В.В. Марченко[*]

ЗАДАЧИ, ОБЪЕКТЫ И МЕТОДЫ КОНКУРЕНТНОЙ РАЗВЕДКИ И ПРОМЫШЛЕННОГО ШПИОНАЖА КАК ФОРМА НЕДОБРОСОВЕСТНОЙ КОНКУРЕНЦИИ

Современный отечественный и зарубежный опыт развития рыночных отношений ярко демонстрирует, что ни одно лицо, ни одна организация не могут эффективно действовать в условиях острой конкурентной борьбы без глубокого и всестороннего понимания рыночной среды и располагать новейшей, полноценной и достоверной информации о том, что в ней происходит. В этом смысле цель конкурентной разведки состоит в анализе деятельности конкурентов с использованием методов обработки открытой информации, используя исключительно легальные методы сбора и обработки информации, ориентируясь на открытые источники. Но существует противоположное понятие «промышленный шпионаж», которое имеет свои отличия.

Обобщая методы и формы ведения промышленного шпионажа на современном информационном пространстве, их можно объединить по следующим основным признакам:

- сбор и анализ опубликованной информации, включая официальные документы: статьи, бюллетени, рефераты и т.д. (аналитический открытый метод);

- использование сведений, разглашаемых служащими конкурирующей фирмы или получаемых в результате действий, не выходящих за рамки законности (тайный метод – проведение шпионажа и разведки);

- изучение биржевых документов и отчетов, а также финансовых отчетов конкурирующих фирм и других финансовых документов, имеющихся в распоряжении маклеров и консультантов этих фирм;

- изучение выставочных экспонатов и проспектов (брошюр), донесения различного вида, которые представляются подчиненными филиалами в центральный аппарат по существующим между ними

каналам связи (сочетание аналитического открытого и тайного технического методов);

- изучение продукции (состава, комплектующих, технологии) конкурирующих фирм;

- использование данных, полученных из бесед (проводимых в рамках закона) со служащими конкурирующих фирм (аналитический открытый метод);

- "выуживание" информации из персонала конкурирующей фирмы путем специально разработанных ("замаскированных") вопросов на научно-технических конференциях, совещаниях или симпозиумах (аналитический открытый метод);

- непосредственное наблюдение, осуществляемое скрытно (тайный метод);

- беседа при найме на работу со служащими конкурирующей фирмы без намерения принять его на вакантную должность при помощи специально разрабатываемых вопросников (аналитический открытый метод);

- организация "ложных" переговоров с фирмой-конкурентом относительно приобретения лицензии на интересующую их продукцию (аналитический полуоткрытый метод);

- наем на работу персонала конкурирующей фирмы в целях получения потенциальной производственной информации о порядке изготовления продукции или содержащейся в ней передовой технологии, и прежде всего, – НОУ-ХАУ (аналитический открытый метод);

– подкуп служащего конкурирующей фирмы или лица, занимающегося реализацией ее продукции (шпионаж);

- использование завербованного агента для получения информации на основе изучения и сопоставления переданной им информации и имеющейся документации (аналитический и тайный методы);

- подслушивание переговоров, перехват сообщений и переговоров, проводимых с использованием технических средств (шпионаж);

- кража образцов продукции, чертежей, документации по технологии ее производства и т.д. (шпионаж);

- шантаж и вымогательство (шпионаж);

- переманивание наиболее грамотной инженерно-технической элиты из конкурирующих фирм и/или из других стран, получившее название в СМИ как процесс "утечки мозгов" – (шпионаж).

Большинство преступлений, посягающих на правила конкуренции, связанные с нарушением конкурентного законодательства: Закона Шермана – Клейтона (США), Закона о недобросовестной конкуренции (ФРГ), Закона о компаниях (Великобритания), Закона Украины «О защите от недобросовестной конкуренции».

Рассмотрим основные виды преступлений против конкуренции. С некоторой долей условности их можно объединить в две группы – преступления, связанные с монополистической деятельностью и недобросовестная конкуренция. Существует известное выражение: «кто владеет информацией – тот владеет миром». В условиях предпринимательства можно сказать «кто владеет информацией – тот является лидером рынка». Ведь иметь сведения о конкурентах и партнерах, об изменениях ситуации на рынке – это не просто владение ситуацией. При умении пользоваться этой информацией – это лидерство на рынке, поэтому владельцы бизнес структур создают конкурентную разведку [4].

