www.securityinfowatch.ru

№7 апрель 2013

БЕЗОПАСНОСТЬ

информационное обозрение

Тема номера

Безопасное обучение персонала

18+

БЕЗОПАСНОСТЬ:
информационное обозрение
№ 7 апрель 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

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

Обучение персонала – путь к безопасности бизнеса

Все мы помним этот момент, когда придя со студенческой скамьи во «взрослую жизнь» – во время производственной практики или при первом трудоустройстве по полученной специальности – понимаешь, что знаний и навыков, обретенных в стенах родного вуза, явно недостаточно для быстрого и качественного исполнения своих обязанностей. Мы молоды, уверены в себе, целеустремленны, а начальство не доверяет нам важных поручений, отдавая предпочтение нашим старшим коллегам, да и сами себе на их фоне мы кажемся медлительными и неумелыми.

Как говорится, все приходит с опытом. Иногда проблемы новичков в компании решаются сами собой – по истечении определенного времени, благодаря общению с другими работниками, непрерывной практике и активному самообразованию. В некоторых случаях требуется дополнительное обучение. Всевозможные семинары и курсы повышения квалификации помогают не только вчерашним студентам освоиться в профессии, но и позволяют актуализировать знания опытным сотрудникам. Технологии не стоят на месте – тем, кто работает в сфере безопасности, полезно постоянно помнить об этом.

В предыдущих номерах мы поднимали очень важную сегодня проблему обеспечения кадровой безопасности предприятия. На этот раз мы решили поговорить об обучении персонала. Регулярное повышение квалификации, переподготовка сотрудников, взаимодействие и обмен опытом с представителями разных подразделений компании и других предприятий, осуществляющих деятельность в той же сфере, не только увеличит объем знаний, профессиональную компетентность работников, но и будет способствовать построению надежной системы защиты бизнеса.

Чего не хватает выпускникам вузов для удачного трудоустройства? Как проверить подлинность диплома соискателя? Кто должен оплачивать обучение – сотрудник или работодатель? Кого предпочитают нанимать производители ПО для защиты информации? Эти и многие другие вопросы задавали себе наши авторы, работая над этим выпуском журнала. Надеемся, полученные нами ответы будут вам полезны.

Адель Соколова

Тема номера

Кто должен оплачивать обучение - сотрудник или работодатель?

«КОШАЧЬИ БОИ». КОГДА В ЭПИЦЕНТРЕ КОНФЛИКТА ЖЕНЩИНЫ.

24

УЧЕНЫЕ СОЗДАЛИ КАРМАННЫЙ РЕНТГЕНОВСКИЙ АППАРАТ.

10

НОВОСТИ

Россияне против «большого ока»

Видеокамеры наружного наблюдения нервируют сотрудников. К такому выводу пришли социологи исследовательского центра рекрутингового портала Superjob.ru. Так, каждый четвертый работник (26% опрошенных) относится к наличию видеонаблюдения с неудовольствием, поскольку оно нарушает личное пространство человека и свидетельствует о недоверии руководства компании к своим работникам. Установку камер видеонаблюдения в офисах одобряют 23% респондентов. В числе плюсов они называют исключение офисного воровства, «слива» служебной информации и отсутствие в офисе посторонних.

Интересно, что во мнениях насчет камер не сошлись у сотрудников разного пола и возраста. Одобряют работодателей, использующих видеокамеры, чаще мужчины, чем женщины (27% против 19%), а также респонденты старше 45 лет (32%). И, наоборот, гораздо тяжелее смириться с постоянным наблюдением бывает женщинам (27%), а также молодежи до 24 лет (29% противников камер).

Разнятся также ответы руководства компаний и сотрудников отдела кадров. Менеджеры по персоналу одобряют видеонаблюдение в офисах, называя его целью обеспечение безопасности работников (41%), контроль над работой сотрудников (34%), охрану имущества и информации, а также предотвращение хищений (23%). Несколько реже упоминались контроль посетителей (5%), защита интересов компании в судебных спорах и другие задачи (по 3%). Большинство сотрудников (47%) утверждают, что им все равно, ведется ли в их офисе видеонаблюдение, однако они никогда не забывают о наличии камер.

Kaspersky Lab представила новое решение для бизнеса

Лаборатория Касперского представила новое решение Kaspersky Endpoint Security for Business (KESB) для обеспечения корпоративной безопасности. Презентация состоялась в Нью-Йорке. Выпуск нового решения ознаменовал выход компании, воспринимаемой как игрока в секторе B2C, на консервативный корпоративный рынок.

Компания позиционирует Endpoint Security for Business как решение для защиты всех видов устройств, имеющих хождение в корпоративном секторе. Оно обеспечивает мониторинг, управление и защиту мобильных устройств, входящих в корпоративную сеть, в том числе и удаленное; криптографическую защиту файлов, удаленный менеджмент корпоративной сети и т.п.

Кроме того, KESB способно ограничивать использование внешних устройств при подключении к корпоративным ПК, блокировать запуск подозрительных программ, поддерживает «черные списки» и защиту от опасных ссылок. В Лаборатории Касперского рассчитывают, что Endpoint Security for Business позволит компании занять третье место на рынке интернет-безопасности, объем которого сейчас, по данным Forbes, составляет около 64 млрд долл.

DARPA разрабатывает «параноидальные» военные сети

Агентство передовых оборонных исследовательских проектов (DARPA) сообщило о запуске проекта по разработке нового типа военной компьютерной сети. Новая беспроводная сеть будет обладать мощной защитой от вредоносных программ, хакерских атак и будет с подозрением исследовать все непредвиденные изменения в процессе обмена данными.

Протоколы беспроводных коммуникационных устройств, объединенных в сети, используемые военными, часто требуют развертывания узлов для координации и управления сетевыми ресурсами. Проблема в том, что компонентам сети приходится «доверять» отдельным узлам поступающей информации и всей сети в целом. Следовательно, вторжение хакеров противника в боевую сеть может целиком вывести ее из строя. Для решения этой проблемы DARPA планирует разработать сеть, которая сможет функционировать, несмотря на случайное или злонамеренное нарушение работы отдельных узлов.

Специалисты DARPA планируют модернизировать нынешние и будущие компьютерные сети таким образом, что они научатся определять жизнеспособность и надежность соседних узлов, блокировать их и адаптировать сеть, сохраняя ее работоспособность. Таким образом, планируется достичь защиты всей сети целиком, а не каждого отдельного узла.

Опытные сотрудники реже конфликтуют

Большинство конфликтов на работе вызвано неотлаженными бизнес-процессами и неэффективной системой коммуникаций в компании. К такому выводу пришла служба исследований компании HeadHunter, занимавшаяся изучением конфликтов на работе. В опросе приняли участие 5718 работников компаний. Немалая доля респондентов (41%) указала, что всему виной объективные причины, ведь несоответствия взглядов, мыслей и идей никак не избежать. Свою лепту также вносят несоблюдение работодателем ТК (17%) и личная неприязнь к коллегам (13%).

По мнению 32% опрошенных, конфликты, с которыми им приходится сталкиваться, чаще всего носят деструктивный характер, так как они обостряют межличностные отношения и тормозят рабочий процесс. Еще больше респондентов (38%) утверждают, что даже те разногласия, в которых они не участвуют, мешают их работе, поскольку сбивают настрой, отвлекают и заставляют нервничать. Перепалки коллег отвлекают от дел (35%), заставляют нервничать (27%) и портят настроение, убивая всякое желание плодотворно трудиться (56%). Вместе с тем стоит отметить, что далеко не все конфликты приносят вред: так, по словам 32% опрошенных, рабочие конфликты нередко приводят к возникновению новых идей и выбору лучшего решения, поэтому идут только на пользу рабочему процессу.

При выполнении служебных задач работники в большинстве случаев стараются полагаться только на себя (79%). Такие люди чаще способны на применение физической силы в конфликтной ситуации, нежели те, кто не прочь обратиться к сторонней помощи. При этом абсолютное большинство опрошенных заявило, что не допускает для себя применение физической силы в конфликтной ситуации. Примерно 17% опрошенных допускают рукоприкладство для разрешения спора, однако чаще как ответную реакцию на соответствующие действия соперника. Тем не менее 13% готовы адекватно ответить обидчику, позволившему себе рукоприкладство, 3% способны помахать кулаками в случае, если их сильно выведут из себя, и 1% предупреждает, что в подобной ситуации может просто не сдержаться. В исследовании отмечается, что применение физической силы в конфликтной ситуации чаще позволяют себе мужчины, нежели женщины.

В соответствии с результатами опроса более половины сотрудников оказываются втянутыми в конфликт не реже раза в месяц, а 16% работников сталкиваются с подобными ситуациями на работе каждый день. Большинство работников компаний в конфликтной ситуации стараются действовать конструктивно, добиваясь компромисса в решении задач. Эксперты отмечают, что опытные специалисты чаще идут на уступки и пытаются прийти к совместному решению проблемы в конфликтной ситуации, нежели новички.

Врач отмечал коллег накладными пальцами

В больнице Samu бразильского города Ферраз-де-Васконселус недалеко от Сан-Паулу один из врачей использовал силиконовые пальцы для того, чтобы отмечать прогуливающих коллег. Полиция изъяла шесть поддельных пальцев с отпечатками, которые 29-летняя Соана Нунес Ферейра прикладывала к специальному датчику, где врачи отмечают свое присутствие.

Всего в афере участвовали по меньшей мере 20 медсестер и 11 врачей, но, по словам мэра города Эйкара Филу, в различных ведомствах около 300 человек получают свою зарплату, вообще не ходя на работу. Филу назвал их «армией призраков» и подчеркнул необходимость поиска «мертвых душ» во всех государственных учреждениях, включая здравоохранение, безопасность и образование.

Соана Нунес Ферейра долгое время находилась под наблюдением правоохранительных органов и была задержана с поличным. После разоблачения доктор дала признательные показания и сообщила, что она действительно фальсифицировала посещение врачей и работников больницы, «пробивая» силиконовые отпечатки пальцев в биометрической машине, которая засчитывает часы работы. Также доктор рассказала, что действовала не по собственной инициативе: это было условием ее трудоустройства – она должна была заниматься «пальцами», иначе потеряла бы работу.

СОБЫТИЯ

ISSE INTEGRATED SAFETY & SECURITY EXHIBITION
МЕЖДУНАРОДНЫЙ САЛОН
КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ

1. «Комплексная безопасность / ISSE-2013», 21–24 мая 2013 г.

Место проведения: Россия, Москва, ВВЦ, павильон № 75.
Сайт: www.isse-russia.ru

VI Международный салон средств обеспечения безопасности «Комплексная безопасность / ISSE-2013» представляет собой крупнейшую демонстрационную площадку, посвященную вопросам комплексной безопасности и входящую по составу участников в перечень наиболее представительных европейских выставок в данной области. В рамках деловой программы запланированы презентации, коллегии, совещания руководителей тыловых и технических служб МВД и МЧС России, конференции и семинары партнеров Салона.

В работе Салона примут участие руководители Российской Федерации, ведущие специалисты Минобороны России, Рособоронзаказа и других федеральных органов исполнительной власти. Обширна и международная программа Салона, который посетят делегации из США, Канады, Малайзии, ОАЭ, Иордании, Китая, Польши, Ирана, Турции, Республики Беларусь и др. Ожидается, что Салон, в котором примут участие более 500 экспонентов из 20 стран мира, посетят более 20 тыс. посетителей.

АНТИТЕРРОР современные системы безопасности

2. «Современные системы безопасности — Антитеррор», 29–31 мая 2013 г.

Место проведения: Россия, Красноярск, МВДЦ «Сибирь».
Сайт: www.krasfair.ru.

«Современные системы безопасности — Антитеррор» — это специализированный форум и выставка систем и средств безопасности, охраны и противопожарной защиты, милицейской и криминалистической техники, аварийно-спасательного оборудования. Организаторы мероприятия – Национальный антитеррористический комитет, аппарат полномочного представителя президента Российской Федерации в Сибирском федеральном округе, администрация губернатора Красноярского края, Правительство Красноярского края, антитеррористическая комиссия Красноярского края, администрация Красноярска и выставочная компания «Красноярская ярмарка».

Помимо традиционных разделов форума в этом году уделяется особое внимание вопросам безопасности топливно-энергетического комплекса. В деловой программе мероприятия будут освещены вопросы организации комплексной безопасности и антитеррористической защиты в различных аспектах (охранное тепловидение, системы видеонаблюдения, пожарная безопасность, пропускные пункты и т.д.) с учетом отраслевой специфики – особенностей охраны таких объектов ТЭК, как атомные, тепловые и гидроэлектростанции, объекты инфраструктуры газонефтяного комплекса.

Разделы выставки:
- Технические средства и системы безопасности.
- Инженерно-технические средства физической защиты.
- Пожарная безопасность и средства безопасности при чрезвычайных ситуациях.
- Аварийно-спасательное оборудование.
- Транспорт -услуги в области безопасности.
- Экипировка. Индивидуальные средства защиты — информационная безопасность.
- Специальные системы связи и управления.
- Безопасность промышленного комплекса.

В программе:
- Научно-практическая конференция «Обеспечение безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса».
- Круглый стол «Защита конфиденциальной информации и персональных данных».
- Круглый стол «Противодействие этнорелигиозному экстремизму и развитие взаимопонимания в молодежной среде».
- Обучающие площадки «Детский городок безопасности».

«Охрана и безопасность 2013»

3. «Охрана и безопасность». «Пожарная безопасность», 29–31 мая 2013 г.

Место проведения: Россия, Тюмень,
Выставочный зал Тюменской ярмарки.
Сайт: www.expo72.ru.

Основные разделы выставки:
- Оборудование, технические и специальные средства для служб охраны, безопасности и защиты правопорядка, пожарной и аварийно-спасательной службы.
- Системы контроля и ограничения доступа.
- Средства и системы предупреждения пожаров и пожаротушения.
- Автоматизированные установки сигнализации и пожаротушения.
- Спецтехника: пожарная техника, бронированные автомобили, спецплавсредства.
- Огнетушащие вещества и механизмы тушения.
- Профессиональная, специализированная, специальная одежда.
- Ведомственная и корпоративная одежда.
- Спецобувь и средства индивидуальной защиты.

Выставка сопровождается показами, деловой программой, широкой информационной поддержкой. Ежегодно мероприятие собирает до 100 экспонентов из разных регионов России. В 2012 г. выставку посетили более 4000 человек – это частные лица, представители власти, руководители и специалисты профильных организаций Тюменской области, соседних городов Уральского федерального округа.

ACFE Association of Certified Fraud Examiners — Together, Reducing Fraud Worldwide

4. Мероприятия Российского отделения ACFE в 2013 г.

Место проведения: Россия, Москва.
Сайт: www.acfe-rus.org.

Темы тренингов:
• Этика ведения бизнеса и ее аудит: основной курс для внутренних аудиторов.
• Аналитические способы выявления хищений.
• Профессиональные навыки проведения интервью.
• Основы проведения расследований для аудиторов.
• Внутренний аудит для службы безопасности.
• VIII ежегодная конференция «Обеспечение безопасности бизнеса в российских компаниях» (октябрь 2013 г.).

Продолжительность тренингов: 2 дня (теория и практика). Лектор – Сергей Мартынов, президент российского отделения ACFE. Квалификации CFE, CISA, CIA, профессиональный бухгалтер (Россия), имеет более чем 15-летний опыт работы во внутреннем аудите, управлении рисками, комплаенс и расследовании хищений на предприятиях топливно-энергетического комплекса и в консалтинге.

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

Ученые создали карманный рентгеновский аппарат

Алексей Степанов

«Рентгеновские аппараты, применяемые в настоящее время, имеют очень большие размеры и значительное энергопотребление. Примерно через три года на основе нашего изобретения мы создадим прототип ручного рентгеновского сканера». Скотт Ковалевски (Scott Kovaleski), доцент в области электрической и компьютерной инженерии из Университета Миссури.

«Наше устройство абсолютно безвредно во время зарядки энергией, и даже после насыщения уровень радиационного излучения остается относительно низким. На настоящий момент это первый прибор подобного плана, который можно включать и выключать. Изобретение имеет огромный потенциал применения». Скотт Ковалевски

Сегодня места большого скопления людей, в частности аэропорты и вокзалы, оснащены вполне эффективными сканерами, способными обнаруживать опасные предметы. Однако эти устройства довольно громоздки и потребляют значительное количество энергии. Созданием портативного рентгеновского сканера озаботились ученые Университета Миссури (University of Missouri, США), разработавшие источник электромагнитного излучения величиной со спичечный коробок или упаковку от жевательной резинки.

По утверждению исследователей, приблизительно через три года на основе этого изобретения будет создан компактный рентгеновский аппарат, который будет востребован в ряде отраслей в первую очередь в безопасности и медицине. Сообщается, что новый ручной сканер может быть использован при поиске дефектов в конструкциях, для проведения обследования багажа, или в космической технике, в частности в марсоходах.

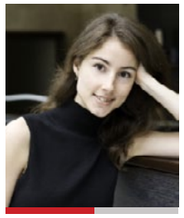
В устройстве использован кристалл, вырабатывающий более 100 тыс. вольт электроэнергии с низким питающим напряжением около 10 вольт. Благодаря низкому уровню энергопотребления, кристалл может заряжаться даже от батареек. Новая разработка основана на кристаллах ниобата лития, которые обладают пьезоэлектрическими свойствами и при механической нагрузке вырабатывают электрический заряд. Таким образом, исследователи надеются, что в будущем им удастся существенно увеличить мощность излучателя: экспериментальная модель смогла поднять напряжение с 10 вольт до 100 тыс. вольт. Разработчики не исключают, что в случае если мощность излучателя удастся еще повысить, данное изобретение наверняка заинтересует военных и представителей спецслужб, поскольку пьезоэлектрический рентген-излучатель может стать мощным скрытным оружием, способным даже убивать.

