
Маргарита Акулич
Промышленный шпионаж

Маргарита Акулич

Промышленный шпионаж

«Издательские решения»

Акулич М.

Промышленный шпионаж / М. Акулич — «Издательские решения»,

ISBN 978-5-44-906165-2

Книга, вероятно, будет интересна, прежде всего, маркетологам, менеджерам, юристам, специалистам в области ИТ и экономистам-международникам. В ней даны основные понятия, касающиеся промышленного шпионажа, приведен ряд примеров компаний и стран, а также раскрыты вопросы, имеющие отношение к промышленному шпионажу и защите от него.

ISBN 978-5-44-906165-2

Содержание

Промышленный шпионаж

Маргарита Акулич

ISBN 978-5-4490-6165-2
Создано в интеллектуальной издательской системе Ridero

Предисловие

Книга, вероятно, будет интересна, прежде всего, маркетологам, менеджерам, юристам, специалистам в области ИТ и экономистам-международникам. В ней даны основные понятия, касающиеся промышленного шпионажа, приведен ряд примеров компаний и стран, а также раскрыты следующие вопросы:

Компьютеры и Интернет. Деяния злоумышленников, угроза, вредоносные программы.

Социальная инженерия.

О шокирующих причинах хищения интеллектуальной собственности и корпоративного моджо.

Положение об общей защите данных Европейского союза.

Пути защиты интеллектуальной собственности и коммерческой тайны.

I Основные понятия, касающиеся промышленного шпионажа

1.1 Суть промышленного шпионажа. О происхождении промышленного шпионажа

Суть промышленного шпионажа

> «Потеря промышленной информации и интеллектуальной собственности посредством киберпреступления представляет собой величайшую вынужденную передачу богатства в истории» (генерал Кит Александр, бывший командующий военным кибер-командованием, в 2013 году состоял в Сенатском комитете США по вооруженным силам).

Промышленный шпионаж (Industrial espionage), называемый еще экономическим шпионажем, корпоративным шпионажем – это форма шпионажа, проводимая в коммерческих целях вместо преследования целей чисто национальной безопасности.

Представляется, что реализация экономического шпионажа или его организация осуществляется правительствами и имеет международный характер, а промышленный или корпоративный шпионаж чаще всего является национальным и происходит между компаниями или корпорациями. Хотя название здесь не играет решающей роли, любой шпионаж, преследующий экономические цели, можно назвать промышленным.

Промышленный шпионаж является скрытой, а иногда и незаконной практикой расследования конкурентов, чтобы получить преимущество в бизнесе. Цель расследования бывает коммерческой тайной, это может быть спецификация или формула проприетарного продукта, или информация о бизнес-планах. Во многих случаях промышленные шпионы просто ищут любые данные, которые их организация (или страна) может использовать в своих интересах.

Экономический шпионаж, иногда называемый промышленным шпионажем, – это, в частности, хищение интеллектуальной собственности, ноу-хау или коммерческой тайны компании.

Промышленный шпион может представлять собой угрозу для инсайдеров. Им например, может быть лицо, которое нанялось на работу в компании с целью шпионажа или недовольный

сотрудник, торгующий информацией ради личной выгоды либо мести. Шпионы могут также использовать тактику социальной инженерии, например, обманывая сотрудника, чтобы разглашать привилегированную информацию.

Шпионы иногда физически расследуют помещение. В этом случае шпион может обыскивать корзины отходов или копировать файлы, или жесткие диски компьютеров, находящихся без присмотра.

Все чаще вторжение происходит через корпоративную сеть. Как правило, целенаправленная атака проводится для получения первоначального доступа к сети, а затем для постоянной кражи данных выполняется расширенная постоянная угроза (APT). Способность сотовых телефонов записывать и передавать информацию может также эксплуатироваться. Телефон иногда оставляют в зале заседаний, например, и контролируют встречу удаленно. Устройства записи также секретируются во множестве предметов, включая очки, ручки и USB-накопители.

О происхождении промышленного шпионажа

Чайник с актрисами, Фабрика фарфора Vezzi, Венеция, с. 1725. Братья Вецци были вовлечены в серию инцидентов промышленного шпионажа. Именно эти действия привели к тому, что секрет производства фарфора Meissen стал широко известен [1]

Работа отца Франсуа Ксавье д'Антреколла, проделанная, чтобы показать Европе методы производства китайского фарфора в 1712 году, часто считается ранним случаем промышленного шпионажа.

Способы манипулирования человеком известны достаточно давно, в основном они пришли в социальную инженерию из арсенала различных спецслужб. Первый известный случай конкурентной разведки относится к VI веку до нашей эры, и он произошел в Китае, когда китайцы лишились секрета изготовления шелка, обманным путем выкранного римскими шпионами.

