К.Б. Беловицкий

ОСНОВНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ ФАКТОВ КОММЕРЧЕСКОГО ШПИОНАЖА

УЧЕБНОЕ ПОСОБИЕ

УДК 338.246
ББК 65.9(2Рос)-98
Б43

Автор:

К.Б. Беловицкий – к.э.н., доцент, доцент кафедры экономической экспертизы и финансового мониторинга ФГБОУ ВО «МИРЭА – Российский технологический университет».

Рецензенты:

В.Н. Анищенко – д.т.н., профессор, профессор кафедры экономических и финансовых расследований Высшей школы государственного аудита МГУ им. М.В. Ломоносова;

С.В. Верёвкин-Рахальский – генерал-лейтенант, почетный сотрудник ФСБ России и ФСНП России, советник генерального директора АО «Объединенная энергетическая компания».

Беловицкий, Константин Борисович.

Б43 Основные методы выявления фактов коммерческого шпионажа : учебное пособие / К.Б. Беловицкий. – Москва : Издательско-торговая корпорация «Дашков и К°», 2021. – 345 с. : ил.

ISBN 978-5-394-04261-4.

В учебном пособии раскрывается история развития коммерческого шпионажа и правовые основы противодействия фактам коммерческого шпионажа, показаны методы противодействия получению закрытой информации через открытые источники и технические каналы утечки информации, а также получению физическими лицами закрытой информации. Дана характеристика и методы противодействия киберпреступности, а также способы защиты информации, составляющей коммерческую тайну.

Для студентов, обучающихся по специальности 38.05.01 «Экономическая безопасность», преподавателей вузов, а также сотрудников подразделений экономической безопасности.

УДК 338.246
ББК 65.9(2 Рос)-98

ISBN 978-5-394-04261-4

СОДЕРЖАНИЕ

Тема 1. ИСТОРИЯ РАЗВИТИЯ, ПОНЯТИЕ И СУЩНОСТЬ КОММЕРЧЕСКОГО ШПИОНАЖА

Введение

В условиях рыночной экономики невозможно получение прибыли от коммерческой деятельности, с одной стороны, без доведения до потребителя информации о товарах, работах и услугах, с другой стороны, без защиты информации о деятельности предприятия от конкурентов.

Сбором и обработкой экономической информации занимаются маркетологи, сотрудники служб безопасности, государственные органы, правоохранительные и специальные службы, сотрудники коммерческих разведок, члены организованной преступности и многие другие. Происходит тотальная разведывательная и контрразведывательная работа. Поэтому хозяйствующие субъекты, чтобы выжить в конкурентной борьбе, вынуждены заниматься как коммерческим шпионажем, так и контршпионажем.

На сегодняшний день существует объективная потребность в такой разновидности деятельности, как частная контрразведка. Это контршпионаж как орган и как функция юридического лица.

Для того чтобы определить подходы к решению указанной проблемы, автор предпринял попытку обобщения материалов о коммерческом шпионаже и противодействии ему, почерпнутых из открытых источников и позволяющих взглянуть на контрразведывательную деятельность с разных точек зрения.

Содержащиеся в учебном пособии сведения помогут в решении практических задач частной службы контршпионажа.

Мероприятия контршпионажа необходимо осуществлять постоянно, в том числе тогда, когда отсутствуют достоверные сведения о конкретной угрозе со стороны конкретных лиц или организации. Кроме того, последствия успешных действий, скажем, разведки конкурентов (в форме скрытого хищения информации), проявляются спустя некоторое время, когда бывает достаточно трудно выявить истинную причину ухудшения финансового положения фирмы или появления у конкурента идентичной продукции. Это не способствуют психологической готовности руководителя к существенным расходам на нужды «своей контрразведки».

Между тем контрразведывательным органам противостоит аппарат разведки противника, использующий разнообразные методы добывания информации, в том числе весьма изощренные, и обладающий современными техническими средствами. Поэтому возможности контрразведки не должны уступать возможностям разведки.

Дисциплина «Основные методы выявления фактов коммерческого шпионажа» имеет своей целью способствовать формированию у обучающихся общепрофессиональных и профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности 38.05.01 «Экономическая безопасность».

