ФБК
Grant Thornton

Экономическая безопасность и корпоративный шпионаж

Сентябрь 2021 | Москва

Что такое корпоративный шпионаж

Корпоративный шпионаж – он же экономический шпионаж, он же промышленный шпионаж.

Суть корпоративного шпионажа – исследование деятельности коммерческой организации.

Отличительные признаки корпоративного шпионажа:

- Негласный характер;
- Ведение наблюдения в интересах другой организации;
- Основная цель – получение преимущества в экономической деятельности;
- Осуществляется незаконными методами (в противном случае он превращается в бизнес-разведку).

Что такое корпоративный шпионаж

Economic Espionage Act, 1996 *(принят благодаря делу Kodak)*

Данный документ различает несколько понятий, которые у нас зачастую путают:

1. Экономический шпионаж (§ 1831). Хищение торговых секретов (trade secrets) в пользу иностранного правительства, иностранного представителя или иностранного агента;
2. Хищение торговых секретов (§ 1832). Хищение информации с целью использования торгового секрета, относящегося к товару, предлагаемому на национальном рынке США или в международной торговле, для получения выгоды иным лицом, нежели обладатель такого секрета.

§ 1837. Данные правила применимы к деяниям, совершенным за пределами США, если виновное лицо является гражданином или резидентом США, либо негативные последствия наступили на территории США.

Что такое корпоративный шпионаж

Что же такое «торговый секрет»?

§ 1839 п.3 Торговый секрет – находящаяся в любом виде финансовая, деловая, научная, техническая, экономическая или инженерная информация, включая модели, планы, отчеты, программные коды, формулы, дизайн-проекты, прототипы, методики, технологии, процессы, процедуры, в осязаемой или неосязаемой форме, зафиксированные в электронной форме, в виде чертежей, фотографий, описаний, при условии, что:
А) владелец этой информации принимает разумные меры по ее сохранению в тайне;
Б) информация представляет собой самостоятельную экономическую ценность, реальную или потенциальную, в связи с ее неизвестностью и недоступностью законным путем со стороны третьих лиц.

§ 1839 п.4 Владелец торгового секрета – физическое или юридическое лицо, в правомерном обладании которого находится секрет или право на него.

Что такое корпоративный шпионаж

Ст. 183 УК РФ

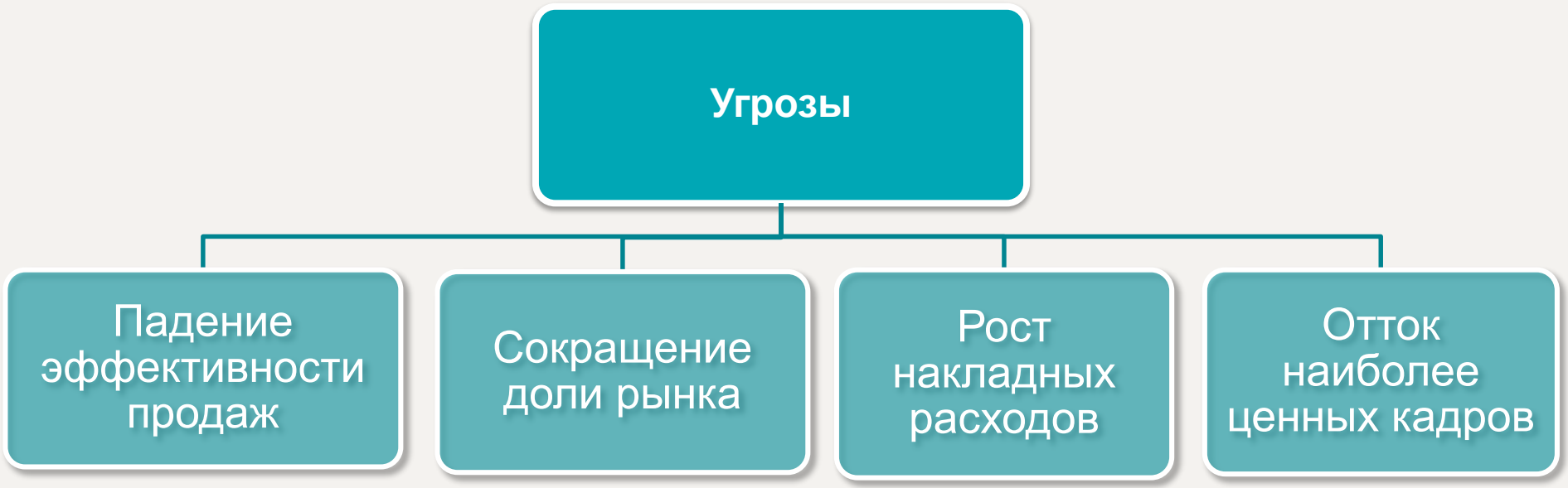
1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну путем похищения документов, обмана, шантажа, принуждения, подкупа или угроз, а равно иным незаконным способом