Кристаллы ниобата лития являются источником рентгеновского излучения, из них извлекается энергия вибрации в виде высоковольтного электронного пучка, тормозящегося металлической пластинкой, которая и производит рентген-излучение. Важным является и то, что в выключенном состоянии портативный источник рентгеновского излучения абсолютно безопасен. Данная особенность позволит заменять им радиоактивные изотопы, ныне широко используемые в различных современных контрольных приборах.

По некоторым данным уже в 2016 г. американские полицейские и врачи получат компактные рентгеновские установки.

Алексей Дрозд: «Вузы уделяют самой важной теме всего 15 минут»

Поскольку темой этого номера журнала «Безопасность: Информационное обозрение» стало обучение кадров, среди его героев оказались специалисты известных компаний, уделяющих большое внимание подготовке молодых сотрудников. Руководитель направления по работе с вузами компании SearchInform Алексей Дрозд рассказал нашему изданию, зачем нужно дополнительное обучение студентов профильных учебных заведений, и чем выгодно подобное взаимодействие. Наша встреча с Алексеем произошла во время его однодневной командировки из Киева в Москву.



Интервью подготовила и провела Адель Соколова

- Доброе утро, Алексей! Как долетели?

- Хорошо, но чувствую себя, конечно, уставшим.

- С вузами каких стран сотрудничает компания Searchinform?

- На данный момент помимо России активная работа ведется на Украине и в Беларуси – более чем в 30 вузах. Есть определенный задел и в Казахстане, но о конкретных результатах пока рано говорить. На названных же странах наше внимание было сфокусировано изначально. Идея сотрудничества Searchinform с вузами зародилась примерно три года назад. Тогда стало очевидно, что из года в год большое число потенциальных сотрудников крупных компаний защищают дипломы, не имея при этом ни надлежащего опыта работы, ни практических навыков. В результате рынок получает вчерашних выпускников с высокими амбициями и ожиданиями по заработной плате, но без какого-либо ценного с практической точки зрения «багажа». Естественно, подобное положение работодателей не слишком радует.

Осознав это, мы прежде всего попытались установить контакт с вузами, в которых представлены наши специализации – экономическая безопасность, защита информации и т.д. Первым вузом, с которым была достигнута договоренность о сотрудничестве, стал Южно-Уральский государственный университет. В Белоруссии нам удалось наладить отношения с двумя топовыми вузами – Белорусским государственным университетом (БГУ) и Белорусским государственным университетом информатики и радиоэлектроники (БГУИР). У нас также есть немало потенциальных партнеров. Например, в России мы могли бы начать сотрудничество с учебными заведениями Хабаровска и Владивостока, но препятствует банальная разница во времени, которая порой создает значительные помехи для делового общения.

- Вы хотите сказать, что университетского образования недостаточно соискателям для успешной работы по специальности?

- Дело в том, что в вузах скорее дают костяк знаний, основы, не углубляясь при этом в конкретные решения. Мешает этому инерционность самой учебной программы. Поверьте, не так просто внести в нее изменения. Чему сегодня хорошо учат в вузах? Криптографии, высшей математике, тензорному анализу и т.п. Но там не готовят профессиональных пользователей, потребителей, а ведь на работе совсем не обязательно постоянно «изобретать велосипед», важно также иметь представление об уже существующих программах. Когда мы обращаемся в вузы с предложением прочитать курс лекций, посвященный нашей продукции, иногда нам отвечают, что студентам важнее научиться самим создавать подобные комплексы. Преподаватели забывают о том, что потребность в сотрудниках такого уровня намного ниже, чем в обычных специалистах по информационной безопасности, которым необходимо иметь представление и уметь работать с тем, что сегодня представлено на рынке ИБ.

Приведу простой пример различия наших с педагогами взглядов на существующие реалии. В вузах часть дисциплин посвящена антивирусной защите. При этом чуть более узкая тема DLP (систем защиты от утечек конфиденциальных данных) практически не затрагивается. В лучшем случае за весь курс обучения ей посвящается не более 15 минут обзорной лекции. Мировой же опыт показывает, что решения класса Data Loss Prevention являются достаточно востребованными. Их предлагают такие известные в отрасли компании, как Symantec, Websense и McAfee. В России момент осознания бизнесом необходимости DLP-систем настал примерно в 2008 г., когда грянул финансовый кризис, и терявшие работу сотрудники старались унести из компаний любую информацию, которая могла бы оказаться им полезной на новых рабочих местах или при поиске работы, например клиентские базы. Тогда-то директора поняли, что деньги надо считать, а внутренние сведения беречь как зеницу ока.

Так сложилось, что функция обслуживания DLP-систем традиционно лежит на техподдержке вендора. Однако в случае с нашей продукцией, на них же накладываются дополнительные обязанности по обучению специалистов информационной безопасности работе с нашим софтом. Оно и понятно: в сети информации подобного рода нет, а значит, качественно и быстро разобраться с системой без посторонней помощи не получится.

- Каким образом осуществляется взаимодействие с вузами?

- Мы разработали многоуровневый курс. Первая ступень состоит из шести лабораторных работ, которые знакомят студентов с одной, но самой востребованной темой – аналитическими возможностями нашей DLP-системы. Поясню. Вся информация на предприятии (от FTP, принтеров, Интернета и других контролируемых каналов) поступает в автоматизированный аналитический

центр под названием AlertCenter. Он, в свою очередь, занимается выявлением различных нарушений в зависимости от заданных настроек и регистрирует инциденты. Например, отдав команду искать в переписке слово «взятка», вы в автоматическом режиме получите уведомление обо всех сообщениях, в которых оно упоминалось.

Наша компания существует с 1995 г. и она с самого начала занималась разработкой корпоративного поисковика. Этакий Google в рамках отдельно взятого предприятия. За шесть лабораторных работ студенты проходят основные поисковые алгоритмы: фразовый поиск, поиск похожих (это наш собственный алгоритм), поиск по цифровым отпечаткам, по регулярным выражениям, атрибутивный поиск и т.д. Лабораторные работы рассчитаны на «массового потребителя» и предназначены для студентов 3–4 курсов в зависимости от пожеланий вуза. Они специально были написаны так, чтобы студенты могли даже самостоятельно дома их «прокликать»: там очень много скриншотов и подробных пошаговых инструкций.

- Для чего же тогда требуется Ваше присутствие на занятиях? Вы могли бы продавать эти лабораторные всем желающим.

- Мы не работаем с вузами на коммерческой основе, мы стараемся расширить кругозор будущих специалистов, за что они нам очень благодарны. Другое дело, что студент, имея мощный личный компьютер, может забрать ту или иную часть работы домой. Для того чтобы студенты понимали, зачем им нужно дополнительное обучение, нами проводится вводная полуторачасовая лекция. Именно на ней доступным языком рассказывается, что сейчас происходит в мире инфобеза, как действуют злоумышленники, почему с ними нужно бороться и, главное, какими средствами. С занятий многие выходят реально заинтересованными, с горящими глазами. Тем более, если студент пройдет все ступени обучения, ему может быть выдан сертификат Searchinform, для получения которого необходимо сдать довольно сложный экзамен. Это связано с тем, что обучение у нас бесплатное, и если мы будем раздавать направо и налево наши «корочки», никакой ценности они представлять не будут. Мы заинтересованы в том, чтобы обладатель нашего сертификата при устройстве на работу, так сказать, не посрамил нас. Как показала практика, получить сертификат «на халяву» изначально желают многие, однако серьезно поработать и обрести новые знания способен далеко не каждый.

- Зачем вашей компании нужно проводить бесплатные занятия со студентами?

- Придя после вуза работать в ту или иную компанию, бывшие студенты уже будут хорошо знакомы с нашими решениями. Наша выгода очевидна. При этом мы не рассказываем на лекциях, какая хорошая компания Searchinform или ее продукция. Поверьте, это не самореклама. Мы рисуем реальную ситуацию, объясняем, к примеру, кто такие социальные инженеры, чем они занимаются, что такое DLP-системы, каких видов они бывают, зачем они нужны и какие задачи способны решать, приводим статистику утечек по России, найти которую самостоятельно непросто. Читая отчеты, публикуемые даже известными изданиями, я порой прихожу в ужас от того, насколько указываемые в них цифры не соответствуют действительности. Отдельное внимание на наших занятиях уделяется законодательным вопросам, знание которых особенно важно для будущих сотрудников банков. Мы также участвуем в процессе написания студентами дипломных и курсовых работ.

- Каким образом вы участвуете в их подготовке?

- Мы предоставляем студентам техническую информацию по их темам. Где им еще ее достать?

- А с трудоустройством можете помочь?

- Хорошим студентам мы можем предложить удаленную работу на внештатной основе. У нас сейчас так работают 2 человека из Киева. Мы, конечно, не можем взять к себе всех желающих, нам просто не нужно такое количество сотрудников.

- Какие задания можно поручить молодому специалисту, не имеющему большого опыта работы?

- Он может, например, наполнять базу с инцидентами, проводя их поиск и категоризацию. Грубо говоря, будет «Аналитик 1 левела».

- Существует ли в России дефицит квалифицированных кадров в сфере информационной защиты?

- Наблюдается дефицит в IT-отрасти в принципе и в сфере безопасности в частности.

- С какими проблемами при трудоустройстве может столкнуться выпускник вуза?

- Часто молодые специалисты, не имеющие опыта работы, рассчитывают на высокие зарплаты, которые им никто не хочет предлагать. С этим, пожалуй, связано главное разочарование за стенами родного вуза. Если посмотреть исследования компании HeadHunter, то среднее предложение от работодателей по Москве для «безопасников» – 50 тыс. руб.

- Это мало?

- Нет, но выпускник же хочет сразу 100. Многие из-за зарплаты идут работать не по специальности. И это проблема не конкретного взятого вуза или специальности.

- Каковы возможные пути решения данной проблемы?

- Частично ее удается решать за счет профильных мероприятий, например конференций. Так, в Киеве каждый год проводится конференция Ukrainian Information Security Group Conference, на мой взгляд, очень полезная и для студентов. Там они могут пообщаться с представителями крупных компаний – потенциальных работодателей, спросить, какие именно знания и навыки потребуются им для работы в той или иной сфере или организации. Другое дело, что таких полезных мероприятий не так уж и много. Часто они платные, что является значительным препятствием для студентов.

- Вы имеете опыт преподавания в вузах разных стран. Где, на Ваш взгляд, лучше готовят специалистов по информационной безопасности?

- По уровню технических знаний, безусловно, Москва в лидерах. Но сильные, талантливые студенты есть во всех вузах. Кстати, мы работаем не только со студентами, но и с действующими специалистами. В частности, в декабре 2012 г. к нам на стажировку в Минск приезжали 11 человек из Тверского государственного университета. А в январе к нам приезжали два специалиста из Новосибирского государственного университета. Пройдя в течение недели стажировку, они смогли потом заниматься дополнительным обучением своих коллег в Новосибирске.

- Алексей, где предприятию найти хорошего специалиста в области информационной безопасности?

- Хороший вопрос! Дело в том, что большинство компаний хотят получить в свои ряды специалистов уже с опытом работы. Обучение молодых сотрудников чревато тем, что они, получив необходимые знания, уйдут работать в другую организацию. И тогда компания потеряет вложенные в обучение средства. В Белоруссии существует распределение, т.е. выпускник, получивший бесплатное образование, обязан два года отработать там, куда его направили. Возможно, это и неплохая практика.

- Алексей, спасибо Вам за интересные ответы.

Путевки в жизнь. Бизнес на бланках

Наталья Елина

Востребованность высшего образования объяснить легко. Многие работодатели полагают, что человеку с вузовской подготовкой, привыкшему справляться с большими объемами заданий и решать сложные задачи, не надо объяснять детали производственного процесса. Он сам задаст наводящие вопросы, сам изучит вспомогательную информацию, да еще и оптимизирует процесс. Таким образом, вчерашний студент при должном уровне подготовки вполне может стать спешным управленцем, занять достойное место в компании, сколотить свою команду и даже возглавить подразделение. К сожалению, в погоне за быстрыми деньгами молодые люди иногда забывают о поговорке «встречают по одежке, провожают по уму» и рассчитывают, что смогут создать себе деловую репутацию без надлежащей теоретической подготовки. Криминальный рынок услуг уже давно сориентировался в веяниях и потребностях рынка труда и предлагает дипломы любого образца – синие и красные «корочки», заполненные и нет, самых престижных вузов страны и небольших областных институтов...

Приобретение диплома об окончании высшего учебного учреждения не всегда совершается из желания блеснуть заветной корочкой. Случается, что человек сначала устраивается на работу в конкретную компанию и лишь затем, получив некий опыт работы, задумывается над покупкой диплома. С одной стороны, как кадр он гораздо ценнее, чем обычный выпускник вуза, не имеющий за спиной нескольких лет практики. С другой, покупка диплома – это преступление, за которое человек может понести наказание – от выплаты денежного штрафа до лишения свободы на несколько месяцев.

Даже при наличии малейших сомнений в подлинности диплома работодателю следует задуматься, насколько ему дорог конкретный сотрудник и готов ли он простить ему огрехи молодости. Или же, наоборот, найти таким образом причину, чтобы избавиться от не слишком расторопного работника.

Глобальная липа

Дипломы подделывают во всем мире, так что эта проблема имеет поистине глобальные масштабы. Однако в некоторых странах с ней практически справились, использовав современные технические возможности. Так, американские работодатели без лишнего труда используют общую интегрированную базу данных по выпускникам, окончившим образовательные учреждения (Integrated Postsecondary Education Data System), которая ведется Национальным центром по статистике образования. В Великобритании подлинность диплома можно проверить в онлайн-режиме посредством систем HEFCE и BIS, а также Datacheck (HEDD), разработанных по поручению британских университетов и колледжей. В Финляндии существует агентство «Статистика Финляндии», которое ведет два регистра: завершенного образования и степеней (Register of Completed Education and Degrees). Единая электронная база дипломов работает с начала 2012 г. и на Украине, причем, по заверению министра образования и науки, молодежи и спорта Дмитрия Табачника, проверка занимает не более 15 минут.

С 1994 г. все дипломы государственного образца, выдаваемые в РФ, имеют утвержденный приказом Минобразования России вид и многочисленные типографские степени защиты. В частности, на левой стороне бланка диплома видны слова «Россия» и «Диплом». Кроме того, на копии, произведенной копировально-множительным аппаратом, проявляется слово «Копия». На левой стороне бланка видно полное название Министерства просвещения или Федерального агентства по образованию, набранное очень мелким шрифтом, а также слово «РФ».

В России разговоры о создании и внедрении электронной базы данных для проверки подлинности дипломов о высшем образовании ведутся с 2005 г., когда Минобразования РФ инициировало начало разработки информационной системы. В настоящее время проектом создания Федерального реестра выпускников высших учебных заведений занимается Центр бюджетного мониторинга Петрозаводского государственного университета

(ПетрГУ). Ввод в действие пилотной версии базы данных намечен на текущий 2013 год.

По утверждениям разработчиков макета реестра, он будет вестись по всем уровням профессионального образования (высшему, среднему и начальному). База будет содержать в себе следующие сведения: ФИО и иные паспортные данные выпускника, код заведения по Общероссийскому классификатору предприятий и организаций и его наименование, год окончания и специализацию/направление профессии, серию и номер диплома, а также дату его выдачи. Кроме того, в базу будут внесены первое место трудоустройства специалиста, данные о наименовании организации, ИНН и должность, которую занимал выпускник в компании.

Пока же отечественные работодатели, которые не принадлежат к государственным структурам, вынуждены проверять дипломы соискателей либо используя личные каналы информации в силовых ведомствах, либо путем официальных запросов через вузы. Официальный путь верификации диплома – самый долгий (от 1 до 7 месяцев) и чаще других заканчивается ничем, поскольку часто вузы просто-напросто отказываются предоставлять информацию коммерческим предприятиям, ссылаясь на соблюдение политики конфиденциальности. Кроме всего прочего мошенники, подстраховываясь от возможных проверок, выбирают недавно закрытые или реорганизованные вузы, архивы которых – все равно что дно Марианской впадины…

Как пекутся «корочки»

Подделка диплома может осуществляться разными способами. Специалисты говорят о двух основных методах. В первом случае в процессе участвуют недобросовестные работники вузов или типографий, которые имеют доступ к изготовлению собственно корочек, а также к процессу подготовки и выдачи дипломов. Таким образом, государственные бланки дипломов действительно подлинные, но вот данные, внесенные в них, – заведомо фальшивые, как и удостоверяющие подписи и печати.

Во втором случае своими дипломами с мошенниками добровольно или принудительно делятся реальные выпускники вузов, а те впоследствии вносят в них фальшивые сведения путем подчисток и дописок. Следовательно, верификация диплома может носить разный характер – иногда сам соискатель дает согласие на проверку, иногда в вуз направляется запрос, а иногда, при наличии следов подделки, работодатель вправе провести экспертную проверку документа через правоохранительные органы. В последнем случае проверка проводится прокуратурой, а вердиктом становится экспертное заключение и справка из вуза, выданная по запросу правоохранительных органов. Вместе с тем надо учесть, что у прокуратуры есть дела и поважнее, чем проверка сотрудников коммерческих предприятий, поэтому в заявлении в этот орган работодатель должен обосновать свои подозрения к данному диплому и предоставить веские причины с целью аргументировать запрос.