В результате изучения дисциплины обучающийся должен:

знать:

– основные направления профилактики коррупционного поведения;

– законодательные, организационно-правовые основы, механизмы экономико-правовой защиты частной, государственной, муниципальной и иных форм собственности;

– факты, события и обстоятельства, создающие угрозы экономической безопасности;

– положения материального и процессуального права в вопросах противодействия угрозам экономической безопасности;

– средства, приемы и методы психологического воздействия, их сущность, составные части и основы применения при решении профессиональных задач;

– формы предварительного (досудебного) расследования экономических преступлений;

– источники и порядок получения информации о субъектах предпринимательства;

– методы сбора, анализа, систематизации, оценки и интерпретации данных, необходимых для решения профессиональных задач;

уметь:

– юридически правильно квалифицировать факты, события и обстоятельства, создающие угрозы;

– осуществлять анализ и диагностику финансового состояния и результатов деятельности хозяйствующего субъекта;

– оценивать эффективность его работы, в том числе его структурных подразделений и работников;

– осуществлять выбор инструментальных средств для обработки экономических данных в соответствии с поставленной задачей, анализировать результаты расчетов и обосновывать полученные выводы;

– анализировать юридические факты и возникающие в связи с ними правовые отношения, экономические последствия, оценивать их значение для решения задач защиты частной, государственной, муниципальной и иных форм собственности; применять экономико-правовые методы защиты собственности;

– осуществлять расследование экономических преступлений в форме дознания;

– организационно-правовые основы, принципы, факторы, механизмы, методы и средства обеспечения экономической безопасности;

– применять средства управления состоянием человека при решении профессиональных задач;

владеть:

– навыками выявления и устранения причин и условий, способствующих коррупционным проявлениям в служебном коллективе;

– навыками выявления, оценки, локализации и нейтрализации угроз частной, государственной, муниципальной и иным формам собственности от мошеннических и иных преступных посягательств, экономико-правовой защиты прав и законных интересов их владельцев;

– навыками реализации норм материального и процессуального права, способствующих устранению угроз экономической безопасности;

– навыками выявления, оценки, локализации и нейтрализации угроз экономической безопасности, формирования модели системы безопасности;

– навыками получения юридически значимой информации;

– навыками выявления и устранения причин и условий, способствующих зарождению угроз экономической безопасности;

– совокупностью средств психологического воздействия и алгоритмами их использования;

– навыками получения информации с использованием различных форм предварительного расследования экономических преступлений;

– навыками сбора, анализа и обработки экономической и социально-экономической информации в целях решения профессиональных задач.

Дисциплина «Основные методы выявления факторов коммерческого шпионажа» относится к вариативной части профессионального цикла учебного плана специальности 38.05.01 «Экономическая безопасность».

Студенты найдут ответы на следующие вопросы:

- Что надо защищать?
- Каким угрозам подвергаются объекты защиты?
- Какие способы и средства защиты целесообразно применять?
- Как организовать службу «своей контрразведки»?
- Как осуществлять эту деятельность законно?

Без правильных ответов на эти вопросы защита будет осуществляться хаотично, будет требовать больших финансовых затрат с минимальным результатом.

С учетом открытого характера пособия, в нем изложены основы контрразведывательной деятельности на базе синтезированного материала, без раскрытия конкретных механизмов применения оперативных (оперативно-розыскных, оперативно-технических, агентурно-оперативных) мероприятий, которые регламентированы закрытыми нормативными актами правоохранительных органов и государственных спецслужб. Но и тот материал, что приведен, вполне достаточен, чтобы получить необходимые знания о сущности, формах и методах контрразведывательной деятельности коммерческих организаций и успешно применять их на практике.

1.1. КОММЕРЧЕСКИЙ ШПИОНАЖ В ДРЕВНОСТИ, В СРЕДНИЕ ВЕКА И В НАСТОЯЩЕЕ ВРЕМЯ

1.1.1. Коммерческий шпионаж до нашей эры

Одним из древнейших промышленных шпионов был древнегреческий титан Прометей. По древнейшей версии мифа, Прометей похитил огонь у Гефеста, спрятал его в полом стебле тростника, унёс с Олимпа, передал людям и показал, как его сохранять, присыпая золой. Этот тростник имел внутренность, заполненную белой мякотью, которая могла гореть как фитиль.

За похищение огня Зевс приказал Гефесту приковать Прометея к Кавказскому хребту. Он был наказан за то, что ослушался Верховного Бога.

Прометей был прикован к скале и обречён на непрекращающиеся мучения: прилетавший каждый день орёл, клевал у Прометея печень, которая в дальнейшем вновь отрастала. Эти муки, по различным античным источникам, длились от нескольких столетий до 30 тысяч лет, пока Геракл не убил стрелой орла и не освободил Прометея.

Налицо классическая шпионская схема: похищение образца, передача заказчику, раскрытие сотрудниками контршпионажа, наказание за содеянное.

Не обошлось без шпионов и в Библии. Так описывается разведывательная операция примерно XIII века до нашей эры:

«И послал их Моисей высмотреть землю Ханаанскую, и сказал им: пойдите в эту южную страну, и взойдите на гору, и осмотрите землю, какова она, и народ, живущий на ней, силен ли он или слаб, малочислен ли он или многочислен? И какова земля, на которой он живет, хороша ли она или худа? И каковы города, в которых он живет, в шатрах ли он живет или в укреплениях? И какова земля, тучна ли она или тоща? Есть ли на ней дерева или нет? Будьте смелы и возьмите от плодов земли. Было же это ко времени созревания винограда... Они пошли и высмотрели землю от пустыни Син даже до Рехова... и пошли в южную страну, и дошли до Хеврона... и пришли к долине Есхол, и срезали там виноградную ветвь с одною кистью ягод, и понесли ее на шесте двое, [взяли] также гранатовых яблок и смокв. И высмотрев землю, возвратились они через сорок дней» (Книга Чисел 13:18-26).

