



Информационная безопасность предприятия.  
Противодействие промышленному шпионажу.

### Содержание темы:

1. Введение, история вопроса
2. Основные способы промышленного шпионажа
3. Классификация субъектов, объектов и методов
4. Оперативные виды разведки
5. Технические виды разведки
6. Электронные виды разведки
7. Вопросы права
8. Заключение

### Контрольные вопросы:

1. Что такое промышленный шпионаж?
2. Назовите основные исторические этапы его развития.
3. Каковы основные способы промышленного шпионажа?
4. Какие методы сбора разведданных используются в промышленном шпионаже?
5. Что понимается под оперативными видами разведки?
6. Какую роль играют технические средства промышленного шпионажа?
7. Что такое электронная разведка?
8. Чем можно объяснить дуализм отношений бизнеса и государства в сфере промышленного шпионажа?
9. Что вам известно о плане операции «Эшелон»?

## История вопроса

Китайцы в течение тысячелетий производили фарфор высокого качества. Секрет производства был найден китайскими алхимиками и, подобно всем алхимическим секретам, был окружен легендами и облечен в форму мифа. Согласно этому мифу, фарфоровая масса находится под землей в некоторых священных местах и охраняется злыми духами. Она превращается в фарфор под благотворными лучами солнца. Но из легенды нельзя было почерпнуть сведения о производстве фарфора. Поэтому в Китай засылали множество шпионов, чтобы они овладели секретом. Первым, кто в этом преуспел, был французский иезуит. Ему удалось посетить закрытый город Цзиндэчжень, где находилась императорская фарфоровая мануфактура. Он описал этот город в своих письмах, датированных сентябрем 1712 г. и январем 1722 г. На производстве работало свыше 1 млн. рабочих на 3 тысячах фарфоровых печей. Монах не только описал процесс производства, но и выкрал образцы сырья.



В докладе специальной комиссии Конгресса США, возглавлявшейся сенатором-республиканцем Кристофером Коксом (1999 г.), содержались утверждения о причастности Китайской народной республики (КНР) к краже секретных сведений в области военных ядерных технологий. В частности, в докладе говорилось, что в работах по созданию нейтронного оружия китайцы использовали секретные сведения, полученные из Ливерморской национальной лаборатории США. Упомянулось также и об утечке из Лос-Аламосской национальной лаборатории секретных сведений о конструкции самой совершенной американской ядерной боеголовки W-88 для БРПЛ Д-5 (Трейдент-2), что позволило китайцам значительно улучшить характеристики своих ядерных боеприпасов. Общеизвестно, что китайские разведчики проявляют повышенный интерес ко всему, что связано с боевой техникой и военными технологиями. Логика проста – украд документацию, можно сэкономить на закупках, собственное производство обходится до 100 раз дешевле импорта.

## ЧТО ТАКОЕ ПРОМЫШЛЕННЫЙ ШПИОНАЖ?

Промышленный шпионаж в России не юридический термин в отличие, скажем, от США, где есть Закон о промышленном шпионаже. Однако в большинстве случаев смысл его понятен даже непрофессионалам.

**Промышленный шпионаж — одна из форм недобросовестной конкуренции, применяемая на всех уровнях экономики — начиная с небольших предприятий и заканчивая государствами. Основная его составляющая — незаконное добывание сведений, представляющих коммерческую ценность.**

В межгосударственных отношениях промышленный шпионаж используется достаточно широко, но в отличие от бизнеса для государственной разведки важную роль играет обеспечение национальной безопасности. А в таких вопросах, как известно, допустимы любые средства и методы работы. Применительно к бизнесу задача разведки сужается от масштабов целой страны до одной или нескольких фирм-конкурентов. Такой бизнес-шпионаж обычно преследует одну из двух целей: проверить благонадежность делового партнера либо вытеснить его. Основное предназначение промышленного шпионажа — экономия средств и времени, и в этом он полностью совпадает с конкурентной разведкой.

Конкурентная разведка (КР) — это сбор и обработка данных из разных источников для выработки управленческих решений с целью повышения конкурентоспособности коммерческой организации, проводимые в рамках закона и с соблюдением этических норм.

Главное отличие конкурентной разведки от промышленного шпионажа состоит в законности методов получения информации.



# Кейс

## Секрет производства стали



В XVIII веке в Сторбридже (графство Вустер) жил английский поэт и музыкант Фоли. По основной профессии он был литейщиком. Считая, что английская сталь тех времен была очень низкого качества, Фоли взял свою скрипку, облачился в одежду менестреля и начал бродяжничать по континенту. Босой, в лохмотьях, зарабатывая на жизнь игрой на постоялых дворах и в замках, Фоли скитался по Бельгии, Германии, Богемии, Северной Италии и Испании и выкрадывал секреты производства стали. Вернувшись в Англию, он, проведя несколько опытов, нашел, что сталь еще не очень хороша, и снова вернулся на континент. На этот раз ему повезло больше. Лица, подсланные гильдиями литейщиков Европы, пытались его убить, совершали диверсии на его заводах. Ничего сделать им не удалось, и Фоли умер богатым. Его дети получили дворянский титул. Промышленный шпионаж вознаграждается!

