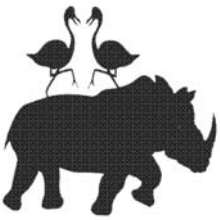

Крис Палларис:

НОВЫЕ ТЕХНОЛОГИИ В РАЗВЕДКЕ

Могут ли инструменты предиктивной аналитики предсказывать рабочий график В.В. Путина? В чем заключается основное отличие разведки из открытых источников от традиционной разведывательной деятельности, которой занимаются в основном государственные секретные службы? Какие факторы подстегнули развитие коммерческой разведки из открытых источников? Какое место в такой разведке играют информационно-коммуникационные технологии?

На вопросы корреспондента журнала Индекс Безопасности отвечает Крис Палларис, директор и главный консультантом компании i-intelligence. Компания работает с государственными и частными организациями, помогая им развить свой потенциал в области стратегической коммерческой разведки и сбора информации, а также обучая их персонал эффективной работе в постоянно меняющихся внешних условиях.

ИНДЕКС БЕЗОПАСНОСТИ: Коммерческая разведка из открытых источников является достаточно новым видом деятельности. Какие факторы подстегнули ее развитие — как для Вашей компании, так и для всего европейского рынка? Каким Вам видится будущее разведки из открытых источников в течение следующих трех-пяти лет?

ПАЛЛАРИС: Вопреки широко распространенному мнению, коммерческая разведка не является новой дисциплиной. Истоки ее можно проследить как минимум до XVII в. и Ост-Индской компании. Я подозреваю, что первые примеры такой деятельности появились еще раньше.

В своей нынешней форме коммерческая разведка появилась после окончания холодной войны. Благодаря спаду напряженности в международных отношениях тысячи профессионалов в области разведки пришли в частный сектор, предлагая тем отраслям промышленности (энергетика, финансы, фармацевтика, и т. д.), у которых хватило здравого смысла воспользоваться их услугами, свой уникальный набор знаний, умений и навыков. Со временем эти профессионалы организовали собственные консалтинговые компании.

В настоящее время на рынке присутствуют самые разнообразные фирмы, специализирующиеся на коммерческой разведке — от крупных компаний, которые работают во многих отраслях промышленности, до небольших высокоспециализированных организаций, работающих в узкой отрасли или даже на одного-единственного клиента. Сама отрасль уже превратилась в глобальный феномен. Везде, где зарабатываются деньги, существует необходимость в информации — хотя бы для того, чтобы свести к минимуму риски и по максимуму использовать коммерческие возможности.

Компании, работающие в нашей отрасли, отличаются своей специализацией и конкретной сферой работы. К примеру, *i-intelligence* специализируется на тренинге и консультировании клиентов, которые желают за небольшие деньги приобрести собственный конкурентоспособный потенциал в области сбора информации, используя при этом широко доступные инструменты и технологии. Иными словами, существует столько же разных видов коммерческой разведки, сколько существует областей, где могут применяться наши знания и умения.

Интернет и широкое распространение IT-технологий сыграли значительную роль в стимулировании роста данной отрасли. Количество всевозможных источников информации продолжает расти настолько быстрыми темпами, что большинство организаций за этим ростом просто не поспевают. К примеру, типичному отделу продаж коммерческой компании приходится вести мониторинг сотен отдельных субъектов (клиенты, конкуренты, и т. д.), черпая информацию из десятков источников, в том числе из открытых социальных сетей в интернете и баз данных с ограниченным доступом. Конечно же, интернет не является единственным источником данных для конкурентной коммерческой разведки. Более того, иногда он даже не является наилучшим из имеющихся источников. Но он незаменим в плане изучения рынка и конкурентной среды. К сожалению, большинство организаций не знают, как воспользоваться возможностями интернета с наибольшей отдачей. Не знают этого и те выпускники университетов, на которых такие организации часто возлагают свои надежды в данной области. В результате многие функции по текущему сбору данных и информации часто передаются внешним организациям в рамках аутсорсинга.

