БЕЗОПАСНОСТЬ БИЗНЕСА

Д. В. Зеркалов

КОНТРРАЗВЕДКА И ШПИОНАЖ

В четырех книгах

Книга 2

Хрестоматия

Киев

Видавництво
Науковий світ®
2008

ББК 65.290
З-57

Рецензенты: *И. М. Аксенов* – полковник СБУ в отставке, канд. экон. наук; *А. И. Баскаков* – начальник Департамента МВС Украины; *С. В. Тандура* – директор ТОВ "digital and analog systems" (защита информации).

Зеркалов, Д. В.
З-57 **Контрразведка и шпионаж** : хрестоматия / Д.В.Зеркалов. – К. : Наук. світ, 2008. – 109 с. – (Безопасность бизнеса : в 4 кн. ; кн. 2).

ISBN 978-966-675-564-6

Обобщен международный и отечественный опыт использования спецслужб в современных условиях. Описана их структура на уровне государства и предприятия, а также работа по пресечению разведывательной деятельности и промышленного шпионажа недобросовестных конкурентов, мошенников, криминальных элементов. Рассмотрены история и особенности этой работы.

Для преподавателей и студентов высших учебных заведений, руководителей и менеджеров компаний, коммерческих структур, специалистов по безопасности бизнеса, организаций, учреждений и органов исполнительной власти, полезна широкому кругу читателей.

ББК 65.290

ISBN 978-966-675-564-6

Шановні читачі!

Національна безпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам.

Одними з пріоритетів національних інтересів України є гарантування конституційних прав і свобод людини і громадянина; створення конкурентоспроможної, соціально орієнтованої ринкової економіки та забезпечення постійного зростання рівня життя і добробуту населення; збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку.

Серед реальних та потенційних загроз національній безпеці України та стабільності в суспільстві на сучасному етапі є поширення корупції та хабарництва в органах державної влади, організованої злочинної діяльності, нестабільність у правовому регулюванні відносин у сфері економіки, відсутність ефективної програми запобігання фінансовим кризам; зростання кредитних ризиків; критична залежність національної економіки від кон'юнктури зовнішніх ринків, недостатні темпи диверсифікації джерел постачання енергоносіїв та відсутність активної політики енергозбереження, „тінізація" національної економіки, переважання в діяльності управлінських структур особистих, корпоративних, регіональних інтересів над загальнонаціональними.

Зважаючи на це гостро потребує подальше вдосконалення правового, інтелекттуального та інформаційного забезпечення безпеки підприємницької діяльності будь-якої форми власності.

Серія «Безопасность бизнесу» в 4-х книгах містить систематизовану та структуровану інформацію щодо міжнародного та вітчизняного досвіду забезпечення безпеки та захисту підприємницької діяльності, розкриває методи та особливості розвідки, контррозвідки та шпіонажу, доволі повно та досконало висвітлені економічні проблеми та аспекти безпеки, надані рекомендації з безпеки здійснення та захисту ведення бізнесу в сучасних умовах.

Зазначена хрестоматія, на мій погляд, це вагомий здобуток та подія для керівників та працівників різних галузей економіки, фахівців з безпеки бізнесу, організацій, установ та органів виконавчої влади, викладачів та студентів навчальних закладів, а також широкому колу читачів.

З повагою,
Начальник Департаменту МВС України О.І. Баскаков

1. Служба контрразведки MI5*

Генеральный директор Джонатан Эванс (с 20.04.07),
до него Элиза Мэннингэм-Буллер
(Eliza Manningham-Buller до апреля 2007 г.

Методы работы, структура и другие характеристики всех основных разведок и контрразведок мира примерно одинаковы. Поэтому рассмотрим деятельность контрразведки на примере известной своим коварством британской так называемой «Службы безопасности М15».

Долгое время в британской контрразведке считали главным врагом не террористов, а шпионов из стран Советского блока, экстремистские политические движения и профсоюзы, подрывающие основы государственного устройства. Методы MI5 были под стать целям – внедрение и вербовка агентов в левацкой среде, прослушивание телефонов лидеров политических партий, при обнаружении шпионов – долгая, иногда многолетняя оперативная игра в стиле Мюллера и Штирлица.

В этом британцы были похожи на своих коллег из КГБ – закрытый элитарный клуб сотрудников, слежка за собственными гражданами, боязнь шпионов и предателей. В создавшейся системе британским контрразведчикам было вполне уютно. Любопытно, что когда перебежчики из советской разведки в конце 80-х рассказывали британцам о том, что КГБ вовсе не столь успешно работает в Англии, как им это представляется, руководство MI5 не прислушивалось к этому. Им было бы удобнее, чтобы КГБ оставалось страшной угрозой для Британии, на борьбу с которой можно получать большие средства.

Однако Холодная война кончилась, и главным врагом стал террорист. Еще с 70-х Великобритания постепенно превращалось в убежище для политических диссидентов со всего Ближнего Востока. В результате очень быстро страна превратилась в поле битвы для террористов исламистского толка. Британским спецслужбам пришлось меняться. Однако путь реформ, который они выбрали, не похож на российский.

Ирландский вопрос

Исторически, MI5 практически не действовала в Северной Ирландии, имея там лишь одного офицера связи (в Белфасте). Борьбой с ИРА занимались полицейское подразделение Royal Ulster Constabulary (RUC) (4 ноября 2003 года RUC была переименована в Police Service of Northern Ireland (PSNI)), военная разведка и спецподразделение местной полиции. Внутри MI5 долгое время считалось, что теракты должна расследовать полиция. В самой Британии за борьбу с ирландскими террористами отвечали спецподразделения местной полиции (Metropolitan Police Special Branch – MPSB).

---

* Основной источник информации: Defending the realm / Inside MI5 and The War On Terrorism. Mark Hollingsworth and Nick Fielding.

Ситуация изменилась в начале 90-х, когда MI5 возглавила Стелла Римингтон, которая решила превратить контрразведку в главное ведомство Британии по борьбе с терроризмом. Это вызвало противодействие офицеров MPSB, которые ссылались на отсутствие у MI5 опыта в борьбе с террористами. Весной 1992 после волны терактов в Лондоне MI5 победила в этом противостоянии. Вскоре в службе было создано новое подразделение антитеррора – T Branch в составе 75 человек. В середине 90-х в T Branch были переброшены лучшие офицеры из F Branch (борьба с подрывной деятельностью) и K Branch (контршпионаж). С того момента MI5 стала координировать спецподразделений местной полиции в борьбе с террором. Из собственно отделов MI5 в Северной Ирландии действует только служба наружки A4.

Смена методов

По ходу работы выяснилось, что для борьбы с террористами прежняя технология – долгосрочная разработка террористических групп – не эффективна. В середине 90-х случалось, что MI5 допускала некоторые теракты со стороны ИРА только для того, чтобы не сорвать многолетнюю оперативную игру.

Однако Аль-Каида оказалась намного опаснее, чем ИРА: не сравнимое число жертв, кроме того, из-за использования шахидов террористическую сеть стало сложнее отслеживать. Да и структура террористических ячеек болееподвижна, чем у ИРА. В результате сегодня полиция настаивает на немедленном аресте террористов, как только о них становится известно, в то время как MI5 пытается сохранить старые методы «долгой игры».

Теперь главная задача MI5 – выявить угрозу на ранней стадии. Основываясь на информации британской радиоэлектронной разведки GCHQ и ее американского коллеги NSA, MI5 регулярно рассылает такие предупреждения по защищенной электронной почте заинтересованным министерствам, а также большим корпорациям, в частности British Petroleum и Shell, из-за потенциально высокой угрозы их объектам.

Ориентировки, выпускаемые MI5, циркулируют в очень узком кругу. Он включает Даунинг стрит, 10 (резиденцию премьер-министра) и ключевых министров. Если информация носит исключительный характер, то она направляется напрямую премьер-министру Тони Блэру сэром Дэвидом Омандом (David Omand), координатором кабинета по вопросам безопасности и разведки. Так было, например, в феврале 2003 года, когда из-за угрозы теракта спецподразделения и танки ввели на территорию аэропорта Хитроу.

Один из приоритетов контртеррористической борьбы MI5 – отслеживание студентов из мусульманских стран, поскольку они являются объектами вербовки экстремистами. Но и здесь приходится соблюдать права человека. Так источник в MI5 заявил «Гардиан»: «Мы можем выявить этих лиц, но мы не можем выслать их на родину, где не соблюдаются права человека. Многие из них разыскиваются Индией, Египтом, Россией или Турцией и получат обвинения в терроризме, если вернутся. Мы не можем вышвырнуть их только потому, что они мусульмане».

Между тем, в конце 90-х для слежки за юными мусульманами в MI5 был создан специальный отдел. Кроме того, контрразведчики попросили универси-

тетские власти обращать особое внимание на студентов с Ближнего востока, особенно тех, кто изучает дисциплины, которые могут быть использованы для создания оружия массового поражения.

Бюджет

Бюджет MI5 (сейчас он оценивается в 200 миллионов) распределяется следующим образом: 56,9% на контртерроризм, 14,4% – контршпионаж, 11,5% на борьбу с серьезными преступлениями и 11% – на обеспечение безопасности правительственных зданий.

Персонал

Столкнувшись с Аль-Каидой, руководство MI5 увеличило штат на 25%, доведя его до 2400 сотрудников. Однако этого оказалось недостаточно, необходимо было изменить сам принцип комплектования спецслужбы.

MI5 всегда испытывала проблемы с набором новых сотрудников. Новобранцев подбирали по семейным связям, в университетах, среди общих знакомых и проч. В результате MI5 превратилась в некий закрытый клуб выпускников Оксфорда и Кембриджа, бывших колониальных чиновников и армейских отставников. Эти люди прекрасно работали на Уайтхолле, но действовать где-нибудь в восточном Бэлфасте им было проблематично.

Впервые изменить принцип комплектования решили только в середине 70-х, когда обнаружилось, что большинство предателей, завербованных КГБ и внедренных в MI5, закончили как раз Кембридж или Оксфорд. Тогда решили набирать людей из более широкого социального круга. Однако при Маргарет Тетчер реформа забуксовала – амбициозные молодые люди предпочитали работу в Сити, и основной поток новобранцев формировали бывшие полисмены и отставные военные.

Лишь в 90-е годы MI5 удалось привлечь в службу другой пласт людей. Прежде всего благодаря изощренной рекламной кампании в прессе. Так, Дэвида Шейлера, бывшего сотрудника MI5, впоследствии раскрывшего множество тайн своей службы, как человека творческого и образованного, удалось завербовать объявлением, начинавшимся фразой «Годо никогда не придет». Суть объявления – нечего ждать у моря погоды, надо брать судьбу в свои руки и идти в контрразведку.

Согласно данным Дэвида Шейлера, до 1994 года офицеры MI5 вербовались только из тех, кто имел дедушек и бабушек, родившихся в Великобритании. В результате в Службе почти не оказалось сотрудников, которые могли бы заниматься проникновением в исламские экстремистские организации. Первый темнокожий офицер появился в MI5 только в середине 90-х. Сейчас черных в штате Службы 3%, и ни одного – в высшем руководстве MI5. Служба изменила свою политику только в 1998 году, когда разместила в газетах рекламные тексты, призывающие поступать на службу британских мусульман. В 2000 году такие объявления появились в этнических газетах -- Eastern Eye и New Nation – под заголовком «Жизнь, лишенная обыденности».

В феврале 2004 года MI5 решила увеличить свои штаты, причем довольно существенно. К 2 тысяч нынешних сотрудников было решено привлечь еще

тысячу. MI5 понадобились сотрудники для кабинетной работы — лингвисты и аналитики.

Технологии

Впервые компьютерный учет досье MI5 появился в конце 1977 года. Однако идея создать единую базу данных контрразведки появилась только спустя десять лет. Проект получил название «Grant», однако ему сразу была уготована плохая судьба из-за отказа MI5 использовать программное обеспечение, разработанное на стороне. Исходя из интересов безопасности, MI5 предпочла бы, чтобы все было создано внутри самой службы. В результате все равно пришлось обратиться к людям без погон – были наняты специалисты из соответствующих корпораций. Им пришлось платить по рыночным ценам, что резко увеличило затраты на создание Grant. В результате Grant стоил службе 25 млн фунтов, и получился крайне неудобным в использовании. Предполагалось, что новая информационная система будет единой для трех служб – MI5, МИ6 и GCHQ. Однако в 1997 году лишь 40% персонала MI5 получило к ней доступ. В результате MI5 пришлось купить по принтеру каждому офицеру, хотя изначально предполагалось, что Grant избавит службу от лишних бумаг.

Не повезло и другим компьютерным системам MI5. Например, базе данных Hawk, где должны были храниться файлы с информацией на политически неблагонодежные движения, за которыми следило подразделение F Branch. П создавали Hawk, угроза от этих движений резко уменьшилась и база стала не нужна. А поскольку Hawk был создан специально для мониторинга политической активности, для других подразделений MI5 программа не годилась. Не повезло и подразделению антитеррора T Branch. Для него была создана база данных Durbar. От нее пришлось отказаться из-за массовых отказов (например, многие документы оказались без даты, а на запрос по связям разрабатываемого лица с террористами компьютер выдавал только ответ «да» или «нет», но не выдавал имена).

Международное сотрудничество

В июне 2003 года в MI5 был создан Joint Terrorism Analysis Centre (JTAC). Руководитель JTAC подчиняется генеральному директору MI5, однако Центр действует как отдельная структура, в составе которого работают сотрудники 11 правительственных агентств и департаментов. В MI5 Центр тесно сотрудничает с управлением International Counter Terrorism branch.

JTAC является одним из трех элементов глобальной антитеррористической сети, создаваемой США, Великобританией и Австралией с лета 2004 года. Кроме JTAC, в эту сеть входят австралийский NTAC (National Threat Assessment Centre) и американский TTIC (Terrorist Threat Integration Center). Сеть должна предотвращать акции «Аль-Каеды» и союзных ей группировок на всей территории земного шара.

Штаб-квартира MI5

В начале 90-х службы MI5 размещались в пяти различных зданиях в центральном Лондоне. Это приводило к путанице, потере документов, а главное – в новых изменившихся условиях, когда иногда дело решают минуты, британцы не успевали координировать операции.

Было принято решение свести всех сотрудников контрразведки в одно здание. Для новой штаб-квартиры был выбран так называемый «Темз Хаус», здание в духе нео-классицизма, построенное сэром Фрэнком Бэйнсом в 1928 году на набережной примерно в 300 метрах от парламента. Ранее это здание использовалось как штаб-квартира Департамента энергетики, но оно было полностью перестроено и перепланировно. Реконструкция продолжалась три года и стояла бюджету 265 миллионов фунтов стерлингов. Они были закончены в 1994 году.

В результате в здании появились офисы для 2,300 человек персонала и подземная парковка на 800 мест. Комнаты офицеров оформлены в современном стиле – светло-серые тона и стеклянные перегородки. В здании, кроме гимнастического зала и зала для аэробики, предусмотрели даже два бара, но они не используются офицерами из-за запрета на курение и опасения попасться на глаза начальства в «неподобающей» компании. Кабинет генерального директора находится на пятом этаже напротив библиотеки. Для доставки досье из хранилища предусмотрена мини-железная дорога, доставляющая документы в специальных емкостях на все восемь этажей. Правда, до сих пор ходят слухи о явно завышенных затратах на постройку здания, так как только один квадратный метр ковра в ресторане для руководства стоит не менее 70 фунтов. Кстати, только заказанное французскому скульптору шестифутовое изваяние креста MI5 (так выглядит герб службы) стоило 25 тысяч фунтов. Конечная цена новой штаб-квартиры превысила два годовых бюджета МИ5 (первоначальная смета была 85 млн фунтов стерлингов).

Поначалу фешенебельным видом новой штаб-квартиры MI5 обманывались не только туристы, которые принимали ее за Тэйт Галлери, но и люди более информированные. Например, так ошибся лидер партии Шин-Фейн (легального крыла ирландских националистов) Мартин Макгиннес, который зашел в здание, думая, что это штаб-квартира лейбористской партии. Он подошел к стойке в холле, назвал себя и попросил позвать своего друга. Шокированные сотрудники безопасности попросили его присесть и вызвали руководство. В этот момент волна паники охватила уже все здание. В конце концов кто-то подошел к Макгиннесу и очень мягко указал ему, куда тому нужно пройти, чтобы попасть в нужное ему заведение.

Бойцы

Для проведения силовых акций, осуществления наружного наблюдения, вербовки агентов и проч. MI5 до сентября 2006 года активно использовала офицеров так называемых Metropolitan Police Special Branch (MPSB) – спецподразделений местной полиции. Их называли «глазами и ушами» MI5. Их роль – поддержка операций контрразведки на местном уровне. Отлично образованные офицеры MI5 смотрели на сотрудников MPSB свысока, считая их «рабочими лошадками». Они действительно чаще «работали в поле». А одно из них – MPSB Скотланд-Ярда – обеспечивало безопасность премьер-министра. Кстати, шефом этого подразделения 1 декабря 2003 года впервые в истории была назначена женщина – Джанет Вильямс.

2 октября 2006 года на базе двух полицейских подразделений – спецподразделения Metropolitan Police Special Branch /MPSB/ и Антитеррористического

управления SO13 была сформирована новая структура – контртеррористическое подразделение SO15. Его штат – около 2 тыс. сотрудников.

Для захватов террористов, шпионов и проч. используются подразделения армейского спецназа SAS (Специальной авиадесантной службы). В отличие от ФСБ, MI5 отнюдь не стремится класть яйца в одну корзину, создавая у себя собственной спецназ, тюрьму, авиаотряды, пограничные войска и проч.

Структура MI5

Высшее руководство

- Director-general / Генеральный директор / Джонатан Эванс
- Deputy Director-general / Заместитель генерального директора / В настоящее время мистер Фрэйзер Уилсон (Fraser Wilson)
- Director and Co-ordinator of Intelligence (responsible for Northern Ireland) / директор и координатор по разведке (отвечает за Северную Ирландию) /
- Legal Adviser (Правовой советник)

Департаменты

A Branch -Оперативная поддержка

- A1A: технические операции, скрытое проникновение, прослушка, камеры наружного наблюдения CCTV.
- A1F: то же самое, но в отношении долгосрочных объектов – посольств и проч.
- A2A: Переводы перехваченных сообщений
- A3 и A5: Техническая поддержка операций. Включает специальную скрытую фотосъемку и прочее оборудование для скрытого проникновения.
- A4: Мобильные и стационарные подразделения наблюдения.

B Branch – Людские ресурсы

- B1: Безопасность Службы, включая обеспечение безопасности здания и сотрудников MI5
- B2: персонал
- B7: Обучение и набор сотрудников

D Branch - Нетеррористические организации

- D1: Проверка людей вне MI5
- D4: Контршпионаж против России и Китая
- D5: Работа с агентами этого branch
- D7: Организованная преступность

G Branch - Международный терроризм

- G2P: Борьба с распространением терроризма
- G3A: Координация подразделений, борющихся с угрозой терроризма
- G3C: Противодействие терроризму в тех частях мира, которые не покрываются G Branch
- G6: Работа с агентами G Branch
- G9A: Противодействие ливийским, иракским, палестинским и курдским террористическим группам
- G9B: Борьба с угрозой иранского государственного терроризма и иранских диссидентских групп
- G9C: Борьба с исламскими экстремистами

H Branch - Корпоративное подразделение

▪ H1 и H2: Контакты с Уайтхоллом и СМИ. Занимается финансовыми запросами Службы. Отдел также отвечает за контакты с полицией, таможнями, портами и иммиграционными властями. Также отвечает за информационные технологии в Службе.

▪ H4: Финансы

▪ Следующие отделы также включены в состав H Branch:

▪ R2: Главная регистратура

▪ R5: Секретные досье. Файлы с ограниченным доступом

▪ R10: Регистратура для временных досье.

▪ R20: Отвечает за распределение материала, полученного от GCHQ.

T Branch - Ирландский терроризм

▪ T2A: Расследует республиканский и лоялистский терроризм в самой Британии

▪ T2B: Контакты с местными спецподразделениями и агентами

▪ T2C: Оценка угроз от ирландских террористических групп

▪ T2D: Исследования тергрупп

▪ T2E: Контакты со спецподразделением Metropolitan Police Special Branch, базирующемся в Скотланд-Ярде

▪ T5B: Расследования продаж оружия

▪ T5C: Противодействие ирландскому терроризму в континентальной Европе, включая республику Ирландия

▪ T5D: Противодействие ирландскому терроризму в других частях света

▪ T5E: Изучение террористической логистики

▪ T8: Работа с агентами T Branch; включает отдел, базирующийся в Северной Ирландии

PS. MI5 также имеет офицеров связи в центрах в Германии, Вашингтоне и на Кипре.

▪ Английская версия структуры

История службы (официальная версия MI5)

В октябре 1909 года, следуя рекомендации Комитета имперской безопасности, в которой указывалось на опасность немецкого шпионажа для британских портов ВМФ, капитан Вернон Келл (Vernon Kell) южностаффордширского полка и капитан Мэнсфилд Камминг (Mansfield Cumming) из Королевского флота вместе создали бюро Секретной службы.

Получив дополнительный запрос от Адмиралтейства информации о новых немецких кораблях, Келл и Камминг решили разделить их работу. В результате «К» стал отвечать за контрразведку (будущую MI5), а «Си» – за шпионаж (MI6).

С 1909 года до начала Первой мировой войны бюро Секретной службы выявило более чем 30 шпионов, входящих в сеть Германской разведслужбы. В это время бюро состояло всего из 10 человек, включая Келла. В начале войны бюро было переподчинено военному кабинету. В январе 1916 года бюро стало частью нового Управления военной разведки (Directorate of Military Intelligence) и получило наименование MI5.

Во время войны функции MI5 были расширены, и теперь они включали координацию политики правительства в отношении союзников, вопросы безопасности и проч. MI5 также начало заниматься контрразведкой по всей Европе. К концу войны, во время которой были пойманы 35 шпионов, штат MI5 состоял уже примерно из 850 сотрудников. Детали о работе MI5 в этот период доступны в отчетах службы за этот период в архивах Public Record Office, рассекреченных в ноябре 1997 года – www.pro.gov.uk/releases/.

После революции 1917 года в России, работа MI5 стала включать предупреждение коммунистической угрозы и саботажа в армии. Эти угрозы получили дополнительный резонанс в середине 20-х, после публикации неизвестного письма Зиновьева, в котором Коминтерн назначался ответственным за поддержку британской коммунистической партии, которая должна заниматься саботажем внутри Империи. Это письмо вызвало фурор. Расследование, проведенное недавно историками Форин Офиса, показало: «Разведка царской России была отлично организована. Вполне возможно, что ее агентура использовалась белыми для того, чтобы сфабриковать документ, который разрушал англо-советские связи и должен был привести к краху лейбористское правительство…» (‘A most extraordinary and mysterious business’: The Zinoviev Letter of 1924, by Gill Bennett, Chief Historian, FCO).

15 октября 1931 года формальная ответственность за предупреждение угроз национальной безопасности Соединенного Королевства в части борьбы с ирландскими террористами и анархистами, также была возложена на MI5. Эта дата считается днем создания «Секретной службы». Это название заменило «MI5» в обиходе.

После прихода Гитлера к власти, новая служба должно было бороться с новой угрозой фашизма. В начале 1939 года Служба насчитывала только 30 офицеров и ее отдел наблюдения состоял всего из шести человек. Вскоре после начала Второй мировой войны, Секретная служба переехала в здание тюрьмы «Вормурд Скрабс», однако в конце 1940 года большая часть аппарата Службы была эвакуирована в Бленхейм Пэлас (Blenheim Palace). В сентябре 1940 года большая часть архивов Службы сгорела в результате немецких бомбежек. К началу войны Служба была плохо подготовлена к возросшим угрозам. В начале 1941 года Дэвиж Петри (David Petrie) был назначен первым генеральным директором Секретной службы. Новый начальник начал с коренной перестройки всей организации Службы.

Впрочем, это не помешало службе успешно справляться с задачами контршпионажа. После захвата в 1945 году архивов немецкой разведки выяснилось, что за время войны в Великобритании действовали 115 агентов Германии, при этом все, кроме одного, были успешно выявлены и арестованы. Лишь один избежал ареста – он покончил жизнь самоубийством. Кстати, часть агентов были перевербованы Службой и поставляли немцам дезинформацию. Рассекреченные архивы на эту тему можно посмотреть здесь Openness и www.pro.gov.uk/ releases/mi5.

После начала Холодной войны, внимание Службы переключилось на борьбу с советской угрозой. Служба сконцентрировалась на деятельности коммуни-

стической партии Великобритании, которая в начале 40-х имела 55 тысяч членов. Впрочем, существование «кэмбриджской пятерки» прекрасно иллюстрирует тогдашние возможности советской разведки по вербовке агентов на идеологической основе.

В 1952 году премьер-министр Уинстон Черчилль передал персональный контроль над Секретной Службой Секретарю по внутренним делам (HomeSecretary), который выпустил директиву, определившую структуру и задачи Службы вплоть до 1989 года.В начале 50-х, штат Службы вновь вырос до 850 человек, включая 40 офицеров связи по всему миру.

В 60-е годы были идентифицированы еще несколько советских шпионов, например Джордж Блейк и Джон Вессал. Доклад лорда Деннинга по «делу Профьюмо» в 1963 году впервые открыл публике некоторые сведения о роли и задачах Службы. Кульминация этого периода случилась в 1971 году, когда были высланы 105 сотрудников советского посольства.

В конце 1970-х ресурсы Службы были частично перенаправлены на борьюу с международным и ирландским терроризмом. Первые антитеррористические подразделения появились в службе в конце 60-х, в ответ на несколько террористических атак.

Захват иранского посольства в Лондоне в 1980-м и бюро ливийского народа в 1984 году вызвало увеличение финансирования этих подразделений. В течение 70-х и 80-х гг. Служба играло лидирующую роль в координации борьбы с терроризмом среди западных спецслужб.

В 1983 году, Майкл Беттани (Michael Bettaney), сотрудник Службы, завербованный КГБ, был осужден за шпионаж. После запроса Комиссии по безопасности, в котором упоминались недостатки в деятельности службы, новым генеральным директором MI5 был назначен Энтони Дафф (Antony Duff), бывший директор Форин Офис. Он начал разработку новой законодательной базы для деятельности Службы, и в результате в 1989 году был принят Security Service Act 1989.

Окончание холодной войны привело к большим изменениям в работе службы. В октябре 1992 года функции борьбы против ирландского терроризма были переданы из Метрополитан полис в MI5.

♦ ♦ ♦ ♦ ♦

2. Деятельность спецслужб Украины

Спецслужбы Украины

Законодатель выделил в Украине из правоохранительной системы следующие службы и подразделения, в названии или в определении которых присутствует категория *специальный:*

- спецподразделения налоговой службы;
- Служба безопасности Украины;
- специальная милиция;

• спецподразделения по борьбе с организованной преступностью (БОП) МВД и СБУ.

Следует отметить, что Совет национальной безопасности и обороны Украины не характеризуется в законодательных актах, как специальный.

Законами об этих органах установлены основы их организации и деятельности. Однако, основным законом, который достаточно полно описывает деятельность этих и некоторых других подразделений, следует считать Закон Украины *«Об оперативно-розыскной деятельности (ОРД)».* ОРД, как записано в законе, – это система гласных и негласных розыскных, разведывательных и контрразведывательных мероприятий, которые осуществляются с применением оперативных и оперативно-технических средств. В статье 5 этого закона приведен перечень субъектов, которые вправе заниматься оперативно-розыскной деятельностью (могут иметь законное право добывать различные тайные знания):

МВД Украины: криминальная, транспортная и специальная милиция, спецподразделения по борьбе с оргпреступностью, обеспечением безопасности работников суда, правоохранительных органов и участников криминального судопроизводства;

СБ Украины: органы разведки, контрразведки, военной контрразведки, защиты национальной государственности, спецподразделения по борьбе с коррупцией и оргпреступностью, подразделения оперативно-технические, внутренней безопасности, оперативного документирования, борьбы с терроризмом и защитой участников криминального судопроизводства, работников правоохранительных органов;

Пограничные войска Украины: разведывательный орган Госкомитета по делам государственной границы Украины, подразделения по оперативно-розыскной работе;

Управление государственной охраны: подразделение оперативного обеспечения охраны, исключительно с целью обеспечения безопасности лиц и объектов, в отношении которых осуществляется охрана;

Органы государственной налоговой службы: оперативные подразделения налоговой милиции;

Органы и учреждения Госдепартамента Украины по вопросам исполнения наказаний: оперативные подразделения;

Разведывательный орган Минобороны Украины: оперативные, оперативно-технические, собственной безопасности подразделения.

Последний включен в перечень субъектов, которые вправе заниматься оперативно-розыскной деятельностью, после принятия Закона «О разведывательных органах Украины» 22 марта 2001 года. Согласно этому закону (ст. 6), разведывательную деятельность в интересах национальной безопасности Украины и с целью защиты от внешних угроз исключительное право имеют осуществлять: разведывательные органы Службы безопасности Украины – для обеспечения интересов государства в политической, экономической, военно-технической, научно-технологической, информационной и экологической сферах; разведывательные органы Министерства обороны Украины – для опреде-

ления уровня военной угрозы, обеспечения обороны и интересов государства в сферах: военной, военно-политической, военно-технической, военно-экономической, информационной и экологической; специально уполномоченного органа исполнительной власти по вопросам защиты государственной границы Украины – для обеспечения интересов государства в сферах пограничной и иммиграционной политики, а также в других сферах, которые относятся к вопросам защиты государственной границы Украины, ее суверенных прав в исключительной (морской) экономической зоне и континентальном шельфе.

Основные задачи разведывательных органов, согласно статьи 4 закона, следующие:

♦ добывание, аналитическая обработка и предоставление определенным законом органам государственной власти разведывательной информации;

♦ содействие специальными мероприятиями осуществлению государственной политики Украины в экономической, политической, военной, военно-технической, экологической и информационной сферах, укрепление обороноспособности, экономического и научно-технического развития;

♦ обеспечение безопасного функционирования учреждений Украины за рубежом, безопасности сотрудников этих учреждений и членов их семей в стране пребывания, а также откомандированных за рубеж граждан Украины, которые ознакомлены со сведениями, составляющие государственную тайну;

♦ участие в борьбе с организованной преступностью, в том числе с терроризмом, незаконным оборотом наркотических средств, незаконной торговлей оружием и технологиями его изготовления, незаконной миграцией.

В Указе Президента Украины от 15.12.99 №1573 приведена схема организации и взаимодействия центральных органов исполнительной власти. В разделе 3 этой схемы указаны центральные органы исполнительной власти, имеющие специальный статус:

- Антимонопольный комитет Украины;
- Государственная налоговая администрация Украины;
- Государственная судебная администрация Украины;
- Государственная таможенная служба Украины;
- Государственный комитет Украины по вопросам регулирующей политики и предпринимательства;
- Государственный комитет ядерного регулирования Украины;
- Национальная комиссия регулирования электроэнергетики Украины;
- Государственная комиссия по ценным бумагам и фондовому рынку Украины;
- Государственный департамент Украины по вопросам исполнения наказаний;
- Фонд государственного имущества Украины;
- Служба безопасности Украины;
- Управление государственной охраны Украины;
- Главное управление государственной службы Украины;

• Министерство экономики и по вопросам европейской интеграции Украины;

• Национальный координационный центр адаптации военнослужащих, уволенных в запас или отставку, и конверсии бывших военных объектов;

• Государственная служба экспортного контроля Украины;

• Государственный комитет Украины по вопросам технического регулирования и потребительской политики.

