"Бизнес-разведка" № 25

Оглавление

"BusinessWeek Россия" о финансовой конкурентной разведке в России

«BusinessWeek Россия» о финансовой разведке как методе конкурентной борьбы в России

В последнее время в российской печати все чаще стали появляться публикации о бизнес-разведке, что, конечно, является благоприятным знаком постепенного распространения идей и методологии деловой разведки не только в сфере деятельности узких специалистов, но и среди достаточно широкого круга читателей, интересующихся в целом вопросами экономики и бизнеса.
К числу таких недавних публикаций можно отнести статью в популярном журнале «BusinessWeek Россия» от 17 марта 2007 года «Финансовая разведка становится методом конкурентной борьбы на российских рынках». Автор – Ян Арт. Предлагаем вниманию читателей изложение наиболее интересных, по нашему мнению, фрагментов этой статьи.

Финансовая разведка становится методом конкурентной борьбы на российских рынках

У Вас продается славянский шкаф?

Еще недавно экзотические для нас понятия «финансовая разведка» и «финансовая контрразведка» становятся привычной частью конкурентной борьбы. Финразведка в России, подобно многим видам бизнеса, прошла путь от «подполья» до вполне легитимного вида деятельности и в качестве части конкурентной разведки признана естественным бизнес-инструментом.
Цели финразведки понятны: обеспечить получение актуальной информации о финансовых возможностях и планах конкурентов или контрагентов. А уже в зависимости от того, о каком рынке идет речь, объектом разведки может стать все что угодно, от цены закупки ручек для шкафов в соседнем мебельном салоне до перспектив перестановок в коридорах власти.
Впрочем, мэтры этого жанра как раз считают правильным выяснять цену ручек. Экономисты Кристофер Ботан и Майкл Инглиш, специализирующиеся на методах конкурентной борьбы, констатируют: «Ставить перед финансовой разведкой слишком большие и общие цели все равно что пытаться вскипятить океан».
Развитие финразведки в России шло стихийно. В конечном счете, в большинстве крупных корпораций ее структуры сложились на стыке служб безопасности и аналитических отделов: первые добывают закрытую часть необходимой информации, вторые изучают открытые источники и интерпретируют сведения, выдавая на гора сценарии вероятных действий конкурентов или анализ перспектив деловых партнеров. Сегодня подобные «справки» уже не экзотика, а норма. «Я не принимаю решения о партнерских программах с каким-либо банком, предварительно не получив справки о том, с какими деньгами работает этот банк и кто его
неофициально патронирует», — сообщил «BusinessWeek Россия» шеф одной из крупнейших страховых компаний страны.

Мы за ценой не постоим

Спрос рождает адекватное предложение: сегодня на рынке есть целая группа фирм, предлагающих полный или частичный набор классических услуг финразведки.
Подобные услуги на рынке оказывают «Арсин» (специализируется на мониторинге масс-медиа, подготовке бизнес-обзоров, проверке деловых контактов), «Бизнес-эксперт К», «Шериф» и «Амулет-Инфо» (предлагают услуги по изучению деятельности конкурентов и

их финансового положения), «Интегрум» (оператор медиа-мониторингов и иных банков данных), а также некоторые другие.

Наиболее известные участники рынка финансовой разведки
- «Амулет-Инфо» Информирование заказчика о потенциальных бизнес-партнерах и их финансовом положении
- «Интегрум» Мониторинг масс-медиа, документарной базы и различных баз данных
- СИнС (Специальная информационная служба) Аналитические обзоры по отраслям, аналитические справки о бизнес-партнерах и конкурентах
- «Арсин» Мониторинг масс-медиа, проверка бизнес-партнеров и персонала заказчика, создание служб конкурентной разведки на предприятии заказчика
- Poisinfo Предоставление информации о финансовом состоянии бизнес-партнеров и конкурентов
- «Шериф» Аналитические обзоры по отраслям, предоставление информации о бизнес-партнерах и конкурентах
- «Информбюро» Предоставление информации о собственниках, топ-менеджерах и аффилированных структурах компаний, предоставление информации о схемах офшорных операций
- «Бизнес-эксперт К» Аналитические обзоры по отраслям, предоставление информации о финансовом состоянии и рыночной политике конкурентов

Одним из наиболее частых источников информации для финразведки остаются так называемые черные базы данных. На рынке можно приобрести базы кредитных историй, абонентов сотовых компаний, участников внешнеэкономической деятельности, сделок с недвижимостью, автомобилей, зарегистрированных в ГИБДД. Цена колеблется в пределах $20–100. Другое дело, что эта информация часто липовая или содержит устаревшие сведения, поэтому профи выходят на их источники, минуя «жучков» с Митинского рынка и Горбушки, или же выборочно проверяют содержащиеся в них сведения.

Источником информации для финразведчиков может быть также отслеживание контактов ключевых фигур изучаемой компании. Здесь возможности отработаны, начиная от классического «наблюдения за объектом» и заканчивая мониторингом телефонных переговоров. Например, распечатку бесед «подопечного» по мобильнику можно приобрести за $1000. Часть информации добывают «свои» люди в налоговых инспекциях, органах регистрации сделок по недвижимости, Госкомстате. Стоимость копий документов «на заказ» — $50–500.

«В госорганах на уровне низовых звеньев купить можно практически любую информацию», — говорит Алексей Кулагин (фамилия изменена), сотрудник разведфирмы. — В сочетании с нашими оперативными мероприятиями она складывается в необходимую заказчику «картинку».

Что касается цен на услуги самих финразведчиков, то говорить о каких-то прайсах или стандартах стоимости не приходится: все зависит от объемов и сложности конкретной задачи. Например, мониторинг масс-медиа может стоить от $90 до $1300 в месяц, а цена

аналитической справки — отличаться на порядок, варьируясь в пределах $500–5000. И это понятно: в одном случае речь идет, скажем, о супермаркете, в другом — о «нефтянке».

Пресса решает все

Основной источник информации финразведчиков весьма далек от государственных и коммерческих тайн, слежки, подслушки и пр. Речь идет о прессе. Специалисты констатируют, что тут принципы финансовой разведки полностью соответствуют положению дел в разведке настоящей: 70–90% необходимой информации можно добыть из вполне открытых и даже публичных источников: масс-медиа, Интернета, открытых отчетов, буклетов и брошюр, а также на выставках, конференциях и корпоративных сайтах.
На подобной «открытой» аналитике специализируются несколько ведущих российских фирм по конкурентной разведке. Лакуной на этом поприще пока остается развитие банков деловой информации. Например, в США такие компании, как Dun & Bradstreet (D&B) или Experian Information Solution (EIS), оперируют постоянно обновляемыми данными на несколько миллионов фирм. В России подобные структуры пока в зародыше. Есть сведения, что банк бизнес-данных предполагается создать на базе одного из российских бюро кредитных историй.
Отечественные технологии, позволяющие такие базы данных эффективно формировать, уже появляются. Сейчас на рынке продается по меньшей мере десяток операционных систем, предназначенных автоматизировать процессы сбора и обработки информации о субъектах бизнеса: Info Tailor, Tracer, «Медиалогия», CronosPlus, Cros, Intellectum.BIS, «Монитор», информационно-поисковая система «Артефакт», система медиа-мониторинга «Медиалогия» и др. Стоимость подобных систем составляет $2–40 тыс. в зависимости от степени сложности.