Что мы видим? Инструктаж шпионов о маршруте, о конкретных сведениях, которые необходимо получить. Кроме получения экономической информации дается задание добыть и принести для оценки образцы продукции. И по окончании рейда – отчет о выполнении задания.

В европейском раннем средневековье центром шпионажа стала Византия. Любопытно, что создательницей его выступила Феодора – дама с весьма нетривиальной биографией: начинавшая карьеру как проститутка (Прокопий Кесарийский писал: «Она не была ни флейтисткой, ни арфисткой, она даже не научилась пляске, но лишь продавала свою юную красоту, служа своему ремеслу всеми частями своего тела»), она сумела женить на себе императора Юстиниана!

Впрочем, и этим дело не закончилось: сочетая религиозный фанатизм с изрядной жестокостью, Феодора весьма эффективно распространяла христианство – и после смерти была канонизирована!

1.1.2. Коммерческий шпионаж до XIX века

Пожалуй, самый ранний описанный случай промышленного шпионажа – история с тутовым шелкопрядом. Точнее, сразу две истории примерно одного времени – четвертого-пятого веков нашей эры. Сначала в качестве промышленного шпиона выступила китайская принцесса, не испугавшаяся суровых законов (по которым за такое полагалась не самая легкая смерть) и провезшая драгоценные яйца шелковичных червей и семена тутового дерева в высокой вычурной прическе в качестве приданого своему будущему супругу. Так шелкопряд оказался в Индии. Далее уже по приказу императора Юстиниана двое монахов храма Настури вывезли из Индии в Византию шелкопрядов внутри пустотелого бамбукового посоха.

Сложно даже подсчитать ущерб, который нанесли экономике Китая (до того – шелкового монополиста) всего три человека, похитившие то, что можно спрятать в прическе или палке...

Военный шпионаж всегда шел рука об руку с промышленным.

На Западе в те времена шпионаж был связан в первую очередь с торговой деятельностью и с интригами внутри государств и между ними. Так, без развитой сети разведчиков не смогла бы стать первым европейским экономическим сообществом Ганза – союз немецких свободных городов. Период политической неустойчивости XIII века, пока династия Габсбургов еще не заняла главенствующего положения, а от рыцарей-разбойников было некуда деваться, стал для Ганзейского союза временем подъема и распространения торговли через Балтийское и Северное моря и по всей Северной Германии. Точное знание, когда будут блокированы те или иные города, а, следовательно, какие товары вскоре будут в дефиците и могут быть проданы с большей прибылью, и позволяло доминировать на североевропейских и западноевропейских рынках купцам из Гамбурга, Бремена, Любека.

В XVIII–XIX веках промышленный шпионаж всячески стимулировался на государственном уровне. Так, например, именно благодаря ему в 1712 году в Париж пришли первые данные, касающиеся

производства китайского фарфора (которые в течение столетий держались в тайне от европейцев), – постарался французский священник-иезуит д'Антреколь. Французы смогли создать фарфор, равноценный китайскому... и не смогли сохранить тайну: всего через несколько лет английские, австрийские и саксонские шпионы лишили Францию европейской монополии.

Французский закон 1791 года любопытно (и абсолютно в духе времени) подходил к проблеме авторского права: он предоставлял первому ввезшему во Францию какой-либо новый иностранный продукт те же права, что и его создателю! Благодаря этому мудрому нормативному акту Франция обогатилась паровыми машинами, промышленными хлопковыми тканями, производством каучука... и даже рецептом сахара из сахарной свеклы! Любопытно, что распространению последнего поспособствовали как Англия (устроившая морскую блокаду в ответ на действия Наполеона), так и шпионы Наполеона, нашедшие малоизвестных химиков в Силезии: те, в 1802 году, основали первую подобную мануфактуру.

Любопытно, что довольно многие творческие личности сочетали профессию шпиона с писательской. По-своему логично: объяснение «я ищу новые темы для книг» прекрасно гармонирует с сованием носа в самые разные дырки! Одним из первых в череде таких «совместителей» стал автор знаменитого романа «Робинзон Крузо» Даниэль Дефо – работавший в тогда враждебной Шотландии и написавший труд по теории шпионажа. Несколько позже во Франции на скользкую дорожку агента вступил Пьер-Огюстен Карон де Бомарше – знаменитый французский драматург и публицист, а также дуэлянт, скандалист и интриган... то есть настолько публичная личность, что заподозрить его в тайных махинациях было просто невозможно! А зря – как шпион Бомарше был весьма удачлив и успешен: его наработки и сегодня используют спецслужбы (скажем, он ввел в практику открытие фиктивных предприятий).