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

Цели корпоративного шпионажа

Основная цель корпоративного шпионажа – это получение конкурентного преимущества для себя, или устранение имеющегося конкурентного неравенства с другим участником рынка.

Опасность корпоративного шпионажа



Дело компании Gillette (1997)

Gillette

Подряд на разработку производственного оборудования

Wright | Industries
Engineering Success

Производство Mach 3

Steven L. Davis
Инженер-технолог

American Safity Razors Co

Bic

Schick-Wilkinson Sword

Как видно из материалов дела, Дэвис был достаточно амбициозным типом, и его вывел из себя тот факт, что он не был назначен руководителем проекта. Им двигало стремление навредить как своему работодателю, так и Gilette, в силу чего он предложил чертежи машины по сборке лезвий сразу трем конкурентам. Из них только Schick сообщил об этом Gillette, а те связались с ФБР.

Дело компании Kodak (1995)

Harold Worden (стаж работы в компании – 28 лет)

Eastmen Kodak

Приглашение сотрудников Kodak

Г. Уорден увольняется в 1992 г. и создает свою консалтинговую фирму в Южной Каролине.

Г. Уорден работал проектным менеджером на заводе в г. Рочестер. В его компетенцию входило определение патентоспособности изобретения. Технологические процессы, применяемые на заводе, представляли существенный секрет для компании. Поэтому сведения о них были разделены на части, и ни один сотрудник не владел всей полнотой информации, а знал только то, что положено ему для выполнения работы. Однако, благодаря концентрации бывших сотрудников Kodak, а также благодаря неформальным связям с другими работниками, Г. Уорден смог составить три справочника: по химическому составу и производству пленки, по оборудованию для нанесения светочувствительного состава (общая стоимость – 500 млн. долл.), по процедурам контроля качества.
В 1994 г. руководители Konica и Agfa-Gevaert сообщили в ФБР, а также в Kodak, что им поступили предложения продать секреты производства. После этого два детектива, привлеченные Kodak, под видом представителей китайской компании вступили в контакт с Уорденом, который предложил им технологию производства высококачественного ацетата, представлявшему секрет производства. В результате проведенной операции Уорден был арестован ФБР, а потом осужден и приговорен к штрафу 30 тыс. долл. и заключению на 1,5 года. Однако до этого бизнес Уордена процветал. Его клиентом было 3М.

Дело компании Avery Dennison (1999)

Производство клейких материалов

AVERY DENNISON

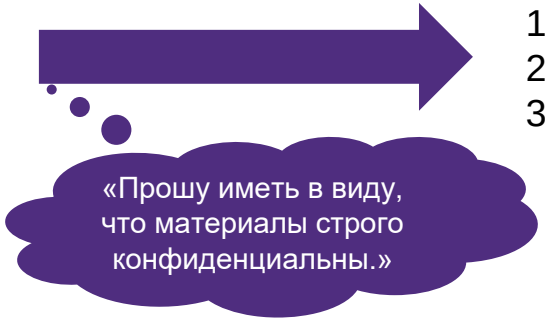
(США)

Victor Lee

FOUR PILLARS ENTERPRISE CO. LTD.

(Тайвань)

Выходец из Тайваня, из бедной семьи. Смог получить образование в Техасском технологическом университет, стал инженером-химиком. В 1986 г. поступил на работу в Avery Dennison. Его должность предполагала доступ к техническим секретам, о сохранении которых он давал подписку.



1. Формулы продуктов;
2. Планы разработок.
3. Семинары для сотрудников.