Оперативно-розыскная деятельность в законодательстве Украины

Основаним для проведения оперативно-розыскной деятельности, в соответствии со ст. 6 закона об ОРД♦, являються:

1) наличие достаточной информации, полученной в установленном законом порядке, которая требует проверки с помощью оперативно-розыскных мероприятий и средств о:

• преступлениях, которые готовятся или уже совершены не установленными лицами;

• лицах, готовящих или совершивших преступление;

• лицах, которые укрываются от органов дознания, суда или избегают уголовного наказания;

• лицах, без вести пропавших;

• разведывательно-подрывной деятельности спецслужб иностранных государств, организаций и отдельных лиц;

• реальной угрозе жизни, здоровья, жилища, имуществу сотрудников суда и правоохранительных органов в связи с их служебной деятельностью, а также лиц, которые участвуют в криминальном судопроизводстве, членам их семей и близким родственникам, с целью создания необходимых условий для надлежащего проведения правосудия; сотрудников разведывательных органов Украины в связи с их служебной деятельностью, их близких родственников, а также лиц, которые конфиденциально сотрудничают или сотрудничали с разведывательными органами Украины и членов их семей с целью надлежащего осуществления разведывательной деятельности;

2) запросы полномочных государственных органов, учреждений и организаций о проверке лиц в связи с их допуском к государственной тайне и к работе с ядерными материалами и на ядерных установках;

3) потребность в получении разведывательной информации в интересах безопасности общества и государства.

В законе также указаны типы документов, которые могут служить основаним для проведения оперативно-розыскных мероприятий:

♦ заявления, сообщения граждан, должностных лиц, общественных организаций, средств массовой информации;

♦ письменные поручения и постановления следователя, указания прокурора, решения суда по криминальным делам, которые находятся в его производстве, материалах органов дознания, других правоохранительных органов;

♦ Оперативно-розыскная деятельность

♦ запросы оперативных подразделений международных правоохранительных органов и организаций других государств;

♦ запросы полномочных государственных органов, учреждений и организаций, определенных Кабинетом Министров Украины о проверке лиц в связи с допуском к государственной тайне и к работе с ядерными материалами и на ядерных установках.

Запрещается принимать решение о проведении оперативно-розыскных мероприятий в случае отсутствия оснований.

♦ ♦ ♦ ♦ ♦

3. Деятельность иностранных разведок

Неофициальный документ

По материалам органов военной контрразведки ФСБ России за последние пять лет пресечена шпионская деятельность 28 иностранцев, 29 человек осуждены за разглашение государственной тайны и около 700 – за хищения, растраты и взяточничество, заявил директор ФСБ России генерал армии Николай Патрушев накануне Дня защитника Отечества в интервью «ИНТЕРФАКСУ». Директор ФСБ также прокомментировал шпионский скандал, связанный с разоблачением британских разведчиков.

Николай Платонович, несмотря на то, что Вы согласились ответить на вопросы, касающиеся деятельности военной контрразведки, прошу Вас вначале прокомментировать шпионский скандал, связанный с деятельностью британских разведчиков в России.

– С учетом того, что в СМИ достаточно широко освещалась данная тема, хотел бы отметить следующее. С начала 90-х годов между Россией и Великобританией существуют партнерские отношения. Они основаны на подписанных в 1992 году Совместной декларации Российской Федерации и Соединенного Королевства Великобритании и Северной Ирландии «Партнерство на 90-е годы», а также Договоре о принципах отношений между этими странами. В рамках межгосударственного партнерства осуществляется сотрудничество ФСБ России и британской МИ-6 по борьбе с международным терроризмом и незаконным оборотом наркотиков, в других сферах. Вместе с тем, было бы наивно считать, что разведслужба Великобритании ограничивается только представительскими функциями и не занимается своими прямыми обязанностями. Здесь уместно вспомнить известное изречение У.Черчилля: «У Англии нет постоянных врагов и постоянных союзников, у нее есть только постоянные интересы». Полагаю, что этим принципом спецслужбы Великобритании руководствуются и в современных условиях.

Одна из задач ФСБ – своевременно выявить среди находящихся в нашей стране иностранных граждан, в том числе дипломатов, тех, кто занимается разведывательной и иной противоправной деятельностью. В ходе проведенной в конце прошлого года операции нами были разоблачены сотрудники британской

резидентуры в Москве, проводившие разведывательные акции под дипломатическим прикрытием. Это – 2-й секретарь политического отдела посольства Великобритании Марк Доу, секретари-архивисты Кристофер Пирт и Эндрю Флеминг. Установлена также причастность к шпионской деятельности и помощника официального представителя МИ-6 в России Пола Кромптона.

Нами добыта шпионская аппаратура, изготовленная на высоком техническом уровне. По факту обнаружения в Москве шпионского электронного устройства ближней агентурной радиосвязи Следственным управлением ФСБ возбуждено уголовное дело по статье «шпионаж», в рамках которого проводятся соответствующие следственные и оперативно-розыскные мероприятия. Британская спецслужба МИ-6 – это профессиональная разведка, активно действующая во многих регионах мира.

Однако Ми-6 нарушила установленную практику, согласно которой официальные представители спецслужб не занимаются разведывательной деятельностью на территории страны пребывания. Между ФСБ и Ми-6 как спецслужбами-партнерами существует практика не предавать гласности данные о деятельности друг друга, а решать возникающие проблемы по каналам партнерского взаимодействия. В соответствии с этим и с учетом полученной информации о деятельности британских разведчиков, в ФСБ была проведена беседа с официальным представителем МИ-6 в Москве. Ему было предложено обсудить факты использования МИ-6 дипломатических должностей посольства Великобритании в Москве в качестве прикрытия для проведения разведывательной деятельности. Однако он отказался обсуждать эту тему. После этого у нас не оставалось иного выбора, как предать гласности ставшие известными ФСБ факты.

Принимая во внимание сложившийся характер межведомственных отношений, мы не стали настаивать на высылке указанных разведчиков. Считаем, что само руководство МИ-6 должно решить, как поступить со своими сотрудниками. Очевидно, что если они останутся в России, то будут работать под нашим контролем. ФСБ России располагает достоверными документальными материалами об активных устремлениях британской разведки к российским военным секретам, о чем свидетельствуют факты арестов разоблаченных военной контрразведкой двух агентов этих спецслужб. Нам известны и другие разведывательные акции спецслужб Великобритании, о которых более подробно говорить пока рано.

Почему в рамках этого скандала большой шум вызвал факт связи представителя британской спецслужбы с российскими НПО?

– Полагаю возможным обратить внимание на отдельные весьма любопытные моменты, ставшие известными в ходе работы по упомянутым сотрудникам МИ-6. Особый интерес наших контрразведчиков привлекла личность английского разведчика Марка Доу. По должности прикрытия в посольстве он поддерживал контакты с различными российскими НПО. Как было установлено, он принимал непосредственное участие в финансировании ряда таких организаций, подтверждением чему являются имеющиеся в нашем распоряжении платежные документы посольства с подписью Доу о переводе средств на счета НПО. По нашему мнению, использование для контактов с НПО кадрового раз-

ведчика явилось большой ошибкой англичан и дискредитировало искренность «поддержки» Великобританией построения в России гражданского общества.

Мы исходим из того, что российские НПО – важный инструмент гражданского общества. Однако при этом полагаем, что они должны дорожить своей репутацией и обязаны знать, от кого получают финансовую поддержку, которая национальным законодательством не запрещена. Если у них есть сомнения в источниках финансирования, пусть обращаются в соответствующие правоохранительные органы. Кстати, анализ российского и зарубежного правового регулирования деятельности политических партий и общественных организаций, показывает, что наше законодательство в ряде случаев более демократично.

В частности, в Японии предметом деятельности НПО не могут быть политика и религия. При регистрации НПО в этой стране неукоснительно используется критерий лояльности государственному строю и соответствия законодательству. За финансовой деятельностью НПО осуществляется жесткий контроль. В Израиле поступающие из-за границы в адрес НПО финансовые средства автоматически блокируются Минфином вплоть до особого разрешения на их использование. По решению суда НПО могут быть лишены регистрации за деятельность, не совместимую с их уставными целями и задачами, или за ущерб основам государственного строя. Все финансовые средства НПО подлежат проверкам, а банки обязаны докладывать о сомнительных переводах средств. Во Франции использование иностранных грантов национальными НПО осуществляется с разрешения МВД и по согласованию с МИД.

Тем не менее некоторые представители НПО заявляют, что воспользовавшись этим шпионским скандалом, ФСБ начала широкомасштабную спецоперацию по дискредитации российских неправительственных организаций?

– Это на их совести. Никаких спецопераций против НПО мы не планировали и не планируем. Деятельность НПО, как я уже сказал, мы считаем важным инструментом гражданского общества. При этом мы не имели права скрывать от нашего общества факт вмешательства иностранной спецслужбы в деятельность наших общественных организаций. НПО должны сами решить - принимать им эту поддержку зарубежных спецслужб или нет и как они это будут объяснять нашим гражданам.

Спасибо за подробные ответы. Перейдем непосредственно к деятельности военной контрразведки. Какие задачи она решает в российских Вооруженных Силах?

– Вооруженные силы были и остаются неотъемлемым атрибутом любого государства и по их состоянию во многом оценивается его способность обеспечить суверенитет и территориальную целостность. Именно в связи с этим столь важное значение придается ограждению армии и флота от внешних и внутренних угроз их безопасности. По линии ФСБ указанная задача возложена на военную контрразведку. Эти подразделения в войсках ранее называли «особыми отделами». Сейчас военная контрразведка входит в единую структуру ФСБ и приобрела новое название - органы безопасности в войсках. Военные контрразведчики работают непосредственно в армейских и флотских частях и подразделениях и по сути являются членами воинских коллективов.

В последние годы Россия стала равноправным партнером «большой восьмерки», играет важную роль в обеспечении политической и военной стабильности в мире. Руководство страны, министерство обороны много делают для укрепления Вооруженных Сил. Существенно возросли объемы финансирования, активизировалась боевая подготовка. Проведены крупнейшие за последние годы учения, в том числе на территориях Китая, Индии, Узбекистана совместно с вооруженными силами этих стран. Осуществлены успешные испытания новейших образцов боевой техники и вооружения, увеличивается гособоронзаказ.

Происходящие в армии процессы, планы реформирования Вооруженных Сил и оборонно-промышленного комплекса всегда вызывали повышенный интерес у иностранных спецслужб. Противостоять этим устремлениям, помочь военному командованию реализовать стоящие перед Вооруженными Силами задачи – приоритетное направление деятельности военной контрразведки. С учетом активизации международного терроризма возросли требования к военной контрразведке по обеспечению безопасности объектов хранения оружия, особенно массового поражения, боеприпасов и взрывчатых веществ.

Военная контрразведка во взаимодействии с военной прокуратурой и другими государственными органами противодействует организованной преступности, коррупции, контрабанде, незаконному обороту наркотиков и оружия, другим негативным проявлениям в армии и на флоте. Функции органов безопасности в войсках несколько шире, чем функции других контрразведывательных подразделений ФСБ, поскольку в Вооруженных Силах нет своих специальных служб, которые бы занимались оперативно-розыскной деятельностью в интересах борьбы с преступлениями, не относящимися к компетенции ФСБ России. В армии и на флоте к мнению представителей военной контрразведки прислушиваются при решении вопросов расстановки военных кадров. Она обеспечивает руководство Минобороны и Генштаба, командование на местах информацией о предпосылках к чрезвычайным происшествиям в войсках и возникающих угрозах их безопасности, оказывает помощь в поддержании на должном уровне боеготовности и боеспособности частей и соединений.

Расскажите более подробно о стремлении иностранных спецслужб получить доступ к нашим военным секретам?

– Мероприятия по повышению обороноспособности, в том числе новые разработки вооружений, а также планы реорганизации военной составляющей России вызвали беспрецедентный интерес и активность иностранных разведок. Их деятельность в России на некоторых направлениях приобретает исключительно дерзкий характер. За последние пять лет по материалам военной контрразведки пресечены шпионские акции со стороны 28 иностранцев. При этом мы получили информацию о новых формах, методах и тактических приемах разведывательной деятельности ряда зарубежных спецслужб, предметы шпионской экипировки.

Отмечается особое стремление иностранных разведок к добыванию информации, касающейся развития стратегических ядерных сил, создания новых образцов вооружений для РВСН. К сожалению, и среди наших граждан, в том числе военнослужащих, еще встречаются люди, которые пытаются поправить

свое материальное положение за счет продажи секретов иностранным спецслужбам. Ради этого они становятся на путь предательства. За пять лет по материалам органов безопасности в войсках пресечена шпионская деятельность 9 агентов и так называемых «инициативников», осуществлявших сбор развединформации в интересах зарубежных специальных служб и организаций.

Приведу несколько примеров. В 2000 году осужден бывший военнослужащий 30 ЦНИИ Минобороны подполковник Авраменко С.И. за попытку передачи представителям иностранного государства сведений о новейших разработках российской военной авиационной техники. В 2002 году при закладке тайника с материалами шпионского характера захвачен с поличным бывший старший преподаватель одной из военных академий Минобороны РФ полковник Сыпачев А.Е., впоследствии приговоренный судом к лишению свободы. В 2004 году на длительные сроки лишения свободы осуждены бывшие военнослужащие Дальневосточного военного округа и жители Приморского края Лукин И.Ю., Артюхов А.А., Смаль В.В., Белошапкин А.И., которые по заданию иностранной разведки похищали и переправляли за границу отдельные образцы российского вооружения и секретные документы.

В настоящее время завершается следствие в отношении еще двух разоблаченных военной контрразведкой российских граждан, которые занимались шпионской деятельностью. Кроме того, за этот же период 29 человек осуждены за разглашение сведений, составляющих государственную тайну. Таким образом, обеспечение защиты государственных секретов в Вооруженных Силах страны является одной из важных задач военных контрразведчиков.

Террористы не скрывают своих попыток завладеть оружием массового поражения. Как обеспечивается безопасность находящегося в войсках ядерного оружия и других средств массового поражения?

– Защита оружия массового поражения и других объектов, представляющих повышенную опасность, от террористических угроз – это общая задача Министерства Обороны, Федеральной службы безопасности, других органов. Наличие таких угроз – это не утопия, а реальность. Некоторое время назад органами безопасности были получены данные о планах А. Масхадова захватить одну из атомных подводных лодок ВМФ России. Необходимо отметить, что руководство Минобороны, командование флотов остро отреагировало на нашу информацию. Совместно были проведены проверки состояния охраны пунктов базирования таких лодок, в короткий срок устранены вскрытые недостатки, разработаны и реализованы дополнительные меры режимного и оперативного характера. В конечном итоге это позволило исключить саму возможность для террористов выполнить задуманное.

Свою роль в защите оружия массового поражения видим, прежде всего, в своевременном вскрытии устремлений к подобным объектам, организации эффективной системы их оперативной защиты, своевременном информировании заинтересованных ведомств об угрозах и проблемах в обеспечении их безопасности. В связи с этим органами безопасности в войсках значительный объем мероприятий проводится по проверке персонала, допускаемого к эксплуатации и охране ядерного оружия. Мы не имеем права допустить факты попадания на

такие объекты не только лиц с террористическими и другими преступными намерениями, но и наркоманов, людей с проблемами психического характера.

Большое внимание уделяем укреплению взаимодействия с другими антитеррористическими ведомствами. В целях совершенствования системы оперативной и физической защиты объектов повышенной опасности регулярно проводим совместные учения и тренировки. Вскрытые предпосылки к чрезвычайным происшествиям устраняются установленным порядком. Во взаимодействии с командованием организована и осуществляется работа по выявлению, предупреждению и пресечению утечки с военных складов оружия, боеприпасов и взрывчатых веществ. Эту деятельность мы рассматриваем как одну из превентивных мер противодействия терроризму.

Но интерес к приобретению оружия и боеприпасов на объектах Вооруженных Сил проявляют не только террористы. В 2005 году криминальные элементы организовали хищение крупных партий оружия со складов Сибирского и Дальневосточного военных округов, Тихоокеанского флота. Военной контрразведке совместно с военной прокуратурой и органами внутренних дел удалось в короткий срок установить и задержать похитителей, вернуть в части почти все утраченное оружие.

Какие задачи органы военной контрразведки решают в рамках контртеррористических операций на Северном Кавказе?

– Серьезной проверкой на зрелость военных контрразведчиков стали контртеррористические операции в Северо-Кавказском регионе. Одним из объектов посягательств лидеров международных террористических и религиозных экстремистских организаций являются части и подразделения Объединенной группировки войск на Северном Кавказе.

Обеспечить безопасность личного состава группировки, оказать помощь командованию в поддержании на высоком уровне боеготовности и боеспособности войск, совместно с другими подразделениями ФСБ нейтрализовать лидеров и активных участников бандподполья – это главные задачи военной контрразведки в зоне КТО.

Сотрудники органов безопасности в войсках помогают добывать сведения о местах возможных засад, минировании коммуникаций и других объектов на маршрутах движения армейских подразделений. Как пример, можно привести своевременное использование полученной военными контрразведчиками информации для предотвращения в 2005 году подрыва колонны 136-й мотострелковой бригады в Дагестане. Вдоль автодороги боевиками были установлены 23 артиллерийских снаряда и трудно представить себе масштаб кровавых последствий этой акции, если бы она была реализована.

С помощью военных контрразведчиков были добыты важные документы спецслужб так называемой «республики Ичкерия», материалы архивов Дудаева и его близкого окружения. Их изучение и анализ позволили повысить эффективность проводимых оперативно-розыскных мероприятий в Чечне и других регионах России. За образцовое выполнение воинского и служебного долга, мужество и героизм, проявленные в ходе контртеррористических операций на Северном Кавказе, многие военные контрразведчики награждены государст-

венными наградами. Шестерым из них присвоено звание «Герой России», в том числе двоим посмертно.

Располагает ли ФСБ сведениями о количестве оружия, которое может быть у бандитов в Чечне. Каковы основные каналы его поступления?

– По нашим данным, с учетом изъятого и уничтоженного в ходе контртеррористических операций вооружения, боевики бандформирований в Чечне располагают еще значительными запасами оружия. Откуда оно? Как показывают проверки по учетам изымаемого у бандитов оружия, оно в основном относится к тому, что было оставлено Дудаеву в период распада Советского Союза и захвачено в результате нападений на арсеналы и склады воинских частей, находившиеся на территории бывшей Чечено-Ингушской АССР.

Только в период 1992-1993 годов из воинских частей Минобороны Дудаеву было официально передано более 40 тысяч единиц стрелкового оружия, в том числе около 28 тысяч автоматов, 10 тысяч пистолетов, около 1700 пулеметов, 200 винтовок. Кроме этого, около 16 тысяч единиц стрелкового оружия в тот период было захвачено в частях внутренних войск, территориальных органах КГБ и МВД.

Таким образом, к моменту начала первой чеченской кампании в 1994 году так называемые «вооруженные силы Ичкерии» располагали огромным арсеналом стрелкового оружия. Оно частично было спрятано по всей Чечне в тайниках и схронах. Его мы находим до настоящего времени. Часть этого оружия оказалась в распоряжении криминальных структур в других российских регионах. Были факты получения боевиками оружия с территории ряда государств ближнего и дальнего зарубежья, а также по криминальным каналам. В частности, нами была раскрыта группа лиц, причастных к незаконным поставкам в Грозный более 4 тысяч пистолетов с одного из российских оружейных заводов через фирму, зарегистрированную на подставное лицо в Республике Кипр. Тогда из незаконного оборота удалось изъять около 3 тысяч пистолетов, приготовленных для отправки в Чечню. Есть и другие примеры.

На боеготовность войск негативно влияют воровство, коррупция и другие злоупотребления должностных лиц. Занимается ли этими проблемами военная контрразведка?

– В последнее время проблема борьбы с коррупцией и вообще с преступностью в войсках и на флоте приобрела особую остроту. С учетом выделения армии значительных финансовых и иных средств на оборону и реформирование у некоторых должностных лиц появилось искушение улучшить противоправным путем свое материальное положение. С указанным злом, характерным не только для Вооруженных Сил, мы боролись и будем бороться в тесном контакте с армейским руководством, Главной военной прокуратурой, другими правоохранительными структурами.

По материалам военной контрразведки органами военной прокуратуры в 2001-2005 годах было возбуждено и расследовано более 1000 уголовных дел. За должностные преступления, хищения и растраты, взяточничество осуждено около 700 человек, предотвращен ущерб государству на сумму примерно 6 млрд. рублей. Причем к подобного рода должностным злоупотреблениям при-

частны не только рядовые снабженцы. За прошедший год по информации военной контрразведки органами Главной военной прокуратуры были возбуждены уголовные дела в отношении семи высших офицеров Вооруженных Сил. С руководством Минобороны по искоренению таких позорных для армии и флота явлений мы работаем в тесном контакте. После доведения дел до судов фамилии этих лиц будут преданы гласности.

Происшествие в Челябинском танковом училище встревожило российское общество, все ветви власти. Может ли военная контрразведка оказать помощь в наведении порядка в армии?

– Здесь, наверное, нельзя ограничиться констатацией того, что армия болеет теми же болезнями, что и общество. Перенос в армию всех негативов общества чреват опасными последствиями. На недавно прошедшей Коллегии ФСБ Президент Российской Федерации поставил органам безопасности в войсках задачу совместно с военным командованием усилить внимание к проблеме соблюдения законности в Вооруженных Силах. Военные контрразведчики должны в полном объеме знать обстановку в войсках. Преступность в армейской среде, неуставные отношения дестабилизируют морально-психологическую ситуацию в частях и подразделениях, негативно сказываются на имидже Вооруженных Сил Российской Федерации и военной службы в целом. Мы используем в полном объеме наши возможности для того, чтобы командование владело полной информацией о том, что творится во вверенных ему армейских и флотских коллективах и принимало соответствующие меры по наведению порядка. В этой работе, мы как и прежде, будем активно взаимодействовать с военной прокуратурой, которая не оставляет без внимания ни один, поступающий от военной контрразведки сигнал о противоправной деятельности в войсках.

Проходят ли в ФСБ России службу военнослужащие по призыву?

– В настоящее время военнослужащие по призыву проходят службу только в пограничной службе ФСБ. Федеральной службой безопасности формируются новые организационные структуры пограничных органов с целью их максимальной адаптации к решению современных задач. При этом предполагается полностью отказаться от использования военнослужащих, проходящих военную службу по призыву. По мере строительства новых пограничных застав, общежитий и объектов социальной инфраструктуры постепенно сокращается численность военнослужащих по призыву. Значительное количество данной категории военнослужащих будет сокращено за счет общего уменьшения численности личного состава, реформирования учебных центров и образовательных учреждений пограничного профиля. Переход к комплектованию пограничных органов ФСБ военнослужащими, проходящими военную службу по контракту, будет полностью завершен в течение 2008 года.

Что бы Вы пожелали сотрудникам органов федеральной службы безопасности в канун Дня защитника Отечества?

– От имени руководства Федеральной службы безопасности хочу сердечно поздравить всех военнослужащих, ветеранов Вооруженных Сил, правоохранительных органов и специальных служб Российской Федерации с Днем защитника Отечества. Нынешние защитники Родины с честью и достоинством несут

нелегкую службу, умело и мужественно действуют в экстремальных условиях и в боевой обстановке. В нашей памяти навсегда останутся имена героев, отдавших свои жизни за свободу и независимость нашей страны, обеспечение ее национальных интересов. Выражаю уверенность в том, что люди, избравшие своей профессией защиту Отечества, будут и впредь верны военной присяге, своему воинскому и служебному долгу. Искренне желаю Вам, дорогие друзья, дальнейших успехов в службе, крепкого здоровья, счастья и благополучия.

♦ ♦ ♦ ♦ ♦

4. Нас подслушивают*

К сожалению, «жучки» – это реальность. 8 из 10 человек, позвонивших по рекламе детекторов подслушивающих устройств, наоборот, сами интересуются, где можно приобрести «жучок». «ПП» решил выяснить истинный размах грозящей опасности. За год в России возбуждается до 120 дел по статье 138 Уголовного кодекса «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», из которых около 100 раскрывается. Как отмечают эксперты, большая часть таких дел связана с незаконным изготовлением и продажей «специальных технических средств», в частности, «жучков» (ч. 3 ст. 138 УК). Что касается собственно дел о посягательстве на неприкосновенность информации, то их единицы. В основном это попытки незаконного прослушивания политиков, чиновников, судей, прокуроров.

В то же время за последние годы ни в Петербурге, ни в стране не было ни одного громкого скандала, связанного с прослушиванием офисов компаний или телефонных переговоров их сотрудников. Что никак не влияет на спрос на системы защиты от «прослушки». Крупные коммерческие структуры предпочитают разбираться с такими проблемами втихомолку, силами собственной службы безопасности. Те же, кто не относит себя к капитанам бизнеса, о проблеме конфиденциальности часто просто не задумываются. И, как считают специалисты, напрасно.

Как попасть «под колпак»

«Сказать, что существует связь между размером или сферой деятельности компании и ее шансами оказаться объектом прослушивания, нельзя, – считает заместитель генерального директора «Агентства технической безопасности». – Хотя, чем у компании больше денег, тем выше к ней интерес». Руководитель направления противодействия промышленному шпионажу компании «Конфидент», впрочем, полагает, что группа повышенного риска все же есть: «Если компания расширяет рынок, ведет конкурентные войны, если ее название на слуху, можно с высокой долей вероятности говорить, что попытки шпионских атак на нее были, есть или будут». Косвенное доказательство того, что «прослушка» конкурентами и прочими заинтересованными лицами в отношении, по крайней мере, крупного бизнеса ведется весьма активно, – это затраты самих

* По материалам журнала «Предприниматель Петербурга» №27 (434).

компаний на обеспечение безопасности. За оборудованием для контроля технических каналов утечки информации ежегодно в специализированные фирмы обращаются несколько сотен петербургских компаний, постоянно отслеживающих новинки в этой сфере. Стоимость комплекта спецтехники, необходимой для оснащения собственной службы безопасности (сканеры, локаторы, детекторы и пр.), начинается с $10-15 тыс. и может доходить до сотен тысяч долларов. Более экономичный, чем собственная служба безопасности, вариант защиты – периодические проверки сторонними специалистами – обходится тоже достаточно дорого – $10-50 за м^2.

Чтобы оправдать эти расходы, служба безопасности должна выявлять за год несколько серьезных враждебных акций. В приватном порядке службисты утверждают, что проблем с обоснованием затрат не возникает: обнаружение и подавление «жучков» для них в целом рутинная работа.

Любопытствующих не останавливает даже то, что «прослушка» – «один из самых простых и часто используемых способов бизнес-шпионажа, но по соотношению затрат и результата один из самых малоэффективных, к тому же незаконный». Хорошее оборудование, как правило, делается на заказ и стоит недешево. При этом всегда остается риск не получить никакой ценной информации, а то и получить дезинформацию. «Собственно, атака по техническим каналам – это лишь один из множества элементов профессиональной атаки».

Наиболее эффективно прослушивающую аппаратуру злоумышленники могут использовать для вербовки «агента» путем сбора на него компромата. Поставить «жучок» дома у топ-менеджера компании-жертвы или на квартире его любовницы намного проще, чем в офисе, и результативнее. Примечательно, что в свое время после трансляции в телеэфире видеокассеты с «человеком, похожим на генерального прокурора», вырос спрос на приборы «Алмаз». До этого предназначенная для обнаружения скрытых видеокамер аппаратура стоимостью в несколько тысяч долларов особой популярностью не пользовалась.

«Жучки» для ревнивых жен

Тому, что «прослушка» идет в народ, способствует и тот факт, что купить «жучок» сегодня ненамного сложнее, чем билет в кино. Набрав в поисковике слово «жучки», можно найти предложения на любой вкус и по вполне умеренным ценам – от $200. Правда, продукция такого рода представляет собой банальный ширпотреб, подчас собранный неизвестными радиолюбителями. Удовлетворяя спрос ревнивых жен и прочих начинающих разведчиков, она обладает целым рядом недостатков: малое время работы, небольшая дальность (до 100 метров) и низкое качество передачи сигнала.

Разумеется, чтобы поставить «жучок», необходимо иметь свободный доступ в помещение, в противном случае цена вопроса возрастает. Например, микрофон с передатчиком, вмонтированные в подарочную пепельницу или часы, которые не стыдно подарить, стоят уже от $1000.

Правда, как отмечают специалисты, сегодня подобная незамысловатая техника, как инструмент бизнес-разведки вообще теряет смысл. Любой офис и без того напичкан уже включенными в сеть микрофонами (мини-АТС, системы громкой связи, мобильники, особенно с гарнитурой, и т. п.), что открывает са-

мые широкие возможности как для дилетанта, так и для профи. Реализовать их, имея доступ в офис, аппаратуру за несколько тысяч долларов и минимальные технические навыки не так уж и сложно.

Они подслушивают законно

По закону об оперативно-розыскной деятельности, право на вмешательство в частную жизнь граждан имеют семь госструктур, которым для установки «жучков» и проведения других подобных мероприятий необходимо решение суда.

Министерство внутренних дел
Федеральная служба безопасности
Федеральная служба охраны
Федеральная таможенная служба
Служба внешней разведки
Федеральная служба исполнения наказаний
Федеральная служба по контролю за оборотом наркотиков

«Прослушка»: мифы и реальность

Миф № 1: в трубке щелчки – значит, телефон слушают

Считается, что определить подключение «третьего лишнего» к телефонной линии можно по характерным щелчкам, звяканью телефона, после того, как вешаешь трубку и т.п.

Реальность. Подобные симптомы могут свидетельствовать разве что об очень топорной работе, вроде подключения параллельного телефона. Для обнаружения закладки необходимо специальное оборудование, причем нет гарантии, что переговоры не слушаются, например, через АТС, и это уже никак не выявить. Кстати, если телефон имеет функцию громкой связи, то при помощи специальной аппаратуры можно прослушивать все разговоры в помещении через его микрофон.

Миф № 2: мобильный телефон – находка для шпиона

Бытует мнение, что переговоры по мобильнику прослушать очень просто. Чем и занимаются все, кому не лень.

Реальность. Слушать разговоры в GSM-сетях – дорогое удовольствие: цена необходимого оборудования составляет $100-120 тыс. Наиболее защищенной считается связь стандарта CDMA (в Петербурге ее продвигает сеть SkyLink), оборудования для перехвата которой пока вообще нет. Зато весьма уязвимыми являются радиотелефоны, настроиться на передающую волну которых можно, сидя в машине за углом. Если ходьба по офису с трубкой вошла в привычку, лучше отдать предпочтение цифровым моделям стандарта DECT.