1.1.3. Коммерческий шпионаж XIX–XXI веков

В 1872 году Альфред Крупп опубликовал правила внутреннего распорядка и роздал их своим рабочим. Впервые была легализована современная промышленная безопасность. Мы можем привести

следующую фразу из этих правил: «Независимо от издержек производства, необходимо, чтобы за рабочим постоянно наблюдали энергичные и опытные люди, которые получали бы премию всякий раз, когда задерживали саботажника, лентяя или шпиона».

В дополнениях к правилам, появившимся позднее, указывалось, что завод должен преследовать и социалистов. Необходимо признать, что Альфреду Круппу удалось создать определенную «крупповскую атмосферу», которая существует и в наши дни. Одновременно с расширением своих служб шпионажа и контрразведки Крупп создавал чрезвычайно крупные, хорошо оплачиваемые научно-исследовательские группы.

В СССР промышленный шпионаж не существовал, так как промышленные предприятия были в основном государственными. Конкуренции внутри страны между предприятиями практически не было. Экономика была плановой и о прибыли речь не шла. Система гарантировала своевременную и стопроцентную оплату всей произведенной продукции. Главной задачей было выполнение производственного плана. Интересы в сфере экономики защищали ОБХСС и спецслужбы.

Однако совершенно другая картина была на международном уровне. Здесь промышленным шпионажем, а вернее научно-технической разведкой и контрразведкой занималось КГБ и ГРУ.

Хотелось бы рассказать об одной уникальной операции проведенной советскими спецслужбами. В 1943 году, по возвращении с Тегеранской конференции, Сталин поставил перед Берией задачу: во что бы то ни стало проникнуть в рабочий кабинет американского посла Аверелла Гарримана. Операция по прослушиванию рабочего кабинета главы американской дипломатической миссии в Москве стала классикой шпионажа и до сих пор является уникальной. Но как установить «жучка» в кабинете Гарримана? Сотрудники НКВД не смогли туда проникнуть даже под видом пожарных, когда в здании посольства был организован грандиозный пожар. И тогда родилась идея вмонтировать микрофон в некий подарок послу... Группа высококвалифицированных сотрудников из оперативно-технического управления госбезопасности под руководством академиков Акселя Берга и Абрама Иоффе изготовили уникальный микрофон. Это было исключительно пассивное подслушивающее устройство, не имеющее ни элементов питания, ни металлических деталей, ни намека на какую бы то ни было генерацию тока, – вообще

ничего такого, что могло быть обнаружено с помощью имевшихся на вооружении специалистов мира того времени технических средств.

Устройство, отдаленно похожее на головастика с маленьким хвостом, виртуозно вмонтированное в американский герб, приводилось в действие внешним источником излучения микроволнового сигнала, который заставлял рецепторы «головастика» резонировать. Голоса людей влияли на характер резонансных колебаний устройства, позволяя осуществлять внятный перехват слов. Что примечательно: даже без помех! Микрофон мог действовать сколь угодно долго. Микроволновые импульсы подавались «головастику» чрезвычайно энергоемким генератором с расстояния примерно в триста метров. Прием, расшифровка и запись на магнитную ленту возвращающихся колебаний осуществлялись другим уникальным устройством, расположенным на одной линии с передающим генератором. Чтобы передающиеся и принимаемые импульсы не накладывались, вся геометрическая фигура должна была иметь форму равнобедренного треугольника. И она такой была с точностью до миллиметра!

Итак, 9 февраля 1945 г. открытие пионерской здравницы «Артек» – с вручением лагерю ордена Трудового Красного Знамени. Накануне Франклину Рузвельту и Уинстону Черчиллю вручили приглашение от детей – знак глубокой благодарности за помощь в годы войны.

Естественно, страшно занятые Рузвельт и Черчилль при всем желании не смогли бы выкроить время.

А следующими по рангу кандидатами на поездку к детворе могли быть только посол США в Москве Аверелл Гарриман и его коллега из Великобритании – сэр Арчибальд Джон Кларк Керр.

И вот кульминация встречи: оркестр грянул американский гимн, хор пионеров (настоящих) запел «звездное время» на английском языке. Гарримана прошибла слеза. В тот же миг четверо пионеров внесли огромный, сверкающий лаком, деревянный... Герб Соединенных Штатов Америки!

Потерявший от восторга дар речи, осторожнейший дипломат Гарриман, едва ли не впервые за свою карьеру выпалил, что думал: «куда же мне его девать?.. Где держать?.. Я же не могу оторвать от него глаз!..» Проинструктированный накануне переводчик Бережков невзначай и ненавязчиво заметил: «да повесьте у себя в рабочем кабинете... Англичане умрут от зависти».

