

оглавление

Деловая разведка - цели и задачи

Деловая разведка в период застоя и спада

**Что мешает развитию деловой разведки в России (Беседа с
Генеральным директором компании «Амулет» А. Крыловым)**

Организация и методы деловой разведки

Понять культуру поведения клиента

Электронный бизнес: как сделать виртуального посетителя реальным покупателем

Как делать внутренний бюллетень конкурентной разведки

**Психология как один из инструментов конкурентной
разведки**

Сотрудник приходит в фирму. Как его проверить

Информационные ресурсы

КПМГ: Инвестиционный интерес к России растет

**Информационная безопасность и борьба с промышленным
шпионажем**

В. Борисов Защита информации при увольнении

Пять лет американского «Акта о промышленном шпионаже»

Безопасность информации: программа OPSEC

Технологии деловой разведки

Передовые информационные технологии для малого бизнеса

Интернет технологии и работа с клиентами

Путешествие в невидимую Сеть

Программа для конкурентной разведки в электронном бизнесе

Этика деловой разведки

Стоит ли рисковать репутацией?

Советы профессионалам деловой разведки

Десять наблюдений и рекомендаций по деловой разведке

© 2001 Светозаров В.Б. svetv@ru.ru

Деловая разведка в период застоя и спада

Деловая разведка - цели и задачи

Деловая разведка в период застоя и спада

Информационные агентства сообщают о продолжающемся спаде в американской экономике, особенно чувствительно проявляющем себя в "новой экономике". И сегодня дело не ограничивается понижением курса акций. Реально сокращается объем услуг и производства. Появилась безработица там, где еще недавно ощущался дефицит - среди программистов, тех, кто работает с Интернет технологиями.

Как считает крупный эксперт в области конкурентной разведки Кеннет Савка, вице-президент исследовательско-консалтинговой компании Fuld & Company Inc., существует реальная опасность, что сокращения могут непосредственно затронуть отделы конкурентной разведки, ибо многие руководители рассматривают это направление как вспомогательное, которым можно пожертвовать в трудные времена. "Нет ничего глупее, - отмечает Савка, - чем сокращение или ликвидация функций конкурентной разведки в периоды экономической неопределенности".

По его мнению, значение КР, напротив, возрастает во времена общего спада. В условиях нормального, прогрессирующего развития бизнеса КР выполняет в основном защитные функции, предупреждает о вероятных действиях конкурентов, представляющих для фирмы потенциальную опасность, о возможных неблагоприятных тенденциях на рынке, или о появляющихся новых конкурентах.

Когда в бизнесе застой или спад, задачи и функции конкурентной разведки несколько видоизменяются. Продолжая заниматься по существу теми же вопросами - поиском и анализом негатива - КР должна делать упор на выявление в этом негативе крупниц положительных возможностей, обнадеживающих перспектив. То, что предлагает Кеннет Савка, представляется весьма диалектичным и психологически мотивированным подходом. Он полагает, что приносить плохие вести руководству компании, переживающей трудные времена, нецелесообразно. В каждом факте и явлении, безусловно негативном на первый взгляд, можно найти и обнадеживающие элементы. Так, например, спад на рынке недвижимости позволяет удешевить строительство нового предприятия. Рост безработицы помогает пополнить команду талантливыми сотрудниками. Даже падение спроса на услуги\товары компании не должно сильно огорчать, поскольку предоставляет возможность ослабить традиционных конкурентов, во всяком случае гарантирует от появления на этом поле новых игроков.

Именно так, считает Савка, должны строиться приоритеты КР, иллюстрируя выводы на примерах своей работы с клиентами из химической промышленности.

(Желающие получить полный текст статьи американского эксперта, обращайтесь в редакцию "Бизнес-разведки")

ЧТО МЕШАЕТ РАЗВИТИЮ ДЕЛОВОЙ РАЗВЕДКИ В РОССИИ

Деловая разведка - цели и задачи

ЧТО МЕШАЕТ РАЗВИТИЮ ДЕЛОВОЙ РАЗВЕДКИ В РОССИИ

Беседа с Генеральным директором компании «Амулет» А. Крыловым

1991 год. Пресса впервые открыто пишет об организованной преступности, о мафиозных структурах. Молодые начинающие банкиры обеспокоены. Они обращаются за консультациями к группе работников МВД с предложением разработать концепцию безопасности банковского бизнеса. Просьба выполняется, и на таком высоком уровне, что заказчик - новорожденная Ассоциация российских банков - предлагает разработчикам покинуть насиженные министерские кресла и организовать частную компанию, которая бы занималась различными аспектами безопасности, в том числе информационной, банковского бизнеса.

Так в конце 1991 года появилась на свет компания «Амулет», позиционирующая себя как универсальное предприятие, которое проводит аудиты безопасности и криминологические экспертизы инвестиционных проектов, обеспечивает юридическое сопровождение дел клиентов, осуществляет охрану бизнеса и личную охрану. Начав с обслуживания российских и зарубежных банков, «Амулет» к сегодняшнему дню имеет обширную клиентуру в различных отраслях экономики. Охранно-розыскные и юридические функции сочетаются с информационным бизнесом, где кампания занимает далеко не последнее место в России.

Об этом, последнем направлении и зашел разговор с Генеральным директором «Амuleта» **Александром Сергеевичем Крыловым**.

Мой первый к нему вопрос касается той настороженности, с которым воспринимаются в нашем бизнесе термины «деловая разведка», «конкурентная разведка», получившие на Западе не только легальную прописку, но и

динамичное развитие в качестве важнейшего компонента современного предпринимательства.

«Проблема здесь упирается прежде всего в существующие правовые нормы», - считает А. Крылов. «Законодатель воспринимает оперативно-розыскную деятельность как исключительно прерогативу государства, которую оно не хочет передоверить частным лицам и компаниям. При этом сложилась парадоксальная ситуация. Формально возможности любого рядового гражданина собирать и анализировать информацию намного шире, чем у лицензированного агентства или частного детектива. Государственная лицензия налагает ограничения, суживающие правовое поле деятельности тех, кто профессионально занимается экономическими расследованиями. Здесь отражается нынешний, специфический этап развития российского рынка и общественного сознания, которое всегда отстает от изменения экономических условий. Перескочить его, сразу шагнуть в новое мышление, невозможно. Мы вынуждены работать в условиях разрыва между растущим спросом на деловую разведку и отсутствием соответствующей законодательной базы. Те, кто занимается сегодня в России деловой разведкой, вынуждены лавировать в этом разрыве, и потому настороженно относятся к вопросам идентификации их деятельности в терминах, устоявшихся за рубежом.

Выходит, деловую разведку загоняют в подковёрную ситуацию?

Так оно и есть. А что делается под ковром, то плохо контролируется. И здесь кроется главный вред для государства и для деловой разведки.

Государство относится к деловой разведке частных компаний настороженно, если не сказать негативно. Поэтому бизнес разведка развивается в России полулегально - я имею в виду прежде всего источники и способы добывания информации.

Речь идет об информации в открытом доступе?

С точки зрения существующего российского законодательства провести границу между открытыми и закрытыми источниками информации очень трудно. Многие формально закрытые данные государственных структур не без причастности коррумпированных чиновников попали на рынок. Любой может пойти на рынок и приобрести по сходной цене служебные базы данных.

Коррупцию в этом деле порождает неоправданная закрытость многих видов информации. Вместе с Ассоциацией российских банков давно добиваемся доступа к официальной информации о мошенниках, действующих в банковской сфере. Ведь это, как правило, одни и те же лица. Попытки безрезультатны.

Что нам удалось сделать, так это наладить обмен такой информацией в рамках

Ассоциации, между службами безопасности банков. Но огромный массив информации, которым, полагаю, должны обладать правоохранные органы, остается для нас недоступным.

Какую конкретно информацию Вы имеете в виду?

Это данные о мошенниках. Это статистические данные, позволяющие выявлять тенденции в деятельности преступников по регионам, во временном измерении.

Наконец, мощный массив регистрационной информации, который никак не может быть закрытым. Например, финансовые балансы компаний, являющиеся визитной карточкой хозяйствующего объекта.

Отсутствием механизма официального доступа пользуются коррумпированные чиновники, готовые предоставлять информацию за приличную мзду. В итоге информация, которая по характеру должна быть открытой, приобретает природу "серой", "черной".

Закрытость информации дает не только материальные, но и политические выгоды ее держателям.

Верно. Существующая практика добывания полулегальными методами служебной информации используется для политического давления. Если ты стал негоден властям, они найдут возможности навредить. Скажем, изъять из компьютеров информацию под предлогом нелегального приобретения. Причем ссылки на Интернет источники по непонятным причинам во внимание не принимаются.

В общем, заниматься информационным бизнесом в нашей стране так же сложно и рискованно, как и другими видами предпринимательства.

Думаю, даже сложнее. К тому же в нынешних российских условиях информационный бизнес не прокормит. Он убыточен, и развивается в пакете с другими видами деятельности, чаще всего в комплексе услуг по безопасности.

Подавляющее большинство компаний, работающих в этой сфере, пока полагается главным образом на охранные функции. Если на Западе охранный персонал малопrestiжна, находится на задворках, то в России специфика нынешней российской ситуации предъявляет повышенные требования к безопасности бизнеса. В этом одно из важных отличий российских компаний от зарубежных. Крупные западные фирмы на плохо организованном российском рынке работают по-другому. Их информационные подразделения и службы безопасности не так заметны, как у российских предпринимателей. Не потому, что их бизнес менее рискованный. Условия - то одни. Просто внутренняя технология и организация бизнеса точно и ясно прописана.

