ПРОМЫШЛЕННЫЙ ШПИОНАЖ - РЕАЛЬНОСТЬ В СНГ

Лихачев Ю.И., ведущий эксперт
НИЦ "Ваша Безопасность"

По фильмам про шпионов и детективам мы знаем, что шпионаж может быть государственным (политическим), военным, экономическим и т.д. Само понятие "шпионаж" означает получение или добывание каких-то сведений, представляющих определенный интерес, незаконными или законными методами. С развитием бизнеса потребность в информации о конкурентах, клиентах или партнерах становится все более важной и актуальной для успешного и стабильного функционирования фирмы. Возникает задача получить эту информацию.

Промышленный шпионаж применительно к бизнесу - это разновидность экономического шпионажа, когда задача по получению интересующей информации сужается от масштабов государства до одной или нескольких фирм-конкурентов. Таким образом, для бизнеса промышленный шпионаж - всего лишь способ конкурентной борьбы. И если в случае экономического шпионажа субъектом (стороной, которая осуществляет активные действия) является государство в лице своих спецслужб, то в случае промышленного шпионажа субъектом является отдельный предприниматель, фирма, т.е. физическое или юридическое лицо. Промышленный, или бизнес-шпионаж, обычно преследует две цели:

- проверить благонадежность делового партнера;
- вытеснить или уничтожить конкурента.

Для достижения цели необходима информация. В первом случае минимальная задача такова: необходимо убедиться, что деловой партнер действительно в состоянии выполнить свои договорные обязательства и, как говорят, вас "не кинет". Во втором случае, о конкуренте желательно знать все: источники поставок товара, готовящиеся контракты, финансовое состояние, методы работы фирмы и постоянные деловые связи, - в общем, все то, что определяет экономическое положение фирмы-конкурента. Получив необходимую информацию, ее анализируют и определяют возможность вступления в деловые отношения с партнером (если цель - убедиться в благонадежности партнера) или определяют способ воздействия на конкурента, например, перехват поставок или контрактов, переманивание наиболее ценных специалистов, передача конфиденциальной информации о конкуренте в правоохранительные органы (всегда лучше, чтобы "черную" работу делал кто-то другой). Словом, способов воздействия на конкурентов много, вплоть до физического уничтожения. Как и любой другой, промышленный шпионаж может быть открытым (легальным) или закрытым (в этом случае используются незаконные методы получения информации). Легальный бизнес-шпионаж (его еще некоторые авторы называют конкурентным шпионажем), включает в себя такие методы, как анализ прессы, рекламных публикаций и т.д. Простой анализ рекламы позволяет оценить прибыль фирмы-конкурента с точностью до 10-15%, наружное видеонаблюдение за офисом позволяет оценить число сотрудников, их материальное положение, привычки, дает возможность выяснить круг лиц, входящих в высшее звено организации. Вся эта информация может стать основой по определению кандидатов для агентурной разработки.

Нелегальный бизнес-шпионаж включает в себя:

- агентурный метод получения информации;
- технические методы получения информации (как-то: перехват телефонных переговоров, аудиоинформации, почтовых и электронных сообщений).

Агентурный метод получения информации - основа основ любого вида шпионажа. Здесь возможны два направления деятельности: или вербовка, или внедрение своего человека. Оба способа имеют место быть и имеют свои преимущества. В любой коммерческой структуре есть вторые или третьи лица, которые по своим знаниям и опыту приближаются к уровню высшего звена и которые способны самостоятельно вести свою игру. Результатом вербовки может быть то, что выгодные заказы пойдут "налево", т.е. тем лицам, которые и организовали бизнес-шпионаж в свою пользу. Если принять, что конечной целью промышленного шпионажа является уничтожение фирмы-конкурента и рассматривается вариант физического уничтожения кого-то из первых лиц, то вариант с внедрением имеет существенные преимущества, т.к. доверие к своему человеку, конечно же, больше. В свое время в Москве был отравлен известный предприниматель И.Х. Кивилиди - кто-то обработал отравляющим веществом трубку его рабочего телефона. Объектами агентурной разработки могут быть не только, скажем, вторые или третьи лица фирмы-конкурента, но и любые сотрудники любого, даже самого низшего, звена. Им вполне по силам осуществить скрытую установку соответствующей аппаратуры, которая в обиходе носит название "жучки", "комары" и т.д. Для установки такой аппаратуры необходимо от нескольких секунд до двух-трех минут, а для установки аппаратуры перехватывающей телефонные сообщения

вообще не нужно проникать в офис, достаточно найти телефониста "дядю Васю", который согласится найти искомый телефонный кабель.