Технология тоже сыграла свою роль. Когда я только начинал свою карьеру в Лондоне, единственным типом компьютеров были настольные рабочие станции. При этом возможности этих станций были ограничены тем набором программного обеспечения, который на них решил установить работодатель. Сегодня компьютер, который помещается в ваш карман, является самым лучшим средством коммерческой разведки — лучшего не купишь ни за какие деньги. Этот компьютер может снимать фотографии и видео, он может записывать беседы с экспертами в необходимой отрасли, он помогает в геолокации новых и уже существующих клиентов. Его функциональность определяется только вашим собственными потребностями и вашей способностью найти нужное для работы программного обеспечения (ПО). Однако даже в данной сфере многие организации плохо себе представляют, как можно использовать эти инструменты и технологии себе во благо, не нарушая при этом никаких законов.

Откровенно говоря, очень многие поставщики услуг в сфере коммерческой разведки с удовольствием эксплуатируют такую безграмотность своих клиентов. Несколько месяцев назад у меня был ланч с представителем одной компании-энерготрейдера. Он утверждал, что поставщик услуг в области коммерческой разведки, нанятый этой компанией, имеет доступ к информации, которую невозможно найти в интернете. На самом деле эта информация в интернете есть, главное — знать, где ее искать. Фактически, фирма обманным путем убедила своего клиента платить ей десятки тысяч долларов за информацию, которую можно было раздобыть бесплатно с помощью мышки и клавиатуры.

Разработчики технологий ведут себя похожим образом — хотя и не все, но довольно многие. К примеру, большинство фирм, специализирующихся на мониторинге СМИ, продают своим клиентам доступ к инструментам и технологиям, которые сильно уступают в эффективности бесплатным инструментам, имеющимся в свободном доступе в интернете. На самом деле все что нужно, чтобы организовать первоклассный мониторинг СМИ или приобрести вполне конкурентоспособный потенциал в области коммерческой разведки — это учетная запись в *Google*.

Что касается тенденций, то одной неизбежной закономерностью, определяющей развитие рынка, является постоянное увеличение потока информации. Потребность в информации и спрос на нее будут расти и далее в обозримом будущем. Давайте, к примеру, рассмотрим те проблемы, с которыми в наше время сталкивается любая компания: постоянная экономическая неопределенность, меняющаяся регулятор-

ная среда, растущая конкуренция, и т. д. Решение этих проблем неизбежно требует все большего количества и качества информации. Это, в свою очередь, влечет за собой необходимость в информационной грамотности сотрудников (либо в услугах компетентной фирмы, специализирующейся на коммерческой разведке).

Смартфоны, планшеты, сенсоры и беспроводные технологии — все это оказывает огромное влияние на *информационный ландшафт*, в котором прокладывают свой путь организации. Количество источников коммерческой информации будет расти по мере роста нашей собственной готовности использовать новые и инновационные каналы коммуникаций. Компания, которая *знает*, какими источниками следует пользоваться, и *умеет* их эксплуатировать, неизбежно получает конкурентное преимущество. Организациям необходимо работать над повышением своей информационной грамотности. Эти знания и умения — не приятный довесок ко всему остальному. Они абсолютно необходимы для самого выживания организации. Более того, от них зависит конкурентоспособность всего государства.

Какое будущее ждет отрасль коммерческой разведки? Учитывая нынешнее состояние экономики, я думаю, что крупные компании консолидируют рынок путем слияний и поглощений. При этом будут продолжать появляться все новые мелкие, нишевые фирмы, специализирующиеся на конкретных узких областях коммерческой разведки.

ИНДЕКС БЕЗОПАСНОСТИ: В чем заключается основное отличие разведки из открытых источников от традиционной разведывательной деятельности, которой занимаются в основном государственные секретные службы? Есть ли прецеденты, когда государственные службы — к примеру, аналитические отделы или даже сами разведслужбы — пытались передать в рамках аутсорсинга отдельные свои функции компаниям, специализирующимся на разведке по открытым источникам? Практикуется ли сотрудничество между такими компаниями и государственными службами на некоммерческой основе?

