Бизнес-разведка № 14

оглавление

Деловая разведка - цели и задачи

В. Креопалов
Как определить целесообразность создания КР на предприятии

М. Белкин
Конкурентная разведка - уже не терра инкогнита
Часть 2 (первая часть опубликована в журнале №2, 2004)

КР - ориентация на конечный результат

Конкурентная разведка улучшает корпоративную культуру

Организация и методы деловой разведки

Е. Кондэ
Создание службы конкурентной разведки банка - основные этапы

Деловые "боевые" игры (business war games). Что не надо делать
(часть 1)

Информационные ресурсы

А. Павлючиков
Формирование запросов в поисковой системе Yandex.

Д. Карпе
Онлайновый поиск персональной информации (часть 1)

Информационная безопасность и борьба с промышленным шпионажем

М. Власенко, О. Левина
Формальные и неформальные виды проверки при найме в банк

А. Ануфриев
Некоторые особенности информационной безопасности банков

Банковская безопасность

Г. Куборский
А сколько у Вас осталось на пластиковой карте?
(Мошенничество на рынке пластиковых карт)

Деловая разведка и право

Что считать конфиденциальной информацией?

Технологии деловой разведки

Где узнать о поисковых машинах англоязычного Интернета

Советы профессионалов

Десять правил написания контента для коммерческого веб-сайта

Рецензии. Обзоры литературы

**"Расследование компьютерных преступлений в странах СНГ",
Вехов В.Б. и Голубев В.А., 2004**

В. Креопалов

В. Креопалов

Как определить целесообразность создания КР на предприятии

Как руководители бизнес-организаций получают информацию, необходимую для принятия решения? Существует множество способов получения информации, но их можно свести к четырем основным, характерным для российских компаний:

Первый способ предполагает появление на рабочем столе руководителя нескольких отчётов, выполненных различными подразделениями. Например, квартальный отчёт отдела продаж об изменениях структуры рынка, долей рынка и.т.д. Часто такой отчёт при его внушительном объёме содержит мало сведений, которые действительно помогают принять оптимальное решение. Фактически большинство таких отчётов представляют собой просто кипы созданных компьютером страниц "сырой" информации. Многим такой метод не по душе, так как они не в состоянии проанализировать все отчёты, которые им надлежит изучить.
Этот способ при некоторых его достоинствах (простота подготовки и исчерпывающее изложение) часто не учитывает информацию, которая напрямую не связана с контекстом. Так отчёт о продажах обычно не показывает, как уровень заработной платы влияет на производство.

Второй способ: информация поступает от консультантов, которые постоянно отслеживают ситуацию в бизнесе и докладывают руководителю о текущем положении дел. К сожалению, этот способ отрицает какие либо отчёты, содержащие компьютерные данные, которые могли бы быть полезны руководителю. Другой недостаток заключается в том, что руководителю приходится подолгу выслушивать мнения, не связанные между собой и не содержащие контекстуальной привязки к информации. Преимуществом же этого способа является то, что он предполагает передачу не только информации, но и некоторого объёма сведений. Когда люди рассказывают о чём-то, они проводят определённый анализ, высказывают свои предположения и дают оценки сценариев и планов действий.

Третий способ основан на двух близких концепциях. Первая из них предполагает выбор некоторого числа индикаторов, отражающих экономическое "здоровье" предприятия и сбор информации по этим ключевым вопросам. В зависимости от вида бизнеса и представлений руководителя критическими для выживания предприятия могут быть такие ключевые индикаторы, как возврат продукции, жалобы клиентов, количество километров на литр бензина для транспортных средств предприятия и.т.д. Вторая концепция аналогична первой, но руководителю сообщаются данные не по всем выбранным ключевым индикаторам, а по тем, где показатели превышают заданную норму. Например, устанавливается предельный приемлемый уровень товарной наличности, а отчёт руководителю предоставляется, только по тем позициям, где этот уровень превышен.
Основное достоинство этого метода в том, что руководитель заблаговременно получает сигналы о неблагополучии в некоторых областях. Его недостаток - руководитель не получает идей, как выправить положение.

Четвертый способ: руководители подают заявки на получение нужной информации.

Потребность сопоставляется с существующими на предприятии информационными источниками, и пробелы заполняются путём создания дополнительных информационных ресурсов. Здесь в расчёт принимаются лишь те запросы, которые руководители считают необходимыми, а не то, что требуется на самом деле.

Очевидно, что ни один из описанных способов не удовлетворяет требованию достаточной осведомлённости руководителя. Руководителям, да и любому работнику предприятия, нужен метод, который позволял бы принимать верные решения, вникать в сущность бизнеса и побеждать конкурентов. Более того, предприятиям необходима должным образом организованная система для продвижения информации и сведений о фирмах, или другими словами конкурентная разведка (КР).

Широкому использованию конкурентной разведки на российских предприятиях препятствует недостаток средств. Рыночная информация, труд квалифицированных экспертов, не говоря уже об информационной технике и средствах связи, стоят весьма дорого. Когда средств не хватает - а их всегда не хватает! - надо внимательно изучить экономическую целесообразность вложения денег в эту службу. Существуют разные методы определения и оценки целесообразности создания КР.

Метод экспертных оценок
Формируется группа экспертов, которая даёт оценку эффективности существующим на предприятии методам получения информации для принятия решений.
Состав группы: руководители высшего звена управления предприятием.
Способ проведения: анкетирование.
Итог: на основании полученных ответов проводится анализ существующих методов и методов сбора и анализа информации, применяемых в конкурентной разведке.
Цель: даётся оценка целесообразности введения нового метода.

Метод "Постфактум" (post factum).
Сущность метода: анализ убытков, понесённых предприятием вследствие не правильно принятого решения в прошлые периоды времени без применения методов конкурентной разведки.
Способ: количественный подсчёт разницы между полученными убытками и затратами на проведение конкурентной разведки по конкретному факту.
Цель: обоснование целесообразности затрат на проведение конкурентной разведки.

Метод использования аналогов
Это изучение различных аспектов и функций процесса ведения конкурентной разведки ведущих в этой области компаний.
Способ: проведение бенчмаркинговых исследований.
Цель: обоснование эффективности деятельности службы конкурентной разведки на предприятии.

Конечной целью исследований является вывод о том, нужна ли КР предприятию.

Об авторе
Креопалов Владимир Владиславович родился 25 февраля 1968 года в городе Красногорске московской области. В 1990 году окончил факультет Электронной и оптикоэлектронной техники Московского Института Радиотехники Электроники и Автоматики, в 1993 году - Детектив-Колледж "Возрождение" на базе Академии МВД РФ. В 1997 году прошёл курс практического обучения в антитеррористической школе И. Линдера. В 2002 году - Институт Повышения Квалификации Информационных Работников по специальностям "Экономическая безопасность" и "Деловая разведка", в 2004 году Институт Безопасности Бизнеса и Личности Московского Энергетического Института (Технического Университета), по специальности Экономика и Управление на предприятии со специализацией управление экономической безопасностью.
С 1993 года занимается вопросами обеспечения безопасности предпринимательства, а также организацией служб безопасности в частных структурах. В 1995 году заместитель начальника службы безопасности крупной строительной компании. В 1998 году руководитель ЧОПа "СТЭК-МА".
С 2002 года и по настоящее время помощник заместителя Генерального директора по безопасности и кадрам ОАО "Красногорский Завод им С.А. Зверева".

М. Белкин

М. Белкин

Конкурентная разведка - уже не терра инкогнита
Часть 2 (первая часть опубликована в журнале №2, 2004)

Итак, вы приступаете к операции КР. Кто бы вы ни были - специалист по программному управлению базами данных, выходец из структур безопасности или недавний выпускник школы МВА, наступает момент, когда вы вступаете на практическую стезю конкурентной разведки.

Допустим, что вы не имеете практических навыков применения разведки в бизнесе, данный вам бюджет незначителен, вам приходится иметь дело с простыми и легкодоступными ресурсами и инструментами поиска, а главное - вы стремитесь как можно скорее доказать полезность и эффективность вашей работы в качестве профессионала КР.

Не надо бояться трудностей. Вы не первый, кто впервые ныряет в малознакомую стихию конкурентной разведки, и многие благополучно достигают своей цели. В только что сформированной службе КР ее руководителю часто приходится осуществлять самому весь цикл работы. Конечно, со временем появятся помощники, какая-то часть работы будет делаться в режиме "аутсорсинга", будут установлены сложные автоматизированные системы поиска, систематизации и анализа информации, но в небольших кампаниях всю эту работу, как правило, выполняет один человек.

Хочу предложить несколько рекомендаций и пожеланий, которые могут пригодиться новичку в области конкурентной разведки.

Быстро овладеть профессией. Коллеги считают, что вы все знаете в КР, но на самом деле это не так. Вы знаете немного. Впрочем, недаром говорят, что "в царстве слепых и одноглазый - король". Но надо еще доказать, что вы действительно король в этом деле. Советую обратиться к литературе по конкурентной разведке, регулярно просматривать учебную и иную, имеющую отношение к КР информацию в Интернете, посещать курсы, семинары, конференции. И вскоре вы обретете уверенность.

Кому вы отчитываетесь. Может быть, это самый деликатный и существенный вопрос. В компании функция КР должна непосредственно обслуживать тех, кто формирует политику компании, определяет ее стратегию. На практике так обстоит дело не всегда. Нередко между первыми лицами и экспертом КР стоят промежуточные лица, не всегда способные компетентно оценить результаты вашего труда. Но в любом случае необходимо помнить, что разведка относится к числу поведенческих дисциплин науки и умение строить правильные отношения с начальством - в зависимости от конкретной ситуации - дает вам огромные преимущества.

Определить задачи. Если служба КР создается с целью помогать формулировать и корректировать стратегию компании, то профессионалу КР необходимо быть в курсе текущих задач компании. Некоторые пытаются составить мнению по материалам внутриофисного Интранета, по поступающим сверху указаниям и документам. Этого, как правило, недостаточно. Известный постулат разведки, что "всегда остается камень, под который надо заглянуть", в нашем случае абсолютно правилен. Конечно, обеспечение доступа ко всем потенциальным источникам, дающим реальную картину политики топ-менеджмента, требует
усилий и затрат времени. Но это важно для того, чтобы ваша работа была высокоэффективной.

Не пренебрегать стандартными приемами. Разведка конкурентная, как и любая другая, не терпит шаблонов. Вместе с тем, не следует пренебрегать стандартными процедурами ведения КР, которые рекомендуют учебные заведения. Просмотрите специальную литературу, снимите копии с предлагаемых схем, стандартных приемов и методов.

Установить компьютерные программы. Чем глубже вы вникаете в процесс конкурентной разведки, тем больше вам требуется данных, тех или иных деталей. Чтобы управляться с

возрастающим потоком информации, надо заменить традиционные папки и каталоги соответствующими программными продуктами. Но при этом важно иметь в виду, что установка соответствующих программ решает не все, а только часть проблем работы с информацией. Необходимо точно знать, какие именно программные решения для вас действительно полезны, и можно ли их интегрировать с корпоративной системой, которая установлена в компании.

Не выбрасывать деньги на ветер. По разным оценкам, от 50% до 70% всей нужной для КР информации можно взять в компании, не прибегая к дорогостоящей внешней подписке. Тратить деньги на покупку информации извне (или привлекать информационные фирмы - "аутсорсинг") следует только в тех случаях, когда требуемая информация крайне необходима для осуществления проект КР, когда ее нет в ресурсах вашей компании, когда она не может быть найдена в свободном и бесплатном Интернете.
Как относиться к Интернету? Для некоторых специалистов нет на свете иных источников информации кроме Интернета. Это дело профессионального выбора. Дискуссия о достоинствах и недостатках Интернета лежит за скобками этой статьи. Хочу лишь отметить, что разведка относится, прежде всего, к личностным представлениям, оценкам и способностям - т.е к тому, что лежит за пределами Интернета.

Не забывать о запретной черте. Вы хотите классно работать. Но и спать спокойно тоже....Бывают ситуации, когда вас вынуждают пересечь правовые и этические границы, залезть в так называемую "серую зону". Ни в коем случае! Практически нет задач КР, которые можно было бы решить, не выходя из легальных и моральных рамок. Нарушение общепринятых ограничений не только создает угрозу престижу и репутации, а, следовательно, интересам фирмы, но и грозит вам бессоницей.

