"Бизнес-разведка" № 16

круглый стол

"Деловая разведка против мошенничества:
проблемы координации "

4 февраля 2005г., X Международный Форум "Технологии безопасности",
Москва, Крокус-Сити.

Организаторы: Группа компаний "Амулет", журнал "Бизнес-разведка"

А.С. Крылов
Генеральный директор Службы безопасности "Амулет"

Баяндин Н.И.
профессор, Институт безопасности бизнеса МЭИ (ТУ)

Рыбин А.Н.
Директор Московского представительства банка "Эллипс банк"

Пилюгин П. Л.
Советник Генерального директора Специальной информационной службы

Лобанов С.Г.
Генеральный директор "Кронос-Инфо"

Кунбутаев Л.М.
Директор Института безопасности бизнеса МЭИ (ТУ)

Минзов А.С.
Зав кафедрой "Комплексная безопасность бизнеса" Института безопасности бизнеса МЭИ (ТУ)

Митрофанов А.
Группа компаний "МИГ" (безопасность бизнеса и консалтинг)

Кузнецов С.В.
Эксперт

Катышев М.В.
Председатель Правления некоммерческого партнерства "Российское общество профессионалов конкурентной разведки"

Куборский Г.В.
Эксперт

Горделян А.А.
Исполнительный директор некоммерческого партнерства "Российское общество профессионалов конкурентной разведки"

Попов В. В.
Информационно-консалтинговое бюро "ДеФакто"

Пучков С.И.
эксперт по экономической и информационной безопасности Балашихинской торгово-промышленной палаты

Доронин А.И.
автор книги "Бизнес-разведка"

16-Крылов

А.С. Крылов
Генеральный директор Службы безопасности "Амулет"

Мы с вами встречаемся уже не первый год. Ряды нашего цеха не растут бурно. Численность людей, проявляющих интерес к нашей тематике, более или менее устоялась. И я думаю, что это хорошо. Бизнес-разведка и деловая разведка это не те отрасли, которые требуют паблисити, широкого внимания журналистов. Во все времена и во всех странах наша деятельность предполагала определенную сдержанность.

В России формируется профессиональный цех. Не первый год мы с радостью замечаем, что использование терминов со словом "разведка" все менее пугает людей. Государственные ведомства, чиновники к нему начинают привыкать.

На наших встречах в последние годы постоянно присутствовала тема взаимодействия специалистов деловой разведки между собой и с государственными органами. Определенный опыт, накопленный за эти годы, говорит о взаимодействии внутри цеха как о состоявшемся явлении, как о факте.

В то же время не всем из нас взаимодействие с государством представляется нужным. Не по причине какой-то "фронды", а по причине характера нашей деятельности. К огромному сожалению, государство не научилось хранить вверенные ему секреты. Все базы данных, которые, как официально декларируется, должны охраняться как "зеница ока", на самом деле становятся доступными не только профессионалам конкурентной разведки, но и любому, даже малосостоятельному человеку. Конечно, это общая беда. И, тем не менее, мы живем в реальном мире, и если такая форма взаимодействия устраивает чиновников - не в нашей власти резко ее изменить. Не думаю, что это и наша задача, хотя повторю, что искренне сожалею, что такое положение сложилось.

Хочу далее остановиться на двух обстоятельствах, которые, по моему мнению, по сравнению с последними годами вносят определенный элемент новизны в нашу работу.

Первое. Это появление долгожданного закона о кредитных историях. В свое время к нам многие обращались с предложениями ускорить принятие такого закона, предлагались банки данных, в частности, Ассоциации российских банков. Но случилось так, что законодатели пошли по пути, проторенному другими странами. Выбрана либеральная модель работы кредитных бюро. Они никоим образом не заменяют нашу деятельность. Эти бюро будут оперировать исключительно переданными им на добровольной основе очень ограниченными объемами информации, примерно, по такой схеме: "заемщик Х получил такой-то кредит, дисциплина его возврата такова...". И ничего более того. Других комментариев закон "О кредитных историях" не предполагает. Конечно, он имеет большое значение для профилактики мошенничества, но это не то, с чем мы привыкли работать. Реально банкиры будут ощущать определенную неудовлетворенность. Во многих случаях им потребуется дополнительная информация. Прежде всего, информация о юридических лицах, поскольку даже успешная, но короткая кредитная история конкретного лица еще не является гарантией его безупречности в будущем. А что касается массового потребительского кредитования, которое, по некоторым оценкам охватило уже 30% трудоспособного населения страны, то здесь к нам будут обращаться в случае

всевозможных эксцессов, т.е. при не возврате кредитов. Подозреваю, что будет достаточно большой объем работы по механизму распределения кредитов - традиционно во всех странах нарушений в этом деле немало. Конкурентная борьба за заемщика уже сейчас развернулась. Таким образом, сам факт появления кредитных бюро не только не составит нам конкуренцию, но напротив, прибавит работы.

Второе обстоятельство, на которое есть смысл обратить внимание. Недавно "Альфа банк" отсудил у газеты "Коммерсант" многомиллионную (в долларах) сумму денег за публикацию, которая, по мнению банкиров, нанесла им существенный материальный вред. Это первый большой и яркий эпизод такого рода. На самом деле, у многих банков и предпринимателей давно чешутся руки заняться защитой своих интересов, чести и достоинства. И в этом смысле было важно создать судебный прецедент. А если принять во внимание, что наши суды не независимы, то такие судебные процессы могут стать инструментом конкурентной борьбы.