Миф № 3: телевизор говорит моим голосом

Считается, что работающий «жучок» создает помехи на телевизионных каналах или определенной радиочастоте. Тогда по телевизору или в радиоэфире можно услышать собственный голос.

Реальность. Такое действительно возможно, если речь идет о радио-«жучке». Один из специалистов рассказал, что в его практике был случай, когда клиент случайно обнаружил «жучок», услышав свой голос в телевизоре по одному из дециметровых каналов. Правда, обольщаться не стоит – это опять-таки

признаки непрофессиональной работы и того, что «жучок» – скорее всего, самоделка низкого качества.

Миф № 4: на всякий «жучок» найдется «антижучок»

Многие полагают, что обезопасить себя от прослушки можно с помощью так называемого «генератора белого шума», который якобы гасит все попытки снятия информации. Стоимость прибора в интернете – от 10 тыс. руб.

Реальность. То, что выдают за «антижучки», – как правило, генераторы радиопомех, которые по своим техническим характеристикам способны блокировать радиосигнал (и то не любой) только в непосредственной близости от приемника. Для блокирования каналов утечки в помещении требуется целый комплекс оборудования, которое все равно не дает 100% гарантии и предполагает целый ряд других мер.

Миф № 5: кто защищает от «прослушки», тот и «слушает»

Логика подобных рассуждений проста – больше всего о защите знает тот, кто умеет нападать. И с другой стороны, тот, кто занимается защитой, хорошо осведомлен, как ее обходить.

Реальность. С 2000 года рынок прослушивающих устройств и рынок средств защиты от них сильно разошлись в связи с уходом первого «в тень». Компаниям, которые официально занимаются продажей и установкой систем безопасности, вести двойную игру рискованно. Во-первых, их бизнес лицензируется. Во-вторых, он предполагает работу с оглядкой на «компетентные органы» (чтобы ненароком не помешать их деятельности).

♦ ♦ ♦ ♦ ♦

5. Этика использования конкурентной разведки и промышленного шпионажа*

«Современная научная, промышленная и экономическая информация большей частью легко доступна. 95% интересующих Вас данных можно получить из специальных журналов и научных трудов, отчетов компаний, внутренних изданий предприятия, брошюр и проектов, раздаваемых на ярмарках и выставках. Цель шпиона – раздобыть оставшиеся 5% информации, в которой и кроется фирменный «секрет», «тайна мастерства».

Французский исследователь методов промышленного шпионажа М. Денюзьер

Что такое «**конкурентная разведка**»? Если спросить наугад отобранных людей, большинство, в том числе предприниматели, пожмут плечами: «Приличное название для кражи чужих секретов...»

Это распространенное заблуждение далеко не соответствует действительности. В США и странах Европы принято различать конкурентную разведку

* С. Чертопруд. Автор книги «Научно-техническая разведка от Ленина до Горбачева»

(competitive intelligence; в России также можно встретить названия «деловая разведка», «бизнес-разведка») и промышленный шпионаж. Отличие заключается в строгом соблюдении закона в первом случае и нарушениях уголовного, авторского или любого другого права – во втором. В качестве примера классической операции в сфере конкурентной разведки рассмотрим действия японской фирмы JVC против Sony. После того, как Sony выпустила новую модель цифровой видеокамеры, JVC, оценив по объему продаж конкурента рыночные возможности продукта, предложила собственную камеру, в которой были учтены все недостатки предшественницы. Отметим, что в этом случае JVC не преступила черту закона: никто не взламывал сигнализацию в офисе Sony, чтобы похитить чертежи, не подкупал сотрудников – видеокамера-образец была просто куплена в магазине и разобрана «по винтику».

В России и конкурентная разведка, и промышленный шпионаж существуют пока что «стихийно», и часто грань между ними невозможно провести.

Как выяснилось на данный момент в России под конкурентной разведкой подразумеваются четыре различных направления сбора информации, на которых стоит остановиться подробнее:

1. Сбор данных о партнерах и клиентах для предотвращения мошенничеств с их стороны. В США, например, такой проблемы не существует: есть банки данных «кредитных историй»; открыт доступ к материалам судебных дел за последние пятьдесят лет, что позволяет, не прибегая к специфическим приемам, выяснить, с кем имеешь дело. Достаточно распространены и «черные списки» тех, кто запятнал свою деловую репутацию. В России пока что каждой заинтересованной организации приходится самостоятельно собирать и анализировать информацию, причем координация усилий отсутствует даже на уровне государственных органов: одни и те же сведения добывают по своим каналам МВД, ФСБ, налоговая полиция. Обмен этими данными представляет собой громоздкую и медленную процедуру. В бизнесе нечто подобное отраслевым «черным спискам» существует только у страховых обществ и банков. Промышленные компании вынуждены поодиночке создавать собственные технологии проверки кредитных историй, что эффективно удается лишь гигантам, способным содержать мощную службу безопасности.

А между тем выявление мошенничеств еще на этапе их подготовки – более чем актуальная задача. Достаточно одного примера из российской действительности. При проведении приватизации алюминиевого завода был объявлен тендер. Одна из компаний, участвовавших в тендере, решила собрать максимум информации о соперниках, и в результате изучения открытых источников выяснилось, что четыре других участника имеют одного и того же учредителя. Таким образом стало ясно: соперник использует нечестные методы.

Неоднократно предпринимались попытки со стороны коммерческих структур наладить официальное сотрудничество с правоохранительными органами, чтобы сделать «открытой» информацию об уже осужденных мошенниках и лицах, находящихся в федеральном розыске. Пока что это остается на уровне благих пожеланий, и сотрудничество идет только на неофициальной основе.

Выявлением мошенничеств активно занимаются также частные детективные агентства и службы безопасности, причем в последнее время разработано несколько отечественных технологий выявления мошенничеств на этапе их подготовки.

2. «Подсветка» потенциальных партнеров и сотрудников. Речь, в первую очередь, идет о реальном финансовом положении и наличии и/или характере «крыши» (криминальные структуры, милиция, спецслужбы, «афганцы» и пр.). Обычно этим занимаются отделы безопасности компаний или частные детективные агентства. Это очень сложная сфера, в которой легко переступить грань закона, особенно если речь идет о физических лицах – так, при приеме на работу нового сотрудника легально заниматься сбором информации о его частной жизни можно только с письменного согласия проверяемого. Как правило, получить такое согласие не составляет особого труда, поскольку в ином случае претендент рискует остаться на улице. Не менее часто приходится, однако, проверять сотрудников компании-партнера – ведь если выяснится, например, что заместителя директора, подписавшего договор, за сутки до этого уволили, его подпись окажется недействительной, а последствия сделки – непредсказуемыми. Однако в подобных случаях открытая проверка невозможна.

3. Выполнение услуг предусмотренных «Законом о частной детективной и охранной деятельности» (поиск имущества должника и т.п.). Легально на этом сегменте рынка могут действовать только детективы, имеющие необходимую лицензию. В противном случае собранную ими информацию сложно будет реализовать в суде. Впрочем, часто клиента интересует только адрес, по которому скрывается задолжавший; остальное уже – дело рук структур, в высшей степени далеких от государственной правоохранительной системы...

4. Сбор информации маркетингового характера. Именно этим, собственно, на Западе занимается большинство специалистов в сфере конкурентной разведки, тогда как в России этот вид деятельности только зарождается.

Существует несколько групп потребителей, которым нужны чужие тайны. Самые скандально известные – представители СМИ, специалисты по черному PR и мастера «активных мероприятий» («слив» компромата в правоохранительные органы и т. п.).

Вторая группа – учредители (хозяева) и клиенты различных негосударственных служб безопасности и охранных предприятий. Их интересуют три направления: сбор информации о конкурентах и партнерах (потенциальных партнерах); проверка лояльности персонала; выполнение заказов третьих лиц (например, фиксация факта супружеской неверности). Часто предприниматели обходятся собственными силами, не прибегая к помощи специалистов. Третья группа – криминальные структуры, за последние десять лет усовершенствовавшиеся от примитивного рэкета до сложных экономических комбинаций.

Сведения разрешенные и запрещенные

Различные трактовки термина «конкурентная разведка» связаны с особенностью доступа к информации в разных странах. Например, в США в 1996 году был принят «Закон о свободе информации», который обязал федеральные ведомства обеспечить гражданам свободный доступ ко всей информации. Огра-

ничения касаются лишь материалов, имеющих отношение к национальной обороне, личных и финансовых документов, а также документов правоохранительных органов. Отказ в доступе к информации можно обжаловать в суде, сведения должны быть представлены в десятидневный срок, а споры разрешаются в течение 20 дней. При этом по статистике большинство запросов исходит от фирм, которые хотят получить государственную информацию о конкурентах.

Существенную роль играет и общественная организация «Точность в средствах массовой информации» (Accuracy in Media – AIM). Она объединяет 345 тысяч членов и осуществляет контроль над тем, чтобы публикуемые или передаваемые в эфир материалы соответствовали фактам.

Особая сложность заключается при этом в проблеме доступа к персональной информации. При том, что такие данные являются предметом особого спроса, в большинстве развитых стран личная информация строго охраняется. Много говорится о том, что, в случае вступления России в ЕС, ей придется привести свои законодательство и реально существующую практику в соответствие с жесткими европейскими законами, Однако в том же ЕС существует и мощное лобби маркетинговых, информационно-аналитических и финансовых компаний, успешно блокирующее применение законодательства. В частности, когда более десяти лет назад Европарламент попытался ужесточить законодательство в сфере предоставления информации о персональных данных (принял Personal Data Information Act), то столкнулся с очень жестким сопротивлением, и до сего дня только две трети членов ЕС реально изменили свое национальное законодательство.

Даже незыблемая концепция банковской тайны в Европе и США подверглась не так давно серьезным изменениям в связи с законами об отмывании средств. Более того, благодаря законопроекту под громким названием «Акт об объединении и усилении Америки» (Uniting and Strengthening America Act, или просто USA Act), который был одобрен в США, широчайшие полномочия в этой сфере получает американское Министерство финансов: если возникает подозрение (даже без доказательств), что тот или иной финансовый институт занимается отмыванием денег, министерство вправе потребовать от банка любую информацию о корсчетах этого финансового института и людях, которые пользуются этими счетами. В результате институт банковской тайны в США практически перестает существовать. Напомним, что в России раскрытие банковской тайны возможно только с санкции прокурора в рамках уголовного дела либо по решению суда. Очевидно, что эти нововведения, относящиеся не только к американцам, но и к иностранным гражданам и финансовым институтам, облегчают всевозможные злоупотребления и фактически нарушают право на неприкосновенность личной жизни.

В России же вопросы права на информации полны парадоксов. С одной стороны, существует более 20 видов тайны, поэтому теоретически можно ограничить доступ к сведениям почти по любой тематике. При этом отсутствует законодательство, которое регулирует открытость различных категорий данных (тех же кредитных историй юридических и физических лиц). С другой стороны, коррупция чиновников всех уровней позволяет без особого труда добыть нуж-

ные сведения. На рынках, торгующих электроникой, и в Интернете можно купить CD-ROM со служебными базами данных практически всех государственных ведомств: начиная с таможни (самая дорогая база данных – $1000 в Москве) и ГИБДД ($400), заканчивая списками владельцев элитного жилья и базами данных телефонных сетей (от $100 до $250). Причем в последних есть даже «закрытые» телефоны и адреса сотрудников МВД, ФСБ, судей, политиков, эстрадных звезд.

Проблема невозможности законного доступа к информации спровоцировала массовое использование специальных технических средств. По оценкам МВД РФ, годовой оборот рынка РЭС (радиоэлектронных средств, к которым относятся и «жучки») в России составляет $1–2 млрд. в год (в 1995 году – всего $150–170 млн.), в то время, как оборот рынка средств защиты от наблюдения с помощью спецтехники составляет не более $100–200 млн. По рентабельности этот вид бизнеса занимает третье место после торговли оружием и наркотиками, а по количеству изъятой правоохранительными органами аппаратуры измеряется тоннами или автофургонами (речь идет о выемках во время обысков в помещениях служб безопасности крупных компаний или у оптовых продавцов).

Впрочем, эксперты считают, что в мире выявляется только 1–2% применяемой шпионской техники, а оставшиеся позволяют получить до 60% информации. В Москве ежедневно используется негосударственными структурами от 300 до 600 «закладок», к которым следует добавить средства для скрытого видеонаблюдения, радиомониторинга и другую шпионскую аппаратуру.

В последнее время некоторая либерализация законодательства позволяет надеяться на то, что в продаже недобросовестными чиновниками ведомственных данных просто не будет необходимости. Так отношение ФАПСИ к вопросам безопасности постепенно становится менее жестким. Например, еще год назад сотрудники этого федерального агентства заявляли, что 90% внутриведомственного документооборота государственных органов – секрет, но недавно заместитель начальника главного управления ФАПСИ В. Задорожный сильно снизил порог секретности: теперь, по его оценкам, до 70% информации гражданских ведомств не является закрытой. Впрочем, сотрудники разных ведомств, ссылаясь на собственный опыт, говорят, что на практике соотношение закрытой и открытой информации по-прежнему ближе к 99% и 1%...

Источники

Как известно, 70–90% всей информации разведка получает из открытых источников. Основную роль в этой категории сегодня играет Интернет, открывающий доступ к СМИ, сайтам компаний, профессиональным базам данных и т. п. «Всемирную паутину» можно сравнить с информационным Клондайком. Проблема в том, что данные не структурированы, и зачастую их невозможно найти с помощью поисковых систем. Вторая группа источников – всевозможные бумажные документы: подшивки газет и журналов, реклама, пресс-релизы; еще в 1930-е годы аналитики советской и германской разведок могли похвастаться многочисленными достижениями в этой сфере.

Приведем типичный пример из сегодняшней российской практики. Отечественная производственная компания решила поглотить один из региональных

заводов. Для этого ей потребовалось оперативно достать реестр акционеров – имея список держателей акций, можно было бы склонить их к сотрудничеству или уговорить продать свои акции. Быстро достать документ не удавалось, и аналитики, работавшие на компанию, нашли другой выход. За несколько дней они собрали информацию об основных акционерах из открытых источников: региональной и федеральной прессы, баз данных регистрационных и других государственных органов. Компания договорилась с несколькими крупными акционерами – и дело было в шляпе.

Кроме того, очень популярны имеющиеся в продаже, но в отличие от упоминавшихся выше, вполне легальные базы данных госучреждений. Особенно часто используются базы данных Московской регистрационной палаты, регистрационных органов других городов и регионов России, Госкомстата, Торгово-промышленной палаты, Госкомимущества. Отдельные доступные базы данных есть в некоторых министерствах и комитетах. Существует негосударственная база данных «Лабиринт», составленная на основе публикаций ведущих изданий, с помощью которой можно получить обширную информацию о конкретных персоналиях и компаниях.

Для облегчения работы аналитиков существуют специальные компьютерные программы, позволяющие в кратчайшие сроки отбирать и сортировать информацию из СМИ и баз данных. На сегодняшний день их разработано более двухсот. Впрочем, не все можно эффективно использовать в сфере коммерческой разведки – большинство едва способны обеспечить хранение больших объемов информации, а уж о качественном анализе можно только мечтать.

Однако утверждение о том, что работа менеджера по конкурентной разведке – это постоянное путешествие по «виртуальному» миру или изучение гор бумажных документов, не совсем корректно. В отличие от аналитиков спецслужб, специалистам компаний иногда приходится работать и «в поле», общаясь с живыми людьми. Так, например, одна западная консалтинговая фирма, занимающаяся деловой разведкой, получила от клиента задание выяснить, где компания-конкурент планирует строительство нового завода. Вначале сотрудник фирмы выяснил из прессы и справочников, какое агентство занимается подбором кадров для конкурента, затем провел мониторинг местной прессы и вскоре обнаружил в газете одного небольшого городка объявление этого агентства о найме менеджеров, администраторов и других специалистов. Сотрудник позвонил по телефону, представившись кандидатом на одну из должностей, – и дело было сделано. Агент по найму охотно поделился с ним деталями будущей работы...

Другой пример. Однажды служащий компании Chrysler узнал, что лучший фотограф Ford едет в Париж, и сообщил об этом руководству своей компании. Представительство Chrysler в Париже установило, что объект намерен снять новую модель автомобиля-конкурента на фоне Эйфелевой башни. Оказалось также, что после Парижа фотограф направляется в Гонконг. После анализа собранной информации эксперты Chrysler сделали вывод, что Ford в ближайшее время планирует выпуск недорогого малолитражного автомобиля, предназначенного для продаж в большинстве стран мира.

Наконец, массу информации дает вдумчивое наблюдение. Приведем пару реальных историй из отечественной практики. Директор одного крупного склада перед тем, как организовать работу собственных подчиненных, в течение нескольких дней наблюдал за работой конкурентов. Владелец крупной кондитерской фабрики посетил компании-дистрибьюторы конкурентов и выяснил все условия их работы (цены, скидки, форму оплаты). Собранную таким образом информацию он использовал при создании собственной сбытовой сети в регионах.

Кадры решают все

Сейчас большинство людей, занятых в сфере деловой разведки, – это выходцы из оперативных подразделений правоохранительных органов. По официальной статистике Управления лицензионно-разрешительной работы (УЛРР) МВД РФ, в частных охранных предприятиях и Службах безопасности большинство сотрудников пришло из МВД и ФСБ и лишь немногие – из налогового ведомства. Как следствие, большинство специалистов по конкурентной разведке, приступая к новой работе, уже более или менее владеют методами проверки физических и юридических лиц, тогда как для проведения маркетинговых исследований им нужно как минимум год учиться. Неудивительно, что иногда вместо скрупулезной и трудоемкой работы с «открытыми» источниками они предпочитают использовать спецтехнику.

Реально большинство отечественных специалистов не «учтено» в УЛРР, так как они не оформляют необходимую лицензию. Причина проста – прав у частного детектива при сборе информации значительно меньше, чем у журналиста или обычного гражданина. Если не имеющий лицензии аналитик не использует спецтехнику или не пытается добыть государственные секреты, то, скорее всего, он ничем не рискует – пока не принят Закон «О коммерческой тайне», статья в Уголовном кодексе, карающая за разглашение чужой коммерческой информации, эффективно работать не будет.

Тем не менее, большинство участников «круглого стола» признали, что в сфере подготовки специалистов по конкурентной разведке есть серьезные проблемы. Нового массового притока профессионалов из спецслужб, как то было в начале 1990-х, ждать уже не приходится. Из тех же, кто пришел десять лет назад, многие уже доросли до руководителей подразделений, и основной спрос сегодня – на молодежь для работы «в поле», на низовых должностях аналитиков и оперативников. Можно, конечно, брать выпускников вузов, но у них нет опыта работы, тогда как еще десять лет назад сфера конкурентной разведки укомплектовывалась профессионалами с многолетним стажем, которые владели специфическими навыками (например, умели работать на враждебной территории). Проблемой остается и специализация выпускников: в вузах экономического профиля не учат основам оперативно-розыскной работы, а в Академии МВД или ФСБ дают недостаточно знаний по экономике.

Хотя говорить о том, что в нашей стране вообще не готовят специалистов по «конкурентной разведки», не совсем корректно. Есть группа вузов, где обучают навыкам противодействия «промышленному шпионажу», а говоря другими словами, защищать конфиденциальную информацию от охотников за чужи-

ми тайнами, будь то сотрудники иностранных спецслужб или конкурирующих фирм. Для создания эффективной обороны надо прекрасно разбираться в средствах нападения. Другое дело, что уровень преподавателей и материально-техническая база не позволяет отработать все виды атак, да и большинство студентов не стремится получить дополнительную подготовку. А зря – у настоящего профессионала в области «деловой разведки» есть как минимум два преимущества перед выпускниками специализированных вузов.

Во-первых, выпускники Факультетов защиты информации имеют базовую подготовку как в области экономики (маркетинг, менеджмент, хозяйственное право), так и спецдисциплин (использование специальных технических средств, основы оперативно-розыскной работы. Во-вторых, они не работают по традиционным схемам, используют приемы не только из арсенала маркетологов или спецслужб. Самый большой в России опыт подготовки специалистов по комплексной защите информации имеет факультет защиты информации Российского государственного гуманитарного университета (РГГУ), функционирующий уже более десяти лет. Если раньше основной контингент его выпускников находил работу в государственных организациях – СВР, ФАПСИ, ФСБ, Гостехкомиссия, ГТК РФ, – то теперь большинство студентов целенаправленно готовят для коммерческих организаций.

Сегодня точное число членов виртуального «профсоюза менеджеров конкурентной разведки» в России назвать не может никто. По мнению генерального директора компании «СИнС» С. Ю. Минаева, тех, кто специализируется исключительно на деловой разведке, зарабатывает только на ней, – очень мало. Если говорить о тех фирмах, где деловая разведка составляет лишь одно из важных направлений, их можно насчитать до десятка практически в каждом субъекте Российской Федерации и около 100 – в Москве. Это немало для страны с переходной экономикой.

До кризиса 1998 года главную скрипку в этой отрасли играли частные охранные предприятия (ЧОПы), сотрудники которых совмещали функции телохранителей и разведчиков. Однако после дефолта спрос на их услуги сильно упал, а расценки снизились в 5–7 раз. Оказавшись в плачевной ситуации, многие руководители ЧОПов осознали, что пора заниматься не только охраной, но и аналитикой. Некоторые полностью перешли в новую область бизнеса, другие открыли у себя соответствующие подразделения или дочерние предприятия, где деловая разведка занимала одно из приоритетных мест. Бизнес, правда, оказался здесь не таким простым, как представлялось со стороны, но в целом этот сегмент российской экономики довольно быстро развивается. Добавим, что расценки на данный вид услуг колеблются от $50 до $50 тыс. в зависимости от сложности заказа. Многие компании предпочитают создавать собственные подразделения конкурентной разведки, которые могут называться по разному (информационно-аналитическое подразделение, департамент маркетинга, отдел сбыта), но имеют общую задачу – сбор и анализ информации, необходимой для выживания компании на рынке.

Реальный мир российской конкурентной разведки, не говоря о промышленном шпионаже, покрыт мраком тайны. Более или менее точное число случа-

ев 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 России пока находятся в стадии становления. По всей вероятности, рано или поздно службы сбора коммерческой информации в нашей стране начнут работать по западному образцу, предполагающему, в частности, что «агент» использует только законные методы и обязательно представляется и партнерам, и конкурентам фирмы как сотрудник отдела деловой разведки. В России это пока немыслимо.

К тому же на данный момент большинство заказчиков никакой маркетинговой информации от профессионалов и не ждет. Немудрящий список пожеланий клиента обычно сводится к ответам на вопросы: «Кто это? Что это? Где мои деньги?». Да хорошо еще, если только к ним, – как с обидой признают специалисты по деловой разведке, сплошь и рядом их просят деньги не только найти, но и «выбить», путая с криминальными структурами, хотя это, как говорят в Одессе, две большие разницы...

Законодательство

В заключение немного сухой теории. Всю информацию ограниченного доступа можно условно разделить на две категории. Первая группа – государственные секреты. Это «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации» (Закон РФ «О государственной тайне»). Их состав определен в ст. 5 данного закона. Во вторую категорию входит остальная защищаемая информация. Ее состав определен в «Перечне сведений конфиденциального характера» (утвержденный Указом Президента РФ от 6 марта 1997 г. № 188).

Начнем с первой категории. «Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности Российской Федерации» однозначно трактуется как шпионаж (ст. 276 УК РФ).

Возможности применения на практике этой статьи более широкие, чем это принято считать. В данном случае речь идет об оказании услуг в сфере сбора и анализа информации, которая формально считается «открытой». Во–первых, всегда есть вероятность того, что внезапно могут быть засекречены сведенья, которые раньше считались «открытыми». Во-вторых, сюда относится передача или собирание сведений, не содержащих государственной тайны, но могущих быть использованными в ущерб внешней безопасности РФ (если, например, это делается по заданию иностранной разведки. Такие действия квалифицируются так же, как шпионаж. Государство почти всегда может защитить свои интересы. Не важно, кто противник – иностранная спецслужба или отечественные «промышленные шпионы». Поэтому многие частные агентства, по возможности,

избегают оказания иностранным организациям услуг в сфере сбора и анализа информации.

А вот ситуация со сбором сведений, не содержащих государственной тайны, намного сложнее. В «Перечне сведений конфиденциального характера» перечислено шесть групп тайн. В первую отнесены «сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные)». В эту же категорию можно отнести информацию, касающуюся частной жизни граждан. Во вторую группу – «сведения, составляющие тайну следствия и судопроизводства». Третья – «служебные сведения, доступ к которым ограничен органами государственной власти» (служебная тайна). Четвертая группа – «сведения, связанные с профессиональной деятельностью, доступ к которым ограничен» (профессиональная тайна). Пятая – «сведения, связанные с коммерческой деятельностью» (коммерческая и банковская тайны), шестая – «сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них». Для большинства категорий этих сведений предусмотрены различные виды ответственности за их сбор или разглашение.

Начнем с коммерческой тайны. Информация подпадает под это определение, если «имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности» (ч. 1 ст. 137 Гражданского кодекса РФ). Согласно ч. 2 указанной статьи, «лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору».

Согласно Закону РФ от 22 марта 1991 г. № 948 – 1 «О конкуренции и ограничении монополистической деятельности на товарных рынках», одной из форм недобросовестной конкуренции является «получение, использование, разглашение научно–технической, производственной или торговой информации, в том числе коммерческой тайны, без согласия ее владельца» (ст. 10 Закона). «За виновные противоправные деяния, нарушающие антимонопольное законодательство, должностные лица федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления, коммерческие и некоммерческие организации или их руководители, а также граждане, в том числе индивидуальные предприниматели, несут гражданско-правовую, административную либо уголовную ответственность» (ст. 22 – 1 Закона).

Более четко ответственность за «промышленный шпионаж» определена в статье 183 УК РФ. Она предусматривает ответственность за «незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну». Законом предусмотрено два состава этого преступления: «собирание сведений, составляющих коммерческую или банковскую тайну, путем похище-

ния документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений» (ч.1 ст. 182), или «незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб» (ч.2 ст. 182). Определение банковской тайны дано в ст. 857 Гражданского Кодекса РФ и в ст. 26 Федерального закона от 3 февраля 1996 г. № 17 – ФЗ «О внесении изменений и дополнений в Закон РСФСР «О банках и банковской деятельности в РСФСР» (с изменениями).

Начнем с определения банковской тайны данной в ГК РФ.

«1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом.

3. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков».

В законе «О банках и банковской деятельности в РСФСР» это понятие расписано более подробно. «Кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Аудиторские организации не вправе раскрывать третьим лицам сведения об операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и их работники несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом».

Предметом личной и семейной тайны могут быть сведения о фактах биографии лица, о состоянии его здоровья, об имущественном положении, о роде занятий и совершенных поступках, о взглядах, оценках, убеждениях, об отношениях в семье или об отношениях человека с другими людьми. Предусмотрена уголовная ответственность за «незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тай-

ну, без его согласия» (ст. 137 УК РФ). Под незаконным собиранием сведений о частной жизни следует понимать собирание вопреки закону лицом, не уполномоченным на это, сведений о частной жизни другого лица, содержащих его личную или семейную тайну. Информация может собираться тайно, под благовидным предлогом или даже открыто путем ознакомления с документами в учреждениях и других местах, путем бесед с родственниками, соседями, сослуживцами потерпевшего, его лечащими врачами, получения ее из других источников. Распространение сведений о частной жизни потерпевшего – это сообщение виновным без согласия потерпевшего о таких сведениях третьим лицам в разговоре.

Профессиональная тайна – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна и т.п.). Федеральное законодательство устанавливает запрет для лиц, которым конфиденциально были доверены сведения, касающиеся частной жизни, затрагивающие личную и семейную тайну, предавать эти сведения огласке. В частности, согласно ст. 61 Основ законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 г. № 5487–1 не допускается разглашение составляющей врачебную тайну информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении. Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, наравне с медицинскими и фармацевтическими работниками с учетом причиненного гражданину ущерба несут за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность (ст. 137 УК РФ (нарушение неприкосновенности частной жизни). В Законе Российской Федерации от 2 июля 1992 № 3185–1 «О психиатрической помощи и гарантиях прав граждан при ее оказании» сказано (ст. 9), что «сведения о наличии у гражданина психического расстройства, фактах обращения за психиатрической помощью и лечении в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья являются врачебной тайной, охраняемой законом».

В ст. 16 Основ законодательства Российской Федерации «О нотариате» от 11 февраля 1993 г. указывается, что «нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности». При этом требование сохранения тайны распространяется не только на содержание нотариального действия, но и на сам факт обращения с просьбой о его совершении. В ст. 16 Положения об адвокатуре РСФСР, утвержденного Законом РСФСР от 20 ноября 1980 г. указывается, что «адвокат не вправе разглашать сведения, сообщенные ему доверителем в связи с оказанием юридической помощи». В ст. 12 Федерального закона от 15 ноября 1997 г. № 143 «Об актах гражданского состояния» указано, что сведения, ставшие известными работнику Загса в связи с государственной регистрацией акта гражданского состояния (рождение, заключение брака, расторжение брака, усыновление (удочерение), установление отцовства, перемена имени и смерть), являются

персональными данными, относятся к категории конфиденциальной информации, имеют ограниченный доступ и разглашению не подлежат.

Другой важный фактор, влияющий на тяжесть наказания, – способ добычи (получения) конфиденциальной информации. Наиболее распространенные из них отражены в Федеральном законе от 12 августа 1995 г. № 144 – ФЗ «Об оперативно-розыскной деятельности». Согласно ст. 6, «при осуществлении оперативно-розыскной деятельности проводятся следующие оперативно–розыскные мероприятия:

1. Опрос.
2. Наведение справок.
3. Сбор образцов для сравнительного исследования.
4. Проверочная закупка.
5. Исследование предметов и документов.
6. Наблюдение.
7. Отождествление личности.
8. Обследование помещений, зданий, сооружений, участков местности и транспортных средств.
9. Контроль почтовых отправлений, телеграфных и иных сообщений.
10. Прослушивание телефонных переговоров.
11. Снятие информации с технических каналов связи.
12. Оперативное внедрение.
13. Контролируемая поставка.
14. Оперативный эксперимент».

Запрещается проведение оперативно–розыскных мероприятий и использование специальных и иных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, не уполномоченными на то настоящим Федеральным законом физическими и юридическими лицами (ст. 6 данного закона).

Перечень специальных технических средств, утвержденных постановлением Правительства РФ от 1 июля 1996 г. № 770:

1. Специальные технические средства для негласного получения и регистрации акустической информации.
2. Специальные технические средства для негласного визуального наблюдения и документирования.
3. Специальные технические средства для негласного прослушивания телефонных переговоров.
4. Специальные технические средства для негласного перехвата и регистрации информации с технических каналов связи.
5. Специальные технические средства для негласного контроля почтовых сообщений и отправлений.
6. Специальные технические средства для негласного исследования предметов и документов.
7. Специальные технические средства для негласного проникновения и обследования помещений, транспортных средств и других объектов.