Профессиональные ассоциации могут быть полезными. Они бывают двух видов: отраслевая ассоциация в сфере профильной деятельности вашей компании, и ассоциация, связанная с вашей профессиональной работой, т.е. конкурентной разведкой. И те, и другие представляют ценнейший ресурс информации, без которой не обойтись. А главное, причастность к цеху придает чувство профессиональной уверенности.

Об авторе
Микаел Белкин - консультант по деловой и конкурентной разведке консалтинговой компании Shafran Ltd (Тель-Авив). Один из основателей и президент Форума конкурентной разведки Израиля. Член международного Общества профессионалов конкурентной разведки (SCIP), организатор и ведущий многих европейских конференций SCIP.
belkine@shafran-intelsec.com

КР - ориентация на конечный результат

КР - ориентация на конечный результат

Когда наступают трудные времена и приходится экономить, нередко служба конкурентной разведки оказывается в списке на сокращения. Почему так происходит? Что надо делать, чтобы этого не было?

Автор вопросов, А. Джонсон (www.AuroraWDC.com/arik.htm) пытается на них же и ответить в scip.online, issue # 33.

Как он считает, многие практики КР. будучи профессионалами, акцентируют внимание на процессе своей работы, на технике разведки, на деталях, иногда упуская из виду результат, ожидаемый заказчиком.

Сегодня от специалистов КР требуются разнообразные качества - знание всей информации о рынке и конкурентах, понимание, что такое risk management, умение разбираться в стратегическом планировании и многое другое. Стремясь к овладению знаниями, профессионал опять же решает задачу КАК работать. Это естественно для тех, кто

впервые пришел в конкурентную разведку. Они должны учиться тому, КАК успешно выполнять свою работу. Но не менее важно, подчеркивает Джонсон, понимать, КАКАЯ работа должна быть проделана, КАКИЕ результаты должны быть получены. В результате основное внимание надо фокусировать на процессе, а не на итогах. В этом отчасти виноваты и потребители КР, нередко спрашивая "всю информацию об объекте исследования", не утруждая себя вопросом, а зачем нужна эта информация, какие задачи она должна решать.

Поэтому, делает вывод А. Джонсон, деятельность КР-службы не всегда напрямую сопрягается с успехами и провалами компании. Конечно, ориентация на конечный результат - вещь для службы КР рискованная. Но риск оправдан. Успех работы меняет отношение внутри компании к экспертам КР в лучшую сторону, позволяет установить доверенные отношения с менеджерами других управлений, обеспечивает поддержку руководства. Наконец, уменьшает риск появления службы КР в списках на сокращение.....

КР улучшает корпоративную культуру

Конкурентная разведка улучшает корпоративную культуру

Наш журнал неоднократно публиковал материалы, доказывающие необходимость распространения системы КР предприятия/компании на все основные подразделения - отделы по продажам, поставкам и т.п. Практика давно доказала, что подключение к конкурентной разведке в той или иной форме служащих фирмы резко повышает реальную отдачу КР.

Райан Данн из государственного университета Идахо (Ryan Dunn - dunnchar@isu.edu) считает, что вовлечение персонала в КР благотворно влияет не только на сбор и анализ информации, но и на другие важные аспекты деятельности компании. В своей статье (scip.online, issue 33) он отмечает, что сопричастность сотрудников к КР позитивно воздействует на их профессиональные подходы и интересы, конкурентноспособность, лояльность, чувство корпоративности.

Организационную перестройку, связанную с созданием широкой системы КР, охватывающей все основные структуры компании, по его мнению, надо начинать с основных подразделений, занимающихся продажами, работающими непосредственно с клиентурой. Тех служащих, которые впервые сталкиваются с КР, необходимо обучить основам процесса КР, растолковать значение информации, которой они обладают. В идеале сотрудники помимо своих основных функций должны стать "информационными агентами", преодолевая узко-производственный подход к своим прямым обязанностям, разумеется, не в ущерб им. Более того, они расширяют свои знания о деятельности компании и отрасли в целом, что не может не сказаться на их работе благотворно.
При этом они должны понимать, что руководство ценит их и как работников, и как носителей важной информации, ждет эту информацию. Их участие в процессе конкурентной разведки заслуживает поощрения.

С другой стороны, прямая причастность персонала к КР помогает минимизировать риск несанкционированных утечек информации - на выставках, через сайты, рекламу и пресс-релизы. В ходе обучения азам КР служащие лучше осознают, насколько ценна информация, которой они обладают, как важно не допустить, чтобы она попала к конкурентам. Служащие учатся отличать праздное любопытство собеседников от профессиональных попыток что-то у них выведать.

Вовлеченность в процесс КР меняет отношение персонала к окружающей их информационной среде, воспитывая сдержанность в передаче информации о своей работе и компании, и в то же время приучая внимательно отслеживать поступающие извне новости о конкурентах, о рынке, об отрасли, своевременно передавая ее в службу КР. Так, например, водитель грузовика, доставляющий продукцию компании до потребителей,

может не без успеха собирать информацию о своих коллегах из конкурирующих фирм, развозящих товар по определенным адресам.

Е. Кондэ

Е. Кондэ

Создание службы конкурентной разведки банка - основные этапы

Без специализированной службы, которая занималась бы сбором и обработкой информации, в современной рыночной экономике выжить становиться весьма затруднительно. Противоборство в банковской сфере предполагает борьбу за клиентов, поиск и внедрение новых технологий, уменьшение "банковских рисков", связанных с "невозвратом" кредитов или неправильной прогнозной оценкой конкурентной среды. При ведении переговоров важна также информация о намерениях и добросовестности клиентов банка (особенно при кредитовании). Необходимым условием устойчивости банка становится наличие в распоряжении руководства аналитической информации о конкурентной среде, в которой функционирует банк.

Основные задачи, которые должна решать информационно-аналитическая служба банка:
* Сбор, оценка и накопление на регулярной основе информации в соответствии с рубрикатором, согласованным с руководством банка на регулярной основе (состав рубрикатора может быть достаточно различным, в зависимости от конкретного банка и его стратегических целей, ниже будет приведен пример подобного рубрикатора).
* Проведение мониторинга текущей информации о внешней конкурентной среде.
* Автоматический предварительный анализ потока собранных сведений (классифицирование).
* Анализ полученной информации и подготовка аналитических документов для руководства.
* Создание информационного массива данных для эффективного решения стратегических и тактических задач информационно-аналитической службы.
* Хранение и распространение аналитических материалов, подготовленных информационно-аналитической службой.
* Своевременное информирование лиц, принимающих решения и персонала о критически важных событиях.
* Разработку рекомендаций по совершенствованию системы экономической безопасности.
* Организацию информационного взаимодействия с единой информационной службой банка.
* Поддержание деловых контактов с сотрудниками министерств и ведомств, представителями деловых, научных и журналистских кругов.

Чтобы успешно решать эти задачи служба КР в коммерческом банке должна включать в себя и объединять в единое целое: добывающие структуры - источники информации; блоки сбора, обработки, анализа и предоставления информации; блоки оперативной оценки и предоставления информации; блоки управления информационно-аналитической системой. Причем не обязательно это должно быть большое подразделение с многочисленным штатом.

Не стоит забывать что чем больше подразделение, тем труднее им управлять. Кроме того, некрупные и молодые банки могут просто не найти средств на содержание большого отдела. В этом случае некоторые блоки могут перекрываться, дополняя друг друга. Такое решение может привести к увеличению времени поиска и обработки информации, но, с другой стороны, позволит значительно сократить расходы. Некоторые функции можно переложить на различные внешние консалтинговые агентства. Так, например, в случае, когда информационно-аналитическая служба только начинает свою деятельность и не может работать в полную силу, для решения некоторых, особенно критичных по времени исполнения ситуаций, можно привлечь сторонних подрядчиков. Однако, в этом случае банку может грозить некоторая утечка информации.

В идеальном варианте служба конкурентной разведки состоит из аналитического отдела, внешней и внутренней сетей сбора информации, а также обеспечивающих подразделений.

Основным правилом ее нормального функционирования является непрерывность работы. Задачи, решаемые этим подразделением, делятся на стратегические и оперативно-тактические. Причем для каждого конкретного банка соотношение стратегических и оперативно тактических задач различно. Это соотношение во многом определяет организационную структуру построения службы и специализацию персонала. Последний не обязательно раздувать, но он должен быть высокопрофессиональным. В составе команды должны быть специалисты различного профиля: поисковики информации, аналитики, специалисты в области информационных технологий. Нельзя экономить и на техническом вооружении этой службы.

Первым делом необходимо подобрать начальника создаваемой службы. Выбор во многом определяет будущую работу всего подразделения. В его обязанности входит координация внутренних и внешних информационных потоков, своевременная и полная информационная поддержка руководства при принятии решений, связанных с обеспечением безопасности банка в условиях конкурентной борьбы. Его должен полностью поддерживать руководитель банка.

Основные требования к личности руководителя информационно-аналитической службы можно сформулировать следующим образом:
* Личная преданность руководителю банка. Через него проходит вся информация, в том числе и компрометирующая руководство. Также в его распоряжении находятся конфиденциальные сведения, которые в случае, если они попадут к конкурентам, могут доставить большие неприятности вплоть до банкротства..
* Хорошая профессиональная подготовка.
* Финансовая независимость и кристально чистая репутация.
* Умение работать с собственным коллективом и представителями других подразделений банка и внешних организаций. Хорошая харизма полезна в любых сферах деятельности, но здесь она просто необходима.
* Смелость говорить правду в лицо вышестоящему начальству.
* Иметь высокую внутреннюю культуру.
* Физическое и психическое здоровье также играет немаловажную роль. Работа руководителя информационно-аналитической службы достаточно нервная и не во-время слегший в больницу начальник вполне может сорвать важный контракт.
* Последнее, и, наверное, одно из самых важных требований - умение держать язык за зубами.

Известный американский специалист в области деловой разведки сравнивает работу начальника информационно-аналитической службы с должностью королевского шута. "Шут был единственным в королевстве, кто мог непосредственно общаться с самим королем. Уважая мнение короля, он, тем не менее, не всегда соглашался с ним. В отличие от действительных королевских советников шут всегда оставался безнаказанным, когда говорил неприятные вещи. Ему была гарантирована защита от королевского гнева. Шут был находчивым и ловким человеком. Прогуливаясь по городу и слушая людей, он всегда знал, о чем говорят и думают королевские подданные. У него была налажена собственная информационная сеть, которая обеспечивала его надежной и своевременной информацией. Шут знал, что делает короля веселым, а что - грустным. Ему часто приходилось выполнять многие конфиденциальные поручения короля. Король понимал, что шут не всегда думает то, что говорит, однако часто следовал его советам" По сути, начальник информационно-аналитической службы должен уподобиться королевскому шуту. Он всегда должен говорить начальству правду, какой бы горькой она ни была.

Следующий шаг - разработка "программы реализации системы конкурентной разведки в банке". Программа разрабатывается начальником новой службы. В ней определяются цели и задачи новой службы, представлена организационная структура и этапы её развития, сформулированы функциональные обязанности сотрудников, определены источники финансирования, источники информации, приведен перечень основных потребителей аналитической информации и определены принципы взаимодействия с другими структурными подразделениями банка и внешними организациями. Определяется место информационно-аналитической службы в структуре банка.

При этом необходимо помнить, что основным потребителем продукции информационно-аналитической службы является первое лицо банка. Поэтому и сама служба должна быть подчинена непосредственно руководителю. Если информация доходит до руководства

через посредников (например, в роли посредника может выступать служба безопасности банка), нередко получается "испорченный телефон", посредники искажают или не пропускают не устраивающие их сведения.

Далее следует оценить информацию, уже находящуюся в распоряжении банка, и на основании полученных результатов создавать собственную систему сбора о распространения информации.
Заключительным этапом создания информационно-аналитической службы является подбор кадров и разработка этических и юридических норм. Подобранная команда должна быть сплоченной. Еще раз подчеркну, что большое количество кадров не нужно, главное, чтобы они были профессиональными. Требования к ним практически полностью повторяют требования к руководителю информационно-аналитической службы.