Означает ли это, что Россия и здесь идет своим особым путем?

Та классическая бизнес разведка, которая сложилась и развивается сегодня в западном бизнесе, в России пока не созрела. Она только зарождается в ограниченном кругу продвинутых компаний, стремящихся овладеть современными методами информационно-поисковой и аналитической работы. Но будущее не за охранными функциями, которые на Западе занимают подчиненное, малозаметное место. Будущее за информационными технологиями деловой разведки. И к этому надо сегодня готовиться.

Как готовится к светлому будущему «Амулет»?

Мы вкладывали и продолжаем вкладывать в развитие информационно-аналитического направления нашей компании немалые средства.

Прибыли пока она не дает. Работаем на перспективу, считая, что сбор и анализ рыночной информации, экономическое прогнозирование - наиболее эффективный и перспективный инструмент, который рано или поздно будет преобладать в нашей деятельности.

Некоторые подвижки есть. Еще вчера аналитика и прогнозы не пользовались большим спросом у наших клиентов. Последние обычно интересовались статичной информацией о потенциальном партнере – кто учредители, опыт работы и т.п.

Но сегодня у российских предпринимателей пробуждается понимание, что без глубокого анализа происходящих на рынке процессов, без прогноза его развития успешный бизнес скоро будет невозможен. И они приходят к нам с вопросами о потенциальных экономических и политических рисках, о перспективах территориального и профильного расширения бизнеса.

Аналитика и прогнозы требуют специальной подготовки и высокой квалификации. Получая заказ на сложное исследование, вы используете собственные кадры

или прибегаете к услугам аналитиков со стороны?

У нас была альтернатива - или пригласить дорогостоящего специалиста со стороны, или вкладываться в подготовку своих сотрудников. Мы остановились на втором варианте. Во-первых, специфика работы требует высокой степени доверия, которой безусловно пользуются проверенные стажом работы работники “Амулета”, впитавшие традиции и особенности нашей компании. Во-вторых, приглашать со стороны не всегда рентабельно, но всегда рискованно.

В-третьих, необходима слаженность во взаимодействии аналитиков с другими службами и подразделениями, а на создание команды, где каждый понимает другого с полуслова, уходит много времени. В “Амулете” команда сложилась.

Поэтому мы и выбрали путь постепенного выращивания собственных профессиональных кадров бизнес разведки.

То же самое можно сказать и об информационных продуктах. В работе с клиентом опираемся, как правило, на собственные информационные базы. В их развитие вкладываем деньги. Дело не только в том, что пользование чужими платными ресурсами стоит дорого. Собственное программное обеспечение отвечает фирменному стилю «Амулета». Плюс уверенность в сохранении конфиденциальности. Потихоньку развиваем свои ресурсы, которых хватает на информационное обслуживание клиента в рамках проекта, где информация является одной из составляющих, зачастую не самой главной.

Несмотря на некоторое оживление спроса, мы по-прежнему испытываем дефицит заказов на сложные аналитические, прогностические исследования. В то же время перегружены рутинной, черновой информационной работой, которая не требует высочайшей квалификации, но позволяет компании выживать и развиваться в остроконкурентной среде.

Не сомневаюсь, что вы отслеживаете коллег по бизнесу, ведете конкурентную разведку «для себя» .

Эту работу мы ведем постоянно. Сравниваем наши возможности с возможностями аналогичных фирм. Анализ подсказывает, что источники информации у нас и у них по сути одни и те же. Мы высоко оцениваем профессиональный уровень аналитической работы коллег, умение готовить отчеты, вплоть до таких нюансов как язык и стиль. Следим и стараемся перенимать все лучшее, во всяком случае, не отставать.

Желаю Вам удачи и процветания.

Беседовал и готовил интервью В. Светозаров

ЧТО МЕШАЕТ РАЗВИТИЮ ДЕЛОВОЙ РАЗВЕДКИ В РОССИИ

Деловая разведка - цели и задачи

ЧТО МЕШАЕТ РАЗВИТИЮ ДЕЛОВОЙ РАЗВЕДКИ В РОССИИ

Беседа с Генеральным директором компании «Амулет» А. Крыловым

1991 год. Пресса впервые открыто пишет об организованной преступности, о мафиозных структурах. Молодые начинающие банкиры обеспокоены. Они обращаются за консультациями к группе работников МВД с предложением разработать концепцию безопасности банковского бизнеса. Просьба выполняется, и на таком высоком уровне, что заказчик – новорожденная Ассоциация российских банков – предлагает разработчикам покинуть насиженные министерские кресла и организовать частную компанию, которая бы занималась различными аспектами безопасности, в том числе информационной, банковского бизнеса.

Так в конце 1991 года появилась на свет компания «Амулет», позиционирующая себя как универсальное предприятие, которое проводит аудиты безопасности и криминологические экспертизы инвестиционных проектов, обеспечивает юридическое сопровождение дел клиентов, осуществляет охрану бизнеса и личную охрану. Начав с обслуживания российских и зарубежных банков, «Амулет» к сегодняшнему дню имеет обширную клиентуру в различных отраслях экономики. Охранно-розыскные и юридические функции сочетаются с информационным бизнесом, где кампания занимает далеко не последнее место в России.

Об этом, последнем направлении и зашел разговор с Генеральным директором «Амuleта» **Александром Сергеевичем Крыловым**.

Мой первый к нему вопрос касается той настороженности, с которой воспринимаются в нашем бизнесе термины «деловая разведка», «конкурентная разведка», получившие на Западе не только легальную прописку, но и

динамичное развитие в качестве важнейшего компонента современного предпринимательства.

«Проблема здесь упирается прежде всего в существующие правовые нормы», - считает А. Крылов. «Законодатель воспринимает оперативно-розыскную деятельность как исключительно прерогативу государства, которую оно не хочет передоверить частным лицам и компаниям. При этом сложилась парадоксальная ситуация. Формально возможности любого рядового гражданина собирать и анализировать информацию намного шире, чем у лицензированного агентства или частного детектива. Государственная лицензия налагает ограничения, суживающие правовое поле деятельности тех, кто профессионально занимается экономическими расследованиями. Здесь отражается нынешний, специфический этап развития российского рынка и

общественного сознания, которое всегда отстает от изменения экономических условий. Перескочить его, сразу шагнуть в новое мышление, невозможно. Мы вынуждены работать в условиях разрыва между растущим спросом на деловую разведку и отсутствием соответствующей законодательной базы. Те, кто занимается сегодня в России деловой разведкой, вынуждены лавировать в этом разрыве, и потому настороженно относятся к вопросам идентификации их деятельности в терминах, устоявшихся за рубежом.

Выходит, деловую разведку загоняют в подковерную ситуацию?

Так оно и есть. А что делается под ковром, то плохо контролируется. И здесь кроется главный вред для государства и для деловой разведки.

Государство относится к деловой разведке частных компаний настороженно, если не сказать негативно. Поэтому бизнес разведка развивается в России полулегально - я имею в виду прежде всего источники и способы добывания информации.

Речь идет об информации в открытом доступе?

С точки зрения существующего российского законодательства провести границу между открытыми и закрытыми источниками информации очень трудно. Многие формально закрытые данные государственных структур не без причастности коррумпированных чиновников попали на рынок. Любой может пойти на рынок и приобрести по сходной цене служебные базы данных.

Коррупцию в этом деле порождает неоправданная закрытость многих видов информации. Вместе с Ассоциацией российских банков давно добиваемся доступа к официальной информации о мошенниках, действующих в банковской сфере. Ведь это, как правило, одни и те же лица. Попытки безрезультатны.

Что нам удалось сделать, так это наладить обмен такой информацией в рамках Ассоциации, между службами безопасности банков. Но огромный массив информации, которым, полагаю, должны обладать правоохранительные органы, остается для нас недоступным.

Какую конкретно информацию Вы имеете в виду?

Это данные о мошенниках. Это статистические данные, позволяющие выявлять тенденции в деятельности преступников по регионам, во временном измерении.

Наконец, мощный массив регистрационной информации, который никак не может быть закрытым. Например, финансовые балансы компаний, являющиеся визитной карточкой хозяйствующего объекта.

Отсутствием механизма официального доступа пользуются коррумпированные чиновники, готовые предоставлять информацию за приличную мзду. В итоге информация, которая по характеру должна быть открытой, приобретает природу "серой", "черной".

Закрытость информации дает не только материальные, но и политические выгоды ее держателям.

Верно. Существующая практика добывания полулегальными методами служебной информации используется для политического давления. Если ты стал негоден властям, они найдут возможности навредить. Скажем, изъять из компьютеров информацию под предлогом нелегального приобретения. Причем ссылки на Интернет источники по непонятным причинам во внимание не принимаются.

В общем, заниматься информационным бизнесом в нашей стране так же сложно и

рискованно, как и другими видами предпринимательства.

Думаю, даже сложнее. К тому же в нынешних российских условиях информационный бизнес не прокормит. Он убыточен, и развивается в пакете с другими видами деятельности, чаще всего в комплексе услуг по безопасности.