А был ли мальчик?

Как было сказано выше, верификация дипломов соискателей на должности в государственные учреждения и крупные коммерческие компании происходит по своим законам. В прочих случаях, когда проверка подлинности диплома представляет некоторые трудности – надеемся, временно – прежде чем предпринимать какие-либо действия, опытные кадровики просто сообщают соискателю о необходимости проверки документов о его образовании. Зачастую одного этого уже достаточно для того, чтобы работник тем или иным образом выдал себя. Между тем работодатель имеет полное право и заявить о проверке, и провести ее – в соответствии со статьей 86 «Общие требования при обработке персональных данных работника и гарантии их защиты» Трудового кодекса Российской Федерации. Сам факт несогласия работника на запрос в учебное заведение уже может рассматриваться как косвенное подтверждение его недобросовестности.

Стоимость диплома начинается от 10–20 тыс. рублей. «Сопровождение» диплома, т.е. подтверждение его данных сотрудниками вуза в случае запроса – от 70 тыс. рублей. Стоимость диплома с подписью ректора, официальными печатями и внесением в университетский реестр варьируется от 500 тыс. до 1,5 млн рублей.

Некрупные компании больше ориентируются на наличие практических результатов соискателя и на рекомендации от его предыдущих работодателей, а потому в этом случае подлинность диплома не критически важна. Другое дело если возникают сомнения в подлинности и рекомендаций – тогда сверки предоставленных соискателем данных не избежать.

По оценке МВД, на сегодняшний день в России по поддельным дипломам работают не менее 200 тыс. человек. По опросам центров изучения общественного мнения, в РФ 30% дипломов фальшивые.

Официальная проверка выглядит следующим образом: после получения запроса из компетентного органа уполномоченный работник вуза выполняет сверку регистрационных номеров распоряжений о поступлении человека на факультет и сличает подписи педагогов, поставленные на допуске к защите дипломного проекта. Если всё в порядке, то проверка на этом заканчивается, но в случае обнаружения несовпадений работник вуза обязан запросить архив.

Есть один вид проверок, к которому работодатели в отсутствие электронной базы данных прибегают все чаще – это просмотр вузовских групп в социальных сетях, где можно удостовериться, что соискатель на самом деле существовал, или навести о нем справки у его однокурсников. Правда, возможность такой неформальной проверки может быть осуществлена в отношении недавних выпускников – сеть «Одноклассники», к примеру, была основана всего лишь в 2006 г.

Согласно опросу фонда «Общественное мнение» 11% пожилых респондентов, 22% участников среднего возраста и 35% молодых людей полагают, что при определенных обстоятельствах покупка диплома о высшем образовании вполне допустима.

Ваше мнение и комментарии присылайте по адресу

info@csc.ru

Кто должен оплачивать обучение – сотрудник или работодатель?

Сергей Свитлимский

Сегодня мы живем в мире, скорость развития и движения вперед которого растет с каждым днем. Непрерывно появляются всё новые и новые технологии, методики и способы эффективного решения различных задач, оптимизируются старые. Неудивительно, что также растут и требования к квалификации соискателей при найме на работу и уже работающих на предприятии сотрудников. Поэтому специалисты различного профиля, особенно те, кто работает в наиболее динамично развивающихся областях (например телекоммуникация и связь) заинтересованы в улучшении и актуализации знаний и повышении своих профессиональных навыков. В большинстве случаев различные способы самостоятельного обучения имеют немного преимуществ, так как не позволяют в полном объеме освоить новую, зачастую достаточно сложную информацию в короткие сроки. Оптимальным решением в данной ситуации становится прохождение необходимого курса в соответствующем учебном заведении (тренинг-центре, центре повышения квалификации и т.п.), заключительным этапом обучения в котором становятся сдача итогового экзамена и получение соответствующих дипломов и сертификатов.

Стоит отметить, что в России, в отличие от стран Европы и США, где сертификация и повышение квалификации сотрудников все чаще осуществляются за счет предприятия, данный аспект расходов и политика обучения сотрудников все еще представлены слабо. Отсутствует понимание важности данного процесса, и зачастую новое оборудование и другие технологии, внедряемые на предприятии, не предусматривают обучения, или предоставляются сотрудникам на самостоятельное освоение.

С точки зрения сотрудника как специалиста и отдельно взятой личности все достаточно просто. В данном случае решение об инвестировании денег и времени в свое будущее, знания и карьеру каждый принимает сам. Также требование к обладанию какими–либо специфичными или конкретными знаниями диктует отрасль, рынок труда. Зачастую беглый анализ вакансий по соответствующему профилю способен определить перечень необходимых сертификатов, которыми должен обладать соискатель при приеме на работу.

Сегодня в среде молодых специалистов все бóльшую популярность приобретает получение второго высшего образования или прохождение различных курсов в тренинг-центрах. Это обусловлено возрастающей конкуренцией и потребностью в высококлассных специалистах, которых не нужно дополнительно обучать после принятия на работу, появлением и последующим развитием тренинг-центров при вузах, а также наличием достаточно крупных скидок на обучение и последующую сертификацию для студентов.

Что же касается уже работающих кадров, то тут обучение без отрыва от производства может осуществляться либо во время отпуска, либо в вечернее или другое свободное от работы время. К сожалению, оба варианта не являются оптимальными. Время отпуска имеет ограниченные рамки и не позволяет проходить длительные курсы (например длиной в полтора и более месяцев). При этом не происходит непосредственно самого отдыха от рабочего процесса. Освоение материала после окончания рабочего дня также не является эффективным, так как в этом случае отвлекающим фактором является усталость, что не может не сказываться на качестве освоения материала.

Стимулирующим фактором для сотрудника может стать то, что его обучение происходит за счет предприятия. В таком случае необходимо выделить несколько важных для работодателя пунктов:

1. Необходимость обладания сотрудником определенными знаниями или их последующего получения могут и должны быть сформулированы на стадии планирования вакантных должностей и доведены до сведения соискателей. В перечне требований к кандидатам должны быть указаны сертификаты и другие документы, подтверждающие наличие важных для работодателя знаний. Стоит отметить, что на данном этапе необходимо точно определить, являются

ли знания, подтвержденные сертификатами, действительно необходимыми или желательными. В случае необходимости четко сформулированные требования с точными названиями сертификатов указываются в тексте. Важно понимать, что если обучение требует значительных финансовых затрат для потенциального соискателя, это скорее всего отразится на его требованиях по заработной плате. В случае если наличие таких знаний желательно, но не обязательно, владение соответствующими навыками указывается в графе желательных требований.

2. На этом же этапе следует определиться, необходимы ли компании уже готовые специалисты или она обладает ресурсами для самостоятельного «выращивания» высококвалифицированных кадров. Во втором случае возможность прохождения обучения за счет предприятия является хорошим мотивирующим фактором. Сертифицированное обучение может пройти один сотрудник, который впоследствии передаст знания другим на рабочем месте, или же целая группа сотрудников.

3. В случае если работодатель закупает крупную партию оборудования или другой сложной продукции, требующей дополнительной квалификации, вендором могут быть предоставлены бесплатные ваучеры на обучение.

4. Логичным решением может стать децентрализация получаемых знаний. В этом случае на обучение отправляются сотрудники разных отделов, которые могут впоследствии обмениваться друг с другом полученной информацией. При использовании данного подхода практически исключена ситуация, когда при увольнении сотрудника все полученные знания «уходят» вместе с ним, а предприятие терпит убытки (особенно если обучение было дорогостоящим и требовало дополнительных расходов на дорогу и проживание работника).

Предотвратить неприятные ситуации, связанные с увольнением сотрудников, прошедших курс повышения квалификации, может заключение дополнительного договора на обучение или внесение соответствующих изменений в трудовой договор сотрудника, согласно статье 197 ТК РФ.

В данном договоре должна быть в явном виде прописана следующая информация:

- даты начала и окончания обучения;
- предполагаемая цель обучения;
- тип документа, который получит работник по окончании обучения за оговоренное время (диплом, сертификат об окончании курсов и т.п.);
- стоимость обучения и документы, ее подтверждающие;
- обязанности сотрудника пройти обучение и затем проработать, согласно трудовому договору, определенный период времени, оговоренный с работодателем;
- условия, по которым будет производиться возмещение работодателю затрат в случае увольнения сотрудника без уважительной причины или до окончания срока отработки за оговоренный период времени.

В соответствии со статьей 249 ТК РФ работник обязан возместить затраты работодателя на обучение в случае увольнения без уважительной причины до окончания срока отработки. Уважительными причинами, согласно российскому законодательству, являются:

- Перевод одного из членов семьи на работу в другую местность, направление мужа или жены на работу (службу) за границу или переезд.
- Болезнь, препятствующая продолжению работы или проживанию в данной местности.
- Случаи крайней необходимости ухода за инвалидами I группы или больными близкими (если это подтверждено соответствующими документами).
- В случае избрания на должности, замещаемые по конкурсу.
- При зачислении в вуз, среднее специальное учебное заведение, аспирантуру или призыве на военную службу.
- Нарушение работодателем коллективного или трудового договора.
- Наступление чрезвычайных обстоятельств, препятствующих выполнению трудовых обязательств, например стихийные бедствия, катастрофы или военные действия.
- Выход на пенсию.

Дополнительно рекомендуется указать все другие уважительные причины в трудовом договоре или договоре на обучение. Также следует определить сумму и перечень возмещаемых затрат, включая расходы на проезд, проживание, питание и учебные материалы. В том же ключе следует оговорить и возмещаемые затраты в случае посещения работником различных кратковременных учебных мероприятий: тренингов, конференций, семинаров.

Ваше мнение и комментарии присылайте по адресу

info@csc.ru

«Кошачьи бои». Когда в эпицентре конфликта – женщины

Наталья Литова

Ученые Университета Британской Колумбии в Канаде огласили результаты исследования в области менеджмента, которое показало, что конфликты между женщинами являются наиболее разрушительными для офисной жизни. Проведя опрос 152 сотрудников различных компаний, исследователи Лия Д. Шеппард (Leah D. Sheppard) и Карл Акино (Karl Aquino) убедились в том, что спор двух дам может иметь более тяжелые последствия, нежели расхождение во взглядах между мужчинами или мужчиной и женщиной.

Участникам исследования предлагалось рассмотреть воображаемые конфликты, развивающиеся при одних и тех же обстоятельствах. Разница состояла в том, что в одних случаях в центре событий оказывались некие Адам и Стивен, в других – Адам и Сара и в-третьих – Сара и Анна. Опрашиваемым предлагалось оценить вероятность того, что в ходе последующей совместной работы этим сотрудникам удастся восстановить нормальные отношения. Респонденты неизменно признавали ссору между женщинами наиболее опасной и чреватой неприятными последствиями.

Пытаясь выяснить причины негативного отношения именно к женским спорам, ученые выдвинули ряд предположений. «Конфликты между женщинами нарушают некие неписаные социальные нормы, от женщин обычно не ожидают участия в конфликтных ситуациях. Конечно, мы понимаем, что женщины могут вести себя агрессивно, относиться друг к другу со злобой. Это может быть, но всем кажется, что так быть не должно», – комментирует Лиа Шепард.

Синдром пчелиной матки

Рассматривая конфликты между женщинами, западные исследователи используют выражения «кошачьи бои» и «синдром пчелиной матки». Если первым пренебрежительно характеризуются обычные склоки между женщинами-коллегами, то вторым ученые «окрестили» явление, когда начальницы чаще оказывают помощь в продвижении по службе коллегам противоположного пола. По мнению исследователей, за «синдромом пчелиной матки», помимо соревновательного момента, скрывается стремление женщин вписаться в круг коллег-мужчин и компенсировать таким образом существующее между ними неравенство. Ни для кого не секрет, что даже в современном мире руководящие позиции чаще всего распределяются между мужчинами, а потому делиться опытом и советами с представителями противоположного пола для женщины – способ почувствовать себя наравне с ними.

«В прессе не раз говорилось о том, что из женщин получаются лучшие управленцы, так как они оказывают большую поддержку коллегам, отличаются ответственностью и способствуют развитию карьеры подчиненных, особенно женщин, работающих под их крылом. На самом деле, все обстоит иначе, и основную заботу со стороны начальниц получают мужчины», – считает профессор Дэвид Маум. В то же время ученые полагают, что подобное поведение женщин впоследствии может крайне негативно отразиться на их здоровье.

Впрочем, есть и иная точка зрения. Например, профессор Кэрри Купер из Университета Ланкастер считает, что, продвигая по служебной лестнице мужчин, дамы стараются избежать обвинения в корпоративной женской солидарности. При этом осознание негативного отношения общественности к женским конфликтам может удержать некоторых представительниц прекрасного пола от желания принять участие в выяснении отношений на рабочем месте.

Свое открытие относительно женских конфликтов на рабочем месте исследователи из Университета Британской Колумбии собираются использовать в борьбе с гендерными предубеждениями. Лия Д. Шеппард и Карл Акино полагают, что осведомленность в вопросах конфликтов пойдет только на пользу женщинам – вероятнее всего, они будут пытаться разрешать разногласия более мирными способами.

Искусство делового общения

Иногда для начала конфликта на рабочем месте достаточно небольшого разногласия в интересах или взглядах, неправильного распределения работы между сотрудниками (когда один завален ответственной работой, а другой успевает читать онлайн-журналы и общаться в социальных сетях), распространении информации о различиях в заработной плате людей, занимающих примерно одинаковые позиции. Случается, что в коллектив приходит «эмоциональный садист» – человек, получающий удовольствие от создания конфликтных ситуаций и участия в офисных «боевых действиях». Часто причиной недоразумения становится отсутствие у коллег навыков делового общения, неумение изложить свою точку зрения и адекватно отреагировать на замечания окружающих.

Когда «обстановка накаляется», психологи рекомендуют воспользоваться некоторыми нехитрыми приемами, которые помогут свести конфликт в коллективе на нет.

1. Остановите спор хотя бы на 10 секунд. Дайте время себе и своему оппоненту успокоиться.
2. Дышите глубоко и медленно.
3. Используйте юмор. Представьте себе комичную ситуацию, это развеселит вас и поможет избежать скандала. Обычная улыбка может предотвратить конфликт.
4. Подумайте о том, что вашим оппонентом может двигать чувство обиды. Возможно, у него проблемы в семье или со здоровьем, и он позволил себе перейти черту делового общения неосознанно.
5. Будьте вежливы. Если чувствуете, что не в силах сдержать свой гнев, на время удалитесь в другое помещение.
6. Слушайте собеседника. Проанализируйте, что конкретно вызывает у вас отрицательные эмоции, и старайтесь обсуждать с собеседником только это, не касаясь его личных качеств.
7. После конфликта, вне зависимости от его исхода, необходимо признать, что ситуация исчерпана, и восстановить с оппонентом нормальные деловые отношения.

Ваше мнение и комментарии присылайте по адресу

info@cse.ru

«Всегда быть в маске – судьба моя...»

Наталья Елина

Главным отличием Фердинанда Уолдо Демары (1921–1982) от всех остальных граждан, зарабатывающих на жизнь нечестным путем, является удивительный факт: этого человека не интересовало материальное благополучие. Все невероятные вещи, которые он совершал бóльшую часть своей жизни, диктовало ему совершенно иное чувство, нежели корыстолюбие. Сложись его жизнь иначе, он наверняка стал бы великим артистом, но, с другой стороны, свою порцию аплодисментов он получил сполна.

В погоне за тенью

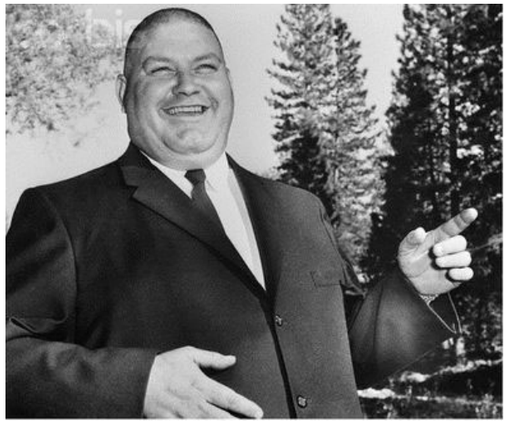
Отец Фреда, Фердинанд Уолдо Демара-старший, имел славную работу: он был оператором в кинотеатре, которым владел его дядя, Наполеон Луи Демара, а заодно был активным членом профсоюза. Дела семейства шли прекрасно – Демара жили в самом престижном районе города Лоуренс (штат Миссисипи), в собственном доме, имели большой штат прислуги, ни в чем не нуждались и были ревностными прихожанами католической церкви. В 4-летнем возрасте Фред был представлен слугам как молодой хозяин и с тех пор именовался не иначе как «мистер Демара».

Но в начале 1930-х годов с наступлением Великой депрессии, семья разорилась и была вынуждена переехать из великолепного особняка в центре города в небольшой домик на самой его окраине. Юного Фреда больно ранило пренебрежение, с которым рабочие выгружали их вещи из грузовика и переносили в новое жилище, но еще сильнее огорчила его потеря статуса: из хозяина жизни он в мгновение ока превратился в ничтожество… Он делал отчаянные попытки выделиться из массы одноклассников, по-прежнему искал особого к себе отношения. Позднее он вспоминал, что скопил денег, отказывая себе во всем, на лаковые туфли и тайком надевал их перед самой школой, а еще угощал весь класс на день святого Валентина дорогими шоколадными конфетами. Это был его первый опыт перевоплощения: он надевал на себя маску человека, который успешнее других, чтобы приподняться в первую очередь в своих собственных глазах.