Союз «шпионов»

Четыре года назад финразведчики России сформировали профессиональный союз — Российское общество профессионалов конкурентной разведки (РОПКР). Помимо чисто «профсоюзных» функций РОПКР намерено заниматься разработкой методологии отечественной конкурентной и финансовой разведки вплоть до преподавания этих дисциплин в экономических вузах.
Так что, вполне вероятно, недалек день, когда в перечне вузовских специальностей появится позиция «разведчик».
Еще одна задача, взятая на себя профсоюзом шпионов, этическая. По мнению Алексея Горделяна, исполнительного директора РОПКР, институту финразведки необходимы саморегулируемые принципы ведения дел. РОПКР выступает за создание кодекса финразведки, который был бы основан на трех базовых постулатах: отказе от получения информации путем обмана или шантажа, отказе от противоправных действий, отказе от причинения физического вреда людям или материальным объектам с целью приобретения конкурентных преимуществ.
Что же касается юридической основы деятельности финразведчиков, то ее определяют законы «О коммерческой тайне», «Об информации, информатизации и защите информации», «Об оперативно-розыскной деятельности», «О кредитных историях» и официальный перечень сведений, составляющих государственную тайну. О разработке специального закона, регламентирующего негосударственную разведку, речь пока не заходила.

"BusinessWeek Россия" о финансовой конкурентной разведке в России

«BusinessWeek Россия» о финансовой разведке как методе конкурентной борьбы в России

В последнее время в российской печати все чаще стали появляться публикации о бизнес-разведке, что, конечно, является благоприятным знаком постепенного распространения идей и методологии деловой разведки не только в сфере деятельности узких специалистов, но и среди достаточно широкого круга читателей, интересующихся в целом

вопросами экономики и бизнеса.
К числу таких недавних публикаций можно отнести статью в популярном журнале «BusinessWeek Россия» от 17 марта 2007 года «Финансовая разведка становится методом конкурентной борьбы на российских рынках». Автор – Ян Арт. Предлагаем вниманию читателей изложение наиболее интересных, по нашему мнению, фрагментов этой статьи.

Финансовая разведка становится методом конкурентной борьбы на российских рынках

У Вас продается славянский шкаф?

Еще недавно экзотические для нас понятия «финансовая разведка» и «финансовая контрразведка» становятся привычной частью конкурентной борьбы. Финразведка в России, подобно многим видам бизнеса, прошла путь от «подполья» до вполне легитимного вида деятельности и в качестве части конкурентной разведки признана естественным бизнес-инструментом.
Цели финразведки понятны: обеспечить получение актуальной информации о финансовых возможностях и планах конкурентов или контрагентов. А уже в зависимости от того, о каком рынке идет речь, объектом разведки может стать все что угодно, от цены закупки ручек для шкафов в соседнем мебельном салоне до перспектив перестановок в коридорах власти.
Впрочем, мэтры этого жанра как раз считают правильным выяснять цену ручек. Экономисты Кристофер Ботан и Майкл Инглиш, специализирующиеся на методах конкурентной борьбы, констатируют: «Ставить перед финансовой разведкой слишком большие и общие цели все равно что пытаться вскипятить океан».
Развитие финразведки в России шло стихийно. В конечном счете, в большинстве крупных корпораций ее структуры сложились на стыке служб безопасности и аналитических отделов: первые добывают закрытую часть необходимой информации, вторые изучают открытые источники и интерпретируют сведения, выдавая на гора сценарии вероятных действий конкурентов или анализ перспектив деловых партнеров. Сегодня подобные «справки» уже не экзотика, а норма. «Я не принимаю решения о партнерских программах с каким-либо банком, предварительно не получив справки о том, с какими деньгами работает этот банк и кто его
неофициально патронирует», — сообщил «BusinessWeek Россия» шеф одной из крупнейших страховых компаний страны.

Мы за ценой не постоим

Спрос рождает адекватное предложение: сегодня на рынке есть целая группа фирм, предлагающих полный или частичный набор классических услуг финразведки.
Подобные услуги на рынке оказывают «Арсин» (специализируется на мониторинге масс-медиа, подготовке бизнес-обзоров, проверке деловых контактов), «Бизнес-эксперт К», «Шериф» и «Амулет-Инфо» (предлагают услуги по изучению деятельности конкурентов и их финансового положения), «Интегрум» (оператор медиа-мониторингов и иных банков данных), а также некоторые другие.

+----------+
| |
| *Наиболее известные участники рынка финансовой разведки* |
|
- «Амулет-Инфо»
| Информирование заказчика о потенциальных бизнес-партнерах и |
| их финансовом положении
|
| - «Интегрум» |
| Мониторинг масс-медиа, документарной базы и различных баз |
| данных |

| - СИнС (Специальная информационная служба) |
| Аналитические обзоры по отраслям, аналитические справки о |
| бизнес-партнерах и конкурентах
|
| - «Арсин» |

| Мониторинг масс-медиа, проверка бизнес-партнеров и персонала |
| заказчика, создание служб конкурентной разведки на предприятии |
| заказчика |

| - Poisinfo |
| Предоставление информации о финансовом состоянии |
| бизнес-партнеров и конкурентов |

| - «Шериф» |
| Аналитические обзоры по отраслям, предоставление информации |
| о бизнес-партнерах и конкурентах |

| - «Информбюро» |
| Предоставление информации о собственниках, топ-менеджерах и |
| аффилированных структурах компаний, предоставление информации о схемах офшорных операций |

| - «Бизнес-эксперт К» |
| Аналитические обзоры по отраслям, предоставление информации |
| о финансовом состоянии и рыночной политике конкурентов |
+----------+

Одним из наиболее частых источников информации для финразведки остаются так называемые черные базы данных. На рынке можно приобрести базы кредитных историй, абонентов сотовых компаний, участников внешнеэкономической деятельности, сделок с недвижимостью, автомобилей, зарегистрированных в ГИБДД. Цена колеблется в пределах $20–100. Другое дело, что эта информация часто липовая или содержит устаревшие сведения, поэтому профи выходят на их источники, минуя «жучков» с Митинского рынка и Горбушки, или же выборочно проверяют содержащиеся в них сведения.
Источником информации для финразведчиков может быть также отслеживание контактов ключевых фигур изучаемой компании. Здесь возможности отработаны, начиная от классического «наблюдения за объектом» и заканчивая мониторингом телефонных переговоров. Например, распечатку бесед «подопечного» по мобильнику можно приобрести за $1000. Часть информации добывают «свои» люди в налоговых инспекциях, органах регистрации сделок по недвижимости, Госкомстате. Стоимость копий документов «на заказ» — $50–500.
«В госорганах на уровне низовых звеньев купить можно практически любую информацию», — говорит Алексей Кулагин (фамилия изменена), сотрудник разведфирмы. — В сочетании с нашими оперативными мероприятиями она складывается в необходимую заказчику «картинку».
Что касается цен на услуги самих финразведчиков, то говорить о каких-то прайсах или стандартах стоимости не приходится: все зависит от объемов и сложности конкретной задачи. Например, мониторинг масс-медиа может стоить от $90 до $1300 в месяц, а цена аналитической справки — отличаться на порядок, варьируясь в пределах $500–5000. И это понятно: в одном случае речь идет, скажем, о супермаркете, в другом — о «нефтянке».