Причем основой для серьезных судебных исков могут быть не только газетные публикации. Надо признать, что нередко подготовленные нами и переданные клиентам информационно-аналитические материалы "утекают" на сторону, в том числе в СМИ и в Интернет. Хотя фирмы, занимающиеся бизнес-разведкой, не любят печатать свои исследования на фирменных бланках, в случае суда доказать авторство той или иной справки возможно. Боюсь, что уже в скором времени мы столкнемся с такого рода репрессиями. Причем некоторые чиновники с удовольствием попытаются "навести порядок" в наших рядах. Прокуратура, полагаю, будет с радостью помогать в этом процессе. Это новый момент, достаточно опасный, который необходимо учитывать в работе с клиентом. Особенно когда готовится аналитическая информация, оценивающая состоятельность конкурента. Ведь известно, что некоторые факты можно оценивать по-разному. Например, судимость, которая за давностью лет снимается. Но клиента интересует не давность, а сам факт судимости и мы должны указывать этот факт. Формально можно придраться, что мы "оскорбляем" кого-то. И подобных поводом высказать неудовольствие нашей работой множество. На это необходимо обратить самое пристальное внимание.

16-Баяндин

Баяндин Н.И.
профессор, Институт безопасности бизнеса МЭИ (ТУ)

Хочу отметить, что конкурентная разведка и мошенничество имеют между собой общее - это информационно-аналитическая основа. Ведь любое мошенничество, которое все чаще строится на информационных технологиях, предполагает сбор и анализ информации об объекте. Поэтому можно говорить об информационном поединке между мошенником и фирмой, которая должна защищать себя (или клиента). На что надо обратить внимание при защите от мошенников?

Надо выявить на ранней стадии признаки атаки. Разработанная система индикаторов позволяет выявить сборщиков информации. Каких именно?

Во-первых, это сбор информации у сотрудников предприятия, особенно бывших. Поэтому важно по-доброму расставаться с коллегами, заключать соглашения, которые позволяют сохранить конфиденциальную информацию, и, может быть, получить впоследствии сигналы о проявленном кем-то интересе к такой информации.

Во-вторых, деятельность проверяющих организаций, за которой могут скрываться небескорыстные конкурентные или мошеннические интересы. Здесь важно иметь разработанный план поведения во время проверок.

В третьих, это мониторинг деятельности и поведения собственных сотрудников. Внутренние угрозы составляют почти 80% всех угроз безопасности предприятию. За рубежом, например, американским ФБР, разработаны схемы проверок персонала, которые включают как обязательные элементы: секс, деньги, идеологию, компромат, свойства личности. По этим критериям ведется постоянный мониторинг. Система предполагает

отслеживание коммуникаций, которыми пользуется персонал.

В-четвертых, важное значение имеет создание корпоративных баз данных по случаям мошенничества, которые бы включали судебные дела по раскрытым фактам, публикации в СМИ, а также данные, содержащиеся в платных информационных системах. Такие корпоративные базы данных могут создаваться при поддержке Российского общества профессионалов конкурентной разведки или группы компаний "Амулет", работающей под эгидой Ассоциации российских банков.

16-Рыбин

Рыбин А.Н.
Директор Московского представительства банка "Эллипс банк"

Предшествующие выступления меня раздосадовали как практика.

1. На сегодняшний день создание межбанковской базы данных - утопия. Если говорить честно, то нейтральной информации, которую я бы мог дать для использования своему банку, просто нет. Поэтому все предложения о создании межбанковской базы данных звучат хорошо. Но на практике все немножечко не так. Межбанк умер в 1995 году. Примерно, в это же время умерли доверительные отношения между банками. Я в этой связи хочу рассказать одну короткую историю. Министерство путей сообщения не имело своей службы экономической безопасности. Когда понадобилось, там создали такую службу всего за полгода. И никого из частного охранного бизнеса туда не пустили. Нет доверия.

2. Много говорим о технологиях бизнес-разведки. Но это пока удел очень узкого слоя специалистов высочайшей квалификации, которые могут заниматься в одиночку минимизацией всевозможных рисков. Я не знаю ни одной удачной компании. В ком действительно заинтересованы банки, кого они приглашают на работу - это профессиональные аналитики, пользующиеся личным доверием. Основная проблема этого вида бизнеса - отсутствие доверия. Между собой. Между партнерами.

3. Нет правовой базы нашей деятельности. Нет закона об экономической безопасности. Нет инициативных групп по его подготовке. Нет ни терминологии, ни глоссария, ни желания объединиться, чтобы все это расписать. Правовое поле, возможно, появится лет так через двадцать. Не раньше.

4. Аналитика подготовить нельзя. Способность аналитически мыслить дается свыше. Либо он сознательно приходит в этот бизнес и занимается на основе классических знаний и реального опыта. Или этого нет. Не так давно произошел обмен мнениями в группе банковских экспертов. Пришли к заключению, что в стране нет компании, которой можно поручить такое серьезное дело как бизнес-разведку. Буду рад, если меня убедят, что такие компании есть. Будем рады воспользоваться их услугами. "Круглый стол" можно будет считать удачным, если он завершится какими-то договоренностями, практическими результатами.