В 1988 г. одноклассник В. Ли предложил ему выступить с лекцией в тайваньском Industrial Technology Research Institute (ITRI). На лекции присутствовал представитель Four Pillars Enterprises Co, который пригласил Ли прочитать лекцию сотрудникам компании. После этого его пригласил на обед глава Four Pillars Пин Ен Янь (Pin Yen Yang). Ли было предложено 25 тыс. долл. в год за оказание консалтинговых услуг (годовой оклад в Avery Dennison – 45 тыс.). В рамках «консультаций» Ли передал 12 тыс. страниц документов.
На их основе Four Pillars Enterprises Co разработало собственные материалы, которые направляло Ли для испытаний. Испытания делались в лаборатории Avery Dennison. Деньги за информацию выплачивались через его родственников в Тайване.
В 1996 г. один из сотрудников Four Pillars решил начать работу в Avery Dennison. Об этом узнал Янь, и категорически запретил ему переход. Однако к тому времени предложение уже было принято, и внезапный отказ удивил Avery Dennison. В результате расспросов тот обмолвился, что у Four Pillars есть свой человек в компании. За Ли было установлено наблюдение. В 1997 г. ему дали папку с документами о планах продаж в Азии, предупредив об их конфиденциальности. На оперативном видео было зафиксировано, как Ли выносит материалы из своего офиса, предварительно надев перчатки. На основании этой записи Ли был задержан и признался в шпионаже. После этого он согласился провести под контролем ФБР встречу с Янем, который собирался прибыть в США, и который был очень заинтересован узнать про планы Avery Dennison в Азии, а также как устранить сложности в работе оборудования. Во время встречи Янь получил материалы с грифом «Конфиденциально», срезал их ножом и положил в свой портфель. Его задержали в аэропорту.

Дело компании IBM (1983)

Kenji Hayashi,
Старший инженер

Isao Ohnishi,
Менеджер программного дивизиона

IBM 3081 – машина нового поколения

Raymond Cadet, компьютерный специалист IBM

В 80-ые годы японские компании пытались нарушить монополию IBM на рынке компьютеров при этом было понятно, что даже в этом случае японские компьютеры должны работать на программном обеспечении, совместимом с IBM, поскольку это было важно для пользователей.
В 1980 г. Кадет уволился из IBM и перешел на работу в National Advanced Systems (Силиконовая долина). При этом он прихватил с собой с прежнего места работы с десяток тетрадей технической документации для машин поколения 308, над которыми работал. Об этих тетрадях он сообщил своему новому руководителю, Barry Saffaie. National Advanced Systems занималось продажей японских компьютеров в США, и Саффе во время одной из поездок в Токио показал отрывки из этих тетрадей специалистам Hitachi, среди которых был Кензи Хаяси (Kenji Hayashi).

Дело компании IBM (1983)

Через некоторое время Хаяси случайно упомянул о данных по проекту 308 в разговоре с компьютерным консультантом Максвеллом Пейли (Maxwell Paley). Пейли до этого проработал в IBM 20 лет, и немедленно предложил Хаяси свой отчет, который, по его словам, мог составить на основании открытых источников. Но Хаяси не выразил интереса. Впрочем, как он отметил, если у него есть тетради технической документации под определенными номерами (те, которые Кадет не смог вынести), то они бы представляли ценность для «Хитачи». Пейли утверждал, что почувствовал неладное – уж очень велика была осведомленность Хаяси о технической документации по новому компьютеру.

Хотя контракты с «Хитачи» составляли 20 % от доходов Palyn Associates (фирмы Пейли), Пейли все же позвонил своему другу, Бобу Эвансу, вице-президенту IBM по новым разработкам и технологиям. В разговоре он высказал свои опасения относительно очень уж высокой осведомленности японских конкурентов.

Руководитель службы безопасности IBM Ричард Каллахан (Richard A. Callahan) решил начать с проверки факта утечки информации в «Hitachi», для чего решил использовать Пейли. По его указанию Пейли отправил Хаяси сообщение, что у него есть та информация, которая представляет интерес. На встрече с Хаяси в Токио он передал ему рукописный список всех тетрадей технической документации по проекту 308. Он утверждал, что у него имеется возможность получить доступ к этим материалам, но предварительно он просил показать, как именно выглядят те самые тетради, чтобы случайно не ошибиться. И Хаяси действительно показал ему документы, украденные Кадетом. На основании полученных сведений Каллахан решил, что речь действительно идет об украденных материалах.