Ж. Бержье, Промышленный шпионаж, 2011, М., Вузовская книга



Ответы  
практики...

### 1791 год

во Франции издан закон  
«О патентах на изобретение»

### 1875 год

на заводах Круппа создана полиция в  
целях охраны секретов фирмы



С академической точки зрения...

Юридическая защита прав на изобретение, полицейские меры охраны секретов и судебное преследование явились цивилизованными мерами поддержки прав частной собственности. Они не остановили промышленный шпионаж...

# Кейс

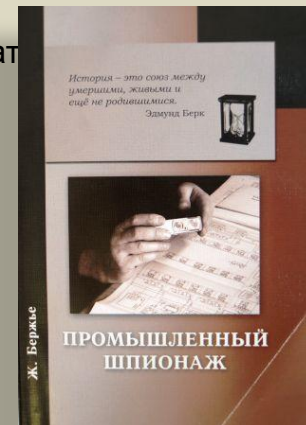
## Между двумя мировыми войнами



По данным доктора Уорта Уэйда, опубликованным в журнале «Кемикл инджиниринг» 23 мая 1965 г., были описаны средства промышленного шпионажа, применявшиеся в США в период между I и II мировыми войнами. Первые 7 соответствовали американскому законодательству, остальные 13 – входили с ним в противоречие:

- 1) Публикации конкурентов и отчеты о процессах, полученные обычными путями.
- 2) Сведения, данные публично бывшими служащими конкурента.
- 3) Обзоры рынков и доклады инженеров-консультантов.
- 4) Финансовые отчеты.
- 5) Устраиваемые конкурентами ярмарки и выставки, издаваемые ими брошюры.
- 6) Анализ изделий конкурентов.
- 7) Отчеты коммивояжеров и закупочных отделов.
- 8) Попытки пригласить на работу специалистов, работающих у конкурента, и заполненные ими с этой целью вопросники.
- 9) Вопросы, осторожно задаваемые специалистами конкурента на специальных конгрессах.
- 10) Непосредственное тайное наблюдение.
- 11) Притворное предложение работы служащим конкурента без намерения брать их на работу с целью выведать у них информацию.
- 12) Притворные переговоры с конкурентом якобы для приобретения лицензии на один из патентов.
- 13) Использование профессиональных шпионов для получения информации.
- 14) Сманивание с работы служащих конкурента для получения информации.
- 15) Посягательство на собственность конкурента.
- 16) Подкуп сотрудников закупочного отдела конкурента или его служащих.
- 17) Засылка агентов к служащим или специалистам конкурента.
- 18) Подслушивание разговоров у конкурента.
- 19) Похищение чертежей, образцов, документов и т.д.
- 20) Шантаж и различные способы давления.

Ж. Бержье, Промышленный шпионаж, 2011, М., Вузовская книга



## Основные способы промышленного шпионажа

«К основным источникам, обладающим, владеющим или содержащим конфиденциальную информацию, можно отнести: **людей, документы, публикации, технические средства обеспечения производственной и трудовой деятельности, продукцию фирмы, производственные отходы.** Основными способами несанкционированного доступа к конфиденциальной информации могут быть:

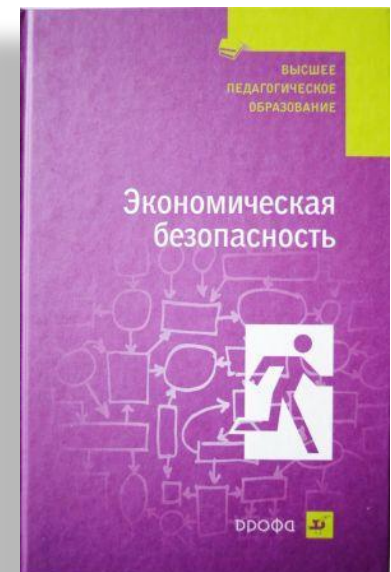
- Инициативное сотрудничество;
- Склонение к сотрудничеству;
- Выпытывание, выведывание;
- Подслушивание разговоров различными путями;
- Негласное ознакомление со сведениями и документами;
- Хищение;
- Копирование;
- Подделка (модификация);
- Уничтожение (порча, разрушение);
- Незаконное подключение к каналам и линиям связи и передачи данных;
- Перехват;
- Визуальное наблюдение;
- Фотографирование;
- Сбор и аналитическая обработка.

Системы защиты конфиденциальной информации включают целую совокупность организационных, правовых, экономических, технических и иных мероприятий».