16-Пилюгин

Пилюгин П. Л.
Советник Генерального директора Специальной информационной службы

Отвечая на выступление г-на Рыбина, хочу коротко заметить, что те, кто не пользуется доверием, на рынке бизнес-разведки попросту не выживают.

Теперь что касается Закона "О кредитных историях". Этот вопрос мы давно и глубоко изучаем. Работала специальная комиссия в Торгово-промышленной палате. Проблема в том, что закон может быть очень хорошим. Но не факт, что он будет работать. В

позапрошлом году мэр Москвы Лужков предложил создать городское бюро кредитных историй. Поручено это было управлению экономической безопасности московского правительства, с которым наша компания тесно взаимодействует. В результате мы пришли к той же схеме, которая прописана в упомянутом Законе. Схема включает информацию о субъекте, о его действиях, а главное - закрытую информацию, кто и когда о нем информацию запрашивал. Анализ привел нас к той же проблеме, о которой говорилось - проблеме доверия. Нет доверия - не будет никакой информации от банка. Доверие возникает не сразу. Требуются многие годы совместной работы. Поэтому важно было разобраться, что надо делать, чтобы ускорить процесс возникновения, укрепления доверия.

Мы сделали макет технологии, который продемонстрировали в прошлом году на конференции "ИнфоФорума", опубликовали в журнале "Банковские технологии". Основная идея в том, что информация о субъекте должна храниться в зашифрованном виде. Если базу данных украдут, пустят на продажу, то все равно несанкционированные пользователи в ней ничего не поймут - кто, когда и как взял кредит. Поиск легальный осуществляется по совпадению зашифрованных полей. Но опять же требуется высокий уровень доверия к потенциальному клиенту, прежде чем вы решитесь предоставить ему кредитную информацию, причем при согласии субъекта этой информации. Вот такую технологию мы разработали и, надеюсь, она пригодилась московскому правительству, действует на практике.

Еще две короткие реплики.

Первое. Два года назад была у нас конференция Всемирной ассоциации детективов. Выступал президент Ассоциации, который сказал примерно следующее: "Мне предложили выступление на тему о том, как государство работает с частными сыскными мероприятиями. Я долго думал и решил ограничить свое выступление по этому вопросу одним словом - никак". В таких условиях частные сыскные компании, профессионалы деловой разведки живут, а иные и процветают.

Второе. Не все так плохо с кредитными бюро. Например, кредитные бюро в Финляндии выдают не сведения о том, кто и как возвращает кредиты, а дают рейтинги доверия, основанные на кредитных историях. На основе рейтингов банки принимают решения о выдаче кредитов и процентов по ним. Если бы у нас действовала такая же система, то в кредитные бюро выстроились бы очереди желающих дать о себе информацию.

16-Лобанов

Лобанов С.Г.
Генеральный директор "*Кронос-Инфо*"

К вопросу о взаимодействии с государственными органами. Как взаимодействовать? Писать письмо министру? Абсурд. Договариваться с его помощником? Похоже на коррупцию. В любом случае эта работа с конкретными людьми, представляющими государство. К сожалению, мы с ними разговариваем на разных языках. Имею в виду информационные языки. Здесь важны информационные технологии, которые способствуют информационному общению. Государство проповедует "защиту информации" с позиции ее закрытости и секретности. А между тем, информационная открытость как раз и является необходимым элементом информационной безопасности.

В условиях административной реформы многим чиновникам-исполнителям открываются возможности быстрого административного роста. Усвоив современные представления об информационных технологиях, информационной безопасности, чиновник, став начальником, способен разговаривать с нашей сферой бизнеса нормальным, современным языком.

За последние 10 лет сформировался слой специалистов в области информационных технологий. Высшее звено представляют аналитики. Но информационная работа не ограничивается чистой аналитикой. Эта работа достаточно рутинная. Информационщиков-аналитиков никто не готовит. За исключением Института безопасности бизнеса (МЭИ), и,

может быть, еще двух-трех учебных заведений.

Что касается борьбы с мошенничеством, то нежелание банковских служащих делиться информацией не может не удивлять. Ведь мошенники уже объединяются, выступают достаточно сплоченной группой преступников.
Противопоставить им можно и нужно организованное сообщество предпринимателей и банкиров, которое нуждается в доверии. Отдельно взятый банк преступнику "расколоть" ничего не стоит. Организованное противодействие преодолеть намного труднее.

16-Кунбутаев

Л.М. Кунбутаев
Директор Института безопасности бизнеса МЭИ (ТУ)

Начался интересный разговор о взаимодоверии внутри банковского сообщества. Эта тема поднимается и в прессе, и на профессиональных встречах банкиров и банковских служащих. Но воз и ныне там.

Действительно, с одной стороны, очевидно, что сотрудничество банков в области обмена информацией позволило бы значительно снизить банковские риски (инвестиционные, кредитные и др.), связанные с мошенничеством со стороны партнёров и клиентов. А с другой, - много ли банков, которым иной банкир готов доверить свою служебную информацию? Сдаётся, что при современном уровне мошенничества в сфере банковского бизнеса большинство банкиров предпочитают бороться со своими рисками в одиночку, нежели провоцировать возникновение новых рисков, создаваемых недобросовестными коллегами по бизнесу.