Пресса решает все

Основной источник информации финразведчиков весьма далек от государственных и коммерческих тайн, слежки, подслушки и пр. Речь идет о прессе. Специалисты констатируют, что тут принципы финансовой разведки полностью соответствуют положению дел в разведке настоящей: 70–90% необходимой информации можно добыть из вполне открытых и даже публичных источников: масс-медиа, Интернета, открытых отчетов, буклетов и брошюр, а также на выставках, конференциях и корпоративных сайтах.
На подобной «открытой» аналитике специализируются несколько ведущих российских фирм по конкурентной разведке. Лакуной на этом поприще пока остается развитие банков деловой информации. Например, в США такие компании, как Dun & Bradstreet (D&B) или Experian Information Solution (EIS), оперируют постоянно обновляемыми данными на несколько миллионов фирм. В России подобные структуры пока в зародыше. Есть сведения, что банк бизнес-данных предполагается создать на базе одного из российских бюро кредитных историй.
Отечественные технологии, позволяющие такие базы данных эффективно формировать, уже появляются. Сейчас на рынке продается по меньшей мере десяток операционных

систем, предназначенных автоматизировать процессы сбора и обработки информации о субъектах бизнеса: Info Tailor, Tracer, «Медиалогия», CronosPlus, Cros, Intellectum.BIS, «Монитор», информационно-поисковая система «Артефакт», система медиа-мониторинга «Медиалогия» и др. Стоимость подобных систем составляет $2–40 тыс. в зависимости от степени сложности.

Союз «шпионов»

Четыре года назад финразведчики России сформировали профессиональный союз — Российское общество профессионалов конкурентной разведки (РОПКР). Помимо чисто «профсоюзных» функций РОПКР намерено заниматься разработкой методологии отечественной конкурентной и финансовой разведки вплоть до преподавания этих дисциплин в экономических вузах.
Так что, вполне вероятно, недалек день, когда в перечне вузовских специальностей появится позиция «разведчик».
Еще одна задача, взятая на себя профсоюзом шпионов, этическая. По мнению Алексея Горделяна, исполнительного директора РОПКР, институту финразведки необходимы саморегулируемые принципы ведения дел. РОПКР выступает за создание кодекса финразведки, который был бы основан на трех базовых постулатах: отказе от получения информации путем обмана или шантажа, отказе от противоправных действий, отказе от причинения физического вреда людям или материальным объектам с целью приобретения конкурентных преимуществ.
Что же касается юридической основы деятельности финразведчиков, то ее определяют законы «О коммерческой тайне», «Об информации, информатизации и защите информации», «Об оперативно-розыскной деятельности», «О кредитных историях» и официальный перечень сведений, составляющих государственную тайну. О разработке специального закона, регламентирующего негосударственную разведку, речь пока не заходила.

Конкурентная разведка в юридическом бизнесе

Конкурентная разведка в юридическом бизнесе

Конкурентная разведка более двух десятилетий активно проявляет себя в различных сферах экономики и бизнеса, но только в последние годы начинает привлекать внимание адвокатских и других фирм, предоставляющих юридические услуги.

Автор статьи в журнале “Law Times” (05 March, 2007) Джим Миддлмисс приводит высказывания ряда экспертов, занятых в сфере юридического бизнеса, которые свидетельствуют о растущем интересе к использованию конкурентной разведки в этой сфере.

По мнению Жана Риверса (юридическая компания Dorsey & Whitney, Toronto office), КР пока делает лишь первые шаги на рынке юридических услуг, но в будущем будет приоритетным направлением.

Что заставляет юристов обращаться к инструментарию КР? Как считает Дуг Гувер (Thomson West), - обостряющаяся конкуренция между юридическими компаниями. «Сражение за рынок юридических услуг становится все ожесточеннее. Наблюдается тенденция консолидации между разными компаниями. Главным оружием конкуренции становится снижение ставок и тарифов».

Желание выжить вынуждает обраться к методам конкурентной разведки. Последние опросы показывают, что 89 процентов юридических фирм планируют взять КР на вооружение в ближайшие два года. Уже сегодня 60 процентов фирм так или иначе еженедельно ведут КР-исследования. Однако, только 27 процентов имеют для этой деятельности отдельную строку в своем бюджете.

КР может служить самым разным задачам, в том числе для анализа процессов слияния и поглощения, подбора кадров, планирования работы клиентских компаний, нахождения новых клиентов….
Развитию КР способствует и быстро растущие объемы информации, требующие постоянного анализа. Так, например, упомянутая выше компания Thomson наладила четырех-модульную систему мониторинга, которая помогает отслеживать события и тенденции в области судебных тяжб между фирмами, а также в сферах интеллектуальной собственности, коммерческих сделок, деятельности собственно юридических фирм.

Нередко, замечает Ж. Риверс, задачи КР возлагаются на информационно-библиотечную службу, на специалистов-маркетологов. Неэффективность использования КР объясняется отсутствием стратегии, плохой координацией работы сотрудников внутри компании, отличительными особенностями организации работы юридических фирм.

Вместе с тем, обращает на себя внимание огромное количество объявлений, приглашающих на работу в юридические компании специалистов по конкурентной разведке, что позволяет утверждать, что КР сегодня представляет наиболее быстро растущую сферу интереса на рынке юридических услуг.

Конкурентная разведка для системы материально-технического снабжения

Конкурентная разведка для системы материально-технического снабжения предприятий

Этому вопросу посвящена пространная публикация в “Supply Chain Management Review” (01.01.2007), некоторые фрагменты которой журнал «Бизнес-разведка» начинает публиковать в текущем номере. Автор публикации – Ричард Уилкинс, Concordia Intel (консалтинг по менеджменту).

Нужно ли анализировать, как действует на предприятии система материально-технического снабжения, особенно в сравнении с конкурентами? Вопрос во многом риторический. Главный смысл этого, как пишет Р.Уилкинс, заключается в том, чтобы ваша система работала не хуже, а желательно лучше, чем у ваших конкурентов. Кроме того, бенчмаркинг способствует нахождению возможностей для улучшения работы системы обеспечения.

Надо не только отслеживать процесс материально-технического снабжения, но и делать это систематически, регулярно. Автору публикации известны компании, которые проводят такое исследование ежегодно, обычно за четыре месяца до принятия нового бюджета. Этого явно недостаточно. Ведь конкуренты, особенно если речь идет о небольших фирмах, способны в любой момент начать выпуск новой продукции, заключить стратегические партнерства с оффшорными снабженческими компаниями, поменять топ-менеджмент, пустить в дело новые маркетинговые стратегии, изменить ценовую политику, начать агрессивную рекламную кампанию. Те, кто занимается КР время от времени, не постоянно, могут просмотреть важные изменения в деятельности конкурентов.

Какая именно информация применительно к системе материально-технического обеспечения наиболее важна? Чтобы понять, надо сформулировать и попытаться ответить на такие вопросы:

- в каком состоянии находится система снабжения у конкурентов (лучше чем у нас, т.е. дешевле, быстрее, эффективнее,…). Если система у конкурентов лучше, то что следует предпринять для преодоления их преимуществ?

- автоматизируют ли конкуренты какие либо звенья системы снабжения для удешевления и выигрыша во времени?

- какую роль играет аутсорсинг в снабжении конкурентов?

- как сами клиенты оценивают эффективность системы снабжения у вас и ваших конкурентов?

Особого внимания заслуживает мониторинг конкретных факторов, определяющих эффективность работы системы снабжения:

• Затраты времени на операцию заказ-получение

• Способность адаптации к новым продуктам, услугам, клиентам.

• Стоимость сырья, полуфабрикатов и готовой продукции

• Прозрачность системы снабжения и сбыта, т.е. ее доступность для оперативного мониторинга, анализа.

• Надежность партнеров (фирм, занимающихся снабжением с бытом).

Российское общество профессионалов конкурентной разведки

А. Горделян
Исполнительный директор РОПКР

«Российское общество профессионалов конкурентной разведки»

Начало XXI века ознаменовалось приходом новой - "интеллектуальной экономики", где главным источником роста благосостояния становятся не природные ресурсы, а результаты созидания человеческого ума - идеи и основанные на них нововведения. На первых ролях сегодня страны и сообщества, экономики которых основаны на знаниях.