Деловые игры

Деловые "боевые" игры (business war games). Что не надо делать
Часть 1

Марк Чуссел, автор серии статей в scip.online о деловых играх по конкурентной разведке, более 30 лет посвятил вопросам разработки стратегии и принятия решений, в том числе н менее 16 лет - деловым играм. Возглавляя собственную кампанию Advanced Competitive Strategies, он сыграл ключевую роль в создании симуляционной программы ValueWar (mchussel@competing.com).

Его публикации в упомянутом издании (scip.online, ##31,32) в основном касаются того, чего следовало бы избегать при планировании и проведении деловых игр по КР.

Разработчики бизнес стратегии находят деловые "боевые" игры полезными по нескольким причинам. В частности, они помогают избегать не всегда приятных сюрпризов, дают возможности в спокойной обстановке "проиграть" различные варианты стратегических решений, прежде чем вкладывать деньги, способствуют установлению консенсуса в команде разработчиков бизнес-стратегии, позволяют приобретать опыт анализа состояния рынка, потребителей, конкурентов. В конечном счете, деловые игры помогают принимать правильные решения. В этом главное.

Итак, чего следует избегать?

Отсутствие четкой и ясной задачи.
Что вы хотите достигнуть с помощью деловой игры? Обучить анализу менеджеров? Подготовиться к совещанию по продажам? Стимулировать творческий подход? Отрепетировать новую стратегию? Подготовиться к принятию ответственного стратегического решения?
Важно определиться и соответственно выбрать подходящую модель игры - их много.

"*Играть в игру*"
Участвующие в игре естественно хотят выиграть и подстраивают игру под свои цели, идя по пути наименьшего сопротивления. Довольно легко можно выиграть, если строить модель деловой игры на основе предыдущего опыта, последних тенденций. Результаты игры в этом случае предсказуемы. Но и пользы от такого расклада мало. Гораздо труднее предвидеть, какие шаги и действия оправдывают себя, а какие нет, если использовать реалистическую модель деловой игры, базирующуюся на конкурентной динамике, которая не всегда предсказуема и очевидна. Программа деловой игры тогда действительно полезна, когда она выдает неожиданные результаты.

Шаблонный подход.
Никто сознательно не выбирает модель игры, опирающуюся на стандартные, штампованные походы. Все хотят, чтобы игра велась на принципах нетрадиционного мышления. Но часто происходит наоборот, причем подсознательно, когда выбирается

традиционный метод анализа.
Это может происходить в следующих случаях:

Когда отбираются варианты возможной стратегии. При этом игнорируются такие потенциальные варианты поведения, которые ни игроки, ни их конкуренты никогда не практиковали. Заранее даются параметры задачи: 10% сокращение расходов и т.п. Принимаются во внимание только собственные варианты стратегии, а конкурентам отводится пассивная роль, не учитываются их возможные контрмеры.

Когда игра выявляет победителей и проигравших. Модель игры, учитывающая изученный спрос, известные интересы потребителей, сама по себе не плоха. Но еще лучше такая модель, которая построена на принципе "что - если", т.е. что будет, если, к примеру, возможные в будущем изменения спроса неизбежно отразятся на избранной стратегии. Опять же речь идет о нестандартных размышлениях, выходящих за рамки статус-кво, которое установилось на рынке. Если участники игры упирают на "опыт", "историю", "тенденции", "прогнозы экспертов" и прочее, то вероятность шаблонного подхода высока.

А. Павлючиков

А. Павлючиков

Формирование запросов в поисковой системе Yandex.

Существуют два способа поиска в сети Интернет с применением поисковой машины Яндекс .

Простой поиск

Этот способ подходит тем, кто не разбирается в языке формального описания поисковых систем, однако хочет найти полезную для себя информацию в сети Интернет. При простом поиске необходимо лишь задавать Яндексу вопрос, как вы задаете его в беседе со знакомым. Например, "как пройти в библиотеку", "как продать гитару".
Если поиск не нашел ни одного документа, то вы, возможно, допустили орфографическую ошибку в написании слова. Если же вы набрали целую строку, то ошибка, скорее всего, будет в том слове, на которое вовсе нет или очень мало ссылок (эти ссылки мелким шрифтом выводятся под поисковой строкой Яндекса).

Если список найденных страниц слишком мал или не содержит полезных страниц, попробуйте изменить слово. Можно задать для поиска три-четыре слова-синонима сразу. Для этого перечислите их через вертикальную черту (|). Тогда будут найдены страницы, где встречается хотя бы одно из них. Например, вместо "фотографии" попробуйте "фотографии | фото | фотоснимки".
Если же список найденных страниц чрезмерно велик, попробуйте добавить несколько ключевых слов, касающихся основной цели поиска, в запрос. Например, вместо слова "гитара" можно ввести словосочетание "акустическая гитара".

Можно также воспользоваться поиском среди найденных страниц по измененному запросу. Для этого надо поставить галочку в соответствующем окне "поиск в найденном" на той же странице, где вы задаете свой вопрос Яндексу, а затем изменить ключевые слова запроса и запустить поиск заново.
Начиная слово с большой буквы, вы не найдете слов, написанных с маленькой буквы, если это слово не первое в предложении. Поэтому не набирайте обычные слова с Большой Буквы, чтобы увеличить количество найденных страниц. Заглавные буквы в запросе используйте только в именах собственных. Например, "карта России", "группа Машина времени".

Если один из найденных документов ближе к искомой теме, чем остальные, нажмите на ссылку "найти похожие документы". Ссылка расположена под краткими описаниями найденных документов. Яндекс проанализирует страницу и найдет документы, похожие на

тот, что вы указали.

Чтобы исключить документы, где встречается определенное слово, поставьте перед ним знак минуса. А чтобы определенное слово обязательно присутствовало в документе, поставьте перед ним плюс. При этом между словом и знаком плюс-минус не должно быть пробела. Например, запрос "частные объявления продажа велосипедов" выдаст вам много ссылок на сайты с разнообразными частными объявлениями о продаже самых неожиданных вещей, не имеющих никакого отношения к велосипедам. А запрос с "+" "частные объявления продажа +велосипедов" покажет объявления о продаже именно велосипедов.

С помощью специальных знаков вы сможете сделать запрос более формальным, а значит более точным. Например, укажите, каких слов не должно быть в документе, или что два слова должны идти подряд, а не просто оба встречаться в документе. Вы можете указать Яндексу не перебирать все словоформы, поставив восклицательный знак перед конкретным словом.

Яндекс умеет искать не только в тексте документа, но и отыскивать картинки по названию файла или подписи. Для этого на поисковой странице yandex.ru нажмите ссылку "расширенный поиск". В поле "Название картинки" впишите слова для поиска по названиям картинок, обычно появляющихся, когда к картинке подводится курсор.
В поле "Подпись к картинке" впишите название файла, содержащего картинку. Например, запрос dog найдет в сети Интернет все картинки, в имени файла которых встречается слово "dog".

Расширенный поиск

Яндекс обладает развитым языком запросов, позволяющим осуществлять тонкий поиск. Чтобы воспользоваться широким спектром возможностей, используйте страницу "расширенный поиск", где большая часть настроек Яндекса задается простым образом. Если вас интересуют операторы языка запросов, обратитесь к странице формального описания.
Посвятим несколько слов разделам страницы "расширенный поиск".

Словарный фильтр
Здесь вы можете указать, какие слова обязательно должны встретиться в документе, каких быть не должно, а какие желательны (то есть могут быть, а могут не быть). Поле "все формы" или "точная форма" указывает Яндексу, надо ли учитывать при запросе все словоформы. "Точная форма" обычно требуется только для поиска цитат.
Зоной поиска слова может быть как текст документа (слова находятся в одном предложении или всем документе), так и его заголовок, аннотация (тэг description), ссылка (подпись URL) или адрес (сам URL). Вариант "во фразе" означает необходимость искать слова в том порядке, в котором они введены. Вы можете задать несколько слов через запятую.

Дата
Ограничение выдачи документов по дате. Документы с неизвестной датой в этот список не включаются.

Сайт/вершина
Запрос идет только по страницам указанного сайта или поддиректории (вершины) сайта. Поиск будет проведен среди всех поддиректорий. Здесь же (в соседнем поле) вы можете исключить из поиска страницы определенного сайта. Вы можете внести несколько адресов, перечислив их через пробел.

Ссылка
Как узнать, кто ссылается на ваш ресурс? Введите в этом поле адрес вашей страницы, и вы это узнаете. Если адрес вашего сайта начинается с www, то впишите его целиком, включая www. Здесь же вы можете исключить из поиска страницы, где стоит ссылка на определенный адрес.
На основе этой возможности рассчитывается индекс цитируемости. Чтобы исключить все внутренние ссылки (то есть с одних страниц вашего ресурса на другие его страницы), используйте поле сайт/вершина и исключите ресурс из поиска ссылок.

Изображение
Поиск документов, содержащих картинку с определенным названием или подписью. Файл картинки может называться, например, applegreen.jpg. Тогда найти такие файлы можно запросом: apple. Запрос аналогичен apple*.*. Для поиска в подписи к изображению (тэг alt) впишите запрос в соседнее поле.

Специальные объекты
Поиск страниц, содержащих файлы объектов: скрипт, объект, апплет, java. В поле указывается имя объекта.

Язык
Яндекс умеет определять язык документа. Вы можете задать язык документа, где надо провести поиск. В базе Яндекса находятся только документы русскоязычного Интернета (по умолчанию в поисковую машину вносятся сервера в доменах su, ru, am, az, by, ge, kg, kz, md, tj, ua, uz), а также зарубежные сайты, представляющие интерес для русскоязычного поиска.

Формат выдачи
"Краткая выдача" означает, что будет выдан только список заголовков документов. "Только URL" - только адреса найденных страниц.

Об авторе:
Павлючиков Александр Евгеньевич, 1983 года рождения, студент Московского Энергетического Института.
E-mail: pavlu4ikov@yandex.ru

Д. Карпе

Д. Карпе

Онлайновый поиск персональной информации (часть 1)
scip.online, issue 32

Мне не раз приходилось по заказу клиентов погружаться в океан информации в попытках собрать персональную информацию либо о руководителях компаний и организаций, либо о достойном кандидате на вакансию, либо в процессе подготовки операций по слиянию и поглощению. Накопленный опыт позволяет предложить читателю некоторые ресурсы, которые могут весьма полезны. (Автор имеет в виду исключительно англоязычные источники - ред).

Зарплата и доходы

Если объект вашего исследования трудится в открытой акционерной компании (типа ОАО), то легко соберете массу информации о его/ее доходах на сайтах www.10Kwizard.com и www.edgar-online.com. Но они платные.
Правда, можете попытать счастья на правительственном (США) сайте www.sec.gov, где информация в свободном доступе.

Важно иметь в виду, что большинство открытых компаний указывают данные о зарплатах в ежегодных отчетах и иных аналогичных официальных документах. Поэтому можно найти искомую информацию, просматривая базы данных по предприятиям и фирмам, корпоративные сайты.

Сложнее обстоит дело с частными фирмами закрытого типа. Здесь вам помогут консалтинговые компании, которые специализируются именно в этом сегменте информации. Это, например, Hoover's или AON, которая предлагает бесплатный доступ к некоторым базам данных о персоналиях на сайте www.eComponline.com

Лично автор предпочитает обращаться к сайтам www.Salary.com и www.CareerJournal.com

(последний принадлежит журналу Wall Street Journal.

Советы Директоров

Вашему клиенту важно знать, в советы директоров каких корпораций искомый объект входит. Здесь полезными могут быть специализированные издания и публикации по вопросам корпоративного управления, равно как и многочисленные исследовательские центры. Мне особенно нравится журнал
Board Member magazine (www.Boardmember.com), но доступ в него платный. Я также часто использую библиотечные источники разных бизнес-школ, но они отнимают немало времени.
Что касается упомянутых выше центров и исследовательских групп, то я предпочитаю The Corporate Library (www.thecorporatelibrary.com). Можно им позвонить или послать запрос по электронной почте. Можно также попробовать "покопать" информацию на сайте (www.nacdonline.org), принадлежащем National Association of Corporate Directors. Если вы ищете персональную информацию по Европе, то полезно обратиться в European Corporate Governance Institute (www.ecgi.org).

