Национальный исследовательский университет
«Высшая школа экономики»

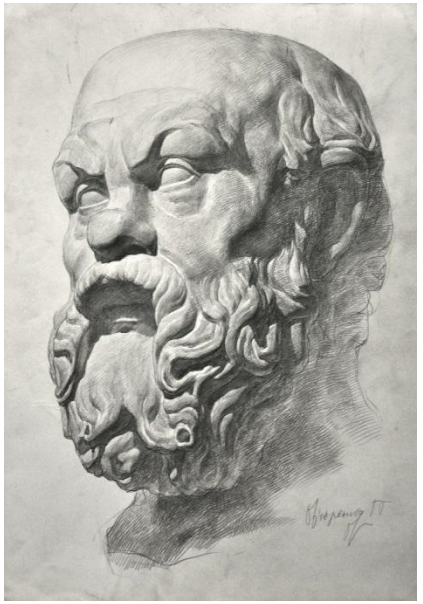
Институт проблем безопасности

2015/2016-2016/2017 гг.

майнор

Безопасность предпринимательской деятельности

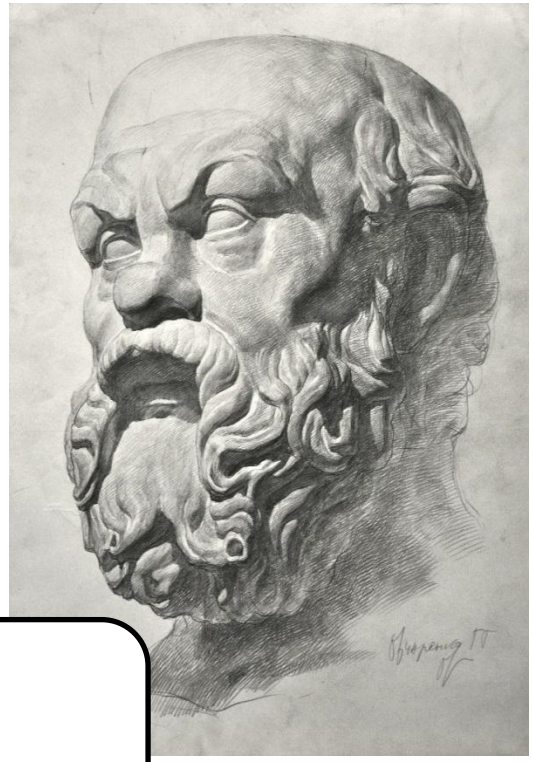
Безопасность предпринимательской деятельности



1-й и 2-й модули 2016/2017 учебного года:
сентябрь, октябрь, ноябрь, декабрь
190 академических часов

Дисциплина № 3

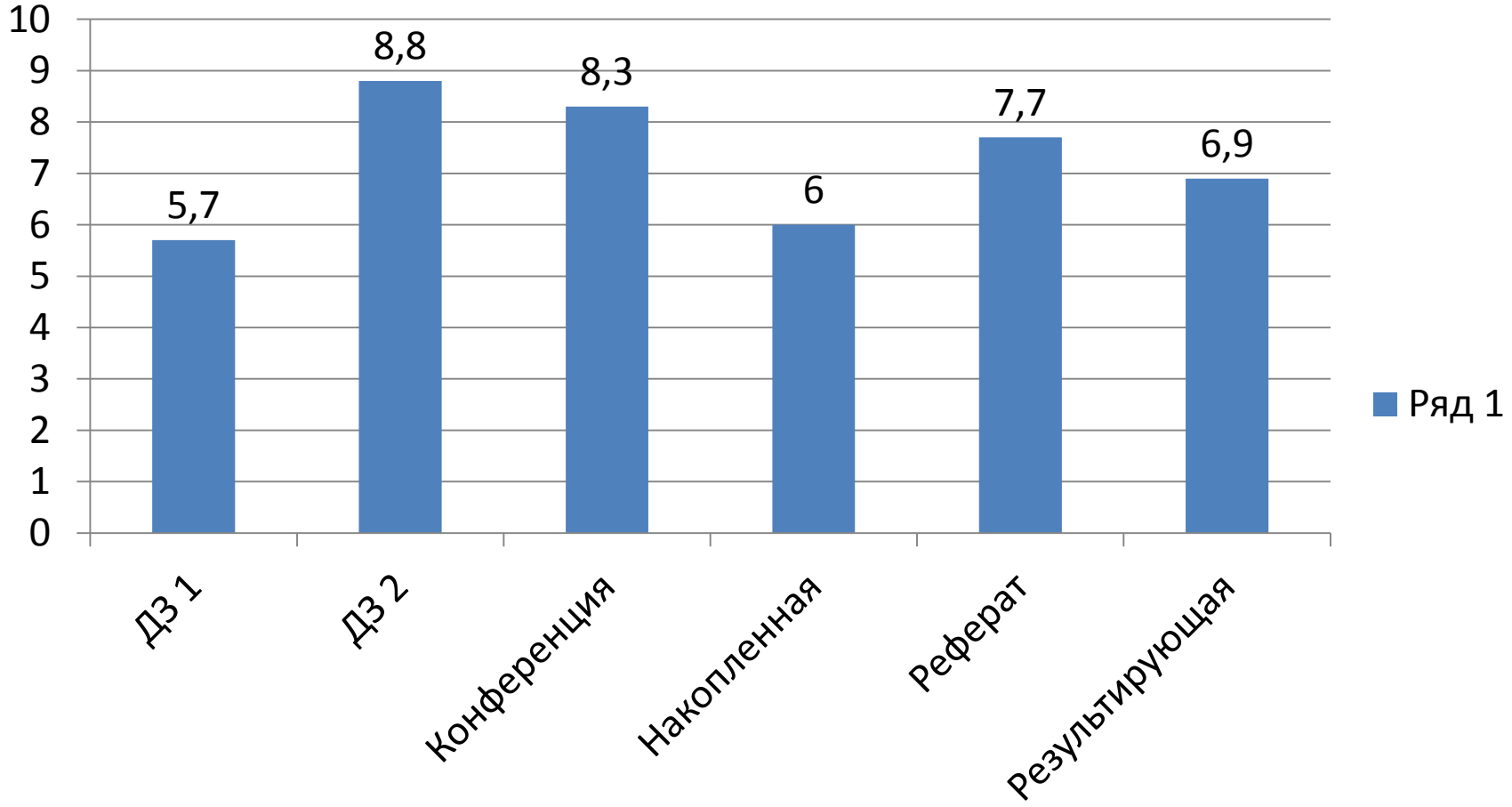
Комплексное противодействие атакам на информационные и материальные ресурсы бизнеса