Новая эпоха предъявляет и новые требования к руководству предпринимательством, главной чертой которого является гибкость и быстрота реакции на внешние условия. Однако при резком росте объемов циркулирующей в мире информации ни один руководитель не в состоянии охватить её без предварительного анализа и оценки профессионалами. И, как следствие, ключевая роль теперь отводится функции обеспечения руководителей актуальными, специально ориентированными на принятие стратегических решений сведениями (разведывательными сведениями) о деловом окружении и конкурентной среде вокруг своей организации (фирмы, компании).

По мере утверждения и в России рыночных отношений, становится все более очевидной ориентация информационной потребности нового поколения руководителей компаний на конечный результат - производство и прибыльный сбыт конкурентоспособной продукции, основанный на последних научно-технических достижениях. Изменение характера инновационных процессов, более тесная увязка создания новых технологий с их правовой охраной, необходимость обеспечения конкурентных позиций самой России на мировом рынке - требуют радикальной перестройки в информационно-аналитическом обеспечении стратегических решений.

Для обеспечения конкурентных преимуществ и как следствие - успешного развития бизнеса, - в компаниях промышленно развитых стран на исходе XX века стали создавать специальные службы "конкурентной разведки" (КР). Основными функциями данных служб являются сбор разведывательных сведений о намерениях конкурентов, основных тенденциях развития бизнеса, возможных рисках для бизнеса, новых возможностях бизнеса и т.д., их анализ, подготовка выводов и прогнозов, и, как следствие, их учет при принятии стратегических управленческих решений. Конкурентная разведка - это не просто информация, а, прежде всего, постоянный анализ и прогноз изменений на рынке.

Конкурентная разведка - это проводимые на постоянной основе сбор информации и исследования как рынка, так и всей деловой среды с целью выявления реальных и потенциальных факторов, которые влияют или могут повлиять на способность фирмы успешно конкурировать на данном рынке.

Результаты исследований конкурентной разведки обрабатываются таким образом, что они непосредственно служат основой для принимаемых стратегических решений или являются вводными для процесса стратегического планирования. Конкурентная разведка основана на факторе времени и привязана к нему.

По мере глобализации конкурентной борьбы потребность в конкурентной информации становится все более острой. А это ставит целый ряд организационно-правовых и этических вопросов осуществления конкурентной разведки, в частности таких, как:
Какова оптимальная инфраструктура КР? Где все-таки проходит грань между легальными и нелегальными, этичными и неэтичными методами сбора информации? Допустима ли кооперация корпоративных и государственных служб разведки и контрразведки?

Указанные обстоятельства, а также все возрастающая потребность бизнеса России в практическом использовании конкурентной разведки, подвигли группу российских специалистов в области конкурентной разведки на создание и регистрацию в г. Москве 29 августа 2002 года юридического лица в виде некоммерческой организации в организационно-правовой форме некоммерческого партнерства «Российское общество профессионалов конкурентной разведки» (РОПКР).

Членом некоммерческого партнерства может стать любое физическое или юридическое лицо, заинтересованное в совместном достижении уставных целей Партнерства.

В Партнерстве также существует институт Консультантов. Войти в состав консультантов могут представители государственных органов и учреждений, коммерческих и некоммерческих организаций, общественных и профессиональных объединений, а также лица, согласные оказывать Партнерству и его членам содействие в достижении уставных целей и задач.

Основными целями деятельности Партнерства являются:
• оказание помощи членам организации в их профессиональном развитии;
• создание условий для объединения специалистов профессионально занимающихся конкурентной разведкой и специалистов других сфер деятельности, интересующихся теорией и практикой конкурентной разведки;
• сотрудничество с международными и зарубежными организациями аналогичного профиля с целью обмена информацией, опытом в области конкурентной разведки;
• содействие и поддержка международной конкурентоспособности России, ее отраслей и отдельных предприятий (компаний) посредством внедрения и совершенствования функций конкурентной разведки;
• разработка, внедрение и совершенствование методической, методологической базы конкурентной разведки в Российской Федерации, с учетом действующего законодательства и международного опыта. Обобщение и распространение опыта практической работы членов Партнерства;
• внедрение обучающих программ и методик по специальностям в сфере конкурентной разведки в учебных заведениях Российской Федерации. Проведение обучения специалистов посредством организации Партнерством дополнительного образования;
• сотрудничество с государственными, общественными, образовательными и коммерческими структурами по развитию цивилизованного бизнеса и конкуренции, цивилизованной защиты бизнеса.

В рамках осуществления своей уставной деятельности Некоммерческое партнерство:
• - налаживает взаимодействие с различными общественными, государственными и коммерческими структурами;
• - устанавливает связи с различными регионами России;
• - развивает международное сотрудничество с аналогичными и родственными организациями.

Более подробно с целями и задачами, стоящими перед РОПКР, условиями членства в РОПКР и в институте консультантов можно ознакомиться на сайте (www.rscip.ru)

Конкурентный анализ в онлайновом маркетинге

Конкурентный анализ в онлайновом маркетинге

Интернет-маркетинг, в частности, регулярная рассылка электронных писем, выпуск онлайновых бюллетеней, становится все более важной частью борьбы за клиентов, за рынки.

Здесь предоставляется широкое поле для конкурентной разведки и анализа. Ниже следует сокращенный перевод некоторых рекомендаций, которые предлагает эксперт в области e-mail marketing Ж. Дженнингс ("Emaillabs", March 26, 2007)).

Самое простое для начала – подписаться на электронные бюллетени, выпускаемые вашими конкурентами. При этом советовал бы не давать персональный или корпоративный адреса, но воспользоваться нейтральным, временным адресом. Далеко не все компании проверяют адреса подписчиков, но некоторые это делают. Также было бы неплохо держать корреспонденцию бюллетеня отдельно от других писем в своем компьютере. Регулярный просмотр рассылочных материалов конкурентов позволит анализировать такие вещи как:

- регулярность рассылки;

- виды рассылки (коммерческие или нет, их формат и т.п.)

- периодичность и время рассылки;

- какие товары и услуги рекламируются, или упоминаются;

- какие содержательные виды используются (короткие или длинные, редакционные или рекламные).

- качество контента (отличное, плохое, равное вашему бюллетеню).

Желательно вовлекать в процесс анализа своих коллег – они могут обратить внимание на то, что ускользает от вашего взгляда, дать ценные рекомендации к улучшению собственной рассылки.

Главная же цель – сравнить бюллетени конкурентов со своим, сделать правильные выводы.

Обнаруживаем слабости конкурентов:

- например, электронный бюллетень конкурирующей компании, рассылаемый по понедельникам вечером, содержит новости прошедшей недели. Вам нужно эти новости печатать немедленно, тем самым, опережая конкурентов.

- конкурент не фокусирует внимание на отраслевых сегментах, вы можете сделать это в своей рассылке;

- коммерческие рассылки конкурентов не содержат упоминания о возможных скидках в предстоящих продажах. Вы можете переключить внимание на себя, указав в своих сообщениях готовность на 10% скидки.

Обнаруживаем сильные стороны конкурентов, представляющие собой угрозу для вас:

- еженедельный анализ правовых аспектов бизнеса делается блестяще. Тогда, возможно, вам не стоит тратить на это время и ресурсы.

- конкурент привлекает к подготовке бюллетеней специалистов со стороны. Здесь следовало бы в свою очередь пригласить экспертов для работы над вашими материалами, но, конечно, не ангажированных конкурентами;

- конкурент регулярно рассылает специальные предложения по вторникам во второй половине дня. Можете действовать на опережение, начав рассылку своих предложений по понедельникам.