Подавляющее большинство компаний, работающих в этой сфере, пока полагается главным образом на охранные функции. Если на Западе охранный бизнес малопrestiжна, находится на задворках, то в России специфика нынешней российской ситуации предъявляет повышенные требования к безопасности бизнеса. В этом одно из важных отличий российских компаний от зарубежных. Крупные западные фирмы на плохо организованном российском рынке работают по-другому. Их информационные подразделения и службы безопасности не так заметны, как у российских предпринимателей. Не потому, что их бизнес менее рискованный. Условия - то одни. Просто внутренняя технология и организация бизнеса точно и ясно прописана.

Означает ли это, что Россия и здесь идет своим особым путем?

Та классическая бизнес разведка, которая сложилась и развивается сегодня в западном бизнесе, в России пока не созрела. Она только зарождается в ограниченном кругу продвинутых компаний, стремящихся овладеть современными методами информационно-поисковой и аналитической работы. Но будущее не за охранными функциями, которые на Западе занимают подчиненное, малозаметное место. Будущее за информационными технологиями деловой разведки. И к этому надо сегодня готовиться.

Как готовится к светлому будущему «Амулет»?

Мы вкладывали и продолжаем вкладывать в развитие информационно-аналитического направления нашей компании немалые средства.

Прибыли пока она не дает. Работаем на перспективу, считая, что сбор и анализ рыночной информации, экономическое прогнозирование - наиболее эффективный и перспективный инструмент, который рано или поздно будет преобладать в нашей деятельности.

Некоторые подвижки есть. Еще вчера аналитика и прогнозы не пользовались большим спросом у наших клиентов. Последние обычно интересовались статичной информацией о потенциальном партнере - кто учредители, опыт работы и т.п.

Но сегодня у российских предпринимателей пробуждается понимание, что без глубокого анализа происходящих на рынке процессов, без прогноза его развития успешный бизнес скоро будет невозможен. И они приходят к нам с вопросами о потенциальных экономических и политических рисках, о перспективах территориального и профильного расширения бизнеса.

Аналитика и прогнозы требуют специальной подготовки и высокой квалификации. Получая заказ на сложное исследование, вы используете собственные кадры

или прибегаете к услугам аналитиков со стороны?

У нас была альтернатива - или пригласить дорогостоящего специалиста со стороны, или вкладываться в подготовку своих сотрудников. Мы остановились на втором варианте. Во-первых, специфика работы требует высокой степени доверия, которой безусловно пользуются проверенные стажом работы работники "Амулета", впитавшие традиции и особенности нашей компании. Во-вторых, приглашать со стороны не всегда рентабельно, но всегда рискованно.

В-третьих, необходима слаженность во взаимодействии аналитиков с другими службами и подразделениями, а на создание команды, где каждый понимает другого с полуслова,

уходит много времени. В “Амulette” команда сложилась.

Поэтому мы и выбрали путь постепенного выращивания собственных профессиональных кадров бизнес разведки.

То же самое можно сказать и об информационных продуктах. В работе с клиентом опираемся, как правило, на собственные информационные базы. В их развитие вкладываем деньги. Дело не только в том, что пользование чужими платными ресурсами стоит дорого. Собственное программное обеспечение отвечает фирменному стилю «Амulette». Плюс уверенность в сохранении конфиденциальности. Потихоньку развиваем свои ресурсы, которых хватает на информационное обслуживание клиента в рамках проекта, где информация является одной из составляющих, зачастую не самой главной.

Несмотря на некоторое оживление спроса, мы по-прежнему испытываем дефицит заказов на сложные аналитические, прогностические исследования. В то же время перегружены рутинной, черновой информационной работой, которая не требует высочайшей квалификации, но позволяет компании выживать и развиваться в остроконкурентной среде.

Не сомневаюсь, что вы отслеживаете коллег по бизнесу, ведете конкурентную разведку «для себя» .

Эту работу мы ведем постоянно. Сравниваем наши возможности с возможностями аналогичных фирм. Анализ подсказывает, что источники информации у нас и у них по сути одни и те же. Мы высоко оцениваем профессиональный уровень аналитической работы коллег, умение готовить отчеты, вплоть до таких нюансов как язык и стиль. Следим и стараемся перенимать все лучшее, во всяком случае, не отставать.

Желаю Вам удачи и процветания.

Беседовал и готовил интервью В. Светозаров

Понять культуру поведения клиента

Организация деловой разведки

Понять культуру поведения клиента

Профессионалам конкурентной разведки важно уметь взглянуть на проблему глазами клиента. Для этого необходимо проникнуть во внутреннюю культуру клиента. Если использовать антропологические термины и методологию, необходимо распознать свойственные для него символы, деловой стиль, ритуалы, присущие ему мифы. Это позволяет понять, какая именно информация интересует клиента, интегрировать некоторые из индивидуальных ценностей клиента в осуществление проекта, говорить с ним на одном языке и в обстановке полного доверия.

Символы. Они включают язык (используемые термины и названия), действия, истинный смысл которых понятен тем, кто включен в данную культуру. В этом смысле важно посмотреть, какой офис у клиента, какие картины висят на стене и что они означают для служащих компании, какие особые слова любит использовать клиент и какие действия под ними подразумеваются,

Деловой стиль. Необходимо понять отношение клиента к переговорам и совещаниям. Насколько они важны в его работе. Что он предпочитает - вести переговоры по телефону, по электронной почте, с глазу на глаз, вместе с коллегами. Как он ведет себя - сдержанно и формально, или расположен к неформальному стилю.

Мифы. Речь идет об отношении клиента к окружающим или историческим персонажам. Кто ему нравится и почему. Знание этого помогает войти в доверие к клиенту. Здесь уместно выяснить, каких людей в команде он выдвигает, кто учредители\владельцы компании и как клиент к ним относится. И т.д.

Суммирование вышеперечисленных наблюдений способствует формированию правильной стратегии и тактики работы с клиентом

Электронный бизнес: как сделать виртуального посетителя реальным покупателем

Как организовать деловую разведку

Электронный бизнес: как сделать виртуального посетителя реальным покупателем

Знание в деталях, кто посещает коммерческий веб-сайт, имеет исключительное значение в искусстве превращения случайного посетителя в регулярного пользователя информации сайта, пользователя – в покупателя рекламируемой продукции, и, наконец, – в устойчивого, долгосрочного клиента.

Интернет гигантски расширил потенциальную клиентуру по сравнению с традиционными методами рекламы и торговли, но имеет один существенный изъян: оставляет анонимными большинство посетителей виртуального магазина или офиса. Как их распознавать? Эта проблема становится ключевой для бизнеса в современных условиях, когда редкое предприятие не имеет представительства в Интернет Сети. Джорджия Стил, автор публикации в журнале "Mortgage Technology" (август 2001), исследует некоторые новые программные продукты, созданные для решения этой проблемы.

Среди них неплохо зарекомендовали себя интернет-платформа CommerceTrend VRM Platform, предлагаемая компанией Web Trends, которая расположена в Портленде. Программа позволяет собирать с сайта данные об интересах, предпочтениях и поведении посетителей. Помимо функции мониторинга и анализа движения на сайте, платформа обладает способностью систематизировать данные для маркетинговых отчетов, находить нужную информацию в хранилищах и онлайн-информационных системах, помогать в проведении рекламных кампаний, персонализировать полученную информацию. И все это делать на основе мониторинга сайта.

В статье отмечается, что применение данной платформы позволяет достигать наивысшего результата в сочетании с маркетинговым продуктом Data Conduit, выпускаемом компанией Siebel eBusiness Applications. Здесь удачно комбинируются возможности отслеживания веб-посетителей с проведением маркетинговых кампаний. По словам автора, благодаря получаемой детальной информации о посетителях, включая данные об их платежеспособности, о их особом интересе к тем или иным товарам, о просматриваемых

ими страницах и затрачиваемом для этого времени, достигается высокая степень взаимодействия с потенциальными и состоявшимися клиентами.

Завлекать посетителей и превращать их в клиентов - процесс не простой. Он начинается с попыток привлечь внимание пользователей Интернета к веб-сайту. Следующий этап: дать посетителям нужную информацию, обогатить и заинтересовать их, предлагая специальные услуги, предоставляя льготы, тем самым завоевать его доверие и превратить в покупателя, причем не в разового, а в постоянного, можно сказать "пожизненного" клиента.

Как делать внутренний бюллетень конкурентной разведки

Методы деловой разведки

Как делать внутренний бюллетень конкурентной разведки

Рекомендации на этот счет излагаются в июньском номере журнала Competitive Intelligence Magazine за этот год.

Автор статьи - Дейл Феринджер, вице-президент по маркетинговой разведке компании Visa International (Сан-Франциско), делится опытом издания внутреннего бюллетеня, посвященного анализу изменений на рынке и в первую очередь - действиям конкурентов. Начало было положено несколько лет назад выпуском закрытого месячного бюллетеня, предназначенного всего для нескольких лиц. Сегодня бюллетень получают более 400 сотрудников компании. Он стал необходимой частью всей системы конкурентной разведки Visa International.

Вот некоторые из рекомендаций Феринджера для тех, кто выпускает либо планирует выпускать подобное издание в своей фирме.