Для того чтобы доверия было больше, нужно улучшить ситуацию с преступностью в банковской сфере, а на это требуется время. Основные пути позитивного воздействия на ситуацию известны. Это совершенствование законодательства и разработка эффективных механизмов его реализации, наращивание прозрачности в деятельности государственных и муниципальных органов управления, борьба с повальной коррупцией в обществе, и прежде всего, в правоохранительных и контрольно-разрешительных структурах, повышение эффективности борьбы с оргпреступностью, поднятие престижности соблюдения писаных и неписаных правил профессиональной этики работников банковской сферы и т.д.

16-Минзов

Минзов А.С.
Зав кафедрой "Комплексная безопасность бизнеса" Института безопасности бизнеса МЭИ (ТУ)

Сегодня я вижу в зале много наших выпускников и преподавателей Института. Вообще складывается впечатление, что каждый десятый специалист в области экономической безопасности - наш выпускник, что весьма отрадно.

Я согласен, что аналитические способности заложены от рождения. Но, чтобы стать хорошим аналитиком, нужны знания, причем специфические знания, которые не даются в обычном ВУЗе. Я не буду говорить о всех направлениях информационно-аналитической деятельности и тем более об информационных продуктах, чтобы не делать им рекламу. Приведу только те направления, которые необходимо освоить современному аналитику в области обеспечения экономической безопасности бизнеса. Это, прежде всего, методы и информационные технологии прогнозирования, выявления структур, классификаций и скрытых закономерностей; методы оценки рисков; технологии выявления причинно-следственных связей; методы извлечения знаний; технологии извлечения данных из неструктурированной информации; технологии работы с электронными базами данных. Мы понимаем важность этого направления в образовательном процессе, поэтому организуем круглые столы, а также международные конференции (в этом году в Гурзуфе с 20 по 30

мая и в Сочи с 1 по 10 октября), которые посвящены проблемам информационно-аналитического обеспечения безопасности бизнеса. Более подробную информацию по этому направлению и условиях участия в конференциях вы можете найти на сайте http://ibbusiness.ru .

Наш разговор протекает в русле вопросов, связанных с мошенничеством, с банковскими рисками и т.д. Я бы хотел несколько расширить тему. Сегодня мошенничество непосредственно затронуло и сферу деятельности деловой разведки. На этом рынке услуг много предложений. Но при рассмотрении оказывается, что очень часто лица, выдающие себя за специалистов деловой разведки, не имеют соответствующих знаний и в лучшем случае прослушали 72-часовой курс. Они полагают, что необходимо иметь компьютер, купленные на рынке базы данных, немного уметь работать в Интернете - и всего этого вполне достаточно, чтобы именоваться экспертом. Наличие малоквалифицированных работников в деловой разведке также служит росту недоверия к этой профессии.

Другой аспект проблемы доверия упирается в профессиональную этику, в декларирование и честное следование правовым и этическим принципам в такой деликатной области деятельности как деловая разведка. К сожалению, здесь нет представителей крупного бизнеса, которые имеют собственные службы безопасности. А малому бизнесу деловая разведка представляется ненужной и дорогой затеей. Держать собственную службу конкурентной разведки затратно, приглашать со стороны - рискованно из-за возможной утечки конфиденциальной информации.

Доверие к деловой разведке напрямую зависит от ее этических стандартов. Необходимость профессиональной этики давно поняли маркетологи. Это стали понимать и "пиарщики". Но еще большая необходимость - в создании профессионального кодекса для специалиста в области безопасности бизнеса. На недавно организованном нашим Институтом семинаре мы попытались выработать Кодекс этики конкурентной разведки. С ним, а также с другими публикациями по этой теме можно ознакомиться на сайте Института (http://ethics.ibbusiness.ru).

В заключение хочу сказать, что в настоящее время мы работаем над созданием на базе Института организации или ассоциации, которая будет проводить сертификацию специалистов по профессиональной этике в области информационно-аналитического обеспечения безопасности бизнеса.

16-Митрофанов

Митрофанов А.
Группа компаний "МИГ" (безопасность бизнеса и консалтинг)

Вопрос доверия или недоверия не сильно связан с нашей практической деятельностью. Главное в том, что банковская деятельность не очень нуждается в деловой разведке. Спрос на деловую разведку не у тех, кто занимается финансами - банковские структуры достаточно зарегулированы, а у тех, кто занят реальным бизнесом - промышленным производством, т.е. там, где механизмы регламентации, регулирования намного слабее, где больше неопределенностей и задач, решаемых деловой разведкой.

Что же до борьбы с мошенничеством, то она начинается с идентификации объекта. И здесь главная проблема, с которой сталкиваются разведчики - информация, с помощью которой выявляется мошенник. До 2002 года можно было недорого приобретать данные в городских регистрационных палатах. Потом регистрационные данные передали в налоговые структуры. В прошлом году Министерство по налогам и сборам разродилось достопамятным приказом, разрешающим с 1 января 2005 года всем налоговым управлениям вести торговлю своей информацией по Интернету. При этом надо заплатить за разовый доступ - 50 тысяч рублей, за годовой доступ - 150 тысяч. Такие расценки доступны для крупных компаний. Те же, кто занимается обслуживанием среднего бизнеса, едва ли могут платить такие деньги.

