



ХИЩЕНИЕ МОЗГОВ

Российские компании интересуются не технологическими секретами, а их авторами. Примеров удачных похищений столько же, сколько неудачных. **НАТАЛЬЯ ГОТОВА**

Помните анекдот про неуловимого Джо? Которого никто не может поймать, потому что он никому не нужен? Пикантные мероприятия, связанные с промышленным шпионажем, нужны большинству российских компаний примерно так же, как Джо. Для того чтобы у кого-то что-то украсть, надо, чтобы этот кто-то обладал неким технологическим секретом, похитив который конкурент немедленно сделает качественный скачок в развитии.

Совокупные потери мировой экономики в прошлом году из-за утечки коммерческих секретов оцениваются в \$175 млрд. Но в России пока весьма низкий уровень инновационной деятельности, и отечественные компании не обладают многомиллиардными ноу-хау, так что воровство новейших разработок в нашей

стране находится в зачаточном состоянии. Зато из-за роста конкуренции российские предприниматели начинают чаще прибегать к легальным, не нарушающим законодательство об авторском праве или о коммерческой тайне методам получения информации о деятельности соперников по бизнесу — конкурентной разведке и бенчмаркингу (сравнению собственных экономических показателей с данными других участников рынка). И наконец, самым популярным способом обезоруживания конкурентов в РФ считается «кража» у конкурентов самих создателей интеллектуальной собственности. Зачислив в активы лучшие мозги в определенной сфере деятельности, компания может не опасаться соперников. Партнер компании «ЭКОПСИ-Консалтинг» Роман Иванов говорит: «Лучшая защита — успевать придумывать новые идеи быстрее, чем у тебя их воруют».

ТАЙНА КОЛБАСНЫХ ОБОЛОЧЕК

ОСНОВНЫЕ отрасли, в которых компаниям следует опасаться тайного вторжения конкурентов, — те, где создаются новые продукты, в частности индустрия высоких технологий, IT-бизнес, фармацевтика, пищевая отрасль, модная индустрия. Подсчитать количество компаний, ставших жертвами промышленного шпионажа, эксперты не берутся, поскольку считают, что львиная доля случаев хищения конфиденциальной информации остается неизвестной широкой общественности. Фирма, ставшая мишенью конкурентов, часто боится дискредитации собственного имиджа, поэтому разбирается со шпионами втихомолку — до суда и уголовного преследования дело доходит редко.



Показателен пример производителя мясных оболочек «Атлантис-Пак», который ведет в своем сегменте разработки, внедряет инновационные продукты и усовершенствует производственное оборудование. Эта ростовская компания за несколько лет подверглась такому количеству атак со стороны конкурентов, что службе безопасности «Атлантис-Пака» в пору писать шпионский роман.

В корпоративном издании глава управления внутренней безопасности компании Равиль Бичурин рассказывает, что «есть компании, которые используют незаконные способы, стремясь найти доступ к коммерческой тайне своих конкурентов. И методы разведки достаточно разнообразны. Это и получение публикуемой в открытой печати информации о фирме, «работа» во время выставок, семинаров, изучение проспектов, буклетов, незаконное получение отчетных документов о производственной, финансово-экономической деятельности компании через государственные и коммерческие учреждения — таможенные и налоговые органы, банки». Осенью 2005 года несколько сотрудников «Атлантис-Пака» разных специальностей дружно перешли на другое предприятие, также занимающееся производством оболочек для колбас и сосисок. Людей привлекла более высокая зарплата — это тоже один из приемов разведки. «Конкуренты могут размещать в газетах объявления о поиске работников для своих предприятий

и филиалов и на собеседовании узнавать ценную информацию о нашей фирме, а также принимать бывших наших сотрудников к себе на работу», — говорит Равиль Бичурин. В объявлениях, размещенных рыночными соперниками «Атлантис-Пака», даже рабочим предлагали зарплату в размере 45 тыс. рублей в месяц. Желающих оказалось немало, но кадровые службы отказывали всем, кроме сотрудников «Атлантис-Пака». Уже через пару месяцев,

КОНКУРЕНТНЫЕ РАЗВЕДЧИКИ

добывают секретную информацию и на выставках

когда перебежчики раскрыли всю известную им внутреннюю информацию «Атлантис-Пака», их уволили.