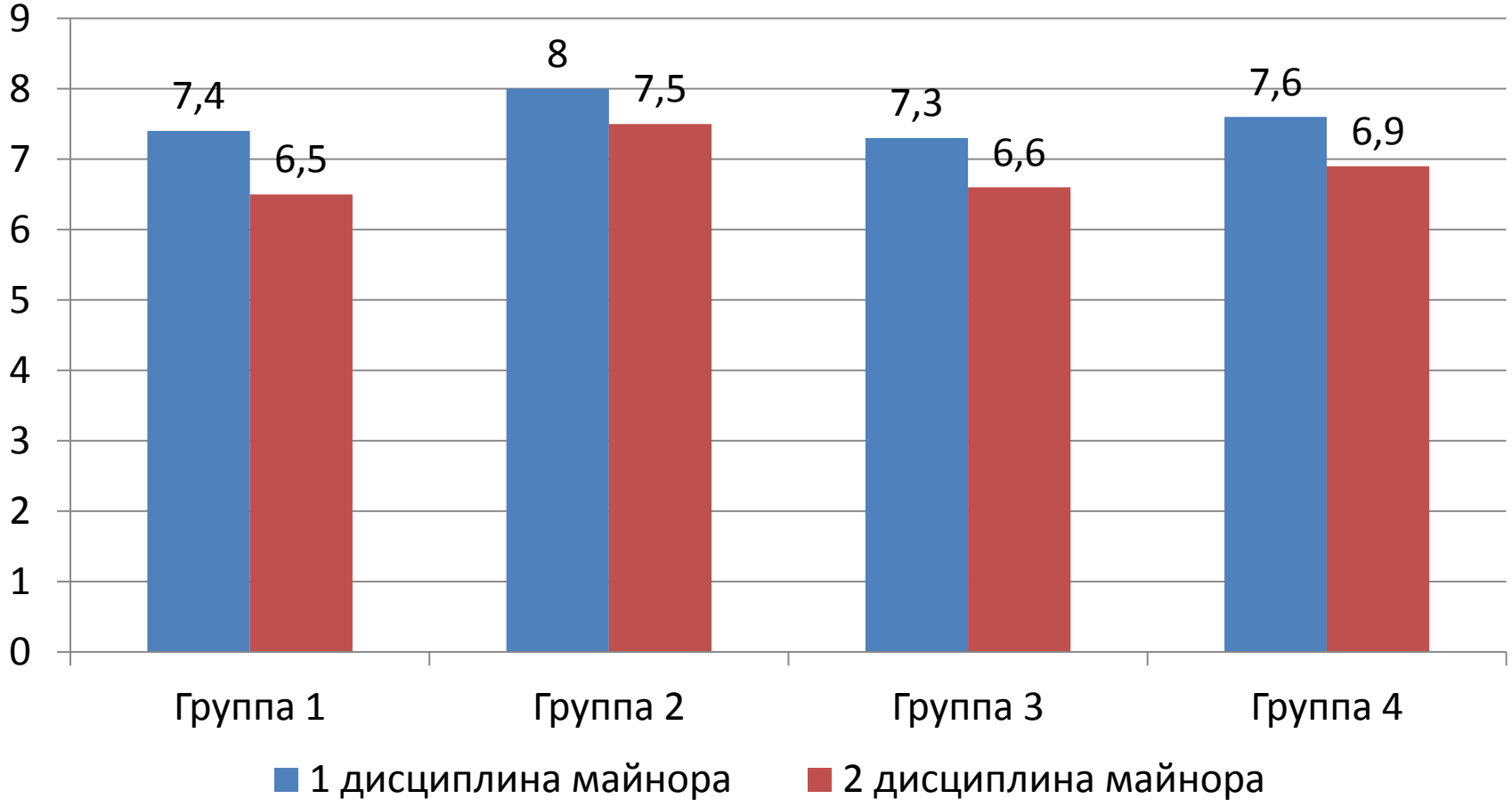
Сократ, мудрец

Итоги 2015/2016 учебного года

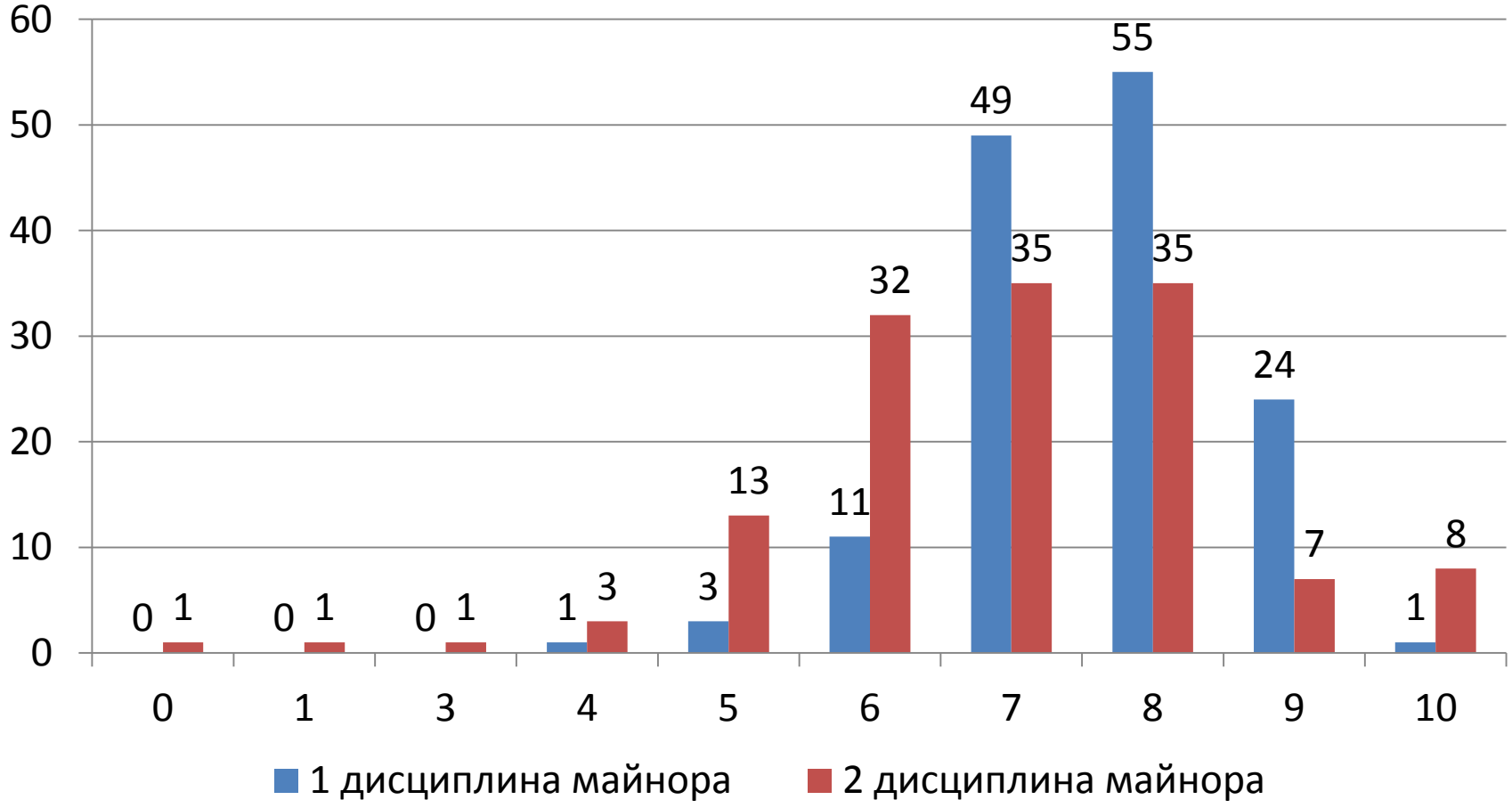
Средние баллы по всем видам контроля за вторую дисциплину майнора



Средний итоговый балл по группам за две дисциплины майнора



Распределение числа студентов по баллам



Реакция на «красную кнопку»

О ПОЛЗЕ И VREDE UCHENIA

А.В. Юрченко

2015 – 2016

1 2 3 4 5

13 человек

6 7 8

109 человек

9 10

19 человек

Методика оценивания обучения на майноре 1-2 модуль:

Текущий контроль

(ДЗ1, ДЗ2, ДЗ3)

Работа в аудитории

(1 деловая игра)
Тесты на занятии для обратной связи

Самостоятельная работа (СР)