Таких нехитрых приемов ему хватило ненадолго: еще через пару лет стало очевидно, что семейству Демара не вернуться в большой богатый дом, и тогда Фред сбежал. Какие чувства руководили им? Возможно, стыд – стыд перед знакомыми, которые, видя его, каждый раз вспоминали, как низко он однажды пал, и от этого стыда он бежал так далеко, как только мог, – в цистерцианский монастырь. Что происходило за монастырскими стенами – тайна, покрытая мраком. Известно только одно: какими бы ни были его планы, монастырские стены не смогли укротить его честолюбивые устремления. Демара бросился в другую крайность – ему было уже 20 лет, и, раз уж ему не удалось достичь победы над своей душой, он возжаждал побед ратных – и поступил на службу в армию.

Суета сует

Увы, армейская жизнь слишком однообразна, а для того чтобы получить высокое звание и начать вершить судьбы, нужно пролить немало пота и крови. Все это показалось юному Фреду



чересчур опасным и утомительным, и он, присвоив имя своего армейского товарища, дезертировал. Монастырь принял обратно своего блудного сына, но через год Демара прозрел: не армия, а флот был его призванием!.. Во флот его также приняли, ведь по документам дезертиром он не числился. Но спустя год Фред Демара бежал и оттуда, причем для этого ему пришлось инсценировать самоубийство.

На этот раз он не стал возвращаться в монастырь, а представился религиозно ориентированным психологом и открыл частную практику. Немало этим занятиям способствовали его наблюдательность, феноменальная память на детали и высокий уровень интеллекта, благодаря чему молодой человек легко находил общий язык с любым человеком и всем нравился. Но едва он вошел во вкус, как на него обратило внимание ФБР, и Фреду Демаре пришлось прервать все гражданские занятия по причине полуторагодичного тюремного заключения.

Смогло ли наказание образумить молодого человека и заставить его поискать более праведные пути, например получить образование или устроиться на работу? Скорее, наоборот. Во время работы психологом, предшествовавшей заключению, Демара познакомился с молодым талантливым хирургом Джозефом Кайром, и тот так впечатлил его, что наш герой в следующий раз решил представиться именно им.

Подвиги доктора Кайра

Последующие приключения Демары начались с того, что он выехал на территорию Канады, подделал документы и в качестве канадского подданного британской короны был с радостью принят на должность военного хирурга на эсминец «Каюга». Эсминец участвовал в боевых действиях во время Корейской войны (1950–1953), так что Фреду Демаре и в самом деле пришлось регулярно выполнять должностные обязанности хирурга и весьма успешно. Наиболее заметными в его «хирургической практике» стали операции 16 раненых, доставленных на «Каюгу».

Во время того, как пациентов выгружали на корабль и готовили к операции, Демара закрывался у себя в каюте и штудировал учебник по общей хирургии. Феноменально, но все оперированные (причем речь шла и об обширном ранении грудной клетки) выжили! С инфекциями самозваный доктор так же легко расправлялся при помощи щедрого количества пенициллина.

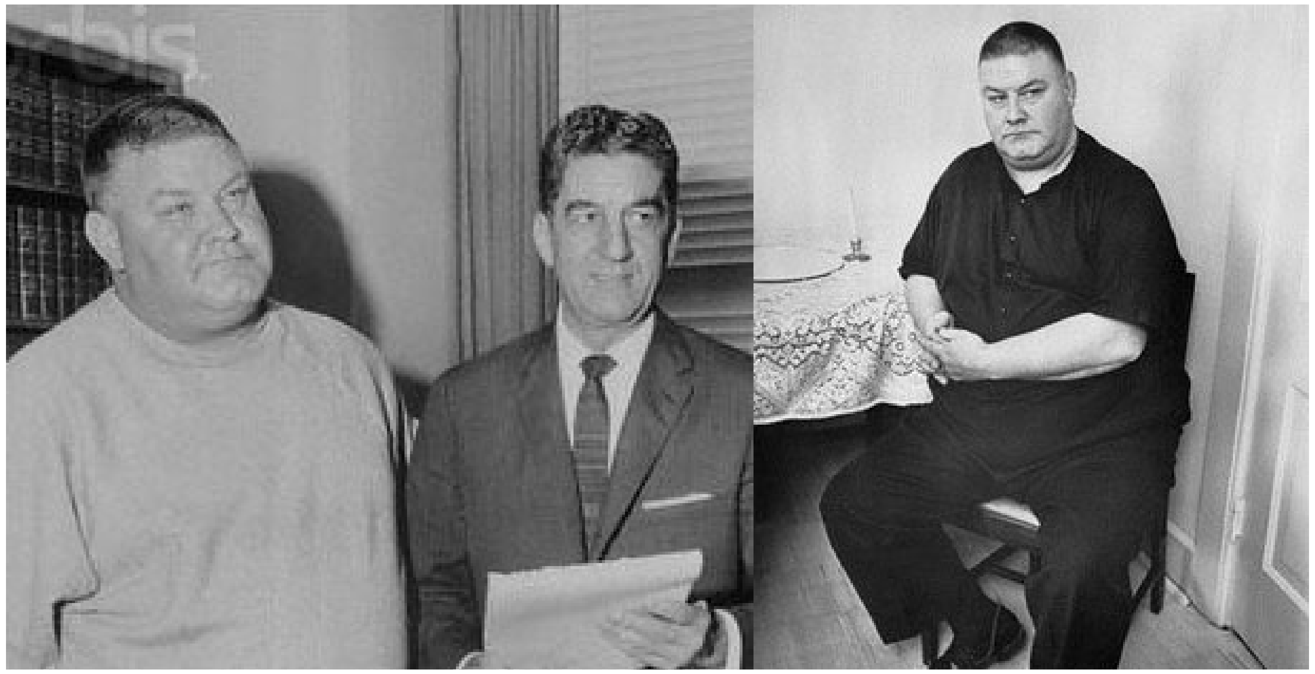
Подвела «доктора» самонадеянность: его статью об удачном опыте извлечения пули прочитала мать реального доктора Кайра, который в это время работал в канадском Гранд-Фолс (провинция Нью-Брансуик). Миссис Кайр незамедлительно обратилась в полицию, и новости достигли «Каюги», когда эсминец еще нес дежурство у берегов Кореи. Капитан судна был так потрясен известием, что долгое время отказывался верить в то, что перед ним действительно самозванец, а не жертва наговора. Не исключено, что в результате именно его заступничества ВМС Канады решили не выдвигать обвинения, и Демара смог безнаказанно вернуться в Соединенные Штаты.

У него ничего не было за душой, поэтому он решил немного подзаработать на собственной славе и продал свою историю журналу Life. В лучах славы он искупался, но находить объекты для перевоплощения после этого стало значительно сложнее: Демара обладал примечательной внешностью – высокий здоровяк весом более 150 кг – и многим запомнился. Тем не менее, вновь подделав документы, он поступил на службу… охранником в тюрьму в Техасе. Меньше чем через месяц он получил повышение за умение мирно улаживать опасные конфликты и стал помощником главного надзирателя особо охраняемого крыла тюрьмы. Мошенника сдал другой мошенник: один из заключенных нашел в старом номере журнала Life статью с фотографией Демары…

Следующим этапом его «карьеры» стало преподавательство: под именем Мартина Годгарта он учительствовал на острове Норт-Хейвен (штат Мэн), обучая детей английскому, французскому, латыни, а заодно возглавляя отряд скаутов и заведуя воскресной школой. Он пробыл там всего один учебный год, но успел влюбить в себя всех, с кем только познакомился, а потому его арест стал для населения острова настоящим шоком. Жители Норт-Хейвен уговорили судью отпустить Демару на свободу и даже предприняли попытку убедить представителей закона позволить ему продолжить учить их детей.

Последнее прибежище

За 40 лет своей мошеннической карьеры Фердинанд Уолдо Демара сменил не один десяток личностей, побывав, кроме монаха, доктора психологии и хирурга, еще и адвокатом, редактором, онкологом, преподавателем, специалистом по уходу за детьми, инженером-строителем, помощником шерифа и пр. Единственная роль, ко-



торая оказалась ему не по зубам, была реальной киноролью – Демара не смог лицедействовать по заказу, когда ему была предложена совсем небольшая роль врача-хирурга.

В 1960 г. Роберт Кричтон написал книгу «Великий самозванец» о жизни Фердинанда Демары, по которой был снят одноименный фильм с Тони Кертисом в главной роли. Зрители приняли фильм прохладно – им не понравилось, что здоровяка Демару играет красавчик-плейбой Кертис, зато психологи всего мира от личности Великого Самозванца до сих пор в восторге. Фердинанд Уолдо Демара, сам того не ведая, был необычайно одарен по части социальной инженерии, хотя сам он описывал свои приемы как «мошенничество, чистое мошенничество».

Помимо того, что Демара нравился людям, он также умел упорно трудиться и за короткое время овладевать необходимыми навыками. Но кроме этих полезных качеств ему помогали и чисто мошеннические приемы, например умение создать имидж невероятно компетентного человека. По случаю он приобрел подержанный чемодан, густо покрытый наклейками дорогих отелей и знаменитых курортов; в разговоре демонстрировал познания и привычки, свойственные выбранной им «профессии», но вместе с тем никогда никому не навязывал свое мнение. Если же вдруг у знакомых и коллег возникали сомнения в его компетентности, Демара использовал довольно простой метод: надвигался на усомнившегося всем своим огромным телом, изображая праведный гнев.

В запасе Фердинанда Уолдо Демары было множество и других приемов: он делал и говорил то, чего от него ждали, и люди ценили это редкое качество. Но все же с каждым своим перевоплощением он становился все дальше и дальше от своей цели – стать достойнее других людей. Можно только представить, какой страх он испытывал, опасаясь быть разоблаченным, особенно после того как его стали узнавать на улицах, и даже на уединенном острове он не мог получить желаемого покоя.

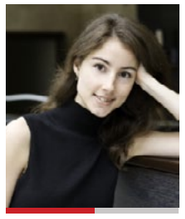
В последние годы жизни Демара, осознавая, что вся его мистификация провалилась, и он всю свою жизнь был просто-напросто мошенником, сильно пил. Автор книги «Великий Самозванец», лично общавшийся со своим героем, записал его горькие слова: «Каждый раз, когда я приобретал новую идентичность, какая-то часть настоящего меня умирала, кем бы этот настоящий я ни был».

Фердинанд Уолдо Демара-младший умер от сердечной недостаточности в 1982 г. в возрасте 60 лет. Практически все газеты, решившие опубликовать его некролог, упомянули о том, что больше половины жизни – 37 лет – Демара прожил под чужими именами. Получив в 46 лет первый и единственный документ об образовании – диплом Библейского колледжа в Портленде (штат Орегон), он работал в молодежном лагере, в миссии спасения бедных, а в последние годы был священником баптистской церкви. По признаниям прихожан, священником он был замечательным, умел слушать и утешать, как никто иной. Б

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

Корпоративные хищения: Причины и методы противодействия

«Если у работников магазина есть шанс украсть товар или деньги, они их украдут», – утверждают авторы книги «Основы розничной торговли» Майкл Леви и Бартон А. Вейтц. Руководитель проекта «Безопасность для всех», старший преподаватель кафедры защиты, охраны и безопасности ГУФиС РМ Анатолий Брединский рассказал журналу «Безопасность: Информационное обозрение», почему сотрудники воруют у работодателя, и как сократить число краж на предприятии.



Интервью подготовила и провела Адель Соколова

«Многочисленные исследования показали, что людей изначально плохих, настроенных на совершение негативных действий, не более 10% от общего числа, примерно столько же ангелов».

- Анатолий, насколько актуальна сегодня проблема хищений, совершаемых персоналом?

- Спросите у любого руководителя или владельца предприятия о его сотрудниках и наверняка услышите в ответ:«Воруют». Правда, одни, словно параноики, твердят: «Да у меня одни воры работают!»; другие же флегматично соглашаются: «Ну да, подворовывают, а что поделать?». Проблема воровства персоналом, безусловно, существует, но нельзя мести всех под одну гребенку, так же как и пускать проблему на самотек.

- В чем, на Ваш взгляд, кроется основная причина воровства в компаниях?

- Думаю, Вам неоднократно приходилось сталкиваться с мнением о том, что человек по природе своей порочен, что его снедают зависть и корысть, что воруют все, просто не всех ловят и прочее, и прочее. На самом же деле эти утверждения не имеют под собой никакого основания, являясь лишь измышлениями, основанными на негативном опыте их авторов. Многочисленные исследования показали, что людей «изначально плохих», настроенных на совершение негативных действий, не более 10% от общего числа, примерно столько же «ангелов», т.е. кристально честных, не способных на подлость и преступление ни при каких обстоятельствах. Основная же часть – это серая масса, т.е. те, кто способен продемонстрировать как положительные, так и отрицательные черты, в зависимости от обстоятельств, в которые они попадают. Именно поэтому нельзя утверждать, что главным и единственным мотивом воровства персонала является жажда наживы и безграничная корысть. Все гораздо сложнее, и причины, толкающие людей на воровство, могут быть самыми разными.

- То есть офисное воровство бывает разным?

- Условно причины воровства в компаниях можно разделить на несколько групп:

1. Воровство по случаю.

Таковы уж особенности нашего менталитета, что многие, хотя далеко не все, считают, что украсть то, что плохо лежит – это наказать владельца за безалаберность и глупость. Поэтому часть сотрудников может спокойно и даже добросовестно работать до определенного момента, когда проявит себя змей-искуситель в виде благоприятно сложившихся обстоятельств. То есть, оказавшись в ситуации, когда можно совершить кражу, да еще и будучи уверенным, что это останется безнаказанным, определенная категория работников не будет долго терзаться моральными переживаниями и сомнениями – «красть или красть, вот в чем вопрос?». Они украдут.

2. Воровство из интереса.

Для некоторых людей совершенно неважно, что именно украсть, важен сам процесс кражи. Для такой категории еще в XIX в. был придуман термин «клептомания».

3. Воровство как промысел.

Это, пожалуй, одна из самых опасных категорий, в которую входят работники, считающие, что нет смысла зарабатывать, если можно легко украсть. Они специально устраиваются в компании с целью значительно увеличить свое благосостояние. Как правило, первое время такие лица присматриваются, стараясь создать себе репутацию честного и добросовестного работника, а затем начинают воровать. Причем такие воры бывают двух типов: первый тип – это крадуны, совершающие довольно примитивные хищения, которые быстро обнаруживаются и раскрываются. Второй – это профессиональные воры, которые умеют создавать довольно хитроумные схемы воровства, пользуясь выявленными ими недочетами в системе контроля и учета на предприятии. Иногда они специально создают такие бреши для своих нужд. Некоторые из них, понимая, что в одиночку кражи совершать им не под силу, начинают подговаривать других работников, создавая целые «преступные группировки». Нередко они вовлекают в этот процесс руководителей среднего звена, а иногда даже сотрудников службы безопасности, которые, получая свою долю, покрывают воров.

4. Воровство как источник существования.

К сожалению, существуют ситуации, когда работники просто вынуждены совершать хищения. Увы, ни для кого не секрет, что в некоторых организациях заработная плата не соответствует даже прожиточному минимуму. Особенно это касается оплаты низкоквалифицированных специалистов и обслуживающего персонала.

5. Воровство из мести.

Кражи для представителей этой категории – это акт возмездия за некие негативные, по их мнению, действия начальства. Наиболее часто они совершают кражи, столкнувшись с унижениями и оскорблениями со стороны руководителей, системой драконовских штрафов, необходимостью бесплатно трудиться в выходные или праздничные дни. В результате у таких работников возникает сильное желание сделать что-то плохое своему начальнику, отомстить, хоть как-то компенсировать свои унижения или материальные потери.

Предметы, наиболее часто уносимые сотрудниками офисов:
- бумага для принтера;
- мелкие канцтовары;
- калькуляторы;
- обогреватели;
- органайзеры, папки, блокноты, ежедневники;
- зарядные устройства;
- книги;
- посуда и столовые приборы.

- Анатолий, что чаще всего воруют сотрудники предприятий?

- На самом деле похитить могут абсолютно все, в том числе и вещи, которые ни продать, ни использовать по хозяйству вор не сможет. Однако можно выделить некоторые тенденции. Как показывают исследования, чаще всего корпоративные воры уносят:

- бумагу для принтера;
- мелкие канцтовары;
- калькуляторы;
- обогреватели;
- органайзеры, папки, блокноты, ежедневники;
- зарядные устройства;
- книги и справочную литературу;
- посуду и столовые приборы.

В целом у воров популярностью пользуются небольшие по размеру (легко спрятать, унести), но при этом ценные предметы. При кажущейся незначительности вышеуказанного если эти хищения совершаются регулярно и массово, то суммарно они могут причинить существенный ущерб.

- Как именно совершаются хищения?

Существует несколько распространенных приемов:

• присвоить предмет, надеясь, что никто не заметит;

• сделать вид, что украденное было случайно уничтожено, испорчено или израсходовано;

• сделать вид, что была совершена кража иными лицами или неизвестными;

• заменить новые вещи, принадлежащие компании, другими, старыми или более низкого качества.

- Могли бы Вы дать краткие советы, как предотвратить кражи на предприятии?