Подражать - еще не значит конкурировать

Подражать – еще не значит конкурировать

В онлайновом издании Search Engine Guide, April 3, 2007, опубликована статья Дианы Аул, в которой рассказывается о том, как борьба с конкурентами, превращаясь в нечто самодовлеющее и самодостаточное, пагубно влияет на собственный бизнес. Пример из реальной практики автора, возможно, поможет избежать некоторых ошибок и заблуждений, подстерегающих предпринимателей на этапе начального выстраивания бизнеса. Предлагаем краткое изложение этой поучительной истории

Однажды автора этой публикации друзья попросили помочь с установкой бухгалтерской системы в только что созданной ими фирме. Диана сделала все, что они просили, и на прощание дала несколько советов. Некоторые были приняты к сведению. Другие нет. Вскоре ее друзья столкнулись с серьезной проблемой, поставившей их новый бизнес на грань банкротства. А проблема заключалась в том, что в центр своей деятельности они поставили борьбу с конкурирующей компанией, причем, конкуренцию буквально по всем направлениям. У конкурента новый фешенебельный офис? Мы тоже снимем дорогостоящее, ничем не уступающее помещение. Конкурент держит офисную администрацию? Что ж, и мы наймем офисного менеджера. На этом не остановились: зарплаты у нас будут выше, а цены – ниже...Все помыслы сосредоточились на том, чтобы превзойти во всем конкурента.

При этом, конечно, не было принято во внимание, что конкурент начинал с малого, как небольшая по размеру и размаху фирма – первые два года в ней работали всего два человека, владелец и его сводный брат. Постепенно, по мере развития бизнеса, росла и сама фирма. Не сразу у нее появилось шикарный офис, административные помощники...

Естественно, что при таком подходе вскоре у друзей возникли трудности. Затраты на помещение и штат съедали все доходы, и без того небольшие как результат демпинга. Один из них не выдержал, сошел с дистанции, двое взяли дополнительную работу на стороне, чтобы хоть как-то сводить концы с концами. И только четвертый из партнеров продолжал упорно рулить по той же дорожке.

Конечно, жизненно важно следить за конкурентами. Но это не означает рабское копирование. У каждого из конкурентов свой портфель проблем и свой набор ресурсов и средств их решать. То, что работает у конкурента, совсем не обязательно будет работать у вас.

Диана Аул советует в заключение смотреть одним глазом на конкурента, а другим – на собственные дела и общее состояние рынка. Делайте свое дело наилучшим образом и в один день вы обнаружите, что конкуренты внимательно за вами следят!

Анонсирование вакансий как информационный ресурс

Анонсирование вакансий как информационный ресурс конкурентной разведки

Уже некоторое время распространяются слухи, что Google работает над новым проектом, связанным с мобильными средствами связи. Но слухи есть слухи, и некий Брайн Колфилд решил проверить методом внимательного изучения открытых корпоративных источников

этой компании. О методике и результатах исследования он рассказал в репортаже «Как я шпионил за Google», опубликованном в марте на сайте forbes.com (March 20.2007).

Брайн зашел на раздел сайта, где размещаются объявления о работе. Там он прочитал, что «компания проводит эксперименты в области беспроводных коммуникационных систем», и далее: «компания создает компактную команду аналоговых и цифровых разработчиков, способную создать всемирную информационную систему, бесплатную и доступную из любой точки земного шара».

Google, утроившая за последние два года численность своих работников, готовится удвоить персонал к концу 2007 года. Трудно хранить секреты при таком стремительном развитии. Анализ объявления и реклам Google дает возможность сделать вывод, что компания готовиться к прямой конкуренции с Microsoft. Некоторые эксперты считают, что Google, которая недавно купила фирму Энди Рубина, известного разработчика беспроводных систем, работает над каким-то мобильным и компактным средством коммуникации.

Официальные представители Google отмалчиваются. Но на одном испано-язычном сайте можно найти признание сотрудника, что компания «экспериментирует с мобильными телефонами».

Изучение предложений о работе в Google позволяет выявить и другие интересные данные. В частности, Google ищет высококвалифицированных инженеров по производству компьютерных изделий и разработчиков софтов. При этом предпочтение отдается выпускникам престижных вузов, таким как Массачусетский Технологический Институт, Мичиганский университет.

Подбором специалистов для Google занимаются кадровые агентства в Европе. Конечно, такой широкий заброс невода содержит риск утечки информации о проектах компании. Но есть и своя положительная сторона – собеседования с тысячами умных людей относительно возможной их работы в Google помогают уже на предварительном этапе узнать, насколько хорошими на самом деле являются планируемые проекты.

Криминологический аспект защиты информации

В.Шарлот

Криминологический аспект защиты информации. Криминальная мотивация

Часть-1

Согласно исследованию компании Info Watch - "Внутренние ИТ-угрозы в России-2006" - респонденты выделяют утечку конфиденциаль¬ной информации в качестве самой опасной угрозы информационной безопасности (ИБ) (65,8%). Сразу за утечками следует халатность служащих (55,1%). Индекс опасности вирусных атак занимает лишь третье место (41,7%), затем идет информационный саботаж (33,5%). Другими словами, из 4 наиболее опасных угроз 3 относятся именно к рискам внутренней ИБ. Кроме того, исследование выявило, что российские государственные и коммерческие организации отчетливо осознают все отрицательные последствия утечек конфиденциальной информации и других инсайдерских инцидентов: прямые финансовые убытки (46%), удар по репутации (42,3%) и потерю клиентов (36,9%).

Для обеспечения ИБ компании необходимо учитывать потребности, интересы и ценности человека, а не рассматривать его как винтик большой машины, лишь пытаясь выжать из него максимум эффективности. Нужно понимать, что никакие формальные запреты и ограничения реально не могут повлиять на поведение сотрудника, кроме его собственного сознания. Временно можно подчинить его волю своим интересам, но если человек решил извлечь пользу из своего служебного положения, этому очень трудно помешать. Однако, зная мотивы такого поведения и условия их формирования, с одной стороны, и склонности

сотрудников - с другой, вполне можно предсказать развитие подобных тенденций и предотвратить неблагоприятные последствия. Для этого необходимо рассмотреть криминальные мотивы поведения сотрудников, т.е. мотивы, направленные на удовлетворение индивидуальных потребностей в ущерб фирме. Криминологи различают несколько структурных элементов преступного деяния, осуществленного в виде сложного волевого действия:
1) мотивация преступного действия;
2) формирование цели преступного действия;
3) принятие решения о совершении конкретного преступного деяния, направленность и содержание преступного умысла;
4) способы осуществления преступного деяния;
5) достижение результата и отношение субъекта к этому результа¬ту.
Только на основании анализа всех этих элементов, можно построить целостную систему защиты информации.

Мотивация, по мнению многих исследователей, как психическое явление, характеризующее личность, является ключевым элементом преступного поведения. Необходимо разделять сознательные и неосознанные, а также умышленные и неумышленные действия и мотивы. Это разделение необходимо для выстраивания сбалансированной системы профилактических мер, выбор адекватных методов и средства воздействия на сотрудника.

Сознательные нарушения совершаются при полном контроле сознания за собственными действиями, они могут быть как умышленными, т.е. иметь определенное намерение, оцениваемое как преступное, так и неумышленными, когда сотрудник не имеет намерение совершить противоправное деяние.

Умышленные и неумышленные нарушения в СЗИ различаются также по степени угрозы для различных видов уязвимости информации.

НЕУМЫШЛЕННЫЕ НАРУШЕНИЯ

В криминологии специфика объяснения умышленного и неосторожного преступного поведения объясняется позицией личности (особенностей ее потребностей, интересов, ценностных ориентаций). Искажение позиции у лиц, которые совершают умышленные преступления, чаще всего, носит иной характер, нежели у тех, которые совершают неосторожные преступления. В первом случае типичной является деформация смыслообразующих ценностей (например, уважение к чужой жизни, достоинству, собственности и т.д.), во втором случае - наличие "облегченного" отношения к ролевым обязанностям и функциям при признании основных базовых ценностей. Причина некоторых неумышленных преступлений состоит также в том, что у человека отсутствует потребность постоянно контролировать свои самые ответственные действия или прогнозировать будущее развитие событий. Следовательно, профилактические меры, направленные на предотвращение нарушений режима конфиденциальности, также должны учитывать различные аспекты личности сотрудников.