Кто и как спонсирует политические партии и организации

В поисках ответа на такой вопрос нелишне начать с ресурса правительства США - Federal Election Commission. На сайте комиссии (www.fec.gov) масса линков. Вы можете, например, поискать по адресу: http://herndon1.sdrdc.com/fecimg/query.html. Если безрезультатно, то посмотрите карту сайта и войдите в раздел search/view reports.

В целом же данные здесь рекомендации позволяют раскрыть достаточно полную информацию практически о любом, независимо от того, в какой корпорации он работает или руководит. Конечно, важно иметь в виду этические и моральные аспекты, вытекающие из специфики персональной информации. Поэтому так важно, приступая к работе, хорошенько подумать, зачем вам (клиенту) нужна персональная информация и что с ней собираются делать.

Об авторе
Дэвид Карпе (David Carpe) закончил George Washington University и имеет MBA диплом в области финансов и предпринимательства Babson College.
Работал в качестве консультанта по менеджменту, основателем и руководителем одной из компаний по программному обеспечению, а в последнее время сотрудничает с Clew, LLC (www.clew.us).
С Дэвидом можно контактировать через contact@clew.us

Д. Карпе

Д. Карпе

Онлайновый поиск персональной информации (часть 1)
scip.online, issue 32

Мне не раз приходилось по заказу клиентов погружаться в океан информации в попытках собрать персональную информацию либо о руководителях компаний и организаций, либо о достойном кандидате на вакансию, либо в процессе подготовки операций по слиянию и поглощению. Накопленный опыт позволяет предложить читателю некоторые ресурсы, которые могут весьма полезны. (Автор имеет в виду исключительно англоязычные источники - ред).

Зарплата и доходы

Если объект вашего исследования трудится в открытой акционерной компании (типа ОАО),

то легко соберете массу информации о его/ее доходах на сайтах www.10Kwizard.com и www.edgar-online.com. Но они платные.
Правда, можете попытать счастья на правительственном (США) сайте www.sec.gov, где информация в свободном доступе.

Важно иметь в виду, что большинство открытых компаний указывают данные о зарплатах в ежегодных отчетах и иных аналогичных официальных документах. Поэтому можно найти искомую информацию, просматривая базы данных по предприятиям и фирмам, корпоративные сайты.

Сложнее обстоит дело с частными фирмами закрытого типа. Здесь вам помогут консалтинговые компании, которые специализируются именно в этом сегменте информации. Это, например, Hoover's или AON, которая предлагает бесплатный доступ к некоторым базам данных о персоналиях на сайте www.eComponline.com

Лично автор предпочитает обращаться к сайтам www.Salary.com и www.CareerJournal.com (последний принадлежит журналу Wall Street Journal.

Советы Директоров

Вашему клиенту важно знать, в советы директоров каких корпораций искомый объект входит. Здесь полезными могут быть специализированные издания и публикации по вопросам корпоративного управления, равно как и многочисленные исследовательские центры. Мне особенно нравится журнал
Board Member magazine (www.Boardmember.com), но доступ в него платный. Я также часто использую библиотечные источники разных бизнес-школ, но они отнимают немало времени.
Что касается упомянутых выше центров и исследовательских групп, то я предпочитаю The Corporate Library (www.thecorporatelibrary.com). Можно им позвонить или послать запрос по электронной почте. Можно также попробовать "покопать" информацию на сайте (www.nacdonline.org), принадлежащем National Association of Corporate Directors. Если вы ищете персональную информацию по Европе, то полезно обратиться в European Corporate Governance Institute (www.ecgi.org).

Кто и как спонсирует политические партии и организации

В поисках ответа на такой вопрос нелишне начать с ресурса правительства США - Federal Election Commission. На сайте комиссии (www.fec.gov) масса линков. Вы можете, например, поискать по адресу: http://herndon1.sdrdc.com/fecimg/query.html. Если безрезультатно, то посмотрите карту сайта и войдите в раздел search/view reports.

В целом же данные здесь рекомендации позволяют раскрыть достаточно полную информацию практически о любом, независимо от того, в какой корпорации он работает или руководит. Конечно, важно иметь в виду этические и моральные аспекты, вытекающие из специфики персональной информации. Поэтому так важно, приступая к работе, хорошенько подумать, зачем вам (клиенту) нужна персональная информация и что с ней собираются делать.

Об авторе
Дэвид Карпе (David Carpe) закончил George Washington University и имеет MBA диплом в области финансов и предпринимательства Babson College.
Работал в качестве консультанта по менеджменту, основателем и руководителем одной из компаний по программному обеспечению, а в последнее время сотрудничает с Clew, LLC (www.clew.us).
С Дэвидом можно контактировать через contact@clew.us

М. Власенко, О. Левина

М. Власенко, О. Левина

Формальные и неформальные виды проверки при найме в банк

Безопасность банков в значительной мере зависит от лояльности персонала. Как показывают социологические исследования, проводимые в России и за рубежом, наибольшее число преступлений в кредитно - финансовой сфере совершаются собственными служащими, либо при их пособничестве или бездействии.

Наиболее распространены такие преступления как продажа информации о деятельности собственной организации и клиентах, движение финансовых средств по счетам криминальным структурам и конкурентам, участие в переводе денег по фальшивым авизо, обмен фальшивой валюты, наводки грабителей и рэкетиров на свой банк, его обменные пункты. Наряду с этим в век активного развития информационных технологий, основная проблема персонала, особенно ИТ-служб и подразделений ответственных за безопасность, которые лучше других должны разбираться в предмете - халатное отношение к сохранности в тайне паролей доступа к информационным ресурсам банка.

Преступными элементы и конкуренты широко внедряют "своих людей" в банковские и деловые структуры. Применяются различные способы:
- вербовка уже работающего в банке или на предприятии сотрудника:
- внедрение под благовидным предлогом (трудоустройство, предложение консалтинга, аудита) в банк или предприятие профессионала-финансиста (экономиста, юриста и т.п.), подконтрольного криминальной структуре или конкурентам, далее постепенное его продвижение на ответственные посты в банке;
- подбор, воспитание и последующее внедрение в финансовые и деловые структуры наиболее талантливых студентов финансовых, экономических, юридических и технических ВУЗов, часто без согласия и ведома последних (использование "втемную").

Данные обстоятельства во многом определяют необходимость системного подхода к кадровой работе, начиная с осмысления и формализации требований к будущему работнику, грамотно организованной и тщательно проведенной процедуры поиска, проверки кандидата на должность, реализации комплекса контроля текущей деятельности, развития персонала и т.д.

Методы проверки при первом приближении....

Вся сообщенная кандидатом информация должна быть тщательно проверена подразделением банка, отвечающим за безопасность, а в идеале дополнительно подтверждена независимыми источниками. Не важно, идет ли речь о представленных документах или озвученных фактах из биографии кандидата.

В реальной жизни наиболее часто проверяется информация, лично сообщенная кандидатом. Традиционно эти сведения собственноручно излагаются кандидатом в специально разработанной анкете, которая органично дополняет стандартную форму Т-2, не дающую объективного и всестороннего представления о личности будущего сотрудника.
Специальные анкеты, наряду с вопросами о предыдущих местах работы (причины увольнения, выполняемые трудовые обязанности, взаимоотношения с коллегами по работе и т.п.), дополняются рядом других позиций, существенных для выполнения обязанностей на предлагаемой должности.
Перечни вопросов для таких анкет составляют специалисты подразделений, где предстоит работать будущему сотруднику совместно с представителя ми подразделения безопасности,, службы персонала. В отдельных случаях могут привлекаться психологи, специалисты узкого профиля по ключевым для данной должностной позиции направлениям.
Например, вопросы могут включать: сведения о судимостях, обязательствах перед другими организациями, ограничения по здоровью или командировкам, выездам за границу, другие...
Часто такие проверки сводятся к формальной сверке данных и телефонному опросу руководителя, кадровика или представителя безопасности бывшего работодателя.
Объективность, полнота и достоверность таких опросов не поддается никакой критике, особенно если речь идет о целевом внедрении такого "кандидата" в конкурирующую

структуру. "Легенда", информационное, организационное, документальное и другое обеспечение готовится на высшем уровне. Будущий работодатель получит исключительно положительный отзыв, без тени сомнения "проглотит наживку".

Проверка кандидата. Более серьезный подход....

Более информативной и результативной является проверка документально подтвержденных фактов биографии будущего коллеги. При этом проводится дополнительный сбор и уточнение заявленных данных в местах его работы за последние 10-15 лет.

Проверке подлежат следующие данные:
- Сведения о рождении (не живет ли он по чужим документам, не разыскивается ли).
- Образование (соответствие знаний диплому и факт учебы в ВУЗе). Необходимо учитывать тот факт, что в этот период формируются личностные качества. Изучая проявления человека в период обучения в ВУЗе, многое можно о нем узнать. Беседы с преподавателями, бывшими сокурсниками помогут более глубоко раскрыть личности кандидата.

Интересные факты можно узнать анализируя общественную деятельность кандидата, которая развивает у человека навыки общения, развивает организаторские способности, коммуникабельность, кругозор, профессиональные знания, дает связи и признание.

О многом могут поведать причины перехода с одной работы на другую. Формальные записи в трудовых книжках не раскрывают в полной мере глубину межличностных конфликтов и истинных причин перемены мест. Совместительство, подработки и прочее не фиксируются вообще.
Беседа с поручителями или людьми, рекомендовавшим Вам кандидата, в большинстве случаев не будет в полной мере объективна. Первые склонны к приукрашиванию ситуации, не откажутся от своих слов и в большинстве случаев положительно охарактеризуют рекомендуемого. Часто скрываются истинные причины частой смены работы, негативные личные качества, отрицательные проявления, имевшие место во время работы.

Большой плюс таких мероприятий- возможность через рекомендателя выхода на людей, хорошо знающих кандидата, от которых можно получить дополнительные сведения о конкретном человеке.
В этом случае работает золотое правило: "Сколько людей- столько мнений". В то же время нужно помнить, что правило: "Такое количество людей не может ошибаться" может сформировать у проверяющего субъективное представление об исследуемом объекте и как следствие - принятие неправильного решения относительно его личностных качеств. Как следствие- потеря ценного кадра.
Об этом необходимо помнить!

Что касается мнения соседей - данная информация не может приниматься за основу, так как человек склонен к противоправным деяниям, никогда не станет афишировать свои намерения. Такие люди отличаются нейтральностью в поведении и скрытностью образа жизни. Все, о чем говорят соседи, лишь косвенно может подтверждать или опровергать имеющиеся данные, да и то только в совокупности с другими сведениями.

Многие руководители кредитных организаций, ответственные за принятие решения о приеме на работу, "попадаются на удочку", веря словесным рекомендациям своих друзей, знакомых, сотрудников банка, экономя средства и время на проведение более глубокой проверки деловой репутации будущего сотрудника, уровня его компетентности, профессиональных качеств, оценке степени соответствия вакансии.

Еще одно, активно используемое направление кадровой работы, практикуемое в коммерческих банках - попытка вскрытия негативных фактов из жизни кандидата.

Поиск и сбор таких данных - вещь дорогостоящая, довольно трудоемкая и сложная. Не во всех случаях гарантирован результат. Вместе с тем, данный подход обладает одним несомненным преимуществом - при проведении такого поиска часто вскрываются сведения, прямо или косвенно связанные жизнью изучаемого объекта фактами, обозначенными в ранее заполненной анкете и письменно подтвержденные последним.

Проверяющий должен быть готов к подтверждению сомнительных и, на первый взгляд, невероятных фактов биографии, или опровержению ранее сделанных выводов, казалось бы, не подлежащих сомнению.

Информация собирается таким образом, чтобы объект изучения не мог повлиять на результаты исследований, либо ему проблематично было бы оказать такое воздействие.
В силу существующих законодательных ограничений, мероприятия по сбору информации, ее систематизации, в большинстве случаев решаются силами аналитиков подразделения безопасности банковской структуры, иногда через их связи в правоохранительных органах. Иногда такого рода поручения выполнят на договорной основе специализированные организации или частные детективы.