ПАЛЛАРИС: Обычно ответ на подобный вопрос звучит примерно так: разведка из открытых источников — это сбор данных из несекретных источников информации. В традиционной, или засекреченной, разведке используется более широкий спектр источников и методов получения нужной информации, включая агентурную работу, фотографии со спутников, и так далее.

На самом деле я не уверен, насколько такое определение было и остается правильным. Поясню: информация из открытых источников составляет 95% всей информации, которая необходима разведслужбам для обеспечения национальной безопасности и принятия политических решений. Почему это так? Потому, что добывать засекреченную информацию трудно и дорого. Ценность такой информации зачастую сомнительна, при этом она имеет свойство быстро устаревать. Конечно, это не значит, что такая информация бесполезна. Но ценность ее всегда является ограниченной.

Разведка из открытых источников является одним из ведущих направлений развития традиционных разведслужб. В откровенном разговоре любой профессионал в области разведки признает, что информация из открытых источников всегда являлась главной опорой любой компетентной разведслужбы. Во времена холодной войны советские разведчики значительную долю своего времени тратили именно на внимательное чтение газет, журналов, каталогов и тому подобных печатных источников в поисках информации, которая может оказаться полезной для агентуры. По имеющимся данным, результаты этой работы были очень впечатляющими.

Секретные службы собирают данные из всех возможных источников — но в очень многих случаях они полагаются прежде всего на информацию из открытых источников. Иными словами, в некоторых вопросах безопасности именно к такой открытой информации обращаются в первую очередь. А во всех остальных вопросах к ней обращаются в первую, последнюю и единственную очередь. Соответственно, умение работать с информаций из открытых источников — а также профессио-

нализм во всех остальных областях, относящихся к сбору информации и разведке — является залогом успешной разведывательной работы.

Дефицит профессионалов в данной области может объяснять тенденцию к аутсорсингу сбора информации — но это не единственное объяснение. За последние десять лет государственные органы начали рассматривать с точки зрения безопасности все до единого аспекты жизни страны — продовольственная безопасность, водная безопасность, энергетическая безопасность, экономическая безопасность, и т. д. Почему так происходит — тема для отдельного разговора. Но конечный результат очевиден: это постоянно растущая потребность в информации. Поясню: безопасность ведет к уверенности. Чем прочнее безопасность, тем больше уверенность в завтрашнем дне. И наоборот, отсутствие безопасности ведет к неуверенности и неопределенности. Чем выше степень неопределенности, тем больше нам нужно информации, чтобы эту неопределенность снять. Любое правительство работает в условиях большой неопределенности. Соответственно, продолжает расти его потребность в информации. Ни у одного правительства в мире нет достаточных ресурсов, чтобы полностью удовлетворить все свои потребности в информации — отсюда тенденция к аутсорсингу разведки и сбора информации.

Характерно, что большинство коммерческих компаний, которым госорганы передают некоторые свои функции в области сбора информации, работают исключительно с открытыми источниками. Отсюда следует, что если бы государственные служащие были лучше обучены работе по сбору информации из открытых источников, то расходы на аутсорсинг этих функций можно было бы значительно сократить.

Тем не менее, мне кажется, что рынок коммерческой разведки будет продолжать расти, хотя бы в силу того множества рисков и вызовов, с которым сталкиваются правительства.

ИНДЕКС БЕЗОПАСНОСТИ: Есть ли у вас планы развития, которые предполагают сотрудничество с компаниями (или даже государственными службами) из России, постсоветских стран или государств Восточной Европы? Есть ли планы прямой экспансии на этих рынках? Какие крупные национальные или региональные рынки за пределами Западной Европы кажутся наиболее привлекательными для компаний, специализирующихся на разведке по открытым источникам?

ПАЛЛАРИС: Пока что мы не занимались никакими совместными проектами за пределами Европы и Северной Америки. Однако мы готовы выслушать предложения, и каждое такое предложение мы рассмотрим индивидуально.