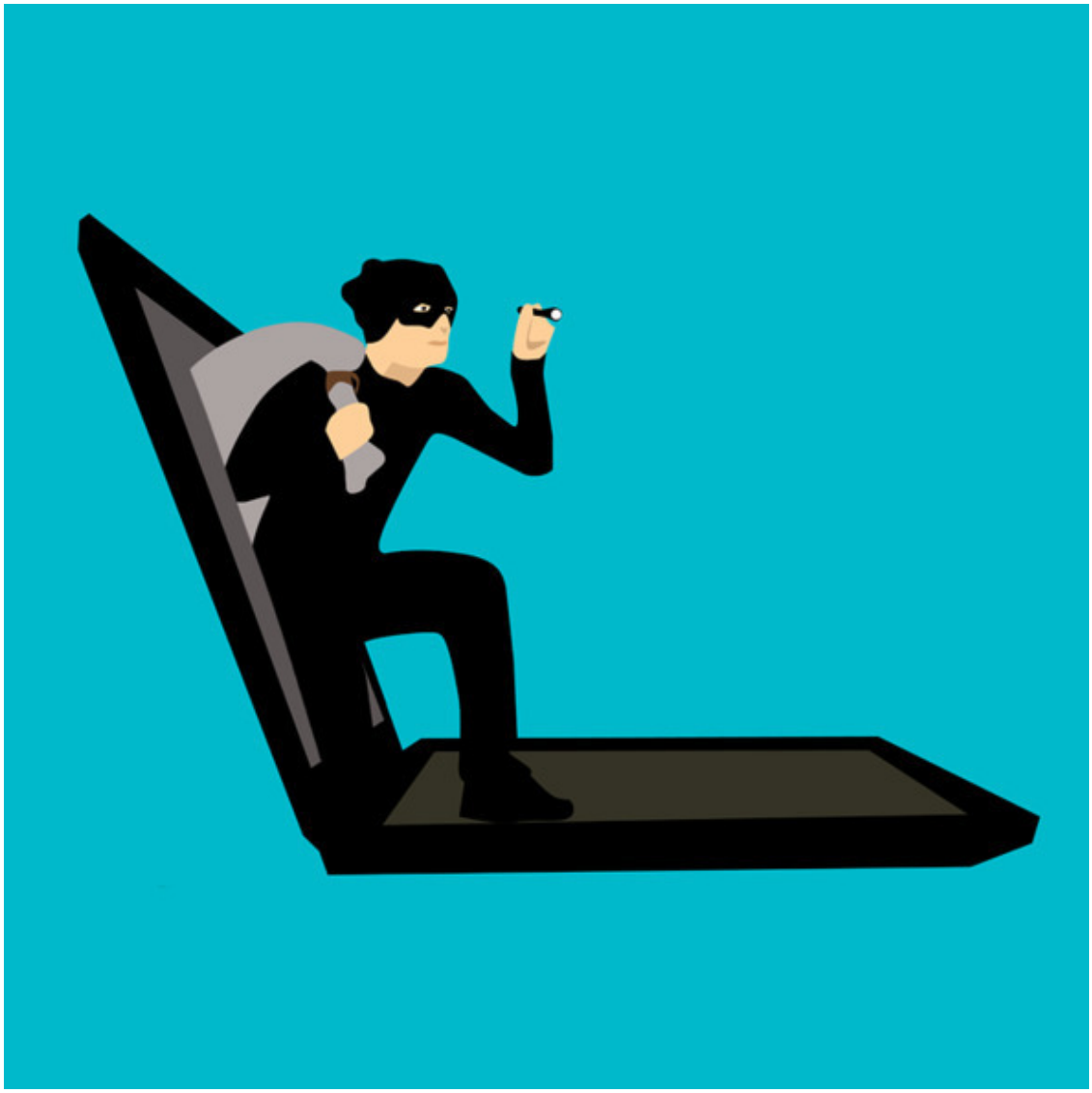
Были написаны исторические отчеты о промышленном шпионаже между Великобританией и Францией. В связи с появлением в Британии «промышленного кредитора» во втором десятилетии 18-го века появилось крупномасштабное мероприятие, спонсируемое государством, чтобы тайно взять британские промышленные технологии во Францию. Свидетели подтвердили факты шпионской деятельности как торговцев за границей, так и размещенных в Англии учеников.

Протесты таких людей, как работники железных дорог в Шеффилде и сталеваров в Ньюкасле из-за привлечения квалифицированных промышленных рабочих за границу, привело

к первому английскому законодательству, направленному на предотвращение использования метода экономического (промышленного) шпионажа.