Грунин О.А., А.Д. Макаров, Л.А. Михайлов, А.Л. Михайлов, А.С. Скаридов, Экономическая безопасность, 2010, М., Дрофа

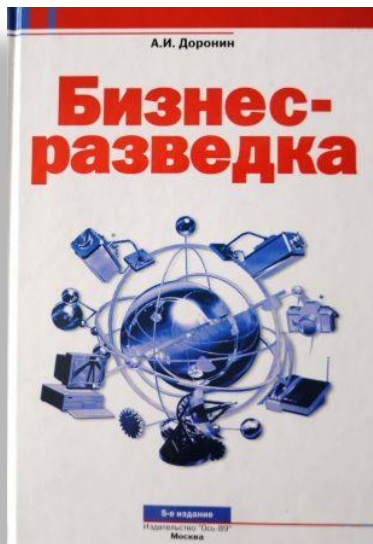


**Цитата**





## Цитата



### Методы сбора разведанных:

- Закупка товаров конкурента;
- Неизменное присутствие на ярмарках, выставках, конференциях и т.п., при этом собирается вся доступная или оставленная по недосмотру документация и информация, фотографируется все, что возможно;
- Посещение предприятий;
- Финансирование контрактов на выполнение научно-исследовательских работ за рубежом с целью проникновения в некоторые лаборатории;
- Отправка на учебу за рубеж студентов и стажеров;
- Бесконечные безрезультатные переговоры, в процессе которых постоянно запрашивается дополнительная информация;
- Похищение чертежей и технической информации;
- Агентурное проникновение и простое воровство.

Доронин А.И., Бизнес-разведка, 2010, М., Ось-89



## Кейс

В апреле итальянского г. Модена, где расположена штаб-квартира Ferrari, признал двух бывших работников этой компании виновными в промышленном шпионаже. По словам представителя обвинения, сотрудники Ferrari Анджело Сантини и Мауро Яккони, уволившись из фирмы в 2002 году, перешли на работу в компанию Toyota. Однако перед своим увольнением они скачали файлы с конфиденциальной информацией о разработках Ferrari в области проектирования болидов Формулы-1, которые впоследствии были переданы представителям японского автопроизводителя. Полученные данные были использованы японцами при создании болида Toyota FT103y.

25.04.2007 г.

[auto.mail.ru/news?id=22216](http://auto.mail.ru/news?id=22216)





До появления электронных средств шпионажа



В различных средствах массовой информации и научных журналах 1960-х годов описывали технические средства получения информации, применявшиеся государственными спецслужбами и службами промышленного шпионажа. Среди них: прибор снятия вибрации с оконного стекла, микро-телевизионная камера, аппаратура снятия информации со слаботочного оборудования, дистанционный детектор лжи, радиозакладки со сверхчувствительными микрофонами, микро фотоаппараты в пуговице костюма, телевизионные камеры в бюстгальтере, датчики контроля в телефонных аппаратах, миниатюрный магнитофон в портсигаре (зажигалке), камуфляжи этих и других изделий под любые вещи.

В тот период существовала отрасль безопасности ПДИТР – противодействие иностранным техническим разведкам.



# Классификация субъектов, объектов и методов

С

Государственные органы

Субъекты промышленного шпионажа

Частные предприниматели

О

Места сосредоточения интересующей субъекты информации

Объекты промышленного шпионажа

М

Оперативные

Технические

Электронные

Методы промышленного шпионажа

## Оперативные виды разведки

Оперативные виды разведки являются традиционными и наиболее древними из всех видов промышленного шпионажа. В детективной литературе их часто называют **тайными операциями**. Данный инструмент используют не только государства, но и частные субъекты предпринимательской деятельности.

Набор видов и средств оперативной разведки относительно невелик и прост:

- a) Сбор первичной информации из легальных источников
- b) Разовое получение информации путем выведывания у носителей информации
- c) Продвижение своего человека на объект изучения
- d) Приобретение инсайдера на объекте изучения
- e) Получение от инсайдеров требуемой информации в любой форме
- f) Использование возможностей инсайдеров для негласного ознакомления и возможного изъятия закрытой информации
- g) Использование возможностей инсайдеров для оказания выгодного воздействия на объект изучения
- h) Использование возможностей инсайдеров и других сил и средств для нанесения ущерба объекту изучения
- i) Техническая и электронная разведки наиболее эффективны в совокупности с оперативной разведкой
- j) Использование любых возможностей для поддержания надежной двусторонней связи с инсайдерами.

Искусство проведения тайных операций разведки состоит в том, чтобы не допустить непрофессионализма и излишне стандартных действий, т.к. любой шаблон является гарантированной предпосылкой для провала не только данной, но и возможных последующих операций.

Иногда раскрытие только своего интереса к объекту изучения может дать в руки конкурента нежелательные аргументы.



Данным видом разведки владеют, правда в разной степени, практически все спецслужбы самостоятельных государств



## Технические виды разведки

Технические виды разведки первоначально являлись дополнительным инструментарием оперативной разведки, своеобразным следствием научно-технического прогресса.

Набор видов технической разведки сложно ограничить:

- a) Использование всех видов зрительных приборов
- b) Использование всех видов аудио записи
- c) Использование всех видов фото, кино, видео записи
- d) Использование всех видов устройств радио перехвата
- e) Использование всех средств подавления излучений приборов
- f) Использование всех видов шифровальных устройств
- g) Использование любых форм надежного шифрования информации
- h) Использование всех видов дешифровальных устройств
- i) Использование всех видов носителей средств технической разведки (СТС)
- j) Использование всех видов маскировки СТС
- k) Использование всех видов камуфлирования СТС

Процесс усовершенствования существующих и изобретения новых средств технической разведки продолжается. Искусство их сочетания с оперативными видами разведки является свидетельством профессионального мастерства.