Превратите новости в исследование

Новости сами по себе не содержат достаточной информации для понимания происходящего и адекватной ответной реакции. Поэтому стремитесь обогатить известие, трансформировав его с помощью дополнительного материала в своего рода "историю" с выводами и предложениями. Источниками информации, дополняющими и детализирующими новость, могут служить публикации и веб-сайты (конкурентов), статьи в прессе, а также ваша внутренняя информация (аналитика, архивы и пр.). К примеру, сообщение, что конкурирующая фирма X планирует предложить свою продукцию новому сегменту потребителей. Важно к этому сообщению присовокупить точку зрения самого конкурента, мнение вашего аналитика, оценки независимых экспертов (по запросу либо из прессы). В результате может сложиться картина о перспективности/неперспективности данного шага. Подготавливаемый материал можно обогатить цитатами, статистикой, анализом общего бэкграунда, напоминанием об аналогичных действиях, предпринимавшихся какой-либо другой фирмой.

Старайтесь избегать использования конфиденциальной информации.

В крайнем случае, если руководство не возражает, сделайте соответствующую пометку, предупреждающую, что данный пассаж/страница/текст является конфиденциальным и не подлежит распространению.

Важно, чтобы бюллетень имел точный адресат внутри компании - вышший исполнительный менеджмент, информационно-аналитические службы, и т.д.

Время от времени выявляйте реакцию читателей, их отношение в целом к бюллетеню, к отдельным материалам. Это необходимо для корректировки, улучшения издания, превращения его в эффективный инструмент конкурентной разведки.

(Желающие получить полный текст статьи могут обратиться в редакцию)

Психология как один из инструментов конкурентной разведки

Методы деловой разведки

Психология как один из инструментов конкурентной разведки

Психология, изучающая характер и поведенческие особенности людей, может эффективно служить задачам конкурентной разведки, утверждает Черил Энн Уэллс в августовском выпуске журнала "Competitive Intelligence Magazine". По ее мнению, профессионалу конкурентной разведки полезно знать и применять методы психологов для познания поведения конкурентов - предпринимателей и в целом организаций - в контексте рыночной динамики.

Знание определенных поведенческих стереотипов, которыми обычно оперируют психологи, облегчают задачу изучения рыночного конкурента. Анализ "корпоративного типа (или характера)" особенно ценен сейчас, в эпоху глобализации и быстрых изменений в мировом бизнесе. Вторжение Интернет технологий усложняет и делает более разнообразными бизнес структуры и их взаимосвязи.

Автор рекомендует аналитикам конкурентной разведки пользоваться системой Meyers-Briggs Type Indicator, появившейся на свет в сороковых годах прошлого столетия. Типологический индикатор личностных профилей позволяет определять поведение в четырех психологических измерениях:

1. Экстраверсия и интроверсия.

Экстраверт открыт для общения, а интроверт, напротив, замкнут в себе.

2. Осмысление и интуиция.

Человек из первой категории склонен к системной работе и анализу, в то время как его антипод в большей степени полагается на интуицию.

3. Рассудок и чувства

Люди рассудка принимают решения, опираясь на логику и анализ объективных обстоятельств, а другие доверяют больше своим чувствам.

4. Суждение и непосредственное восприятие

По тому, как люди относятся к окружающему их миру, можно судить, насколько они в своих действиях полагаются на анализ или на непосредственные ощущения. Первые

предпочитают иметь хорошо организованные структуры для, а вторые склонны к импровизации и спонтанным шагам.

Эти характеристики верны как для отдельных личностей, играющих в бизнесе важную роль, так и для предприятий в целом. Они позволяют с той или иной точностью понять, насколько конкурентные компании готовы к кооперации и сотрудничеству. Анализ того, как конкуренты собирают и как работают с информацией, помогает установить, к чему они тяготеют - к хорошо продуманным и просчитанным решениям и шагам, либо к интуитивным решениям и действиям.

СОТРУДНИК ПРИХОДИТ В ФИРМУ. КАК ЕГО ПРОВЕРИТЬ?

Области применения деловой разведки

СОТРУДНИК ПРИХОДИТ В ФИРМУ. КАК ЕГО ПРОВЕРИТЬ?

Воровство и казнокрадство, к сожалению, в России не редкость. Не будем вспоминать изречения литературных классиков на этот счет. Они всем известны. Даже сталинский тотальный и жестокий контроль, когда за "три колоска" давали пять и больше лет лагерей, не искоренил до конца отечественную склонность к расхитительству. А фельетоны и карикатуры на "несунов" хрущевско-брежневского периода вообще не воспринимались как серьезный инструмент улучшения общественных нравов.

Многие привыкли считать, что непреодолимая тяга уносить с работы все, что плохо лежит и что можно «загнать» либо приспособить в домашнем хозяйстве, - нечто укорененное в русском характере, национальном менталитете, то, что отличает нас от европейцев и североамериканцев, особенно тех, кто воспитан в строгих правилах протестанской этики.

Поэтому несколько неожиданным для нашего читателя может показаться, что и на благополучном Западе проблема воровства на службе не только не решена, но, пожалуй, обостряется. Различные исследования, социологические опросы, в частности, проводимые SDR (?), свидетельствуют, что на фоне некоторого уменьшения случаев насилия пьянства и увлечения наркотиками на рабочих местах, число краж сотрудниками компаний возрастает. Служебное воровство - это непреходящая головная боль руководителей компаний практически всех отраслей американской экономики, за исключением, пожалуй, только сферы образования. Особенно оно характерно для бизнеса, связанного с розничными продажами, а также в фармацевтической промышленности.

Службы внутренней безопасности, имеющиеся на всех крупных и средних фирмах, как могут борются с этим явлением, ужесточая режим контроля за персоналом с помощью видеокамер, подслушивания телефонных разговоров, перехвата электронной корреспонденции, негласных обысков и т.п. Чаще всего эти меры не помогают.

По некоторым расчетам, ежегодный ущерб от злоупотреблений и преступлений, совершаемых персоналом американских компаний, составляет 400 миллиардов долларов. Это значительно превышает ущерб, наносимый хакерами и другими внешними криминальными субъектами. В числе главных причин, порождающих эту тенденцию, эксперты по занятости называют рекордно низкий уровень безработицы в США и бурное развитие технологий, за которым не поспевает рынок высококвалифицированного труда.

Чтобы уменьшить риск при найме новых работников, все большее число компаний использует различные процедуры проверки кандидата. Собственно, это не новый способ обезопасить компанию от сомнительных личностей. Характерной особенностью последних лет становится применение новейших информационных технологий в изучении персонального бэкграунда, а также обращение в специализированные фирмы, занимающиеся расследованиями, которые этими технологиями владеют. С использованием Интернет технологий время, затрачиваемое на проверку кандидата, включая просмотр онлайн-файлов криминальной статистики, заметно сократилось с нескольких недель до одного-двух дней. В настоящее время в семи американских штатах благодаря поддержке местных властей созданы онлайн-информационные системы проверки криминального бэкграунда, которыми широко пользуются расположенные там компании при найме на работу новых сотрудников.

Такая система действует, в частности, с мая 2001 года в штате Индиана. Она содержит базы данных полиции, которые отражают историю взаимоотношения каждого жителя штата с законом и властями, фиксируя все факты задержания, арестов, участия в уголовно наказуемых деяниях, решения судов и т.п. Ежегодно полиции штата Индиана приходится осуществлять свыше 200 тысяч таких проверок. С введением онлайн-информационно-поисковой системы процедуры упростились и ускорились. Любая компания может на нее подписаться. Стоимость подписки - \$50 плюс \$20 за каждый поиск. Для образовательных учреждений и некоммерческих организаций поиск осуществляется бесплатно.

Раньше каждый отдельный поиск занимал от недели до десяти дней. Многие компании такие сроки не устраивали, ибо приглянувшийся кандидат нередко находил за это время работу в другом месте. Теперь спрос на услуги резко возрос.

Социологические исследования показывают, что когда компании сами пытаются установить прошлое того или иного соискателя, ошибки их преследуют много чаще, чем в случаях обращения в специализированные организации. По американской статистике, более половины средних и крупных фирм США (с персоналом более 250 человек) прибегают к услугам сторонних специалистов.

Получают все более широкое распространение специальные программные продукты. Например, компания BrassRing Systems в кооперации с некоторыми другими фирмами выпускает интернет-решения, позволяющие в течение нескольких минут в онлайн-режиме осуществить проверку резюме, получить информацию, необходимую для принятия кадрового решения.

Надежность информации имеет первостепенное значение. Соискатель на рабочее место в компании проверяется не только с точки зрения его возможного криминального прошлого. Проверке подвергаются многие сведения, содержащиеся в представленном резюме. При этом выясняется, что очень часто резюме (примерно 30%) грешат неточностями. Например, завышается размер зарплаты на последнем месте работы. Или кандидат, набивая себе цену, приписывает образование, которого на деле не получал. Замалчиваются неприглядные факты, как, например, лишение водительских прав, штрафы за вождение в нетрезвом виде, и прочее. Все это подлежит проверке.

Стопроцентная надежность информационных систем по персоналиям сегодня не достижима. Отмечаются случаи, когда автоматизированный поиск путает однофамильцев, выдавая сведения, не имеющие отношения к проверяемой личности. В "черные списки" нередко попадают люди, задержанные полицией, но отпущенные либо оправданные по суду. Такие ошибки случаются, но никто не ставит под вопрос целесообразность использования онлайн-информационных систем при найме на работу или проверке служащих компании.