В итоге «златоуст», обрамленный гербом Соединенных Штатов, благополучно оказался на сверхсекретном этаже здания американского посольства в Москве, конечно, после тщательной проверки американскими специалистами. Операция НКВД под кодовым названием «исповедь» – прослушивание совещаний, проводимых послами, – началась. И продолжалась 8 (восемь!) лет. «Златоуст» пережил четверых чрезвычайных и полномочных послов Соединенных Штатов Америки в Москве. Самое удивительное: каждый из них стремился полностью – от чернильницы до паркета на полу – поменять интерьер кабинета. Неизменно оставался на своем месте только герб. Его художественное совершенство действовало гипнотически – даже шторы на окнах и мебель подбирались в тон гербовой цветовой гамме. Сталин узнавал о принятых там решениях раньше президента США.

Герб в кабинете посла пережил четырех хозяев, пока в 1952 году завербованный ЦРУ офицер ГРУ Петр Попов не предупредил американцев об информационной утечке из посольства. До получения агентурной информации от Попова о подслушивании американцы периодически проверяли кабинет, но ничего подозрительного не находили. Однако получив «наводку» из ЦРУ, американские поисковики приступили к более тщательным обследованиям с использованием детектора электромагнитных излучений. Тогда и был обнаружен подозрительный сигнал на частоте 800 МГц, локализуя который специалисты сосредоточили свое внимание на деревянном гербе.

Техники разобрали герб и нашли внутри него необычную начинку. Как писали сами американцы, обнаруженное устройство оказалось настоящей революцией в технике подслушивания. Оно было спрятано в середине герба, в специально вырезанной нише, имевшей тщательно скрытое акустическое отверстие (оно выходило в ноздри орла).

Наконец-то обнаружив «златоуста», американцы семь лет хранили в тайне это унизительное для них открытие. И только в мае 1960 года, после того как сбили самолет-шпион «У-2» с Гарри Пауэрсом на борту, Вашингтон обнародовал эту историю: мол, советы шпионят не меньше нашего.

Обнаружив «златоуст», американцы и англичане пытались сделать с него копию. Тщетно! Они так и не сумели разгадать тайну генератора, излучающего микроволны.

И еще об одной успешной операции советской разведки на ниве промышленного шпионажа.

По мнению академика Курчатова, работа немецких учёных и материалы из Германии после окончания Великой отечественной войны позволили сократить время на создание советской бомбы, минимум, на год. Ещё на несколько лет этот срок уменьшили разведывательные донесения из США другого немецкого учёного – эмигранта из Германии Клауса Фукса главного атомного разведчика СССР, участника «Манхэттенского проекта».

В феврале 1950 года, после провала советской агентурной сети в результате расшифровки АНБ советского шифра в рамках проекта «Венона», физик-теоретик Клаус Фукс был арестован в Англии; Фукс выдал Голда, который 23 мая был вынужден сознаться, что он связной советской разведки. Голд выдал Грингласса, а Грингласс – Розенбергов. Клаус Фукс был осуждён на 14 лет.

Полный список переданной гражданином США Юлиусом Розенбергом информации продолжает оставаться секретным. Известно лишь, что сам «Либерал» в декабре 1944 года добыл и вручил советскому разведчику Александру Семеновичу Феклисову (один из шести советских разведчиков, удостоенных звания Герой России за вклад в решение «атомной проблемы» в нашей стране) подробную документацию и образец готового радиовзрывателя. Это изделие высоко оценили наши специалисты. По их ходатайству было принято постановление Совета Министров СССР о создании специального КБ для дальнейшей разработки устройства и о срочном налаживании его производства. Между тем, после окончания Второй мировой войны американская печать писала о том, что созданные в период войны радиовзрыватели по своему значению уступают лишь атомной бомбе и на их создание было истрачено свыше одного миллиарда долларов! Розенберги были единственными гражданскими лицами, казнёнными в США за шпионаж за время холодной войны, это произошло в 1953 году.

В США ежегодные потери бизнеса от экономического и промышленного шпионажа, в соответствии с отчетами ФБР, составляют до 100 млрд. долл. Значительную лепту в общий объем потерь США, как никакой другой страны мира, вносит кибершпионаж, в настоящее время являющийся одной из главных составляющих как экономического, так и

промышленного шпионажа. Причиной тому является то, что Соединенные Штаты сильнее других государств зависят от сетевой инфраструктуры: здесь сосредоточено более 40% вычислительных ресурсов мира и около 60% информационных ресурсов Интернета.