Конкурентная (экономическая, коммерческая, бизнес) разведка (англ. Competitive Intelligence, сокр. CI) – проводится, в рамках закона и с соблюдением этических норм, сбор и обработка данных из разных источников для принятия управленческих решений с целью повышения конкурентоспособности коммерческой организации. Но это, так сказать, законный инструмент для принятия тех или иных решений с целью получения большей прибыли от деятельности и для занятия более высоких позиций на рынке. Поскольку такое понятие в украинском законодательстве не определено, соответственно, конкурентная разведка и не запрещена, и не разрешена.

Службу конкурентной разведки нужно четко отделять от службы безопасности предприятия, так как сферой деятельности и объектами коммерческой разведки компании являются исключительно внешние

риски, возможности и угрозы, влияющие на возможность достижения компанией стратегических целей. Риски и возможности, исследуемые системой коммерческой разведки организации, имеют исключительно рыночный характер и в большей степени относятся к будущей конъюнктуры рынка и рыночных условий. В это же время сферой деятельности и объектами исследований службы безопасности, как правило, являются внешние и внутренние риски и угрозы текущей деятельности компании, имеющие криминальный характер и нарушают нормальную повседневную деятельность компании. Еще одной сферой активной разработки службы безопасности является активность конкурентного окружения, связанная с недобросовестной конкуренцией и прямолинейно претендует на нормальную деятельность компании, а также лояльность и добросовестность партнеров, сотрудников и других участников, влияющих на деловую активность компании.

Можно выделить следующие функции конкурентной разведки:

- изучение деятельности конкурентов и конкурентной среды;
- проверка надежности деловых партнеров;
- сбор информации в сети Интернет и мониторинг СМИ;
- исследование и оценка рынков или целых регионов (совместно с другими отделами, например, маркетинговым отделом);
- прогнозирование изменения ситуации на рынке и действий конкурентов;
- выявление новых или потенциальных конкурентов;
- оказания помощи руководству в процессе заимствования положительного опыта других компаний;
- получение информации законным путем и анализ новых технологий, продуктов или процессов, которые могут существенно повлиять на бизнес компании;
- выявление слабых сторон конкурентов;
- совместно со службой безопасности выявлять потенциальные источники утечки конфиденциальной информации внутри компании [1].

Существует очень похожий инструмент для принятия тех же решений – промышленный шпионаж, но он не определен в Законе Ук-

раины «О защите от недобросовестной конкуренции». По мнению многих людей, конкурентная разведка и промышленный шпионаж тождественны, но в действительности это не так. Ведь, несмотря на то, что цели этих видов деятельности часто совпадают (добыча максимально полной и достоверной информации о деятельности конкурентов), их методы отличаются.

Промышленный шпионаж – форма недобросовестной конкуренции, при которой осуществляется незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну с целью получения преимуществ при осуществлении предпринимательской деятельности, а также получения материальной выгоды. Целью промышленного шпионажа является получение данных о перспективах деятельности конкурента, производственных процессах, торговой стратегии и результаты научных исследований и промышленных разработок, об организации, продающие его товар, списков потребителей, расчетных документов.

Промышленный шпионаж может решать одну из следующих задач: получение информации о конкуренте, что само по себе при этом не всегда влечет вред для объекта шпионажа, незаконными являются лишь методы ее получения. Обычно это первый этап информационной разведки. Полученные сведения обобщаются и анализируются, после чего принимаются решения о дальнейших направлениях работы. Необходимость в промышленном шпионаже для простого сбора информации может возникнуть при разведке рынка в определенном регионе. Однако полученная информация может быть использована во вред тому, у кого она получена. Это относится к случаям перехвата выгодных сделок и инвесторов, использование сведений о работниках предприятия для получения дополнительных подходов к интересному объекту. Полученная информация также может быть выгодно продана другим конкурентам.

Внесение изменений в источники информации. Решение этой задачи возможно как активными (подделка, подчистка, стирание и т.д.),

так и пассивными действиями (невнесение данных, неисправленными имеющихся ошибок в базах данных). Наиболее часто преследуемые цели – дезинформация конкурента, введения его в заблуждение, что неизбежно влечет для него материальные потери. Например, с помощью дезинформации можно заставить конкурента заключить заведомо невыгодный контракт, перевести деньги мошенникам, нанять некомпетентных специалистов.