Ранее технические средства были достоянием только государственных спецслужб. В настоящее время часть этого рынка стала открыта для гражданского общества и, соответственно, участников предпринимательской деятельности.





## Источники информации о скрываемых объектах

Электро-магнитные излучения  
ультрафиолетового, видимого  
и инфракрасного диапазонов

Электро-магнитные излучения  
радиодиапазона

Акустические поля в водной  
среде

Акустические поля в  
воздушной среде

Химические выбросы и отходы  
в окружающей среде

Радиоактивные излучения

Деформационные и сдвиговые  
поля в земной коре

Локальные изменения  
магнитного поля Земли

Электронные базы ЭВМ



## Виды технической разведки

1

Оптическая разведка  
(ОР)

2

Оптико-электронная  
разведка (ОЭР)

3

Радиоэлектронная  
разведка (РОР)

4

Гидроакустическая  
разведка (ГАР)

5

Акустическая разведка  
(АР)

6

Химическая разведка  
(ХР)

7

Радиационная разведка  
(РДР)

8

Сейсмическая разведка  
(СР)

9

Магнитометрическая  
разведка (ММР)

10

Компьютерная разведка  
(КР)

# Оптическая разведка

1

Оптическая разведка  
(ОР)

Визуально-  
оптическая разведка  
(ВОР)

Процесс получения информации при непосредственном наблюдении объектов невооруженным глазом и с использованием наблюдательных оптических приборов.

Фотографическая  
разведка (ФР)

Фотографическое изображение позволяет получать оптические изображения объектов наиболее высокого качества. Это используется при ведении космической, воздушной, морской и наземной разведок.



# Оптико-электронная разведка



2

## Оптико-электронная разведка (ОЭР)

Под ОЭР понимается процесс добывания информации с помощью средств, включающих входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечивают прием и анализ электромагнитных волн видимого и инфракрасного диапазонов, излученных или отраженных объектами и местностью.

Инфракрасная разведка (ИКР)

Лазерная разведка (ЛР)

Телевизионная разведка (ТЛВР)

Разведка лазерных излучений (РЛИ)



# Радиоэлектронная разведка

Это процесс получения информации в результате приема и анализа электромагнитных первичных и вторичных излучений радиодиапазона, создаваемых работающими радиоэлектронными средствами.

3

## Радиоэлектронная разведка (РОР)

Радиоразведка (РР)

Радиотехническая разведка (РТР)

Радиолокационная разведка (РЛР)

Радиотепловая разведка

Разведка ПЭМИН



4

## Гидроакустическая разведка

Гидроакустическая  
разведка (ГАР)

Гидроакустическая  
разведка активная  
(ГАР-А)

Гидроакустическая  
разведка сигнальная  
(ГАР-С)

Гидроакустическая  
разведка пассивная  
(ГАР-П)



Под ГАР понимается получение информации путем приема и анализа акустических сигналов инфразвукового, звукового и ультразвукового диапазонов, распространяющихся в водной среде от надводных и подводных объектов. Активные средства – гидролокаторы (облучение цели акустической энергией и прием эха), пассивные средства – шумопеленгаторы (перехват шумов, непреднамеренно создаваемых целью). Оба вида средств гидроакустической разведки принимают полезные сигналы и перехватывают информацию, передаваемую по каналам гидроакустической связи, выявляют дислокацию объектов и занимаются картографированием морского дна.

## Акустическая разведка

Акустическая разведка  
(АР)

Акустическая  
разведка сигнальная

Акустическая  
разведка речевая



Под АР понимается получение информации путем приема и анализа акустических сигналов инфразвукового, звукового, ультразвукового диапазонов, распространяющихся в воздушной среде от объектов разведки. АР обеспечивает получение информации, содержащейся непосредственно в произносимой либо воспроизводимой речи (акустическая разведка речевая) и в параметрах акустических сигналов, сопутствующих работе вооружения и военной техники, механических устройств оргтехники и других технических систем (акустическая разведка сигнальная).