Выделить и проанализировать отдельно сумму потерь от экономического и промышленного шпионажа не представляется возможным. Вместе с тем проведенный американскими специалистами анализ показывает, что в 58% случаев экономический и промышленный шпионаж осуществлялся по заданиям зарубежных компаний, в 22% – в интересах иностранных правительств и в 20% – частных и государственных зарубежных научных центров и лабораторий. При этом менее развитые страны, как правило, стремятся к вывозу технологий, доступных на коммерческом рынке. По данным исследования, проведенного Американским обществом промышленной безопасности, было установлено, что в большинстве случаев осуществления промышленного шпионажа наибольшую ценность для конкурирующих компаний представляла информация о научных исследованиях и разработках (49%).

Фактов промышленного шпионажа на американской земле можно приводить очень много. Свежим примером промышленного шпионажа является осуждение семейной пары за кражу технологий у концерна General Motors (GM). Злоумышленники, американцы китайского происхождения, похитили технологии гибридных силовых установок у концерна GM, чтобы продать их Китаю для последующего воспроизведения. Им удалось скопировать около 16 тыс. документов компании, 20 из которых содержали коммерческую тайну. Суд штата Мичиган оценил украденные технологии в 46 млн. долл. и осудил супружескую пару к тюремному заключению и выплате штрафа в размере 40 тыс. долл.

В Германии нелегальное присвоение секретов производства (ноу-хау) только иностранными фирмами, по заявлению главы Рабочей группы по безопасности в экономике ФРГ Бертольда Штоппелькампа, обходится экономике страны не менее чем в 20 млрд. евро каждый год. По словам Штоппелькампа, не более 6% случаев становится достоянием гласности. Более трети немецких компаний считали, что у них была осуществлена кража промышленных секретов, однако обращения в

правоохранительные органы сделаны не были. Только в Мюнхене за период с начала 2010 года по сентябрь 2011 года от такого рода действий пострадало более 250 фирм, общие убытки составили 35 млн. евро. По мнению немецких аналитиков, если в 2000 году объектом охотников за коммерческими тайнами была каждая десятая компания в Германии, то сегодня – каждая четвертая. Интерес для промышленных шпионов, по данным германских исследователей, представляют научные исследования и конструкторские разработки (16%). Основными способами незаконного получения конфиденциальной информации являлись: вербовка сотрудников конкурирующих организаций; получение информации через поставщиков услуг и консультантов; хакерские атаки на компьютерные системы; технический перехват электронных сообщений; кража документов, материалов и образцов; прослушивание и перехват конфиденциальных переговоров.

1.1.4. Ущерб от коммерческого шпионажа в некоторых странах

В Великобритании, по данным Управления компьютерной безопасности и информационной надежности (OCSIA), потери британских корпораций из-за краж интеллектуальной собственности – конфиденциальных данных по проектам, методикам и разного рода коммерческим тайнам, за год составили почти 9,2 млрд. фунтов стерлингов. Кроме того, в соответствии с обнародованными данными, ежегодные потери от непосредственно организованного промышленного шпионажа составляли 7,6 млрд. фунтов стерлингов. Подчеркивалось, что при этом 1 млрд. фунтов стерлингов пропадает из-за воровства персональных данных.

В Японии, по результатам проверки Министерством экономики, торговли и промышленности 625 предприятий, выяснилось, что в 35,8% из них были случаи утечки информации, связанные с промышленным шпионажем. Основными выявленными методами недобросовестной конкуренции являлись: копирование конфиденциальных документов, в том числе электронных баз данных, сотрудниками за денежное вознаграждение от конкурентов; получение информации через сотрудников, приглашенных работать по совместительству в конкурирующие компании (например, в выходные); через партнеров – поставщиков оборудования.

В качестве примера можно привести факт осуждения двух бывших сотрудников одной из крупных японских компаний. Они были признаны виновными в том, что передали фирме КНР чертежи, представляющие коммерческую тайну. Воришек приговорили к двум годам лишения свободы и штрафу по 13 тыс. долл.

Примерно такая же ситуация наблюдается и в других передовых европейских и азиатских странах.

По данным одной из российских консалтинговых фирм, примерно в 90 из 100 обследованных отечественных компаний и фирм были случаи кражи информации. При этом лишь 5% их руководителей решились подключить к расследованию правоохранительные органы.

Объяснением этому служит то, что обнаруженные факты «промышленного шпионажа» в российских условиях получают огласку только в крайних случаях. Злоумышленникам нет резона обнародовать свои подвиги, а потерпевшей стороне не хочется подрывать свою репутацию. В большинстве фирм интеллектуальная собственность не защищена патентами, свидетельствами, не введен режим коммерческой тайны. Существуют и определенные трудности и противоречия при уголовном преследовании коммерческих шпионов.

1.2. ПОНЯТИЕ И СУЩНОСТЬ КОММЕРЧЕСКОГО ШПИОНАЖА

В предпринимательской деятельности существенную роль играет информация, влияющая на принятие необходимых оперативных решений. Большое значение имеет научно-техническая информация, которая содержит новые научные знания, сведения об изобретениях, технических новинках собственной фирмы и фирм-конкурентов.