(проектная работа)

Накопленная оценка (НО)

=0,6(ДЗ1+ДЗ2 +ДЗ3):3 +0,2 (ДИ1+ДИ2):2 + 0,2СР

50%

Результирующая оценка за дисциплину= 0,5(НО)+0,5(ИК)

Итоговый контроль (ИК)

(экзамен в форме тестирования)

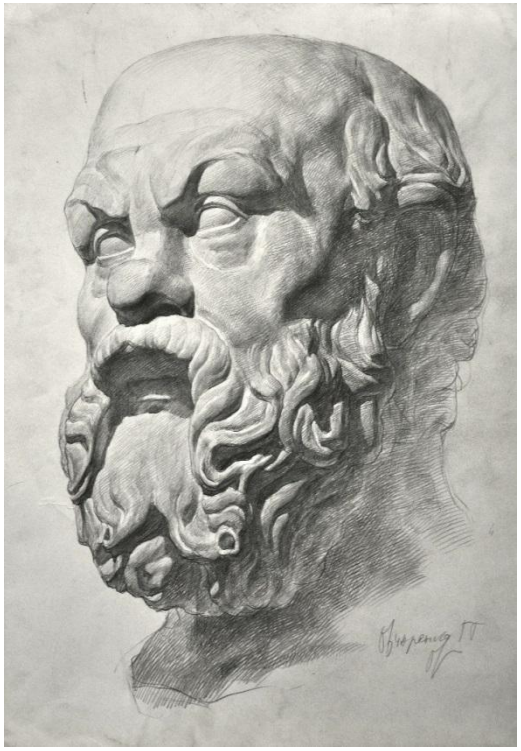
50%

Комплексное противодействие атакам на информационные и материальные ресурсы бизнеса

Тема № 1

Угрозы в области информационной безопасности

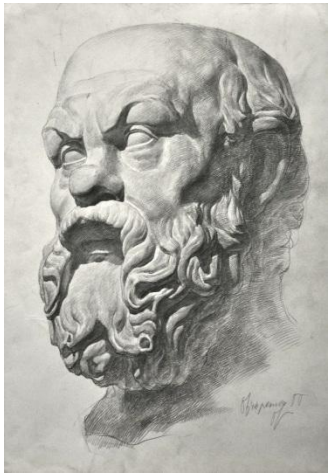
Лекция, 2 часа



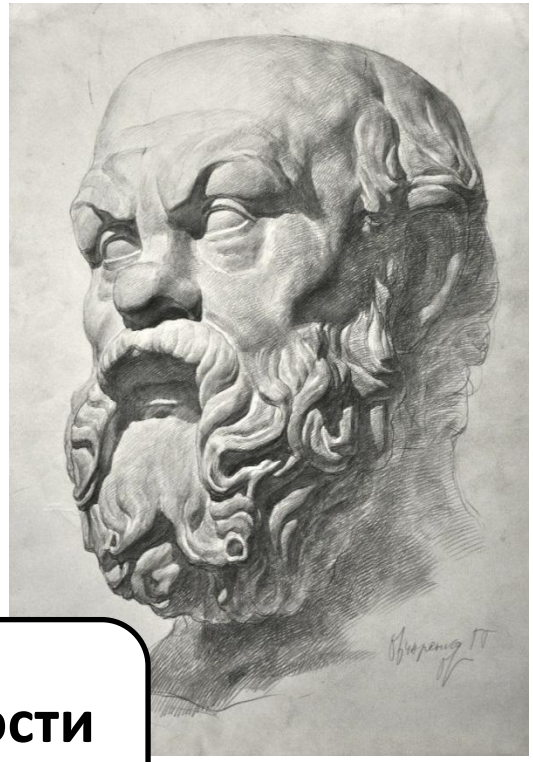
Сократ, мудрец

Информационная безопасность

Оглавление



Философия информационной безопасности бизнеса



Сократ, мудрец

ПОНЯТИЕ «ИНФОРМАЦИЯ»