Дело было решено передать в ФБР, тем более что с этой организацией у IBM существовали давние связи на почве подготовки агентов. По приглашению Пейли в Лас-Вегас прилетел Хаяси, которому был представлен Каллахан в качестве «человека со связями». Каллахан, в свою очередь, познакомил Хаяси с Аланом Гарретсоном, «человеком из IBM», который на самом деле был агентом ФБР. В ходе бесед, которые были записаны на пленку, японцы подтвердили, что осознают противоправный характер своей деятельности, но все равно желают приобрести нужные материалы.

Для того, чтобы как можно больше втянуть «Hitachi» в оперативную комбинацию, Каллахан и Гарретсон убеждали руководство IBM предоставить японцам еще больше материалов. Всего им было передано документов и образцов на 600 тыс. долл.

Однако в ФБР стремились «подтянуть» к делу высший менеджмент «Hitachi». Поэтому Каллахан и Гарретсон сообщили представителям «Hitachi» о том, что у них имеется возможность получить ключевые данные по новому компьютеру (программное обеспечение, аппаратная часть и пр.), которые могут предоставить сотрудники IBM, собирающиеся в отставку, но сейчас занимающие высшие посты в руководстве. Но, якобы в силу своего положения, они были готовы встречаться только с теми представителями «Hitachi», которые занимают сопоставимые должности. И тогда Хаяси пригласил на очередную встречу Кисабуро Наказаву (Kisaburo Nakazawa), директора фабрики по производству компьютеров. Во время встречи Каллахан даже просил нарисовать органиграмму «Hitachi», чтобы лучше понимать, кто был вовлечен. Наказава заверил Каллахана, что лично скопирует все документы с отметкой «IBM. Конфиденциально» и будет хранить их у себя в сейфе. Кассету с компьютерными данными должен был вывезти в Японию Айсао Охниши. С ними он и был задержан в аэропорту.

Дело Apple (2010)

Сведения о производственных планах Apple

Пол Девин, менеджер отдела международных поставок

Выгодные условия поставок

Поставщики комплектующих из Кореи и Сингапура

Пол Девин занимал в корпорации пост менеджера международных поставок, работая с 2005 г. В 2007 г. он установил связь с представителями компаний из Сингапура и Южной Кореи, которые поставляли необходимые комплектующие. В рамках этого соглашения он предоставлял им сведения о производственных планах, ценовых ориентирах, других поставщиках, ценовых предложениях от иных компаний. Это позволяло поставщикам выстраивать на переговорах с Apple более сильную позицию и получать дополнительные средства. Часть из них «откатывалась» Девину. Общая сумма откатов составила чуть меньше 1 млн. долл. Деньги выплачивались в корейский банк на счет фиктивной компании CPK Engineering. Его годовой оклад составлял около 600 тыс. долл.
Девин был арестован в 2010 г. Основанием для ареста стало обнаружение на его рабочем ноутбуке кеша of Hotmail и Gmail – продукции Microsoft. В результате удалось вскрыть его переписку с «партнерами».

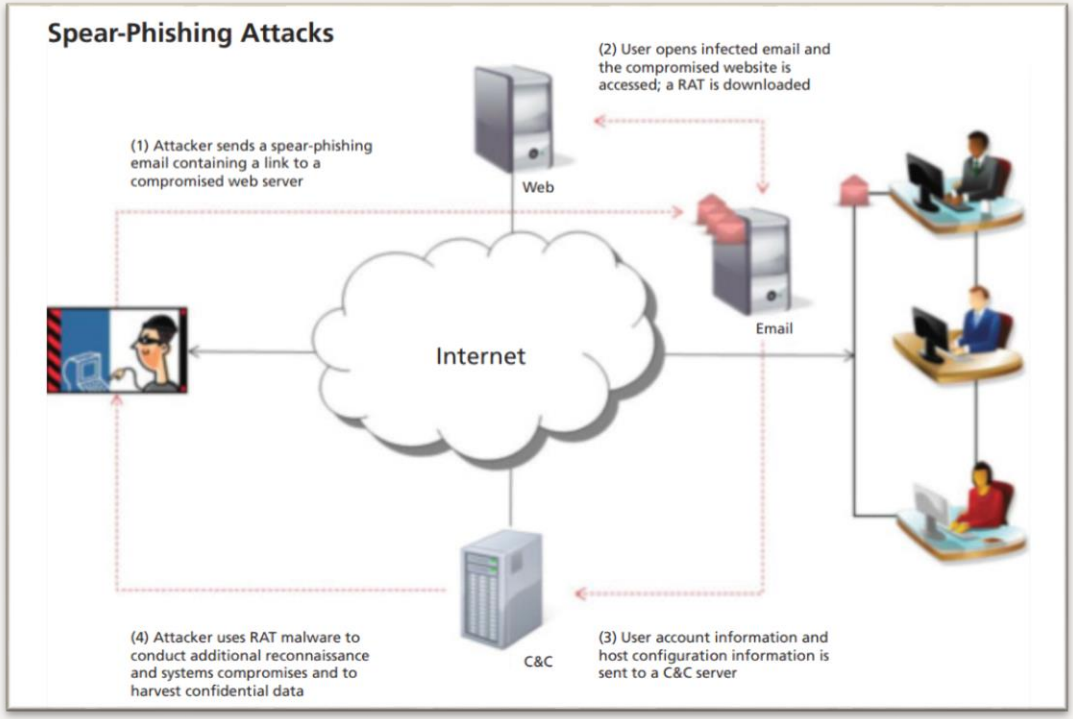
Операция «Ночной дракон» (2006-2010 г.)