8. Специальные технические средства для негласного контроля за перемещением транспортных средств и других объектов.

9. Специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.

10. Специальные технические средства для негласной идентификации личности.

Начнем с «экзотического» метода получения чужих секретов – использования хакерских приемов для добычи конфиденциальной информации. В УК РФ есть ст. 272 (неправомерный доступ к компьютерной информации). Состав преступления – «неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети». Способы неправомерного доступа к компьютерной информации могут быть различными: представление фиктивных документов на право доступа к информации, изменение кода или адреса технического устройства, нарушение средств или системы защиты информации, кража носителя информации.

Правда, в России более популярно использование различных специальных технических средств (далее – СТС) для негласного получения информации. Если при этом произошло «нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений... совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации», то это считается уголовно наказуемым деянием (ст. 138 ч. 2 УК РФ). Если не были использованы СТС, то данное деяние подпадает под действие ст. 138 ч.1 УК РФ.

Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений заключается в ознакомлении с их содержанием без согласия лица, которому эта информация принадлежит, а также при отсутствии для такого ознакомления законных оснований, например, если нет решения суда, подтверждающего необходимость ограничения права гражданина на тайну переписки или телефонных переговоров.

Конфиденциальная информация, как любой товар, продается и покупается. И что бы ее получить порой бывает достаточно заплатить определенную сумму человеку, имеющему к ней законный доступ. В российском законодательстве предусмотрена ответственность за коммерческий подкуп. Согласно ч. 1 ст. 204 УК РФ, это «незаконная передача лицу, выполняющему управленческие функции в коммерческой или иной организации, денег, ценных бумаг, иного имущества, а равно незаконное оказание ему услуг имущественного характера за совершение действий (бездействия) в интересах дающего в связи с занимаемым этим лицом служебным положением». Среди таких действий может быть разглашение этим лицом информации, составляющую коммерческую тайну организации, раскрытие производственных секретов, дающее стороне, подкупившей соответствующего служащего конкурирующего предприятия, незаслужен-

ное преимущество в хозяйственной деятельности. Также предусмотрена уголовная ответственность за «незаконное получение лицом, выполняющим управленческие функции в коммерческой или иной организации, денег, ценных бумаг, иного имущества, а равно незаконное пользование услугами имущественного характера за совершение действий (бездействия) в интересах дающего в связи с занимаемым этим лицом служебным положением» (ч. 3 ст. 204 УК РФ).

Отдельно предусмотрен перечень действий, которые не могут выполнять частные детективы. Согласно ст. 7 Закона РФ от 11 марта 1992 г. № 2487–1 «О частной детективной и охранной деятельности в Российской Федерации», представителям этой профессии запрещается:

- выдавать себя за сотрудников правоохранительных органов;
- собирать сведения, связанные с личной жизнью, политическими и религиозными убеждениями отдельных лиц;
- осуществлять видео – и аудиозапись, фото – и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных или частных лиц;
- прибегать к действиям, посягающим на права и свободы граждан;
- совершать действия, ставящие под угрозу жизнь, здоровье, честь, достоинство и имущество граждан.

Проведение детективами сыскных действий, нарушающих тайну переписки, телефонных переговоров и телеграфных сообщений либо связанных с нарушением гарантий неприкосновенности личности или жилища, влечет за собой установленную законом ответственность, о которой было подробно рассказано выше.

♦ ♦ ♦ ♦ ♦

6. Конкуренция и безопасность

Конкуренция как неизменный атрибут всего живого приобрела цивилизованную форму и сместилась в экономическую сферу жизнедеятельности человека.

Экономическая конкуренция

Всякая предпринимательская инициатива, в условиях рыночной экономики, неизбежно попадает под воздействие конкуренции, как одного из основных условий эволюционного развития общественных отношений.

Конкуренция может существовать в различных формах: *соревнование*, как наиболее цивилизованная форма – аукционы, тендеры, биржи; *борьба*, также цивилизованная форма конкуренции в рамках закона, но связана с подавлением и уничтожением конкурентов посредством применения новых технологий, освоения новых рынков сбыта, ценовой политики; *война* – это недобросовестная конкуренция, физическое воздействие, вооруженные конфликты.

По украинскому законодательству экономическая конкуренция – это соревнование между субъектами хозяйствования с целью получения, благодаря собственным достижениям, преимуществ над другими субъектами хозяйствования. Потребители и субъекты хозяйствования имеют возможность выбирать между несколькими продавцами и покупателями, а отдельный субъект хозяйствования не может определять условия обращения товаров на рынке (см. ЗУ «О защите экономической конкуренции»).

Теневая экономика

Одной из основных тенденций, которые наблюдаются в коммерческой сфере деятельности общества, является тенизация экономики. Кроме конкурентного состязания отдельных товаропроизводителей и отраслей, существует также и соперничество двух сфер экономики – законной и теневой, которые сращиваются, взаимопереплетаются и функционируют неразрывно. При этом капитал может мигрировать из официальной экономики в теневую и обратно.

Конкурентная борьба и тенизация экономических отношений оказывает двойственное влияние на предпринимателей.

Предприниматель, работающий в рамках закона на контролируемом государством рынке, сталкивается с конкуренцией со стороны предпринимателей, использующих незаконные методы: контрабанду, уклонение от уплаты налогов, незаконное, следовательно бесплатное, использование авторских прав, взятки, направленные на «упрощение» разрешительной системы государства, получение госзаказов, лицензий и прочих выгод. При этом честному предпринимателю выдержать конкуренцию со стороны коллег, нарушающих закон, становится не возможным, если они способны наполнить рынок товарами в объеме адекватном платежеспособному спросу. Достигая этого уровня они либо вытесняют с рынка законопослушных предпринимателей, либо последние тоже переходят к использованию незаконных методов. Об этом свидетельствует то, что подавляющее число предприятий при осуществлении одинаковых хозяйственных операций используют и одинаковые схемы уклонения от налогов. Причем распространение таких схем после очередного изменения законодательства происходит очень быстро путем использования бартера, оффшор, векселей, фиктивных фирм, обналичивания под маркетинг, частных предпринимателей и других ухищрений.

При конкурентной борьбе в условиях тенизации получить большую прибыль возможно только через контрабандные либо другие нелегальные схемы. С легальной экономикой конкурирует также и черный рынок – рынок товаров, запрещенных к обращению либо реализуемых без получения разрешения со стороны государства – это торговля наркотиками, оружием, людьми, незаконные валютные операции и др. Норма прибыли на черном рынке наиболее высока, но настолько же высока и степень риска потери капиталов, инвестируемых в производство и торговлю «черными» товарами и услугами.

Теневая экономика – это система отношений, которая постоянно самовоспроизводится и развивается. История ее возникновения уходит своими корнями в далекое прошлое, когда вместе с законами появились и их нарушители. Поэтому экономические преступления имеют наиболее легко преодолимый пси-

хологический барьер. Например, рабочий, который ворует на своем заводе какие-нибудь детали, может не считать себя виновным в краже, так как где-то воруют миллионами, а ему зарплату не платят. Примерно такими же психологическими установками руководствуются и предприниматели, которые понимают, что соблюдение законов ставит их в невыгодное положение по отношению к конкурентам.

Теневые отношения в экономике с одной стороны позволяют значительно повысить прибыльность бизнеса, а с другой – увеличивают степень риска. Они становятся для предпринимателя и врагом, и союзником одновременно.

Национальной особенностью борьбы с теневой экономикой является постоянное декларирование со стороны государства необходимости остановить развитие теневых отношений в экономике страны. Для этого ежегодно принимаются различные законы, постановления, указы, распоряжения, которыми утверждаются концепции, программы, даются поручения многим ведомствам и министерствам, чиновники которых погрязли в коррупции. При этом реальная борьба ведется против криминалитета и некоторых конкурентов, а условия функционирования теневой экономики, как конкурентной среды, не уничтожаются.

Недобросовестная конкуренция

Недобросовестная конкуренция – это любые действия, противоречащие правилам, торговым и другим честным обычаям в предпринимательской деятельности (ст. 1 Закона Украины «О защите от недобросовестной конкуренции»). Честность в отечественном предпринимательстве еще не стала правилом, а является скорее исключением. Именно поэтому данный закон изначально представлялся многим как мертворожденный.

Закон определяет следующие виды недобросовестной конкуренции:

1. Неправомерное использование чужих обозначений, рекламных материалов, упаковки, при которых товары на «черном» и «сером» рынках реализуются в основном с неправомерным употреблением всемирно известных брендов и торговых марок.

2. Неправомерное использование товара другого производителя – пиратство. Особенно это касается незаконного производства и экспорта CD, по которым Украина занимает одно из первых мест в мире

3. Копирование внешнего вида изделия. Такие действия, как и определенные в первых двух пунктах, частично ограничиваются также и системой законов о защите интеллектуальной собственности: «Об авторском праве и смежных правах», «Об охране прав на знаки для товаров и услуг», «Об охране прав на промышленные образцы», «Об охране прав на открытия и полезные модели» и многими другими нормативными актами. Ответственность за такие нарушения предусмотрена Кодексом Украины об административных нарушениях (ст. 164/3 «Недобросовестная конкуренция»).

4. Сравнительная реклама – действия запрещенные Законом Украины «О рекламе» (ст. 8 «Общие ограничения рекламы», ст. 10 «Недобросовестная реклама»).

5. Дискредитация хозяйствующего субъекта путем так называемого, «черного» PR. Подобная «антирекламы» развивается специалистами привлеченными для проведения очередной предвыборной кампании, после окончания которой они перемещают свою активность в сферу экономики и маркетинга.

6. Купля-продажа товаров, выполнение работ, предоставление услуг с принудительным ассортиментом, когда некоторый ходовой товар можно купить с нагрузкой в виде какого-нибудь неликвида путем предложения различных призов и подарков, стоимость которых включается в стоимость основного товара и оплачивается самим клиентом.

7. Склонение к бойкоту хозяйствующего субъекта.

8. Склонение поставщика к дискриминации покупателя (заказчика).

9. Склонение хозяйствующего субъекта к расторжению договора с конкурентом.

10. Подкуп работника поставщика.

11. Подкуп работника покупателя.

(Ответственность за действия, предусмотренные пп. 7-11 могут быть квалифицированы как преступные в соответствии с УК ст. 364 «Злоупотребление властью или служебным положением», а по пп. 10-11 и по ст. 368 «Получение взятки», 369 «Дача взятки»).

12. Достижение неправомерных преимуществ в конкуренции предпринимателями, занимающимися сокрытием доходов от налогообложения, а также использующих любые другие незаконные методы ведения бизнеса.

Перечисленные методы недобросовестной конкуренции завуалировано используются на отечественном рынке для продвижения товаров, как самими товаропроизводителями (посредниками), так и рекламными компаниями.

Добросовестная конкуренция

Украинское законодательство не содержит определения видов добросовестной конкуренции, а в Законе Украины «Об ограничении монополизма и недопущении недобросовестной конкуренции в предпринимательской деятельности» дано следующее определение: конкуренция – это соревновательность предпринимателей, когда их самостоятельные действия ограничивают возможности каждого из них влиять на общие условия реализации товаров на рынке, и стимулируют производство тех товаров, в которых нуждается потребитель. Исходя из правового принципа, *что не запрещено законом, то разрешено,* добросовестная конкуренция – это:

1. Управление качеством: улучшение качества с одновременным увеличением цены; улучшение качества без увеличения цены; снижение качества с одновременным снижением цены;

2. Ценовая политик: повышение цены, снижение цены, система скидок;

3. Управление прибылью: управление доходами, управление расходами;

4. Реклам: реклама в СМИ, упаковка и дизайн;

5. Создание бренда.

6. Расширение рынка сбыта: организация дилерской сети, диверсификация товарных потоков, слияние, поглощение.

Вышеперечисленные приемы могут быть добросовестными, если они не противоречат законодательству.

Монополия

Конкуренции разрушается с появлением губительного воздействия монопольных образований, существование которых несло, несет и всегда будет нести явную и скрытую угрозу для всякого общества. Это послужило толчком к созданию антимонопольного законодательства. Экономическая конкуренция, как необходимое условие естественного отбора несвязанных товаропроизводителей, стала всячески оберегаться и отдельными государствами, и международным законодательством.

Законом Украины «О защите экономической конкуренции» установлено, в частности, что субъект хозяйствования занимает монопольное (доминирующее) положение на рынке товара, если его часть превышает 35% и, если он не докажет, что испытывает значительную конкуренцию. Монопольным также может быть признано положение субъекта, если его часть на рынке составляет 35% и меньше, но он не испытывает значительной конкуренции, например вследствие сравнительно небольшого размера частей рынка, которые принадлежат конкурентам.

Монополизированные рынки как объект демонополизации также рассматриваются с точки зрения наличия и размеров искусственно созданных барьеров вступления предприятий на такие рынки. Данные барьеры, как правило, возникают вследствие дискриминации предпринимателей со стороны государства и антиконкурентных действий со стороны отдельных предпринимателей.

Дискриминацией со стороны органов власти считается:

- запрет и ограничения создания новых предприятий в какой-либо сфере деятельности, а также установление ограничений на проведение отдельных видов деятельности;
- принуждение предпринимателей к приоритетному заключению договоров, первоочередной поставке товаров определенному кругу потребителей;
- принятие решений про централизованное распределение товаров, которое обеспечивает монопольное положение на рынке определенным предпринимателям;
- установление запрета на реализацию товаров, произведенных в одном регионе страны, в других регионах;
- предоставление отдельным хозяйствующим субъектам налоговых, кредитных и других льгот, бюджетных дотаций и субсидий, если это приводит к монополизации рынка отдельных товаров;
- ограничение прав хозяйствующих субъектов относительно приобретения и реализации товаров, в том числе путем установления квот, лицензий во внешнеэкономической деятельности, таможенных тарифов;
- введение ограничений на инвестиции, в том числе иностранные.

Конкуренцию также могут сдерживать:

♦ государственное регулирование цен и тарифов.

♦ неблагоприятные условия для предпринимательской деятельности (большие налоги, неконвертированность национальной валюты, сложность и противоречивость законодательства).

♦ ограниченный доступ на валютные рынки.

♦ недостаточно развитая банковская система и рыночная инфраструктура.

Демпинг

Генеральное соглашение о тарифах и торговле от 1947 г. (ГАТТ) определяет демпинг как распространение товаров одной страны на рынке другой по цене ниже нормальной, если оно причиняет или может причинить значительный вред производству, основанному одной из стран-участниц, или существенно замедляет создание национальной продукции (ст. 6). Нормальной цена не признается если она ниже цены на соответствующее изделие, применяемой при обычных коммерческих операциях к аналогичному товару, реализуемому в стране экспортера. Из определения следует, что в качестве основного критерия демпинга используются цены внутреннего рынка, а в случае их отсутствия допускается использование цен экспорта в третьи страны, но при этом сопоставление должно производиться с наиболее высокой экспортной ценой.

Международный антидемпинговый кодекс, принятый на конференции по тарифам стран-участниц ГАТТ в 1967 г. в Женеве предусматривает включение в соответствующее законодательство отдельных стран параграфа о «нанесенном ущербе» предприятиям в импортирующей стране и представлении доказательств об этом.

В антидемпинговом законе, принятым в Австрии в 1962 г., впервые приведены количественные параметры демпинга: для экспортной цены, если она на 20% и более ниже, чем на внутреннем рынке страны происхождения товара, или минимум на 8% ниже мировой цены.

Демпинг – это один из классических приемов конкурентной борьбы, целью которого, как правило, является завоевание рынка, оттеснение конкурентов или доведение их до банкротства. При этом демпинг подразумевает реализацию товаров с запланированным убытком, который должен быть в последствии компенсирован за счет завышенных монопольных цен. Законодательство Украины не содержит ограничений по поводу минимальных цен на продукцию отечественных товаропроизводителей на внутреннем рынке (исключение составляют некоторые группы подакцизных товаров, а также товары, реализуемые по бартеру). Демпинг может вполне легитимно применяться национальными компаниями в пределах таможенных границ, особое для «раскрутки» новых торговых марок и брендов. После того как потребитель «привыкает» к новому продукту, цена на него значительно возрастает.

♦ ♦ ♦ ♦ ♦

7. Всемирная история шпионажа

Во все времена тайные службы оказывали большое влияние на ход истории. Но известно совсем немного случаев, когда их работа заслуживала официальное признание. Военачальники и государственные деятели, как правило, не упоминают в своих мемуарах о помощи, оказанной им тайными агентами. Документы секретных разведывательных служб бессрочно хранятся в архивах, и содержание большинства из них не станет известным миру до тех пор, пока существует государство или, по крайней мере, не изменится общественный строй. Например, в архивах британской Интеллидженс Сервис (Secret Intelligence Service) до сих пор находятся под замком бумаги, датированные XVI-XVII вв. Возможно, их обнародование заставило бы переписать некоторые главы британской истории. Похожим образом обстоит дело с тайными архивами в других странах. В этом отношении Россия не является исключением.

Необходимость выведать намерения, планы, возможности своих врагов появилась у людей, должно быть, тогда, когда человечество впервые начало воевать. Так что явление, которое ныне называется шпионажем, существует уже тысячелетия, и профессия шпиона, пожалуй, заслуживает того, чтобы носить титул «наидревнейшей» (кстати сказать, род деятельности, претендующий на звание древнейшей из профессий, всегда служил целям шпионажа и был частью его тактики.

В начале рассмотрим понятие шпион. Согласно принятой на Брюссельской конференции 1874 г. «Декларации о правилах ведения войны», которая указывает, что «шпионом… называется лицо, которое тайно или ложным предлогом занимается сбором информации другой стороне» Помимо того что шпионаж признавался дозволенным средством ведения военных действий и как понятие получал статус международно-правовой нормы, создатели Декларации сделали попытку сформулировать отличие шпиона от разведчика, указав, что последним может считаться лазутчик, не скрывающий своей принадлежности к военнослужащим. Однако на практике оба понятия постоянно переходят друг в друга и в смысловом отношении являются почти синонимами. Несмотря на то, что с позиций международного права шпионаж допустим, он все же остается крайне рискованным занятием. Шпион, арестованный во время войны и уличенный в совершенном преступлении, вероятнее всего, будет казнен: воюющее государство вправе защищаться от противников с помощью наиболее эффективных в данный момент мер.

Шпион не должен находиться в центре политических событий и ни в коем случае не должен идти на авантюры, постоянно рисковать своей жизнью. Наоборот, именно незаметность, так называемая «открытая скрытность» является признаком настоящего разведчика. Лоуренс Аравийский, раскрывая собственный опыт социальной и психологической мимикрии, необходимой для универсального шпиона, писал: «Я не был солдатом, которым движет один лишь инстинкт, который автоматически повинуется своей интуиции и внезапным счастливым озарениям. Когда я принимал или менял решения, то прежде всего насколько мог вникал в любой важный, а порой и незначительный вопрос. Гео-

графию, обычаи, религию, социальные условия, язык, жесты, шкалу духовных ценностей – все это я постигал до мелочей, чувствовал и осознавал досконально. Врага я знал почти так же хорошо, как своих соратников». История шпионажа, особенно двух последних столетий, показывает, что настоящий разведчик, каким бы он характером не обладал, отличается высоким интеллектуальным потенциалом. Разведка это ристалище интеллектуалов. Достаточно вспомнить Карла Шульмейстера, Томаса Лоуренса, Сиднея Рейли, Вильгельма Васмуса, Рихарда Зорге, Кима Филби или Рудольфа Абеля… Список можно продолжать. Именно деятельность таких людей доказывает, что и в мирное, и в военное время разведывательная служба сильна не столько количеством, а сколько качеством. В сущности, состояние разведывательной системы государства отражает его «здоровье», то есть силу и международный авторитет.

Задачи шпионажа исторически определились как информационная (в том числе предупреждающая шпионаж и диверсии со стороны противника) и наступательная, то есть контрразведка и проведение локальных подрывных и военных операций в тылу врага. Сбор информации в наши дни зачастую упирается в проблему обработки и анализа официальной информации, которая благодаря деструктивной власти СМИ циркулирует по информационным каналам, начиная с газет и телепрограмм, заканчивая набирающей силу сетью Интернет.

Географические карты и расписания движения поездов, дающие представление о пропускной способности транспортных сетей, публикация стратегических данных, списков должностных лиц и тому подобных данных позволяют получить немало полезных сведений о любой стране. Эксперты в соответствующей области, эти теоретики от статистики стали первыми, кто находит шпионам работу, указывая цель и возможное решение. Они также сопровождают собранную информацию необходимыми комментариями, позволяющими своевременно оценивать намерения явного или вероятного противника. Остальное дело политиков и военных. Похоже, бывший директор ЦРУ Маккоун был недалек от истины, когда заметил: «Все войны нашего века, в том числе и первая мировая война, начались в результате ошибочной оценки ситуации из-за недостаточной и плохо проанализированной информации». Тот же Вьетнам, Афганистан теперь Чечня. В этом смысле современный шпионаж – прежде всего работоспособная эффективная агентурная сеть, развернутая в стане противника. Образ удачливого шпиона-одиночки, имеется ввиду Джеймса Бонда, идеализированного кинематографом, становится все менее актуальным.

И все же вопрос о причинах побуждающих людей заниматься шпионажем, остается наиважнейшим для кадровой службы любой разведки мира. Психологи давно дали удручающий ответ: мотивы, как правило, не ясны, а попытки свести их к каким-то конкретным свойствам человека, например ненависти, патриотизму, легкомыслию, жажде приключений или корыстолюбию, не решают проблему состоятельности или не состоятельности агента. Тем не менее лучшими шпионами становились те, кто предлагал свои услуги по идейным убеждениям. Еще сложнее объяснить эффект двойного (или даже тройного) агента, который работает сразу на обе (несколько) сторон. Как ни странно, но объединительный европейский процесс, американизация образа жизни и вооб-

ще медленное, но явное стирание государственных различий, по крайней мере в Европе и США, в современную эпоху как бы поощряет» двойничество» секретных агентов. Психологи назвали это явление «феноменом добродушного попутчика». Но это, как говорится, особая тема, и она лишь дополняет главную – шпионаж как явление мировой истории.

♦ ♦ ♦ ♦ ♦

8. Из истории шпионажа*

Многочисленная армия фанатов «Формулы-1» все еще не оправилась от громкого скандала вокруг предполагаемого акта промышленного шпионажа, совершенного командой McLaren против команды Ferrari. Болельщики итальянцев возмущены, ведь McLaren так и не была наказана за то, что каким-то явно незаконным образом раздобыла секретную документацию Ferrari. Между тем таковы правила мира промышленного шпионажа – здесь обычно не наказывают, а отвечают конкурентам действиями собственной промышленной разведки.

Китайская грамотность

Взломать систему безопасности,
защищавшую секрет китайского фарфора,
сумели хорошо подготовленные иезуиты

Если бы не промышленные шпионы, научно-технический прогресс остановился бы, не успев начаться. Счастливые обладатели ноу-хау почили бы на лаврах, довольствуясь старыми, но проверенными технологиями, а их конкуренты годами бы пытались изобрести то, что уже давно изобретено. К счастью, промышленный шпионаж возник тогда же, когда появился первый секрет, скрываемый от конкурентов, то есть примерно в эпоху изобретения каменного топора. Первые случаи похищения экономических секретов произошли так давно, что остались в памяти людей лишь благодаря мифам и легендам. В Европе, например, древнейшим мифом о промышленном шпионе, безусловно, является легенда о Прометее. В Китае же существует легенда о принцессе, которая, чтобы угодить зарубежному возлюбленному, вывезла из Поднебесной шелковичных червей, спрятав их в цветах, украшавших ее прическу. Однако расцвет промышленного шпионажа пришелся на куда более поздние эпохи, когда от обладания технологиями или коммерческой информацией стало зависеть процветание или банкротство крупных корпораций.

Принципы коммерческой разведки веками оставались неизменными. Основную часть полезной информации давал анализ открытых источников, на втором месте стоял опрос агентов, завербованных на предприятии конкурента, и лишь на третьем — собственно шпионские операции, включая несанкциони-

* По материалам журнала «Деньги» № 31 (637), Кирилл Новиков.

рованное проникновение, копирование секретной документации и т. п. Все эти составляющие промышленного шпионажа использовались уже в XVIII веке, о чем говорят, в частности, письма иезуитского миссионера Пьера д`Энтреколя. Проповедуя в Китае, он не забывал попутно собирать информацию о технологии изготовления фарфора. Свои методы иезуит описывал так: «Помимо того, что я видел своими глазами, я многое узнал от моих вновь обращенных, из которых некоторые работали с фарфором, а некоторые торговали им. Правдивость их сообщений я подтвердил изучением китайских трактатов по данному вопросу, так что я многое почерпнул из этих книг, посвященных изумительному искусству фарфора». Помимо вербовки путем обращения в христианство ничего не подозревавших китайцев и изучения технической литературы, находившейся в открытом доступе, святой отец несколько раз проникал на императорские фарфоровые фабрики, куда чужакам был вход заказан. Хотя д'Энтреколь кое-что напутал в своих описаниях, информация, присланная им во Францию, оказалась бесценной. Вскоре французы приступили к производству собственного фарфора, и даже превзошли немцев, которые к тому времени самостоятельно научились производить фарфор. Затем секрет фарфора стал известен в Англии и других европейских странах, что пагубно сказалось на многовековой китайской монополии, но отвечало интересам потребителей и бизнесменов.

В XVIII веке Франция стала настоящей кузницей кадров для промышленных шпионов, причем шпионили в основном за соседней Англией, которая в области технологий заметно опережала другие страны Европы и при этом имела законодательство, запрещавшее вывоз станков и технической документации. Французские же законы признавали права изобретателя за каждым, кто привезет в пределы страны какое-нибудь техническое чудо, так что заниматься шпионажем в пользу французской короны многим казалось весьма выгодным делом. Одним из первых предпринимателей, решивших всерьез заняться перекачкой ноу-хау через Ла-Манш, был англичанин Джон Холкер. В своей деятельности он не видел ничего зазорного, поскольку имел зуб на английское правительство: будучи сторонником свергнутой династии Стюартов, он видел в шпионаже способ послужить правому делу. Холкер, попавший в Англии в тюрьму за свои убеждения, сумел сбежать и скрылся во Франции. Поскольку до ареста он был специалистом в области производства шерстяных тканей, он немедленно предложил свои знания французскому правительству. Информация, переданная им, была чрезвычайно ценна, но главная его услуга Франции заключалась в другом. Холкер создал на Британских островах шпионскую сеть, главной задачей которой стало переманивание во Францию лучших технических кадров. Организованная им утечка мозгов принесла его новой родине немалую выгоду. Сам он тоже не остался внакладе: 8,6 тыс. ливров, которые он ежегодно получал от французского правительства, были хорошей суммой для неимущего иммигранта. Французские покупатели тоже были рады, ведь отечественные товары стоили дешевле тех, что привозили из-за Ла-Манша.

Агент 64

Хотя тайное переманивание сотрудников, владеющих технологическими и коммерческими секретами, до сих пор входит в компетенцию промышленных шпионов всего мира, этим их деятельность не ограничивается. Если Холкер в основном охотился за специалистами, то другой французский шпион — Ле Тюрк — искал чертежи, станки и техническую документацию, то есть был промышленным шпионом в современном смысле этого слова. Как и Холкер, Ле Тюрк был предпринимателем. Он пытался наладить производство фламандских кружев, но не преуспел, а потому решил попытать счастья в новом качестве.

В 1785 году Ле Тюрк, получив от французского правительства 10 тыс. ливров, направился в Англию с целью добыть образцы новых ткацких станков, появившихся в Ноттингеме. Вывозить эти станки из Англии было запрещено, однако предприимчивый француз нашел способ провезти их контрабандой. Операция прошла успешно, и с тех пор Ле Тюрк занялся промышленным шпионажем на постоянной основе. Образцы английских машин он провозил, спрятав их в ящиках с товарами, разрешенными к вывозу, а также среди сувениров, которые он скупал под видом добропорядочного туриста. Ле Тюрк стал настоящим мастером конспирации и даже задолго до Джеймса Бонда придумал для себя цифровое обозначение. Вся его шпионская переписка имела подпись — «64». С годами его осторожность росла и в конце концов превратилась в паранойю: ему повсюду начали мерещиться английские шпионы и контрразведчики, которые мечтают увести его прямо в Тауэр.

Ле Тюрк мечтал основать во Франции собственную текстильную фабрику, которая бы работала на ворованных станках с применением ворованных технологий, однако мечтам его не суждено было сбыться. С началом революции во Франции он лишился финансирования. Помещение под фабрику, которое он просил, ему не дали. В результате ему пришлось ограничиться открытием небольшой мастерской, которая занималась пошивом трехцветных кокард для революционных парижан. Свои дни Ле Тюрк окончил в государственной лечебнице нищим и полусумасшедшим стариком, однако ремесло промышленного шпиона привлекло впоследствии еще многих искателей приключений и коммерческой выгоды.

Отчаявшись самостоятельно раскрыть секрет английской стали, Альфред Крупп украл его

В XVIII и XIX веках профессиональных промышленных шпионов было немного. В основном этим делом занимались сами предприниматели, желавшие подзаработать за счет чужой интеллектуальной собственности. Те же Ле Тюрк и Холкер были в первую очередь бизнесменами, пытавшимися организовать собственное производство. То же можно сказать и о знаменитом Альфреде Круппе, который, по легенде, сумел построить бизнес благодаря своим шпионским талантам. Его отец Фридрих Крупп, основавший сталелитейный завод, умер в 1826 году, когда Альфреду было всего 14 лет. В тот момент семейный бизнес был отягощен долгами и почти не приносил прибыли, поскольку качество вырабатываемой стали заметно уступало английскому. В 1838 году 24-летний Альфред Крупп уехал в Англию, где прожил несколько месяцев. По не-

подтвержденной информации, в Англии он под чужой фамилией устроился работать на одном из сталелитейных заводов, где и овладел секретами британского мастерства. Так или иначе, когда он вернулся в Германию, дела у его фирмы быстро пошли в гору, поскольку качество продукции значительно улучшилось. В пользу шпионской версии успеха Круппов говорит и та продуманная система контршпионажа, которую Альфред Крупп создал на своих предприятиях. Главный принцип этой системы сам пушечный король сформулировал так: «На заводе нужно иметь вторых доносчиков, чтобы они контролировали первых, и третьих, которые бы следили за вторыми». В уставе, который Альфред Крупп ввел на своих заводах в 1872 году, говорилось: «Независимо от издержек необходимо, чтобы за каждым рабочим постоянно наблюдали энергичные и опытные люди, которые получали бы премию всякий раз, когда задерживали саботажника, лентяя или шпиона».

«Меня били четверо негров-наемников»

Круппу было от чего волноваться, потому что к концу XIX века ситуация в мире индустриального шпионажа стала быстро меняться. Чем больше стран вступало на путь промышленной революции, тем большее значение приобретали технологии, а также информация о том, что задумали конкуренты. Крупные бизнесмены стали обзаводиться собственным штатом агентов, которые занимались сбором сведений, составляющих чужую коммерческую тайну. От их успеха порой зависело благосостояние их нанимателя. Агенты не брезговали и прямым вредительством, так что меры предосторожности Круппа не были напрасными.