В философском смысле

информация есть отражение в сознании людей объективных причинно-следственных связей в окружающем нас реальном мире

Информация есть характеристика не сообщения, а соотношения между сообщением и его потребителем.

В практическом смысле

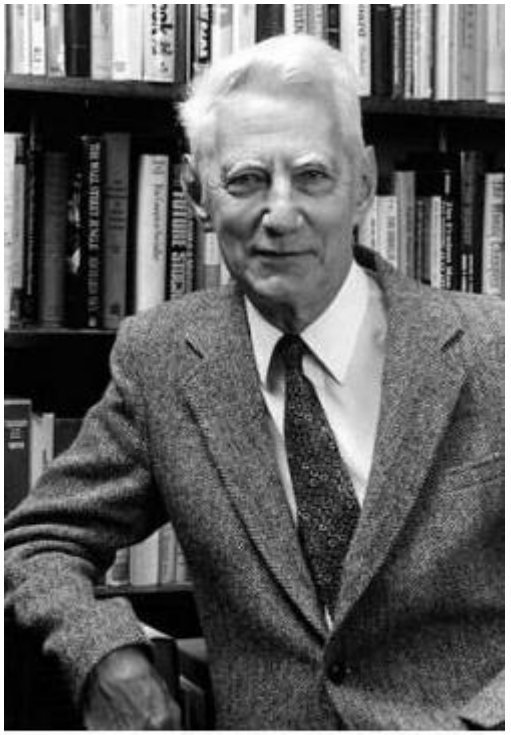
информация – есть все сведения, являющиеся объектом хранения, передачи и преобразования.

Количественным описанием процессов информации и математическими закономерностями занимается ТЕОРИЯ ИНФОРМАЦИИ.

ТЕОРИЯ ИНФОРМАЦИИ

Посвящена решению проблемы измерения информации

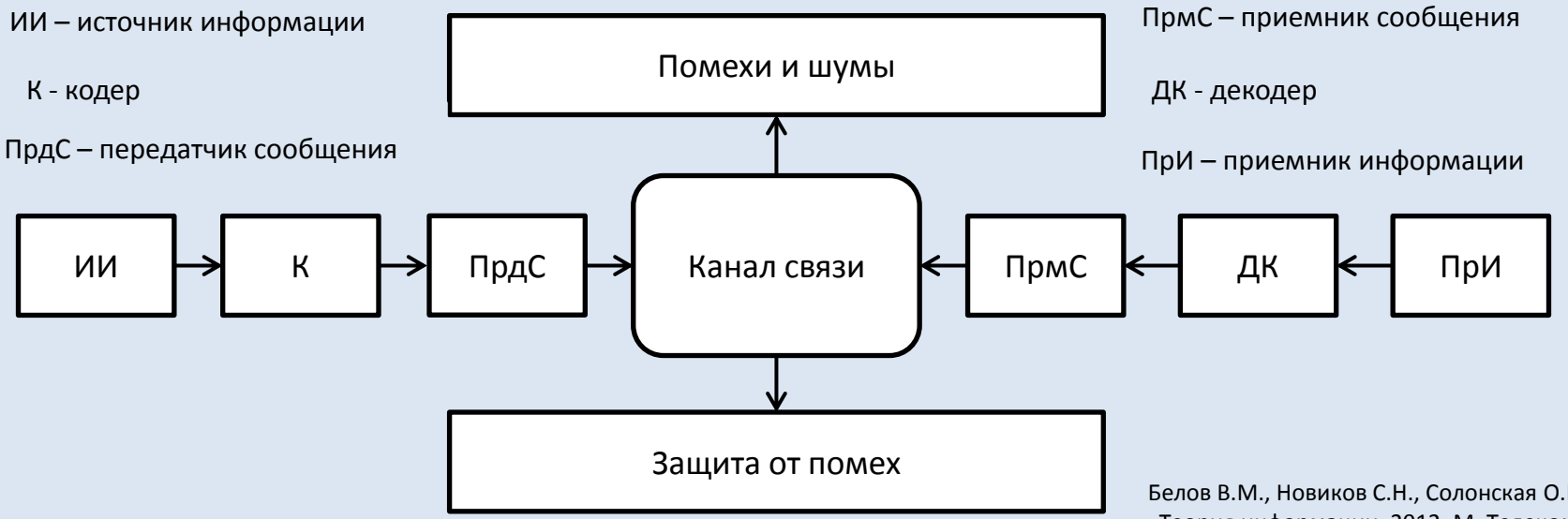
- **Информация это снятая неопределенность наших знаний о чем-либо.**
- **Информация в наиболее общем понимании – это отражение предметного мира с помощью знаков и сигналов.**



Клод Шеннон(1916-2001) – основатель теории информации

БАЗОВЫЕ ПОНЯТИЯ ТЕОРИИ ИНФОРМАЦИИ

Схема передачи информации



Белов В.М., Новиков С.Н., Солонская О.И. Теория информации. 2012. М. Телеком

Канал связи – это среда передачи информации, которая характеризуется в первую очередь максимально возможной для нее скоростью передачи данных емкостью канала связи).

Шум – это помехи в канале связи при передаче информации.

Кодирование – преобразование дискретной информации одним из следующих способов: шифрование, сжатие, защита от шума.