Классических «засланных казачков» в «Атлантис-Паке» ловили несколько раз. В 1997 году в компанию устроился



оператором экструзионной линии человек, который, как выяснилось позже, был связан с украинскими конкурентами россиянина. Внедренец завербовал нескольких сотрудников «Атлантис-Пака», которые за \$50—70 передавали шпиону ксерокопии технической документации, образцы сырья, готовой продукции. Через 11 месяцев украинский агент 007 возвратился в родную компанию, которая попыталась внедрить технологии, выведенные в ростовской фирме. В марте 2004 года работник «Атлантис-Пака» попытался похитить секретную информацию по технологии подготовки производства, скачав данные с одного из компьютеров при помощи часов с flash-накопителем. Шпионские игры так понравились сотруднику, что он никак не мог смириться с увольнением и предлагал деньги, чтобы вернуться на свое полное тайн рабочее место. В 2005 году один из работников компании украл из компьютерной базы своего предприятия документы, составляющие коммерческую тайну. Разоблаченного злоумышленника арестовали и открыли уголовное дело по ст. 183 УК РФ (разглашение коммерческой тайны). В этом же году конкуренты продолжили попытки вербовать сотрудников «Атлантис-Пака». Например, некий оператор сушки Проценко умудрился похитить с предприятия несколько подлинных документов и несколько копий. Заказчики заплатили за ворованные бумаги сумму в размере месячной зарплаты. Через некоторое время должностное преступление было раскрыто, но нелояльный сотрудник раскаялся, и компания не стала преследовать его в уголовном порядке.

(СЛЕВА НАПРАВО) ФОТОХРЕС: ДМИТРИЙ КОРОБЕЙНИКОВ/ЗЕРКАЛО, ФОТОХРЕС

Начальник отдела продаж «Атлантик-Пака» Игорь Переплетчиков сказал *«BusinessWeek Россия»*, что в конечном счете шпионская история пошла предприятию на пользу, поскольку конкуренты дискредитировали себя на рынке. «Мы постарались, чтобы эти случаи стали известны профессиональному сообществу, которое не одобряет подобных методов. Кроме того, раз у нас есть что воровать, значит, мы чего-то стоим».

«ВЕРОФАРМ» ОСТАЛСЯ С ПОХМЕЛЬЕМ

ЕЩЕ ОДНА тенденция, связанная с хищениями конфиденциальной информации, при этом напрямую под понятие промышленного шпионажа не попадающая, — это «заимствование» раз-



работок у независимых ученых, нередкое в российской фармацевтической отрасли. Представитель одной компании говорит, что для российского фармбизнеса, не располагающего огромными бюджетами на R&D, наиболее эффективным является сотрудничество с учеными, которые генерируют оригинальные идеи. У разработчиков нет средств на многолетнее тестирование и регистрацию продукта, поэтому они обращаются к крупным участникам фармрынка. Но иногда компании поддаются искушению зарегистрировать патент самостоятельно, не поделившись доходами с автором идеи.

В 2006 году холдинг «Отечественные лекарства» вывел на рынок препарат от похмелья «Зорекс», созданный старшим научным сотрудником Московского научно-практического центра наркологии кандидатом биологических наук Сергеем Зеновичем.

Разработчик сначала решил показать новую лекарственную формулу, основанную на веществе унитиол и пантотенате кальция, «Верофарму». Через некоторое время фармхолдинг объявил, что унитиол был синтезирован еще в середине прошлого века и широко известен в качестве антидота к отравляющим веществам. Поэтому не будет ничего страшного, если компания выпустит на основе этого вещества лекарство под другим брендом. «Отечественные лекарства» использовали ситуацию в свою пользу, профинансировав судебные разбирательства в защиту патентных прав ученого. Разумеется, право управления продажами «Зорекса» Сергей Зенович предоставил именно «Отечественным лекарствам».