Другие методы проверок "своими силами", практикуемые при приеме на работу.

Проверка представленных кандидатом документов.

В век научно- технического прогресса, развития компьютерной и множительной оргтехники, моды на фальшивомонетничество, актуальным стал вопрос проверки подлинности документов предъявляемых при приеме на работу.
В последние годы получили развитие изощренные высокотехнологические приемы подделок. Практикуется и банальная переклейка фотографий в паспортах (в том числе нового образца), замена страниц. Активно покупаются свидетельства и сертификаты о профессиональной переподготовке, дипломы о высшем образовании. Приобретаются как чистые бланки с последующим внесением всех необходимых записей, так и подлинные документы ВУЗа без прохождения какого-либо обучения в нем.
В любом из этих случаев под удар некомпетентности отдельного индивида ставиться не только репутация банковской структуры, но и вся деятельность организации.
Рассказ о технологии проверки подлинности представленных кандидатом на должность документов - тема отдельного разговора.

Обратим внимание на некоторые виды возможных проверок кандидата по линии государственных структур.

Проверка сведений, изложенных кандидатом в анкете, при условии его письменного согласия (наличия записи о разрешении на проверку собственноручно подписанной кандидатом) может осуществляться на вполне законных основаниях через государственные структуры:
по учетам МВД РФ (проверяется наличие судимостей, статьи по которым был осужден кандидат, наличие материалов компрометирующего характера - связей в преступном мире, другие...);
по учетам территориальных отделов милиции - факты и причины задержания, исполнение приговоров;
по административной линии - алименты, штрафы, факты и условия владения оружием (охотничьим, служебным, спортивным, самообороны);
работа в негосударственных предприятиях безопасности, наличие лицензий (допуска) к охранной или детективной деятельности, причин увольнения с правоохранительных органов, и т.п.);
по учетам наркологического и психоневрологического диспансеров;
ЖЭКи и домоуправления по месту жительства- сведения о прописке, жилплощади, членах семьи, владельцах недвижимости.
Паспортные столы- замена, утеря паспорта. Оформление загранпаспорта.
Военный комиссариат- данные о прохождении службы, льготах....
Поликлиника по месту жительства- состояние здоровья, даты и причины обращений, больничные.
Отдел ГИБДД района- сведения об автотранспорте, водительском удостоверении, нарушениях правил вождения, административных взысканиях.

Другие возможные источники информации о кандидате.

отделы кадров по месту его прежней работы;
общественные организации, в которых состоял (состоит) проверяемый;
коммерческие структуры, с которыми ранее работал кандидат;

руководители и сотрудники организаций, где часто бывает данное лицо;
спортивные клубы, автосервис, магазины, лечебные заведения.
школы, ВУЗы, техникумы (директора, учителя могут дать независимую объективную характеристику кандидату);
беседы с лицами, которые рекомендовали его на работу в коммерческую структуру (учитываются их взаимоотношения).
соседи по дому, гаражу, даче.
коллеги по увлечениям, занятиям спортом.
использование специализированных баз данных, находящихся в свободном доступе в Интернет и в свободной продаже на рынках;
изучение публикаций о кандидате, или за его авторством в СМИ (в том числе электронных);
поиск информации в Интернет о переписке, записи в телеконференциях, обмен данных в ICQ и других интернет ресурсах.

Подробный анализ сведений из выше представленных источников позволит выявить скрытые от посторонних глаз (в том числе умышленно) грани жизни будущего коллеги: его наклонности, пристрастия, сильные и слабые стороны, увлечения, состояния здоровья, и т.д.

Кого проверять?

Каждый сотрудник, выполняя свои служебные обязанности, принимая участие в бизнес процедурах, наделяется определенными полномочиями и получает доступ к внутренней информации банка. Его положение в иерархии бизнес - структуры прямо связанно с возможностями нанесения ущерба, его величиной и возможными последствиями.
Технология проверки, глубина, финансирование контрольно - проверочных мероприятий зависят от величины риска (вероятности) нанесения интересующим лицом отрицательных последствий.

С учетом вышесказанного, ответим коротко: Проверять нужно всех кандидатов! А вот насколько тщательно?...

Как проверять?

Технологию проверки кандидата по длительности, тщательности проведения, полученному результату условно можно разделить на три уровня: поверхностный, средний и глубокий.

ПОВЕРХНОСТНЫЙ уровень проверки предполагает получение информации от самого кандидата, визуальную проверку подлинности представленных им документов, оценку степени соответствия его деловых и личностных качеств требуемой должности.
Проводится на первом собеседовании силами сотрудника службы персонала.

Основными достоинствами этого метода является:
быстрое получение информации непосредственно от кандидата, возможность выяснить степень соответствия уровня профподготовки необходимому для конкретной должности.
Возможность расстаться с кандидатом без взаимных претензий и исполнения в будущим, каких - либо обязательств.
Нет необходимости раскрывать специфику должностных обязанностей и содержание бизнес - процессов в своей организации, что положительно с точки зрения защиты информации. Кандидат получит минимум сведений об организации (если причина поступления на работу - их сбор).
На его проверку будет затрачено минимальное количество ресурсов. Это особенно актуально при массовом приеме сотрудников;
Позволяет сразу отсеять неподходящих кандидатов с позиции профессионализма силами сотрудника службы персонала.

Основной недостаток этого метода - нет гарантий выявления негативных фактов из жизни кандидата, отсутствует возможность проверки подлинности представленных документов. Не факт, что отдельные записи в них не будут фальсифицированы.

В качестве примера: В филиал одного из быстро развивающегося банка г. Москвы пришла на собеседование представительная молодая девушка на должность менеджера

кредитного департамента. Уровень профессиональной подготовки, правил ведения бизнеса, уверенное владение финансовыми программами и оргтехникой полностью соответствовали предъявленным требованиям. Она имела достаточный опыт работы в профильных организациях.
При рассмотрении менеджером по персоналу ее анкеты, насторожил факт частой смены работодателей. После тщательно проведенной проверки сотрудники службы безопасности банка выяснили, что девушка неоднократно подозревалась бывшим руководством в сговоре с клиентами, получении денежных вознаграждений от них. Правда, доказать этого не разу не удалось - она работала очень аккуратно. Когда ее деятельностью начинали активно интересоваться, уходила сама.

Каждый руководитель перед принятием решения о зачислении в штат нового сотрудника должен отдавать себе отчет в том, что вскрыть истинные причины прихода в организацию нового сотрудника, его мотивы, получить подтверждение истинности изложенных кандидатом сведений о себе возможно только при более глубоком уровне проверки.
Такие проверки требуют более глубокого изучения кандидата, сбор дополнительных сведений, больших трудозатрат, времени и соответствующего финансирования. В большинстве случаев, мнимая экономия и самоуверенность в неуязвимости руководимой структуры приводит к фатальным последствиям последней.

СРЕДНИЙ уровень проверки предполагает детальное изучение, дополнение и подтверждение сведений сообщенных кандидатом о себе ранее.
Проводится во время и после второго собеседования силами сотрудника службы персонала и представителя безопасности.

В отличие от поверхностного уровня, на среднем уровне проверки, полученные от кандидата данные проверяются, дополняются и уточняются силами подразделения безопасности с использованием методов, источников и технологий, о которых говорилось выше. Задействованы альтернативные источники. Проводится сравнительный анализ, сопоставление и комбинация данных.

Если в результате проверки никаких компрометирующих (препятствующих принятию на работу) обстоятельств не обнаружено, считается, что кандидат успешно выдержал и эту проверку.
Несмотря на это, необходимо помнить, что в его биографии могут существовать некие отрицательные моменты, вскрыть которые пока не удалось. Возможно, ваш кандидат более профессионален в искусстве обмана , чем ожидалось..
Помните: Благонадежные на первый взгляд люди могут отрицательно проявлять себя с самой неожиданной стороны при соответствующем стечении обстоятельств.

В качестве примера: Один из московских банков, обслуживающий бюджетные организации и коммерческие фирмы, в конце 2002 года потерял крупного клиента - одно из предприятий строительного комплекса г.Москвы, работающего по правительственным программам строительства жилья. Убытки банка составили более 5 миллионов долларов.
Причиной послужила выходка сотрудника отдела информационных технологий, продавшего за 500$ программу шифрования информации в каналах клиент- банк, с генератором ключей, точно повторяющих алгоритм формирования для указанной организации.
Данный программный продукт был случайно обнаружен службой безопасности строительной компании на одном из рынков Москвы в свободной продаже. Экстренно принятые меры позволили предотвратить утечку сведений о платежах и контрагентах.
При проведении расследования служба безопасности банка вскрыла факты продажи сотрудником отдела информационных технологий, нелегальной продажи программных продуктов, другие серьезные нарушения, а также факт принудительного увольнения данного сотрудника с предыдущего места работы (где работал по трудовому соглашению без записи в трудовой книжке) за нелегальное копирование и продажу программного обеспечения, принадлежащего на правах собственности бывшему работодателю.

Третий - этап ГЛУБОКОЙ проверки - предусматривает углубленное изучение кандидата по отдельным направлениям с целью выяснения его истинного содержания, а не продемонстрированного в процессе прохождения собеседования, а позднее и испытательного срока.
Проводится перед принятием решения о начале прохождения испытательного срока и в

течение этого срока силами сотрудников подразделения безопасности, привлеченных психологов, медиков, специалистов полиграфа, других.
Возвращаясь к истории с нерадивым сотрудником отдела ИТ. Кроме поиска и проверки на предыдущем месте работы сотрудник службы безопасности мог бы поговорить с его коллегами по подразделению, близкими друзьями. Наверно он был бы очень удивлен, услышав, что первый мог с легкостью потратить 3500$ на портативный компьютер, через два месяца приобрести тур по Европе, а спустя полгода снять дорогую квартиру при зарплате чуть менее 700$ в месяц. Задуматься об источниках "левого" дохода. Задать эти и другие "щекотливые" вопросы при подключенном полиграфе...

При реализации этапа глубокой проверки предполагается:
тестирование на профессиональную пригодность, определение уровня IQ, скорость и нестандартность принятия решений, истинные мотивации прихода в компанию, состояние здоровья, быстрота реакции, психофизиологическое и ряд других.
Проведение проверок правдивости изложенных о себе сведений с использованием полиграфа (детектора лжи).
Проведение проверок на выявления скрытых психофизиологических реакций его организма, о которых не знает сам испытуемый.
В некоторых случаях положительный эффект дает метод провокаций и участие испытуемого в ситуационных играх.

Пара слов о рекомендациях и резюме.

Еще один важный элемент, на который также стоит обратить пристальное внимание. Это рекомендации и резюме.
Наличие рекомендаций у кандидата еще не факт, подтверждающий его эффективную трудовую деятельность на прошлом месте работы. Большинство российских компаний никогда не проверяет рекомендации. А зря. На Западе официально признано, что 25% рекомендаций представляемых кандидатами - фальшивые, а остальные не рассматриваются в качестве весомого аргумента в пользу высокого профессионализма кандидата.
С резюме похожая ситуация. Некоторые западные специалисты называют резюме "кривыми зеркалами". Они отражают лишь то, что выгодно кандидату. Поэтому все рекомендации желательно тщательно проверять, а вместо представленного резюме самостоятельно подготовить объективную справку о кандидате. Иногда этим занимается менеджер по персоналу, часто совместно с психологом и сотрудник подразделения безопасности по результатам собеседований, тестирований, на основе предоставленных кандидатом и собранных о нем дополнительных сведениях.

Несколько советов: как работать с письменными рекомендациями.