Об операции известно на основании доклада компании McAfee. В соответствии с данными, атаки происходили по следующему алгоритму:

1. Проникновение на сервер «экстранета» с помощью SQL-инъекции.
2. Через пораженный сервер загружаются вредоносные программы, позволяющие проникать в «интранет» и подключаться к отдельным компьютерам.
3. На пораженные компьютеры внедряется вредоносное ПО, позволяющее осуществлять хищение паролей и кодов доступа.
4. Используя уязвимости браузера Internet Explorer, сервер «экстранета» подключался к наиболее важным компьютерам и обеспечивал их прямой выход в Интернет.
5. Через установленную связь на пораженные компьютеры загружалась программа удаленного доступа (RAT), через которую и происходила выгрузка существенной информации.

Атака шла через арендованное серверное пространство на серверах США, а также через серверы в Нидерландах. Их целью были энергетические, нефтедобывающие и нефтехимические компании. Объекты атак располагались в Греции, Тайване, Казахстане и США.

Операция «Ночной дракон» (2006-2010 г.)



По оценкам специалистов McAfee, источник атак находился в г. Хэцзе провинции Шандунь. Инициатор атак определен как фирма, предоставляющая услуги по аренде серверного пространства. Атаки происходили в период с 9:00 до 17:00 по Пекинскому времени. Для перехвата паролей использовались программы Hookmsgina и WinlogonHack, разработанные и широко применяемые в Китае. Как отмечалось агентством Reuters, злоумышленники смогли взломать компьютерные системы пяти транснациональных нефтегазовых компаний, и получили доступ к планам торгов и другой важной информации, являющейся собственностью компаний.

Российские реалии

РОСГОССТРАХ

В департамент экономической и информационной безопасности начали поступать сообщения о том, что страховым брокерам кто-то предлагает страховым брокекрам базу данных по каско и ОСАГО клиентов Росгосстраха.

Во взаимодействии с МВД сотрудники СБ вышли на анонимного продавца с предложением приобрести базу на 34 тыс. клиентов с указанием номеров их телефонов, моделей принадлежащих им машин, а также размер страховых премий и номера страховых полюсов

При передаче денег был задержан специалист отдела телефонных продаж "Росгосстрах-Столицы", гражданин Молдавии Иван Швага

И. Швага полностью признал свою вину. В ходе следствия выяснилось, что доступа к базе данных он не имел, и получил ее от своих коллег, «введя их в заблуждение».

Российские реалии

Транснефть
АО «Транснефть - Диаскан»

Конструкторская документация и
и программные алгоритмы устройства, позволяющие проводить эффективную внутритрубную диагностику для обнаружения дефектов, в том числе и незаконных врезок (стоимость разработки – 2 млрд.)

Сергей Зубин, главный инженер, Заместитель директора

Предприятие, созданное после увольнения

Через это предприятие проводился поиск покупателей на документацию, причем предлагалась она за 400 млн.