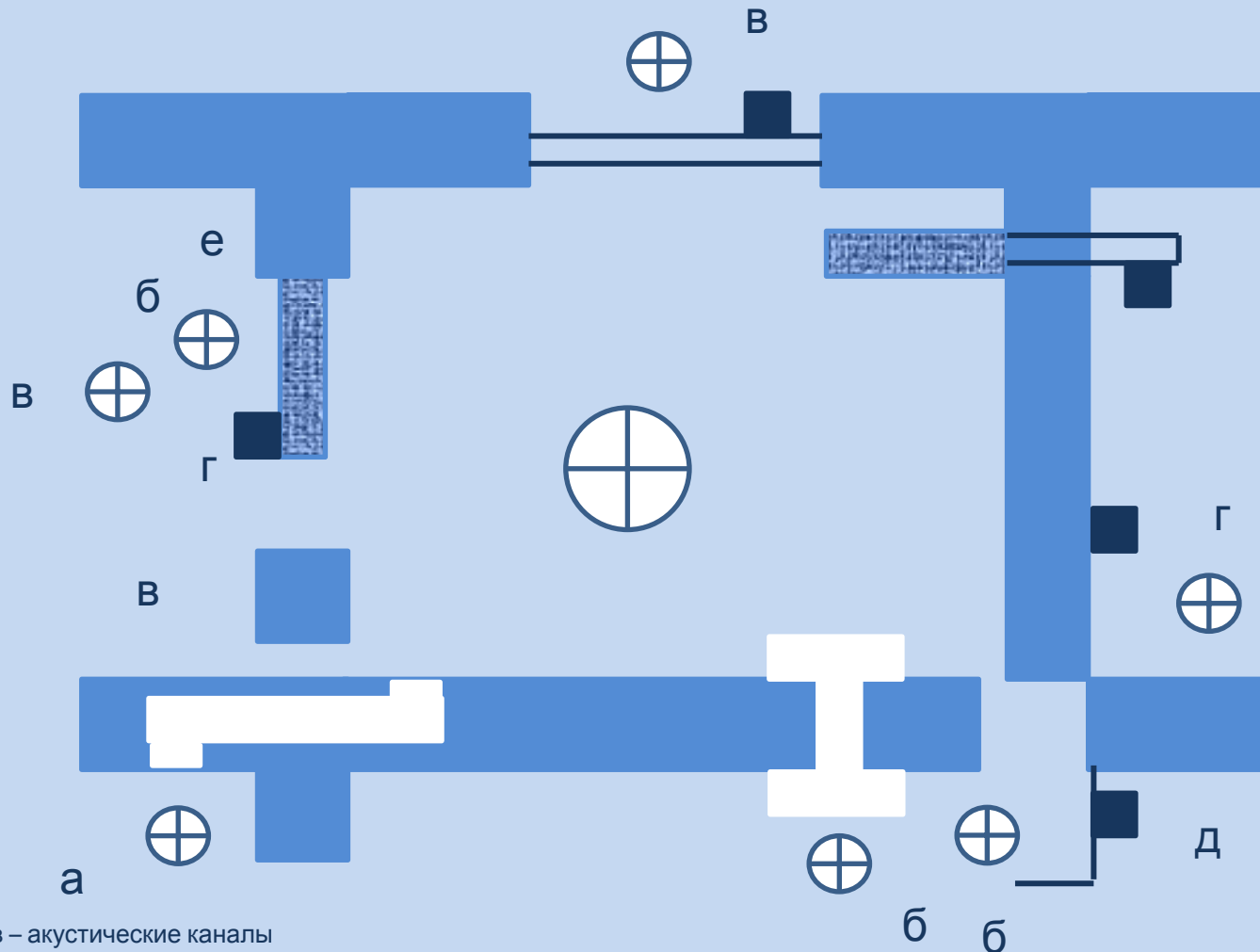
# Классификация акустических закладок



Меньшаков Ю.К. Теоретические основы технических разведок. 2008, М. МГТУ им Баумана, Стр. 290

# Основные каналы утечки речевой информации

Бузов Г.А., Практическое руководство по выявлению специальных технических средств несанкционированного получения информации, 2010, М., Горячая линия - Телеком



а, б, в – акустические каналы  
г, д, е – вибрационные каналы

6

## Химическая разведка

Химическая разведка  
(ХР)

Химическая  
разведка контактная

Химическая  
разведка  
дистанционная



Под ХР понимается добывание информации путем контактного или дистанционного анализа изменений химических свойств состава окружающей среды под воздействием выбросов и отходов производства, работы двигателей, в результате взрывов и выстрелов, преднамеренного рассеивания химических веществ, испытаний и применений химического оружия.

## Иные виды технических разведок

7

### Радиационная разведка (РДР)

Выбросы и отходы атомного производства, хранения и транспортировки расщепляющихся материалов, ядерных зарядов и боеприпасов, местонахождением реакторов и заражением местности.

8

Сдвиги земной коры под воздействием взрывов.

### Сейсмическая разведка (СР)



9

Под ММР понимается добывание информации путем обнаружения и анализа локальных изменений магнитного поля Земли под воздействием объектов с большой магнитной массой. ММР ведет обнаружение и определение таких статических и динамических объектов на земле, в земле и в водной среде.

### Магнитометрическая разведка (ММР)

10

### Компьютерная разведка (КР)

Сейчас, по мнению авторов, это уже составная часть электронной разведки





Принципы: глобальность и тотальность.  
Ведущим органом технической разведки США является  
**Агентство национальной безопасности**

В соответствии с Патриотическим актом (принят администрацией республиканца Буша и пролонгирован администрацией демократа Обамы), спецслужбы США получили право на перлюстрацию электронных сообщений и отслеживание посещений WEB-страниц, прослушивание телефонных переговоров, проведение негласных обысков и слежки.



Разведывательное сообщество США традиционно ведет все виды технической разведки на территории Земли, в наземном, морском, воздушном и космическом пространствах







В период «холодной войны» разведывательное сообщество США свыше 80% разведывательной информации об СССР и его союзниках получало с помощью технических средств разведки.