Рекомендации имеют смысл, когда информация, содержащаяся в них, непосредственно связана с работой. Запрашиваемая информация должна относиться к знаниям, умениям и навыкам или другим характеристикам кандидата, необходимым для успешного выполнения конкретной работы. Акцент следует делать на те характеристики, которые отличают эффективных работников от неэффективных.
Проверка рекомендаций должна быть справедливой и валидной. Если система проверки рекомендаций несправедливо дискриминирует какую-либо группу или не имеет отношения к успешности выполнения работы, следует изменить эту систему или отказаться от нее. Если этого не делать, то это не только юридически неправомерно, но и будет ставить под сомнение способность организации отбирать компетентных работников.
При проверке рекомендаций следует опираться на объективную информацию (биографическую или поведенческую), а не на субъективную (например, субъективная оценка личностных качеств).
У кандидата следует запрашивать письменное разрешение на контакт с теми лицами, которые дали им рекомендации. При контакте с лицом, давшим рекомендацию, следует выяснить, как долго он (она) знает рекомендуемого, какие у них сложились отношения и какую должность он (она) занимает (занимали ранее). Эти сведения могут оказаться полезными для оценки достоверности информации, указанной в рекомендательном письме, и выяснения того, занимает ли данное лицо ту должность, которая дает ему законные основания давать рекомендации.

Люди, проводящие проверку рекомендаций по телефону или в личных контактах, должны пройти соответствующее обучение, как проводить интервью с лицом, давшим рекомендацию. Необходима соответствующая подготовка, как правильно формулировать вопросы, как записывать полученную информацию, чтобы повысить ее объективность.
Вся информация, полученная в результате проверки рекомендаций, должна фиксироваться в письменном виде.
Если кандидат предоставил рекомендации, но эта информация не поддается проверке, попросите у кандидата дополнительные рекомендации. Зачисление в штат кандидата, не прошедшего полной проверки рекомендаций, - дело достаточно рискованное.
Проверяйте всю информацию, приведенную в форме "Сведения о кандидате" и в резюме. В частности, следует проверять информацию из школы, какую закончил кандидат (подтверждение наличия грамот, медалей за успехи в учебе), института (наличие красного диплома) и информацию с прежних мест работы (правильность указанных сроков работы, наименование занимаемой должности, исполняемые обязанности). Если обнаруживаются какие-то расхождения - это сигнал к тому, что здесь требуется особое внимание.
Используйте негативную информацию осторожно. Негативная информация, полученная в ходе проверки рекомендаций, часто служит основанием для отказа кандидату. До того, как использовать полученную негативную информацию, следует подтвердить ее точность через другие источники. Кроме того, решения, принимаемые по разным кандидатам, должны быть последовательными (т.е. приниматься на основе сопоставимой информации).

Об авторах
ВЛАСЕНКО Мизаил Николаевич
Помощник директора Института Безопасности Бизнеса ИББ МЭИ
(ТУ, Советник начальника Главного управления МВД РФ по борьбе с
экономическими преступлениями, старший преподаватель
кафедры экономики ВГНА, профессор.
Родился 05 марта 1965 года в селе Лосиновка, на Украине.
С отличием закончил Рязанское высшее военное училище связи (РВВКУС) и Академию им. Дзержинского в г.Москве. 1982-1994г. проходил службу в Вооруженных Силах РФ на командных и технических должностях. Специалист по телекоммуникациям, защите информации, комплексной безопасности бизнеса.
Автор более 30 статей, методических разработок и учебных >пособий в области безопасности бизнеса, управления персоналом, защиты информации. Автор 12 изобретений в области телекоммуникаций и защиты информации.
www.ibbusiness.ru
E-mail: VlasenkoMN@ibbusiness.ru
Тел: (095)362-7255
Факс:(095)362-7255

ЛЕВИНА Оксана Владимировна
Менеджер службы персонала "Видеоленд" концерна "Видеосервис".
Выпускник Института Безопасности Бизнеса
www.videolend.ru
E-mail: olevina@videosrv.com.ru
Тел: (095) 362-73-07
Факс:(095) 362-73-07

А. Ануфриев

А. Ануфриев

Некоторые особенности информационной безопасности банков

Со времени своего появления банки неизменно вызывали интерес преступного мира. И этот интерес был связан не только с хранением в кредитных организациях денежных средств,

но и с тем, что в банках сосредоточена важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств. Так, еще в XVIII веке недоброжелатели известного Джакомо Казановы опубликовали закрытые данные о движении средств по его счету в одном из парижских банков. Из этой информации следовало, что организованная Казановой государственная лотерея приносила доход не только казне, но и (в не меньших масштабах) ему лично.

В наши дни в связи с всеобщей информатизацией и компьютеризацией банковской деятельности значение информационной безопасности банков многократно возросло. Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Однако прогресс в технике преступлений идет не менее быстрыми темпами, чем развитие банковских технологий. В настоящее время свыше 90% всех преступлений связана с использованием автоматизированных систем обработки информации банка (АСОИБ) Если в обеспечении физической и классической информационной безопасности давно уже выработаны устоявшиеся подходы (хотя развитие происходит и здесь), то в связи с частыми радикальными изменениями в компьютерных технологиях методы безопасности АСОИБ требуют постоянного обновления. Как показывает практика, не существует сложных компьютерных систем, не содержащих ошибок. А поскольку идеология построения крупных АСОИБ регулярно меняется, то исправления найденных ошибок и "дыр" в системах безопасности хватает ненадолго, так как новая компьютерная система приносит новые проблемы и новые ошибки, заставляет по-новому перестраивать систему безопасности.

Особенно актуальна данная проблема в России. В западных банках программное обеспечение разрабатываются конкретно под каждый банк и устройство АСОИБ во многом является коммерческой тайной. В России получили распространение "стандартные" банковские пакеты, информация о которых широко известна, что облегчает несанкционированный доступ в банковские компьютерные системы.

Чтобы обезопасить себя и своих клиентов, большинство банков предпринимают необходимые меры защиты, в числе которых защита АСОИБ занимает не последнее место. При этом необходимо учитывать, что защита АСОИБ банка - дорогостоящее и сложное мероприятие. Так, например, Barclays Bank тратит на защиту своей автоматизированной системы около $20 млн. ежегодно.

В первой половине 2002 г. Datapro Information Services Group провела почтовый опрос среди случайно выбранных менеджеров информационных систем. Целью опроса явилось выяснение состояния дел в области защиты. Было получено 1.153 анкеты, на основе которых получены приводимые ниже результаты:
* около 25% всех нарушений составляют стихийные бедствия;
* около половины систем испытывали внезапные перерывы электропитания или связи, причины которых носили искусственный характер;
* около 3% систем испытывали внешние нарушения (проникновение в систему организации);
* 70-75% - внутренние нарушения, из них:
- 10% совершено обиженными и недовольными служащими-
пользователями АСОИБ банка;
- 10% - совершены из корыстных побуждений персоналом системы;
- 50-55% - результат неумышленных ошибок персонала и/или пользователей системы в результате небрежности, халатности или некомпетентности.

Эти данные свидетельствуют о том, что угрозы чаще всего исходят не от хакеров, а изнутри. В то же время именно внешние умышленные атаки на компьютерные системы приносят наибольший единовременный ущерб, а меры защиты от них наиболее сложны и дорогостоящи.

Стратегия информационной безопасности банков весьма сильно отличается от аналогичных стратегий других компаний и организаций. Это обусловлено, прежде всего, специфическим характером угроз. Преступления в банковской сфере имеют свои особенности :

* Многие преступления, совершенные в финансовой сфере остаются

неизвестными для широкой публики в связи с тем, что руководители банков не хотят тревожить своих акционеров, боятся подвергнуть свою организацию новым атакам, опасаются подпортить свою репутацию надежного хранилища средств и, как следствие, потерять клиентов.
* Как правило, злоумышленники используют собственные счета, на который переводятся похищенные суммы. Большинство преступников не знают, как "отмыть" украденные деньги. Умение совершить преступление и умение получить деньги - это не одно и то же.
* Большинство компьютерных преступлений - мелкие. Ущерб от них лежит в интервале от $10.000 до $50.000.
* Успешные компьютерные преступления, как правило, требуют большого количества банковских операций (до нескольких сотен). Однако крупные суммы могут пересылаться и всего за несколько транзакций.
* Большинство злоумышленников - клерки. Хотя высший персонал банка также может совершать преступления и нанести банку гораздо больший ущерб - такого рода случаи единичны.
* Компьютерные преступления не всегда высокотехнологичны. Достаточно подделки данных, изменения параметров среды АСОИБ и т.д., а эти действия доступны и обслуживающему персоналу.

Соответственно, свои особенности имеет и информационная защита финансово-кредитных организаций.

Главное в защите финансовых организаций - оперативное и по возможности полное восстановление информации после аварий и сбоев.
По некоторым опросам, около 60% зарубежных финансовых организаций имеют план такого восстановления, который ежегодно пересматривается в более чем 80% из них. В основном, защита информации от разрушения достигается созданием резервных копий и их внешним хранением, использованием средств бесперебойного электропитания и организацией "горячего" резерва аппаратных средств.

Следующая по важности для финансовых организаций проблема - это управление доступом пользователей к хранимой и обрабатываемой информации. Здесь широко используются различные программные системы управления доступом, которые иногда могут заменять и антивирусные программные средства. В основном используются приобретенные программные средства управления доступом. Причем в финансовых организациях особое внимание уделяют такому управлению пользователей именно в сети. Однако сертифицированные средства управления доступом встречаются крайне редко (3%). Это можно объяснить тем, что с сертифицированными программными средствами трудно работать и они крайне дороги в эксплуатации, поскольку параметры сертификации разрабатываются с учетом требований, предъявляемым к военным системам.

К отличиям организации защиты сетей ЭВМ в финансовых организациях можно отнести широкое использование стандартного (т.е. адаптированного, но не специально разработанного для конкретной организации) коммерческого программного обеспечения для управления доступом к сети, защита точек подключения к системе через коммутируемые линии связи. Скорее всего, это связано с большей распространенностью средств телекоммуникаций в финансовых сферах и желание защититься от вмешательства извне. Другие способы защиты, такие как применение антивирусных средств, оконечное и канальное шифрование передаваемых данных, аутентификация сообщений применяются примерно одинаково и, в основном (за исключением антивирусных средств).

Большое внимание в финансовых организациях уделяется физической защите помещений, в которых расположены компьютеры. Это означает, что защита ЭВМ от доступа посторонних лиц решается не только с помощью программных средств, но и организационно-технических (охрана, кодовые замки и т.д.).

Шифрование локальной информации применяют редко. Причинами этого являются сложность распространения ключей, жесткие требования к быстродействию системы, а также необходимость оперативного восстановления информации при сбоях и отказах оборудования.

Меньше внимания в финансовых организациях уделяется защите телефонных линий связи и использованию ЭВМ, разработанных с учетом требования стандарта Tempest (защита от

утечки информации по каналам электромагнитных излучений и наводок). В государственных организациях, решению проблемы противодействия утечек информации с использованием электромагнитных излучений и наводок, уделяют гораздо больше внимания.

Об авторе: Ануфриев Александр Евгеньевич
В 1997 г. окончил РГАФК (Российская Государственная Академия Физической Культуры),кафедру теории и методики преподавания восточных единоборств.
В 2003-2004 гг. получил дополнительное образование в ИББЛ по специальности экономическая безопасность фирмы.
Обучает простой и очень эффективной японской системе медитации Сей-За(побочными эффектами такой практики являются:здоровье,ясность мышления,уверенность,ощущение внутренней психологической безопасности,увеличение внутренней свободы,радости,силы и т.п.).Увлекается и занимается антиквариатом,спортом, развитием своих возможностей.
" <*sashel69@yandex.ru*>

Г. Куборский

Г. Куборский

А сколько у Вас осталось на пластиковой карте?
(Мошенничество на рынке пластиковых карт)

Как и всякий высокодоходный бизнес, а в особенности в сфере денежного оборота, банковская пластиковая карта давно стала мишенью для преступных посягательств. По данным зарубежных источников, банки несут значительные потери от преступлений в сфере оборота банковских пластиковых карт.

За последние годы преступность в сфере оборота банковских пластиковых карт претерпела качественные изменения - от деяний, совершаемых одиночками и небольшими группами, до преступлений, совершаемых хорошо организованными группировками и преступными сообществами (численностью до 50 человек). На вооружении таких группировок находится самая современная техника, необходимые документы прикрытия. В них входят квалифицированные специалисты. Для осуществления преступной деятельности создаются фиктивные предприятия, банки. Примером может служить разоблачение одной фирмы, которая занималась оказанием посреднических услуг в оформлении карт зарубежных платёжных систем. Мошенники открывали корпоративный счёт, выдавая его клиенту за индивидуальный. В нужный момент, когда ничего не подозревающий владелец, убедившись в том, что карта нормально функционирует в нашей стране и за рубежом, переводил на свой счёт крупную сумму денег, преступники, обладающие равными правами, распоряжались её по своему усмотрению.