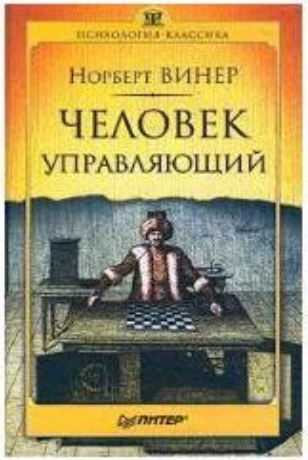
КИБЕРНЕТИКА

- **Информация есть информация, а не материя и не энергия.**

Норберт Винер, Кибернетика, М., 1968 г., «Наука», с. 201.

- **Информация — это обозначение содержания, полученное нами из внешнего мира, в процессе приспосабливания к нему нас и наших чувств.**

Норберт Винер (1894-1964)-
основатель кибернетики

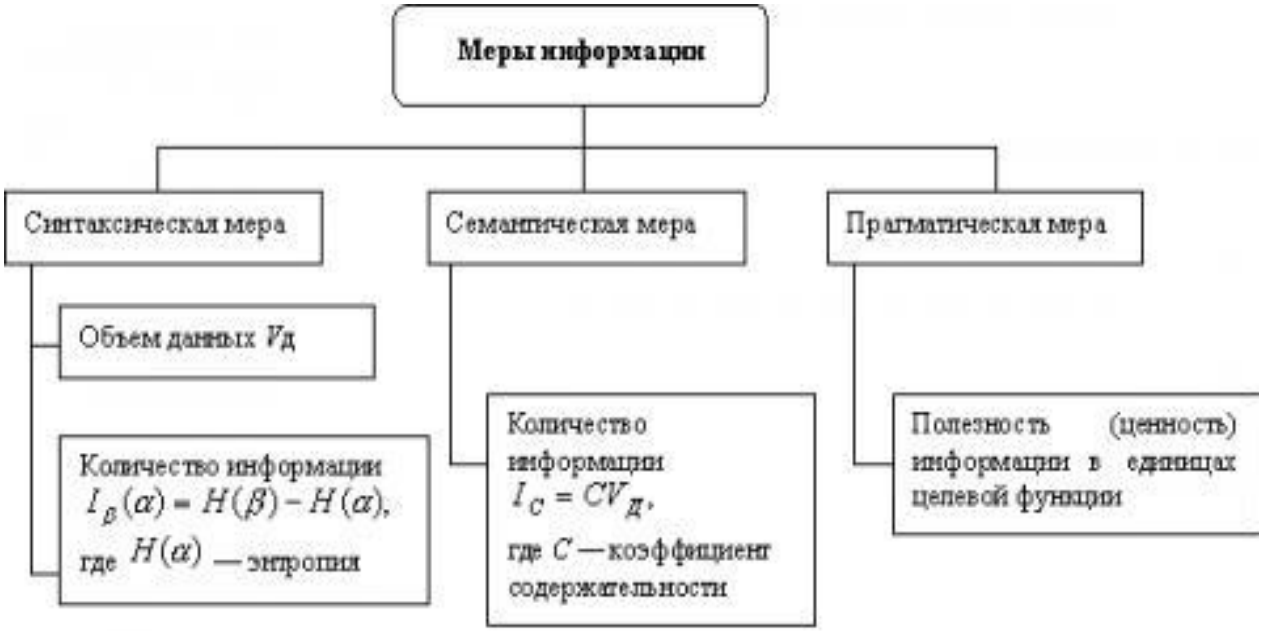


ИНФОРМАЦИЯ В КИБЕРНЕТИКЕ

- **используется для описания процессов управления в живых организмах или технических устройствах**

- **процессы управления включают в себя получение, хранение, преобразование и передачу информации**

РОЛЬ ИНФОРМАЦИИ В КИБЕРНЕТИКЕ



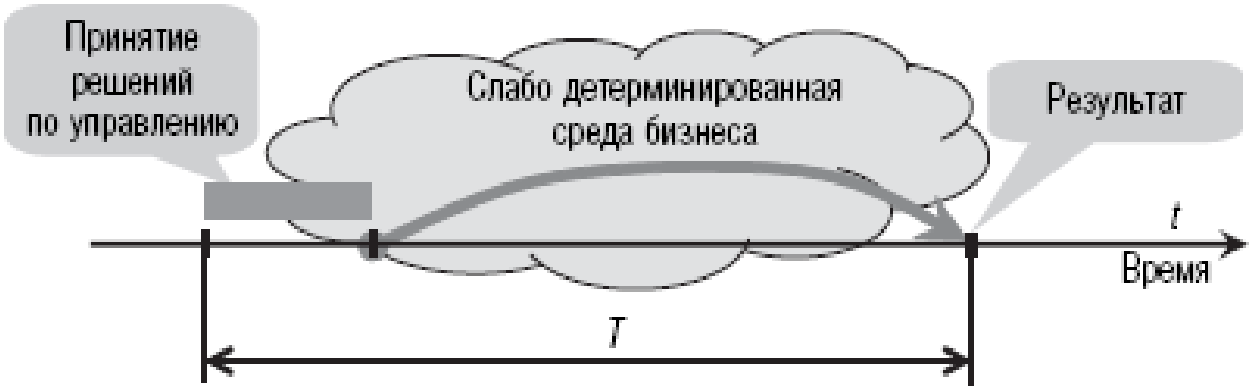
"Лучшей материальной моделью кошки является другая, а желательно, та же самая кошка."

Норберт Винер «Философия науки»

ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ

При информационном взаимодействии приемник получает информацию, а источник не теряет её. Информационное взаимодействие несимметрично.

