенсионном обеспечении работников (Employee Retirement Income Security Act);
- Законе о предоставлении отпуска по болезни и семейным обстоятельствам (Family and Medical Leave Act);
- Законе об американцах-инвалидах (Americans with Disabilities Act);
- комплаенс-контроле.

2. Натали Иви. Как провести внутреннее расследование. Практический гид для HR-специалиста (Natalie Ivey. How to Conduct Internal Investigations: A Practical Guide for Human Resource Professionals).

Язык: английский.

Дата выхода: 24 июля 2013 г.

Руководство содержит не только рекомендации по проведению внутренних расследований, но и обзор превентивных мер, которые помогут снизить риски нарушений на предприятии. В книге описывается, как противостоять враждебности в коллективе, проявлениям дискриминации, злоупотреблению законом о предоставлении отпуска по болезни и семейным обстоятельствам, кражам корпоративного имущества, некорректному поведению сотрудников и многим другим традиционным проблемам. Благодаря описанным приемам читатель сможет улучшить свои навыки проведения интервью со свидетелями и сократить время принятия критически важных решений.

Автор Натали Иви имеет квалификации MBA и SPHR, является основателем и президентом компании Results Performance Consulting. RPC была создана в 2002 г., основными направлениями ее деятельности являются кадровый консалтинг и организация обучения для специалистов по рекрутингу.

3. А. Попов. Производственная безопасность.

Язык: русский.

Дата выхода: 2013 г.

В учебном пособии представлены общетеоретические, правовые и организационные основы производственной безопасности, проанализированы методы и средства предупреждения производственного травматизма в растениеводстве, животноводстве, при выполнении погрузочно-разгрузочных работ, транспортном обслуживании, ремонте сельскохозяйственной техники, эксплуатации сосудов высокого давления и систем газоснабжения и газопотребления. Автор рассматривает основы электро- и пожарной безопасности.

Книга предназначена для студентов высших учебных заведений, обучающихся по направлению «Техносферная безопасность». Может быть полезна инженерно-техническим работникам сельскохозяйственных предприятий.

4. Э.В. Пьядичев, В.С. Шкрабак, Р.В. Шкрабак, О.А. Хорошилов. Пожарная безопасность.

Язык: русский.

Дата выхода: 2013 г.

Книга знакомит читателя с основами пожароопасности веществ, материалов, жидкостей и газов, основами процессов горения и их физическими моделями, категорированием зданий и наружных установок, систем пожарной сигнализации и взрывозащиты, способами и средствами тушения пожаров на промышленных и сельскохозяйственных предприятиях с целью профилактики пожаров, их локализации и тушения.

Работа предназначена для студентов вузов. Содержит материалы, которые будут полезны специалистам в области пожарной безопасности.

5. А.В. Бабаш, Е.К. Баранова, Д.А. Ларин. Информационная безопасность. История защиты информации в России.

Язык: русский.

Дата выхода: 2013 г.

Авторы книги обращаются к истории отечественной криптографии IX–XX вв. В пособии подробно разбираются вопросы зарождения и становления российского криптоанализа, особое внимание уделяется виднейшим специалистам в этой сфере, а также личностям, связанным с криптографией, – революционерам, разведчикам. Работа содержит ссылки на многие исторические документы. Цель издания – популяризация криптографического подхода к защите информации и всестороннее ознакомление студентов профильных вузов с историческими предпосылками в данной области.

Работа предназначена для студентов высших учебных заведений (бакалавриат, магистратура), обучающихся по направлению информационной безопасности и прикладной информатики, а также для всех интересующихся криптографией.

12[Я] МЕЖДУНАРОДНАЯ ВЫСТАВКА

HI-TECH BUILDING

29-31 октября 2013
Экспоцентр

www.hitechbuilding.ru

- **ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ:**
  - ВИДЕОНАБЛЮДЕНИЕ
  - ОХРАННОЕ ТЕЛЕВИДЕНИЕ
  - КОНТРОЛЬ, УЧЁТ И УПРАВЛЕНИЕ ДОСТУПОМ
  - ОХРАННО-ПОЖАРНАЯ СИГНАЛИЗАЦИЯ
  - МОНИТОРИНГ СОСТОЯНИЯ ИНЖЕНЕРНЫХ КОНСТРУКЦИЙ
- **АВТОМАТИЗАЦИЯ ЗДАНИЙ**
- **СИСТЕМЫ «УМНЫЙ ДОМ»**

16+

НАЦИОНАЛЬНАЯ ПРЕМИЯ
HI-TECH BUILDING AWARDS
www.htb-awards.ru

Реклама

Купон на **БЕСПЛАТНОЕ** посещение выставок **HI-TECH BUILDING 2013** и **Integrated Systems Russia 2013**

12-я Международная выставка

HI-TECH BUILDING 2013

Москва, Экспоцентр, пав. 1 и ФОРУМ

Время работы:

29 октября: 11.00 – 18.00

30-31 октября: 10.00 – 18.00

Конференции:

- «Интеллектуальное здание»
- Форум KNX «Применение мобильных платформ (IOS, Android) в проектах KNX»
- «Умный Дом»
- «Энергосберегающие технологии в строительстве – PASSIVE HOUSE»

Проекты:

- **УМНЫЙ ДОМ** – экскурсии по жилым помещениям «**Умного Дома**»
- **PASSIVE HOUSE. GREEN BUILDING**
- **HI-TECH BUILDING AWARDS** – национальная премия по оснащению коммерческой и жилой недвижимости

www.hitechbuilding.ru

Безопасность: информационное обозрение

Организатор

MIDexpo МЕЖДУНАРОДНЫЕ ВЫСТАВКИ И ЯРМАРКИ

При поддержке

KNX · BIG-RU BACnet Interest Group · enocean alliance · LONMARK Rus · CABA · GREEN BUILDING COUNCIL RUSSIA