Можно разделить информацию на два блока: коммерческую информацию и промышленную информацию.

Что касается промышленной информации, то сюда относится сведения о технологиях и способах производства, технические новинки, «ноу-хау», конструкторская документация и т.д. Если говорить о коммерческой информации, то это бухгалтерская отчетность предприятия, сведения о кредитах и банковских операциях, о заключаемых договорах

и контрагентах, структуре капиталов и планах инвестиций, стратегических планах маркетинга, анализе конкурентоспособности собственной продукции, клиентах, планах производственного развития, деловой переписке и пр. Такая информация имеет различное влияние на предприятие и, как следствие, ее разглашение может привести к ущербам различной степени тяжести. Исходя из вышесказанного, можно классифицировать информацию следующим образом (рисунок 1.1).

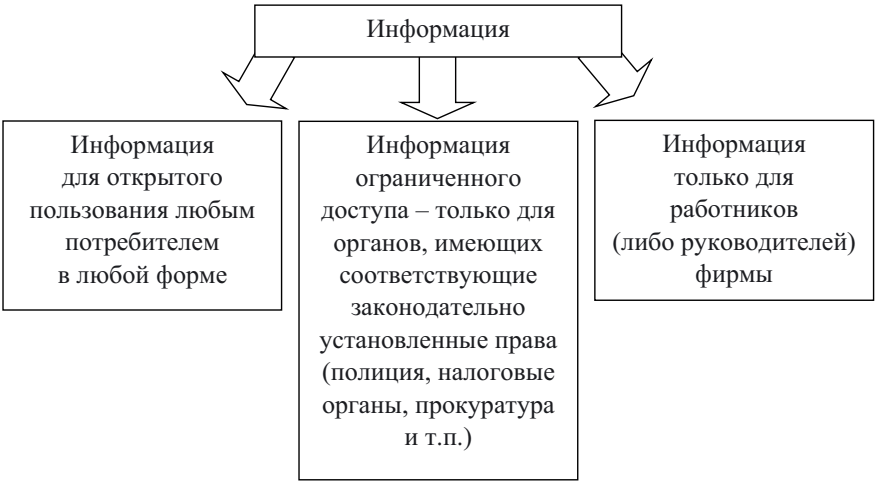

Рисунок 1.1. Классификация информации

В отношении информации, которая относится ко второй и третьей группам, применяется термин «конфиденциальность» (от лат. *confidentia* – доверие). Согласно пункту 7 статьи 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» конфиденциальность информации определяется как «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя». Указом Президента РФ от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера» установлен перечень сведений, отнесенных к конфиденциальной информации:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность

(персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

7) сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 года № 229-ФЗ «Об исполнительном производстве».

Для хозяйствующего субъекта утечка конфиденциальной информации (коммерческой тайны) может грозить фатальными последствиями, такими как банкротство. Исследования показывают, что при потере хотя бы 20% конфиденциальной информации, банкротство наступает в 60 случаях из 100. По статистике, 93% организаций, которые подверглись рассекречиванию конфиденциальной информации путем потери к ней доступа более чем на 10 дней, сразу заявляли о своей несостоятельности. Из этого следует вывод, что конфиденциальная информация хозяйствующих субъектов является объектом пристального внимания конкурентов и заинтересованных в ее разглашении лиц.

В общем случае сложившиеся к настоящему времени виды тайн классифицируются в основном *по характеру, содержанию относимых к ним сведений.*

К государственной тайне относятся сведения, затрагивающие коренные интересы обеспечения суверенитета государства – его обороноспособности и безопасности.

К коммерческой тайне – интересы субъекта предпринимательской деятельности, обеспечивающие его успешную работу на рынке в целях извлечения прибыли.

К процессуальным тайнам – сведения, необходимые для реализации задач соответствующей процессуальной деятельности.

Профессиональные тайны в основном защищают личную тайну клиентов, обратившихся за услугой, либо сведения, которые они полагают своей коммерческой тайной.

Помимо этого, тайны можно классифицировать *по числу субъектов, которые обладают теми или иными сведениями и от которых они скрываются*. Для личной тайны обладателем сведений, естественно, является один индивид и скрываются они ото всех остальных. Для подавляющего большинства остальных систем ограничений – группа индивидов, и сведения скрываются от всех, кто не имеет полномочий для ознакомления с ними. А для такой системы как тайна усыновления (удочерения) круг субъектов, ознакомленных с данным фактом, может быть не ограничен, но все они должны быть обязаны не сообщать данный факт приемному ребенку без разрешения приемных родителей.