- Данному вопросу можно посвятить не одну самостоятельную статью, поэтому я ограничусь лишь общими способами.

• Очень тщательно подбирать сотрудников.

• Осуществлять обязательный гласный и негласный контроль за персоналом.

• Сформировать эффективно работающую систему контроля рабочего процесса и его результатов.

• Регулярно проверять имущество предприятия.

• Иметь агентов среди работников и вести разъяснительную работу, чтобы вора не покрывали коллеги.

• Тщательно исследовать любые подозрительные случаи или информацию о возможных кражах.

• Формировать систему перекрестного контроля, не допуская, чтобы все находилось в руках у одного человека.

• Интересоваться личной жизнью работников с целью выявления резкого роста их благосостояния из неизвестных источников.

• Создавать дружественную атмосферу в коллективе, уважительно и внимательно относиться к работникам.

• Вводить дифференцированную оплату труда в зависимости от результата, а также систему поощрений. Стремиться к повышению заработной платы.

Конечно, нельзя даже в очень объемной статье осветить все аспекты корпоративных хищений, тема эта многообразна и весьма многогранна. Вместе с тем, надеюсь, что мысли, суждения и рекомендации, данные мной, будут полезны тем, кто сталкивается с этой проблемой в своей практике.

Ваше мнение и комментарии присылайте по адресу

info@csc.ru

Профилактика утечки информации через уволившихся сотрудников

Максим Кикеня

Существует тысяча причин, по которым сотрудник компании может пожелать сменить текущее место работы. А кто покажет работодателя, который полностью уверен в верности общему делу своих подчиненных? Вы можете не согласиться, но отыскать такого человека совсем не просто, если вообще возможно. Сегодня одним из ключевых факторов, влияющих на стабильное развитие компании, остается текучесть кадров. Несмотря на широкое применение программ выработки лояльности сотрудников к компании, недовольные кадры всегда были, есть и будут. Но если для одной компании текучесть кадров является проблемой, то для другой – к примеру, средством снижения расходов на персонал.

Каковы же причины текучести кадров? Охватить весь спектр недовольства будет сложно, так как человеческая фантазия – вещь многогранная, поэтому мы ограничимся наиболее популярными примерами: низкая зарплата, сложные отношения в коллективе, недостойные условия труда, отсутствие карьерного и профессионального роста, неудобные графики работы и т.д. Разочарованный и обиженный сотрудник в порыве отчаяния и из жажды мести может нанести ощутимый ущерб компании. Согласно исследованию, проведенному Ponemon Institute в 2009 г., почти 60% уволившихся или сокращенных работников в 2008 г. в США перед своим уходом воровали конфиденциальную информацию. Около 40% респондентов признались, что основным мотивом преступления для них стало чувство неприязни по отношению к бывшему работодателю.

С уходом сотрудника из компании связан ряд последствий, которые ложатся на плечи работодателя. Так, например, необходимо выполнить череду процедур и формальностей, прописанных в трудовом законодательстве. Для этого потребуется задействовать усилия административного аппарата и учесть финансовые затраты на канцелярию. Определенный объем работ, который выполнял бывший сотрудник, придется поручить кому-то другому или распределить между всем коллективом, добавив дополнительную нагрузку каждому сотруднику и в ряде случаев снизив эффективность их труда. Увольняющемуся работнику нужно подобрать равноценную замену, что не так-то просто. А новому сотруднику понадобится время на адаптацию.

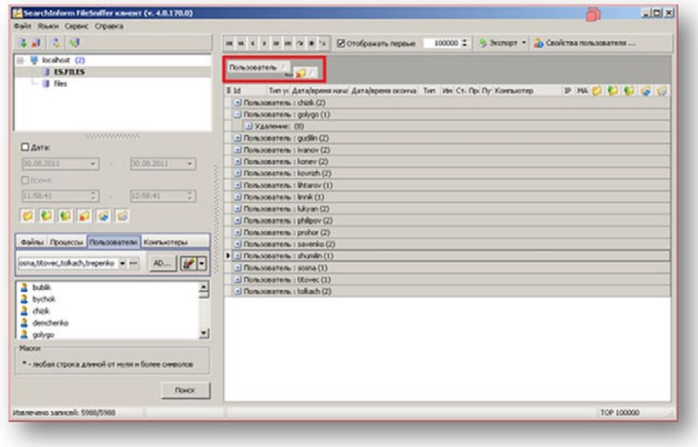
Также существует риск утечки информации, к которой имел доступ работник. Естественно, что чем более ответственную должность он занимал, тем шире был его доступ к корпоративным данным. Так, например, у топ-менеджера доступ к информации гораздо шире, чем у рядового сотрудника. Логично предположить, что негативные последствия предательства со стороны сотрудника, занимавшего руководящую должность, более существенны, нежели от разглашения каких-либо сведений простым служащим. Поэтому к увольнениям топ-менеджеров относятся более внимательно и действуют аккуратнее. Многие компании, например, щедро вознаграждают уволенных топ-менеджеров. В знак благодарности бывшему сотруднику за его молчание может быть выплачен солидный гонорар или отойти в личную собственность служебное имущество (автомобиль, квартира и т.д). Вариантов масса, но и они не дают гарантию, что коммерческая тайна останется таковой и после ухода сотрудника.

Вне зависимости от того, каким образом (мирно или в результате конфликта) бывший сотрудник покинул свой пост, следует задумываться о принятии мер по обеспечению безопасности известных ему данных. В противном случае нельзя быть уверенным в том, что на следующий день на различных веб-ресурсах не появятся материалы, оскверняющие и порочащие имя вашей компании, или бизнес-планы, на разработку которых ушло много времени и средств.

Во избежание множества проблем при увольнении сотрудников следует обратить внимание на следующие моменты:

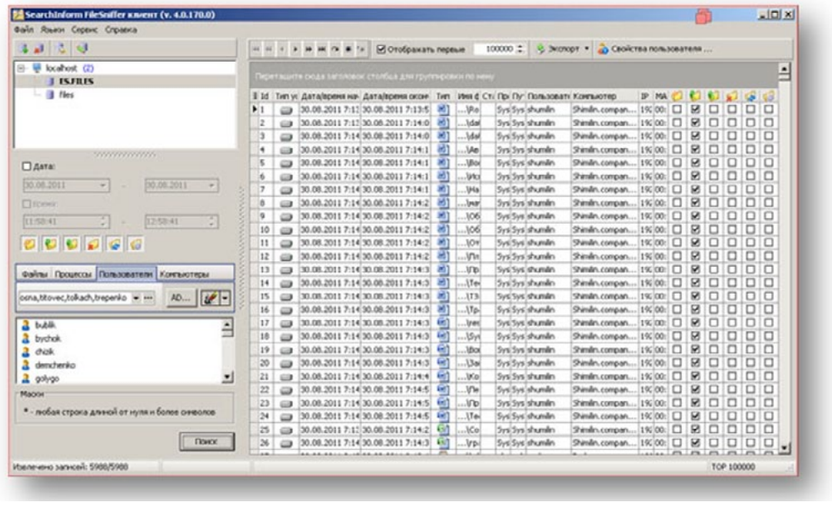
- Определить объем конфиденциальной информации, к которой имел доступ уволенный сотрудник.
- Провести анализ работоспособности носителей информации и оборудования.
- Определить возможные риски, связанные с разглашением информации и минимизировать их.
- Определить круг сотрудников, с которыми поддерживал отношения бывший работник.
- Поставить действующий персонал и клиентов в известность, что данный сотрудник больше не является представителем фирмы.
- Провести беседу с действующим персоналом о запрете на обсуждение рабочих моментов с бывшими сотрудниками.
- После увольнения провести мониторинг Сети на наличие негативных отзывов о компании и конфиденциальной информации.

Следует также указать на некоторые приемы, при помощи которых можно выяснить, к какой информации имел доступ ваш экс-сотрудник. Например, можно уточнить данный момент у его коллег, проанализировать архив документов, с которыми велась работа, или воспользоваться специализированными инструментами. Рассмотрим пример с FileSniffer – инструментом, входящим в состав «Контура информационной безопасности SearchInform» и позволяющим фиксировать активность пользователя (создание, удаление, копирование, переименовывание и т.д.) при работе с файлами.

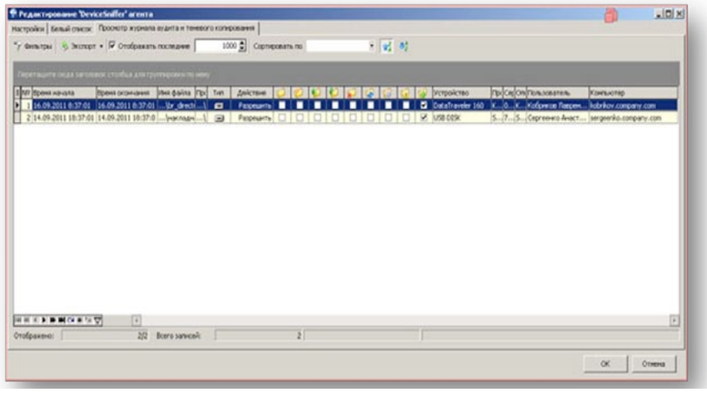


Выбрав определенный период, можно определить все файлы, к которым имел доступ сотрудник и все действия, которые с ними совершал.

Продукт DeviceSniffer позволит проконтролировать все внешние устройства, подключенные к рабочей станции. Рассмотрим одну из его функций – Журнал аудита и теневого копирования – в контексте нашей задачи.



Изначально отображаемая информация кажется сложной для восприятия, однако блок фильтрации позволяет группировать её с использованием условий и необходимых требований. Ниже представлены примеры группировки информации по учетным записям в Active Directory и по действию с файлом (удаление).



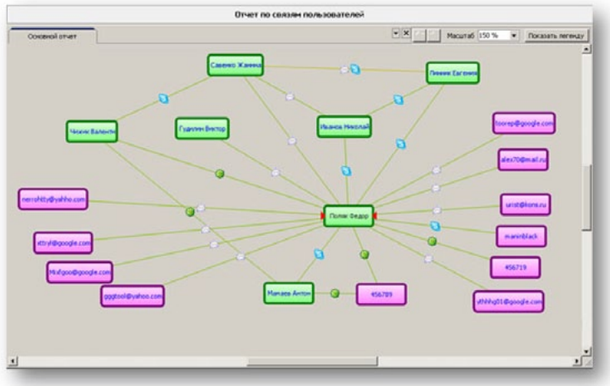
В Журнале аудита и теневого копирования фиксируется время подключения устройства, выполненные действия, учетная запись, имя компьютера, а также имя файла.

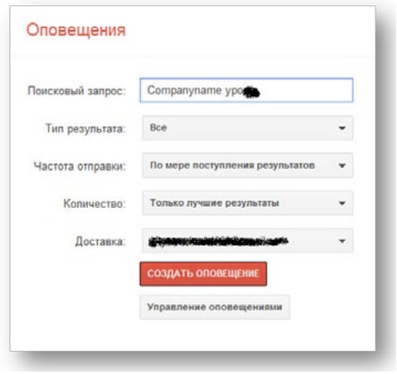
Далее можно определить круг общения увольняемого сотрудника, например с клиентами или коллегами. Общение с клиентами можно определить на основании активности в CRM-системе или проанализировать корпоративный почтовый ящик сотрудника. С коллегами ситуация сложнее. Нужно узнать круг товарищей, предварительно опросив рядом сидевших сотрудников и т.п. А можно проконтролировать активность коллег в социальных сетях, «аське», «скайпе», что поможет выявить друзей по переписке и сыграть на руку безопаснику.

Если рассматривать данный подход с точки зрения этики, то он лежит в рамах закона, поскольку не предполагает чтения чужой переписки, а лишь фиксирует данный факт. Речь идет об одном из отчетов, генерируемых в программном продукте ReportCenter (входит в состав «КИБ SearchInform»). Отчет по связям пользователей отображается в виде статистики, представленной с помощью графа. Такая статистика может быть полезна, так как вычислить все связи коллектива исходя из анализа данных невозможно.

Фиолетовым цветом подсвечиваются внешние контакты, зеленым – корпоративные. Цвет нитей связи меняется в случае, когда количество сообщений достигает пороговых показателей (100, 500, 1000, …, N). На каждой нити отображается пиктограмма, называющая канал связи, по которому происходила коммуникация. Так, если сотрудник был уволен, то с помощью данного отчета можно определить его общение с коллегами.

После ухода сотрудника не лишним будет провести мониторинг Сети на наличие конфиденциальной информации компании и высказываний, порочащих ее имя. Одним из бесплатных сервисов, позволяющих осуществить сбор информации, является Google Alerts. Однако анализ попрежнему остается за человеком. Доставку же результатов можно получить как на почтовый ящик пользователя, так и в фид.





Важно понимать, что люди являются самым важным ресурсом компании. Поэтому увольнение сотрудника – всегда негативный процесс. Тем не менее последствия расставания можно свести к минимуму, используя различные способы, выбор которых зависит от ценности (или угрозы), которую несет работник. Б

Ваше мнение и комментарии присылайте по адресу

info@csc.ru

«Москвич» с вертикальным взлетом, или Некоторые итоги прошедших выставок

Игорь Собецкий,
Зав. лабораторией
Учебного центра «Информзащита»

- Вас обвиняют в мошенничестве – вы продавали простакам эликсир вечной молодости. Ранее Вы привлекались к уголовной ответственности?
- Да, в 1467, 1545 и 1739 годах.
Из материалов дела о незаконной торговле

Закончился традиционный форум «Технологии безопасности». Осенью параллельно – да здравствует конкуренция! – отгремели ИнфобезЭкспо и Infosecurity Russia. И сейчас под впечатлением от этих выставок хотелось бы обратить внимание сообщества на тревожную тенденцию. Целый ряд компаний – разработчиков и дистрибьюторов средств защиты – вместо формирования рынка и реального внедрения инновационных технологий фактически решили потрафить самым темным суевериям, сложившимся на российском рынке безопасности. И ведь, на первый взгляд, не секрет, что систему безопасности, как и любую другую систему, необходимо строить комплексно и системно. И многих воротит от слайдов, на которых докладчики говорят о необходимости системного подхода, мол, «плавали, знаем», ты нам суть давай.

Однако же на выставках чаще можно встретить не системные решения, а именно инструменты для этих решений. Отчасти оно и понятно, интегратору рассказать о своих достижениях либо нелегко (мощный и сложный проект, заточенный под заказчика и неповторимый – лишь иллюстрация способности что-то построить), либо и вовсе стыдно, когда речь идет о кургузом частичном решении, получившемся в результате неожиданного ограничения сроков или бюджета. Демонстрируемые же на выставках инструменты, т.е. конкретные частные решения, – привлекательны. Производители говорят о том, какие системы можно на них построить, но тактично умалчивают о том, что все эти системы должны быть комплексными, и сами по себе порой не стоят ломаного гроша. Давайте рассмотрим эти умолчания более подробно.

Итак, первое чудо нашего рынка. Различные навигационные системы, основанные на GPS или ГЛОНАСС. Спору нет, система геопозиционирования на транспорте может оказаться весьма полезной. Такие системы практически в любых условиях могут применяться для контроля за действиями водителя (маршрут, соблюдение правил дорожного движения, скоростного режима), а также как часть системы обеспечения безопасности транспорта и перевозимого груза. Именно как часть, потому что системы геопозиционирования сами по себе ничего не охраняют. Применение такой системы имеет смысл, например, при наличии «группы поддержки» на некотором удалении от перевозимого груза[1] или в крайнем случае соглашения о взаимодействии с государственными правоохранительными органами. То есть системы геопозиционирования эффективны лишь при интеграции их в целый комплекс организационных мероприятий.

Но вместо взвешенного подхода на выставках различные производители представляют широкий ассортимент трекеров, навигаторов и прочего оборудования сомнительной полезности, вплоть до регистраторов. При этом все поставщики принципиально ничего не рассказывают о необходимости дополнительных организационно-административных мер и уж тем более не предлагают подготовить для заказчиков соответствующие регламенты. Складывается ощущение, что на современном этапе любая критика систем геопозиционирования воспринимается как подкоп под устои.

В результате разрекламированные трекеры эффективны исключительно для подтверждения честности таксистов и дальнобойщиков. Конечно, если в этой честности предварительно убедились. Потому что нечестному водителю ничего не стоит разделаться с трекером. Достаточно вспомнить, что трекер передает данные на центральный пост по каналу GSM – т.е. по обычной мобильной связи. Соответственно каждый любитель приватности может приобрести специальный прибор для подавления GSM-сигналов, благо в настоящее время такие приборы находятся в свободной продаже. Типовой представитель этого семейства, по заявлению разработчика, обеспечивает подавление связи стандартов GSM (900/1800), 3G, GPRS, EDGE, WiFi, Bluetooth, AMPS, NMT, CDMA, TDMA, UMTS, причем дальность действия прибора составляет 12 м. Цены на подобные устройства вполне демократичны – от 12 до 18 тысяч рублей, что делает подавители доступными для всех желающих. Особые ненавистники систем позиционирования могут потратиться на специальный подавитель систем геопозиционирования. Всего за 12 тысяч рублей чудо-прибор обеспечивает подавление всех сигналов GPS / ГЛОНАСС, использующих частоты L1, L2 и L5, т.е. блокирует абсолютно все гражданские сигналы в частотных диапазонах GPS. Радиус действия устройства составляет 15 м, причем для удобства водителей предусмотрено питание от прикуривателя.