Вопрос идентификации мошенничества волнует всех нас. И здесь надо серьезно обдумать возможности взаимодействия на базе организаций, которые обладают большими

информационными ресурсами. Я не вижу большой пользы от кредитных бюро. Информация о том, что имярек взял и вернул кредит, еще не говорит о его честности Мне кажется, что это мертворожденная идея.

Есть специальные аналитические методы идентификации мошенничества. Основной из них - метод аналогии, когда мы сравниваем образ реального мошенника с данными образа исследуемого объекта. Находим совпадающие признаки и делаем соответствующее заключение. Для такой работы нужны хорошие аналитики, обладающие знаниями конкретной отрасли экономики, в которой проводится исследование. Такие аналитики требуются и в банковских структурах, и в промышленности. Сейчас имеются и технические инструменты осуществления сравнительного анализа.

Предвидя возражения под лозунгом защиты частной жизни, личной переписки и т.п., хочу отметить, что мы занимаемся исследованиями в сфере общественного производства, подвергаем изучению субъекты экономики, где права личности не играют роли.

16-Кузнецов

Кузнецов С.В.
Эксперт

Я занимаюсь технологией аналитической деятельности, в частности, конкурентной разведкой через Интернет. Хочу предложить свой взгляд технолога на ряд проблем, озвученных на круглом столе.

Проблема консалтинга. Клиент часто не знает, что он хочет. Поэтому пенять на заказчика - признак профнепригодности.

Взаимодействие с властью. Полагаться на помощь государства в деле обеспечения безопасности конфиденциальной информации нельзя.
Лояльность государственных служащих ниже нуля. Оплата труда чиновников не позволяет рассчитывать, что в этой сфере останутся компетентные лица. Плюс взяточничество.

Информационная уязвимость. Фирмы, исповедующие информационную открытость, наиболее уязвимы с точки зрения враждебного поглощения.

О кредитных историях. Там информации мало, поскольку нет системного мониторинга всех источников информации, в том числе СМИ - где что может всплыть. Кроме того, отсутствует мотивация давать о себе информацию. Более того, часть информации может быть использована против самого донора информации. Выносить информационный сор из избы в России очень опасно.

Аутсорсинг услуг деловой разведки. Мне не известны фирмы, которые предоставляют такие услуги по нормальным гражданским договорам, предполагающим ответственность за результат. Еще одна проблема аутсорсинга - передача материалов исследования конкурентам заказчика, чреватая тяжелейшими последствиями. Как оценивать качество услуг аутсорсинга в области деловой разведки? Довольно просто. Мы обычно объявляем тендер, просим подготовить предложения по конкретному объекту. Потом выбираем лучший отчет и заключаем с консультантом/фирмой т.н. "тяжелый договор", проверяя попутно персонал на лояльность.

Кадровый вопрос. Традиционно в компании деловой разведки приходят много людей из правоохранительных органов. Ставка на профессиональных оперативников себя не оправдывает Аналитическая подготовка у них часто оставляет желать лучшего. Нужны независимые аналитики, с иммунитетом против ощущения безнаказанности, которое нередко формируется у работавших во властных структурах. Добиться лояльности к фирме от человека, проработавшего ряд лет в органах - сверхзадача. Все упирается, в конечном счете, в доверие, в лояльность персонала. В компаниях, как правило, нет аудита лояльности, этичности персонала. Большинство взломов - результат сочетания некомпетентности с отсутствием лояльности. Нам не мешало бы взять на вооружение модели контроля, используемые в ряде азиатских стран (Япония, Корея), когда разведкой

занимается весь персонал фирмы, все следят за признаками мошенничества - они заинтересованы, компетентны, мотивированы, уверены, что фирма их защитит. Зарубежный опыт защиты от мошенничества надо тщательно изучать. В нем обязательно присутствуют три компонента - 1)лояльность, 2)компетентность персонала, 3)внутренняя система обучения, осведомленность о рисках, о признаках мошенничества.

Хочу обратить внимание на технологии разведки по открытым источникам, в частности, на использование этих технологий для аудита безопасности информационных проектов.

Юридические моменты. Имеет место некомпетентность юристов, которые, допуская "дырки" в клиентских договорах, создают условия для мошенничества. Следующий момент - непрозрачность законодательства и неумение юристов работать с правовыми базами данных, например, находить судебный прецедент. Кроме того, из-за коррупции нельзя рассчитывать на судебную помощь. Единственный выход - сценарная экспертиза, о чем говорил г-н Пилюгин.

16-Катышев

Катышев М.В.
Председатель Правления некоммерческого партнерства "Российское общество профессионалов конкурентной разведки"

Есть в зале представители администрации Президента РФ, правительства, МВД? Нет. Так кому же мы жалуемся? Может быть, не надо жаловаться друг другу. Мне представляется, что сегодняшние вопросы - это не наш уровень обсуждения. Если даже на уровне Госдумы, министерств, силовых органов не в состоянии понять, что надо делать, то что нам тут обсуждать! Да, действительно не хватает аналитиков. Действительно многие из тех, кто имеет склонность к нашей работе, не находят места под солнцем, вынуждены заниматься совершенно непрофильными делами, чтобы только прокормиться.

Мне кажется, что мы должны настроить себя на положительную волну. В конце концов, мы - профессионалы конкурентной разведки. Мы работаем и зарабатываем.