Уничтожения информации. Наиболее простой способ причинения вреда посредством промышленного шпионажа. Уничтожение сведений может быть выгодно, если информация является обязательным условием для решения каких-то определенных задач бизнеса. Например, для справочной службы уничтожения баз данных ведет к полной парализации работы. Для частного детективного агентства уничтожения источников информации приводит к потере добытых доказательств. Для промышленного предприятия уничтожения документации может привести к невозможности реализовать проект или к потере репутации (если документы необходимо было предоставить заказчику или в государственные органы). Уничтожаться может как сама информация (например, стирание файлов на компьютере), так и ее источники (сжигание бумаги, поломка аудионосителей). Вышеперечисленные задачи могут решаться при осуществлении промышленного шпионажа как отдельно, так и комплексно. Исходя из поставленных задач выбираются как методы ведения шпионажа, так и меры противодействия им [3].

В наше время промышленный шпионаж – довольно распространенное явление. Благодаря не честным или продажным сотрудникам, компания может попасть под атаку рейдеров или вовсе стать банкротом.

Экономической основой процветания промышленного шпионажа является конкуренция. Важным условием эффективности конкурентной борьбы является сохранение в тайне сведений, овладение которыми посторонними лицами могло бы ослабить экономические позиции предприятия и нанести ему вред. Данные сведения описываются

понятием коммерческая тайна, разглашение которой считается нарушением конкурентного законодательства.

Промышленный шпионаж не позволяет реализовать предприятию конкурентные преимущества, обесценивает значительные расходы, связанные с осуществлением исследований, опытно-конструкторских разработок и других мероприятий.

Методы промышленных шпионов аналогичные методам правительственных разведывательных организаций, поэтому для их описания используется разведывательная терминология, например:

клиентом, запрашивающим услуги на разведывательную деятельность, в промышленности является сам конкурент. Клиент определяет то, что ему нужно, определяет мертвые точки, с которых он никак не может сдвинуться и выделяет деньги на осуществление шпионажа;

шпионом является лицо, занимающееся выявлением талантов, наиболее важный элемент шпионской сети. Выявление талантов требует тщательных исследований и терпеливого наблюдения. Существует несколько методов для того, чтобы заставить людей шпионить, так как очень многие из них не хотят этого, при этом важно определить области, в которые нужно проникнуть, выявить людей, которые уже работают в этих областях, и заставить их шпионить, превращая в шпионов;

ловушка считается наиболее эффективным методом шпионажа, рассчитанным прежде всего на доверчивых людей. Эрозия лояльности, стабильности и карьеры делает заманивание в ловушку более простым. Методы заманивания в ловушку включают в себя использование любви к интригам, самолюбие, тщеславие, честолюбие, желание получить похвалу со стороны «друга», который нанял человека в шпионы.

Наиболее эффективным методом скрытного получения информации является ложное интервью, с помощью которого выявляются достижения в работе и в научных исследованиях. Эффективными методами заманивания в ловушку являются шантаж с использованием

компрометирующих сведений и деньги. Руководители агентов (резиденты) управляют работой агентов. При этом необходимо сохранять в тайне отношения резидента с агентами, иначе шпионская сеть может быть раскрыта.

Типы агентов – легальные и нелегальные. Легальный агент является сотрудником фирмы, а нелегального агента вводят в фирму по фальшивым документам[2].

Хотя метод сбора разведывательной информации с помощью агентов является основным методом разведывательной деятельности, существуют и другие методы: подслушивания и исследования выбрасываемого мусора работниками различных фирм. Это достаточно эффективные методы, так как в мусорные корзины иногда попадают документы, содержащие секретную информацию[4].

В странах Европейского Союза, а также и в Украине не принято прямых законов, непосредственно направленных на борьбу с промышленным шпионажем. В то же время законодательство некоторых штатов США рассматривает промышленный шпионаж как преступление. Владельцам бизнеса ученые советуют не быть уверенными в своей защищенности, а прибегать хотя бы к минимальным мерам безопасности:

- ответственно относиться к вопросам подбора кадров и контроля над действующим персоналом;

- устанавливать режимность в доступе к документации;

- проверять потенциальных партнеров (контрагентов) перед заключением договорных отношений;

- систематически (в зависимости от бизнеса – не реже раз в полугодие) проверять рабочие помещения на наличие скрытых устройств для негласного съема информации;

- принять в штат специалиста по информационной безопасности и внимательнее относиться к информации, хранящейся на компьютерах (в зависимости от финансового уровня – завести личный удаленный сервер и раз в день архивировать все данные именно на него);

- оборудовать рабочие помещения сигнализацией.