ВМЕСТО ВЗВЕШЕННОГО ПОДХОДА НА ВЫСТАВКАХ РАЗЛИЧНЫЕ ПРОИЗВОДИТЕЛИ ПРЕДСТАВЛЯЮТ ШИРОКИЙ АССОРТИМЕНТ ТРЕКЕРОВ, НАВИГАТОРОВ И ПРОЧЕГО ОБОРУДОВАНИЯ СОМНИТЕЛЬНОЙ ПОЛЕЗНОСТИ, ВПЛОТЬ ДО РЕГИСТРАТОРОВ.

Использование таких приборов в нашей стране принципиально недоказуемо и не наказуемо. Ни один оператор мобильной связи не гарантирует покрытия своей сети на 100% территории без изъятий. Соответственно, тот же водитель фуры целиком и полностью в своем праве: ну вот не было связи на дороге, не было! Не знаю, почему не было, все вопросы к оператору! И в результате дорогостоящее оборудование можно было и не распаковывать – результат не изменился. Все участники бизнес-процесса совершенно довольны: чиновники отчитались за исполнение правительственной программы по GPS, ГЛОНАСС или Galileo, разработчики выгодно продали свои изделия, компания-владелец транспортных средств теперь полностью контролирует процесс перевозки, а водитель ездит куда хочет и как хочет. Все при деле!

Увы, при деле оказываются и разбойники всех мастей. Если в деле охраны груза за трескотней про устройства слежения забыты организационные мероприятия, то ограбление оснащенного трекером «дальнобоя» становится тривиальной задачей. Надо только не забыть прихватить на дело, помимо формы ГАИ и электрошокера, еще и упомянутый подавитель мобильной связи. В помощь грабителям на той же выставке демон

[1]Обычная практика при перевозке особо ценных грузов – золота, наличности и т.п.

стрируются приборы, работающие не только от автомобильного прикуривателя, но даже от встроенных аккумуляторов. Соответственно, в момент ограбления злодеям надо только не забыть нажать кнопочку. Всё. Любая система геопозиционирования отдыхает.

Несмотря на эти общеизвестные соображения, никто из участников выставок не пытается предложить клиентам полный пакет услуг – не только систему трекинга и контроля, но и пакет нормативных документов, разработанный с учетом специфики клиентского бизнеса. Неужели потому, что вторая услуга куда более сложна и менее рентабельна, нежели первая? Будем надеяться, что самые худшие предположения ошибочны, и дело всего лишь в отсутствии системного подхода в компаниях-разработчиках.

Второй рецепт ханаанского бальзама – разнообразные системы видеонаблюдения. Рынок таких систем переполнен, каждая уважающая себя компания-поставщик предлагает клиентам по несколько сотен моделей видеокамер и пару десятков видеорегистраторов. Поставщиков можно понять – у них развернуто производство или налажены связи с зарубежными производителями, нанят персонал, арендован офис... Словом, бизнес летит вперед, как паровоз, и останавливать его не хочется. А если все клиенты, которым в принципе может пригодиться видеонаблюдение, уже купили необходимое им количество камер[2], это не проблема! Надо только убедить клиента, что проданные ему в прошлом году замечательные камеры уже устарели, и эту рухлядь необходимо срочно заменить. Вот и просачиваются на рынок камеры в квадратном и в круглом корпусе, вандалозащищенные и термоизолированные[3], под метрическое и под дюймовое крепление, со светофильтрами и без оных... И все как один – аналоговые. Неуправляемые, не слишком высокого разрешения, да к тому же рассчитанные на определенную модельную линию регистраторов. Налетай, подешевело!

На самом деле видеонаблюдение является неотъемлемой частью системы обеспечения безопасности. Без профессионально поставленного видеонаблюдения охрана большинства объектов просто немыслима. Вот только во многих случаях проектировщики систем видеонаблюдения решают поставленные задачи примерно так же, как известная героиня басни Крылова «Мартышка и очки» исправляла дефекты своего зрения. А под пространные рассуждения о перекрытии зон наблюдения и необходимости видеть камеры с других камер для усложнения демонтажа и навязывания нам продается немыслимое количество камер. Хотя, как известно, большинство помещений (а равно строений, земельных участков и т.п.) сколь угодно сложной конфигурации можно было бы просмотреть при помощи существенно меньшего количества интеллектуальных камер.

Логичным в такой ситуации представляется использование интеллектуальной системы видеонаблюдения, включающей управляемые IP-видеокамеры и сервер видеонаблюдения. По команде с видеосервера IP-камера автоматически наводится на движущиеся объекты (например на работников, входящих в помещение), фиксирует лицо крупным планом, после чего вновь берет общий план помещения. При желании пользователь может установить на конкретную персону специальную «метку», после чего видеосервер проследит все ее передвижения. Как правило, видеосервер может работать с произвольным числом видеокамер в пределах полосы пропускания сети. Система в целом получается дешевле и надежнее, чем пригоршня аналоговых видеокамер, подключенных к специализированному видеорегистратору.

НА САМОМ ДЕЛЕ ВИДЕОНАБЛЮДЕНИЕ ЯВЛЯЕТСЯ НЕОТЪЕМЛЕМОЙ ЧАСТЬЮ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. БЕЗ ПРОФЕССИОНАЛЬНО ПОСТАВЛЕННОГО ВИДЕОНАБЛЮДЕНИЯ ОХРАНА БОЛЬШИНСТВА ОБЪЕКТОВ ПРОСТО НЕМЫСЛИМА.

Вот только поступить так просто – неспортивно. Мы должны сами себе создать трудности, а затем геройски преодолеть их. Поэтому на тех же выставках предложения интеллектуальных систем составляют не более 10% общего объема предложений по видеонаблюдению. Клиент, купивший такую систему, почти потерян для поставщиков. Установленная система удовлетворяет все потребности клиента, так что не возникает потребности в ее замене. В отсутствие «мёртвых» зон нет необходимости в приобретении дополнительных камер, за исключением замены вышедших из строя. Если система стабильно работает даже несколько лет подряд, трудно убедить клиента, что эта рухлядь срочно требует замены.

В результате даже многие руководители служб безопасности крупных компаний мало что знают об интеллектуальных системах видеонаблюдения. Соответственно продолжаются закупки старомодного оборудования, а обновление систем сводится к латанию дыр и дальнейшему

[2]Плюс еще резерв 25%, по настоятельному совету поставщика.
[3]Что особенно актуально при установке в офисных помещениях – автор имел удовольствие видеть три таких ус-пешно сданных проекта.

расширению сети аналоговых камер. И серьезных просветительских усилий поставщиков интеллектуальных систем видеонаблюдения что-то не видно[4].

Наконец, очередным модным решением всех проблем стали приборы для поиска закладок и всевозможные индикаторы полей. Разумеется, эта чудесная аппаратура (множество кнопочек, лампочек, жидкокристаллических дисплеев, все мыслимые сертификаты прилагаются!) сама легко и непринужденно решит все проблемы с защитой корпоративной информации безо всяких усилий со стороны подразделений безопасности. Надо только прикупить что-нибудь модное. Конкуренция в этом сегменте рынка достаточно острая, так что продавцы спецтехники рекламируют свой товар с полным напряжением сил. Так, согласно рекламе, среднестатистический индикатор поля обнаруживает сотовые телефоны всех мыслимых стандартов (GSM900/1800, UMTS(3G), CDMA450), беспроводные телефоны стандарта DECT, устройства Bluetooth и Wi-Fi, беспроводные видеокамеры, радиопередатчики с аналоговой модуляцией (АМ, ЧМ, ФМ), радиопередатчики с цифровой модуляцией и непрерывной несущей (FSK, PSK и др.), радиопередатчики с широкополосной модуляцией с полосой до 10 МГц. Еще круче нелинейный локатор – этот прибор обнаруживает вообще все закладочные устройства. Несомненно, от такой всевидящей техники не спрятаться никакому электронному шпиону. Цены при этом вполне демократичные, годовые бюджеты во многих компаниях еще не сверстаны. Так что ж мы стоим? Срочно за покупками!

ОДНАКО ПРИОБРЕТЕНИЕ ОТДЕЛЬНЫХ ПРИБОРОВ – ЛИШЬ СПОСОБ СНИЗИТЬ ТРЕВОЖНОСТЬ РУКОВОДСТВА КОМПАНИИ И ПОПУСТУ ПОТРАТИТЬ ДЕНЬГИ.

Как и всегда, дьявол скрывается в нескольких мелких деталях. Вопреки настойчивой рекламной агитации, высокотехнологичные «ящички» сами по себе ничего в вашем офисе не найдут. К чудодейственным приборам должен прилагаться специалист с опытом работы. И этот специалист сразу же пояснит вам, что с помощью индикатора поля, как и другого поискового оборудования, в принципе возможно обнаруживать лишь определенные типы специальных технических средств для негласного получения информации. Существует множество СТС, которые либо все ничего не излучают в эфир, либо передают информацию короткими импульсами в ночное время. Соответственно, даже в руках специалиста поисковые приемники (а также индикаторы поля и даже спектральные корреляторы) будут эффективны лишь для решения некоторых частных задач.

Обеспечение же надежной защиты корпоративной информации от перехвата СТС возможно лишь при использовании системного подхода, включающего не только приобретение чудо-приборов, но и в первую очередь организационно-административные меры (например выделение специальных помещений для ведения конфиденциальных переговоров, разграничение офиса компании на зоны доступа, специальные мероприятия, усложняющие внос СТС в помещения компании). А уж когда дело доходит до закупок, то приходится приобретать не один чудо-ящичек, а целую линейку дорогостоящего оборудования, включая непременно комплекс круглосуточного радиомониторинга[5]. В расходную часть бюджета предстоит включить и затраты на специалиста[6] по технической защите информации, зарплата которого начинается от 100 тысяч рублей в месяц. Полный комплекс мероприятий по защите информации от перехвата обойдется недешево, поэтому жертвы рекламы предпочитают купить хоть что-нибудь. Однако приобретение отдельных приборов – лишь способ снизить тревожность руководства компании и попусту потратить деньги. К сожалению, поставщики спецтехники почему-то умалчивают о таких подробностях. А их реклама вместо объективной картины формирует у потребителей образ устройства-панацеи: только купили, и вот уже никаких проблем[7]! Очевидно, что подобная реклама дезориентирует в особенности представителей малого и среднего бизнеса, порождая у них весьма легковесное отношение к собственной безопасности.

Автор надеется, что в ближайшем будущем участники рынка безопасности наконец повернутся лицом к клиенту. Давайте вспомним, что далеко не всем разработчикам удается пробиться в придворные поставщики компаний калибра «Газпрома» или «ЛУКОЙЛ». Многим приходится довольствоваться клиентами – представителями компаний, далеких от современных информационных технологий, и даже компаний среднего бизнеса. И в таких местах решение о закупке принимает не какой-нибудь департамент информационной безопасности (50 сотрудников, защищенный бюджет, непререкаемый авторитет в компании), а главный (он же зачастую единственный) специалист по безопасности. Причем этот специалист сражается за каждый рубль бюджета, как царь Леонид при Фермопилах. Естественно, что такой специалист заинтересован в комплексном решении стоящих перед ним вопросов. Вариант же, когда сделанные закупки оказываются на поверку малоэффективными либо тут же влекут за собой новые проблемы, не привлекателен ни для кого. Заказчик готов «от сердца оторвать» деньги за решение проблемы, а не за новую головную боль. Как мы видим, слепое следование за рыночными заблуждениями не решает проблем, а лишь приносит эту самую головную боль. Так не лучше ли продолжить формирование цивилизованного интеллектуального рынка безопасности?

Еще одной чрезвычайно полезной для рынка новеллой могло бы стать повсеместное введение кредитования и рассрочек. На данном этапе компании-поставщики делают вид, что вовсе и не знакомы с такими терминами[8]. Между тем многие заказчики вынуждены укладываться в прокрустово ложе ранее сверстанного бюджета. И здесь рассрочка платежей стала бы спасательным кругом для корпоративного подразделения безопасности, позволив приобрести необходимое оборудование и услуги именно тогда, когда они требуются. А уж при составлении бюджета на следующий год появляется возможность продемонстрировать руководству компании экономическую отдачу от закупок. Так что компании, разучившие с менеджерами по продажам средств защиты такие специфические термины, как «скидка», «кредит» и «рассрочка», смогут оставить конкурентов на корпус позади. Б

[4]Перелопатив папку «СПАМ» на корпоративном почтовом сервере, автор нашел 211 приглашений на различные мероприятия с представлением новых аналоговых камер и только 3 – на демонстрацию систем интеллектуального видеонаблюдения. Это уже статистика.
[5]Стоимость такого комплекса составляет от 100 тысяч (такие в принципе продаются) до 300 тысяч рублей (а такой комплекс хотел бы приобрести автор).
[6]Имеется в виду настоящий специалист с опытом работы, который может решить все поставленные задачи.
[7]Автор только что отверг заманчивое предложение провести поисковые мероприятия в 3-этажном офисном здании заказчика с использованием его же радиосканера. На работу щедро выделялось полдня и гонорар 500 рублей.
[8]В лучшем случае рассрочку удается вырвать у поставщика после многотрудных переговоров.

Конфликты. Зачем о них знать безопаснику?

Алексей Дрозд,
аналитик компании SearchInform

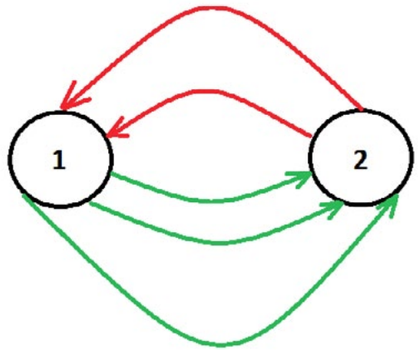
Не хочу никого обидеть, но лично для меня психология всегда была в какой-то мере псевдонаукой. Ведь человеческое поведение далеко не всегда является предсказуемым. Тем не менее я признаю, что в некоторых ситуациях спрогнозировать реакцию на то или иное событие реально. Например, во время конфликта. В этом материале мы рассмотрим конфликт в контексте информационной безопасности и разберем не только его структуру и причины, но и варианты разрешения ситуации.

Теоретизируем

Прежде всего, для предметного обсуждения конфликта необходимо убедиться, что понимаем мы под этим словом одно и то же. Именно поэтому сформулируем определение. *Конфликт – это противоборство двух сторон.* Говоря языком математики, это определение необходимое, но недостаточное. Оно упускает много нюансов.

Во-первых, сторон все же не две, а три. Вспомните любой анекдот про тещу. Она и есть та самая третья сторона, которая натравливает жену на мужа. В контексте информационной безопасности третьей стороной выступают все те, кто получит выгоду от утечки информации. К примеру, конкуренты подкупают сотрудника нашей компании. В этом случае конфликт происходит между сотрудником и компанией, а третьей стороной являются конкуренты. Другой пример: обиженный сотрудник из чувства мести (а заодно и личной выгоды) крадет какую-либо информацию, чтобы в дальнейшем кому-нибудь продать. В данном случае третьей стороной выступит «таинственный покупатель», так как именно ему это принесет наибольшую выгоду. Наконец, даже если кто-то просто выложит в Сеть «чувствительную информацию» без корыстных мотивов, третьей стороной выступят конкуренты, так как им выгодна такая ситуация хотя бы с точки зрения имиджа. К чему все эти примеры? Ответ прост – всегда ищите третью сторону.

Итак, с количеством участников конфликта разобрались. Приступим к «противоборству». Ничто не возникает просто так, и конфликты в том числе. Для противоборства нужны причины и повод. Но перед ними существует еще одна стадия – противостояние. Это своеобразная подготовка к активным действиям, заключающаяся в том, что обстановка между конфликтующими сторонами накаляется до определенного предела «по нарастающей».