В бывшем СССР промышленные и военные секреты, в условиях отсутствия частной собственности и основанного на ней предпринимательства, защищались Государственной технической комиссией при СМ СССР, КГБ СССР и его органами, режимно-секретными органами предприятий и организаций. Субъектами разведывательных устремлений могли быть как зарубежные спецслужбы, так и негосударственные службы безопасности зарубежных корпораций. Противодействие иностранным техническим разведкам (ПДИТР) осуществлялось на всей территории Советского Союза по единому скоординированному замыслу. Меры защиты носили стандартный характер и во многом зависели от отрасли и степени секретности защищаемой информации. В эти меры постоянно вносились коррективы, которые вырабатывались на основе данных об устремлениях, технических средствах, методах и приемах деятельности «вероятного противника».



Орбитальная группировка Вооруженных сил США позволяет снабжать политическое и военное руководство страны объективной информацией



## Электронные виды разведки



Принципы: глобальность и тотальность.  
Ведущим органом электронной разведки США является  
**Агентство национальной безопасности**

С появлением электронно-вычислительной техники, индивидуальных, корпоративных, социальных, международных и глобальных сетей, изобретением и совершенствованием цифровых технологий мир стал иным.

По иному на него взглянули специальные службы самостоятельных государств, транснациональные корпорации, международные военно-политические организации и современные тайные общества.

Электронные виды разведки стали ведущим средством ведения промышленного шпионажа...

Оперативная и техническая виды разведки уступили приоритеты, но сохранились в общем арсенале разведки...

В арсенале электронной разведки:

- a) Контроль глобальных телекоммуникационных сетей
- b) Контроль глобальных платежных систем и коммуникаций
- c) Контроль глобальных социальных сетей и электронных СМИ
- d) Контроль корпоративных и локальных электронных систем
- e) Возможность открытого или скрытого влияния на системы
- f) Возможность временного или постоянного вывода систем из строя

Средства электронной разведки настолько дороги, что их могут содержать только крупные мировые державы.



В конце 1996 г. эксперт Пентагона Роберт Банкер предоставил доклад, посвященный новой программе строительства и боевого применения вооруженных сил США в XXI веке (концепция Force 21). В ее основу было положено разделение всего театра военных действий на две составляющие – традиционное и киберпространство, причем последнему придавалось более важное значение. В октябре 1998 г. министерство обороны США ввело в действие Объединенную доктрину информационных операций:

## **ЦЕЛЬ - ИНФОРМАЦИОННОЕ ПРЕВОСХОДСТВО**

Информационная операция – это действия, предпринимаемые в целях затруднения сбора, обработки, передачи и хранения информации системами противника при защите собственной информации и систем.

Информационная война – комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, ее военно-политическое руководство, которое уже в мирное время привело бы к принятию благоприятных решений, а в ходе конфликта полностью парализовало инфраструктуру управления противника.

# Кейс

## Национальный бизнес и национальные спецслужбы



- ❖ Одной из жертв Агентства национальной безопасности США стал германский производитель ветровых электрогенераторов «Энеркон». В его исследовательских лабораториях была разработана новая технология, позволявшая получить электричество с помощью энергии ветра значительно дешевле, чем раньше. Но когда компания попыталась наладить маркетинг своих изделий в США, она столкнулась с американским конкурентом «Кенетек», который заявил, что запатентовал почти аналогичную разработку. Дело закончилось весьма показательно: «Кенетек» подал на «Энеркон» в суд, добившись запрета продажи его изделий в США. Ситуация с чистотой «патентов» «Кенетека» прояснилась, когда не назвавшийся сотрудник АНБ США в интервью германскому телевидению признал, что линия связи между исследовательской лабораторией «Энеркон», расположенной на берегу Северного моря, и производственным подразделением фирмы, находящимся примерно в 25 километрах, прослушивалась с помощью спутников. А затем все полученные данные об этих разработках были переданы АНБ «Кенетек».  
(Колчанов Р., Шпионы держат нос по ветру, Труд, 30.-0.1999 г.)
- ❖ В начале 1999 года французская разведка поставила на прослушивание телефоны всех ведущих менеджеров немецкого концерна VEBA. Причиной этого шага стал интерес французских конкурентов к состоянию переговоров, касавшихся закрытия в Германии ряда атомных электростанций. Получив необходимые данные, французские фирмы смогли заключить многомиллиардный контракт на работы по восстановлению и обогащению урановых стержней. Годом ранее французским спецслужбам удалось получить исследовательские материалы концерна Daimler Chrysler по проекту «Топливные элементы для автомобильных двигателей», которые были переданы французским автомобилестроительным фирмам.  
(Демин В.А., Экономический и промышленный шпионаж: расширение масштабов и рост агрессивности, Защита информации, Кофидент, № 3 2002)

Доронин А.И., Бизнес-разведка, 2010, М., Ось-89



## Кодовое название «Эшелон»

Доронин А.И., Бизнес-разведка, 2010, М., Осб-89, стр.634



Много копий в западной прессе сломано по поводу оглашения секретного пакта, заключенного между разведслужбами США, Великобритании, Австралии, Канады и Новой Зеландии. На его основе создана и функционирует самая крупная в мире система прослушивания и перехвата телефонных разговоров, факсов и электронной почты (кодовое название «Эшелон»), способная улавливать до 100 миллионов переговоров в месяц.