Проведенными правоохранительными органами мероприятиями в последнее время удалось пресечь деятельность ряда лже-фирм в Москве, а их участников привлечь к уголовной ответственности. Кроме того, совместными усилиями сотрудников МВД, ФСБ и службы безопасности Сбербанка удалось разоблачить преступную деятельность группы мошенников, пытавшихся похитить 1,5 млрд. рублей через банкоматы отделений Сбербанка в Перми, Москве и Санкт-Петербурге. Главные исполнители преступления установлены и привлечены к уголовной ответственности.

На сегодняшний день из известных видов мошенничеств "лидирует" подделка карты. На заготовки полностью подделанных карточек наносятся логотип эмитента, поле для проставления подписи, точно воспроизводятся все степени защиты. В данном случае используются подлинные реквизиты существующих карт. На международном рынке в изготовлении и использовании поддельных пластиковых карт "лидирует" Юго-Восточная Азия, откуда осуществляется большинство операций. Активно действующие "филиалы" есть в Испании, Италии и Великобритании. Ведущая роль в этой сфере принадлежит гонконгским китайцам. Азиатские группировки преступников уже давно изготавливают высококачественные дубликаты карточек, которые как на азиатском, так и на европейском рынках использовались до сих пор без риска для приобретения высококачественных

товаров. Необходимые для изготовления дубликатов данные (номер карточки, дата прекращения действия, имя и др.) преступники, как правило, получают через служащих предприятий - участников договора.

Во второй половине 90-х годов в сфере полных подделок банковских пластиковых карт в Европе африканские группировки стали теснить азиатские. В отличие от азиатов, африканцы используют подделки преимущественно в банках для получения напрямую наличных денег. Преступники даже не затрудняют себя "приобретением товаров", чтобы затем, пройдя этап укрывательства, получить деньги. При этом преступники удостоверяют свою личность с помощью украденных (подделанных) идентификационных документов. Используемые африканцами полные подделки изготавливаются в США (Западное побережье). В Калифорнии (район Лос-Анджелеса) неоднократно ликвидировались мастерские по производству фальшивок. По качеству азиатские подделки значительно выше африканских.

По частоте совершения затем следуют преступления, которые можно объединить в группу "незаконное использование подлинной карточки". Сюда можно отнести "превышение счета" (floor limit); операции с краденной, потерянной карточкой; так называемая "двойная прокатка" (изготовление продавцом нескольких копий слипа, которые используются в дальнейшем для оплаты товара). Пути незаконного приобретения карточек различны: умышленная передача третьим лицам, преступное завладение картой (утрата при пересылке по почте, кража и т.п.). Известны случаи, когда недобросовестные работники банков и фабрик по изготовлению карточек пользуются задержкой между открытием счета и доставкой карточки владельцу и совершают операции в этот период. Имеют место факты, когда владельцы карточки заявляют её как украденную или потерянную. Как правило, пока процессинговый центр включит номер в стоп-лист и известит торговые точки проходит несколько дней. За это время владелец старается провести операции, а затем заявляет претензии банку.

К незаконному использованию подлинной карты следует отнести и частичную подделку (фальсификацию). Этими деяниями фактически началась история злоупотреблений с пластиковыми карточками. Преступник (чаще всего владелец) изменяет лишь некоторые реквизиты - номер, либо фамилию. Соответственно, товар приобретается, но не оплачивается. В данном случае информация о счете, эмбоссированная на карточке, удаляется (термическим, механическим или иным способом), а на ее место наклеивается новый номер, срезанный с другой карточки. Этот простейший метод получил настолько широкое распространение в мире, что для него даже родилось специальное название: shave & paste ("сбрить и наклеить").

Банковские пластиковые карты, доставляемые по почте, как правило, похищаются при пересылке клиенту от эмитента или изготовителя. Такие карты имеют ряд предпочтений для преступного использования:
-- утрата (кража) подобных карт замечается с большим опозданием;
-- карты в момент утраты, как правило, не подписаны, поэтому преступник сам может поставить подпись на карточку.
За рубежом известны случаи, когда преступники специально устраиваются работать на почту или в частные службы доставки, чтобы во время работы непосредственно изымать отправления с банковскими картами или направлять их на подготовленный ими самими почтовый адрес.

В конце 70-х годов появилась распространенная сегодня схема мошенничества, получившая название "белый пластик". Такие карты не имеют "опознавательных знаков" банка и платежной системы (отсюда и название). На чистый лист пластмассы (без логотипа эмитента, голограммы и других степеней защиты) переносятся данные существующих карт (тиснение и кодирование). Такие карточки могут быть предъявлены только при условии соучастия в преступлении владельца или служащих предприятия-участника договора, поскольку фальшивка визуально определяется сразу. Далее производится "замывание" (маскировка) слипов (чеков) среди подлинных. По дебетовому счету, образованному в результате использования "белого пластика", позднее уже практически невозможно установить, была ли предъявлена настоящая или поддельная карта. Кроме того, в практике мошенничества по схеме "белый пластик" нередко создаются целые фиктивные предприятия. Недавно появилась еще одна разновидность "белого пластика". Преступники подделывали электронный или магнитный носитель информации на картах и снимали

деньги посредством банкоматов.

Преступникам не чужд технический прогресс. С развитием глобальной компьютерной сети Интернет и появлением так называемых "виртуальных магазинов", где можно сделать заказ с персонального компьютера на получение товара по почте, расширилось поле деятельности для мошенников. Для оплаты в таких магазинах достаточно указать реквизиты карты. Следовательно, любая утечка такой информации (а это может произойти при любой операции) чревата для владельца большими потерями. А способов "выманить" у владельца реквизиты карты существует множество. Сейчас уже известно около 30 приёмов мошеннических действий с помощью Интернета.

Вал преступлений в сфере оборота пластиковых карт грозит подорвать авторитет пластиковой карты как финансового инструмента. Недавний скандал с компрометацией банковских карт российских эмитентов побудил многих пользователей переходить на дорожные чеки.

Как показывает практика, борьба с преступлениями в данной сфере кредитно-денежных отношений усилиями одних лишь правоохранительных органов весьма затруднительна. К сожалению, в нашей стране законодательство, как правило, отстает от реальной жизни. Положение Центрального банка Российской Федерации о порядке эмиссии и проведении операций вышло лишь в апреле 1998 года, тогда как рынок пластиковых карт реально существовал в нашей стране уже более десятка лет.

Налицо и объективные трудности правоохранительных органов: дефицит средств не позволяет на должном уровне поддерживать техническое оснащение, квалифицированно обучать сотрудников, организовывать в достаточном количестве служебные командировки для участия сотрудников в семинарах, проводимых ведущими платежными системами и банками. Как негативный фактор следует отметить и то, что отсутствие эффективного правового регулирования не позволяет соответствующим образом организовать взаимодействие со службами безопасности заинтересованных организаций, сводя все к личным контактам.

Все это создает серьезные проблемы борьбы с преступностью в сфере оборота банковских пластиковых карт. В связи с этим, по нашему мнению, эффективная борьба с преступлениями на пластиковом рынке возможна при тесном взаимодействии профессионалов служб безопасности, специалистов банков и процессинговых компаний с правоохранительными органами.

Виды мошенничества в РФ

Основные виды:

Воровство данных с магнитной полосы (Skimming). Высокотехнологичный вид мошенничества. Сканирование в гостиницах, торговых точках и т.д. данных с магнитной ленты. Выпуск карты двойника со сканированной магнитной ленты, содержащей легальными CVV и CVC и данными клиента.
В последнее время стали появляться российские подделки - двойники очень высокого качества, выполненные на банковском оборудовании, как правило, со всеми видами защиты. Большое количество подделок выплеснулось на российский чёрный рынок. Цена через интернет одной карты составляет от 150 до 450 долл., комплект из 10 карт на чёрном рынке от 2000 до 4000 долл.

Массовая закупка ниже лимита авторизации. Как правило, деятельность международных ОПГ. Цепочка выстраивается по схеме:
- захват карт российских банков эмитентов обычно происходит через подставных лиц (схем захвата множество);
- переправка в страны Европы с высокими лимитами авторизации (лимиты авторизации могут доходить до 1500-2000 долл.);
- закупка товаров;
- сбыт товаров.
Использование карты, как правило, не более трёх дней. Ущерб банка эмитента может составить до 100 тыс.долл. с одной карты.

Мошенничество в торговых точках. Сотрудники делают более одного отпечатка карты и дополнительные отпечатки далее используют для генерации новых платежных документов.

Мошенничество сотрудников банка.
- пополнение счёта
- лимит кредита (увеличение)
- сговор (выдача наличных)
- задержка транзакции

Почему рынок РФ стал привлекателен для этих видов мошенничества?

Слабое законодательство. ОПГ проводит постоянный мониторинг рынка банковских услуг и выявления более слабых и уязвимых мест. Мошенники опираются на такие факторы как человеческий фактор (невнимательность, безразличие, непрофессионализм, корысть) и технологические уязвимость системы защиты.

Куборский Григорий Владимирович
grigorys@ztel.ru
тел. 8 910 425 96 48

Что считать конфиденциальной информацией

Что считать конфиденциальной информацией?

17 июня в здании Правительства Москвы прошла летняя сессия Шестой Всероссийской конференции "Информационная безопасность России в условиях глобального информационного общества" - ИНФОФОРУМ-6.
Организаторами конференции по традиции выступили: Комитет Государственной Думы по безопасности, Аппарат Совета Безопасности Российской Федерации, Управление Правительства Москвы по экономической безопасности города Москвы и журнал "Бизнес и безопасность в России".

В этот раз конференция была посвящена проблемам обеспечения информационной безопасности на уровне региона, города.
Четыре года назад в России была принята Доктрина информационной безопасности. Восприятие ее неоднозначно. Продолжаются дискуссии, нужна ли вообще такая доктрина. Тем не менее, идея о необходимости обеспечения информационной безопасности не только выжила, но и перешла с федерального на региональный уровень.

Участникам конференции были представлены основные положения проекта Концепции информационной безопасности Москвы, главной целью которой декларируется защита информационных ресурсов населения, организаций, предприятий и органов власти региона от несанкционированного доступа, защита информационных и телекоммуникационных систем от преступлений и актов терроризма с использованием информационных технологий.
Проект концепции предусматривает создание "комплексной системы информационной безопасности" с развитой инфраструктурой, соответствующей материально-технической базой, квалифицированным штатом. Эта система должна обеспечивать управление и мониторинг обеспечения информационной безопасности в проектах городской целевой программы "Электронная Москва".

Одно из трех секционных заседаний было посвящено вопросам совершенствования законодательства о конфиденциальной информации.
На секции прозвучало 8 докладов, обсуждались вопросы систематизации правовых режимов конфиденциальной информации в целях совершенствования российского законодательства, включая защиту персональных данных, банковской и коммерческой

тайны, профессиональных тайн, определение сферы государственного регулирования обращения конфиденциальной информации, установление ответственности за нарушение режимов конфиденциальности.

Ведущая секции - советник аппарата Комитета Государственной Думы по безопасности **Елена Волчинская** рассказала вашему корреспонденту:

"В отличие от предыдущих обсуждений в рамках данного форума, когда рассматривались конкретные законопроекты, приоритеты законодательного регулирования, в этот раз обсуждались проблемы теоретические. Без них невозможно двигаться ни в совершенствовании законодательства, ни в правоприменении.

Секция задумывалась и готовилась как расширенное заседание секции Экспертного совета Комитета Госдумы по безопасности. Большинство членов секции этого совета были в числе участников заседания. А общее количество присутствовавших в зале превысило 50 человек.

Основной вопрос, по которому необходимо достигнуть согласия - что защищать? То есть, что такое конфиденциальная информация? На этот вопрос нет однозначного ответа - ни в законодательстве, ни в науке, ни в реальной жизни. К сожалению, обсуждение на секции недостаточно приблизило нас к общему пониманию - слишком велик разброс мнений и подходов. Тем не менее, начало разговору положено, - подчеркивает Елена Волчинская..