Будучи профессионалом в области образования, я особенно стремлюсь к сотрудничеству с университетами и бизнес-школами, чтобы помочь им обеспечить своих студентов теми знаниями и умениями, которые незаменимы в XXI в. Сюда входит умение собирать и анализировать информацию; обмениваться информацией; работать в условиях неопределенности и учитывать множество факторов; заниматься стратегическим планированием и прогнозированием; думать критически, креативно и концептуально, чтобы всегда быть хорошо приспособленным к быстро меняющейся деловой среде; а также уметь извлекать пользу из рисков и возможностей. Насколько можно судить, такие знания и умения сейчас в дефиците. В университетах такому учат редко, а на рабочем месте — практически вообще никогда. Мне такая ситуация кажется удивительной — ведь именно такие качества желают видеть в своих сотрудниках руководители компаний на протяжении вот уже двадцати лет.

Более того, я бы даже сказал, что нынешний экономический кризис во многом объясняется тем, что значительный процент европейской рабочей силы не имеет умений и навыков, необходимых для работы в экономике знаний. К примеру, средний офисный работник тратит до двух дней в неделю на безуспешные поиски информации. Подумайте, насколько более продуктивной стала бы их работа, если бы они на эти поиски тратили на 50 или на 80% меньше времени?

Нарастающая проблема кибершпионажа отражает эту динамику. В условиях нынешней экономики существует три способа получить необходимую для успешной конкуренции информацию. Можно инвестировать время и ресурсы в то, чтобы самостоятельно получить подробную картину своих рынков, клиентов и конкурентов. Можно эту работу поручить кому-то другому, в надежде, что подрядчик ее выполнит качественно. И, наконец, можно нанять хакера, чтобы он для вас крал любую информацию, которая ему подвернется под руку.

Только первый из этих трех подходов гарантирует получение дивидендов. Почему? Потому что те организации, которые учатся тщательным и этически безупречным образом собирать самостоятельно всю необходимую информацию, одновременно совершенствуют саму свою *способность учиться*. Именно способность учиться отличает успешные организации от неудачников. Красть чужие секреты легко — но вовсе не факт, что эти секреты пойдут на пользу вашей организации.

ИНДЕКС БЕЗОПАСНОСТИ: Насколько активно ваша компания использует для сбора информации социальные сети? Какие аналитические инструменты используются для обработки и анализа огромных массивов данных, полученных их социальных сетей и всего интернета?

ПАЛЛАРИС: Социальные сети и социальные СМИ сейчас являются очень актуальной темой для профессионалов в области как коммерческой разведки, так и национальной безопасности. Возможно, это объясняется тем, что профессионалы во всех аспектах разведки и сбора информации с очевидным запозданием осознали ценность и потенциал этих источников.

Чтобы понять эту ценность, нужно сперва понять человеческое поведение. Для людей характерно непреодолимое желание общаться. Общение — будь то с друзьями, семьей, или с миллионами незнакомых людей в интернете — является для нас некой валидацией нашего существования. Социальные сети удовлетворяют и усиливают наше стремление осознавать, что мы живы, и взаимодействовать с другими людьми. Это может звучать цинично, но на самом деле это вполне естественное для любого человека желание. Все это в равной степени относится и к организациям, которые состоят из отдельных людей.

Неизбежным образом эти отдельные люди делятся друг с другом информацией, которую, возможно, им стоило бы держать в секрете. Это информация о новых клиентах, о корпоративной стратегии своей компании, о провалах каких-то проектов, и так далее. Они при этом используют каналы, которые открыты для всех, в том числе и для профессионалов в области коммерческой разведки и сбора информации. Все, что нужно, чтобы получить такую информацию из социальных сетей — это хорошее знание источников информации и знание основ RSS/XML. Не обязательно даже добавлять организацию в свои *друзья* в *Facebook* или *Twitter,* чтобы узнать, о чем эта организация думает, чем она занимается и о чем говорит.

Профессионалы в области безопасности и правоохранительной деятельности также все больше осознают ценность социальных СМИ. Приведу лишь один пример: в этом году вышло несколько статей о том, как китайские блогеры, интересующиеся военной техникой, публикуют в своих блогах фото новейших китайских боевых самолетов и кораблей. Делают они это из соображений национальной гордости, в порыве искреннего энтузиазма. Но тем самым они также снабжают иностранные разведслужбы ценной информацией, на получение которой у тех могли бы уйти недели или месяцы, а также десятки тысяч долларов. Поэтому знание того, какие блоги представляют ценность, и как правильно проводить их мониторинг, становится очень важным.