Разумеется, время от времени всплывает вопрос о правовых и этических границах вторжения в частную жизнь. Что касается уголовно наказуемых деяний, то в США и странах Западной Европы господствует мнение, что данные, касающиеся криминальной истории личности, не могут скрываться от общества. Общественность вправе знать

нарушителей закона. Сложнее дело обстоит с предоставлением сведений, не имеющих прямого отношения к служебной деятельности (алкоголь, наркотики, мелкое хулиганство, проблемы с дорожной полицией). Надо отметить, что подавляющее большинство предпринимателей правовой аспект не слишком заботит. Пользуясь услугами специализированных организаций, они получают лицензированную, легальную информацию. Но главное, что ставки очень высоки - кадровая ошибка, особенно при найме на ответственную должность, может очень дорого компании обойтись.

Информационное вторжение в личную жизнь соискателя не считается чем-то предосудительным топ менеджменту компаний, где практикуют мониторинг электронной почты и работы персонала в Интернет-сети, осмотр и обыск рабочих мест, и даже личных машин. Хотя такие методы в целом негативно сказываются на внутреннем климате, служащие крайне редко обращаются в суд с жалобой на неправомерные, на их взгляд, действия администрации.

Предприниматели, в свою очередь, не любят выпускать за пределы компании информацию о неблагоприятных поступках своих служащих. А это оборачивается тем, что уличенные в воровстве или других нехороших делах бывшие работники избегают попадать в "черные файлы" и благополучно устраиваются на другую работу.

Обзор по материалам зарубежной прессы подготовил В.Б.

ИНВЕСТИЦИОННЫЙ ИНТЕРЕС К РОССИИ РАСТЕТ

Информационные ресурсы деловой разведки

В. Борисов

ИНВЕСТИЦИОННЫЙ ИНТЕРЕС К РОССИИ РАСТЕТ

отмечают в международной консалтинговой компании KPMG

В 1870 году Уильям Барклай Пит основал в Лондоне бухгалтерскую фирму William Barclay Peat & Co.

Спустя 27 лет в Нью-Йорке возникла бухгалтерская фирма Marwick, Mitchel and Co. Ее основатели - Джеймс Марвик и Роджер Митчел.

Обе компании объединились в 1911 году. Так позднее появилась крупная международная компания по бухгалтерскому учету и консалтинговым услугам Peat Marwick International (PMI).

Во второй половине 20 столетия произошло объединение нескольких европейских фирм в одну - Klynveld Main Goerdeler (KPG).

Едва ли бы кто сегодня вспоминал об этих фактах давней и недавней истории, если бы в 1987 году не началось слияние PMI и KPG в одну компанию - KPMG.

Ныне KPMG - один из мировых лидеров финансового консалтинга. Отделения KPMG

открыты в десятках стран мира, включая ряд независимых государств на территории бывшего Советского Союза. Представительство компании в России было открыто еще до распада СССР, а в 1992 преобразовано в российскую аудиторскую фирму ЗАО «КПМГ», где работают более 600, в основном российских специалистов.

КПМГ заняла прочное место среди ведущих консалтинговых компаний в России, рассказывает заместитель директора Отдела консалтинга **Алексей Бурлацкий**. «В предлагаемые нами услуги входят исследования, связанные с оценкой бизнеса и его перспективами. Такие исследования необходимы при принятии стратегических решений о наращивании активов, создании холдингов, других крупных шагах по развитию предпринимательства. Здесь и оценка стоимости бизнеса, и замеры эффективности управления, и анализ информационного обеспечения.

Работая с инвестиционными проектами, мы прежде всего уделяем внимание изучению рынка, присутствующих на нем компаний – потенциальных партнеров и конкурентов, анализу каналов реализации продукции или услуг, то есть всему, на чем строится стратегия вхождения в новый рынок или расширения».

Среди клиентов КПМГ, потенциальных инвесторов, преобладают зарубежные фирм. Партнер компании **Ричард Гласспул** убежден в инвестиционной привлекательности российской экономики: «после спада, последовавшего за финансовым кризисом 1998 года, вновь повышается внимание международных инвесторов к России. Интерес проявляют прежде всего европейские компании. Наиболее активны немецкие бизнесмены, готовые вкладывать хорошие деньги в приобретение российских предприятий, в новые деловые проекты. Это весьма позитивный знак. КПМГ интенсивно работает с международными инвесторами, помогая им определить потенциальные объекты для приобретений, найти надежных российских партнеров для совместной деятельности. И главной предпосылкой правильного выбора, хорошо просчитанного решения является наличие точной информации, дающей неискаженную картину ситуации на рынке»

По мнению **Гласспула**, революционные изменения в информационных технологиях преобразили современный бизнес: «Судьба любого бизнес-проекта в определяющей степени зависит от объема и точности информации. Получить ее, как правило, нелегко. Но тот, кому это удастся, получает существенные конкурентные преимущества. Отсюда – возрастающее значение информационно-поисковой и аналитической работы. В ней испытывают огромную потребность международные корпорации, присматривающиеся к российскому рынку. Она объективно нужна и российским компаниям, особенно тем, которые расширяют свой бизнес в России и за рубежом. КПМГ предоставляет информационно-консалтинговые услуги и тем, и другим.»

В принципе нетрудно догадаться, какую информацию по России хотят получать иностранные инвесторы. А что отличает информационные запросы российских клиентов КПМГ? «Российских предпринимателей в первую очередь интересуют экспортные возможности, - говорит **Ричард**. - Но не только. Нас нередко просят помочь в изучении зарубежного опыта успешного бизнеса. Другая популярная услуга, оказываемая КПМГ российским клиентам – “benchmarking”, сопоставление, сравнительный анализ деятельности аналогичных российским иностранным компаний с целью выявления, в чем наши клиенты отстают от зарубежных коллег, в чем их слабости, что надо делать для улучшения бизнеса. Но в любом случае клиентам нужна выверенная, максимально детальная информация о том, что происходит в интересующем их секторе. Какие компании здесь присутствуют. Кто основные потребители. Какие банки связаны с данной отраслью. Степень надежности последних. И так далее. Причем необходимо знать не только текущее состояние, но и предысторию развития этого бизнеса, и его перспективы».

Маркетинговые исследования – анализ конкретных продуктов и рынков (динамика цен, объемы, брэнды, потребители, процедуры и регламент, история и прогнозы) - в последнее время стали очень популярными среди российских бизнесменов, отмечает **Алексей Бурлацкий**: «Особенно их интересуют экспортные возможности в страны СНГ и дальнего зарубежья. Такие исследования мы часто предпринимает совместно с маркетинговыми

фирмами, специализирующимися в одной или нескольких отдельных областях. Мы вместе осуществляем сбор и первоначальный анализ рыночной информации. Затем проводим углубленное исследование, содержащее не только выводы, но самое главное и ценное для нашего клиента – четкие и конкретные рекомендации, программу практических действий».

Недавно в КПМГ завершили исследование рынка электроэнергетики в странах Северной Европы по заказу одной российской компании. Заказчика интересовала реальная ситуация на рынке – объемы, спрос, оптовые и розничные цены, пропускная способность сетей, а также процессы интеграции энергетических мощностей в этом регионе. Это исследование компания провела своими силами. Будучи глобальной компанией со множеством отделений во всех регионах мира, КПМГ способна обходиться экспертами, работающими в филиалах и дочерних фирмах, без привлечения специалистов со стороны. «Но, естественно, - подчеркивает **Бурлацкий**, - ни одно серьезное и сложное исследование не обходится без тщательного сбора и анализа всей доступной информации, в том числе в онлайн-базах данных».

Так и в данном конкретном случае использованы различные исследования и области электроэнергетики Европы, позволившие проследить изменения в этой отрасли за последние десятилетия по странам, по ценам и т.д. Это в первую очередь, документы Европейской Комиссии, материалы специализированных организаций, занимающихся этими проблемами. Много информации взято в Интернет Сети. Хотя такая отрасль мировой экономики как электроэнергетика весьма информативно насыщена и много материалов имеются в открытом бесплатном доступе, были приобретены дорогостоящие платные отчеты и обзоры.

Информационно-аналитической работой в КПМГ занимаются ряд структурных подразделений, прежде всего Отделы рынков (маркетинга) и управленческого консультирования.

Консультанты отвечают на запросы клиентов, опираясь обычно на оперативные базы данных. При фундаментальных запросах используются как специализированные подразделения в КПМГ – отделы налогов, корпоративных финансов, так и Центры накопления и использования передового опыта (Due Excellence?). В них хранятся данные, а также рекомендации и методологии работы. Центры строятся по отраслевому принципу: черная металлургия, автоиндустрия, нефтедобывающая промышленность и т.д., аккумулируя материалы по всему миру.

Другой важнейший ресурс - Knowledge World, хранилище данных по деятельности компании. Сюда стекается информация о всех запросах и выполненных проектах, что составляет важную и обязательную часть работы сотрудников КПМГ. Информация о наработанных методологиях может быть использована в других проектах и регионах.

Когда возникает необходимость, а она возникает часто, мобилизуются внешние ресурсы. В России это, в первую очередь, статистические и регистрационные учреждения. При этом весьма ощутим дефицит выверенной, подробной информации.