1.2 Конкурентная разведка и экономический (или промышленный) шпионаж. Формы промышленного шпионажа

Конкурентная разведка и экономический (или промышленный) шпионаж



Значительный объем данных о том, что делают конкуренты, поступает из рутинных и нетрадиционных источников. Например, в некоторых крупных розничных сетях используются агенты для проверки цен и продуктов конкурентов путем сравнительного шопинга. Не менее плодотворными являются регулярные линии коммуникации, такие как отчеты продавцов, торговые журналы, информационные бюллетени, бизнес-соглашения, ярмарки и экспонаты, а также контакты с поставщиками. Анализ продуктов конкурентов является еще одним источником важной коммерческой разведки.

Фактические коммерческие тайны могут проникнуть на открытый рынок по нескольким каналам. Нелояльный сотрудник, к примеру, может украдкой искать конкурентов и продавать им конфиденциальные данные по высокой цене.

Более распространенным методом является групповой заговор: несколько сотрудников, как правило, техников и других высокого управленческого калибра, оставляют компанию и создают конкурирующую фирму, спекулируя на откровенности, полученной ими во время их работы в организации своего бывшего работодателя. Вариант этой практики возникает, когда конкурент заманивает ценного сотрудника предложением о большем количестве денег и льгот в надежде, что пиратский работник сделает свой магазин секретов доступным для своего нового работодателя.

Работодатель, обнаруживший, что его коммерческая тайна применяется конкурентом, обычно принимает юридические меры для предотвращения дальнейшего вторжения в его коммерческую тайну. Штрафы против компаний, признанных виновными в узурпации коммерческой тайны, могут служить в качестве судебного запрета на дальнейшее использование знаний, учета и всех прибылей, полученных от использования похищенной информации. Могут иметь место и дополнительные штрафные убытки, если нарушение прав компании было вопиющим.

«Конкурентный интеллект» описывает правовую и этическую деятельность по систематическому сбору и анализу информации о промышленных конкурентах, ее управлению. Он может включать такие мероприятия, как рассмотрение газетных статей, корпоративных публикаций, вебсайтов, патентных заявок, специализированных баз данных, информации на торговых выставках и т. п.

Компиляция этих важнейших элементов иногда называется CIS или CRS, – решением конкурентной разведки или решением конкурентного реагирования. Основываясь на исследованиях рынка, «конкурентная разведка» была описана как «применение принципов и практики из военной и национальной разведки в сфере глобального бизнеса»; это бизнес-эквивалент разведки с открытым исходным кодом.

Разница между конкурентной разведкой и экономическим или промышленным шпионажем не ясна; нужно понять правовые основы, чтобы иметь представление, как провести линию между ними. Другие утверждают, что иногда бывает проблематичным выявление разницы между юридически допустимыми и незаконными методами, в особенности если принимать во внимание этическую сторону сбора информации, что делает определение еще более неуловимым.

Формы экономического и промышленного шпионажа [1]

Экономический или промышленный шпионаж имеет место в нескольких формах.

Целью шпионажа является сбор знаний об организации. Шпионаж может включать информацию о приобретении интеллектуальной собственности, о промышленном производстве, идеи, методы и процессы, рецепты и формулы. Или он может включать в себя секвестирование собственной либо операционной информации, скажем, информации о наборах данных клиентов, данных по ценообразованию, продажам, данных по исследованиям и разработкам, политике, перспективным заявкам, стратегиям планирования, или маркетингу, или изменяющимся составам и местам производства. Он может охватывать такие виды деятельности, как кража коммерческой тайны, взяточничество, шантаж, технологический надзор.

Помимо организации шпионажа в коммерческих организациях, правительства также могут иметь целевые задачи – например, определение условий тендера на правительственный контракт.

1.3 Целевые отрасли. Кража информации и саботаж

Целевые отрасли [1]

Во время тестирования автопроизводители обычно маскируют предстоящие модели автомобилей рисунками, сделанными с помощью камуфляжной краски, предназначенными для обфускации линий автомобиля. Также часто используются мягкие чехлы или обманчивые надписи. Это также должно помешать Motoring Media-выходам испортить большой показ модели.

Экономический или промышленный шпионаж чаще всего связан с высокотехнологичными отраслями промышленности, включая компьютерное программное обеспечение и аппаратное обеспечение, биотехнологию, аэрокосмическую промышленность, телекоммуникации, транспорт и двигательную технику, автомобили, станки, энергию, материалы и покрытия и т. д.

Известно, что Силиконовая долина является одной из самых целевых областей в мире для шпионажа, впрочем, любая отрасль с информацией о конкурентах может стать целью.