Было бы интересно услышать представителей компаний, как они практически борются с мошенничеством. Мошенничество в банковской системе часто оказывается довольно мелким на фоне настоящих, крупных мошенников, которые имеют уже сложившуюся систему своей безопасности, людей, занимающихся промышленным шпионажем, людей с коррупционными связями во властных и правоохранительных структурах. То же самое можно сказать о враждебных поглощениях. Ржавчина, проевшая правоохранительную систему, не дает надежды на защиту со стороны государства. То, что часто называют "административным ресурсом", на самом деле не что иное, как коррупция. Глупо рассуждать о том, что мы способны победить коррупцию. Наша основная задача в данных условиях - просто выжить, набраться знаний, необходимых для профессиональной, квалифицированной работы.

Представляется, что на таких круглых столах, прежде всего, надо обмениваться практическим опытом. Но верно и то, что все меньше остается желающих поделиться собственным опытом, тем, как можно решить ту или и иную проблему.

В силу объективных причин мы вынуждены решать профессиональные задачи, опираясь на базовое образование, которое каждый из нас в свое время получил. Как говорят, "не стреляйте в пианиста, он играет, как может". Действительно, есть острый дефицит аналитиков, толковых, умных людей, занимающихся поиском, обработкой информации. Но если банк хочет создать серьезную службу безопасности, и у него на это есть ресурсы - тогда задача не сложная. Просто нужно просеять огромный список людей, склонных к аналитической работе, и кандидатов реально проверить на профпригодность.

Хорошо, что сегодня немало внимания уделяется образованию в области экономической безопасности. Чем больше людей пройдет хотя бы базовое образование в этой сфере, тем лучше. Поэтому, огромное спасибо тем, кто занимается обучением. Не надо преувеличивать уровень служб безопасности в крупных компаниях. Там работают такие же специалисты,

как и в среднем, и в малом бизнесе. Здесь важно отметить, что новые знания в вопросах конкурентной разведки - главное, что мы можем дать друг другу, участвуя в круглых столах, обмениваясь своим опытом.

16-Куборский

Куборский Г.В.
Эксперт

За последние годы схемы мошенничества с использованием карт в торгово-сервисных предприятиях (ТСП) значительно усложнились. Оснащение банков-эмитентов эффективными системами мониторинга мошеннических операций заставило мошенников искать новые подходы и средства.
Схемы мошенничества становятся все более изощренными и трудно распознаются. И хотя по прежнему время от времени обнаруживается "отмывание" покупок, которое обычно налаживают в небольших торговых точках, ему на смену пришли высокотехнологичные мошеннические схемы, которые изобретают международные преступные группировки.
По сравнению с 2000 годом потери составили 6 миллиардов долл. Уже в 2003 году ущерб составил 17 миллиардов долл. Банки РФ в первую очередь выступают как эквайреры , так как у нас карт еще мало. Оборот по картам банков эмитентов РФ за 2003 составил 12 миллиардов долл. 2005-2006 г. обусловлены переходом к смарт картам. К концу 2005 г. будут вводиться гибриды карт с носителями, как на чипах, так и на магнитной полосе. Будут пересмотрены ответственности между банками эмитентами и эквайрами. Такие переходы всегда обусловлены всплеском мошенничества
Задача эквайреров и эмитентов - адекватно оценивая способности и изобретательность современных преступников, постоянно усиливать и совершенствовать защиту своего бизнеса. И хотя определенная доля мошеннических операций обусловлена специфическим типом продаж Card-Not-Present, (MO/TO) или по Интернету, следует помнить о том, что преступники разрабатывают планы проведения мошеннических операций в странах, где эмитенты, эквайреры и торговые точки наиболее уязвимы.
Каковы наиболее распространенные типы мошенничества при соучастии персонала, с которыми приходится иметь дело банкам-эквайрерам?
Подставные торговые точки. Преступники открывают в банке счет для эквайринга торговой точки. После какого-то периода якобы нормальной торговой деятельности в этом ТСП проводятся мошеннические операции на большие суммы по поддельным или краденым номерам карт. После получения возмещения от банка организаторы ТСП скрываются. Такие подставные точки маскируют под обычные магазины или регистрируют как интернет-магазины.

"Отмывание" покупок. Торгово-сервисное предприятие, заключившее договор с эквайрером, проводит оформленные другим ТСП (не имеющим договора на эквайринг) транзакции как собственные, получая при этом комиссию за их обработку в размере от 1 до 20 процентов. Чаще всего эти транзакции проводят с использованием украденных номеров карт. Через некоторое время ТСП без договора на эквайринг закрывается, а легальная торговая точка несет огромные убытки по отказам от платежей (chargebacks).

Телемаркетинговое мошенничество. Преступники пытаются связаться с держателями карт по почте или телефону с целью получения информации о действительных номерах карт, чтобы проводить по ним несанкционированные держателями списания по счету.

"Кредитовая" схема. Сотрудник или кассир ТСП (посредством фиктивных операций возврата товара) незаконно кредитует счет личной карты Visa, снимая при этом деньги из суммы возмещений ТСП по операциям с картами. Обычно мошенники сначала проводят несколько легальных "расходных" операций по картам своих друзей или родственников, а затем проводят одну или две "кредитовые" операции на счет своей личной карты Visa. Проведение преступниками дебетовых и кредитовых операций на одинаковые суммы осложняет выявление подобных схем мошенничества.