«Управление знаниями (Knowledge Management) развито в России очень слабо» - подчеркивает **Р.Гласспул**: Отсутствуют общенациональные и региональные информационные системы, содержащие точные и детальные данные, в которых нуждается бизнес, да и общество в целом. В этой связи хочу отметить совместный проект с российским фондом «Правовая реформа», цель которого - формирование крупнейшего в стране депозитария данных о федеральном и региональных законодательствах, другой правовой информации. Создание такого хранилища баз данных, доступного всем, кто в нем нуждается - бизнесменам, правоведам, судьям и экспертам, поможет улучшить инвестиционный климат в России, в целом будет служить построению гражданского общества. Но это дело будущего»

СОТРУДНИК УВОЛЬНЯЕТСЯ. КАК ЗАЩИТИТЬ СЛУЖЕБНУЮ ИНФОРМАЦИЮ?

Информационная безопасность

В. Борисов

СОТРУДНИК УВОЛЬНЯЕТСЯ. КАК ЗАЩИТИТЬ СЛУЖЕБНУЮ ИНФОРМАЦИЮ?

В стародавние времена мастера умели хранить свои секреты, держа их в голове и нередко унося с собой в могилу. Для хранения чертежей, рецептов, описаний технологических процессов использовались массивные сейфы, потайные места, добраться до которых стоило немалого труда, а то и жизни.

С появлением компьютеров, и особенно развитием информатики, все кардинально изменилось. Практически вся секретная и конфиденциальная внутриведомственная информация, в том числе технологическая, хранится в памяти компьютеров и как правило доступна достаточно большому кругу специалистов высокой квалификации, работающих в компании. Парадокс вот в чем: информационные технологии обеспечивают конкурентные преимущества и в то же время увеличивают риск их утратить. Последнее нередко происходит, когда сотрудник компании, обладающий доступом к закрытой внутренней информации, переходит работать в конкурирующую фирму.

Что в таких случаях делать?

Для начала уясним, что такое "коммерческая тайна". Под этим обычно понимается интеллектуальная собственность. Она может охраняться законом в качестве торговой марки, патента, авторских прав. Правовая защита может распространяться практически на любую коммерческую тайну, апример, на информацию о клиентах, о технологических и организационных процессах, и что особенно важно – на компьютерные программы и их содержимое.

К сожалению, в России немногие бизнесмены официально регистрируют права на фирменные компьютерные программы и тем самым многократно повышают риск кражи секретов, в том числе бывшими сотрудниками.

Это серьезная проблема не только для предпринимателей России, но и для бизнесменов в странах развитой рыночной экономики, где промышленный шпионаж ведется с использованием весьма изощренных способов.

Весьма распространенный метод - переманивание специалистов, не только в качестве "свежих мозгов", но и как носителей ценной информации о конкуренте. Такие действия формально не противоречат законодательствам. Напротив, свобода выбора - основополагающий принцип рынка труда. И в большинстве стран право на выбор при трудоустройстве закреплен законом.

Наилучшим методом если не предотвратить, то минимизировать риск утечки секретов с увольняющимся работником, считают большинство экспертов, - это правильно составить трудовой контракт, в соответствии с которым поступающий на работу сотрудник дает письменное обязательство не разглашать служебные тайны. Часто речь идет об отдельном документе между администрацией компании и нанимаемым работником - "договоре о неразглашении", или "соглашении о конфиденциальности".

Бредли Адлер, автор публикации "Защищают ли вас антиконкурентные контракты?" ("Workforce", декабрь 1999), предлагает во время собеседования с кандидатом на вакансию в вашей фирме всегда требовать копию трудового соглашения с последнего места работы. Если кандидат отказывается, то лучше не торопиться с его зачислением.

Дело в том, что претендент на рабочее место в вашей компании может быть связан определенными обязательствами перед менеджментом фирм, где он работал или продолжает работать, но не хочет эти обязательства раскрывать. Например, обязательством не работать по завершении контракта в конкурирующих компаниях в течение определенного срока и/или в обозначенных регионах.

Если такого рода контракты нарушаются и дело доходит до суда, то судьи обязаны рассмотреть и взвесить обоснованность зафиксированных в контракте формальных обязательств с точки зрения географии и срока их действия, правомерности в содержательном отношении, соотносительности с действующим законодательством и т.п. Как отмечает Адлер, обычно срок действия таких соглашений не превышает двух лет, а в "новой экономике" - одного года с момента увольнения.

Западные эксперты рекомендуют широко использовать систему регулярной меняющихся паролей на все базы данных и компьютерные программы, содержащие закрытую информацию, чтобы предупредить несанкционированный вход бывшего работника. В частных компаниях США практикуется немедленное изъятие всей служебной информации из компьютера покидающего фирму сотрудника, не дожидаясь последнего дня его работы, и/или изъятие соответствующего оборудования, принадлежащего компании.

СОТРУДНИК УВОЛЬНЯЕТСЯ. КАК ЗАЩИТИТЬ СЛУЖЕБНУЮ ИНФОРМАЦИЮ?

Информационная безопасность

В. Борисов

СОТРУДНИК УВОЛЬНЯЕТСЯ. КАК ЗАЩИТИТЬ СЛУЖЕБНУЮ ИНФОРМАЦИЮ?

В стародавние времена мастера умели хранить свои секреты, держа их в голове и нередко унося с собой в могилу. Для хранения чертежей, рецептов, описаний технологических процессов использовались массивные сейфы, потайные места, добраться до которых стоило немалого труда, а то и жизни.

С появлением компьютеров, и особенно развитием информатики, все кардинально изменилось. Практически вся секретная и конфиденциальная внутриведомственная информация, в том числе технологическая, хранится в памяти компьютеров и как правило доступна достаточно большому кругу специалистов высокой квалификации, работающих в компании. Парадокс вот в чем: информационные технологии обеспечивают конкурентные преимущества и в то же время увеличивают риск их утратить. Последнее нередко происходит, когда сотрудник компании, обладающий доступом к закрытой внутренней информации, переходит работать в конкурирующую фирму.

Что в таких случаях делать?

Для начала уясним, что такое "коммерческая тайна". Под этим обычно понимается

интеллектуальная собственность. Она может охраняться законом в качестве торговой марки, патента, авторских прав. Правовая защита может распространяться практически на любую коммерческую тайну, апример, на информацию о клиентах, о технологических и организационных процессах, и что особенно важно – на компьютерные программы и их содержимое.

К сожалению, в России немногие бизнесмены официально регистрируют права на фирменные компьютерные программы и тем самым многократно повышают риск кражи секретов, в том числе бывшими сотрудниками.

Это серьезная проблема не только для предпринимателей России, но и для бизнесменов в странах развитой рыночной экономики, где промышленный шпионаж ведется с использованием весьма изощренных способов.

Весьма распространенный метод - переманивание специалистов, не только в качестве "свежих мозгов", но и как носителей ценной информации о конкуренте. Такие действия формально не противоречат законодательствам. Напротив, свобода выбора - основополагающий принцип рынка труда. И в большинстве стран право на выбор при трудоустройстве закреплен законом.

Наилучшим методом если не предотвратить, то минимизировать риск утечки секретов с увольняющимся работником, считают большинство экспертов, - это правильно составить трудовой контракт, в соответствии с которым поступающий на работу сотрудник дает письменное обязательство не разглашать служебные тайны. Часто речь идет об отдельном документе между администрацией компании и нанимаемым работником - "договоре о неразглашении", или "соглашении о конфиденциальности".

Бредли Адлер, автор публикации "Защищают ли вас антиконкурентные контракты?" ("Workforce", декабрь 1999), предлагает во время собеседования с кандидатом на вакансию в вашей фирме всегда требовать копию трудового соглашения с последнего места работы. Если кандидат отказывается, то лучше не торопиться с его зачислением.

Дело в том, что претендент на рабочее место в вашей компании может быть связан определенными обязательствами перед менеджментом фирм, где он работал или продолжает работать, но не хочет эти обязательства раскрывать. Например, обязательством не работать по завершении контракта в конкурирующих компаниях в течение определенного срока и/или в обозначенных регионах.

Если такого рода контракты нарушаются и дело доходит до суда, то судьи обязаны рассмотреть и взвесить обоснованность зафиксированных в контракте формальных обязательств с точки зрения географии и срока их действия, правомерности в содержательном отношении, соотносительности с действующим законодательством и т.п. Как отмечает Адлер, обычно срок действия таких соглашений не превышает двух лет, а в "новой экономике" - одного года с момента увольнения.

Западные эксперты рекомендуют широко использовать систему регулярной меняющихся паролей на все базы данных и компьютерные программы, содержащие закрытую информацию, чтобы предупредить несанкционированный вход бывшего работника. В частных компаниях США практикуется немедленное изъятие всей служебной информации из компьютера покидающего фирму сотрудника, не дожидаясь последнего дня его работы, и/или изъятие соответствующего оборудования, принадлежащего компании.

Пять лет американского «Акта о промышленном шпионаже»

Борьба с промышленным шпионажем

Пять лет американского «Акта о промышленном шпионаже»

В октябре исполняется ровно 5 лет принятому Конгрессом США Акту об экономическом шпионаже. Юбилей отмечен громким судебным процессом по делу двух японских ученых, обвиняемых в краже закрытых исследовательских материалов в Кливлендском медицинско-биологическом центре (об этом наш журнал информировал читателей).