При неосторожном нарушении режима конфиденциальности человек не только не старается получить личную выгоду в ущерб организации, но может даже не подозревать о возможности такого ущерба. Здесь необходимо различать преступную неосторожность, преступную самонадеянность и трагическую случайность.

Преступная самонадеянность заключается в том, что сотрудник предвидел негативные последствия своих действий, но легкомысленно надеялся их избежать. Например, если сотрудник оставляет конфиденциальные документы у себя на столе или в кабинете, не оборудованном соответствующими средствами ЗИ, надеясь, что с ними ничего не случиться. Говоря о преступной самонадеянности, следует иметь в виду такие мотивационные и характеризующие личность факторы, как стремление к успеху, склонность к риску, завышенная самооценка, завышенный уровень притязаний.

Преступная неосторожность заключается в том, что сотрудник должен был предвидеть негативные последствия своих действий, но по зависящим от него причинам не сделал этого. Преступная неосторожность действительно предполагает беспечное отношение к своей социальной роли, выражающееся в невнимательности, непредусмотрительности, безответственном отношении. Интересы такого сотрудника будут, скорее всего, лежать

далеко за пределами его работы, а основным мотивом трудовой деятельности, видимо, будет мотив стремления к межличностным контактам в процессе работы (ориентация на других людей). Например, сотрудник откладывает замену технических средств или программного обеспечения по ЗИ по каким-то личным причинам, зная, что уже существует внешняя угроза, которой старые средства противостоять не могут.

Трагическая случайность состоит в том, что сотрудник не мог или не должен был предвидеть негативных последствий своих действий. Невозможность предвидения вредных последствий может быть вызвана как субъективными особенностями лица (отсутствие необходимых знаний, навыков, опыта, болезнь и т.п.), так и обусловлена той конкретной обс¬тановкой, в которой было совершено деяние. Т.е. неблагоприятные пос¬ледствия были итогом ошибки вследствие фатального соединения неблагоприятного стечения обстоятельств и индивидуальных особенностей сотрудника. Например, сотрудник не знал, как вести себя во время чрезвычайной ситуации, в результате чего произошла утрата конфиденциальной информации.

УМЫШЛЕННЫЕ ПРЕСТУПЛЕНИЯ

Умышленные нарушения режима конфиденциальности - самый опасный вид нарушений, характеризующийся целенаправленностью, методичностью и продуманностью. Умышленные преступления наиболее опасны, т.к. сотрудник стремится получить больше благ в ущерб интересам фирмы. Меры противодействия в этом случае будут достаточно сложны и затратны.
Можно выделить два основных типа умышленных преступлений в СЗИ – корыстные и некорыстные нарушения режима конфиденциальности. Каждый из этих типов по-разному влияет на уязвимость информации.

Корыстное нарушение - сознательный поступок, имеющий вполне определенную цель - получение материальной выгоды от совершенных действий. Умысел заключается здесь в ожидании получения какого-либо блага от конкурента или иного заинтересованного лица за действия, которые, как известно сотруднику, нанесут ущерб. Хотя ущерб в данном случае не является самоцелью, но допускается, т.к. в сравнении с желаемым материальным благом для сотрудника не имеет большой отрицательной ценности. Понятно, что такой сотрудник будет обладать не только выраженной корыстной направленностью личности, но и отличаться негативным или безразличным отношением к таким социальным ценностям как справедливость, честность, добросовестность и т.п.

При умышленном нарушении конфиденциальности фактическое пособничество внешнему противнику (разведывательной службы конкурента, представителей криминальных структур, государственных коррумпированных структур) может реализоваться тремя основными способами: инициативное сотрудничество, спровоцированное сотрудничество, сотрудничество под влиянием.

Инициативное сотрудничество - добровольное содействие внешнему противнику, совершаемое или начинаемое по собственной инициативе. Мотивационное основание инициативного сотрудничества часто лежит в стремлении человека к достижению успеха, иногда любой ценой. Не рассматривая сейчас все возможные мотивы, которые могут приводить сотрудника к поиску контактов с конкурентом, следует отметить большую активность такого сотрудника, а также его склонность к рискованным мероприятием, т.к., безусловно, любой контакт с конкурентом может быть раскрыт со всеми вытекающими отсюда последствиями.

Спровоцированное сотрудничество - содействие сотрудника внешнему противнику, так или иначе обусловленное активными действиями лиц (или лица), уполномоченных конкурентом (или любым другим злоумышленником), направленными на сотрудника. Подобное воздействие основано на том, что злоумышленник пытается активизировать потенциальные мотивы сотрудника, направленные на личное обогащение или другие сугубо личные цели, действуя по определенным правилам.

Сотрудничество под влиянием - содействие сотрудника внешнему противнику, когда сотрудник имеет первоначально вполне одобряемые убеждения и мотивы, но изменяет их в результате активного воздействия внешнего противника. Это сотрудничество обусловлено вновь сформированными мотивами деятельности сотрудника, хотя бы и временными.

При склонении сотрудника злоумышленником к нарушению режима конфиденциальности в основном используются следующие мотивы: месть, ревность, корысть, игра, тщеславие.

Месть - мотив сотрудника, ощущающего себя несправедливо наказанным или обойденным, униженным и т.п., который выражается в чувстве обиды на руководство организации, своего непосредственного начальника или коллег. Такой сотрудник стремится нанести ущерб обидчику в ответ на субъективно воспринятую несправедливость по отношению к себе, за причиненное зло, за действия, существенно затрагивающие интересы его или его близких. Ущерб часто разделяют как источник обиды, так и фирма.

Еще один "бескорыстный" мотив - ревность. Ревность, независимо от того, вызвана ли она действительными или ложными основаниями, всегда олицетворяет сомнение, боязнь потери какого-то блага (расположения, внимания, любви, дружбы и т.п.) и связанное с этим стремление любыми средствами удержать это благо, пользоваться вниманием, расположением другого лица. Исходя из данного определения, предметом ревности могут быть отношения начальника со своими подчиненными, отношения неформального лидера с членами своей группы и т.п. Ревность можно понимать как вид страха при стремлении обладать какой-то ценностью или удержать ее. Преступление из ревности побуждается неосознаваемым ощущением своей неполноценности и ущемленности, угрозы своему бытию. Для ревнующего человека то отношение, которое сложилось у него с другим лицом, является чем-то сверхценным, т.е. тем, что приносит не только очевидные блага, следующие из сложившихся отношений, но и удовлетворяет основные потребности человека в принятии, определенности и стабильности, безопасности, самотождественности и т.п.

Игра - мотив сотрудника с авантюристическими наклонностями, нарушающего режим конфиденциальности и наносящего ущерб фирме ради получения удовлетворения от тайного и удачного нарушения установленных правил или запретов. Для игрока характерно сочетание способности к длительной активности и импульсивности, что порождает постоянное влечение к острым ощущениям и переживаниям. Они активно ищут возбуждающие ситуации и нуждаются во внешней стимуляции, это сочетается с пренебрежением социальными нормами, правилами, обычаями и безответственностью. Это люди, в значительной степени идущие на поводу своих желаний и влечений, у них часто встречается склонность к злоупотреблению алкоголем, беспечной праздности, легкой жизни. Смысл игры для такого индивида заключается отнюдь не в выигрыше, а в самом процессе игры, в испытываемом чувстве опасности и своего превосходства над обстоятельствами и людьми.