Инициатором подписания пакта и создания этой системы выступило Агентство национальной безопасности США. Станции перехвата расположены по всему миру – на американских военных базах в Германии, в Тихом океане и в Гонконге. На территории Англии расположены перехватывающие и транзитные станции.

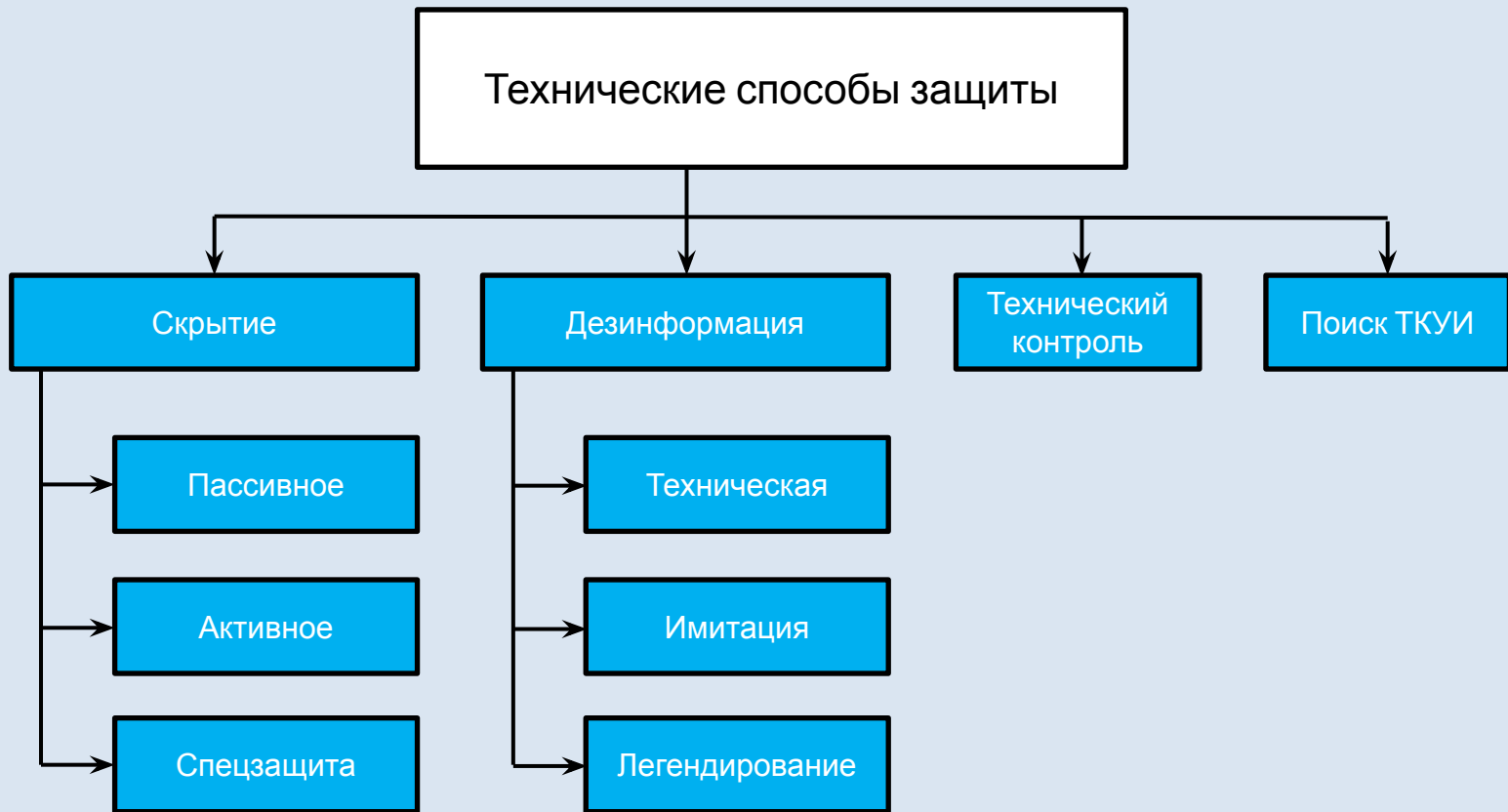
Обработка перехваченной информации осуществляется по принципу ключевых слов. При необходимости подпрограмме, которая называется «Словарь», задается необходимое ключевое слово, например «микропроцессор», и начинается поиск по всему накопленному банку данных перехваченных телефонных переговоров, факсов и сообщений электронной почты. После останется только послушать, кто, кому и по какому поводу говорил это слово.

По оценке независимых западных экспертов, в более чем 80% случаев результаты этой деятельности используются для промышленного шпионажа.