Схема обналичивания. Кассир ТСП проводит транзакцию по личной карте и берет из кассы соответствующую сумму наличными. Такая операция по выдаче наличных "кажется"

легальной. Часто кассир позднее возвращает наличные в кассу и производит соответствующий возврат на карту.

Скимминг. Данные, закодированные на магнитной полосе действительной карты, копируют для последующего нанесения на поддельные, украденные или утерянные карты. Любая карта, имеющая магнитную полосу, может быть перекодирована новыми данными, полученными в результате скимминга.

"Проверка" счета. Чтобы проверить, действителен ли счет, мошенник "пробивает" его, то есть пробует оплатить покупку на небольшую сумму либо запросить авторизацию по номеру карты, полученному нелегальным способом (кража карты, скимминг, генерирование номера). Часто в этом принимают участие кассиры ТСП, состоящие в сговоре с мошенниками.

ТСП в сговоре с мошенниками. Кассир ТСП принимает к оплате карты, которые при иных обстоятельствах не были бы приняты к обслуживанию. Так кассир может принимать грубо подделанные ("белый пластик") или украденные/утерянные карты, пренебрегая необходимыми процедурами проверки карты.

16-Горделян

Горделян А.А.
Исполнительный директор некоммерческого партнерства "Российское общество профессионалов конкурентной разведки"

Многие со мной согласятся, если скажу, что конкурентная разведка - это стратегическая дисциплина, связанная с экономикой. Термин "конкурентная разведка" стал широко применяться в России в последние 1,5 -2 года всеми, кто хочет себя в ней позиционировать. Беда в том, что, используя разные термины: "бизнес-разведка", "деловая разведка", "финансовая разведка", "конкурентная разведка" и т.п., - мы, по большому счету, дезориентируем и себя, и интересующихся конкурентной разведкой, и потенциальных клиентов, и всех, кто в силу профессиональной или иной необходимости занимается конкурентной разведкой. Считаю, что необходимо вносить больше ясности в то, что касается использования терминологии в сфере конкурентной разведки, которая начинает активно внедряться в России. Необходимо начинать работу над терминами и определениями. Это будет только на пользу самой российской конкурентной разведке, её продвижению в бизнес сообщество и её развитию. Мы уже касались этого на предыдущих встречах.

Хорошо, что сейчас делаются попытки организации обучения конкурентной разведке, как стратегической дисциплине. Оценивать уровень современного образования в сфере конкурентной разведки можно по-разному. Главное здесь - начать вырабатывать базисные определения, термины, единые для всех специалистов, чтобы мы могли общаться на одном языке. Или иначе - создавать научно-теоретический и практический фундамент конкурентной разведки. А основное, чтобы нас понимали все, кто так или иначе будет связан с конкурентной разведкой, в т.ч. и потенциальные клиенты практикующих в сфере конкурентной разведки компаний. От этого престиж, статус нашего профессионального сообщества только укрепится. В выигрыше будут все.

16-Попов

Попов В.В.
Информационно-консалтинговое бюро "ДеФакто"

К сожалению, нам не удалось обсудить заявленную тему. Но это не вина организаторов. Мы объективно говорим на разных языках и никогда не договоримся. Тем более до практической координации борьбы с мошенничеством. У нас разные темы выступлений, разные опыт, социальный статус, методология мышления. Вместе с тем, прозвучали

некоторые предложения. Например, один из участников предложил свое видение конкуренции через Интернет. Другие, предположим, рассказали бы о своих насущных проблемах, и мы договорились бы, как их решать. Должна быть методика подобных обсуждений. Я принадлежу к когорте практических сотрудников, хотя много лет занимался наукой. Занимаюсь вопросами обеспечения бизнеса.

В некоторых выступлениях меня поразил дух некорректности в отношении коллег. Например, прозвучало утверждение, что в России "нет ни одной фирмы деловой разведки". Так нельзя говорить. В России сложился рынок деловой разведки. Ему 10 лет. Имеется инфраструктура рынка. У ряда компаний высокий имидж, признанный авторитет.

На круглом столе собрались вместе работники практических организаций в области деловой разведки, представители учебных заведений, работники банков, журналисты, частные эксперты. Поэтому каждый говорил о своем, и единого разговора о тематике не получилось.

У меня предложение. В будущем собираться по секциям. Пусть будет всего 10 человек, но они объединены общим проблемами, общим интересом. И рассматривать один-два конкретных вопроса. К примеру, последние информационные системы сбора, хранения, анализа информации. Это было бы полезно, нужно. Отдельно можно обсудить разнообразные методики мошенничества, используемые частными лицами, страховыми компаниями, зарубежными компаниями и т.д. Интересно было бы узнать о практическом применении методик выявления признаков мошенничества в связи с предлагаемыми инвестиционными проектами.
Здесь говорилось, что можно зарабатывать на клиентах, но не на партнерах. Я считаю, что можно и на партнерах. Приходит потенциальный клиент и предлагает нам исследование того или иного сегмента рынка. Мы готовы принять заказ, но предупреждаем, что его выполнение займет много времени и рекомендуем обратиться к партнерам, которые уже занимались изучением данного вопроса. То есть можно говорить об обмене не только мнениями и опытом, но в отдельных случаях и клиентами. Все это можно делать в рамках нормальных, профессиональных, этических взаимоотношений между коллегами.