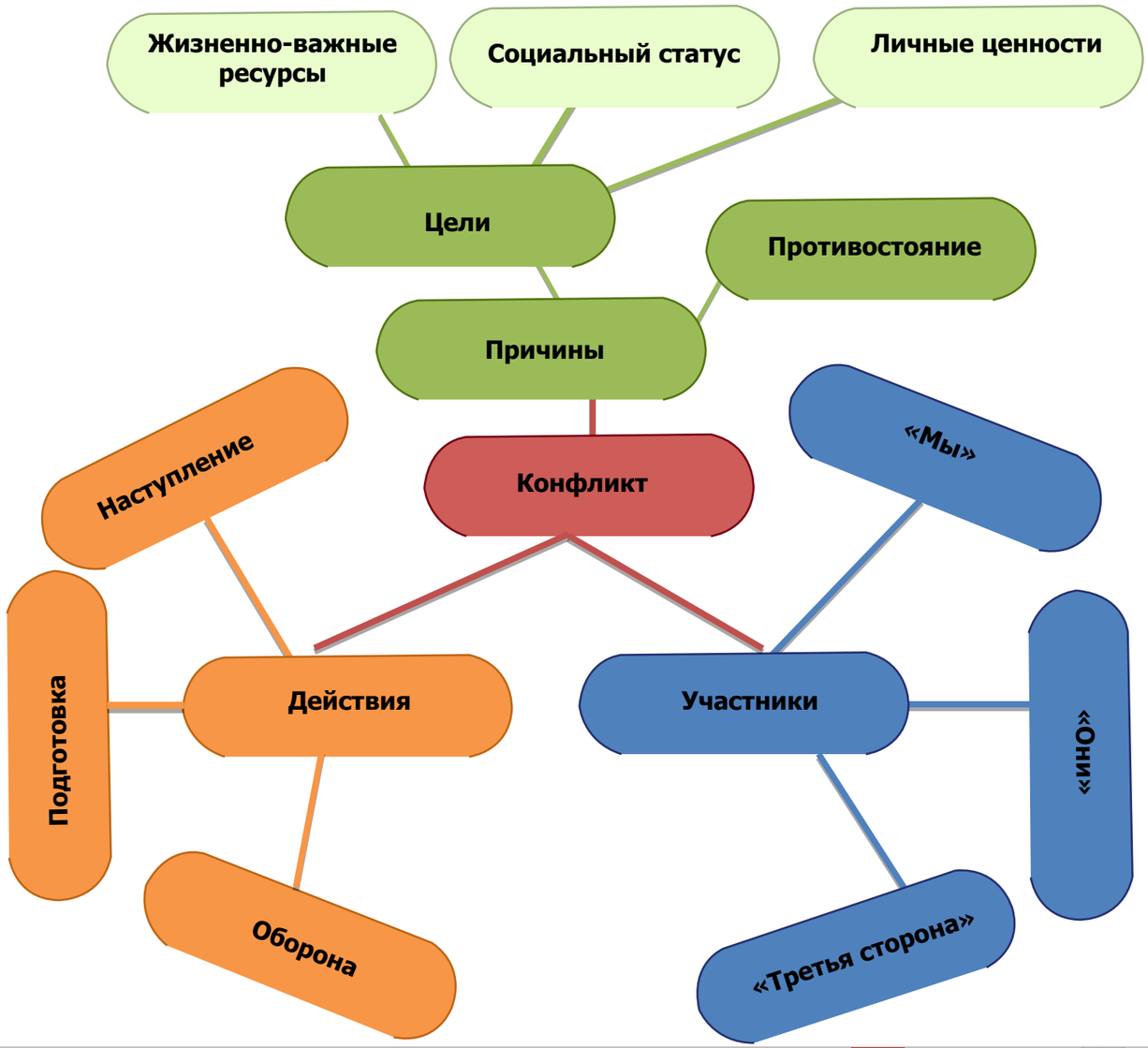


В качестве примера можно привести двух мужчин, которые кричат друг на друга все громче и громче. Но до бесконечности они этим заниматься не будут, а значит, конфликт либо не начнется (его участники разойдутся каждый в свою сторону), либо после очередного «сам дурак!» наступит переход в активную стадию (начнется драка).

По сути, конфликт – это «буфер» между двумя состояниями «системы». Давайте вспомним басню про «Лебедя, Рака и Щуку». Это хрестоматийный пример конфликта: нужно перетянуть воз, то есть переместить его из точки 1 в точку 2. Пока герои басни стоят и рассуждают, в какую сторону тянуть – это противостояние. Как только кто-либо из них начнет двигаться (то есть перейдет к активным действиям), возникнет конфликт.

Но каковы причины конфликтов? Главной причиной конфликта является невозможность одной из сторон достичь поставленной цели. Целей может быть несколько: жизненно важные ресурсы, социальный статус или личные ценности. К примеру, если сотрудник затаил обиду на начальника за то, что тот его отчитал на глазах у коллег, в качестве причины конфликта будет выступать социальный статус, так как именно его работник лишился.

Приведенные выше рассуждения удобно проиллюстрировать блок-схемой, позволяющей наглядно увидеть структуру конфликта.



Зачем?

Всем известно, что «болезнь легче предупредить», а лучшая утечка информации – та, которой не было. Эти истины справедливы и для информационной безопасности. На мой взгляд, «высший класс» специалиста по ИБ проявляется не в способности расследования инцидента (хотя это, безусловно, важно), а в способности его прогнозирования и предотвращения. В то же время множество утечек информации происходят именно вследствие различных конфликтов (личные отношения, размер зарплаты и т.п.). Именно поэтому важно понимать не только структуру конфликта, но и пути выхода из него.

Выход

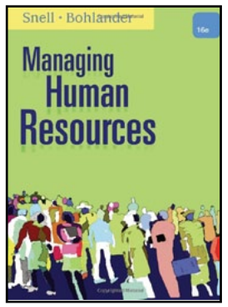
Стратегий выхода несколько. Все они отличаются по уровню эффективности и в жизни редко встречаются в «чистом виде». В основном, конечно, мы используем их комбинации. Рассмотрим некоторые способы выхода из конфликтной ситуации.

1. Отпор \ остановка. Наименее эффективный способ разрешения конфликта, главной целью которого стоит «сбить спесь» с нападающего. Низкая эффективность, как правило, возникает из-за того, что сам способ приводит скорее не к разрешению спора, а к его развитию «по спирали» (см. первый рисунок).
2. Уход \ отступление. Здесь все понятно: если не на кого нападать, то и нет смысла в конфликте.
3. Молчание. Оно, как известно, золото. Расчет идет на то, что ввиду отсутствия действий с нашей стороны, другая сторона со временем «выпустит пар» и успокоится.
4. Обман. Метод действенный, но рано или поздно правда может всплыть, и тогда придется разбираться с новым конфликтом.
5. Переговоры. Это один из самых действенных и самых успешных методов выхода из конфликта. Поэтому и самый популярный.

Ваше мнение и комментарии присылайте по адресу

info@csc.ru

КНИГИ



1. Скотт А. Снелл, Джордж У. Болэндер. Управление человеческими ресурсами (Scott A. Snell, George W. Bohlander. Managing Human Resources).

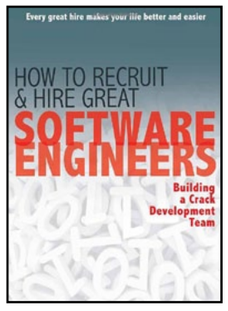
Язык: английский.

Дата выхода: 1 января 2012 г.

16-е издание знаменитой книги «Управление человеческими ресурсами» представляет собой структурированное исследование наиболее острых вопросов управления персоналом и включает ценные рекомендации для специалистов по HR и руководителей компаний. Работа содержит более 500 ярких, актуальных примеров из практики реальных организаций, которые иллюстрируют описания проблем, наиболее часто встречающихся на самых разных предприятиях.

Авторы книги – американские исследователи, преподающие основы менеджмента персонала в вузах страны. Профессор Скотт А. Снелл работает в бизнес-школе при Университете Виргинии. В разное время он оказывал консультационные услуги таким компаниям, как Arthur Andersen, AT&T, GE, IBM, и Shell Chemical, помогая им найти пути усовершенствования системы управления человеческими ресурсами в условиях конкурентной среды. В последнее время Снелл занимается изучением человеческого капитала как источника конкурентного преимущества бизнеса.

Джордж У. Болэндер, заслуженный профессор менеджмента Университета штата Аризона, специализируется на трудовом законодательстве, государственной политике и трудовых отношениях. Является автором более 50 статей и монографий, публикуется в таких изданиях, как National Productivity Review, HR Magazine и Labor Law Journal, выступает в качестве консультанта почтовой службы США, BFGoodrich, Banner Health Services и Del Webb.



2. Патрик Маккаллер. Как нанять великого программного инженера: построение первоклассной команды (Patrick McCuller. How to Recruit and Hire Great Software Engineers: Building a Crack Development Team).

Язык: английский.

Дата выхода: 14 ноября 2012 г.

Книга содержит инструкцию, как найти и нанять в свою команду сильных сотрудников, которые станут конкурентным преимуществом компании и обеспечат ей путь к успеху. Вашему вниманию будут предложены проверенные методы построения и управления процессом найма новых работников от начала и до конца.

Согласно исследованиям в большинстве коллективов есть программисты, которые в пять или даже десять раз более эффективны, чем их коллеги. Как вычислить этих одаренных и старательных людей? Патрик Маккаллер посвятил жизнь изучению методик распознавания по-настоящему стоящих кандидатов, включая подготовку к интервью, формулирование вопросов и упражнений для определения степени компетентности кандидата, моделирование ситуаций.

Книга будет полезна как новичкам в сфере HR, так и опытным специалистам.

3. Е.А. Митрофанова, В.М. Свистунов, Е.В. Каштанова. Организация обучения и дополнительное профессиональное образование.

Язык: русский.

Дата выхода: 2012 г.

Рассматривается система обучения персонала как часть системы стратегического управления организацией. В этом ключе приводятся практические примеры формулирования запроса на обучение персонала, выбора методов, моделей и технологии обучения, адекватных задачам обучения, разработки концепции учебных программ, а также технология оценки эффективности проведенного обучения. Излагаются вопросы планирования и контроля качества обучения персонала организации. Рассматриваются концепция организации обучения конкретного предприятия и положение об обучении персонала.

4. В.В. Семенихин. Кадровый вопрос. Обучение и повышение квалификации персонала.

Язык: русский.

Дата выхода: 2012 г.

Эффективность деятельности любой организации зависит от образовательного, культурного, профессионального и квалификационного уровня ее сотрудников. Потому организации направляют своих работников на подготовку, переподготовку и повышение квалификации. В данном издании читатель узнает все о том, как правильно обучить персонал всему необходимому и когда пришло время повысить его уровень.

5. Н.Е. Папонова. Обучение персонала компании

Язык: русский.

Дата выхода: 2012 г.

Книга представляет собой практическое руководство по организации на предприятии комплексной системы обучения и развития персонала. В издании, в частности, раскрыты вопросы постановки целей и оценки эффективности обучения, выбора форм обучения в соответствии с задачами предприятия, даны технологии проведения систем оценки (в том числе ассессмент-центр, оценка по компетенциям) и организации системы внутрикорпоративного обучения, приведены методики формирования мотивации сотрудников на развитие.

Пособие предназначено для специалистов по управлению человеческими ресурсами, специалистов по обучению и развитию персонала, руководителей организаций, а также преподавателей, аспирантов и студентов по специальности «Управление персоналом».

Международный форум «Технологии Безопасности – 2013»

12-14 февраля 2013 г. в Международном выставочном центре «Крокус Экспо» прошел XVIII Международный форум «Технологии безопасности». В этом году основное внимание участников мероприятия было уделено предотвращению чрезвычайных ситуаций и техническим средствам обеспечения безопасности на транспорте.

По традиции ТБ Форум 2013 представил передовые тренды следующего года. Одна из главных технологических витрин отрасли привлекла внимание инновационных ведоров, госзаказчиков и покупателей из разных регионов России, стран СНГ и мира. Организаторами мероприятия выступили Комитет Государственной думы по транспорту, Постоянная комиссия Межпарламентской ассамблеи СНГ по вопросам обороны и безопасности, Министерство транспорта Российской Федерации, фонд «Транспортная безопасность» и Правительство Москвы.

Одной из наиболее сильных сторон выставки стал раздел, посвященный безопасности транспорта. «В числе первоочередных задач XII Международной научно-практической конференции «Терроризм и безопасность на транспорте» – расширение экспозиции транспортного павильона Форума «Технологии безопасности – 2013». Акцент будет сделан именно на системные решения для транспорта, на инновационные разработки. Кроме того, особое внимание при подготовке мероприятия уделяется привлечению иностранных спикеров и участников», – отметил председатель оргкомитета конференции Александр Старовойтов.

На научно-практических площадках деловой программы, развернувшихся сразу в шести залах, прошли заседания конференций, круглые столы, симпозиумы и практикумы. Обсуждения требований законодательства и вопросов регулирования рынка безопасности вызвали шквал вопросов со стороны разработчиков, поставщиков и дистрибьюторов оборудования. Деловая программа Форума включала в себя более 70 часов выступлений нон-стоп в рамках конференций «Терроризм и безопасность на транспорте», «Безопасность объектов ТЭК», «Передовые методы и средства защиты конфиденциальной информации», «Безопасность мегаполисов и крупных городов», а также Всероссийского совещания проектных организаций и Всероссийского форума НСБ «Стратегия 2020». Тематика заседаний определялась интересами и потребностями крупных российских заказчиков: транспорт и грузоперевозки, промышленность и энергетика, городская и дорожная инфраструктура, торговые сети, объекты культуры, финансы.

ЦИФРЫ И ФАКТЫ
- *248 участников из 14 стран*
- *Делегации 71 субъекта РФ*
- *10 масштабных конференций*
- *Более 50 секционных заседаний, круглых столов, лекций, мастер-классов*
- *14 153 посетителя*
- *Профессиональная поддержка более 20 федеральных министерств и ведомств*
- *Более 400 метров специализированной демонстрационной зоны «Транспортная безопасность»*
- *Ярмарка вакансий*
- *Три демонстрационно-тестовые зоны оборудования: видеонаблюдение, информационная безопасность, досмотр*

Наибольший интерес у посетителей выставки вызвали круглый стол «Инженерно-технические средства защиты банкоматов и платежных терминалов», конференция «Мобильные технологии и мобильные устройства в системе обеспечения безопасности», дискуссия «Передовые технологии защиты периметра и методы их применения», в ходе которых выступили известные эксперты в области защиты информации и прозвучали ответы на самые злободневные вопросы обеспечения своевременного реагирования на внешние угрозы и правонарушения.

Широкие возможности для диалога участникам Форума предоставил раздел «Пожарная безопасность», ставший универсальной площадкой для налаживания контактов между производителями противопожарного оборудования и ОПС, крупнейшими государственными и корпоративными заказчиками, представителями исполнительной и законодательной власти. По прогнозу аналитиков, к 2017 г. объем продаж оборудования охранно-пожарной сигнализации в странах EMEA (регион, включающий в себя Европу, Ближний Восток и Африку) достигнет 1,34 млрд долл. Экспертами было подсчитано, что приблизительно 29% посетителей ТБ Форума работают на пожароопасных объектах – промышленных предприятиях, строительных площадках, опасных объектах и производствах, предприятиях нефтехимической промышленности, объектах культуры и складах. 87% участников деловой программы Форума включают пожарные риски в модели угроз на своем предприятии.

Ключевыми проблемами в рамках данной проблематики были признаны обеспечение безопасности высотных и уникальных сооружений, новые технологии и технические средства защиты объектов транспортной инфраструктуры и транспортных средств от несанкционированного вмешательства и террористических угроз, совершенствование противопожарной защиты объектов ТЭК и внедрение инновационных технологий, передовые технологии охранной и пожарной сигнализации и методы их применения. «Для решения проблем безопасности огромное значение имеет внедрение научных достижений и современных технологий в области гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности, оснащения современной техникой и оборудованием подразделений МЧС России, специальных сил других ведомств и организаций. Для этого необходима самая полная информация о представленных на рынке надежных системах и решениях, о последних научных и технических разработках», – отметил во время Форума заместитель председателя Совета Ю.Л. Воробьев.

Сессионные заседания раздела «Технические средства защиты. Видеонаблюдение. Системы контроля и управления доступом. Интегрированные системы» были посвящены анализу российского и международного опыта эффективного использования систем видеонаблюдения и обсуждению передовых технологий видеонаблюдения, видеоидентификации, видеораспознавания, видеомониторинга и видеообнаружения. Большое внимание собравшихся привлекла конференция «Безопасность мегаполисов и крупных городов», в которой приняли участие представители УВД и соответствующих подразделений администраций 200 крупных городов России и СНГ, представители городских администраций, муниципальных организаций, компаний – владельцев коммерческой недвижимости.

Не смогли организаторы обойти стороной и такие важные темы, как информационная безопасность, защита связи, предотвращение утечек данных, обеспечение нормального функционирования информационной среды государства и частного бизнеса. Их обсуждение стало главной целью производителей, экспонентов и потребителей услуг безопасности. Раздел «Информация и связь» привлек крупнейших корпоративных и государственных заказчиков, отраслевых регуляторов, образовательные и научные учреждения – всех, кто заинтересован в повышении уровня информационной безопасности и разработке инновационных методов защиты связи.

По сообщению организаторов, в настоящее время открыта регистрация на участие в XIX Международном форуме «Технологии безопасности», который состоится 11–14 февраля 2014 г. в Международном выставочном центре Крокус Экспо.

Корпоративная безопасность: От контролирующего органа к эффективному архитектору бизнеса

По хорошей традиции самые сильные мужчины России и СНГ встретили долгожданную весну в профессиональной обстановке в рамках конференции «Корпоративная безопасность», ежегодно организуемой европейской компанией MSB Events.

Вторая ежегодная конференция «Корпоративная безопасность: От контролирующего органа к эффективному архитектору бизнеса» прошла с 28 февраля по 1 марта в московском отеле «Марриотт–Тверская». Главной темой мероприятия стало формирование нового образа директора по безопасности. Сегодня ожидания многих топ-менеджеров и владельцев бизнеса все чаще связаны с функциональным переходом департамента безопасности от контролирующего органа к эффективному архитектору бизнеса, принимающему активное участие в разработке стратегических решений и определении ориентиров дальнейшего развития.

В числе рассмотренных на мероприятии тем были такие, как противодействие коррупции, риск-ориентированный подход в контроле закупочной деятельности, особенности проверок поставщиков и покупателей в условиях применения требований международных антикоррупционных актов, опыт построения эффективных автоматизированных моделей выявления мошенничества в торговле, роль риск-менеджмента в системе экономической безопасности организации, роль департамента безопасности в процессе слияний и поглощений, инструменты службы безопасности, используемые для проведения служебных проверок и расследований, и многие другие.