НА РЕЙДЕ

ЗАМЕСТИТЕЛЬ директора по обеспечению экономической безопасности группы компаний «Бородино» Андрей Акимов считает, что целью промышленного шпионажа может быть не только целенаправленная конкурентная борьба: «Вокруг любой большой и успешной компании, в том числе и нашей, всегда находятся желающие сделать свой маленький бизнес с использованием средств конкурентной разведки». Сфера деятельности ГК «Бородино» достаточно обширна, от строительства и машиностроения до пищевой индустрии. Именно поэтому группу нередко атакуют фирмы, старающиеся узнать секреты ее успешности или собирающие информацию для продажи заинтересованным лицам. «Мы скорее отнесли бы такие попытки к сфере конкурентной разведки, нежели к промышленному шпионажу или бенчмаркингу, — говорит Андрей Акимов. — При построении системы защиты информации компания опиралась на классические направления: объектовая безопасность, кадровый мониторинг, IT-безопасность. Нам удалось создать систему, в которой организационные, кадровые и технические механизмы работают эффективно. Что касается кадрового шпионажа, то откровенно засланных казачков у нас было не так много. Были попытки проникновения на наш завод в Кимрах, сбора информации по производству в Конаково. Гораздо больше примеров недобросовестного ведения бизнеса в торговой сфере и строительстве, в том числе с предварительной разведкой». Кроме того, в течение двух лет служба безопасности группы неоднократно диагностировала попытки удаленного «тестирования на прочность» информационной сети. Называть «поименно» злоумышленников Андрей Акимов не стал, заметив, что группа не ставит задачи найти и наказать их — все равно система защиты, включающая не только программно-технические средства ведущих мировых производителей, но и собственные ноу-хау ГК «Бородино» в области антивирусов и защищенного документооборота, блокирует подобные действия.

Еще одним мотивом для использования шпионажа и конкурентной разведки является возможная рейдерская атака или попытка недружественного поглощения компаний-мишеней. «В прошлом году мы завершили мероприятия по защите от недружественного поглощения в отношении одного из наших предприятий. Естественно, атакующая сторона не обошлась без применения известных разведывательных приемов. Нам пришлось мобилизоваться и по техническим средствам защиты, и по организационно-правовым направлениям», — рассказывает Андрей Акимов.

ЦЕНА ВОПРОСА

\$50 млн.

объем российского рынка информационных систем безопасности в 2006 году

\$95 млн.

прогнозируемый объем этого рынка в 2007 году

\$300 тыс.

средняя цена проекта внедрения комплексной защиты конфиденциальной информации в российской компании

Источник: InfoWatch

ПЛАГИАТОРЫ

В МОДНОМ бизнесе, а также во многих сегментах FMCG промышленный шпионаж и конкурентная разведка в последнее время абсолютно привычное дело. Копируют все и вся, причем уже не во время презентации коллекции на подиуме, а еще на стадии подготовки дизайнерских эскизов. По словам гендиректора компании Fashion Consulting Group Анны Лебсак-Клейманс, чаще всего заимствование эскизов моделей происходит либо при переходе сотрудника из

одной компании в другую, либо у дизайнера-фрилансера, работающего в различных компаниях, либо на выставках. «Примеров очень много, копируют творческие идеи как у российских компаний, так и у европейских», — говорит глава FCG. Как и в других сегментах бизнеса, промышленный шпионаж в моде связан с заимствованием объектов, которые защищаются законодателем: упаковка, торговый знак, фирменное наименование, коммерческие документы и пр. А конкурентная разведка — это «сарафанное радио». Информация, полученная таким образом, не подлежит защите, а подобные действия не подпадают под уголовную ответственность. Многие профессионалы индустрии моды признают данные действия не противоречащими закону, рассматривая их как «стратегию преследования лидера». «Например,

**НОВЫЕ
ЛЕКАРСТВЕННЫЕ
формулы часто крадут**

ны варианты мотивов действий инсайдеров, выявленных компаниями. Руководитель аналитического отдела InfoWatch Алексей Доля прогнозирует, что мотив промышленного шпионажа не превысит 1—2% от числа респондентов. Пока среди инсайдерских утечек лидирует либо халатность, либо саботаж со стороны сотрудников, обиженных руководством.