ИНФОРМАЦИОННАЯ СУЩНОСТЬ БИЗНЕСА



- **Будет ли достигнута цель в том виде, как предполагается?**
- **Достаточно ли в нашем распоряжении операционных возможностей, знаний (опыта), соответствует ли потребностям качество подготовки персонала и система менеджмента?**
- **Достаточно ли привлечено ресурсов для достижения поставленной цели?**
- **Достаточен ли интервал времени, устанавливаемый для достижения цели?**

КАЧЕСТВО И УРОВНИ ИНФОРМАЦИИ В БИЗНЕСЕ

ТРЕБОВАНИЯ:

полезность
доступность
объективность
актуальность
полнота
согласованность
достоверность
релевантность
понятность
защищенность

ТОП-МЕНЕДЖМЕНТ

МЕНЕДЖМЕНТ БИЗНЕС-НАПРАВЛЕНИЙ

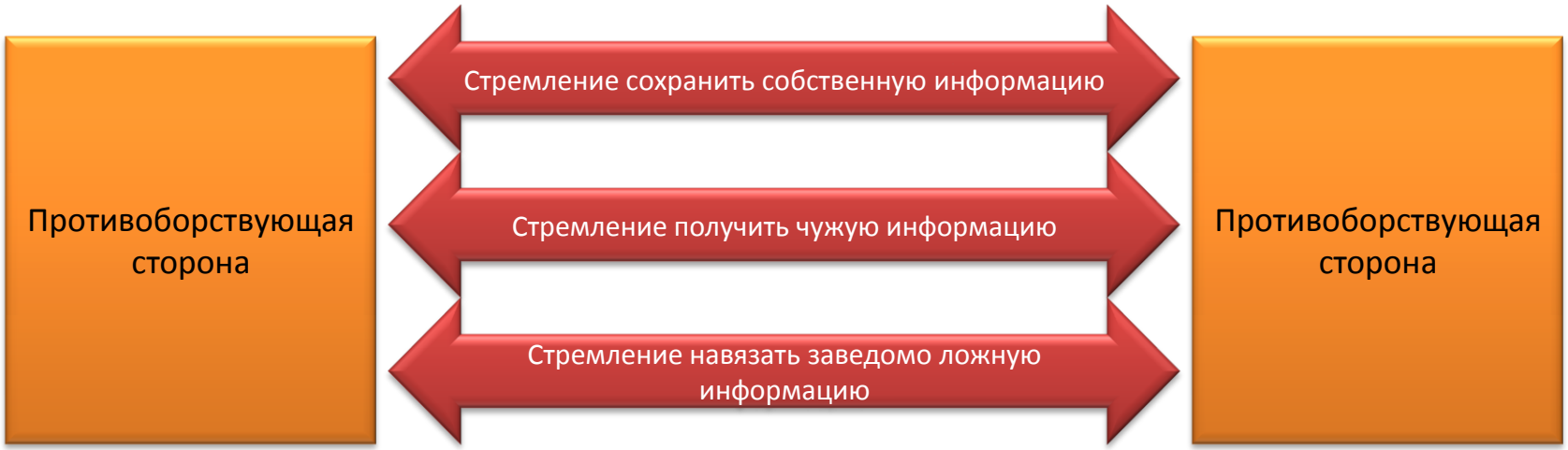
РУКОВОДСТВО СЛУЖБ, ПОДРАЗДЕЛЕНИЙ

ПЕРСОНАЛ

УЯЗВИМОСТИ ПРОЦЕССОВ НАКОПЛЕНИЯ ЗНАНИЙ

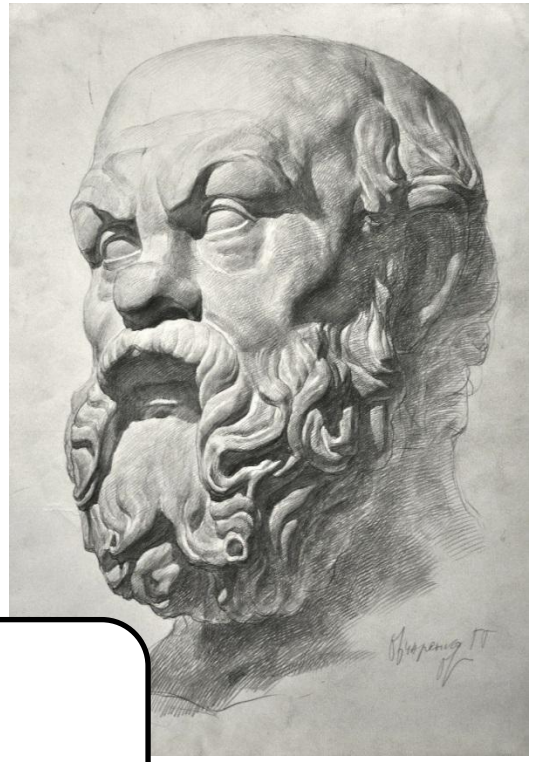
Структура информационной сферы организации

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ



Информационное противоборство – главный инструмент выживания в конкурентной борьбе

Под *информационной безопасностью организации* понимается состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере.



Сократ, мудрец

Угроза разглашения защищаемой информации

Под разглашением защищаемой информации понимается противоправное предание огласке сведений ограниченного доступа посторонним лицом.

При этом посторонним лицом считается любое лицо, которое по характеру служебных обязанностей или выполняемой работы не имеет доступа к защищаемой информации.

Основные группы факторов и предпосылок, которые влияют на разглашение сведений ограниченного доступа

Примеры

ДЕЛО «ЯНДЕКСА», *декабрь 2015 г.*

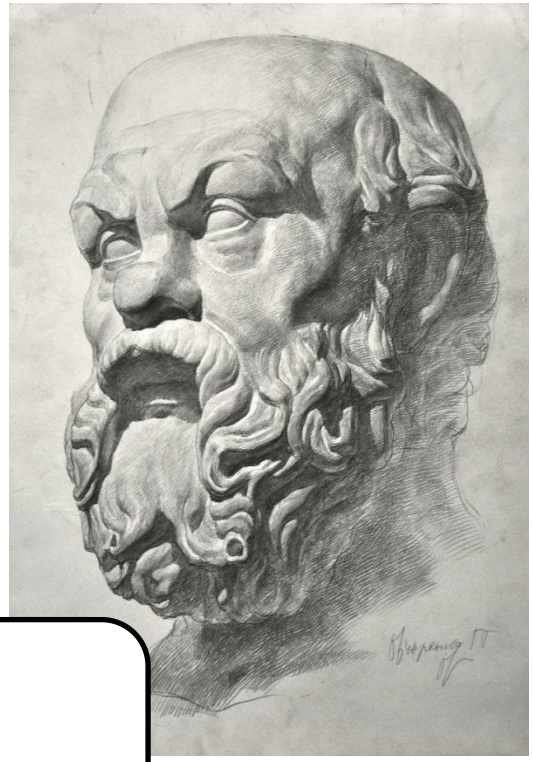
По данным РИА Новости: *Бывший сотрудник «Яндекса» получил 2 года условно за кражу исходного кода и алгоритмов Яндекс-поиска. По данным следствия, злоумышленник скопировал с сервера компании программу «Аркадия», которая содержала код и исходные алгоритмы поисковика. В Яндексе утверждают, что стоимость похищенных данных составляет* ***несколько миллиардов рублей****.*