Однако я не считаю, что социальные сети станут гигантским хранилищем данных, которым может воспользоваться любая желающая организация. Более того, я подозреваю, что в долгосрочной перспективе делать это будет все сложнее.

В любом случае, есть предел тому, что организации реально могут сделать со всей накопленной информацией. Есть, например, чисто практические ограничения на объем информации, который можно хранить. Есть и юридические ограничения: накопление огромного количества личных данных пользователей далеко не приветствуется законодательством, по крайней мере, в Европейском Союзе. Более того, ЕС стремится ввести такие правила, в соответствии с которыми личные данные пользователей, переданные социальным сетям, остаются собственностью самих пользователей. Время покажет, насколько успешной окажется эта инициатива. В любом случае, наиболее существенное ограничение связано тем, что сам объем данных, которые мы постоянно генерируем, огромен. Для обработки всех этих данных просто не хватит ни инструментов, ни технологий, ни людей.

Конечно, многим из нас приятно думать, что правительство внимательно следит за всем, что мы сказали и написали в интернете. Если это действительно так, то я не завидую тем несчастным людям в секретных службах, которым все это приходится читать. Один из несомненных уроков *Арабской весны* состоит в следующем: если вы хотите, чтобы правительство просто накрыло с головой потоком информации, генерируйте как можно больше этой самой информации (причем желательно с использованием новых коммуникационных средств, которые власти еще не успели взять под контроль). Второй закон термодинамики отлично работает в политической практике — в частности, когда речь идет о свержении правящего режима.

ИНДЕКС БЕЗОПАСНОСТИ: Используете ли вы в своей работе новейшие аналитические инструменты, такие как *прогностический анализ*, которым, в частности, пользуется американская компания *Recorded Future*? Как Вы оцениваете потенциал и эффективность использования для прогностического анализа инструментов на основе так называемых *темпоральных аналитических процессоров*?

ПАЛЛАРИС: Я знаком со многими передовыми аналитическими инструментами; некоторые их них я тестировал по заказу наших клиентов. Кое-какие из них действительно очень эффективны. Есть и такие, которые не стоят тех денег, которые за них просят.

Каким бы ни был *калибр* этих инструментов, давайте не забывать, что все эти технологии все еще находятся на очень раннем этапе своего становления. Их способность выдавать точные прогнозы зависит от большого количества переменных, которые не имеют никакого отношения к самой технологии — в том числе от качества тех исходных данных, которые анализирует система, а также от умения аналитика максимально использовать возможности системы.

В любом случае, ни одна технология никогда не сможет делать на 100% точные прогнозы — так же, как этого не сможет сделать ни один человек. К примеру, ваша система может спрогнозировать, что В. В. Путин посетит Лондон во время Олимпийских игр. Она придет к такому выводу, *прочитав* пресс-релиз президентской службы, сообщающий о таком намерении главы государства. Система извлекает все относящиеся к делу данные (имена, даты, планы, географические пункты, и т. д.), сопоставляя их с уже известной информацией (то есть с информацией о том, что в Лондоне пройдут Олимпийские игры). Затем система выдает аналитику свой прогноз действий российского лидера. Если Путин действительно решит побывать на Олимпийских играх, то система окажется права. Если он решит не ехать в Лондон, а посмотреть дома телевизор, то система ошиблась. Это, конечно, очень примитивное описание того, как работают прогностические аналитические системы, но общая идея, надеюсь, вам понятна.

Несмотря на все это, я считаю, что данное направление имеет огромный потенциал, и что оно будет привлекать самых талантливых IT-специалистов всего мира. Наше желание знать или предвидеть будущее непреодолимо. За умение это делать организации готовы платить хорошие деньги. Однако сами по себе инструменты не являются панацеей от риска и определенности. Отдать анализ и принятие решений на откуп компьютеру не получится.