А вот вопросы защиты от похищения кадров «на вес золота» становятся по мере развития конкуренции все более актуальными для российских компаний. Партнер «ЭКОПСИ Консалтинга» Роман Иванов отмечает, что фирмы должны тщательно продумывать, как удерживать от бегства к конкурентам отдельные категории специалистов, которые не относятся к менеджерам и поэтому зачастую не имеют в системе мотивации базовой страховки от

**ВЫСОКАЯ
МОДА
не всегда творчество**

дельные категории специалистов, которые не относятся к менеджерам и поэтому зачастую не имеют в системе мотивации базовой страховки от



Zaga построила империю, руководствуясь именно этой стратегией, — отмечает Анна Лебсак-Клейманс. — Поэтому компании, работающие на модном рынке, все чаще относятся к промышленному шпионажу как к творческому заимствованию. Правда, это в основном касается крупных корпораций, которые поняли, что одна, пусть даже и гениальная модель ничего не решает. Вопрос успеха заключается скорее в том, чтобы попасть в ту модную струю, которая окажется востребованной потребителем. Чем мельче компания, тем больше она боится промышленного шпионажа, считая, что, придумав уникальный дизайн, достигнет успеха на рынке».

КАДРЫ — НАШЕ ВСЕ

СОГЛАСНО итогам опроса представителей бизнес-сообщества и экспертов, основные тренды конкурентной разведки и промышленного шпионажа — использование человеческого фактора при хищении конфиденциальной информации физически или через информационные носители, а также переманивание ценных кадров, являющихся носителями интеллектуальной собственности компании.

По данным разрабатываемой технологии для информационной безопасности компании InfoWatch, которая провела в конце 2006 года опрос среди российских компаний относительно угроз информационной безопасности бизнеса, пока лишь несколько респондентов сталкивались в своей практике с инсайдерами, действующими умышленно. Намного чаще служащие допускают ошибки по незнанию. В анкетировании, которое InfoWatch проведет в ноябре этого года, в перечень вопросов будут включе-

КОМУ ЭТО ВСЕ НАДО
Системы внутренней ИТ-безопасности наиболее востребованы в банковском секторе, телекомах, страховом бизнесе, на предприятиях розничной торговли и ТЭКа. Это связано с тем, что такие компании работают в условиях высокой конкуренции, оперирования большим количеством персональных данных, а также имеют стратегическое значение для экономики.

Источник: InfoWatch.

перекупки. К таким категориям относятся технологи, разрабатывающие банковские продукты, например автокредитование, ипотечное и потребительское кредитование, создатели тарифов и новых услуг в телекоммуникационной отрасли, разработчики рецептур в «пищевке», инженеры-технологи в промышленности, особенно в атомной энергетике, где за дефицитными высококвалифицированными ИТР охотятся не только российские предприятия, но и активно развивающие атомную энергетику китайцы. «Это носители интеллектуальной собственности

компании, и руководство должно работать над тем, чтобы их удержать», — говорит Роман Иванов. При этом простое повышение зарплаты вряд ли поможет сохранить сотрудника. «Это приводит скорее к обратному эффекту — если человек много получает, его легко вычислить. Профессионалы чувствуют собственную значимость и могут начать шантажировать компанию своим уходом». Компаниям следует действовать так, чтобы сотрудник чувствовал себя честным, порядочным и не способным на предательство человеком. ■

(СЛЕВА НАПРАВО) ВАСИЛИЙ МОРЕВ/ИТАР-ТАСС; СЕРГЕЙ АВДУЕВСКИЙ