Опрошенные изданием эксперты полагают, что исходные коды "Яндекса" могли бы быть интересны любому рекламодателю - зная алгоритм формирования поисковой выдачи, они могли бы сделать так, чтобы их сайты всегда попадали на первые строчки в поиске.

ПАДЕНИЕ «TWITTER»

По данным РБК: *Утечка квартальной отчетности Twitter спровоцировала падение акций компании. Финансовые результаты Twitter раньше других опубликованы службой финансовой разведки Selerity (в твиттер-аккаунте). Оборот сервиса микроблогов оказался меньше ожидаемого – $436 млн против $456 млн. После чего и началось падение Twitter. К закрытию торгов акции Twitter подешевели на 18%.*

Это самое значительное падение акций сервиса микроблогов с октября 2014 года.

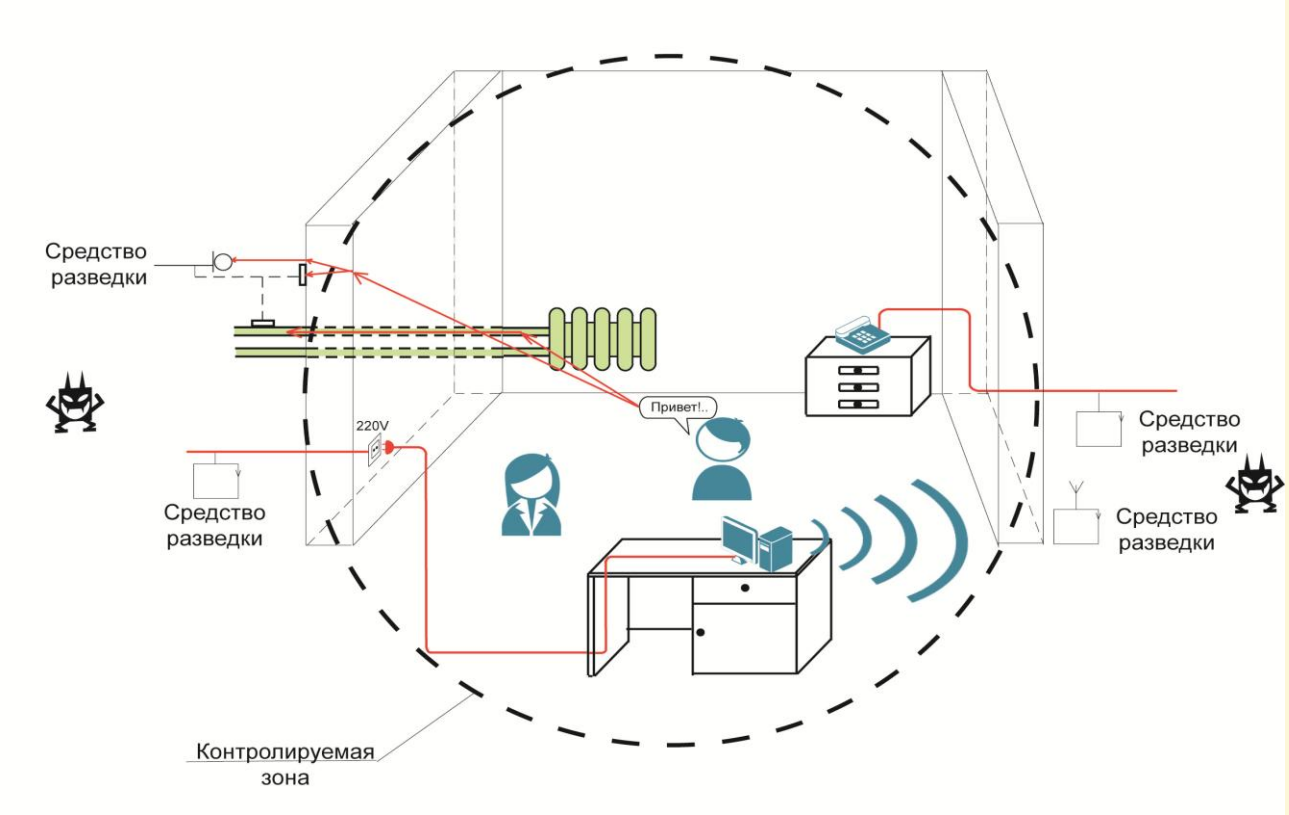


Сократ, мудрец

Угроза перехватов каналов связи и компрометации шифров

Перехват информации – это неправомерное получение данных с использованием технических средств, которое осуществляет поиск, прием и обработку информативных сигналов, то есть, сигналов, по параметрам которых можно восстановить защищаемую информацию.