В части становления институтов конфиденциальной информации пока не так много сделано.
Законопроект "О коммерческой тайне", принятый Госдумой, был отклонен Советом Федерации. Работала согласительная комиссия, в редакции которой закон принят 9 июля.

Другой законопроект - "Об информации персонального характера" - по-прежнему лежит без движения в комитете Госдумы по информационной политике.
Комитетом ГОСДУМЫ по безопасности готовится к внесению законопроект "О служебной тайне".

Вместе с тем, общие положения о структуре конфиденциальной информации, правах и обязанностях лиц, имеющих к ней доступ, ответственности за ее разглашение и неправомерное использование однозначно законодательством не установлены. Первая попытка определения понятия "конфиденциальная информация" была сделана в федеральном законе "Об информатизации и защите информации", где в статье 2 к такой информации отнесена "документированная информация", доступ к которой ограничивается в соответствии с законодательством Российской Федерации". А в соответствии со ст.10 "документированная информация с ограниченным доступом ….подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную".

В отсутствие специальных законов единственным документом, определяющим структуру конфиденциальной информации, является Указ Президента РФ №188 от 6 марта 1997 года. Указом к сведениям конфиденциального характера отнесены:
- сведения о частной жизни гражданина (персональные данные), позволяющие идентифицировать его личность;
- сведения, составляющие тайну следствия и судопроизводства;
- служебная тайна;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебная, нотариальная адвокатская тайна, тайна переписки, телефонных разговоров и т.д.);
- коммерческая тайна;
- информация об изобретениях и новых технологиях (до официальной публикации информации о них).

"В Указе, - отмечает Е. Волчинская, - не выделена в качестве самостоятельного объекта защиты банковская тайна. Между тем, на секции этот вопрос вызвал дискуссию. Работники банков настаивают, что банковская тайна не идентична коммерческой тайне, потому заслуживает отдельного рассмотрения и определения в законодательстве. Приводимые ими аргументы не убеждают многих юристов, которые рассматривают банковскую тайну как вид профессиональных тайн".

В то же время в ряде ключевых правовых документов банковская тайна фигурирует самостоятельно. Например, в Уголовном Кодексе РФ, статья 183, где говорится о незаконном получении и разглашении "коммерческой, налоговой или банковской тайны". Здесь, как видим, банковская тайна четко отделена от коммерческой (как и налоговая тайна). Данная статья запрещает "собирание сведений, составляющих коммерческую, налоговую или банковскую тайну путем похищения документов, подкупа или угроз", а также "незаконное разглашение или использование таких сведений без согласия их владельца".

Похоже, для решения теоретических проблем и для упорядочения законодательства об охране конфиденциальной информации потребуются еще долгие годы.

В. Борисов

Где узнать о поисковых машинах

Где узнать о поисковых машинах англоязычного Интернета

Автор ряда публикаций о ресурсах Интернета Белинда Вивер (belinda@journoz.com) рассказывает о наиболее, по ее мнению, интересных веб-сайтах, содержащих информацию о поисковых машинах (scip.online, issue 33).

Некоторые из них созданы известным экспертом по Интернету Гарри Прайсом. Ему принадлежат веб-сайты:

* DirectSearch (www.freepint.com/gary/direct.htm), врата в "невидимый" Интернет.
* List of Lists (www.specialissues.com/lol), предлагающий блестящий список поисковых машин с их классификацией.
* the Resource Shelf (http://www.resourceshelf.com/), веб-сайт для профессионалов, информирующий о новых системах поиска в Интернете. Можно подписаться на еженедельный бюллетень новостей, но легче самому следить за новой информацией на сайте, обращая внимание на интересующие вас линки.

Также полезными могут быть ежемесячный бюллетень по интернет-ресурсам (www.hw.ac.uk/libWWW/irn/), выходящий дважды в неделю FreePint (www.freepint.com), или еженедельник Scout Report (http://scout.cs.wisc.edu/

Ключевым сайтом автор считает Search Engine Watch (www.searchenginewatch.com/). Сайт предлагает сравнительный анализ различных поисковых систем. Здесь также можно подписаться на ежедневный вестник SearchDay (www.searchenginewatch.com/searchday).

Хорошим источником новостей и информации являются Search Engine Showdown (www.notess.com) и ResearchBuzz (www.researchbuzz.com) .

Те, кто интересуются технологическими аспектами, могут найти много интересного на сайтах CNet (www.cnet.com)

Даже печать уделяет все больше внимания этим вопросам. К примеру, газета Boston Globe опубликовала интервью с генеральным директором Google Эриком Шмидтом. Как следует из его высказываний, компания Google стремится индексировать не только Интернет ресурсы, но и включить в спектр поиска крупнейшие платные коллекции и базы данных, такие как LexisNexis.

Отдельные профессионалы хотели бы иметь поисковые механизмы, встроенные в персональные компьютеры. Им было бы нелишне заглянуть на сайты AgentLand (www.agentland.com) и BotSpot (www.botspot.com).
Здесь можно выгрузить программное обеспечение, которое доводится под требования пользователя. Но, конечно, большинству не под силу это сделать самостоятельно.

Б. Вивер также рекомендует почаще просматривать специализированные директории,

которые не требуют поиска по всему Интернету, часто вслепую по ключевым словам, а предлагают систематизированный материал по конкретной теме. В частности весьма полезным может оказаться Pinakes (www.hw.ac.uk/libWWW/irn/pinakes/pinakes.html). Он содержит 40 тематических разделов по различным областям знаний - социология, биотехнология и т.д.

Автор подчеркивает, что особенно важно следить за новыми системами , которые позволяют приоткрыть окно в т.н. "невидимый" Интернет. Именно там, а не в индексируемых ресурсах, находится наиболее ценная, интересная информация. Ведь базы данных поисковых машин охватывают не более 20% всех ресурсов Интернета.

10 правил написания веб-контента

Десять правил написания контента для коммерческого веб-сайта

Автор книги "Content Critical" Джерри МакГоверн предлагает 10 правил, которыми, по его мнению, следует руководствоваться при написании текстов для сайтов (scip.online, issue 32, 2003)

1. Проанализируйте, кто ваш читатель

Кто он, ваш читатель? Представитель среднего класса? Живет в городе или сельской местности? Семейный и имеет детей? Ну, и так далее...
Должно быть не более чем 2-3 типа наиболее характерных посетителей вашего сайта.

2. Активный подход

Каких-нибудь десять лет назад на домашней странице сайтов авиакомпаний красовалось изображение лайнера. Сейчас их домашняя страничка полна линков и предлагаемых услуг - бронирование и т.д..
Текст на сайте должен побуждать к действию. Ведь Интернет-посетитель пришел к вам на сайт не ради праздного любопытства. Он готов к действию, и содержание сайта должно побуждать к действию.

3. Писать коротко и понятно

Заголовки должны содержать 8 и менее слов, предложения - 15-20 слов, параграфы - 40-70 слов, каждый материал - 500 слов и меньше.
Избегайте изощренных, слов и выражений, "красивостей". Содержание должно бить в точку. Коротко и понятно.

4. Активный стиль

Самое могущественное слово - вы. Вы обращаетесь к читателю и стиль должен быть соответствующим. Надо подбирать слова, которые побуждают читателя к действию - покупке, подписке, заявке, короче - к решению проблемы, которая привела его на сайт.

5. Логичность и последовательность.

Структура сайта должна содержать линки и переходы на классифицированные страницы. Ни в коем случае не оставляйте читателя в тупике, из которого нет выхода.

6. Найти ключевые слова

Надо подбирать такие слова, по которым вас сайт найдут. Об этом подумать заранее, до того, как вы приступили к написанию текстов.

7. Заголовок - ключ к успеху

- Заголовок не должен содержать более 8 слов.
- Позаботьтесь, чтобы заголовок содержал ключевые слова.
- Старайтесь не использовать предлоги и союзы.
- Заголовки должны быть точными и ясными.
- Не умничайте.

8. Тексты должны привлекать

Прежде всего, они должны быть короткими. Они должны побуждать посетителя продолжать знакомство с содержанием сайта. Специфика чтения в режиме online такова, что если первое предложение будет не интересное, то посетитель не будет читать дальше.

9. Классификация должна быть выдержана.

Это означает, что следует четко подразделять страницы сайта. Каждая из них не должна повторять другую, иметь название, точно соответствующее ее уникальному содержанию.

10. Редактировать, редактировать, и еще раз редактировать!

Для редактирования надо выделять время. Обычно, оно занимает 30-40 % времени, которое требуется для написания оригинального текста.
Старайтесь прочитать готовый текст трижды. В первый раз обращайте внимание на тон и стиль. Грамматику и орфографию оставьте напоследок.
Хорошо бы отпечатать текст - так удобнее его редактировать

Об авторе
Джерри Макговерн (Gerry McGovern) девять лет занимается вопросами веб-контента. С 1996 года выпускает посвященный этим вопросам бюллетень New Thinking. Автор книги Content Critical.
Gerry@gerrymcgovern.com

Рецензия

"Расследование компьютерных преступлений в странах СНГ",
Вехов В.Б. и Голубев В.А., 2004

Монография известных ученых, занимающихся вопросами противодействия компьютерной преступности, Вехова В.Б. и Голубева В.А., посвящена наиболее актуальным теоретическим и практическим проблемам расследования компьютерных преступлений в России, Украине и других странах СНГ.

В книге проводится сравнительный анализ действующих национальных законодательств в сфере информации, информатизации и защиты информации указанных стран - участниц Содружества Независимых Государств, в том числе уголовно-правовых норм, устанавливающих ответственность за компьютерные преступления.

На основе обобщения имеющихся методических рекомендаций, разработанных российскими и украинскими учеными-криминалистами, а также передового опыта расследования компьютерных преступлений правоохранительными органами двух государств СНГ предложена родовая методика их расследования.

С учетом последних достижений криминалистики в работе комплексно рассматриваются:

понятие и криминалистическая характеристика данных преступных посягательств; признаки различных способов их совершения; типичные следы и методы их выявления; типичные следственные ситуации и действия сотрудников органов предварительного расследования на первоначальном этапе. Даны практические рекомендации по организации расследования преступлений выделенной категории, тактике и технологии производства отдельных следственных действий, проверочных мероприятий, розыскной деятельности следователя и его взаимодействия с органами дознания и специалистами.

Монография адресована юристам, студентам, аспирантам и преподавателям юридических образовательных учреждений и факультетов, а также практическим работникам органов предварительного расследования

Людмила Горошко, CrimeResearch.ru

Рецензия

"Расследование компьютерных преступлений в странах СНГ",
Вехов В.Б. и Голубев В.А., 2004

Монография известных ученых, занимающихся вопросами противодействия компьютерной преступности, Вехова В.Б. и Голубева В.А., посвящена наиболее актуальным теоретическим и практическим проблемам расследования компьютерных преступлений в России, Украине и других странах СНГ.

В книге проводится сравнительный анализ действующих национальных законодательств в сфере информации, информатизации и защиты информации указанных стран - участниц Содружества Независимых Государств, в том числе уголовно-правовых норм, устанавливающих ответственность за компьютерные преступления.

На основе обобщения имеющихся методических рекомендаций, разработанных российскими и украинскими учеными-криминалистами, а также передового опыта расследования компьютерных преступлений правоохранительными органами двух государств СНГ предложена родовая методика их расследования.

С учетом последних достижений криминалистики в работе комплексно рассматриваются: понятие и криминалистическая характеристика данных преступных посягательств; признаки различных способов их совершения; типичные следы и методы их выявления; типичные следственные ситуации и действия сотрудников органов предварительного расследования на первоначальном этапе. Даны практические рекомендации по организации расследования преступлений выделенной категории, тактике и технологии производства отдельных следственных действий, проверочных мероприятий, розыскной деятельности следователя и его взаимодействия с органами дознания и специалистами.

Монография адресована юристам, студентам, аспирантам и преподавателям юридических образовательных учреждений и факультетов, а также практическим работникам органов предварительного расследования

Людмила Горошко, CrimeResearch.ru