С. Зубин унес секретную документацию с собой во время увольнения из компании. Сначала он попытался продолжить разработки самостоятельно, но уперся в отсутствие средств. Тогда было решено продать часть документов. Поиск покупателей велся в том числе и через интернет. Поступило предложение и предпринимателю, знакомому с С. Зубиным. Тот сообщил об этом в СБ «Транснефти». После этого Зубин был задержан ФСБ при попытке передачи информации.

Как выявить и подавить корпоративный шпионаж

Основный инструменты корпоративного шпионажа

- Финансовые затруднения сотрудника
- Неприязненное отношение к компании
- Легкомысленное отношение к обязанностям
- Стороннее воздействие (шантаж, дружба, привязанность)

- Использование микрофонов (в том числе направленных) и закладок
- Подключение к коммуникациям (в том числе отопление, водоснабжение и пр.)
- Съем информации с твердых поверхностей (окна, стены)
- Подключение к линиям связи (проводным и беспроводным)

- Несанкционированное копирование
- Несанкционированное прочтение (в том числе, с применением спецсредств для просвечивания конвертов)
- Хищение документов

- Получение скриншотов
- Хищение паролей
- Получение несанкционированного доступа к информации
- Хищение носителей электронной информации

Как выявить и подавить корпоративный шпионаж

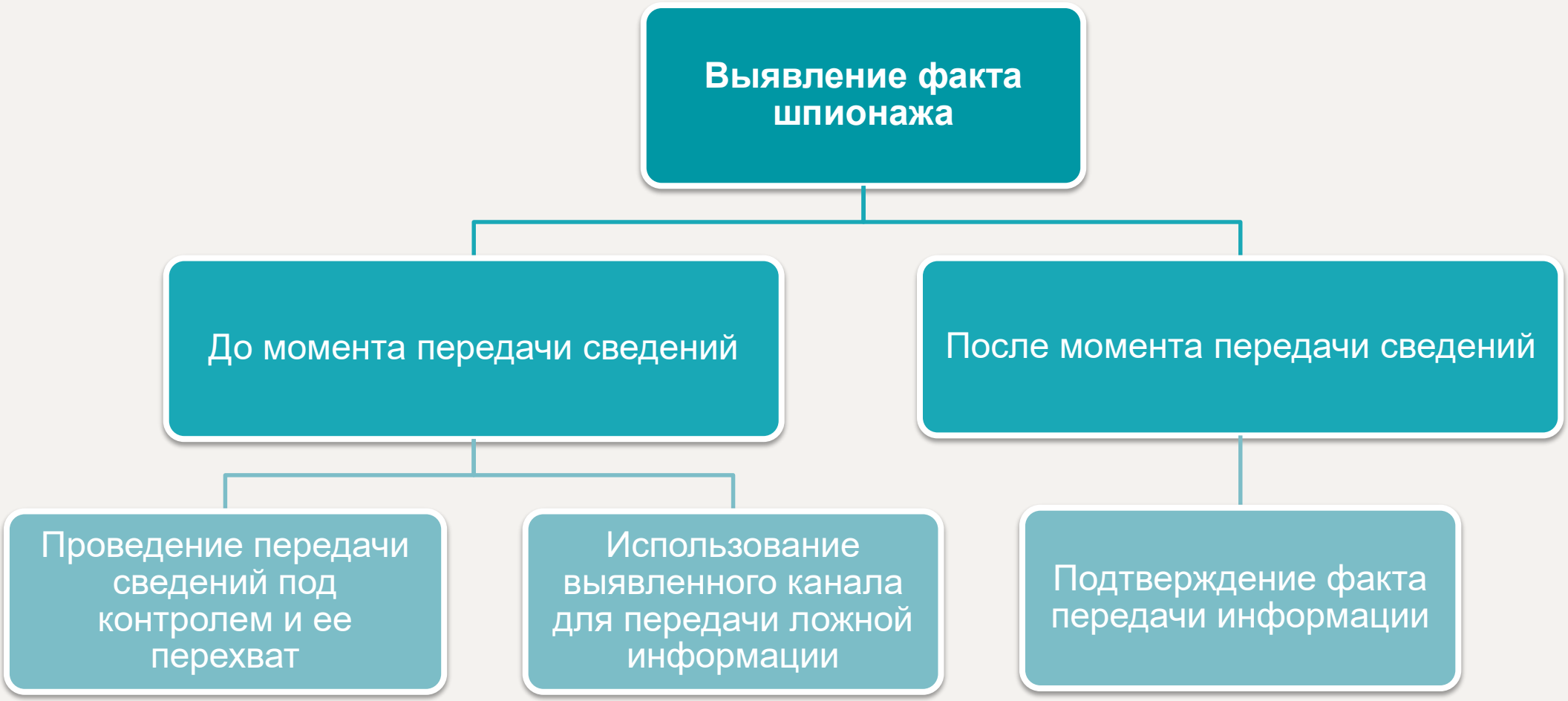
Подавление корпоративного шпионажа

- Определение существенной информации
- Строгое разграничение доступа к существенной информации
- Маскировка существенной информации под несущественную
- Контроль за сотрудниками (включая тестирование)
- Периодическая проверка помещений на предмет спецаппаратуры
- Периодическая проверка электронного пространства

Как выявить и подавить корпоративный шпионаж

Выявление корпоративного шпионажа

Расследование корпоративного шпионажа



Расследование корпоративного шпионажа

Что необходимо доказать

- Защищаемый статус информации (принятие должных мер к неразглашению)
- Наличие защищаемой информации у сторонних субъектов, к которым она не могла попасть правомерно или в силу стечения обстоятельств
- Доступ виновного лица к защищаемой информации (в том числе, санкционированный)
- Осознание виновным недопустимости предоставления защищаемых сведений