Демонстрационная модель пулемета Максима отказывалась ломаться сама по себе — и ей помогли агенты Бэзила Захароффа

Мастером подковерных интриг конца XIX века по праву считается комиссионер шведской оружейной фирмы Nordenfeldt греческого происхождения Бэзил Захарофф. Он как никто другой умел сочетать законные и не совсем законные методы конкуренции. Захарофф привлек промышленных диверсантов, чтобы остановить триумфальное шествие пулемета Хайрама Максима. Захарофф распускал слухи о том, что «максимы» ненадежны и слишком сложны, чтобы быть пущенными в массовое производство, и изобретатель пулемета решил доказать всем, что его детище является образцом надежности. Во время презентации в Италии Максим приказал опустить пулемет на морское дно и оставить его там на сутки, чтобы на следующий день продемонстрировать, что вода не повредила оружию. Однако наутро пулемет не мог сделать ни одного выстрела, потому что ночью ныряльщики, которых нанял Захарофф, достали пулемет, подпилили боек и положили оружие на прежнее место. В итоге Nordenfeldt все же проиграла конкурентную борьбу Максиму, но Захарофф от этого только выиграл, потому что Хайрам Максим пригласил его к сотрудничеству.

Естественно, в такой обстановке возник спрос на промышленных шпионов, которые занимались бы своим делом профессионально, как, например, частные детективы — своим. И действительно, в начале XX века в Европе, но главным образом в США стали появляться конторы, предлагавшие подобные услуги. Одним из наиболее успешных промышленных шпионов 1920-х годов стал аме-

риканец Алмонт Камминг. Он основал собственную фирму, которая официально защищала предпринимателей от шпионов, а на деле занималась разведкой не реже, чем контрразведкой. Камминг изобрел немало уловок, помогавших ему в его непростом деле. Однажды перед ним встала задача ознакомиться с производственным процессом на предприятии, куда вход посторонним был строжайше запрещен. Камминг обратился в полицию и заявил, что его ограбили рабочие с этого завода. В результате шпион совершил прогулку по всем цехам в компании полицейского с целью «опознать» обидчиков. Преступников, конечно, не нашли, а шпионский заказ был выполнен. Своего ремесла Камминг не стеснялся и любил повторять, что «шпионаж — это часть большого бизнеса». Отчасти он был прав, потому что закона, напрямую запрещающего экономическую разведку, в те годы нигде в мире не существовало. Промышленный шпион мог попасть в тюрьму за кражу документов, за незаконное проникновение в офис, за взлом замка на складе готовой продукции и т. п., но только не за то, чем он в действительности занимался.

О том, какого размаха достиг бизнес промышленных шпионов в 1930-х годах, может свидетельствовать интервью, которое некий экономический разведчик дал американскому журналу Modern Mechanix в 1936 году. Аноним, в частности, рассказывал: «Вообще существует два основных метода сбора информации. Первый вариант предусматривает проникновение шпиона на завод будь то в качестве визитера, путем устройства на работу, или же тайно. Второй вариант — это когда вы получаете информацию от сотрудников путем подкупа, лести, организуя для них развлечения и т. п. Звучит просто, да? Но я уверяю вас, что эта работа требует квалификации и интеллекта не меньше, чем у военного разведчика. Подобно военной разведке, некоторые компании имеют агентурные сети по всей стране, которые доставляют информацию в центр. Однажды, например, я был заслан на предприятие под видом инженера-консультанта. Двое моих напарников работали на предприятиях той же компании в других городах вдоль атлантического побережья. У каждого из нас были свои агенты на разных предприятиях по всей стране, которые слали нам информацию. Мы обрабатывали ее и отсылали наверх к нашему боссу».

Кое-что из откровений анонимного шпиона напоминало детектив в стиле нуар: «Как и у военных разведчиков, дело не обходится без риска. Однажды я собирал факты по одной тяжбе, где на кону стоял не миллион, а двадцать миллионов долларов. За мной тогда наблюдал не один детектив, а целых девять детективов. Они работали по трое и менялись трижды в день. Я тогда пытался добиться правды от человека, который много знал, но боялся, что его убьют. Я припарковал машину на обочине, и уже через пару минут меня били четверо негров-наемников. Потом меня допросили с пристрастием и приказали убираться из города. Я избежал многих ловушек. Иногда потому, что был осторожен, но чаще мне просто везло».

В 1930-е годы, чтобы преуспеть в качестве промышленного шпиона, нужно было обладать известной изворотливостью и в идеале что-нибудь смыслить в технологиях, которые надлежало воровать. Однако уже очень скоро от корпоративных и частных разведчиков потребовалось куда больше специальных зна-

ний, потому что на сцену стали выходить технические средства слежения. После второй мировой войны настала эра всевозможных «жучков», и настоящий промышленный шпион был обязан разбираться в подобном оборудовании.

Микрофон в бокале

У всякой великой картины есть скрытый смысл,
а у некоторых — даже скрытые устройства

Первыми до прослушивания телефонов додумались нью-йоркские полицейские, еще в начале XX века предполагавшие таким образом бороться с преступниками и анархистами. Однако уже во второй половине 1940-х годов шпионские технологии шагнули в массы. В первый раз американская общественность узнала о том, что в стране кто-то кого-то прослушивает, в 1955 году, когда в Нью-Йорке на одной из квартир было обнаружено оборудование, позволявшее записывать разговоры тысяч горожан. За прослушивание были задержаны двое — Уолтер Эсман и Карл Рух, причем последний уже давно и весьма успешно трудился на ниве промышленного шпионажа. Эсман и Рух избежали тюрьмы, выдав своего заказчика — частного детектива, который таким способом пытался следить за женой своего клиента, однако это был единственный прокол в карьере Руха.

Карл Рух был экспертом в области прослушивания телефонов и в течение ряда лет сотрудничал с парфюмерной компанией Revlon. В 1950-е годы Revlon активно конкурировала с компанией Hazel Bishop. В мире косметики и парфюмерии любая удачная новинка может помочь компании закрепить за собой сегмент рынка, где ранее господствовали конкуренты, и поэтому охрана собственных секретов считалась приоритетной задачей в обеих фирмах. Особенно усердствовали в этом деле менеджеры Revlon. Нанятый ими Карл Рух установил прослушку на многих телефонах компании, чтобы корпоративная служба безопасности могла вовремя заметить возможную утечку информации. Вскоре президент Revlon Дэн Роджерс заметил, что в трубке его телефона что-то щелкает. Оказалось, что прослушивали даже самого президента, а провода, подключенные к его телефонному кабелю, вели в кабинет начальника службы безопасности компании Билла Трейси, бывшего агента ФБР, – он, собственно, и нанимал Руха.

Трейси удалось выкрутиться, поскольку записывающее оборудование было вовремя удалено из его кабинета. Чьим шпионом он был, так и осталось неизвестным. Зато Рух оказался классическим двойным агентом, который работал одновременно и на Revlon, и на Hazel Bishop. В один прекрасный день хозяин Hazel Bishop Рэймонд Спектор пришел к выводу, что его телефоны прослушиваются. Он заметил, что в последнее время Revlon постоянно оказывается на шаг впереди его фирмы, причем новинки Revlon копируют идеи, которые его компания как раз готовится воплотить. Как только Hazel Bishop собирается предложить покупателям новую помаду или крем, Revlon выбрасывает на рынок аналогичную продукцию. Желая выловить всех «жучков», Спектор нанял лучшего специалиста в этой области — Карла Руха, который мгновенно обнаружил несколько подслушивающих устройств. Однако Спектор не знал, что Рух, работая в то же время на Revlon, скорее всего, сам эти жучки и ставил. Не

удивительно поэтому, что после проверки Руха утечка ценной информации из стен Hazel Bishop продолжилась, и Revlon смогла в последующие годы серьезно потеснить конкурента. Не известно, много ли выиграли потребители от успехов Revlon, но они ничего и не потеряли, потому что вместо одной компании с качественной продукцией они получили две.

Вскоре на рынке шпионских услуг сформировалось целое направление, связанное с разработкой и применением всевозможных подслушивающих и подглядывающих устройств. В 1960-е годы появились настоящие гении прослушки, которых в те времена уважали примерно так же, как сегодня уважают самых способных хакеров. Американец Бернард Спиндель мог похвастаться тем, что своего первого «жучка» смастерил в 12 лет и, спрятав его в корзине с углем, подслушивал, что говорят взрослые. В зрелые годы Спиндель стал работать на коррумпированного профсоюзного босса Джимми Хоффу, которому постоянно требовалось кого-нибудь подслушать. Спиндель работал на всех, кто готов был платить: на корпорации, на мафию и даже на федеральные власти, причем занимался своим бизнесом почти легально, потому что правительственные структуры нуждались в его талантах не менее чем теневые. Другой специалист того же уровня — Хол Липсет специализировался на создании подслушивающих устройств, замаскированных под всевозможные «с виду обычные» предметы. Вершиной его творчества стало передающее устройство, замаскированное под маслину, лежащую в бокале. Коктейльная палочка, воткнутая в «маслину», была антенной.

Друг советского народа

«Жучки», произведенные в странах социализма,
обычно были технически отсталыми,
но это не мешало им находиться на передовых рубежах

Пока умельцы совершенствовали шпионскую технику, в мире появлялось все больше сил, заинтересованных в промышленном шпионаже. Страны победившего социализма стремились преодолеть свою технологическую отсталость, на Востоке просыпались «азийские тигры», да и западноевропейские государства тяготились отставанием от США. В 1960-е годы к активному промышленному шпионажу вернулась Франция, причем, по легенде, генерал де Голль лично приказал своим спецслужбам помочь французской промышленности. Главными европейскими шпионами во времена холодной войны считались страны Варшавского договора, прежде всего СССР. На Западе было принято считать, что экономические секреты воруют агенты зловещего КГБ, однако это было так далеко не всегда. Часто советской разведке помогали все те же добропорядочные западные бизнесмены, подрабатывавшие промышленным шпионажем. Наиболее успешным из таких предпринимателей был житель Западной Германии Ричард Мюллер, который в 1970-е годы переправил с Запада в СССР технологическую информацию и оборудование, оцененное экспертами в $30 млн.

Мюллер родился в 1948 году, так что на момент начала своей разведывательной деятельности он был еще очень молод. Известно, что в начале своей предпринимательской карьеры он ездил в Советский Союз и побывал в Зелено-

граде, считавшемся одним из центров советской электроники. В 1970-е годы СССР был заинтересован в налаживании производства полупроводников, однако не располагал соответствующими технологиями и оборудованием. Восполнить пробел должен был Мюллер, которому, похоже, был открыт неограниченный кредит. Мюллер основал в ФРГ собственную фирму и привлек к делу еще несколько предпринимателей, главным образом западных немцев. Группа Мюллера стала работать в составе синдиката под названием СТС, во главе которого стояли гражданин ФРГ Вернер Бруххаузен и бывший советский гражданин с американским паспортом Анатолий Малюта.

СТС состоял из примерно 20 компаний, работавших в области электроники. Но главной их задачей было прикрытие деятельности группы Мюллера, тайно скупавшей технологии и оборудование для завода по изготовлению полупроводников, который планировалось построить в СССР. В задачу Мюллера также входил поиск бизнесменов, готовых сотрудничать с Советским Союзом. Наиболее активно группа Мюллера действовала с 1977 по 1980 год, после чего ее деятельность была пресечена американскими и западногерманскими спецслужбами. Бруххаузен и Малюта предстали перед американским судом и были признаны виновными в незаконной торговле технологиями, а Мюллер исчез, и следы его затерялись. Деятельность шпиона принесла свои плоды — в 1985 году в СССР открылся первый завод по производству полупроводников.

Основатель Apple Стивен Джобс был удивлен, когда узнал, что его компьютеры уже выпускают на Тайване

В 1980-е годы в мире промышленного шпионажа зажглись новые звезды — фирмы из Тайваня, Гонконга и Южной Кореи воровали все, что только можно было украсть. В частности, компания Apple была вынуждена постоянно судиться с тайваньскими фирмами, которые буквально копировали их компьютеры. Фирма Multitec, например, не стеснялась выпускать обновленные версии своего компьютера после каждой новой версии компьютера Apple. При этом изделия тайваньских мастеров в деталях копировали детище американцев. Еще дальше пошла тайбэйская фирма Guan Haur Industrial, которая скопировала не только сам компьютер, но даже руководство пользователя, написанное основателем Apple Стивеном Возняком. Наконец, компания Sunrise Computer Service, базировавшаяся в том же Тайбэе, не постеснялась позаимствовать у Apple даже название. Свой компьютер Sunrise назвала Apolo, что в китайской транскрипции звучит точно так же, как Apple. При этом тайваньские копии стоили порядка $500, в то время как персональные компьютеры от Apple стоили чуть менее $1,5 тыс., так что потребители, как всегда, только выигрывали от деятельности экономических разведчиков. Методы работы дальневосточных шпионов в то же время оставались вполне традиционными: сбор открытой информации, изучение готовой продукции конкурента, подкуп его сотрудников и т. п.

Впрочем, шпионили не только иностранцы. В США и других развитых странах промышленный шпионаж стал неотъемлемой частью корпоративной культуры, и отказать в удовольствии последить за конкурентами не могли себе даже руководители крупнейших компаний с мировым именем. Бывший топ-менеджер General Motors Джон Делориан, покинув корпорацию, занялся разо-

блачениями нравов, царящих во флагмане американского автопрома. В частности, Делориан сообщил миру, что GM содержала двух шпионов, работавших у извечного конкурента корпорации — Ford Motor. «Однажды, придя на совещание административного совета, – говорил Делориан, – я увидел высших чинов, склонившихся над сверхсекретным документом, в котором раскрывалась вся структура производственных расходов „Форда“. В докладе был дан полный анализ издержек производства и распределения готовой продукции конкурента». Сам Делориан впоследствии погорел как раз на тайной операции. Уйдя из GM, он создал собственную автомобильную компанию DeLorean Motor и начал выпускать практически безупречные автомобили, которые практически не ломались. Конкурентам, включая GM, это, конечно же, не понравилось, и они приложили все усилия к тому, чтобы DeLorean Motor обанкротилась. Делориан пытался избежать банкротства, занявшись контрабандой наркотиков, но недоброжелатели, втравившие его в эту историю, сдали его полицейским вместе с крупной партией кокаина. Избежать тюрьмы ему помогло только искусство адвокатов.

Джон Делориан разоблачал промышленных шпионов из General Motors, пока его самого не разоблачили как наркокурьера

Между тем надвигалась эпоха интернета и мобильных телефонов, которая значительно расширила возможности промышленных шпионов. Шпионящие устройства в то же время становились все более миниатюрными и сложными. Сейчас, например, существуют «жучки», выглядящие как батарейки для мобильных телефонов. Опытному шпиону достаточно несколько секунд подержать в руках мобильник ответственного лица из интересующей его компании, чтобы его телефонные разговоры утратили конфиденциальность. Возможности же компьютерного взлома оказались практически неограниченными.

Стремясь оградить свою индустрию от посягательства зарубежных и отечественных шпионов, американский конгресс принял в 1996 году Акт о борьбе с экономическим шпионажем, который сделал, наконец, незаконной саму деятельность коммерческих разведчиков. Уже в 1997 году несколько шпионов отправились под суд. В частности, попались американцы китайского происхождения Шу Каило и Честер Хо, которые пытались украсть технологию синтеза противоопухолевого препарата «Таксол» у компании Bristol-Myers Squibb. В том же году были пойманы житель Теннеси Стивен Дэвис, укравший технологию производства новых бритв от Gillette, и бывший сотрудник Kodak Харольд Уорден, который приторговывал секретами бывшего работодателя. Однако остановить волну промышленного шпионажа не помогли ни законы, ни показательные аресты. Объясняется это просто. Дело в том, что Bristol-Myers Squibb затратила на разработку технологии производства «Таксола» порядка $15 млн, а неназванная тайваньская компания, которая хотела купить эту технологию, предлагала за нее шпионам $400 тыс. Таким образом, промышленный шпионаж чрезвычайно выгоден как для самих шпионов, так и для тех, кто пользуется их услугами. Последняя история с Ferrari и McLaren — яркое тому подтверждение. Секретная документация Ferrari просто не могла попасть в руки McLaren без посредничества промышленных шпионов. Впрочем, Международная федерация

автоспорта не стала наказывать McLaren, потому что никому не удалось доказать, что команда извлекла какую-либо выгоду из этой кражи. Таким образом, промышленный шпионаж остается не только одним из самых выгодных, но и одним из самых недоказуемых видов преступлений, поэтому подобные скандалы будут случаться и впредь.

♦ ♦ ♦ ♦ ♦

9. Промышленный шпионаж*

Промышленный шпионаж – это добывание противозаконным путем конфиденциальных сведений о деятельности конкурентов, хищение сведений, составляющих ноу-хау, ведение недобросовестной конкуренции, получение персональных данных для их использования в преступных целях. Современный промышленный шпионаж — это еще и сознательное приведение в негодность производственного оборудования, информационных систем, оказание психологического давления на сотрудников с целью дестабилизации деятельности конкурента.

В наших условиях это попытка некоторых фирм стать абсолютными монополистами в городе или даже регионе. Для этого применяются подкуп, угрозы, шантаж сотрудников, сманивание грамотных специалистов от конкурентов, кражи баз данных и описаний технологических цепочек.

ИСТОРИЯ

Промышленный шпионаж имеет многовековую историю, но за это время его методы не претерпели существенных изменений. В то же время, с ослаблением роли государства, он приобретает все большую силу и размах. Достаточно сказать, что все государства мира не чураются красть друг у друга новые технологии, заманивать узких специалистов, тем самым создавая преимущества для себя за счет других. Это общая практика.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Чаще всего применяется подкуп сотрудников конкурирующей фирмы. Сейчас используется также внедрение своих людей в соперничающую структуру для кражи сведений, либо дезорганизации деятельности предприятий. В уголовном кодексе РФ эти деяния классифицируются как взятка, превышение служебных полномочий, злоупотребление служебным положением, посягательство на жизнь и здоровье...

СЪЕМ ИНФОРМАЦИИ

В настоящее время все более актуальной становится проблема съема информации с технических каналов связи с помощью специальной аппаратуры при работе факсов, телефонов, компьютеров. «Новинкой сезона» является внедрение в информационные сети потенциальных соперников «червей» компьютерных вирусов и вредоносных программ.

---

* Материал подготовлен департаментом экономической безопасности ТПП РФ на основе информации А. Брединского – руководителя проекта «Безопасность для всех». Торгово-промышленные ведомости (Москва), 2004 г. № 5.

А начиналось все так «романтично», когда доморощенные «хакеры» пытались взламывать компьютерные сети «просто так»...

ЖУЧКИ

Незаконное внедрение в офис, производственное помещение, либо в жилище важных персон т.н. «жучков» – самый простой и относительно недорогой способ получения информации о конкуренте. Законодательством РФ предусмотрено право проведения таких мероприятий только для спецслужб.

В свою очередь комплексной защитой информации могут заниматься только те организации, которые имеют на это лицензию, располагают сертифицированными средствами защиты.

И не стоит попадаться «на удочку» дилетантов и мошенников, нанимая их для поиска «закладок». Дилетантизм и желание сэкономить в таком важном вопросе часто ведут к непоправимым последствиям.

ХИЩЕНИЕ И УНИЧТОЖЕНИЕ

Хищение документов и иных носителей информации часто приобретает тотальный характер и ведет к потере необходимых баз данных, без которых просто «разваливается» производство. Кража промышленных образцов зачастую сводит на нет преимущества от проведения многолетних научных исследований.

ТИХАЯ ВОЙНА

У читателя возникает справедливый вопрос. Если промышленный шпионаж так развит, почему мы ничего не слышим о его результатах. Ведь криминальная хроника изобилует сообщениями об убийствах и иных «громких» преступлениях, мировая пресса постоянно сообщает о высланных шпионах. А где же разоблаченные промышленные шпионы?!

Во-первых, часто жертва не догадывается о том, что она стала объектом покушения.

Во-вторых, пробелы в законодательстве часто не позволяют привлечь кого-либо к уголовной ответственности.

В-третьих, пострадавшие не спешат сообщить широкой общественности о том, что они стали объектом нападения.

СЕКРЕТ УСПЕХА

Сегодня для того, чтобы заниматься успешным бизнесом даже в таком тихом городе, как Горно-Алтайск, явно недостаточно обеспечить чисто физическую защиту и охрану. Построение надежной системы защиты информации – дело сложное и дорогое. Однако за этим – будущее цивилизованного бизнеса.

Промышленный шпионаж имеет многовековую историю, и в этом легко убедиться, внимательно прочитав страницы древних манускриптов. Но, несмотря на это, большинство бизнесменов продолжают считать, что им это не грозит. Почему же эти опасные заблуждения СТОЛЬ СИЛЬНЫЙ?

Причиной является неправильное понимание самого термина. Рассуждают примерно так: промышленный – следовательно, связанный с промышленностью и производством, а большинство бизнесменов занимаются перепродажей или оказанием услуг, значит, считают они, мне это не грозит. Шпионаж обычно

ассоциируется с разведчиками, спецслужбами и различными тайными операциями.

На самом же деле термин «промышленный шпионаж» вовсе не означает, что его жертвами становятся производства государственного уровня. Этим термином принято обозначать попытку получения информации о конкурентах, хищение коммерческой тайны и «ноу-хау», ведение недобросовестной конкуренции. И совершенно неважно, крупная это корпорация или небольшая фирма. Конкуренты есть у всех, разница лишь в методах, которыми они пользуются.

В советское время промышленного шпионажа внутри страны практически не существовало. Все попытки узнать тайны и секреты исходили из-за границы. А государство очень ревностно хранило свои секреты, поставив на службу государственный аппарат. Надо признать, что система была действительно эффективной. Те, кто работал в государственных учреждениях, не понаслышке знают о «первых отделах», в задачу которых входила безопасность и секретность предприятия. Система исправно работала, и каждая попытка «шпионажа» становилась чрезвычайной ситуацией, которая расследовалась Комитетом государственной безопасности. Но после перестройки система начала быстро разрушаться. Кстати, возможно, это делалось намеренно. И в один прекрасный момент вдруг оказалось, что «спасение утопающих – дело рук самих утопающих». А люди за долгие годы привыкли, что о их безопасности заботятся другие. Долгое время находясь под «крышей» государства, наш человек разучился сам себя защищать. И вот результат. Сегодня, за редкими исключениями, в коммерческих фирмах забота о безопасности отсутствует. Наверняка кто-то скажет: неправда – у нас полно секьюрити. Это еще одно из заблуждений. Охрана – лишь часть безопасности. И перед охранниками стоят совершенно другие задачи.

Но все же вернемся к вопросу – кто может стать жертвой промышленного шпионажа? Ответ прост – практически любой бизнесмен. Более того, крупной фирме разглашение информации может нанести существенный, но все же поправимый ущерб. А для небольшого предприятия такое разглашение станет смертельным и приведет к банкротству. Как считают западные специалисты, утечка 20% коммерческой информации в 60-ти случаях из 100 приводит к банкротству фирмы. Ни одна даже преуспевающая фирма США не просуществует более трех суток, если ее информация, составляющая коммерческую тайну, станет известной. Тот, кто наивно считает, что у него нет информации, которую нужно защищать, очень сильно ошибается. Получение прибыли - это уже предпосылка стать жертвой.

Наличие конкурентов – еще одна серьезная предпосылка. Думать, что все будут соблюдать правила джентльменской игры – большая ошибка. Конкуренты попытаются сделать все возможное и невозможное, чтобы захватить весь рынок и стать монополистом. А как это сделать? Очень просто: побольше узнать о сопернике и его достоинства превратить в его же недостатки. В условиях, когда о своей защите никто не заботится, такая работа не составит особого труда. Кстати, интересный факт из практики: на десяток обращений с просьбой собрать информацию о конкурентах приходится примерно одно о защите своей

информации от шпионажа. Иногда это доходит до абсурда. Бизнесмен просит провести сбор и анализ информации, а на предложение защиты его информации и проведение контрразведывательных мероприятий говорит: «Да кому я нужен, никто обо мне ничего собирать не будет». Человек хочет знать больше о конкурентах, а допустить у них такое же желание не может. Существует очень простой способ определить, есть ли на предприятии конфиденциальная информация. Психологи называют это «ролевыми играми». Нужно представить себя на месте злоумышленника (преступника, конкурента или другого недоброжелателя). А представив, подумать, какую именно информацию вы бы хотели узнать и что будет вам полезно в осуществлении своих «грязных» планов. Если вы представили и пришли к выводу, что ничего – не расстраивайтесь. У вас просто плохо развито воображение, потренируйтесь еще. Привлеките к этому делу близких родственников и знакомых, возможно, они обладают лучшими аналитическими способностями и смогут помочь вам. Возникает справедливый вопрос. Если это явление так развито, почему мы ничего не слышим о нем?

Значит ли это, что его нет? Наоборот, промышленный шпионаж относится к категориям, которые юристы называют «латентными» (скрытыми). Этому способствует ряд причин:

- во-первых, зачастую сама жертва не подозревает, что стала объектом покушения со стороны промышленных шпионов;
- во-вторых, в условиях, когда законодательство изобилует многочисленными пробелами и новые отношения остаются без должного регулирования, очень сложно привлечь кого-либо к ответственности, ведь в праве существует принцип «nullum crimen nullum poena sine lege» (лат.) – «нет преступления и наказания без закона»;
- в-третьих, даже если преступление было зарегистрировано, то практически нет специалистов, которые могли бы его расследовать. Такие преступления имеют особую специфику. Надо отметить, что в России ситуация нормализуется. Созданное специализированное подразделение по борьбе с преступлениями в сфере высоких технологий успешно борется с такого рода правонарушениями;
- в-четвертых, те, кто стали жертвами промышленного шпионажа, не спешат заявить об этом широкой общественности, справедливо опасаясь за свое реноме и не желая «выносить сор из избы».

Вообще-то в отношении к промышленному шпионажу можно выделить три этапа.

Беспечность и наивность. На этом этапе бизнесмен спокойно живет и работает, будучи в полной уверенности, что у него все в порядке и он и его бизнес в безопасности. Состояние это может длиться очень долго, пока не произойдет катастрофа. Тогда наступает вторая стадия.

Технофобия. Выяснив, что сегодня можно узнать практически любую информацию при помощи технических средств, бизнесмен хватается за голову и начинает подозревать наличие «жучков» даже в столовой ложке. Попытавшись защититься, он выясняет, что защита информации при помощи технических

средств – дело не дешевое. Да и к тому же уровень защиты напрямую зависит от вложенных средств, а 100 % гарантии защиты вообще не существует. Вот тут происходит переход на третью стадию.

Пессимизм. Наслушавшись об уровне современной техники, подсчитав стоимость защиты, бизнесмен приходит к неутешительному выводу – если захотят что-то узнать, все равно узнают. А защита нам не по карману. Поэтому лучше ничего не делать, авось да пронесет.

И в результате, действительно, ничего не делается. На самом же деле, несмотря на сложившийся миф, большинство информации добывается не техническими средствами, а оперативной работой. Никто не станет взрывать бронированную дверь, если в помещении открыто окно или ключи от двери лежат под ковриком. Также и в шпионаже. Зачем тратить деньги на подслушивающую аппаратуру и рисковать, когда можно просто незаметно расспросить работников фирмы обо всех секретах. Или же, зайдя в кабинет на время, «позаимствовать» секретные документы. В условиях, когда на предприятии меры безопасности отсутствуют, такой способ намного более эффективен, к тому же прост, дешев и безопасен.

В следующих публикациях мы продолжим эту тему и подробнее рассмотрим, какие методы используются для получения информации и откуда обычно идет утечка информации.

♦ ♦ ♦ ♦ ♦

10. Промышленный шпионаж – основа информационных войн*

«Тот, кто владеет информацией, тот владеет миром»
У. Черчилль

В явной или скрытой форме информационная борьба между странами мира в защиту своих собственных интересов и в осуществлении противоборства за границы политического влияния, рынки и ниши сбыта, спорные межгосударственные территории ведется постоянно. В этой борьбе все заметнее проявляются формы и методы информационного противостояния, получившие в СМИ название «информационная война».

Как правило, в таких интеллектуальных войнах применяются запрещенные и грязные способы ведения промышленного шпионажа. К ним относятся кражи и несанкционированный съем информации о технологии НОУ-ХАУ, о физических и юридических лицах, которые в последующем используются для производства продукций-подделок и создания различного рода компроматов. Далее, спланированные конкурентами контакты, перерастающие в подкуп, угрозу или шантаж и, в конечном итоге, склонение к инициативному сотрудничеству. Способом ведения промышленного шпионажа следует назвать и несанкционированное копирование с помощью оргтехники конфиденциальных документов.

* По материалам журнала «Факт», автор Вячеслав Климов

Активно используют проникновение в персональные компьютеры и компьютерные сети с целью получения информации закрытого характера или персональных данных. И, наконец, существует преднамеренное блокирование работы средств защиты информации, нарушение мер разграничения доступа или допуска к сведениям, данным или документам, отнесенным к коммерческой и иной тайне.

Причины возникновения рисков и угроз разнообразны. Во-первых, необоснованные, а порой и противоправные, корпоративные информационные отношения между группами субъектов экономической деятельности. Во-вторых, отсутствие должного правового обеспечения (прикрытия) или механизмов выполнения законодательных актов в сфере информационной безопасности. В-третьих, неурегулированность информационного рынка, проявление открытых элементов промышленного шпионажа, что в свою очередь и приводит к недобросовестной конкурентной борьбе. По официальным данным, только 25-30% национальных информационных ресурсов России созданы за счет финансовых средств налогоплательщиков органами власти – от федеральной до местной. Остальные находятся в частных руках отечественных и зарубежных собственников. И весь груз защитных мер по охране информации, информационных ресурсов и технологий ложится на плечи их владельцев.

Разведка и шпионаж

Существуют два метода сбора информации: открытый и тайный. При тайном методе используются сотрудники разведки и агентура, а также различные технические средства. После второй мировой войны с помощью технических средств добывается все большее количество необходимой информации, сейчас, вероятно, до 80-90%: Технические методы сбора информации обладают рядом преимуществ, которые способствуют все более широкому их применению: относительная безопасность исполнителей по сравнению с агентурной разведкой и несомненная точность и актуальность информации». Исходя из положения о том, что государственная разведка является прародителем промышленного шпиона, можно сделать однозначный вывод – вышеперечисленные методы находят свое применение и в промышленном шпионаже.