Может быть, и не стоило бы придавать этому процессу большого значения, если бы не одно любопытное обстоятельство. За пять лет существования упомянутого закона на его основании было возбуждено около 30 судебных дел. Все они связаны с акциями промышленного шпионажа в отношении американских организаций и компаний, предпринятыми в большинстве случаев американскими же частными лицами и фирмами. Между тем, Акт об экономическом шпионаже первоначально задумывался как закон, направленный в защиту американских корпораций от зарубежных конкурентов и государств. Но поскольку в таком виде он противоречил ряду международных торговыми соглашениям и конвенций, членом которых являются США, законопроект во время слушаний был дополнен положением о наказуемости промышленного шпионажа, кем бы он ни осуществлялся.

Кливлендское дело - первое за все время после принятия закона, где в качестве обвиняемой стороны выступает фактически зарубежное государство, поскольку оба японца являются штатными сотрудниками национальной научной организации, учрежденной и финансируемой японским правительством. (Уместно заметить, что хотя официальные власти Японии публично отмежевались от содеянного их гражданами, маловероятно, что похитители действовали на свой риск и страх).

То, что Акт призван в первую очередь защищать американский бизнес от зарубежных конкурентов, косвенно свидетельствуют предусмотренные им сроки наказания: до 15 лет в тех случаях, когда замешаны иностранцы, и до 10 лет - во всех других.

Согласно закону, его действие распространяется на защиту "коммерческих тайн", куда включают все основные виды интеллектуальной собственности: авторские права, патенты, торговые марки и т.п. Причем Акт признает правонарушением не только факт кражи интеллектуальной собственности, но и доказанное намерение это совершить.

Сейчас, когда современные информационные технологии придали мощный импульс развитию легального вида деятельности - конкурентной разведки, требуется различать тонкую границу, отделяющую секретную экономическую информацию от открытой, но самое главное и трудное - уметь обращаться с доступной деловой информацией и ее носителями. Связанных с американской наукой и бизнесом иностранцев здесь могут ждать неприятные сюрпризы.

Распространенный пример - найм на работу специалиста с опытом работы на американской фирме, знающего многое из того, что относится к конфиденциальной, служебной информации. Практическое ее использование, равно как и намерение использовать, вполне может трактоваться как нарушение Акта о промышленном шпионаже. Поэтому американские юристы советуют быть осмотрительными в найме на работу людей, активно рекламирующих свои познания в вопросах, затрагивающих чужую служебную тайну.

Точно так же требуется быть очень осторожным, заключая договор с консультантом, имевшим доступ к секретам американских компаний.

Работающим в США иностранным компаниям эксперты The Metropolitan Corporate Counselor рекомендуют:

- Во время собеседования с кандидатом на работу в вашей фирме предупредить его о необходимости следовать Акту о промышленном шпионаже, безотносительно, касается ли это ваших или чужих секретов. При этом беседу задокументировать.

- Проинформировать об этом компанию, где прежде работал ваш новый сотрудник.

- Следить, чтобы знания, принесенные в вашу компанию новым сотрудником и реализованные в ваших инновационных проектах не послужили поводом или причиной обвинения вашей компании в промышленном шпионаже.

Как минимум, рекомендуется иметь в компании официальный документ, декларирующий уважение норм и требований, вытекающих из Акта, а также провести соответствующую работу с персоналом. Это поможет если не выиграть судебное дело по иску конкурента, то по крайней мере смягчить наказание.

Статья подготовлена В.Борисовым по материалам американской прессы.

Безопасность информации: программа OPSEC (Operations Security)

Борьба с промышленным шпионажем

Безопасность информации: программа OPSEC (Operations Security)

Недавнее исследование, проведенное совместно Институтом компьютерной безопасности и ФБР, показало, что средний ущерб американских компаний от краж служебной информации составляет в среднем 1 млн. долларов. На это исследование ссылается журнал *Competitive Intelligence Magazine* в статье, посвященной проблеме обеспечения безопасности внутрифирменной служебной информации. Существует специальная программа безопасности информации, представляющая собой систематизированный свод рекомендаций, универсальный для любой фирмы независимо от ее размера или характера деятельности.

Конкретно предлагается осуществить последовательный ряд следующих шагов.

1. Проанализировать каждый документ, имеющий важное значение для компании, глазами профессионала конкурентной разведки конкурирующей компании. Обычно предприниматели держат в секрете свои маркетинговые планы, ценовую политику, стратегию расширения.

2. Просчитать возможный ущерб, который может нанести конкурент, получив в свое распоряжение эти материалы. Скажем, как бы повел себя конкурент, заблаговременно узнав о планах выпуска нового товара - попытался бы опередить своим продуктом, или пошел бы на существенное снижение цен?

3. Изучить наиболее вероятные пути и способы возможной утечки информации. Например, проверить, оставляют ли сотрудники на рабочих столах конфиденциальные документы, отправляясь на обед. Часто ли работники фирмы болтают по телефону с представителями исследовательских маркетинговых фирм. Имеют ли контрактники такой же доступ к компьютерной сети компании, как и штатные работники.

4. Разработать план контрмер.

5. Реализовать данный план. Например, убрать с сайта и других открытых источников информацию, которая может быть эффективно использована конкурентами. Настоятельно рекомендуется проводить с сотрудниками беседы, обращая внимание на уязвимые с этой точки зрения позиции компании. Призывы к бдительности в этом контексте будут весьма кстати.

Передовые информационные технологии для малого бизнеса

Новые технологии деловой разведки

Передовые информационные технологии для малого бизнеса

Принято считать, что новейшие программные разработки для бизнеса доступны только крупным и средним компаниям. Что это не так, хорошо показано в публикации американского издания «M2 Presswire» от 14 августа 2001 года, посвященной совместному проекту Minnesota Technology, Inc. , государственной организации по развитию промышленной технологии, и компанией Sopheon, крупным международным поставщиком программного обеспечения для управления знаниями (knowledge management), чей головной офис расположен в штате Миннесота.

Суть проекта - в предоставлении тысячам малых предприятий этого штата возможности пользоваться исследовательским Интернет порталом Telthec.com, который Sopheon приобрел через слияние с его разработчиком - Telthec Resource Network Corporation. По словам президента MTI Ж. Коппеля, “благодаря партнерству с Sopheon появилась возможность приобщить предприятия малого бизнеса к Интернет ресурсам, зарекомендовавшим себя как ценный инструмент конкурентной разведки, необходимой для успешного предпринимательства”.

Упомянутый портал предоставляет пользователям быстрый доступ к критически важной коммерческой и технологической информации.

Примеры практического использования портала:

- выявление новых рынков;
- сбор материалов, имеющих значение для конкурентной разведки;
- быстрое освоение новых технологий;
- анализ перспектив развития бизнеса;
- поиск и усвоение успешных новаций в области управления бизнесом;

- поиск информации о патентах и торговых марках;

- знакомство с экспертными оценками в 33 тысячах областях науки, технологии и бизнеса;

Портал размещен на сайте MTI www.minnesotatechnology.org

Интернет-технологии и работа с клиентами

Новые технологии деловой разведки

Интернет технологии и работа с клиентами

Интернет программы Управления связями с клиентами (Customer Relationship Management) стали на Западе весьма популярными. Ими пользуются подавляющее большинство международных и крупных национальных корпораций.

В отличие от традиционных видов маркетинга УСК не просто сфокусировано на изучении поведения и покупательских предпочтений клиентов фирм, но представляет довольно сложную систему взаимосвязи между продавцом и покупателем, где последнему принадлежит во многом решающая роль в определении характера этой взаимосвязи. Продавец не столько формирует покупательский спрос, сколько его прогнозирует, улавливает новые тенденции и подлаживается под них.

Согласно одному из многих определений УСК - это такой вид деятельности предприятия, благодаря которому можно идентифицировать, обретать, выбирать, "окучивать", удерживать и улучшать обслуживание клиентов (покупателей\пользователей). УСК позволяет связать потребности клиента с возможностями компании их удовлетворить.

Особенно широкое распространение УСК получило в "новой экономике". Это объясняется огромными, не до конца оцененными возможностями Интернет технологий собирать, хранить и анализировать мощный массив данных о поведении клиентов, о покупательских предпочтениях, используя как электронную почту, так и веб-сайты. При этом важно учитывать, что Интернет технологии служат обеим сторонам. Электронный бизнес характерен активным вторжением в него покупателя, который посредством компьютеров ведет поиск интересующих товаров\услуг и осуществляет выбор. Более того, Сеть предоставляет покупателям возможность публично высказывать мнение, обмениваться между собой информацией о качестве предлагаемых товаров\услуг. Таким образом, поставщики товаров и услуг утрачивают монополию на рыночные коммуникации.

В ситуации, когда у клиентов большой выбор, а конкуренция возрастает, многие продавцы начинают предлагать нечто большее, чем информацию о своих товарах. Речь идет о появлении онлайн-овых "клубов покупателей", где информация о продажах сопровождается или сочетается с информационными услугами широкого плана, но всегда связанными с данным товаром и привлекательными для постоянного или потенциального покупателя. Так, например, крупная британская компания по продажам продовольственных товаров и одежды, в том числе детской, Tesco разместила на своем сайте полезные советы по уходу за детьми, создала виртуальный клуб для матерей. При

этом членам клуба предоставляются скидки с продаж.