16-Пучков

Пучков С.И.
Эксперт по экономической и информационной безопасности Балашихинской торгово-промышленной палаты

Прежде всего, разрешите поблагодарить организаторов круглого стола "Деловая разведка против мошенничества: проблемы координации" за приглашение участвовать в работе круглого стола и предоставленную возможность выступить на нем. Само название данного мероприятия, по моему мнению, отвечает на вопрос предыдущего круглого стола "Конкурентная разведка - в структуре безопасности бизнеса или вне ее?" состоявшегося в рамках IX Международного Форума "Технология безопасности" (3-6 февраля 2004 г., Москва). Нам не удалось, к сожалению, избежать обсуждения вопросов, не относящихся к теме данного круглого стола. Но это не вина организаторов, а скорее беда сообщества аналитиков России, к которым можно отнести и специалистов по деловой разведки.

Одной из важных мер по профилактике мошенничества в предпринимательской среде - это отработка рыночных механизмов информационного обеспечения предпринимательства, разработка методик определения надежности партнеров на отечественном рынке, выработка методологии работы с информацией в предпринимательской среде.

Система торгово-промышленных палат России придает профилактике мошенничества в предпринимательской среде большое значение. Мы не можем согласиться с западными экспертами по безопасности о том, что в компаниях Восточной Европы "мошенничество зачастую рассматривается как неизбежное зло в бизнесе, как риск, которым невозможно управлять...". Так в настоящее время ТПП РФ и территориальные торгово-промышленные палаты реализуют долгосрочный проект по ведению негосударственного Реестра российских предприятий и предпринимателей, финансовое и экономическое положение которых свидетельствует об их надежности как партнеров для предпринимательской

деятельности в Российской Федерации и за рубежом (Реестр надежных партнеров). Этот проект ведется в целях содействия предпринимательской деятельности, в том числе внешнеэкономическому сотрудничеству, путем предоставления российским и иностранным организациям и предпринимателям необходимой информации для выбора партнеров из числа российских организаций и предпринимателей; повышения доверия к российским предпринимателям на внутреннем рынке и за рубежом.

Возможно, сообществу аналитиков, в том числе и специалистам по деловой разведке, стоит рассмотреть вопросы объединения усилий с ТПП РФ по созданию системы новых источников информации о финансовой состоятельности и платежеспособности юридических и физических лиц, оказания помощи торгово-промышленным палатам Российской Федерации, особенно муниципального уровня. Это, на наш взгляд, позволит резко приблизить предоставление услуг сообщества аналитиков предпринимательству, что в свою очередь будет поднимать социальный статус сообщества. Контактная информация на сайте ТПП РФ (www.tpprf).

Заканчивая выступление, хочется отметить, что временные рамки нашего круглого стола не позволили полнее обсудить возможности взаимодействия государственных и негосударственных структур безопасности по предотвращению мошенничества в предпринимательской среде. И я приглашаю присутствующих 22 февраля 2005 года в конференц-зал Торгово-промышленной палаты Российской Федерации на расширенное заседание Комитета ТПП РФ по безопасности предпринимательской деятельности и Общероссийской общественной организации "Объединение частных детективов России" по теме "Частный сыск: проблемы обеспечения комплексной безопасности предпринимательской деятельности и личности, взаимодействия с правоохранительными органами и иными государственными органами и пути их решения". Многие вопросы, которые будут обсуждаться в ходе этого заседания, будут интересны и представителям сообщества аналитиков России, в том числе и специалистам по деловой разведке.

16-Доронин

Доронин А.И.
автор книги "Бизнес-разведка"

Каждый день мы сталкиваемся с необходимостью принимать решения. Под принятием решений понимается человеческая деятельность, направленная на выбор наилучшего способа достижения поставленной цели.

В общественном мнении предполагается, что руководители должны принимать решения более ответственно, чем это делаем все мы в своей повседневной жизни.

Сегодня в современной России все большее число людей оказывается вовлеченными в процессы принятия деловых решений. Появились частные компании, новые институты власти и вместе с ними - задачи разработки самих основ построения экономической и социальной жизни государства.

Но, к сожалению, новые руководители не получали, как правило, какого-либо специального образования в области управления организационными системами и принятия решений. Это является одной из причин, хотя и не единственной, большого числа ошибок в принятии управленческих решений. Практика показывает, что, как правило, сам потребитель разведывательной информации не может грамотно сформулировать информационное задание и разработать корректные, реализуемые требования.

Это связано с тем, что он не имеет профильного образования, не знает нюансов работы по сбору информации и тем более аналитических возможностей разведывательных технологий. Поэтому, чтобы исключить различные недоразумения возникающие при выдаче неполной или нерелевантной информации потребителю, руководитель информационного подразделения помимо всего прочего, берет на себя функции аналитика-постановщика информационной задачи.

Аналитик-постановщик осуществляет анализ предметной области. На основании своих

знаний, информационных технологий и процесса выполнения оперативной работы он предлагает решение проблем пользователя и сообщает примерную стоимость этого решения. Если заказчик делает заказ, то аналитик разрабатывает технические задания для разработчиков (других участников группы).

При постановке задачи постановщик должен описать на основе знания предметной области все критичные к разработке моменты задачи. Чтобы не пропустить какой-либо важный нюанс в задаче, а также, чтобы текст задания был максимально прозрачным для понимания.