Тщеславие - мотив сотрудника, желающего с помощью нарушения режима конфиденциальности заработать себе определенную репутацию. Такой сотрудник надеется, что наконец-то покажет всем, какой он все-таки бесстрашный, умный, способный, сильный, могущественный (эгоистическая направленность). Либо он уверен в том, что своими действиями он принесет пользу другому человеку или всему обществу, даже ценой какого-либо ущерба для себя (альтруистическая направленность). Главное, чтобы после того, как он это совершит, о нем заговорили значимые для него люди. Здесь может быть важен и сам факт нанесения значительного ущерба большой организации одним человеком. Вознаграждение в этом случае может предусматриваться, но оно не является определяющим фактором.

Необходимо отметить, что вышеприведенные мотивы могут реализовываться и без участия внешнего противника. В замыслах “криминального сотрудника” для достижения своей цели его может вовсе не быть, но коль скоро они наносят ущерб предприятию, играют ему на руку. При совершении таких нарушений как уничтожение или несанкционированная публикация конфиденциальной информации, блокирование доступа к ней, создание препятствий для проведения необходимых мероприятий непосредственно по защите информации, создание конфликтных ситуаций и др. конкурент может и не подозревать о подобных действиях сотрудника, но, чтобы он не смог воспользоваться ситуацией или раскрыть слабости СЗИ, информация о таких нарушениях не должна раскрываться.

(продолжение в следующих выпусках журнала)

Об авторе: Шарлот Всеволод Валерьевич, 34 года, аналитик, член Клуба сотрудников информационный служб (http://club-sis.net/rabota.php), с 1999г. постоянно выходят

Методы Дж.Бонда - на службе безопасности бизнеса

Методы Дж. Бонда – на службе безопасности бизнеса

Одна из крупнейших в мире компаний в сфере розничной торговли Wal Mart внезапно оказалась в центре скандала, когда один из уволенных технических сотрудников заявил, что руководство компании осуществляет операции слежения за сотрудниками, партнерами и консультантами. Брюс Габбард и его непосредственный начальник были уволены, как заявили официальные представители компании, «из-за превышения полномочий». По словам Габбарда, он участвовал в широкой операции слежки за теми, кто выражал недовольство политикой компании. Ему было, в частности, поручено руководителями службы безопасности прослушивать их телефонные разговоры, следить за корреспонденцией. Более того, Габбард заявил в интервью корреспондентам, что начальство внедрило «своего человека в группу недовольных, чтобы выяснить, собираются ли они выражать свои протесты на ежегодном собрании акционеров».

Скандал привлек внимание американской печати и вызвал оживленную дискуссию. Как считают некоторые эксперты, «предпринимаемые компанией Wal Mart усилия по обеспечению безопасности выходят далеко за пределы обычных мер» (Santa Barbara News-Press, April 24, 2007). По их мнению, речь идет не столько о соблюдении правил безопасности, сколько об организации слежки за своими сотрудниками, а также за поставщиками и клиентами. Создание внутри компании собственного мини-ФБР может заставить нервничать ее клиентов, обеспокоенных перспективой нарушения их частных прав.

В этой связи обращает на себя внимание объявление о вакансии работника службы безопасности, размещенное на сайте Wal Mart. Описание функций вакантной должности включает, например, сбор данных в ходе профессиональных контактов, а также открытой информации с целью предупреждения потенциальных угроз, исходящих от «международных процессов, региональных и национальных событий, подозрительных личностей и групп». Любопытно, что в объявлении говорится о желательности владения иностранным языком, предпочтительно китайским или испанским.

Получивший широкую огласку скандал вокруг Wal Mart свидетельствует, как считают многие наблюдатели, что корпорации в стремлении предотвратить утечки служебной информации и прочие угрозы все чаще берут на вооружение методы Дж.Бонда, нанимая бывших сотрудников ЦРУ, ФБР и прочих секретных спецслужб. Но такая политика, становясь достоянием гласности, чревата ущербом престижу компании, в конечном счете – ее позициям на рынке. Кен Спрингер, бывший агент ФБР, президент и учредитель компании Corporate Resolutions, говорит: «Если раньше главной угрозой корпоративной Америке считались кражи, то сегодня большую головную боль вызывают утечки репутационной информации, особенно если речь идет о публикациях в печати и Интернете».

Рассел Корн, управляющий директор компании Diligence, в состав совещательного органа которой входит бывший директор ЦРУ Уильям Уэбстер, отмечает, что внутрикорпоративная разведка как бизнес быстро развивается. За последние годы она выросла втрое и оценивается сегодня в пол-миллиарда долларов в год. Кстати, пару лет назад компания Diligence сама попалась на шпионаже. Международная консалтинговая корпорация KPMG подала на нее иск, заявив, что Diligence подсылала в отделение KPMG на Бермудах своих людей, которые, выдав себя за представителей правительственных структур, пытались выудить служебную информацию.

Oracle против SAP - обвинение в шпионаже

Oracle против SAP – обвинение в шпионаже

Известная софтовая компания Oracle подала в суд иск на не менее известную немецкую фирму SAP, обвинив последнюю в том, что она использовала клиента Oracle для скачивания более 10 тысяч документов из баз данных, предназначенных для поддержки клиентов, в период между сентябрем 2006 г. и январем 2007г. Г.

В конце прошлого года Oracle обратила внимание на «необъяснимо настойчивые» попытки клиентов запрашивать в корпоративных базах данных поддержки (т.е. открытых для клиентов Oracle) разные сведения, иногда даже секунды спустя после получения первых результатов, что говорило об автоматическом процессе поиска и скачивания. При этом «клиенты» скачивали материалы в количествах, намного превышавшие их лицензионные права. Расследование показало, что несанкционированное вторжение в базы данных осуществляется с компьютеров SAP с использованием реквизитов и прав некоторых из клиентов Oracle. Была зафиксирована подозрительная активность дочерней фирмы SAP (SAP TN), обеспечивающей поддержку клиентам компании PeopleSoft, которая в 2005 году была приобретена корпорацией Oracle.

Хотя SAN TN занимается в основном продажами, ее интересовала главным образом техническая документация. «Работники SAP прибегали к использованию идентификационных данных многочисленных клиентов PeopleSoft, чтобы проникнуть в информационную систему Oracle под вымышленными предлогами» (“Security Focus”, 22-03-2007).

Атаки на информационные системы конкурентов становятся головной болью бизнеса. Еще в 2005 году в США отмечались целевые атаки на системы ряда корпораций с целью обмануть информационных работников. С того времени их число, в основном из Китая, только возрастает.

О некоторых мерах предотвращения кражи персональных данных

О некоторых простых мерах предотвращения кражи персональных данных, получаемых в ходе интернет-мониторинга

Охота за персональными данными, особенно в сфере финансово-банковской деятельности, стала в последние годы едва ли не главным видом преступлений, совершаемых в Интернете. Тому объективно способствуют современные Интернет-технологии, позволяющие коммерческим, кредитным, банковским организациям осуществлять детальный мониторинг своих корпоративных сайтов, отслеживая и анализируя посещения потенциальных и реальных клиентов, пользователей. Так накапливаются массивы информации, которые используются бизнес-структурами для повышения эффективности работы с клиентской базой, ее расширения. Но к этой информации проявляют неподдельный интерес и многочисленные хакеры, разного рода мошенники.

О том, как снизить риск несанкционированных утечек клиентских баз данных, информации о посещениях корпоративных сайтов, говорится в публикации Джое Базирико, аналитика по вопросам безопасности компании Security Innovation, в онлайновом издании DM Direct Newsletter, February 23, 2007 Issue.