По мнению бывшего директора British Airways Ларри Хокмана, «клубы покупателей» - шаг к возникновению союзов покупателей, которые по влиянию на рынок, на экономику многократно превзойдут профсоюзы.

Новые тенденции в бизнесе, связанные с все более широким использованием информационных технологий, определяют возрастающий спрос на соответствующее программное обеспечение и продукты. И это несмотря на обвал в “новой экономике”, на кризисные явления в экономике США. На фоне общего спада расходов и инвестиций в сферу высоких технологий в целом, продажи программ деловой разведки для создания и управления хранилищами данных, а также специально предназначенных для управления связями с клиентами устойчиво растут. Так, в частности, мировые продажи продуктов компании SAS, используемых для УСК (SAS\Warehouse Administrator R), увеличились в 2000 год на 66%, прогноз на 2001 год - более 15%. Рост продаж только в США, переживающих экономические трудности, еще более впечатляющий (соответственно 87 и 66 процентов).

Исследования и социологические опросы, проводимые рядом западных центров изучения рынков и бизнеса, отчетливо показывают, что все больше предпринимателей осознают высокую эффективность программ деловой разведки в работе с клиентами. Во всяком случае в таблице приоритетов западных бизнесменов они занимают второе место, между Интернетом как таковым (1 место) и электронным бизнесом (3 место).

Обзор подготовлен В. Борисовым по материалам изданий “Business wire”, “PR Newswire”, “Sunday Business”.

Путешествие в невидимую Сеть

Методы деловой разведки

Путешествие в невидимую Сеть

Иногда встречаются определения “глубокий веб” или “невидимый веб”. Они означают колоссальный массив информации, недоступный для поисковых машин общего пользования, даже таких известных как Alta Vista и Yahoo.

По некоторым оценкам, “невидимая” часть информации в Сети превосходит “видимую” в 500 раз!

Почему и какая именно информация сегодня обычными методами не доступна?

Это информация, хранящаяся в базах данных. Информация на сайтах, где содержание страниц быстро меняется, как, например, на сайтах СМИ, где значительная часть информации просто не успевает быть индексируемой и уходит в базы данных глубокого залегания, не просматриваемые поисковыми механизмами.

Временной фактор играет важную роль. Пользователь общедоступных поисковых машин подобен астроному - он видит прошлое, ибо на экране его компьютера появляется лишь то,

что выло в Сети на момент последней индексации -процесса, всегда занимающего определенное время. Некоторые поисковые системы индексируют новостные сайты, но фактически снимают поверхностный слой информации на момент индексации.

Кроме того, содержимое многих файлов по тем или иным причинам закодировано в специальных форматах, осилить которые обычные машины не могут. Требуется особо настроенное программное обеспечение.

В настоящее время предпринимаются попытки создать программные продукты, ориентированные на поиск в “невидимой” части Всемирной Паутины непосредственно с компьютера пользователя. Среди недавних разработок заслуживают внимание Bullseys 2.0 и Copernic 2001. Как и другие аналогичные разработки, эти программные пакеты принимают поисковый запрос, посылают его на какое-то число сайтов с базами данных, осуществляют при помощи действующих там механизмов поиск и возвращают пользователю результат в консолидированной форме. Преимуществами названных продуктов является их способность осуществлять поиск, причем одномоментно, в разных тематических (новости, здоровье) и функциональных (книги, работа) зонах, а также ряд дополнительных функций, например, умение систематизировать и суммировать найденную информацию, которая обычно поступит к пользователю в виде разрозненных фрагментов. Другая отличительная особенность заключается в том, что пользователь может запрограммировать поиск, который будет осуществляться в автоматическом режиме в заданные промежутки времени. Эта их характеристика особенно важна для мониторинга конкурентов на рынке

Программа для конкурентной разведки в электронном бизнесе

Новые технологии деловой разведки

Программа для конкурентной разведки в электронном бизнесе

Новейшая программная разработка компании Compete Inc., расположенной в Бостоне, позволяет осуществлять сравнительный анализ работы коммерческих сайтов с посетителями и клиентами. По словам ее директора М.Дж. Сингха, сегодня нет необходимости прибегать к нечистоплотным приемам промышленного шпионажа, когда так много информации о конкурентах можно получить через мониторинг сайтов. Так, например, финансовая корпорация FleetBoston, используя соответствующее программное обеспечение, может рассчитать число потенциальных богатых клиентов, перехватываемых онлайн-брокерами. А, скажем, Bank of America обнаружит, что ее клиентура перетекает к Интернет брокерам, предлагающим онлайн-обслуживание банковских депозитов и счетов.

Руководители Compete планируют серьезно заняться консалтинговой деятельностью. К примеру, рекомендовать клиенту, работающему в электронном бизнесе, поднять на доллар расценки на рекламу, не рискуя потерять рекламодателей. Или советовать другому клиенту повысить цену на продаваемые видеомагнитофоны без риска сокращения продаж. Или предсказать вероятные тенденции в традиционной торговле грузовиками - нечто вроде того, что предвидится рост спроса на желтые автомобили Форда в Северной Каролине.

У разработанного Compete программного обеспечения есть и критики. Некоторые отрицают ее способность различать домашних пользователей персональными компьютерами. Другие считают неприемлемым для пользователей Интернета, что их провайдеры разрешают использовать информацию третьей стороной, в данном случае компанией Compete.

На эти замечания представители Compete и другой аналогичной компании

Plurimus уверяют, что снимаемая ими с сайтов информация безлична, она не персонифицирована и ничуть не угрожает правам личности.

В то же время, как заявляет Шейла Олива, менеджер по маркетингу из Plurimus, “реальный путь к познанию, как работает бизнес в Интернете, лежит через знание деталей. Данные о числе посетителей сайта мало о чем говорят”. Под “детальями” подразумевается информация о демографических характеристиках пользователей электронного бизнеса, их покупательских предпочтениях, маршрутах их путешествий по бесконечному Интернет пространству.

Стоит ли рисковать репутацией

Деловая разведка - цели и задачи

Стоит ли рисковать репутацией?

Фирма по продаже пиццы DiGiorno, входящая в компанию Kraft, подала в суд на конкурирующую фирму Schwan. Суть иска: фирма - ответчик

взяла на работу сотрудника маркетинговой компании AC Nielsen, располагающего важной экономической информацией о Kraft.

В другом эпизоде конкурент Kraft нанял расследователя, который, выдавая себя то за репортера, то за активиста-эколога, то за выпускника университета, пытался получить секретную информацию у сотрудников Kraft.

Эти примеры показывают, насколько могут быть уязвимы профессионалы деловой разведки, переступая правовые и этические границы своей деятельности, пишет Джон МакГональ, управляющий партнер компании The Helicon Group, в журнале Competitive Intelligence Magazine (Issue № 3, 2001).

В действительности, нет нужды рисковать. Ведь более 80 процентов необходимой информации можно найти в открытых источниках, и часто этого бывает достаточно для решения задачи. Так стоит ли рисковать репутацией, стремясь любой ценой получить недостающее? Вопрос звучит риторически.

Между тем, здесь немало путаницы. Часто конкурентную разведку смешивают с промышленным шпионажем.

По мнению МакГоналя, между ними отчетливо различимая граница. Промышленный шпионаж предполагает нарушение уголовного или гражданского кодекса и тем отличается от КР. Одно дело, когда вы пользуетесь открыто распространяемыми на выставке материалами, и другое - когда их выкрадывают из сейфов.

В то же время встречаются случаи, когда отделить КР от промышленного шпионажа не просто. Речь идет о действиях, которые формально не нарушают законы, но противоречат корпоративному кодексу этики.

Автор настаивает на необходимости внедрения и неукоснительного следования этическим стандартам, особенно в компаниях, занимающихся конкурентной разведкой. "Действия в рамках закона и этики - не только нравственный бизнес. Это прежде всего хороший бизнес"

(Желающие получить полный текст статьи могут обратиться в редакцию)

Десять наблюдений и рекомендаций по деловой разведке

Советы профессионалам деловой разведки

Десять наблюдений и рекомендаций по деловой разведке

("The Intelligence Edge: How to profit in the Information Age"

G. Friedman, M.Friedman, C.Chapman, J.S.Baker JR)

1. Найти человека, знающего важные секреты, нередко дороже самих секретов.
2. Удачливые бизнесмены - это прежде всего бережливые собиратели информации.
3. Всякий поиск должен иметь четко очерченную и ограниченную задачу. В противном случае вы утонете в море информации.
4. Никогда не беритесь за решение задачи, если заказчик отказывает в допуске к своим источникам информации.
5. Украдите идею у Майкрософта - и вас убьют. Украдите идею у профессора - и вас объявят ученым. Будьте готовы к кропотливому труду - надо "намыть" горы "руды", чтобы добыть ценную информацию.
6. Начинайте всегда с самой легкой задачи. Это часто помогает в решении трудной задачи.
7. Вы добьетесь расположения и помощи коллег, если сможете им внушить, что вы не чужак и зануда, если вы вежливы и даете понять, что рассчитываете на их помощь
8. Некоторые люди - прирожденные коллекционеры информации. Стремитесь их распознать и использовать.
9. Чем больше компания, тем сложнее работать с информацией. Вы не можете разделить ее с кем-то, о ком вы даже не слышали.
10. Интернет бесплатен только для тех, кому некуда девать время.