- Совершение виновным лицом действий, направленных на предоставление защищаемой информации неуполномоченным лицам
- Причинение ущерба в связи с утечкой защищаемой информации

ФБК Grant Thornton

Компания ФБК Grant Thornton — это уникальная команда профессионалов с безукоризненной деловой репутацией, которой удалось завоевать устойчивое доверие клиентов и стать ведущей российской аудиторско-консалтинговой группой

Компания оказывает широкий спектр услуг в сфере аудита, налогов и права, оценки, консалтинга. В состав группы ФБК Grant Thornton, кроме аудиторских и консалтинговых практик, также входят юридическая фирма **FBK Legal** и **FBK CyberSecurity**

с 1990

30 лет лидерства
в аудите и консалтинге

Grant Thornton International Ltd

членство в одной из крупнейших мировых аудиторско-консалтинговых сетей

Ведущие позиции в рейтингах RAEX в течение всего периода их составления

№ 6

в списке крупнейших аудиторских организаций России и крупнейших аудиторских групп и сетей

№ 1

в категориях «Аудит банков» и «Аудит лизинговых компаний»

ТОП-3 в ключевых номинациях

- Финансовый консалтинг
- Юридический консалтинг
- Налоговый консалтинг

№ 15

в списке крупнейших российских консалтинговых групп и компаний

ТОП-10 в номинации

- Оценочная деятельность

ТОП-20 в номинациях

- Аутсорсинг
- IT-консалтинг

Юристы FBK Legal, одной из ведущих юридических фирм страны, неоднократно были рекомендованы к сотрудничеству российскими и международными рейтингами

Best Lawyers · Chambers · ПРАВО.RU 300 · WORLD TAX · INTERNATIONAL TAX REVIEW · Коммерсантъ · РАПСИ · IFLR1000

Нам доверяют

Газпром
ГТЛК
Счетная палата Российской Федерации
Альфа Банк
РОСНАНО
Российская корпорация нанотехнологий
ЕвроХим
Минерально-химическая компания
РОСОБОРОНЭКСПОРТ
РОССЕТИ
Министерство экономического развития Российской Федерации
РОСЭНЕРГОАТОМ
Электроэнергетический дивизион Росатома
Топливная компания Росатома ТВЭЛ
АЛРОСА
@ mail.ru group
ВЕРТОЛЕТЫ РОССИИ
ПСБ
ФОСАГРО
CAMOZZI
YAMAHA
EVRAZ GROUP
HERBALIFE
Jägermeister
iHerb
RANBAXY
KLEEMANN
ECOLAB
cma

**Услуги оказаны головным предприятиям групп компаний и/или их дочерним и зависимым обществам*

ФБК
Grant Thornton

Благодарим за внимание!

ул. Мясницкая, 44/1,
Москва, Россия 101990

T: (495) 737 5353
Ф: (495) 737 5347
E: fbk@fbk.ru

fbk.ru

fbk-pravo.ru