Эксперты отмечает, что современная научная, промышленная и экономическая информация большей частью легко доступна. 95% интересующих Вас данных можно получить из специальных журналов и научных трудов, отчетов компаний, внутренних изданий предприятия, брошюр и проектов, раздаваемых на ярмарках и выставках. Цель шпиона – раздобыть оставшиеся 5% информации, в которой и кроется фирменный «секрет», «тайна мастерства». Излюбленное оружие современного промышленного шпионажа – применение новейшей разведывательной электронной аппаратуры. Это оружие обслуживается не только квалифицированными специалистами из различных областей науки, техники и производства, но и кадровыми шпионами разведывательных спецслужб. Большинство из них в последующем охотно меняет опасное ремесло военных разведчиков на более прибыльное амплуа похитителя частных промышленных секретов. В последние годы ряд западных и отечественных корпораций

и монополий стали позволять себе роскошь – открыто иметь в штате должности контрразведчиков по промышленному шпионажу.

Собственно промышленный (экономический, информационный, технический, компьютерный) шпионаж, получивший свое развитие в мире в конце 50-х, по-прежнему является неотъемлемой частью бизнеса как на западе, так и у нас. При этом уровень его воздействия возрастает из года в год и совершенствуется, исходя из роста информационных технологий и средств их применения.

Промышленный шпионаж

По западной теории, промышленный шпионаж – это добывание законным и незаконным путем у конкурентов сведений или информации из области научных исследований, производства продукции по наиболее перспективной технологии, а также персональных данных с целью их использования в корыстных целях. Современный промышленный шпионаж это, прежде всего, информационный шпионаж в сфере жизнедеятельности человека. И направлен он на решение основной задачи – получение финансовой, политической и иной прибыли (превосходство производственной технологии, оборонного потенциала, партии или личности над другими).

Промышленный шпионаж существует с эпохи зарождения средневековых цеховых производств. Например, в 1295 году в Берлине специальным предписанием властей иностранцам запрещалось работать на местных ткацких станках, дабы те «не узнали секретов их работы». Каменотесы Страсбурга в 1459 году приняли суровое решение, запрещающее «всем купцам ли, болтунам ли открывать секреты, коими они (каменотесы) могут ловко и быстро работать». В XVII веке в немецком городе Насау за разглашение иностранцам секретов кузнецкого мастерства виновных подвергли смертной казне. В XIX-XX веке, когда прогресс человеческой цивилизация в области математики, физики, радиоэлектроники, кибернетики, связи, информатики достиг высокого уровня, во многих государствах мира зародились разведывательные и контрразведывательные спецслужбы, на вооружение которых поступали средства, способные решать задачи по сбору, обобщению информации, так необходимой для принятия государственных решений. Применяемые спецслужбами способы и методы получения нужной и важной информации в скором времени составили основу осуществления промышленного шпионажа.

Развитие электроники и полупроводниковой технологии привело к повсеместному использованию современных технических устройств и средств в решении задач, возложенных на разведку, а затем и на промышленный шпионаж. Оказывается, выгоднее потратить определенную сумму финансовых средств на добывание чужой технологии, чем в несколько раз большую – на разработку и создание собственной. А в политике, бизнесе или в военном деле выигрыш в получении таких данных становился просто бесценным.

Бывший директор ЦРУ США В. Чейтс еще в 80-е годы заявлял, что: «в современных условиях наше ведомство переходит от добывания чисто военной информации к сбору информации экономической». Этого и должны опасаться современные отечественные производители, предприниматели и бизнесмены со стороны западных конкурентов. Ведь ни для кого сегодня не является тайной,

что техническими средствами разведки владеют как государство, так и юридические и физические лица. Ибо конкуренция и промышленный шпионаж в условиях рыночной экономики и нецивилизованных рыночных отношений также неразлучна, как неразделима. И хотя для нас это абсолютно новое явление, мы должны быть готовы к нему, – утверждают многие российские эксперты и специалисты в области обеспечения информационной безопасности. Шпионские страсти, некогда разоблаченные и осмеянные отечественной пропагандой, сегодня бушуют и в столице, и в далекой российской провинции – везде, где ведется конкурентная борьба, особенно, там, где она осуществляется недобросовестными методами.

Промышленный шпионаж в условиях быстрого развития информационной технологии – это конкретный и очень эффективный вид борьбы за монополию. С открытостью российского общества, вызванного объективными и субъективными причинами, он со своими «белыми и черными» пятнами вливается в экономику России.

Шпионаж и информационные войны

Методы и способы ведения промышленного шпионажа постоянно переходят в современные информационные войны – объективно существующее специфическое противостояние алгоритмов и технологий, идей и мыслей, реализованных в информационных устройствах и средствах, предназначенных для нанесение экономического, политического, финансового, психологического и иного урона (ущерба) противнику или конкуренту, и, прежде всего, их информационным и телекоммуникационным системам (сетям), информационным технологиям, ресурсам и средствам.

Информационная пропаганда, в прошлом осуществляемая друг против друга США и СССР, военные и экономические союзы и блоки в целом, разведслужбы и радиотелевизионные «голоса» в отдельности можно причислить к испытательному полигону современных информационных войн. Тогда это противоборство называлось «холодной войной». Ее идеологическая сущность сводилась к одному – убедить народ страны в правильности государственной политики и необходимости привлечении огромных финансовых средств для поддержания (или наращивания) своих вооруженных сил, так как, по мнению идеологических «мыслителей», противостояние в этой войне неизбежно должно было перерасти в мировой вооруженный конфликт.

Поддержка национально-освободительных движений, локальных войн и режимов власти с помощью штыков привела к переделу исторических и географических (этнических) границ, к гуманитарным и иным катастрофам практически на всех континентах. Борьба с «красными ведьмами», диссидентами, уклонистами, за свободу слова и печати позволила создать условия для возникновения и процветания коррупции и криминала в большинстве развитых стран мира. Оба лагеря старательно раскручивали гонку вооружения и милитаризацию промышленности, приведшие многие страны к дестабилизации экономики и к социальным катаклизмам. Результаты не замедлили ждать. Раздел сферы влияния закончился падением Берлинской стены и распадом СССР, социалистического лагеря и Варшавского договора.

Современный промышленный (информационный) шпионаж представляет симбиоз двух направлений партийно-идеологического противоборства мировых систем – сочетание информационного и психологического воздействие на сознание человека. Это сочетание называют третьей мировой информационно-психологической войной. Наиболее опасным из перечисленных направлений такой войны является возможность применения способов воздействия на психику человека помимо его воли. Возможность отрицательного воздействия информации на мозг человека создает предпосылки для производства психологического (психотронного) оружия, которое атакует подкору головного мозга специальными энерго-информационными полями.

Психологическое оружие современности – это совокупность всевозможных форм и методов скрытого подавления в человеке таких его функций как сознание, поведение и здоровье с целью решения задач политического, военного, экономического и иного характера, в том числе осуществления успешной конкурентной борьбы на рынке сбыта. При этом основной формой такого целенаправленного воздействия является способ непосредственного (или через спецсредства) ввода в подсознание человека, минуя его форму осознанного контроля, событий и нужной информации, которая позволяет осуществить над ним необходимые целевые действия. Эти действия и являются главной формой тайного оружия любой информационной войны.

Мощным оружием воздействия на сознание людей являются и СМИ. Оно используется в виде тиражирования информационных «мифов» политического, экономического, сексуального, криминального или иного характера. СМИ, как опытные манипуляторы, обеспечивают «массовую» поддержку даже той политической власти, которая не отвечает чаяньям большинства народонаселения страны. Пресса, телевидение, радио, кино, аудио-видео и другая компьютерная продукция – вот современный театр «боевых действий».

Информационный полигон – Чечня

За последнее время все чаще формы, методы и способы ведения промышленного шпионажа, применяемые в информационных войнах, приводят к прямым вооруженным конфликтам. Примером информационного противостояния российских политиков с сепаратистами могут служить события (развертывание испытательного полигона новых технологий информационной войны) в Чеченской республике. Эта война началась как непонимание или различие в трактовке понятий о суверенитете, а закончилась вооруженной борьбой с организованной преступностью, террористами и радикальным исламизмом.

Исторические события 1-ой чеченской войны (1994-1996 гг.) свидетельствуют о том, что проигранная исполнительными и военными органами власти информационная война того периода, как в теории, так и в практике, способствовала принятию неправильных, а порой и вредных решений по исключению чеченского синдрома. В тот период 70% отечественных и западных СМИ были, условно называя, на стороне чеченских сепаратистов, кто по объективным политическим мотивам, кто – из корыстных соображений, т.е. финансовых интересов. С учетом этих факторов и возникли столь существенные потери со стороны федеральных войск, в три раза превысившие потери при проведении вой-

сками НАТО операции «Буря в пустыне». Но более горькими были сами результаты этого этапа событий – подписание соглашения с самопровозглашенными лидерами Ичкерии, как закономерного результата, прежде всего, неудачного ведения информационной войны.

Отличительной чертой 2-ой чеченской войны является то обстоятельство, при котором федеральная власть, правильно поставив идеологическую работу с российским обществом и СМИ, успешно ведет информационную войну на театре военных действий, отражая и реагируя на все негативные факторы, объективно возникающие в ходе осуществления антитеррористической операции. Несмотря на значительные людские потери со стороны военнослужащих и мирного населения, на возникновение сложной гуманитарной ситуации и постоянного давления (порой предвзятого и субъективного по своей сути) со стороны Запада, это существенным образом не сказывается на общественном мнении россиян в понимании ими предпринимаемых действий.

Кстати, основанием для начала проведения НАТО «миротворческой» операции в Косово послужили ложные сведения о, якобы, существующем геноциде сербов над албанцами. Результат столь серьезно обставленной информационной войны против югославского народа оказался поразительным: по оценке европейских экспертов жертвы мнимого геноцида завышены СМИ в 40 (?!) раз, а нанесенный югославской экономики ущерб составляет сотни миллионов долларов, не говоря о том, что противостояние албанцев против сербов не прекратилось.

Избирательные технологии – та же война

В российских СМИ появляется все больше информационной продукции в виде заказных авторских программ на ТВ (получивших название – телевизионные «киллеры») и «пиаровских» статей в периодической печати. Их теневое и негативное воздействие на многие политические и другие процессы с точки зрения объективности и «независимости» (от государства, но не от возможностей финансовых спонсоров) хорошо проявились при проведении избирательной компании в Государственную Думу и, с еще большой силой, проявляются в ходе выборов Президента России.

Список «грязных» избирательных технологий впечатляет. К ним относится выявление и опубликование компромата на политиков, не угодных власти, в виде высвечивания сведений их личной жизни и здоровья, противоречащих основам правовой защиты конфиденциальной информации. Таким образом происходит запугивание и шантаж в отношении кандидатов и членов их семей, в т.ч. не доказанное законным порядком участие в коррупции и других правонарушениях. Обычно правоохранительные органы отказывают потерпевшей стороне в привлечении к уголовной или иной ответственности тех, кто опубликовал заведомо ложные сведения. Не менее пассивна и судебная власть. Но случается, сам кандидат специально организует «утечку» информации из своего прошлого, чтобы создать ситуацию под названием «чем хуже, тем лучше».

К следующей информационной технологии следует отнести попытки подкупа отдельных кандидатов с «просьбой» в отказе от участия в избирательной компании и, особенно, в тех округах, где количество кандидатов очень боль-

шое. Возможно и нарушение порядка финансирования и представления равных правовых условий для освещения деятельности кандидатов.

Национальной традицией стало создание определенных льгот и привилегий для кандидатов «от власти», в т.ч. предоставление удобного эфирного времени, полос в центральных СМИ, вопреки официального жребия. Это полновесно сочетается с исполнением ими должностных «возможностей» при проведении избирательной компании, привлечением управленческого аппарата, информационных и других ресурсов для осуществления избирательной агитации и работой с электоратом. Подобная практика благоволит к нарушению порядка и условий по созданию партий, движений, блоков и фронтов (сроков регистрации, создании региональных отделений и т.д.), а также отсутствию у них экономических, социально-политических программ или платформ действий. По сравнению с этим, организация митинга, собрания, съезда и другого массового мероприятия в поддержку того или иного кандидата, которое противоречит законодательству о выборах в вопросах их организации и правильности финансирования, кажется невинной шалостью.

Зачастую в избирательной компании участвуют сомнительные имиджмейкеры, политологи и фонды, занимающиеся исследованием «гласа народа». А отсутствие у кандидатов культуры в ведении полемики, дискуссии со своими оппонентами, как правило, сводящейся к необоснованным с точки зрения здравого смысла обвинениям, даже неловко относить к информационным технологиям.

Избирательные технологии – это эффективное использование современных информационных ресурсов, средств и систем с целью повышения избирательских возможностей, в т.ч. подделки необходимого количество подписей с помощью компьютерной графики или открытия сайта в Интернет. Это укоренившаяся практика оплаты (в денежной форме или натуральном эквиваленте) тех, кто собирает подписи, развешивает листовки, участвует в массовых мероприятиях по поддержке кандидата и его платформы. Но самой опасной избирательной технологией является создание виртуальной партии «ПРОТИВ ВСЕХ», формирующей в обществе слой нигилистов, что ведет к коренной ломке конституционных основ – права российских граждан быть избранным и участвовать в выборах.

Мишени в целую систему

Сегодня информационная война – это последовательное продолжение промышленного шпионажа – явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере. В Уставе МО США дано следующее определение: «Информационная война состоит из действий, предпринимаемых для достижения информационного превосходства в интересах национальной военной стратегии и определяемых путем влияния на информацию и информационные системы противника, при одновременной защите собственной информации и своих информационных систем».

Информационное оружие наносит максимальный урон в том случае, если оно применяется против информационно-телекоммуникационных сетей посто-

янно и осмысленно. Причем, мишенью являются все элементы информационных технологий, ресурсов и систем, мыслительная часть человеческой деятельности, имеющие потенциальную возможность для перепрограммирования (воздействия на психику). Заставить противника или конкурента изменить свое поведение можно лишь с помощью создания информационной угрозы (риска). В современной информационно-психологической войне приоритет отдается скрытым (тайным) угрозам, создаваемым на основе аккумулирования человеческих знаний в информатике.

И только открыто говоря о формах и методах ведения промышленного шпионажа, информационной войны можно осуществить организационно-технические меры по объективному противодействию этим угрозам, а также предостеречь российский бизнес от потенциально наваливающего на него информационного оружия современности.

♦ ♦ ♦ ♦ ♦

11. Промышленный шпионаж — реальность в СНГ

Шпионаж может быть государственным (политическим), военным, экономическим и т.д. Понятие «шпионаж» означает получение или добывание каких-либо сведений, представляющих определенный интерес, исключительно незаконными методами. Там, где речь идет о законных методах, то это уже – разведка: деловая, промышленная и др. 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 инфор-

мацию, 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 (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 уго-

ловном 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.

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 всякую новую щититу 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.

♦ ♦ ♦ ♦ ♦

12. Методы шпионажа на российском черном рынке информации*

В современных условиях самое грозное оружие — информация, в том числе и полученная путем прослушивания переговоров абонента сотовой связи

Случай из жизни

Некий отечественный предприниматель, занимающийся посредническими операциями, долго согласовывал с зарубежными партнерами вопрос поставки в Россию дорогого оборудования. Он прекрасно осознавал, что заказчик товара в случае задержки сроков поставки предъявит претензии именно ему — российскому посреднику. Зарубежные партнеры не подкачали, но когда товар уже был на складе, на бизнесмена вышли дельцы в милицейских погонах, которые нашли надуманный, но вписывающийся в рамки закона повод, чтобы наложить на технику арест. Оборотни предложили решить вопрос за деньги и назвали сумму, равную той, что заплатил бы бизнесмен за задержку поставки. Посредник этим мистическим фактом был немало удивлен, но деньги все же заплатил. Как выяснилось позже, осведомленность вымогателей объяснялась просто: бизнесмен стал жертвой «серой» прослушки, организованной его конкурентами. Исполнили заказ нечистые на руку сотрудники органов, которых оборотистые дельцы взяли в долю.

Эта история могла бы показаться скорее сюжетом хорошо закрученного милицейского телесериала, чем фактом реальной жизни, если бы в конце июня в Москве не разразился безобразный скандал. Нескольких высокопоставленных милицейских руководителей заподозрили в организации незаконного прослушивания телефонных переговоров не менее высокопоставленных граждан. То, о чем многие лишь догадывались, получило зримое подтверждение: распечатки телефонных переговоров политиков и бизнесменов, сфальсифицированные заявки на прослушку, крупные суммы денег в милицейских сейфах, происхождение которых никто не мог объяснить... Борис Немцов — человек, чьи телефонные переговоры не раз появлялись на черном информационном рынке, рассказал «Итогам», что ему известно как минимум о пяти случаях, когда его телефоны прослушивались. «Но сегодня у меня такое ощущение, что все друг друга слушают. Спецслужбы — политиков, коммерсанты — конкурентов, мужья — жен. Видимо, у нас нынче в моде такая манера поведения», — сетует политик.

Дело техники

У любого сотового телефона в ряду его достоинств есть и одна не очень приятная особенность: владелец трубки технически находится «под колпаком» своего мобильного оператора. Именно он обладает возможностями знать многое о личной жизни своего абонента: весь телефонный перечень его деловых, дружеских и личных контактов, их регулярность, интенсивность и при желании их содержание. Другое дело, что всю эту информацию мобильные операторы

* По материалам журнала «Итоги» № 27 (577), 07.07.2007. Александр Захаров, Григорий Санин, при участии Степана Кривошеева.

охраняют от посторонних: появись такого рода информация на черном рынке — и абоненты побегут в конкурирующую компанию.

Есть только один фактор, заставляющий мобильного оператора ограничивать тайну переговоров своих абонентов без уведомления последних. «Сотрудникам правоохранительных органов могут выдаваться протоколы соединений абонентов по судебным постановлениям, как того требует действующее законодательство», — говорит пресс-секретарь ОАО «Мобильные ТелеСистемы». По словам менеджера по информационно-аналитическому обеспечению ОАО «ВымпелКом», «такая информация предоставляется со ссылкой на судебное решение, налагающее ограничения на тайну связи, со сроком действия, не превышающим 6 месяцев со дня его подписания, с предъявлением оригинала судебного решения, а также в соответствии с требованиями УПК РФ».

Пожалуй, нет такого телекоммуникационщика, который не слышал бы грозной аббревиатуры — СОРМ. Расшифровывается она как система оперативно-разыскных мероприятий. Согласно российскому законодательству она установлена у каждого сотового оператора и интернет-провайдера. Заниматься негласным съемом информации посредством СОРМ имеют право службы, которые по закону являются субъектами оперативно-разыскной деятельности. С технической точки зрения каналов для контроля переговоров абонентов (на профессиональном сленге «точек») у операторов сотовой связи относительно немного.

Поэтому системой СОРМ, как правило, пользуются лишь при расследовании резонансных преступлений, связанных с терроризмом, заказными убийствами или многомиллионными аферами. Технология выглядит так: расследующий конкретное дело сотрудник органов готовит документ, в котором детально обосновывает необходимость использования специальных технических средств в отношении конкретного гражданина. Непосредственный начальник сыщика рассматривает это ходатайство и в случае своего согласия визирует бумагу. Далее она следует по инстанции — к курирующему заместителю начальника управления.

С двумя визами оперативник отправляется к судье, который должен отдельно санкционировать прослушку каждого из ставящихся на контроль телефонных номеров. С официальным постановлением суда на руках оперативник едет в управление оперативно-технических мероприятий (УОТМ). Там бумагу принимают и передают оригинал постановления в адрес мобильного оператора. Бумага в компании регистрируется и хранится не менее года. Оператор в свою очередь активирует аппаратуру СОРМ, производя аудиозапись по указанным в судебном постановлении номерам. Переговоры пишутся на жесткий носитель, который передается в установленном порядке в УОТМ. Там он расшифровывается и выдается заказывавшему прослушку оперативнику либо на диске, либо в бумажном виде. Все полученные материалы прилагаются к расследуемому делу (уголовному или оперативному) и скрупулезно вносятся в его опись. По истечении срока действия решения суда прослушиваемый абонент отключается от СОРМ.

Подобный механизм существует во многих странах. Правда, там система отлажена более жестко. К примеру, в Латвии после ее вхождения в ЕС прослушка ведется следующим образом. Оперативник оформляет запрос на прослушку конкретного телефона. Если он получает добро, его приглашают в специальный кабинет, открывают аудиодоступ к компьютерному файлу, содержащему перехваченные переговоры, и он их конспектирует — именно конспектирует, а не переписывает дословно. Только голую информацию — цифры, фамилии, адреса, названия фирм.

Во Франции конфиденциальность информации и вовсе возведена в ранг государственной политики. «Оперативные службы имеют право контролировать телефонные переговоры только по конкретному преступлению, — рассказали „Итогам“ в департаменте общественных связей полицейского комиссариата Парижа. — Если человека подозревают в убийстве, то путем прослушивания будут собирать доказательства только этой его вины. Если же он попутно разговорится о своем участии в краже, грабеже или изнасиловании — суд не вправе принять во внимание эту информацию в качестве доказательной».

В США до печальных событий 11 сентября санкции на прослушивание или перлюстрацию корреспонденции нужно было одновременно получать в министерстве юстиции и в ФБР на уровне директоров или их заместителей. Кроме того, разрешение должен был дать суд. Однако объявленная борьба с терроризмом существенно упростила эту систему. Сегодня, чтобы взять человека под контроль, достаточно судебного решения. То есть как у нас.

Черная связь

Существующая в России бюрократическо-правовая база прослушки вполне прозрачна, надежна и логична. Но и в ней есть ряд подводных камней. Дело в том, что такого рода судебные постановления, как говорят знающие люди, зачастую подписываются пачками. А значит, почти не глядя. Да и как может судья вникнуть в суть каждого из особо важных дел, которые исчисляются десятками? Тем более что многие из них находятся в стадии предварительного следствия — сбора оперативной информации и улик. Этим узким местом и пользуются оборотни в погонах: чего проще вписать в абсолютно легальную заявку, кроме действительно подозрительных абонентов, еще и те телефонные номера, которые заказали со стороны. Что обычно и делается. И вообще, как неофициально признаются оперативники, дыр в существующей системе масса. К примеру, многие граждане нередко пользуются мобильными телефонами, оформленными на чужое имя. «Если доказывать суду, что номером, оформленным на законопослушного гражданина Пупкина, пользуется подозрительный гражданин Пипкин, можно потратить годы. А значит, проще вписать в запрос фамилию Пупкина, повесив на него все грехи этого мира. Если покопаться в архивах детально, можно накопать тонны нарушений и злоупотреблений — вольных и невольных», — делится наш источник.

Материалы коммерческой прослушки передаются заказчику обычно на диске. Дело в том, что в бумажном варианте оператор УОТМ, как правило, конспективно передает лишь общую тематику и смысл переговоров, а не нюансы. А ведь важны прежде всего детали. Именно в них и содержится чаще всего ис-

комая коммерческая информация. К примеру, довелось свести знакомство с одним известным московским архитектором, который влип в такую вот неурядицу. Он готовил проект усадьбы на Новой Риге по заказу одного олигарха. Бюджет проекта составлял несколько миллионов долларов. Переговоры длились целый месяц, а в конкурсе участвовало пять крупных архитектурно-строительных компаний. В разгар проведения тендера к моему знакомому пришли сотрудники ОБЭП и нашли массу нарушений с отчетностью, закрыть глаза на которые они были готовы за 15 тысяч долларов. Потом нанесли визит из налоговой. Уладить этот вопрос удалось за 5 тысяч долларов, не считая потраченных времени и нервов. Закончилась полоса неудач тем, что одно из архитектурных бюро предложило заказчику очень похожий проект, но несколько дешевле. Уже когда клиент выбрал конкурирующую компанию, выяснилось, что телефон моего приятеля активно прослушивался. Заказ поступил от конкурентов, и обошелся он им где-то в 50 тысяч долларов, что с лихвой было компенсировано стоимостью полученного не очень честным путем подряда.

По неписаным расценкам нелегальная недельная круглосуточная прослушка разговора одного абонента стоит от 15 до 20 тысяч евро, при том что себестоимость операции сама по себе невысокая. Цена услуги обусловлена конспирацией, а значит, длинной цепочкой посредников. Ведь это своеобразная гарантия анонимности заказчика и исполнителя в случае провала. Что же касается стационарной связи, то здесь широко используются оперативные возможности технических служб ЧОПов. Специалисты могут подключиться прямо к проводам в щитке на лестничной площадке или в коммуникационном колодце. Получение информации по каналам СОРМ в данном случае, говорят, стоит гораздо дешевле — от 3 тысяч долларов в неделю.

Для прослушивания сотовых телефонов есть и еще один технический способ — при помощи аппаратно-программных комплексов. Однако стоит он астрономических денег. В данном случае аппаратура монтируется в машине, а следовательно, должна постоянно находиться неподалеку от объекта прослушки. Комплекс замещает собой базовую станцию — так называемую соту, перехватывая сигнал. Стоит такой комплекс более 150 тысяч евро. Кроме того, для прослушивания абонента цифрового стандарта GSM «с эфира» необходима и дорогая аппаратура для дешифровки разговора, записанного сложными алгоритмами, которые постоянно меняются. И потому можно смело сказать, что подобных услуг по прослушке на сегодняшний день на черном рынке не существует.

Личные дела

Как работает черный рынок прослушки? Коммерческие заказы к оборотням приходят в основном через ЧОПы или службы безопасности частных компаний, где работают бывшие сотрудники органов. Лишь им, как правило, доверяют их прежние коллеги. Человеку со стороны, не имеющему рекомендаций, стопроцентно откажут. Да еще и могут сдать, заподозрив что это проверка на вшивость со стороны управления собственной безопасности.

На первом месте по спросу стоит прослушка конкурентов по бизнесу. Такого рода заказы в большинстве своем появляются накануне крупных аукцио-

нов, рейдерских захватов, слияний и поглощений или же перед собраниями акционеров. В таких случаях заказчик требует едва ли не ежечасный отчет о мобильных контактах абонента, и цена за услугу может возрастать до 30—40 тысяч евро в неделю. На втором месте стоят заказы, связанные с матримониальными делами: супружеские измены, бракоразводные процессы, слежка за членами семьи. И на последнем месте стоит компрометирующая прослушка политиков, общественных деятелей и олигархов. На подобные заказы оборотни идут крайне неохотно — такого рода сведения добываются чаще всего с целью обнародования, что влечет за собой скандал, неминуемое расследование с почти стопроцентным разоблачением. Говорят, что арестованные на прошлой неделе муровцы тоже погорели на «запретке», слушая телефон ну очень крупного бизнесмена, имеющего мощную службу безопасности...

Один из частных детективов рассказал «Итогам», что клиент, единожды заказавший услугу аудиоконтроля, как правило, обратится за помощью еще раз: «Как-то ко мне пришел предприниматель, которому надо было узнать, контактирует ли с арбитражными судьями адвокат его противников по спорному вопросу, связанному с бизнесом. Такая информация была получена, и бизнесмен выиграл арбитраж. А совсем недавно он попросил поставить „уши“ на телефон жены, поскольку частые командировки сделали бизнесмена очень подозрительным».

Докажите это

Как признаются сами «участники рынка», бизнес этот хоть и высокодоходный, но крайне рискованный. Что и подтвердили последние задержания...

Уберечься от прослушки можно, пожалуй, одним-единственным способом — не пользоваться телефоном. «Я знал, что мой телефон слушают, — рассказал „Итогам“ предприниматель Константин Боровой. — Но я прекрасно понимал, что обезопасить себя от этого нельзя. Хотя существуют технические возможности, разработанные для нашей разведки и связанные с различными способами шифрования информации. Однако без регистрации в ФСБ такое оборудование не установишь. Потому что любая информация для спецслужб должна быть прозрачна».

Что делать обычному законопослушному человеку, заподозрившему факт негласной прослушки? Логика подсказывает: обратиться в прокуратуру. Однако там от вас потребуют подтверждений этого факта. Установить факт прослушки через СОРМ невозможно. Все рассказы о том, что в трубке появляются посторонние шумы, щелчки, эхо или что у телефона быстро садится батарея, — не более чем домыслы дилетантов. Психологи дают такой рецепт — нужно попытаться вступить с прослушкой в оперативную игру. Запустить ложную информацию и проследить за реакцией потенциальных заказчиков. Возникнет ответная реакция, значит, что-то не так. Впрочем, дело это весьма утомительное. Проще просто наговорить по телефону с три короба. «Умный человек эту ситуацию может использовать и в своих целях, намеренно дезинформируя слушателя, — говорит старший научный сотрудник Государственного научного центра социальной и судебной психиатрии имени В. П. Сербского. — Наговорить

по телефону можно что угодно. И подслушивающему человеку понять, где правда, а где ложь, будет очень сложно».

Председатель Комиссии Общественной палаты по общественному контролю за деятельностью правоохранительных органов, силовых структур и реформированием судебно-правовой системы советует: «Если человеку стало известно, что его слушают, прежде всего надо понять, кто именно это делает. Если есть мотивированные доказательства, должно последовать обращение в суд. Если речь идет о конкретных должностных лицах — допустим, сотрудниках правоохранительных органов, — можно обращаться в прокуратуру».

«Если вы точно знаете, что вас слушают, фиксируйте свои звонки, — рекомендует адвокат. — Отмечайте их время и продолжительность. После этого подавайте заявление мобильному оператору, где укажите, что такие-то ваши звонки были незаконно прослушаны. Можно сослаться на Закон „Об оперативно-розыскной деятельности“, в котором четко сказано, что любое лицо, в отношении которого проводятся оперативно-разыскные мероприятия, имеет право знать, кто, когда и какую санкцию выносил в отношении него. Оператор сотовой связи обязан знать, санкционировано или нет то или иное оперативное мероприятие, в частности прослушка. Если вам отвечают, что им ничего о такой санкции неизвестно, можете обратиться с точно таким же требованием в органы ФСБ или МВД. Заодно можно обратиться в прокуратуру с просьбой проконтролировать соблюдение законности при осуществлении оперативных мероприятий в отношении вас и вашего телефона. Если вам приходят ответы, указывающие на то, что вас никто не слушает, вы имеете право каждый из этих ответов обжаловать либо в вышестоящем органе, либо в суде.

Если эксперты, выделенные судом, подтвердят, что вмешательство в личную жизнь имело место, то вы вправе требовать компенсацию в гражданско-правовом порядке со стороны нарушителя закона». Суд обязательно прислушается к вашим доводам, поскольку, по словам пресс-секретаря Мосгорсуда Анны Усачевой, подобные действия, совершенные должностными лицами, подпадают под часть 2 статьи 138 УК (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений).

Многие пострадавшие от телефонного пиратства полагают, что ситуацию в судебном порядке скорректировать невозможно и нужно вносить поправки в действующее законодательство. «Произошедшее — характерный пример того, как люди в погонах, призванные защищать граждан, беззастенчиво торгуют властью, — говорит председатель комиссии Госдумы по противодействию коррупции Михаил Гришанков. — Дело в этом конкретном случае не в несовершенстве закона — он-то как раз четко прописывает основания и порядок осуществления оперативно-технических мероприятий, в том числе прослушивания телефонов. Дело в отсутствии должной системы контроля за подчиненными в органах, имеющих полномочия осуществлять такую работу».

Примечание.