Таким образом, мы перешли к техническим методам получения информации. Строго по закону, производство и сбыт такой техники преследуется в уголовном порядке и наказывается длительным сроком. Вопрос заключается только в полной юридической неразберихе, что же понимать под термином "специальные технические средства для негласного получения информации (СТС для НПИ)", ибо есть огромное количество легально продаваемой радиоэлектронной аппаратуры, например, диктофоны, бытовые видеокамеры, сотовые телефоны, радиотелефоны, бинокли и т.д., которые возможно применять для целей негласного получения информации. И есть большое количество аппаратуры, которую можно приспособить для этих целей. Например, радиостанции с широким диапазоном частот или, из другой области, медицинский эхофонендоскоп, можно использовать для снятия информации с вибронесущих конструкций стен, дверей, окон. Если помните, данный способ был продемонстрирован в хорошем новогоднем фильме "Чародеи". Классический способ промышленного шпионажа. С точки зрения автора, основным критерием признать или не признать ту или иную аппаратуру СТС для НПИ является только установленный и доказанный факт применения ее для этих целей. Если вернуться непосредственно к обсуждаемой теме, то можно сказать, что пока есть конкурентная борьба и есть необходимость получения информации, то подобная аппаратура все равно будет появляться в обращении и будет применяться. Есть спрос, будет и предложение. Из опыта работы могу привести пример: две фирмы занимались производством и монтажом шкафов-купе. Одна фирма быстро сообразила, как переманивать клиентов. Все клиенты обычно звонят по телефону, оставляют предварительный заказ и сообщают свои координаты для связи. Значит, формулируется задача: получить информацию об этих клиентах и их заказах. Задача техническими способами была решена, в результате чего менеджеры фирмы-конкурента звонили этим клиентам и предлагали им свои, более дешевые, варианты. Подобная же задача в другом случае решалась агентурным методом. Менеджер-агент посылал по сотовой связи в виде SMS-сообщений информацию о потенциальных заказчиках строительных работ своим новым хозяевам. Насколько это явление промышленного шпионажа распространено сейчас? Как говорится, официальной статистики на этот счет нет. По публикациям в зарубежной прессе в странах с переходной (т.е. неустойчивой) экономикой каждый четвертый предприниматель хоть раз сталкивался с обсуждаемой проблемой. С этими цифрами автор также может согласиться, можно еще добавить что с течением времени мы сможем прогнозировать тенденцию к увеличению подобных случаев в связи с ростом малого и среднего бизнеса в стране.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИРМЫ

Вышеописанная задача, понятно, совершенно противоположна по целям задаче промышленного шпионажа. В данном случае стоит задача максимально снизить потери от утечки информации. Но методы остаются прежними. Только приоритетным становится технический метод, а агентурному отводится роль вспомогательного. По оценкам зарубежных аналитиков, на долю человеческого фактора, т.е. на болтливость сотрудников приходится до 60% всей утечки информации. Остальные 40% - это то, что удается перехватить техническими способами, используя различные каналы утечки информации, которые можно разделить на группы.

Наиболее крупные каналы утечки информации следующие:

Акустический. Средой передачи речевой информации может быть воздух, строительные конструкции и т.д. Способ перехвата - использование специальных средств типа стетоскопов или направленных микрофонов, или средств, которые можно приспособить для этих целей.

Электромагнитный. Информация передается посредством электромагнитных волн, возникающих вокруг проводов, отдельных узлов офисной аппаратуры, используемой внутри помещения или же электромагнитные волны излучаются специально установленными техническими средствами. Способ регистрации информации - использование специальных средств.

Оптический. Носителем информации являются электромагнитные колебания в диапазонах видимого света, инфракрасного или ультрафиолетового излучений. В этом случае можно говорить о подсматривании или визуальном наблюдении. Способ перехвата - использование биноклей, видеокамер, приборов ночного видения.

Таким образом, с технической точки зрения, "болевых точек" утечки информации немного:

- сами помещения (акустика, несущие конструкции, окна);
- излучения от офисной техники;
- компъютеры (несанкционированный доступ и хакерские атаки);
- телефонная связь;

Наиболее просто можно решить вопросы по закрытию технических каналов утечки информации следующими способами. Существующими на данный момент средствами противодействия сейчас это возможно почти на 100% (какой-то процент надо оставить всегда "про запас", ибо научная мысль развивается и на всякий новый щит кто-то обязательно найдет эффективные контрмеры. Собственно, в вечной конкуренции между мечом и щитом состоит диалектика развития всей военной науки). Более сложная задача - снизить процент утечки информации из-за человеческого фактора. Человека можно предупредить об ответственности, взять с него подписку о неразглашении, но это все равно не дает полной гарантии. Следующий шаг: вербовка секретных сотрудников внутри коллектива и установка специальной аппаратуры приводит в действие комплекс проблем, где плотно переплетаются этические, юридические и экономические вопросы. И все равно эти меры позволяют только лишь снизить процент утечки информации. Человек на работе находится определенное количество часов, а все остальное время он с кем-то встречается, общается и т.д., где его почти невозможно проконтролировать. Появляется необходимость в специальной службе и периодических проверках персонала на "детекторах лжи". Автор уже говорил о вечной конкуренции между мечом и щитом. Здесь можно добавить только небольшое замечание: исторически так повелось, что затраты на хороший щит обычно на несколько порядков превосходят стоимость меча. Свои деньги всегда жалко, но отсутствие хорошего щита может привести к более серьезным потерям.