Кража информации и саботаж [1]

Информация может обеспечивать и успех, и неудачу; если коммерческая тайна украдена, конкурентное игровое поле может оказаться выровненным или даже опрокинутым в пользу конкурента.

Несмотря на то, что большая часть сбора информации осуществляется юридически дозволенным образом (посредством конкурентной разведки), корпорации иногда считают, что лучший способ получить информацию – это забрать ее. Экономический или промышленный шпионаж представляет собой угрозу для любого бизнеса, средства к существованию которого зависят от информации.

Можно с уверенностью констатировать, что в последние годы экономический или промышленный шпионаж принял расширенное определение. К примеру, попытки саботировать корпорацию можно считать промышленным шпионажем; в этом смысле данный термин принимает более широкие коннотации его родительского слова.

То, что шпионаж и саботаж (корпоративный или иной) стали более четко связанными друг с другом, также подтверждается рядом профильных исследований, как правительственных, так и корпоративных.

В настоящее время правительство США проводит полиграфическое обследование под названием «Испытание шпионажа и саботажа» (TES), способствующее распространению все более популярного, хотя и не консенсусного мнения тех, кто изучает контрмеры в отношении

шпионажа и саботажа, и взаимосвязи между ними. На практике это особенно касается «доверенных инсайдеров». Они обычно считаются функционально идентичными и используются с целью получения информации для обеспечения контрмер.

1.4 Агенты и процесс сбора информации. Эффективность промышленного шпионажа

Агенты и процесс сбора информации

Промышленный или экономический шпионаж чаще всего обеспечивается одним из двух способов. *Во-первых,* когда недовольным сотрудником присваивается информация в целях продвижения чьих-то интересов либо нанесения ущерба компании. *Во-вторых*, когда конкурент или иностранное правительство ищет информацию ради продвижения своих технологи-

ческих либо финансовых интересов. «Родинки» или доверенные инсайдеры обычно считаются наилучшими источниками шпионажа (промышленного или экономического).

Исторически известный как «patsy», инсайдер может быть вызван с его согласия или под принуждением ради предоставления информации. Первоначально можно попросить передать пассивную информацию, и как только она скомпрометирована из-за совершения преступления, обеспечить передачу более чувствительных материалов. Лица могут оставить одну компанию для работы в другой и получения конфиденциальной информации. Такое явное поведение было в центре внимания многочисленных случаев промышленного шпионажа, приведших к юридическим баталиям.

Некоторые страны нанимают для шпионажа людей, не используя свои разведывательные службы. Академики, бизнес-делегаты и студенты считаются часто используемыми правительствами для сбора информации.

Некоторые из стран, например Япония, как сообщается, ожидают, что ученики будут проинформированы о возвращении домой. Шпион может последовать за экскурсией по фабрике, а затем «потеряться». Шпионом может оказаться инженер, обслуживающий человек, уборщик, инспектор либо страховой агент, одним словом любой, у кого имеется законный доступ к помещениям.

Шпион может ворваться в помещение, чтобы украсть данные, он может осуществлять поиск в макулатуре и мусоре, это известно как «дайверское погружение». Информация может быть скомпрометирована с помощью запросов информации, маркетинговых исследований или использования технической поддержки, или исследований, или программных средств. Аутсорсинговые промышленные производители могут запрашивать информацию вне согласованного контракта.

Компьютеры способствовали сбору информации из-за простоты доступа к солидным объемам информации посредством физического контакта или Интернета.

Эффективность промышленного шпионажа [3]

Фото из источника в списке литературы [3]

Промышленный шпионаж более эффективен, чем R & D (НИОКР).

Исследование: Эрик Мейерсон, профессор Стокгольмской школы экономики объединился с Альбрехтом Глитцем, адъюнкт-профессором Университета Помпеу Фабра для изучения архивов Министерства государственной безопасности Восточной Германии.

Исследователи проанализировали 189 725 отчетов информаторов и сделали сравнение с экономическими данными промышленного сектора Восточной и Западной Германии с 1969 по 1989 год. В их исследовательском отчете было указано, что Восточная Германия имеет значительную экономическую отдачу от своей государственной промышленной операции по шпионажу. Шпионаж сузил технологические пробелы между двумя странами и был настолько успешным, что обусловил приложение усилий на НИОКР на Востоке.

Рассмотрим вопросы HBR к профессору Мейерсону и его ответы на них, они приведены ниже, они взяты из статьи Industrial Espionage Is More Effective Than R&D (Curt Nickisch) [3].

HBR: «Эффективнее ли корпоративный шпионаж, чем инновации? Действительно ли он оправдывает больше надежд, чем законные программы R & D?»

Конец ознакомительного фрагмента.