Если говорить о классификации *по принципу первичности и вторичности систем ограничений в доступе к информации*, то следует исходить из предназначения самих сведений. К первичным следует отнести личную тайну индивида (персональные данные), коммерческую (тайна лица, занимающегося предпринимательской деятельностью) и государственную, обеспечивающую внешнюю безопасность страны. Все остальные системы являются производными, в конечном итоге защищая одну из этих категорий информации.

В системе правового регулирования тайна предстает прежде всего как правовой институт, причем имеющий свою внутреннюю структуру[1].

[1] Беловицкий К.Б. Режим коммерческой тайны в системе обеспечения экономической безопасности хозяйствующего субъекта: учебное пособие. – М.: Научный консультант, 2017. – 124 с.

Ценность представляет не только информация, но и ее неизвестность третьим лицам.

Ограниченная распространенность информации позволяет ее обладателю увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Экономической сущностью коммерческого шпионажа является экономия средств за счет использования информации конкурента, возможность увеличить доходы, избежать расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Еще одним из признаков коммерческого шпионажа является противоправность получения информации. То есть ограничения на использование и защита такой информации прямо указаны в законодательстве.

В настоящее время законодательно не определено понятие «промышленный», «корпоративный» или «коммерческий шпионаж».

Промышленный шпионаж (также экономический или корпоративный шпионаж) – форма недобросовестной конкуренции, при которой осуществляется незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну с целью получения преимуществ при осуществлении предпринимательской деятельности, а равно получения материальной выгоды[2].

Интерпол дает такое понятие промышленного шпионажа: «...это приобретение любым обманным путем интеллектуальной собственности, которая принадлежит любому юридическому лицу, и которая была создана или законно приобретена этим юридическим лицом с целью производства, что имеет или может иметь промышленную ценность...»

Согласно статье 50 ГК РФ все юридические лица разделены на организации, преследующие извлечение прибыли в качестве основной цели своей деятельности (коммерческие организации) либо не имеющие извлечение прибыли в качестве такой цели и не распределяющие полученную прибыль между участниками (некоммерческие организации).

---

[2] Промышленный шпионаж [Электронный ресурс] // Википедия. – Режим доступа: https://ru.wikipedia.org/wiki/Промышленный_шпионаж.

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» к информации, составляющей коммерческую тайну, относит сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

В связи с изложенным, в дальнейшем будем употреблять термин «коммерческий шпионаж».

Коммерческий шпионаж[3] – противоправное собирание, похищение, передача, хранение в целях передачи, чужой информации, а также неправомерный доступ к компьютерной информации с целью получения преимуществ для себя или третьих лиц при осуществлении предпринимательской деятельности, нанесения ущерба собственнику, а равно получения материальной или иной выгоды.

Предметом коммерческого шпионажа является информация, составляющая коммерческую ценность в силу неизвестности её третьим лицам, к которой у третьих лиц нет свободного доступа на законном основании.

Собирание предполагает любой способ получения информации, через преодоление принятых ее обладателем мер по охране конфиденциальности этой информации.

Похищение – это тайное, противоправное, безвозмездное изъятие чужой информации.

Передача означает сообщение, распространение, воспроизведение сведений любым способом.

Хранение сведений представляет собой ограниченное по времени обладание такими сведениями, при этом важно, чтобы они хранились для последующей передачи.

Действующее уголовное законодательство России не предусматривает ответственности за коммерческий шпионаж, что существенно затрудняет уголовное преследование злоумышленников.

[3] Разработано автором.

Может быть, поэтому в последнее время это явление стало достаточно распространенным.

Для того чтобы понять, как с коммерческим шпионажем бороться, необходимо проанализировать некоторые законодательные акты, сложившуюся практику и применяемые при коммерческом шпионаже методы добывания информации.

Классифицировать методы коммерческого шпионажа можно по различным основаниям. Получение информации может осуществляться непосредственно разведчиком или опосредованно. Применение тех или иных средств защиты зависит от носителя информации, которую намеревается получить субъект. Один вид информации может быть похищен, другой прослушан, третий – сфотографирован (или сделаны зарисовки), четвертый записан на диктофон, пятый – снят на видеокамеру и т.д. Иногда используется комплекс специальных мер по ее получению. В зависимости от источника получения информации принимаются соответствующие меры защиты.

Носители необходимой коммерческой информации находятся в открытом или закрытом доступе.

Основными каналами утечки информации являются:

1. Открытые источники.
2. Физические лица – носители информации.
3. Технические средства.
4. ЭВМ.
5. Непосредственное наблюдение.

Получение информации из открытых источников в чистом виде не относится к коммерческому шпионажу, но осветить этот канал ввиду его значимости автор считает необходимым.

Контрольные вопросы

1. Понятие шпионажа.
2. Отличие шпионажа от бизнеса разведки.
3. Организационная структура коммерческой контрразведки.

Темы докладов и рефератов

1. Коммерческий шпионаж до нашей эры.
2. Коммерческий шпионаж до XIX века.