В качестве подтверждения можно привести следующий факт. В 1995 году в прессу просочилась информация о том, что АНБ с помощью системы «Эшелон» перехватывало все факсы и телефонные звонки между европейским консорциумом «Airbus» и Саудовской национальной авиакомпанией. В результате этого были получены сведения о том, что сотрудники «Airbus» предлагали саудитам за заключение 6-миллиардного контракта значительные суммы в качестве взятки. АНБ передало данную информацию в правительство США, чиновники которого сумели убедить своих коллег в Саудовской Аравии отдать данный контракт «Боингу» и «МакДоннел Дуглас К».

Потенциальный объект  
промышленного шпионажа





## Технические способы защиты

Защита объектов от оптической разведки

Защита от оптико-электронных средств разведки

Защита радиоэлектронных средств и информации от радио- и радиотехнической разведки

Защита объектов от радиолокационных средств разведки

Защита лазерных систем от технических разведок

Защита от гидроакустических средств разведки

Защита от средств акустической разведки

Защита технических средств передачи, обработки и хранения информации

Защита информации в средствах электронно-вычислительной техники

Организационно-правовые меры обеспечения безопасности информации и аттестация АС

Ю.К. Меньшаков. Основы защиты от технических разведок. 2011. М. МГТУ.



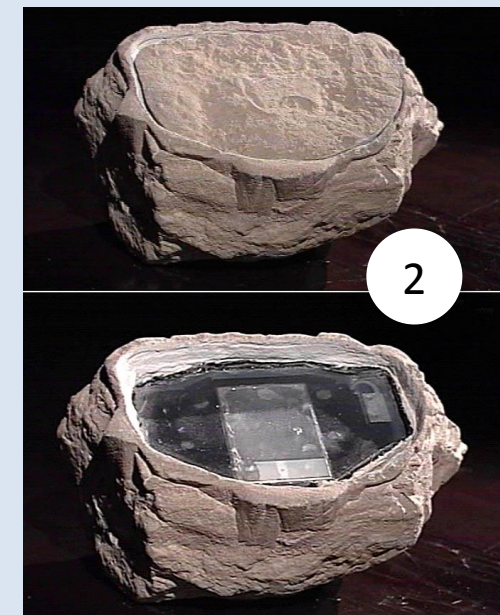
Технический контроль в зонах обнаружения позволил выявить:

1

Прибор радиоэлектронной разведки США «пенек»

2

Прибор радиоэлектронной разведки Великобритании «булыжник»

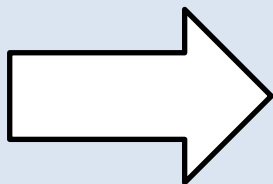


## Технический контроль

эффективности принятых мер защиты

- 1) Выявление демаскирующих признаков объектов защиты и возможных технических каналов утечки закрытой информации;
- 2) Определение (проверка) зон возможного обнаружения объектов технических средств разведки;
- 3) Разработка предложений по совершенствованию системы защитных мер;
- 4) Технический контроль использует разные методы, зависящие от объектов защиты и видов разведки.

Технический контроль в защищаемых зонах позволяет выявлять или подавлять средства снятия речевой информации:



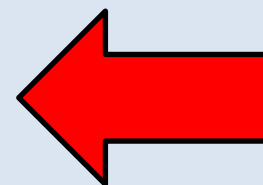
Средства  
подавления



Средства подслушивания



Средства  
выявлени  
я





Деятельность технических разведок и принципы защиты от них детально проработаны в специальной литературе.





**Ст. 138 УК РФ**

Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

**Ст. 139 УК РФ**

Нарушение неприкосновенности жилища

**Ст. 178 УК РФ**

Недопущение, ограничение или устранение конкуренции

**Ст. 204 УК РФ**

Коммерческий подкуп

**Ст. 272 УК РФ**

Неправомерный доступ к компьютерной информации

**Ст. 275 УК РФ**

Государственная измена

**Ст. 276 УК РФ**

Шпионаж

**Ст. 283 УК РФ**

Разглашение государственной тайны

**Ст. 284 УК РФ**

Утрата документов, содержащих государственную тайну

**Ст. 293 УК РФ**

Халатность

## Заключение



Защита субъектов предпринимательской деятельности от угроз оперативной, технической и электронной составляющих промышленного шпионажа в современных условиях стала в нашей стране сферой позитивного сотрудничества в рамках обеспечения безопасности личности, общества и государства. Система мер в данной области представляет собой иерархическую систему, элементы которой участвуют в рамках своей заинтересованности в едином процессе и делегируют часть своих полномочий как сверху вниз, так и снизу вверх.



Промышленный шпионаж из удела одиночек в XXI веке превратился в глобальный фактор современной мировой экономики и политики.





**Указ Президента Российской Федерации от 15 января 2013 г. № 31с (Выписка)  
О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации**

В целях обеспечения информационной безопасности Российской Федерации постановляю:

1. Возложить на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.
2. Определить основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:
  - a) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;
  - b) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;
  - c) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;
  - d) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.
3. Установить, что Федеральная служба безопасности Российской Федерации:
  - a) организует и проводит работы по созданию государственной системы, названной в пункте 1 настоящего Указа, осуществляет контроль за исполнением этих работ, а также обеспечивает во взаимодействии с государственными органами функционирование ее элементов;
  - b) Разрабатывает методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами – на иные информационные системы и информационно-телекоммуникационные сети...