Некоторые из рекомендаций.

Отказаться от политики хранения всей информации. Чем больше накапливаемых данных, тем выше риск нежелательных утечек. Чтобы определить, какая информация заслуживает

длительного хранения, а какая нет, нужно сформулировать и попытаться ответить на вопросы:

• Как данная информация реально помогает в работе с клиентами?

• Что будет, если эта информация попадет в сомнительные руки?

• Может ли хакер воспользоваться ее для выуживания персональных данных?

Иметь план регулярной, систематической чистки баз данных. Информация нередко быстро устаревает, поэтому важно своевременно избавляться от тех данных, которые уже не представляют собой коммерческую ценность.

Хранить данные Интернет-мониторинга и клиентов отдельно от общих корпоративных баз данных. Особенно это касается такой чувствительной информации как имена и пароли, номера кредитных карт, адреса... Желательно размещать такую информацию в базах данных, которые не связаны с корпоративным сервером. Это не только затрудняет охоту за ними со стороны хакеров, но и предупреждает перегрузки сервера.

Продумать систему допуска клиентов на корпоративный сайт. К примеру, предоставлять допуск к коммерческим базам данных только с письменного индивидуального разрешения.

Ставить надежные системы охраны информации, использовать криптографию.

Конкурентная разведка - что такое плохо

Конкурентная разведка: что такое плохо?

В нормальной конкурентной разведке нет ничего противозаконного, неэтичного. Собственно, этот вид деятельности – не более чем сбор и анализ информации из открытых, доступных источников. Однако, как отмечает автор блог-странички Мюрейл Венигопал (www.managerialgrid.blogspot.com), нередко бывает, что времени в обрез, его просто не хватает для неспешного процесса поиска и обработки открытых информационных ресурсов, и тогда возникает искушение воспользоваться некоторыми из приемов, выходящими за границы легальности и этичности. Какие эти методы? Автор рассматривает наиболее часто повторяемые из нежелательных приемов.

Обман

Обычно он заключается в легендировании (использовании фальшивого имени, места работы, придуманного повода) исследователя при знакомстве с носителем информации. Это противозаконно. Не говоря о том, что лгать вообще не достойно. Возможные последствия в случае разоблачения – судебное преследование с возможными штрафами и даже тюремным заключением.

Пример. В 2006 году Hewlett-Packard (HP) нанял фирму, представители которой использовали придуманные предлоги и имена для сбора информации о контактах некоторых директоров корпорации с журналистами.

Копание в мусорных баках

К этому приему прибегают в надежде отыскать в бумажных отходах данные о новых разработках и планах конкурентов. Это тоже попахивает тюрьмой. Самый скандальный случай: обвинение корпорации Procter & Gamble в «изучении» содержимого мусорных баков соперничающей корпорации Univeler. Хотя в этом случае мусорные баки формально не были собственностью конкурента и поведение нанятых Procter & Gamble детективов не давало повода для судебного преследования, скандал удалось замять ценой больших репутационных потерь. Вывод – стоит ли рисковать попаданием на первые полосы газет?

Невыполнение служебных обязательств

В данном случае речь идет о нарушении носителем конкурентной информации данных им по трудовому контракту обязательств хранить конфиденциальную служебную информацию. Некоторые полагают, что это дело совести самого источника информации, но никак не касается профессионала конкурентной разведки, который с ним общается, работает. Однако, полагает Уэнди Шмидт, руководитель компании Forensic & Dispute Services, если исследователю известно, что источник нарушает правила безопасности своей фирмы, то лучше поискать альтернативный ресурс.

Раскрытие источника информации

Предав огласке имя, место работы источника информации вы можете его поставить в весьма затруднительное положение. Поэтому эксперты рекомендуют ограничиваться общими словами, например, «один из менеджеров крупной компании»....Желающих узнать, откуда вы получили ценную информацию, всегда полно. Сохраняя источник в секрете, вы оберегаете его от разных неприятностей, в том числе, увольнения.

Конференции и выставки: сбор и защита информации

«Конференции и выставки: сбор и защита информации»

Фонд конкурентной разведки анонсировал выход в свет книги «Конференции и выставки: сбор и защита информации» (scip.online, Issue 112).

Это второе издание в серии «Темы конкурентной разведки». Книга повествует о практике сбора первичной информации на конференциях, семинарах, симпозиумах, торговых выставках. Объемом 223 страницы, книга отражает опыт профессионалов конкурентной разведки, как академических экспертов, так и практиков.

Разведка на конференциях и выставках решает две главные задачи: сбор конкурентной информации у непосредственных ее носителей и предотвращение утечек собственной корпоративной информации.

Рассматривается полный цикл работы – подготовка к конференции/выставке, работа непосредственно на конференции/выставке, итоговый анализ по окончании мероприятия. В отдельных разделах анализируются этические и правовые аспекты, контрразведка, конкурентная техническая разведка. На двух конкретных примерах рассказывается о законченном процессе КР, включая итоговые рекомендации для топ-менеджмента.

Книга может представить практический интерес для всех, кто занимается конкурентной разведкой, равно как и для организаторов выставок и конференций, и для преподавателей КР.

Стоимость книги $49.95. Заказать ее можно, обратившись в Организацию профессионалов конкурентной разведки (SCIP) – www.scip.org (Trenita Dickley)

Дистанционное обучение

Дистанционные технологии обучения в Институте безопасности бизнеса

Институт безопасности бизнеса в составе Московского энергетического института (технического университета) проводит обучение специалистов, имеющих высшее образование, по программе профессиональной переподготовки «Экономика и управление на предприятии» со специализацией «Экономическая безопасность хозяйствующего субъекта» объемом 546 часов. Настоящая программа разработана по заказу РАО «ЕЭС России», успешно апробирована и реализуется с применением дистанционных технологий обучения через интернет в синхронном режиме работы слушателей, что дает возможность

получения знаний без отрыва от производства.

Обучение ориентировано на руководителей среднего и высшего звена предприятий добывающих, энергетических отраслей народного хозяйства и машиностроения.

Обучение начинается с проведения установочного сбора (1 неделя) и заканчивается итоговым сбором (3-4 дня), в течение которого слушатели сдают комплексный государственный экзамен и защищают выпускные аттестационные работы.

В процессе обучения слушатели изучают 15 дисциплин, в том числе:

1. Блок базовых дисциплин:

* Методика обучения в системе дистанционного обучения;

* Менеджмент,

* Экономика хозяйствующего субъекта;

* Маркетинг.

2. Блок специальных дисциплин:

* Информационно-аналитическое обеспечение безопасности (деловая разведка);

* HR-менеджмент: аспекты безопасности;

* Информационная безопасность;

* Экономическая безопасность;

* Технические средства обеспечения безопасности;

* Экономика обеспечения безопасности;

* Правовые основы обеспечения безопасности;

* Страхование и страховые риски;

* Антикризисный PR и противодействие «черному» PR;

* Профессиональная этика специалиста в области обеспечения безопасности;

* Антитерроризм.

Слушатели обеспечиваются комплектом учебно-методических материалов на CD-ROM, включающих курсы лекций, дайджесты статей и профильных публикаций, программное обеспечение, справочные электронные издания, комплект печатных изданий.

Слушатели, успешно освоившие учебную программу, сдавшие комплексный государственный экзамен и защитившие выпускную аттестационную работу, получают государственный диплом МЭИ (ТУ) о профессиональной переподготовке.

Подробная информация по данной теме размещена в Интернете по адресу:

http://do.ibbusiness.ru <http://do.ibbusiness.ru/>

E-mail: cdo@ibbusiness.ru .

Тел/факс: (495) 362-72-55, тел. (495) 673-02-89.

Телефон (прямой): 8(926) 521-1621