В Украине в настоящее время большая часть баз данных, содержащих конфиденциальную информацию, функционирует с применением минимальных средств защиты и не обеспечивает необходимого уровня конфиденциальности. Все это очень опасно, и наносит ощутимый вред как государству в целом, так и конкретным владельцам массивов конфиденциальной информации. В целом, комплексная защита конфиденциальной информации разделяется на следующие виды:

- защита от акустического контроля помещения, автомобиля, человека;

- защита от прослушивания телефонных каналов, перехвата факсимильной и модемной связи;

- защита от видеоперехвата, средств маркировки и слежения за автотранспортом;

- методы противодействия визуальному наблюдению, скрытой фото- и видео съемке;

– выявление нелояльных фирме сотрудников и обслуживающего персонала [6].

В защите существуют пассивные и активные методы. К пассивным методам относятся различные варианты установки в офисе или жилом помещении аппаратуры технического противодействия. Их существует столько же, сколько и технических средств получения информации.

К активным относятся все виды «чисток» помещений от подслушивающих устройств, соблюдение правил выбора зданий, оборудования мебелью, оргтехникой и предметами обихода, правильная защита информации, эксплуатация связной техники.

Сочетание пассивных и активных методов защиты дает гарантированный успех и называется комплексной защитой информации. В целом же, проведенные исследования показали, что идеальных технических систем, гарантируют полную защиту конфиденциальной информации, не может быть создано в принципе. На любой фирме вопросами экономической разведки, оценки партнеров и конкурентов,

прогнозирование ситуации на рынке занимается аналитическая служба. Она же занимается и контрразведкой [4].

Информационно-аналитическая деятельность фирмы – это деятельность предприятий, учреждений и организаций независимо от формы собственности, направленная на удовлетворение информационных потребностей в сфере обеспечения безопасности сотрудников и осуществления предпринимательской деятельности. Информационно-аналитическая деятельность заключается в формировании и использовании информационных ресурсов по вопросам обеспечения безопасности персонала фирмы и предпринимательской деятельности, создании и использовании информационных технологий и средств их обеспечения, защиты информации и прав субъектов рынка, участвующих в этой деятельности.

Точное количество случаев нарушения действующего законодательства при сборе конфиденциальной информации назвать никто не сможет. Тем более невозможно гарантировать вероятность наказания за это. Все стороны этого вида деятельности – законодательное обеспечение, этика, теория и практика – в Украине пока находятся на стадии становления. Но необходимо помнить, что нужно разграничивать понятия конкурентная разведка и промышленный шпионаж. Они различаются между собой по смыслу, хотя имеют общую цель. Целью, как конкурентной разведки, так и промышленного шпионажа является получение информации, которая бы дала возможность получить конкурентное преимущество на рынке. Главным отличием между конкурентной разведкой и промышленным шпионажем являются методы и способы получения информации. Все, что используется разведчиком, является законным.

Промышленный шпионаж, наоборот, предусматривает нелегальные методы и технологии. Шпионаж заключается в незаконном проникновении на территорию конкурента, снятии информации с каналов связи, слежке, подкупе, шантаже, похищении информации и т.д.

Промышленный шпионаж и конкурента разведка сегодня является неотъемлемой частью бизнеса, как в зарубежных странах, так и у

нас. При этом уровень их влияния возрастает из года в год и совершенствуется, исходя из роста информационных технологий и средств их применения. Поэтому для того, чтобы заниматься успешным бизнесом, недостаточно обеспечить только физическую защиту и охрану, а нужно учитывать и построение надежной системы защиты информации.

Библиографический список

1. Миркин С. Конкурентна розвідка або промислове шпигунство / / Ваш бізнес. – М. – 2011

2. Ткачук Т.Ю. Конкурентна розвідка / Т.Ю. Ткачук. – К. : НА СБ України, 2009. – 272 с.

3.http://ru.neospy.net/articles/slezhenie_za_sotrudnikami.php?id=10&name=promyishlennyiy_shpionaj_i_ego_tseli

4. http://newasp.omskreg.ru/bekryash/ch2p2.htm

5. Бредінскій А. Промислове шпигунство / / Торгово-промислові відомості. – М. – 2010. – №5 .

6. Скрипник Ф. Економічне шпигунство і розвідка / / Фінансовий директор. – К. – 2010. – №4.