Согласно статье 64 Федерального закона РФ «О связи», операторы связи обязаны предоставлять уполномоченным государственным органам информацию о пользователях услугами связи и об оказанных им услугах связи, а так-

же иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами. При проведении уполномоченными государственными органами следственных действий операторы связи обязаны оказывать этим органам содействие в соответствии с требованиями Уголовно-процессуального законодательства.

Согласно статье 13 Закона РФ «Об оперативно-розыскной деятельности», право осуществлять оперативно-разыскную деятельность предоставлено оперативным подразделениям: органам внутренних дел, Федеральной службе безопасности, федеральным органам государственной охраны, сотрудникам таможни, сотрудникам внешней разведки, Федеральной службе исполнения наказаний, Федеральной службе по контролю за оборотом наркотиков. Органам, осуществляющим оперативно-разыскную деятельность, информация из протоколов соединений абонентов предоставляется на основании письменных запросов со ссылкой на судебное решение, налагающее ограничения на тайну связи, со сроком действия, не превышающим 6 месяцев со дня его подписания, с предъявлением оригинала судебного решения, а также в соответствии с требованиями УПК РФ.

Органам, осуществляющим производство предварительного следствия, информация из протоколов соединений абонентов, в соответствии с требованиями Уголовно-процессуального законодательства РФ, предоставляется на основании санкционированного прокурором постановления о производстве выемки по возбужденному уголовному делу (ст. ст. 13, 183 ч. 3 УПК РФ). При производстве выемки уполномоченным лицом соответствующего органа предварительного следствия в порядке ст. 182, 183 УПК РФ составляется протокол выемки, копия которого вместе с копией постановления о производстве выемки передается на хранение оператору.

♦ ♦ ♦ ♦ ♦

13. Офисные шпионские войны*

Шпионские скандалы время от времени возникают в мире большого бизнеса. Насколько безопасно могут себя чувствовать акулы капитала в условиях постоянной слежки?

Шпионаж перестал быть чем-то сверхъестественным и превратился в обыденную вещь, от которой не застрахованы даже самые богатые люди и компании. Несколько недель назад в мире бизнеса разразился шпионский скандал, стоивший кресла Патриции Данн, председателю совета директоров корпорации Hewlett-Packard, одной из крупнейших ИТ-компаний мира.

Коротко суть скандала. Время от времени в деловую прессу попадала информация о вопросах, обсуждаемых в тесном кругу высшим руководством компании Hewlett-Packard. Председатель совета директоров Патриция Данн решила прояснить причины и способы утечки конфиденциальной информации

* Ольга Ватраль, From-ua.com

и поручила расследование специалистам из внешней фирмы безопасности, которые, в свою очередь, наняли специалистов по «претекстингу». Pretexting — это метод детективного расследования, заключающийся в получении обманным путем распечатки записей обо всех звонках по определенному телефонному номеру за указанный период. Так как эта услуга платная, телефонные компании предоставляют ее охотно и с минимумом формальностей при установлении подлинности абонента.

В результате этой процедуры был определен пострадавший — 66-летний Джордж Киуорт, директор HP. Однако поступок госпожи Данн был осужден советом директоров, в результате чего Патриции было предложено покинуть свой пост за неэтичное поведение.

Практически каждая мало-мальски крупная компания проверяет лояльность своих сотрудников, используя куда как более грязные методы — и тотальный контроль за электронной почтой, и прослушивание телефонных разговоров. А еще очень часто вводятся запреты, кажущиеся иногда странными и непонятными.

Например, фирма Samsung из опасений промышленного шпионажа запретила пользоваться мобильными телефонами, оснащенными цифровыми камерами, на своих заводах и в исследовательских центрах. Причем этот запрет распространяется как на гостей, так и на сотрудников компании. Руководство Samsung объясняет свое беспокойство тем, что с помощью мобильного телефона можно делать фотографии незаметно, а это делает весьма реальной угрозу использования отснятого материала в шпионских целях.

Аналогичные меры принимаются и в LG Electronics — для всех десяти научно-исследовательских институтов компании в Корее. В тех институтах LG, где создаются передовые технологии, руководство планирует ввести полный запрет на телефоны с камерами. К таким же методам борьбы с корпоративным шпионажем намереваются прибегнуть и корейские автопроизводители Hyundai и Kia Motors.

Более того, в настоящее время Министерство информации и связи Южной Кореи разрабатывает специальные правила по регулированию использования мобильных телефонов с фотокамерами в стране. Власти рассматривают проект отдельного закона, согласно которому производители телефонов должны были бы в обязательном порядке оснащать такие устройства специальным «генератором шума», который бы издавал звук во время съемки.

Пытаясь защититься от корпоративного шпионажа, фирмы используют также и новейшие технологии. Целью одной, наиболее популярной в последнее время, является маскировка звука: в стены и потолок помещения, в котором ведутся секретные переговоры, монтируются специальные устройства, которые создают небольшой шум. Этот шум не мешает людям в их работе, но в то же время он растворяет голоса людей и препятствует таким образом работе подслушивающих устройств.

А системами выявления телефонных «жучков» или систем бесследной электронной почты сегодня уже мало кого удивишь.

Однако не стоят на месте и технологии тех, кто подслушивает. Технологические новинки и методы шпионажа постоянно совершенствуются. Например, новое устройство Laser-3000 с помощью лазерного луча умеет улавливать вибрации оконных стекол, вызванные голосами тех, кто находится в комнате, и расшифровывать сказанное.

Еще одно известное устройство, созданное для шпионажа, способно реагировать на излучение, исходящее от компьютерного монитора (и таким образом «захватывать» текущую картинку, будь то документ Word, электронная таблица или графический файл).

Но не только технические устройства используют специалисты по корпоративному шпионажу. В их арсенале находится масса других методов, использующих психологические уловки и невнимательность сотрудников.

Так, например, в мае прошлого года группа инженеров HP, работающих над сетевым лазерным принтером нового поколения, подверглись осаде со стороны конкурентов. Служащие компании получали телефонные звонки дома и на работе от мнимых членов команды HP, в которых те спрашивали о подробностях нового принтера. А в 2001 году компания Procter&Gamble призналась в том, что ее сотрудники просматривали мусор англо-голландского концерна Unilever в поисках коммерчески ценной информации.

Секретную информацию могут попробовать получить злоумышленники под видом журналистов. Однажды в офисе раздается телефонный звонок, и некто, представившийся журналистом, начинает задавать вопросы о доле компании на рынке, объеме продаж и планах на будущее. Через некоторое время выясняется, что журналиста с такой фамилией в редакции нет, либо журналист есть, но он никуда не звонил. Скорее всего, этот обманный маневр предприняли конкуренты.

Не менее популярным стал в последнее время и рекрутинговый шпионаж. Фирма объявляет конкурс на замещение высокооплачиваемой должности, и у пришедших на собеседование специалистов пытаются узнать их корпоративные секреты и планы.

Если защититься от подслушивающих устройств еще как-то можно, то человеческий фактор — это самое слабое звено в цепи промышленного и корпоративного шпионажа. В этом случае на помощь подозрительному начальству может прийти только частный детектив, услуги которого также недешевы, но и его могут перекупить конкуренты.

Конечно, можно сказать, что лучшим решением станет бизнес без секретов, но это практически нереально в наше время. Поэтому и процветает индустрия подслушивающих и подглядывающих устройств, а боссы и инженеры придумывают, как бы еще защитить свои секреты от посторонних.

♦ ♦ ♦ ♦ ♦

14. Секреты фирмы стоят дорого*

Конфиденциальная информация о деятельности компаний стала ходовым товаром. В промышленном шпионаже участвуют как отдельные сотрудники, так и целые государства, использующие для этого весь свой разведывательный ресурс. Потери развитых стран от кражи экономических секретов исчисляются миллиардами долларов.

С окончанием «холодной войны» промышленный шпионаж потеснил военную разведку. В то же время сложно определить, где кончается военный шпионаж и начинается промышленный. Последние разработки в области вооружения и боевой техники только на первый взгляд можно отнести к военным секретам. Новые самолеты или оружие демонстрируют и оборонную мощь государства, и его промышленный потенциал, а высокие технологии можно использовать как в мирных целях, так и в военных.

Когда в 70-е годы прошлого столетия советский самолет МиГ-25 был угнан в Японию, им сразу же занялись американские специалисты. МиГ-25 попал под прицел Пентагона и американских спецслужб с конца 1960?х, когда были построены первые опытные самолеты. Спецслужбы много знали о советском высотном сверхзвуковом самолете, но для тщательного исследования информации из открытых источников было недостаточно, требовался образец, и перебежчик Виктор Беленко им его предоставил. Американцы впоследствии при проектировании собственных истребителей использовали очень многие наработки советских конструкторов, а СССР предательство летчика обошлось в миллиарды рублей. С тех пор мало что изменилось, разве что страны стали тратить еще больше денег, чтобы компенсировать потери от экономического шпионажа.

Воруют все

Развитые страны всегда крали друг у друга экономические секреты. Причем сегодня шпионаж поставлен на государственную основу. Наиболее часто объектом любопытства становились американские компании. Подсчитано, что государственные органы примерно 60 стран активно занимаются сбором секретной информации, принадлежащей на правах собственности американским корпорациям. Особенно преуспели в этом разведки Франции, Германии, Японии, в последнее время не отстают от них Россия, Китай и Южная Корея. В бюджетах многих стран предусмотрены расходы на эти цели. Разведданные собираются не только путем прямой кражи секретов из сейфов и лабораторий и подкупа компетентных сотрудников, но и при изучении открытых источников: контрактов между компаниями, сведений о банковских операциях, информации о событиях, которые могут повлиять на формирование цен на рынках. Для получения промышленных секретов в ход идут слияния и поглощения компаний, совместные предприятия, международные программы обмена и общественные организации. Особый разговор о сборе информации с применением высоких технологий: о взломах баз данных, просмотре электронных сообщений – хакерство стало востребованной профессией. При этом не отказываются промыш-

* Светлана Грибанова, «Эксперт Казахстан» №28 (84), 2006 г.

ленные шпионы и от проверенного способа выуживания сведений – ознакомления с содержимым корзин для мусора.

Расцвет промышленного шпионажа пришелся на конец XX века и связан в первую очередь с тем, что мощь государства все больше определяется ее экономическими возможностями. Впереди те страны и те компании, которые первыми придумают что-то новое и смогут продать готовый товар или технологию. Но инновации стоят все дороже. Государства и крупные корпорации вынуждены вкладывать все больше средств в исследования. Однако трудно предугадать, насколько будет велика отдача от новой разработки, к тому же новое становится старым в тот момент, когда сходит с конвейера. Гораздо дешевле выкрасть результаты работы ученых и инженеров конкурирующей компании и запустить их разработку в производство.

Говорят, что своим экономическим прорывом Китай обязан промышленному шпионажу. На любых международных выставках, особенно на тех, где представлены потребительские товары, всегда можно увидеть целый десант специалистов из Поднебесной: они не просто знакомятся с новыми разработками и отслеживают тенденции, а буквально перерисовывают выставленные образцы. Порой новые модели обуви или одежды первыми появляются в Китае, а не там, где были придуманы. Это дает китайцам преимущество во времени, если приплюсовать сюда более низкую стоимость товаров за счет дешевого производства, то понятно, почему западным странам трудно выиграть конкуренцию у Китая хотя бы на территории СНГ.

Высоколобые хищники

Компании становятся объектом промышленного шпионажа не только со стороны конкурентов из других стран, но и со стороны соотечественников. Особенно развит в США так называемый корпоративный шпионаж, когда секреты друг у друга крадут фирмы, работающие в одной области. В частности, это характерно для высокотехнологичных компаний. Это вполне объяснимо, если вспомнить, что быстрее всего устаревают компьютерная техника и программное обеспечение, а также телекоммуникационное оборудование. Исследования, проведенные среди компаний Силиконовой долины, показали, что американские производители страдают как от родственных американских компаний, так и зарубежных. В 1999 году высокотехнологичные фирмы, входящие в клуб наиболее прибыльных компаний Fortune 1000, понесли убытки от кражи конфиденциальной информации в размере 45 млрд долларов. Представители почти половины из обследованных предприятий подтвердили, что они стали жертвой промышленного шпионажа. При этом высокотехнологичные компании несут куда большие потери, нежели обычные. Соотношение ущерба, нанесенного в результате единичного случая кражи конфиденциальной информации рядовой фирме и высокотехнологичной из списка Fortune-1000: 15 к 500 млн долларов.

Компании для защиты своих секретов и сбора информации о конкурентах создают специальные отделы по бизнес-разведке. Этим не гнушаются ни маленькие фирмы из развивающихся стран, ни мировые производители. В 2000 году разразился скандал, в который были замешаны известные высокотехноло-

гичные компании. Исполнительный директор Oracle вынужден был дать объяснения по поводу действий нанятых его фирмой частных детективов, которых уличили в проведении выборочной вербовки среди сотрудников Microsoft и изучении содержимого мусоросборников главного офиса компании, в результате чего конкуренты смогли получить черновики важных документов.

Ранее суд Калифорнии обвинил компанию Broadcom в попытке выведать деловые секреты основного конкурента Intel. Выяснилось, что сотрудники кадрового отдела Broadcom в ходе интервьюирования служащих Intel якобы в целях изучения кандидатур на высокооплачиваемую работу в своей компании задавали в том числе и вопросы, касающиеся конфиденциальной информации. В частности, они выявляли организационную структуру Intel, источники финансирования, инвестиционные планы и данные по заработной плате. Суд расценил эти невинные на первый взгляд вопросы как типичный случай промышленного шпионажа.

Вся королевская рать

Прослушка конкурентов, о которой мир узнал еще во время Уотергейта, до сих пор используется спецслужбами США, правда, объектом ее все чаще становятся деловые секреты. Классическим примером экономического шпионажа считается прослушка ЦРУ торговых переговоров между Японией и США о возможных тарифах на японские автомобили представительского класса. Все отчеты, подготовленные на основании полученной информации, ЦРУ затем передало американскому торговому представителю. Как объяснили представители Центрального разведуправления, они работали не по заказу частной автокомпании, а сведения, полученные таким своеобразным способом, по их словам, представляют национальный интерес.

Агентство национальной безопасности США (АНБ) не только борется с хакерами, но и использует свои ресурсы для защиты экономических интересов государства. В 1990 году с помощью системы «Эшелон» АНБ перехватило переговоры между Индонезией и японской компанией NEC по поводу телекоммуникационной сделки стоимостью 200 млн долларов. В результате NEC пришлось поделиться контрактом с американской фирмой. Печально закончились переговоры с Бразилией для французской телекоммуникационной компании только потому, что интерес к ним проявило АНБ. «Эшелон» опять помог: почти полуторамиллиардный контракт ушел к американской корпорации.

Напиток за 75 тыс. долларов

Нельзя сказать, что абсолютно все компании готовы платить любые деньги за секреты конкурирующей фирмы. Более того, придерживаясь правил честной игры, они сотрудничают с конкурентом при выявлении лиц, виновных в краже секретной информации. В мае этого года компания PepsiCo передала в офис Coca-Cola копию письма, которое пришло по почте в фирменном конверте Coca-Cola. В нем некий Дирк, назвавшийся высокопоставленным сотрудником компании, предлагал очень подробную конфиденциальную информацию. Позже его личность была установлена: это житель Нью-Йорка Ибрагим Димсон. Речь шла о рецепте нового напитка, разработанного Coca-Cola. По версии следствия, Хойя Вильямс, которая занимала должность помощника администрато-

ра, вынесла из здания образец нового напитка и техническую документацию его производства. Эта версия основана на видеозаписи подозрительного поведения Вильямс: женщина просматривала рабочие папки и нужные документы складывала в сумку. Камера также зафиксировала момент, когда она держала в руках контейнер с жидкостью, в котором, как потом выяснилось, находился образец нового напитка. Coca-Cola обратилась в ФБР сразу после того, как получила предупреждение от конкурента, и Димсон уже общался с агентами под прикрытием. Он представил им 14 страниц секретных документов, принадлежащих Coca-Cola, и запросил за них 10 тыс. долларов, за образец нового напитка – 75 тыс. долларов. Агенты, войдя в роль, пообещали Димсону 1,5 млн долларов за дополнительную секретную коммерческую информацию компании.

Все трое преступников – в группу входил еще один человек – были арестованы в начале июля.

Официальный представитель PepsiCo заявил, что в данном случае компания приняла единственно возможное решение. «Конкуренция должна быть честной и законной», – сказал он.

♦ ♦ ♦ ♦ ♦

15. Тотальный шпионаж или телеслежка*

И все руки в гексогене

Советский человек считал, что за ним постоянно следят. Кого-то это заставляло всю жизнь бояться и быть предельно осторожным, кого-то возмущало (но это возмущение редко выплескивалось за пределы собственной кухни). Теперь действительно за всеми следят, и это считается признаком цивилизованного общества. Средний москвич или петербуржец, часто даже не подозревая, пять раз в день попадает в объективы видеокамер. Причем далеко не всегда это камеры наблюдения в торговых залах.

– Современные системы прослушки и видеонаблюдения, которые создают в целях безопасности и во имя человеческой свободы, нередко делают современного гражданина беззащитным перед вторжением в его частную жизнь, – говорит генеральный директор юридической компании «Правовая защита». – Из бутылки выпущен джинн, который уже не контролируется своим создателем. И если в западных странах закон реально защищает личную жизнь граждан, то в России большинство статей на эту тему носят декларативный характер.

В доброй половине петербургских клубов установлены камеры слежения в туалетах. Формально служба безопасности следит, чтобы народ не употреблял наркотики. Только почему-то потом записи тиражируют на пиратских дисках и продают из-под полы любителям. Знатоки говорят, что каждый год на питер-

* По материалам «Совершенно секретно» № 5 за 2006 г., Денис Терентьев

ском рынке появляются по нескольку десятков трехчасовых дисков с записями сексуальных сцен, снятых скрытыми камерами в офисах.

27-летняя петербуржанка Мария Н. по наивности заказала напечатать свои фотографии в стиле «ню» в одном фотоателье. Спустя месяц знакомые обнаружили Машины изображения на сайте «Питерские шлюшки». Барышня уверена, что это работа сотрудников ателье. Но так же точно она уверена, что в случае обращения в суд у нее нет ни единого шанса на успех. Фотографии, несмотря на ее протесты, даже не снимают с сайта. Хотя в цивилизованной стране все по-другому. В Чикаго студенты за продажу их фотографий, снятых нелегально в душе, отсудили у продавца 483 миллиона долларов.

– В России любая сфера человеческой деятельности может быть вынесена на всеобщее обозрение, – говорит координатор проектов Информационного бюро Совета Министров Северных Стран в Петербурге. – У нас же открыто продаются диски с базами данных Регистрационной палаты, налоговой инспекции, сотовых операторов и даже спецслужб. В любой европейской стране это вызвало бы немедленную и жесткую реакцию властей, потому что нарушаются права граждан. У нас структуры, из которых произошла утечка, пытаются предотвратить подобное в будущем – и все. Насколько я знаю, ни одна организация, прошляпившая конфиденциальную информацию о своих клиентах, не принесла извинения людям, которые из-за этого пострадали. У нас нет уважения к тайне личности, понятие privacy пока плохо переводится на русский язык.

Отныне публичным может стать все. Еще до первых шумных разбирательств по поводу авторских прав на тексты начались скандалы с неотъемлемыми правами человека на собственное изображение. Что это такое? За примерами ходить недалеко. Например, каждый день мы видим, как в криминальной хронике подозреваемых в совершении преступлений показывают в фас и в профиль, звучат их имена и фамилии. Вскоре после взрывов московских многоэтажек в 1999 году спецслужбы предъявили виновных: вот они, чеченцы-террористы, – все руки в гексогене. Потом выяснилось, что эти люди ни при чем, но никто из их недавних обвинителей перед ними публично не извинился.

Именно из передач центрального телевидения вся страна узнала, как лежал в постели человек, похожий на Генерального прокурора Скуратова.

– На скандал с Генеральным прокурором наше общество отреагировало нецивилизованно, – считает Вадим Ф. – Такого рода информация о должностном лице, занимающем столь высокий пост, может – и должна – стать предметом широкого общественного обсуждения. А стала предметом политиканского торга и шантажа. Но, собственно, с этой целью ее и сделали достоянием гласности, сыграв на низменном обывательском любопытстве. А общественный интерес и обывательское любопытство – принципиально разные вещи.

Совсем, кажется, другой пример. Ульяна Ивановна и Яков Антонович Ц-ы живут в 500 километрах от Омска. Дороги в село нет, старики даже хлеб сами пекут. Однажды приезжал к ним фотограф из столицы, говорил, что снимает заброшенные деревни для выставки. А чуть позже их семейная фотография появилась на огромных рекламных бильбордах по всему Омску: старики рекламировали пенсионный вклад в частном банке, о существовании которого в

жизни не слыхали. Соседи издевались – просили у «банкиров и звезд рекламного бизнеса» денег на водку. Хорошо, дочки пенсионеров помогли составить иск, суд обязал банк извиниться и заплатить компенсацию – 500 долларов.

Без права быть собой

– Зачастую, поступая на работу, человек отказывается от своих прав, – говорит петербургский адвокат Николай А. – Нового работника могут заставить пройти проверку на детекторе лжи. Или в сопровождении сотрудника фирмы поехать сдавать анализы на СПИД, гепатит и другие болезни. Как ни странно, такую ситуацию считают нормальной и сами сотрудники, и их работодатели: мол, если хозяин платит приличные деньги, то вправе навязывать любые правила игры.

Сотрудницу одной из московских фирм хозяин обязал позировать для приезжих фотографов, которые впоследствии продали фотосессию для зарубежного журнала. Но едва фотомодель заикнулась хозяину о своем проценте от сделки, он ее уволил. Суд признал увольнение законным.

На кассиров в одном петербургском ресторане не только смотрят: его и «слушают». На каждого направлена камера, в каждом кассовом аппарате – микрофон. Кроме видео и звука, на компьютер хозяина передается чек. Служба безопасности сравнивает, что сказал клиент, сколько денег заплатил, сколько было пробито по чеку.

– Плохо то, что аппаратурой тайной слежки пользуются не только для финансового контроля, – считает Николай А. – Она дает хозяину ощущение особой власти над подчиненными, а их самих подавляет. Это не соответствует принципам демократического общества.

Сегодня в школах повсеместно устанавливают видеокамеры слежения, наподобие тех, что работают в банках, тюрьмах и прочих режимных объектах. Казалось бы, это хорошо. Но только системы видеослежения порой устанавливаются почти исключительно внутри здания – на лестницах, в классах, даже в учительской и в курилке. Какой смысл в такой тотальной слежке за самими учащимися?

Недавно в Калининском районе Петербурга задержали группу юных панков, которые по вечерам разгуливали по улицам, разыскивали видеокамеры и «расправлялись» с ними при помощи булыжников. Скорее всего, их осудят условно за порчу чужого имущества – ни одного «глазка» молодежь не похитила. «Нам чужого не надо, но и подсматривать за собой мы не дадим», – говорили на следствии юные радикалы.

– Сегодня безопасность стала крючком, на который ловят обывателя, заставляя отказываться от свобод, – говорит петербургский юрист и правозащитник Андрей В. – Людям внушают, будто слежка за каждым их шагом может принести им безопасность...

Купи себе ошейник

Все это, конечно, не чисто российская, а общемировая тенденция. Обычный американец попадает в объектив видеокамер – в магазинах, банках, на заправках, в своем офисе – примерно по десять раз на дню. В одном небольшом городе в окрестностях Лондона добились снижения уровня преступности в пять

раз, установив на улицах примерно две сотни камер, сверяющих полученные изображения граждан с базой данных подозреваемых и известных преступников (при совпадениях автоматически извещается полиция). А Лондон стал первым мегаполисом мира, в котором вся городская среда просматривается камерами наружного наблюдения. Среднего лондонца не менее трехсот раз в день запечатлевают видеокамеры. По подсчетам юристов английской столицы, это противозаконно в 70 процентах случаев, но ни одного объектива, кажется, так и не убрали. И от терактов прошлым летом они не уберегли.

В английском обществе уже появились опасения, что терророфобия окончательно поставит крест на принципах неприкосновенности частной жизни. Но если джентльмены, ездящие в такси не всегда со своими женами, недовольны тем, что знаменитые «кэбы» начинают оборудовать скрытыми камерами, то другим джентльменам доставляют удовольствие пабы, где посетители общаются друг с другом через видеоглазки, подсоединенные к Интернету.

В Штатах, когда в 1977 году журналисты установили факт видеосъемки улиц в центре, Нью-Йорка агентами ФБР, это вызвало волну национального возмущения. После 11 сентября такого рода наступление на гражданские права американцев уже не возмущает. «Патриотический акт» устранил перегородки, традиционно отделявшие разведку от охраны общественного порядка. ФБР добилось права без специального ордера получать финансовую информацию о гражданах от банков, страховых компаний, бюро путешествий, риэлторских фирм, брокеров, почтового ведомства, ювелирных магазинов, казино, автодилеров и т. д.

Правда, в отличие от России, там не выявлено ни одного случая массовой торговли такого рода данными.

Верховный суд США оставил в силе право Министерства юстиции в исключительных случаях секретно арестовывать жителей страны, не являющихся ее гражданами, а также держать под арестом американских граждан в течение неопределенного срока, не предъявляя обвинения и не предоставляя адвокату доступа к ним. Предполагается запустить в работу обширную компьютерную систему проверки авиапассажиров – где крестился, на ком женился. Еще немного, и будет создана не просто авиационная, а всеобъемлющая общенациональная программа проверки под многообещающим названием Total Information Awareness («Тотальная информационная бдительность»).

Работа в этом направлении ведется с неослабевающим энтузиазмом. В Университете Флориды разработана система видеонаблюдения, способная распознавать движения людей в офисах: например, сотрудник открыл определенную дверь, воспользовался компьютером или телефоном, взял или положил какой-то предмет. Результаты работы системы выдаются в виде текстовых описаний действий, а также набора «ключевых кадров», фиксирующих моменты начала или конца действия (например, телефонного разговора).

В России стараются не отставать. К началу 2006 года в Москве появилось несколько десятков станций приема и обработки информации системы видеонаблюдения «Сота», каждая из которых считывает информацию с 1200 «точек». С 2001 года в Тверском районе Москвы за всеми 1012 подъездами всех 464 му-

ниципальных домов района постоянно следит смена, состоящая из 21 оператора. Четыре года назад система обошлась в 25 миллионов рублей. Эксперимент показал: видеокамеры антивандального образца способны заменить 48 консьержек всего одним оператором у мониторов.

Среди 88 операторов всех четырех смен, сообщили мне, сплошь женщины. Работа здесь и вправду не мужская: приходится следить за тремя мониторами одновременно, на каждом из них – по 16 маленьких картинок, а смена длится 12 часов. Пока картинка на экране в желтой рамочке, на нее можно не смотреть – ничего там не происходит. Как только камера засекла движение, рамочка начинает светиться красным. Оператор не должен упустить, если начинается драка, разгружают или погружают вещи, у подъезда появилась бесхозная сумка или у домофона крутятся подозрительные личности. В таких случаях вызывают наряд из отдела вневедомственной охраны, который на месте разбирается, что же именно творится. В среднем за смену бывает пять-шесть вызовов. Информация с камер записывается посредством цифрового сжатия на жесткий диск, чтобы в случае чего ее могли «снять» органы внутренних дел или другие городские службы.

Камеры слежения позволяют предотвращать или раскрывать преступления. Мужчину в собственной квартире убили и ограбили, а украденное вывезли на его же машине. В архиве нашлась видеозапись, на которой видно, что к машине подошли мужчина и женщина с сумками в руках, сели в нее и уехали. Женщина в итоге оказалась прислугой убитого, которая и навела на работодателя уголовников. А был случай, когда оператор увидела, как человек схватился за сердце и сполз по стенке. И тут же вызвала «скорую».

– И вместе с тем «камеры видеонаблюдения – это палка о двух концах, – считает один из сотрудников петербургской прокуратуры. – С одной стороны, это помогает раскрывать преступления, особенно когда люди не подозревают, что их снимают. Надо видеть глаза подростков, которым прокручивают пленку, зафиксировавшую, как они ночью взламывают ларек. Но у нас был случай, когда при организации заказного убийства киллеры покупали видеозапись подъезда дома, где жила их жертва. В другом случае сами милиционеры, судя по всему, использовали видеосъемку подъездов в качестве наводки для квартирных воров.

Люди постепенно привыкают к тому, что их снимают. Например, участники телепроекта «За стеклом» говорят, что новизна ощущений, связанных с круглосуточным присутствием камер, закончилась дня через три.

В пригородной московской электричке веселятся пассажиры. В стенке вагона – малюсенький «глазок». По словам замминистра внутренних дел РФ Александра Чекалина, «системы внутрисалонного видеонаблюдения» планируется установить на всех пригородных электричках Московской железной дороги. В салоне каждого вагона установлено устройство, передающее на монитор машиниста цветное видеоизображение. Машинист может регулировать поступление информации: например, задать удобное ему время смены изображения из разных вагонов или установить непрерывную трансляцию из любого салона.

Система ведет не только запись происходящего, но и архивирует файлы, которые, в случае необходимости, могут быть предоставлены спецслужбам.

В Петербурге особое внимание – памятникам культуры. Когда на Дворцовой площади открывали ограду Александринского столпа, камеры видеонаблюдения уже имелись. Сегодня их стараются тщательнее скрывать, чтобы не смущать граждан. Последнее достижение – неприметный черный колпачок, под ним панорамная камера, дающая полный круговой обзор. Правда, и самая совершенная камера не отличит мешок с гексогеном от мешка с сахарным песком.

– Телеслежка это шажок в создании глобального ока Большого брата, о котором писал Оруэлл, – считает писатель Михаил В. – Наша сегодняшняя цивилизация – цивилизация рабов. Жадных, меркантильных, трусливых и развратных рабов своего комфорта. А что такое раб? Это человек, который, во-первых, не может сам себя защитить, а во-вторых, не имеет ничего более ценного, чем собственная жизнь. Сегодня многие трясутся от ужаса, что мальчишка с пакетом взрывчатки бродит по мегаполису. В итоге кучка террористов диктует вам свои законы. Если ты боишься сам защищать себя - купи себе ошейник.

Коммерческий шпионаж

– Промышленный шпионаж и получаемая от него прибыль и есть тот локомотив, который двигает развитие технических средств для слежки за людьми, – считает Вадим Ф. – И сегодня бывает непросто разобраться, где шпионят за людьми, а где защищают собственные секреты. Для этого часто используются одни и те же приборы. Нельзя забывать, что защита коммерческих тайн человека не менее важна, чем его право не выносить на суд общественности, с кем он спит, моется в бане и играет в теннис.

Во времена, когда речи о демократических свободах еще не было, существовало понятие коммерческой тайны, которое защищало любое уважающее себя государство. В 480 году агенты византийского императора Юстиниана подкупили китайскую аристократку, которая в своей шляпке провезла в Европу шелковичных червей. Впоследствии это подорвало китайскую монополию на торговлю шелком на Ближнем и Среднем Востоке. А тринадцать веков спустя британский шпион Генри Уикхэм тайно вывез из Бразилии семена гевеи, и вскоре эта страна перестала быть монополистом в производстве каучука. Обе эти операции имели геополитические последствия, изменившие ход мировой истории. Не случайно гильдия каменотесов Страсбурга в 1495 году постановила под страхом смерти не рассказывать «купцам ли, болтунам ли секреты, коими каменотесы могут быстро и ловко работать».