Не могли участники обойти стороной такую популярную в последнее время тему, как рост числа электронных преступлений и атаки через каналы дистанционного банковского обслуживания (ДБО) – пластиковые карты, системы интернет-банкинга, колл-центры. В своем докладе, посвященном данной проблеме, менеджер отдела расследований ЗАО КБ «Ситибанк» Михаил Кутузов отметил, что 99% атак производятся на клиентские компьютеры, а потому пользователям необходимо постоянно помнить о правилах безопасности: осуществлять операции только через официальные сайты банков, не пользоваться услугами ДБО в местах, где Интернет является общедоступным (например в интернет-кафе), защищать свои устройства антивирусными программами и своевременно обновлять антивирусные базы данных.

Эксперт также перечислил основные меры, которые банки принимают для противодействия скиммингу: совершенствование технических средств защиты банкоматов, переход на чипованные карты, мониторинг срабатывания датчиков, видеомониторинг, мониторинг подозрительных операций. Был дан ряд полезных рекомендаций и для клиентов финансовых организаций, например не использовать незнакомые банкоматы, расположенные в затемненных, немноголюдных местах, удобных для деятельности мошенников, набирать PIN-код быстро, заученными движениями и желательно несколькими пальцами, прикрывая клавиатуру свободной рукой, сумочкой или кошельком.

В деловой программе конференции с докладом «Опыт построения эффективных автоматизированных систем выявления мошенничества в торговле» выступил руководитель направления fraud management & revenue assurance компании «Инфосистемы Джет» Алексей Сизов. По результатам исследований 95,5% потери выручки на предприятии происходит вследствие действий мошенников. Подобные преступления специалисты разделяют на внутренние (т.е. реализуемые сотрудниками, агентами или дилерами), клиентские и мошенничества третьих лиц. Основными причинами успешной деятельности преступников являются уязвимости в технологиях, процессах и контролях.

К типичным примерам мошенничества можно отнести сговор с представителями подразделений управления ценами и обработки безналичной оплаты, оформление товаров / услуг / договоров по поддельным документам, использование ошибок ПО и административных привилегий, использование активов компании в личных целях.

Докладчиком были рассмотрены следующие методы борьбы с мошенничеством на предприятии:

- предупредительные (проверки сотрудников, разделения прав и полномочий);
- заградительные (двойной контроль критичных операций, идентификация и аутентификация сотрудников);
- компенсационные (административные расследования, службы взысканий);
- оперативные (видеонаблюдение, охрана и пр.; системы fraud-мониторинга).

Подводя итоги своего выступления, А. Сизов назвал плюсы использования автоматизированных решений для борьбы с корпоративными мошенничествами. Прежде всего, это наличие единого информационного ресурса контроля рисков, открытого и прозрачного инструмента для подразделений безопасности, автоматизированных механизмов реагирования и контроля эффективности ключевых задач.

Актуальная тема конфликта интересов сотрудников контрольных подразделений при проведении специальных проверок была затронута директором департамента по контрольно-ревизионной работе ОК РУСАЛ Р.А. Богаутдиновым. Приведя различные определения понятия «конфликт интересов», докладчик отметил, что, будучи широко распространенным, оно прежде всего связано с рассогласованием личных интересов работника и интересов компании / сообщества. Представитель ОК РУСАЛ привел несколько практических примеров конфликта интересов.

Подводя итоги конференции, участники отметили усложнение бизнес-среды, появление новых видов угроз и необходимость разработки действенных инструментов и решений для успешной работы корпорации. В качестве итоговой сессии лидирующие компании провели отраслевой анализ основных рисков безопасности и выработали рекомендации по их преодолению. Б

«Облачные технологии: в ожидании роста»

19 марта 2013 г. в Москве прошла конференция «Облачные технологии: в ожидании роста». В мероприятии, организованным CNews Conferences и CNews Analytics, приняли участие представители российского рынка ИТ, системных интеграторов, а также специалисты отделов ИТ предприятий разных отраслей и масштаба деятельности.

Почти все игроки рынка облачных сервисов – поставщики, заказчики, эксперты – сходятся в том, что облачные технологии определят будущее ИТ-индустрии. Именно они станут «третьей платформой», которая придет на смену «второй» – персональным компьютерам, в свое время заменившим «первую» платформу – мейнфреймы. Крупному бизнесу облака позволяют высвободить дополнительные ресурсы для профильных направлений, сократив до минимума инвестиции в инфраструктуру и персонал. Для среднего и малого бизнеса – это возможность воспользоваться технологическим сервисом, который ранее был недоступен компаниям такого масштаба из-за высоких капитальных затрат.

ГЛАВНЫЕ РАСХОЖДЕНИЯ СРЕДИ СПЕЦИАЛИСТОВ ВОЗНИКАЮТ ПО ПОВОДУ ТОГО, НАСКОЛЬКО БЫСТРО ОБЛАКА «ЗАВОЮЮТ» МИР.

Расходы на публичные облачные сервисы растут в несколько раз быстрее, чем траты в других сегментах ИТ. По данным IDC, в 2012–2016 гг. темпы роста облачных расходов составят 26,4%, что в пять раз больше показателей ИТ-индустрии в целом. Неудивительно, что вопросы: когда выгодно обратиться к публичным облакам?; когда эффективнее решить бизнес-задачи с помощью корпоративного облака?; какие бизнес-направления удобно информатизировать с помощью облаков?; как выбрать облачного провайдера?; какие требования выдвигает облачная инфраструктура? и т.п. являются одними из самых животрепещущих для российских компаний. Именно на них эксперты попытались дать ответы в рамках конференции «Облачные технологии: в ожидании роста».

Главные расхождения среди специалистов возникают по поводу того, насколько быстро облака «завоюют» мир. «ИТ-индустрия находится в середине пути трансформации, так как компании инвестируют в новые технологии, которые будут драйвером роста и инновации на протяжении следующих двух-трех десятилетий. Мы ожидаем, что к концу этого десятилетия 80% роста отрасли будет так или иначе связано с облачными технологиями», – считает старший вице-президент и ведущий аналитик IDC Фрэнк Дженс.

Наиболее высокие темпы роста рынка облачных услуг в период до 2016 г. покажут Индия, Индонезия, Китай, Россия, Аргентина, Мексика и Бразилия. В Западной Европе рынок будет расти более медленными темпами в связи с экономическими сложностями. Так же замедлятся показатели Азиатско-Тихоокеанского региона из-за проблем на японском рынке.

Аналитики предрекают, что в течение пяти последующих лет на рынке облачных технологий сохранится доминирование США и других развитых стран: на долю Соединенных Штатов придется 61% совокупного роста 2010–2016 гг., еще 17% – на Западную Европу. По данным IDC, на развивающиеся рынки придется 30% от совокупного роста облачных расходов. Это связано с тем, что крупнейшие провайдеры публичных облачных услуг – Amazon, Apple, Google, IBM – имеют американскую прописку и предпочитают размещать дата-центры у себя дома. «Все площадки базируются на территории США, в Западной Европе, а также в Гонконге и Сингапуре. Насколько мне известно, никто из глобальных игроков не планирует в ближайшее время запускать дата-центры для поддержки публичных облаков на территории России», – отметил заместитель генерального директора DataLine Алексей Севастьянов.

«Лидерство принадлежит американскому рынку, именно там формируются тенденции и подходы, а далее они распространяются на Восток. Мы в этой цепочке замыкающие и, к сожалению, сильно отстаем (по моим оценкам, года на три, не меньше). Если посмотреть на ведущие решения, то Amazon на сегодняшний день в роли лидера, большинство остальных можно охарактеризовать, как «догоняющих», – прокомментировал ситуацию Владислав Епишкин, ведущий консультант Центра компетенции по поддержке корпоративных сервисов компании «Микротест».

По мнению специалистов, по мере того как облака будут совершенствоваться, они начнут оттягивать на себя ресурсы, которые крупный бизнес сейчас выделяет на частные облака. В первую очередь корпорации выводят во вне второстепенные сервисы, которые не критичны для бизнеса, например тестирование новых решений. Со временем публичные облака могут оттянуть на себя и более серьезные функции, хотя полный уход в коммерческие облака, скорее всего, будет характерен только для сектора среднего и малого бизнеса. Например, крупный банк вряд ли согласится на вывод во внешнее облако АБС.

Впрочем, этот тренд имеет национальную специфику, связанную с законодательством или уровнем развития облачных технологий в той или иной стране. «В России корпоративный сектор развивает частные облака, которые размещаются либо на их собственных площадках, либо «хостятся» в надежных коммерческих дата-центрах», – поделился заместитель генерального директора DataLine Алексей Севастьянов.

Не могли эксперты обойти стороной такую важную тему, как безопасность в облаках. Ей было посвящено выступление вице-президента Ассоциации профессионалов в области информационной безопасности RISSPA Дениса Безкоровайного «Безопасность данных в облаке – как строить отношения с сервис-провайдером». С хранением данных в облаке связаны основные тревоги пользователей облачных сервисов. Эксперт подчеркнул, что вопрос доверия к облачному провайдеру на сегодняшний день находится в списке наиболее острых. Определению степени надежности провайдера способствуют проведение аудитов со стороны заказчика, аудиты, организованные третьей стороной, а также процедуры сертификации.

Эта же проблема была поднята директором департамента ИТ ВИП Сервис Тимофеем Русских, предложившим поговорить об облаках «не с позиции вендоров». «Кто владеет дата-центром и где он распложен?»; «Сертифицирована ли площадка?»; «Какие дисковые пространства используются?» – эти и многие другие вопросы докладчик предложил задавать провайдерам для принятия верного решения.

В России мероприятия, посвященные облачным технологиям, проходят с завидной регулярностью, в том числе и в рамках профильных конференций по информационной безопасности. И это обоснованно, учитывая темпы роста облачных услуг. Аналитики международной компании IDC полагают, что в ближайшее время российский рынок облаков будет расти в среднем на 100% в год. А значит, экспертам еще долгое время будет что обсуждать.

Ваше мнение и комментарии присылайте по адресу

info@csc.ru

«Система видеонаблюдения: задачи и требования»

Современные системы безопасности предусматривают обязательное наличие систем видеонаблюдения. Сферы их использования столь разнообразны, что перечислить их все непросто. Это и контроль доступа в помещения, и визуальный мониторинг среды в коммерческих, технических, частных помещениях. Видеонаблюдение является непременным атрибутом умных домов. 20 марта информационное агентство РБК провело конференцию «Система видеонаблюдения: задачи и требования», посвященную наиболее актуальным аспектам этого явления.

Камеры видеонаблюдения, которые отслеживают действия покупателей в магазинах, уже давно стали привычны для жителей современных городов. Сегодня потребность в контроле над объектами растет не по дням, а по часам, о чем свидетельствует динамика спроса и предложения. С технической точки зрения реализовать систему видеонаблюдения просто – необходимо приобрести камеру, подключить ее к вычислительной сети и настроить режим фиксации. Именно поэтому сегодня все больше компаний используют одну или несколько камер, выбирая те или иные средства для организации эффективного видеонаблюдения.

Когда речь идет об установке камеры на существующем объекте – в офисе, в зале магазина или на входе в торговый центр, – безусловно, проще всего использовать уже имеющуюся инфраструктуру, подключая камеры напрямую к локальной вычислительной сети (ЛВС), либо проложить отдельный кабель к центру обработки данных (при использовании аналоговых камер). Также необходимо организовать передачу информации в центр обработки данных, выделить отдельные мощности для ее хранения и, возможно, анализа. Если же у компании нет желания заниматься весьма трудоемкими процедурами организации систем видеонаблюдения своими силами, подобные услуги можно заказать у телекоммуникационного оператора. Он де-факто обладает необходимой инфраструктурой для передачи данных, а также вычислительными мощностями и хранилищами данных для ее обработки. В частности, ведущие российские телекоммуникационные провайдеры уже предлагают подобные сервисы своим корпоративным заказчикам.

Сервисы видеонаблюдения востребованы сегодня коммерческими потребителями различных категорий. Они необходимы небольшим розничным магазинам и организациям, которые хотят контролировать доступ в свои помещения круглосуточно, так и крупным предприятиям, испытывающим потребность в улучшении качества наблюдения за всеми важными объектами, которые порой находятся на значительном расстоянии друг от друга.

Не на последнем месте находятся и государственные структуры. Такие как МВД, ГИБДД, МЧС, которые заботятся о повышении качества оперативного контроля над улицами городов и реагирования на экстренные происшествия. Для них дополнительные камеры являются необходимым ресурсом для сбора информации, которая помогает быстрее принимать правильные решения. По словам представителя оператора «ВымпелКом», сервисом видеоконтроля также интересуются крупные клиенты из таких отраслей, как ТЭК и FMCG. В столичной сети оператора на данный момент зарегистрировано 200 клиентов, использующих сервис «Видеоконтроль», но уже в текущем году их количество может достигнуть как минимум двух тысяч.

В 2012 г. были запущены масштабные проекты по созданию инфраструктуры постоянного наблюдения. Например, в Новом Уренгое создается информационная система «Безопасный город», которая будет следить за важнейшими развязками в автоматическом режиме, одновременно предоставляя специалистам доступ к оперативной и архивной информации по запросу. В Москве также растет число камер видеонаблюдения, которые обеспечивают порядок на улицах столицы и во дворах. Единая система городского видеонаблюдения создается в столице в рамках пятилетней программы «Информационный город 2012–2016».

Эксперты отметили, что в дальнейшем системы видеофиксации будут развиваться в сторону увеличения «интеллектуальности», т.е. совершенствовать свои возможности распознавания объектов, перемещений, выявления поведенческих свойств. Помимо выявления нарушений правопорядка, системы видеонаблюдения могут, например, подсчитывать количество объектов – автомобилей или людей. Как отметил заместитель директора департамента по работе с государственными организациями компании «Ай-Теко» Вячеслав Елагин, в настоящее время активно развиваются системы распознавания лиц, находящихся в розыске, причем большого прогресса в этом добились израильские специалисты. «Но наиболее востребованной будет услуга видеофиксации нарушений правил дорожного движения – это будет настоящий хит 2013 года», – добавил эксперт.

ЭКСПЕРТЫ ОТМЕТИЛИ, ЧТО В ДАЛЬНЕЙШЕМ СИСТЕМЫ ВИДЕОФИКСАЦИИ БУДУТ РАЗВИВАТЬСЯ В СТОРОНУ УВЕЛИЧЕНИЯ «ИНТЕЛЛЕКТУАЛЬНОСТИ», Т.Е. СОВЕРШЕНСТВОВАТЬ СВОИ ВОЗМОЖНОСТИ РАСПОЗНАВАНИЯ ОБЪЕКТОВ, ПЕРЕМЕЩЕНИЙ, ВЫЯВЛЕНИЯ ПОВЕДЕНЧЕСКИХ СВОЙСТВ.

Применению систем видеонаблюдения на транспорте были посвящены доклады начальника службы информатизации Дирекции железнодорожных вокзалов ОАО «РЖД» Александра Кархова (Интегрированная комплексная система безопасности железнодорожных вокзалов ОАО «РЖД»), начальника отдела ИТ ГКУ «Центр безопасности дорожного движения Московской области» Юрия Кузьменко («Системы видеонаблюдения для повышения безопасности дорожного движения») и генерального директора компании «БайтЭрг» Андрея

Прудникова («Мобильное видеонаблюдение – видеонаблюдение будущего. Персональное, быстроразворачиваемое, транспортное»).

«Сейчас можно говорить о том, что технологии в сфере видеонаблюдения развиваются по нескольким основным направлениям — интеллектуализация, синергия и интеграция, а также развитие облачных сервисов», – отметил Мурат Алтуев, президент компании ITV | AxxonSoft, выступавший с докладом «Будущее видеоаналитики». По словам Алтуева, главная отличительная черта современного видеонаблюдения – оно становится более умным. Разработка же долгосрочных проектов, таких как «Безопасный город», приводит к наращиванию огромных массивов видеоинформации, которую нужно:

а) эффективно хранить;

б) предотвращать несанкционированный доступ к ней, а также (и это, пожалуй, главное)

с) оперативно и эффективно анализировать. «Стало быть, активность разработчиков сосредоточится на поисках решений в сфере интеллектуального, надежного хранения архивов и баз данных, а также действенных инструментов для быстрого поиска в архиве», – заключил глава ITV | AxxonSoft.

В заключение аналитики подвели главные итоги встречи и назвали не только новые тенденции развития сетевого видео, но и перечислили недостатки предлагаемых решений. Была сформулирована и основная задача, стоящая перед разработчиками, – переход от систем видеонаблюдения к системам безопасности. По мнению собравшихся, в настоящее время системы видеонаблюдения развиваются по путям, далеким от нужд обеспечения безопасности, и вопрос интеграции до сих пор остается нерешенным.

Ваше мнение и комментарии присылайте по адресу

info@cnews.ru

19-я международная выставка и конференция

ОХРАНА, БЕЗОПАСНОСТЬ И ПРОТИВОПОЖАРНАЯ ЗАЩИТА

ufi Approved Event

MIPS MOSCOW

15 – 18 АПРЕЛЯ 2013 ГОДА
МОСКВА, ВВЦ, ПАВИЛЬОН 75

с 2013 года на ВВЦ!

Охранное телевидение и наблюдение

Технические средства обеспечения безопасности

Пожарная безопасность. Аварийно-спасательная техника. Охрана труда

Защита информации. Смарт карты. ID-Технологии. Банковское оборудование

2013 CARDEX IT Security

Организатор:

ITE

Тел.: +7 (495) 935 7350
Факс: +7 (495) 935 7351
security@ite-expo.ru

При поддержке:

МВД России

Генеральный партнер выставки:

BOLID СИСТЕМЫ БЕЗОПАСНОСТИ

www.mips.ru