Первый прообраз коммерческой разведки появился в Венеции в эпоху Возрождения. По существу, все венецианские купцы и дипломаты был и агентами дожа, при котором существовала аналитическая группа для обработки полученных сведений. В XVIII веке «разведслужба» семьи Ротшильдов сделала ее богатейшей династией в мире. Благодаря усилиям 200 агентов Натан Ротшильд первым в Лондоне узнал о поражении Наполеона при Ватерлоо. Он начал сбрасывать акции, вызвав на бирже предположения, что союзники разбиты. Началась паника, курс акций обвалился, и Ротшильд все скупил.

Сто лет спустя англичане уличили своих японских союзников в краже судостроительных секретов. Контрразведка Королевского Адмиралтейства подсунула им чертежи эсминца, который затонул сразу после спуска на воду в Иокогаме. С тех пор разведка развивалась неотрывно от шпионажа.

В Советском Союзе на сбор информации о западных технологиях выделялось 12 миллиардов франков ежегодно. Государственный комитет по науке и технике приобретал за год на огромную сумму западных научно-технических журналов, причем наиболее авторитетные среди них (например, Aviation Week and Space Technology) успевали перевести прямо в самолете при перелете в Москву. Добывать информацию таким образом в десятки раз дешевле, чем тратиться на собственные исследования.

По данным ФБР, советские специалисты были замечены в том, что при помощи клейкой ленты на подошве ботинок собирали микрочастицы сплавов, используемых на авиазаводе в Лонг-Айленде, а южнокорейцы «случайно» макали концы галстуков в жидкости в лабораториях. За последние четыре года ущерб от промышленного шпионажа, который ведут в США иностранцы, оценивается в 90 миллиардов долларов. Ежегодно по этим статьям привлекаются к судебной ответственности 500-700 человек. ФБР вынуждено постоянно держать под контролем 250 тысяч специалистов в 20 тысячах компаний.

В современной России об экономическом шпионаже всерьез заговорили в марте 1995 года, когда были выявлены группы лиц, устроившиеся на работу в коммерческие банки по фальшивым ходатайствам высших должностных лиц Центробанка и Минфина. Первая группа использовала советскую привычку банкиров брать под козырек перед вышестоящими «товарищами». Телефонный звонок от якобы секретарши, например, Петра Ивановича – и все решено. Во втором случае аферисты показывали банкирам фальшивые гарантийные письма на бланках Главного управления Центробанка. Обе группы намеревались с помощью агентуры получить конфиденциальную информацию о деятельности банков, чтобы в дальнейшем дестабилизировать их работу в своих интересах.

Большая охота

С тех пор многое изменилось. Если десять лет назад к шпионажу прибегали в основном криминальные структуры, намеревавшиеся взять какую-либо фирму под контроль или просто ограбить, то сегодня за этим стоят конкуренты. Сейчас охотятся за информацией о контрагентах фирмы, заказах и механизмах их получения, о предложениях на тендерах – всем, что может помочь вытеснить конкурента с рынка. Область бизнеса значения не имеет. Где вращаются самые большие средства и где выше конкуренция – там и больше вероятность столкнуться со шпионажем.

Большее внимание к своим секретам стали проявлять госструктуры. Защищенность информации, составляющей государственную тайну, оценивается специалистами как весьма высокая. А вот защищать коммерческую информацию государство пока не видит ни возможности, ни смысла. Проведение полноценных исследований по этой проблеме тормозит боязнь предоставить исполнителю конфиденциальные сведения. Тем более что среди крупных статистических бюро, действующих в России, много фирм с иностранным капита-

лом. Закрытые отчеты готовятся специалистами силовых ведомств для узкого круга профессионалов. По словам Анатолия Потапенкова, в прошлом сотрудника управления «Р» МВД России, чиновнику, сливающему служебную информацию за деньги, совершенно необязательно знать, при помощи каких методик он будет установлен.

– Промышленный шпионаж далеко не всегда означает охоту за копиями контрактов фирмы, – говорит адвокат Николай А. – Если собрать о ком-то из сотрудников фирмы сведения, что он, например, гей, то это можно использовать в дальнейшем для его шантажа и вербовки в качестве шпиона.

Чем выше прибыль предприятия, тем большие средств необходимо тратить на его безопасность. Для экономически развитых стран доля расходов на безопасность составляет 15-30 процентов прибыли предприятия.

Сегодня 80-90 процентов информации добывается с помощью техники. Закладка радиомикрофона для сотовых телефонов, например, со стандартом GSM позволяет прослушивать переговоры объекта, даже находясь в Новой Зеландии. Или оптоволоконные соединения: установить в них микрофон непросто, зато такой «жучок» крайне сложно обнаружить. Изобретены даже лазерные микрофоны, реагирующие на вибрации стекла в комнате при разговоре. Правда, их использование в условиях города практически невозможно из-за вибраций, вызываемых другими явлениями.

Чаще используются упрощенные методы. Например, подарки «с сюрпризом». Высокопоставленному госчиновнику знакомые поднесли на день рождения подарок – старинную икону, украшавшую в прошлом иконостас храма. Именинник обрадовался и повесил образ над сейфом в рабочем кабинете. Спустя некоторое время у чиновника создалось впечатление, что его кабинет прослушивают. Приглашенные специалисты обнаружили радиомикрофон и несколько крупных круглых батареек, вмонтированных прямо в древесину, на которую нанесено изображение. В другом случае бизнесмену поднесли дорогостоящую модель парусного судна. Оказалось, что в корпусе корабля спрятаны аккумуляторы, а снасти служили антеннами.

Согласно американским стандартам, оснастить аппаратурой поиска группу из пяти профессионалов обойдется в 750 тысяч долларов. На полную проверку помещений общей площадью, например, 300 квадратных метров у этой группы уйдет минимум два дня. Заказчику это обойдется в 200 долларов за квадратный метр. В Петербурге метр «стоит» 20-25 долларов при схожей производительности. В городе действует также ряд полулегальных контор, предлагающих обследовать офис фирмы за пару сотен долларов. Как правило, это мошенники. – Во многих развитых странах для приобретения шпионской аппаратуры нужна лицензия, а ее незаконное хранение является уголовно наказуемым деянием, как, например, хранение оружия, – говорит Николай А. – В российской практике шпиона могут привлечь к ответственности только если удастся доказать, что его действия нанесли кому-то серьезный вред. Формулировка «Нарушение конституционных прав и свобод личности» по-прежнему воспринимается в судах лишь как повод предъявить кому-то материальные претензии.

– Системы защиты от промышленного шпионажа, как и способы проникновения, индивидуальны, – говорит заместитель генерального директора петербургского ЗАО «Лаборатория противодействия промышленному шпионажу». – Самая распространенная ошибка предпринимателей – спохватываться, когда уже поздно. Особенно в небольших фирмах встречается вопиющее пренебрежение мерами безопасности. Например, в одном офисе уборщица заметила, что телевизор в холле воспроизводит голоса людей из соседнего кабинета. При осмотре помещений в коробке на шкафу обнаружили микрофон со множеством батареек. Коробка эта стояла у всех на виду несколько месяцев, а откуда он взялась, никто из сотрудников не помнит.

Другая классическая ошибка: многие руководители считают свой кабинет подходящим местом для конфиденциальных бесед. На самом деле для этого неплохо иметь специальную комнату. Там, где аппаратуру слежения использовать неэффективно, используют агентов влияния. В России нет западной традиции уважения к тайнам личности, поэтому многие видят в ремесле шпиона лишь увлекательную форму заработка. По данным опроса петербургского Центра занятости, около половины молодых петербуржцев не отказались бы попробовать себя в этой роли.

♦ ♦ ♦ ♦ ♦

16. Технологии дискредитации конкурентов – метод контрразведки*

В работе спецслужб наиболее распространенной технологией легендирования источника поступления компрматериалов является его анонимная передача или продажа в один из многочисленных «независимых» информационно-аналитических центров. Центр «совершенно секретно» информирует еще один объект, который в свою очередь передает ее в небольшую газету или местную теле- или радиостанцию, это значительно удлиняет цепь посредников и делает невозможным достоверно установить первоисточник информации. После определенной легализации на информационном рынке подключаются журналисты, которые уже готовят «заказную» статью, ссылаясь на легализовавший ее источник. Информация получает надежность в силу того, что все ее повторяют, но никто не знает, откуда она взялась. Наиболее часто в этих целях используются российские газеты «Сегодня», «Московский комсомолец» и «Совершенно секретно». Иногда при проведении подобных акций имеет место откровенная фабрикация внутренних документов спецслужб и правоохранительных органов. В Украине также четко просматривается использование газет «Сегодня», «Вечерние вести», «Киевские ведомо-

* По материалам сайта «Украина Криминальная»

сти», «Киевский телеграф», газета «2000», телекомпании «Интер», «ТЕТ», «ICTV», «Эра».

В большинстве случаев журналистам за публикации «выгодной» информации выплачивается довольно значительное вознаграждение. Также имеет место и установление прямых контактов со СМИ путем прямого финансирования отдельных изданий и программ, оказания им «спонсорской» помощи или же непосредственного вовлечения работников СМИ в хозяйственную деятельность.

Данный раздел в первую очередь призван помочь разобраться с самим понятием «активные мероприятия» и помочь найти формы и методы защиты от враждебного информационного воздействия на хозяйствующий субъект или на его руководство. Это может выражаться в усилении мер информационной безопасности, организации контрнаблюдения и так далее по полной программе. Так, например, подразделения безопасности некоторых структур ведут постоянный мониторинг на предмет наличия компрометирующих материалов на своих сотрудников с целью подготовки упреждающих заказных статей или передач в СМИ.

Если обратиться к советскому периоду нашей истории то, в качестве примера творческого подхода по противодействию «активным мероприятиям» оппонентов можно привести историю, которая произошла в конце восьмидесятых годов в Москве. Редакция одной газеты, славившейся своей патологической ненавистью к органам госбезопасности, разместила на своих страницах объявление от имени несуществующей школы по подготовке рыцарей плаща и кинжала. Данное учебное заведение якобы предлагало свои услуги по подготовке профессиональных диверсантов, в качестве контактного телефона для желающих был дан телефонный номер одного из подразделений КГБ СССР. Естественно, что когда чекистов стали одолевать звонки от желающих повысить свою квалификацию, то они без труда установили откуда в их сторону дует ветер, но самое интересное не это.

К ответной акции подошли с юмором. На «засвеченный» телефон повесили автоответчик, который милым женским голосом извинялся, что с данного адреса фирма переехала и просил перезвонить по новому номеру телефона. Новый номер - был домашним телефоном главного редактора «шутливой» газеты.

К сожалению, многие руководители различного уровня до сих пор недооценивают разрушительные возможности этих технологий. Как пример можно привести следующий случай из практики российских спецслужб.

Предприятие К. выпускает спортивно-охотничьи боеприпасы, пользующиеся большим спросом на внешнем рынке. Предприятие имеет форму открытого акционерного общества. Пакет акций в раз-

мере 30% сосредоточен в руках фирмы П, которая занимается поставкой на предприятие сырья. 35% акций принадлежит фирме В, которая реализует продукцию предприятия на внешнем рынке. 15% акций принадлежит фирме К. Остальные акции распределены между членами трудового коллектива предприятия. Золотая акция принадлежит Миноборонпрому.

После 17 августа усиливается конфликт между частью акционеров и дирекцией предприятия. Фирма П, владеющая около 30% акций предприятия и обеспечивающая предприятие сырьем, оказывается в достаточно затруднительном положении из-за того, что цены на закупку сырья у поставщиков заключены в долларовом эквиваленте, а на поставку сырья предприятию – в рублях.

Эмиссарами фирмы П начинается активная скупка акций у работников предприятия, а также формируется теневой аппарат управления предприятием, который, в случае, если контроль над предприятием после собрания акционеров перейдет в руки данной фирмы, должен будет заменить команду действующего директора. В теневой аппарат входят в большинстве своем лица, имеющие достаточный опыт работы на предприятии, но по различным причинам недовольные сложившимся положением дел.

В данном случае применяется типовая схема действий разведывательных органов по дестабилизации хозяйствующего субъекта:

Подрывная деятельность. Тактические действия, рассчитанные на подрыв единства команды управления изнутри, создание атмосферы недоверия и подозрительности. Раздувание конфликтных ситуаций. Создание в команде управления предприятия конфликта интересов.

Политические, экономические, социальные и идеологические разногласия между различными группировками в команде управления. Возможное соперничество между ними. Недовольство распределением материальных средств. Корыстные устремления отдельных руководителей. Недовольство трудового коллектива командой управления. Изучается история возникновения команды управления и сложившийся баланс интересов, причины, побудившие того или иного руководителя поддерживать ту или иную группировку в руководстве.

Разжигание противоречий осуществляется с целью углубления и доведения до «точки кипения» имеющихся различий между различными социальными группами и производственными кланами на предприятии. При этом используется недовольство людей действующим руководителем и его командой управления, их неудовлетворенность своим положением на предприятии (уровень заработной платы, распределение социальных льгот и т.д.), а также специально организуемые гонения, притеснения и провокации. В результате формируется своеобразная «пятая колонна», т.е категория лиц, враждебно на-

строенная к руководству предприятия и готовая помогать их оппонентам. Создаются условия для перехода наиболее перспективных кадров в стан оппонентов. Цель данных мероприятий - углубить имеющиеся противоречия до критического уровня и посредством этого максимально снизить способность к сопротивлению в отношении захвата предприятия. Внимание сотрудников предприятия привлекается к фактам коррупции и казнокрадства среди высшего и среднего звеньев менеджмента, их неспособности эффективно управлять предприятием. Такая пропаганда должна вызвать у рабочих и служащих чувство ущемленности, недовольство привилегированным положением высших менеджеров, их высокомерным отношением к подчиненным. Это, в свою очередь, снижает их готовность организованно выступить в защиту действующей команды управления.

Проникновение. Вербовка агентуры влияния в команде управления

Дискредитация руководства и ведущих сотрудников предприятия. (Дискредитация руководства хозяйствующего субъекта бывает эффективна только в том случае, если их популярность и авторитет снизились. В противном случае реакция на подобные акции бывает прямо противоположной. Самый большой пропагандистский характер имеют материалы, не содержащие прямых оскорблений в отношении руководства, так как объекты воздействия могут воспринять данные оскорбления, как личные.)

Вмешательство. Координирование и организованные усилия с тем, чтобы усложнить деятельность команды управления, тем самым снижая прибыль предприятия и увеличивая его расходы.

Информационно-психологическое воздействие (промывание мозгов). Осуществление широкой пропагандистской компании с целью формирования негативного мнения о предприятии и его руководстве. Заказные газетные статьи, теле- и радиопередачи о критическом положении на предприятии, рассчитанные на охват широкой аудитории, очень эффективно формируют негативное общественное мнение в отношении предприятия и его руководства. Одновременно происходит формирование положительного отношения работников предприятия, местных властей и населения к оппонентам действующей команды управления. Основная цель этих действий – сформировать в возможно более широких кругах установку на положительное восприятие своих намерений в отношении предприятия.

Систематическое распространение слухов, особенно правдоподобных. Слухи – это специфический вид информации, появляющийся спонтанно в силу информационного вакуума среди определенных слоев населения, либо специально кем-то распространяемый для воздействия на общественное сознание.

Очень часто с целью создания у общественности неблагоприятного впечатления о предприятии, используются лжесвидетели какого-

либо события, реально произошедшего на данном хозяйствующем субъекте. Слухи, как метод активного воздействия, наиболее опасны в критические для предприятия моменты, особенно, когда правду о реальном положении дел выяснить достаточно сложно, и в связи с этим общественное мнение становится очень восприимчиво к любой новости.

Распространение компрометирующих слухов с целью подрыва авторитета руководства хозяйствующих субъектов является достаточно сложной технологией воздействия, состоящей в составлении и распространении единого, по своей направленности, блока слухов. В него обычно входит информация как явно порочащая объект дискредитации, так и якобы «прославляющая», «защищающая» и «соболезнующая».

«Порочащие» слухи. Конкретные факты коррупции, связи с криминальными структурами, протекционистской кадровой политики. Все обвинения должны соответствовать действительности.

«Прославляющие» слухи. «Умелое» управление предприятием – за время руководства данной командой сокращено всего 70% сотрудников предприятия, оставшиеся 30% должны благодарить за то, что у них такое руководство.

«Защищающие» слухи. Да, предприятие долгое время было убыточным, но директор просто не смог ориентироваться в рыночной экономике.

«Соболезнующие» слухи. Новые акционеры хотят привлечь к ответственности за хищения на предприятии. Но команда управления слишком слаба, чтобы навести там порядок.

Инсинуации, намеки и разоблачения – вот типичный набор информационной войны, к которому прибегает противник. Его стремление сводится к подрыву доверия к доводам оппонента.

При этом используются различные обличительные характеристики, сплетни, недобросовестная информация, сенсационные разоблачения. В разоблачениях упор делается на принцип: «чем невероятнее, тем правдоподобнее «. При этой методике акцент сознательно делается на невероятность информации, во-первых, потому, что именно такая информация вызывает чувство шока, оторопи, и, во-вторых, невероятное правдоподобие так же трудно опровергнуть, как и подтвердить. Как любил говаривать доктор Геббельс: «Чем громаднее ложь, тем охотнее в нее верят».

Анализируя опыт избирательных компаний в местные органы власти можно с уверенностью утверждать о наличии во многих избирательных штабах групп по распространению слухов: откровенно прославляющих «своего» кандидата, взятых с потолка и легко дезавуируемых.

Распространение второго вида слухов решает сразу две задачи, первая – это создание повода еще раз напомнить о кандидате и попутно пнуть неразборчивых в средствах оппонентов, свалив на них ответственность за попытку опорочить светлый образ кандидата. Эти слухи словно своеобразные прививки позволяют увеличить барьер критичности электората по отношению к «активным мероприятиям» конкурентов.

Возвращаясь к выше сказанному – слухи – это форма альтернативного распространения информации. Известна следующая формулировка «закона» распространения слухов: С=Ф (В*Д), т.е. слух есть функция от произведения важности события на его двусмысленность.

По этому «закону» противодействие слухам, их опровержение, объяснение, запоздалая исчерпывающая информация будут лишь способствовать реанимации слухов, ибо все указанные средства ориентированы на устранение одной из составляющих данной формулы – двусмысленности. Но чем больше будет рвение в устранении двусмысленности, тем больше будет внимания привлекаться к самому факту, т.е. компенсаторно будет работать второй сомножитель – критерий важности события. Поэтому устранение слухов заключается в устранении двусмысленности. Полная (и своевременная недвусмысленная) информация о событии превращает второй сомножитель в величину, близкую или равную нулю. Это делает функцию от произведения двух сомножителей предельно мизерной. Говоря простым языком – слухов не будет, если не будет поводов к ним.

Система безопасности предприятия, состоящая из отдела режима и охраны, не в состоянии справиться с нависшей угрозой. Директор предприятия был вынужден обратиться за помощью в консалтинговое агентство. Отсутствие системы комплексной безопасности предприятия вылилось в круглую сумму непредвиденных расходов на скупку акций, на оплату услуг консалтингового агентства, на мероприятия информационного противодействия, штрафы антимонопольному комитету и федеральной комиссии по ценным бумагам, а также нанесло существенный моральный ущерб имиджу и престижу предприятия.

Информационно-психологическое воздействие под заказ

Если говорить о проведении заказных «активных мероприятий» то, с определенной долей обобщения можно выделить следующие категории их направленности:

- информационные войны между государствами;
- информационные войны между финансово-промышленными группами;
- информационные войны между властью и финансово-промышленными группами; информационные войны между властью

и оппозицией, которую в свою очередь поддерживают определенные финансово-промышленные группы (иностранные государства);

• информационные войны, инспирированные противостоянием разных сегментов власти, поддерживающих различные финансово-промышленные группы (иностранные государства).

Еще В.И.Ленин в своих трудах отмечал, что политика является концентрированным продолжением экономики. Если же попытаться построить причинно-следственные связи исследуемых политических событий, то это становится очевидным.

«Активные мероприятия» могут быть направлены на нанесение прямого экономического ущерба, так например в июле 1997 года Дж. Сорос предпринял успешную информационную атаку против национальной валюты ряда стран Азиатско-Тихоокеанского региона – Малайзии, Индонезии, Сингапура и Филиппин.

В итоге произошел скачок цен, национальные экономики этих стран были отброшены в своем развитии на 10-15 лет, а в Индонезии к маю 1998 года начался хаос.

Журнал «Эксперт» № 42 от 03.11.1997 г. так описывает эту ситуацию: «Еще осенью 1996 года появлялись сообщения, что группа фондов Дж.Сороса мобилизует ресурсы для атаки на гонконгский доллар. Глава финансового ведомства Гонконга Дональд Цан вызвал к себе представителей Сороса и ознакомил их с планами защиты гонконгского доллара в случае атак на него. Планы эти произвели на гостей такое впечатление, что они дали обещание не нападать на гонконгскую валюту. Но атаки на гонконгский доллар все же состоялись, и их эффект оказался оглушительным превыше ожиданий: кризис затронул не только Гонконг, но и весь мир.»

Следующим объектом воздействия, впавшего в головокружение от успехов господина Сороса, был Китай. И вот тут-то, как говорил всенародно любимый киногерой Глеб Жеглов, «промашка у вас, граждане, вышла»...

Учтя печальный опыт стран Юго-Восточной Азии, Китай серьезно готовился к предстоящему кавалерийскому наскоку Сороса и встретил его во всеоружии.

В ходе информационного противоборства с США китайским специалистам удалось правильно определить точное время нападения Сороса на китайский фондовый рынок и полностью «переиграть» американцев в ходе информационного противоборства в финансовой сфере в ходе азиатского кризиса 1997-1998 гг.

Проведение китайскими специалистами контрмер заключалось в нейтрализации финансовых атак Сороса на китайском фондовом рынке (поочередной игре на «повышение» или «понижение» путем скупки или, наоборот, экстренной продажи ценных бумаг). Полно-

стью блокировались специально распространяемые Соросом слухи в мировой информационной среде о неустойчивости китайского юаня.

Была предпринята и информационная атака на крупнейшую американскую фондовую биржу. Нью-Йоркская фондовая биржа осуществляет более 70% всех операций с акциями в США и является крупнейшей в мире. Тревожный сигнал об ответном китайском ударе прозвучал для США 27 октября 1997 года, когда курс акций на Нью-Йоркской фондовой бирже обрушился на 554,6 пункта. Это было наибольшее в истории падение акций американских компаний со времен «великой депрессии» 1929 года. В итоге акции американских «голубых фишек» значительно обесценились.

Вскоре китайцы практически полностью разорили Сороса. Его ведущий фонд был просто ликвидирован, а два мелких объединены. Поэтому когда кто-то говорит, что все «это чистая политика», он по меньшей мере лукавит, ну а если не лукавит, то ...

Сакраментальный вопрос: « А кому же это экономически выгодно ?» помогает с большой степенью уверенности, выявить истинных заказчиков того или иного политического явления. Вот по этому и гремят информационные войны, отодвигая от кормушки одних и приближая к ней столь же «хороших» других. В Украине, России, Беларуси, как и во всем мире, информационные войны имеют под собой в первую очередь экономические основания - установление своего контроля над сектором экономики или финансового рынка. Или наоборот защита своего места под солнцем от слишком уж шустрого конкурента.

Конечно, бывают скандалы, которые возникают самопроизвольно. Иногда преследуя свой узкокорыстный интерес, их поднимают на щит и развивают по нарастающей, но в большинстве случаев они заканчиваются так и не начавшись. Катализатором подобных явлений является в основном финансовая подпитка, а так как говорить о самоокупаемости многих СМИ было бы весьма опрометчиво, то вывода делайте сами.

Кстати, в последнее время российская общественность настолько привыкла к тому, что практически все скандалы заказные, что даже то, что не является рукотворным, часто воспринимают как «заказуху».

В регионах информационные конфликты очень редко бывают масштабными и затяжными. Это и понятно, финансовые ресурсы заказчиков весьма ограничены, да и цели в них преследуются в основном оперативно-тактические. «Бои местного значения» становятся всегосударственным и даже международным достоянием, только в том случае если куски делимой собственности настолько значительны, что вызывают интерес у определенных клановых структур, включая столичные.

В основном «активные мероприятия» в регионах решают две типовые задачи. От объекта информационной атаки требуется выполнение определенных действий в интересах инициатора «активки». Объект просто хотят убрать с дороги без применения силовых методов. В последнем случае самой благодарной аудиторией этой информации являются, как правило, местные правоохранительные органы и спецслужбы.

Если попытаться проследить историческую перспективу «активных мероприятий», то без труда можно отметить, что попытки переломить ход событий в свою пользу с помощью различных информационных технологий предпринимались с самого момента зарождения человеческого общества. Для того чтобы подтвердить этот тезис достаточно просто перелистать Библию или нетленное произведение китайского философа Сунь Дзы «Искусство войны». Очень детально и весьма квалифицированно методики информационной войны описаны в « Протоколах сионских мудрецов».

В практическом плане стоит отметить профессионально подготовленные и квалифицированно исполненные «активные мероприятия» американской разведки против СССР: «вброс» на заседание ООН смонтированной в нужном русле записи переговоров центра управления полетами и пилота истребителя, сбившего в 1993 году южнокорейский «Боинг»; компания по обвинению болгарских, и соответственно советских спецслужб в покушении на Папу Римского и многое, многое другое.

Справедливости ради, в качестве весьма эффективного аппарата «активных мероприятий» так же можно привести Службу «А» («активные мероприятия») Первого главного управления КГБ СССР. Не смотря на свою малочисленность (ее аппарат составлял около ста человек), эта служба добивалась значительных успехов, в отличии от огромного и неповоротливого отдела внешнеполитической пропаганды ЦК КПСС. Основные действия Службы «А» были направлены на дискредитацию всех аспектов американской политики, создание условий для конфликтов между США и их союзниками по НАТО, одним из направлений работы была и всесторонняя информационная поддержка западных движений сторонников мира. В качестве наиболее успешных акций ПГУ можно привести распространение информации о том, что вирус СПИДА имел непосредственное отношение к американским военным биолабораториям, а также активное муссирование версий о причастности ЦРУ к убийству Патриса Лумумбы, Мартина Лютера Кинга и Улофе Пальме.

Кстати, в усилении интенсивности скандала о применении американцами на территории бывшей республики Югославия боеприпасов с низкообогащенным ураном явно чувствуются умелые руки и

светлые головы сотрудников соответствующих подразделений российской внешней разведки.

Да и случай с опубликованием именно в России мемуаров бывшего сотрудника английской разведки MI-6 Ричарда Томлинсона «Большой провал», скорее всего можно расценивать как «наш ответ Чемберлену» на книгу К.Эндрю и О.Гордиевского по истории советской разведки. У ребят из Ясенева в этом отношении всегда была очень хорошая память.

К тому же в связи с ростом профессионализма российской организованной преступности многие специалисты, в частности, ныне к сожалению покойный С.С.Овчинский, открыто ставят вопрос об использовании методик «активных мероприятий» (ранее свойственных в основном спецслужбам) органами Министерства внутренних дел и Федеральной службы налоговой полиции.

Активные мероприятия в современных условиях

В последнее время в связи с развитием технического прогресса технологии «активных мероприятий» становятся все более и более изощренными. И если раннее шекспировскому Яго, для компрометации Дездемоны, в глазах объекта информационной атаки Отелло, достаточно было просто шепнуть ему об этом на ухо, то сегодня скорее всего эти сведения были бы размещены на одном из интернетовских сайтов.

Первым догадался использовать «мировую паутину» для «активных мероприятий» американский прокурор Кеннет Старр: именно благодаря ему весь мир смог детально ознакомиться с трогательной историей любви практикантки Белого дома Моники Левински, а также тщательно изучить отдельные моменты анатомического строения Президента Соединенных штатов Б.Клинтона.

Днем рождения российского сетевого компромата можно считать 26 ноября 1998 года, именно в этот пасмурный день и появился сайт «Коготь», в тот же самый день оперативно закрытый российскими спецслужбами. Информационное наполнение сайта состояло из восемнадцати файлов, содержащих в себе сводки прослушивания телефонных переговоров чиновников и политиков высокого ранга.

По информации Интернет-провайдеров российские информационные узлы политической и экономической направленности, а также сайты средств массовой информации посещает более 1.000.000 человек. Это говорит о том, что уже сегодня число русскоязычных пользователей Интернета, позволяет серьезно использовать его возможности для ведения масштабных информационных войн.

Для российских технологов «активных мероприятий» Интернет интересен еще и тем, что он является входным информационным каналом для определенной целевой аудиторией. Каждый пользователь сети в процессе общения со своим окружением становится передат-

чиком (транслятором) полученной информации. Отдельные категории интернетовской аудитории, такие например как журналисты, способны многократно усилить волну от брошенного в информационное море камешка. Как пример, можно привести все тот же «Коготь», число его посетителей было невелико, но широким читательским массам он стал доступен благодаря публикациям его данных в газетах «Московский комсомолец» и «Московские новости».

Это еще раз подтверждает тезис о том, что в кризисных ситуациях даже небольшие информационные выбросы способны привести к весьма серьезным результатам. В качестве еще одного высокоэффективного «активного мероприятия» можно привести сайт «Коготь-2». Размещенная на нем информация, была посвящена различным деяниям тогдашнего хозяина Красноярского алюминиевого завода Анатолия Быкова. Но вот, что показательно, если для широкой российской публики этот была лишь очередная сенсация, быстро вытесненная новыми скандалами, то в Красноярском крае акция дала совершенно определенный политический и экономический результат.

♦ ♦ ♦ ♦ ♦

СОДЕРЖАНИЕ

Книга 1. Разведка

Книга 2. Контрразведка и шпионаж

Книга 3. Экономические проблемы

Книга 4. Защита

Навчальне видання

Зеркалов Дмитро Володимирович

КОНТРРОЗВІДКА І ШПИГУНСТВО

У чотирьох книгах
Книга 2

Хрестоматія

Авторське редагування
Відповідальний за випуск – О. Т. Ростунов
Комп'ютерний макет – Р. М. Мубараков

Підписано до друку 03.04.2008 р. Формат 60x84/16.
Папір Data Copy. Гарнітура Таймс. Друк циф. дублікатор.
Ум. друк. арк. 11,19. Обл.-вид. арк. 11,05.
Тираж 300. Зам. 4/03.
Видавництво – «Видавництво "Науковий світ"»®.
Друк – друкарня ПП Ростунова О.Т.
Свідоцтво ДК № 249 від 16.11.2000 р.
03680, м. Київ, вул. Боженка, 17, оф. 504.
тел. 200-87-15, 200-87-13, 8-050-525-88-77.
E-mail: nsvit@mail.ru