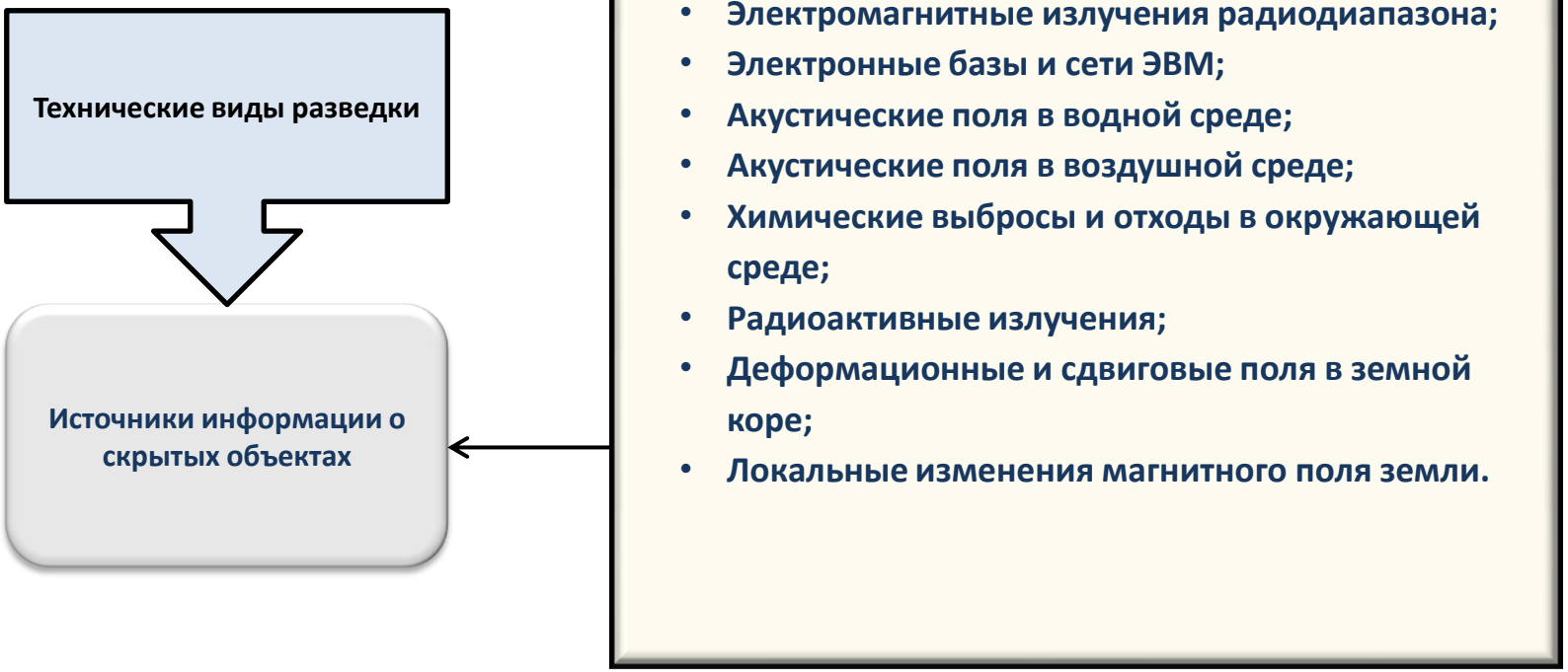
Неконтролируемое носителем защищаемой информации распространение информации через физическую среду до технического устройства, которое осуществляет перехват информации, называется *утечкой* информации по техническому каналу



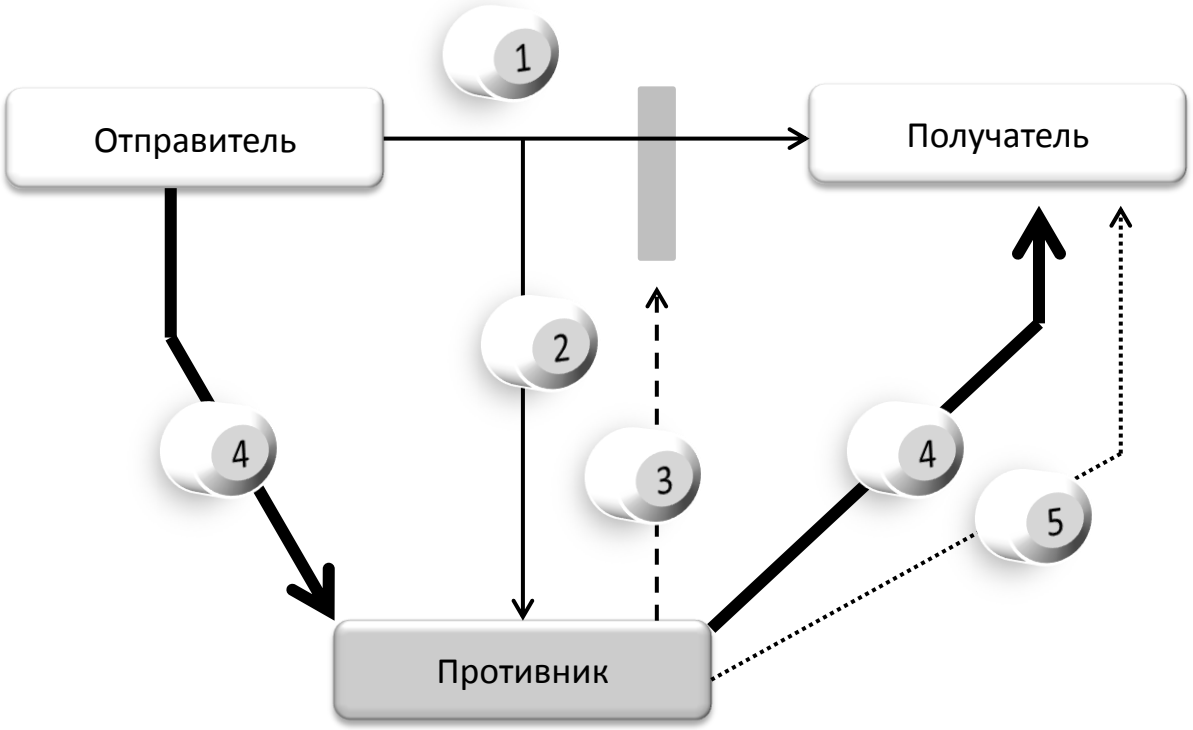
Механизм возникновения каналов утечки информации за пределы контролируемой зоны

ИНФОРМАЦИОННЫЕ ФИЗИЧЕСКИЕ ПОЛЯ

(ПО МЕНЬШАКОВУ Ю.К.)

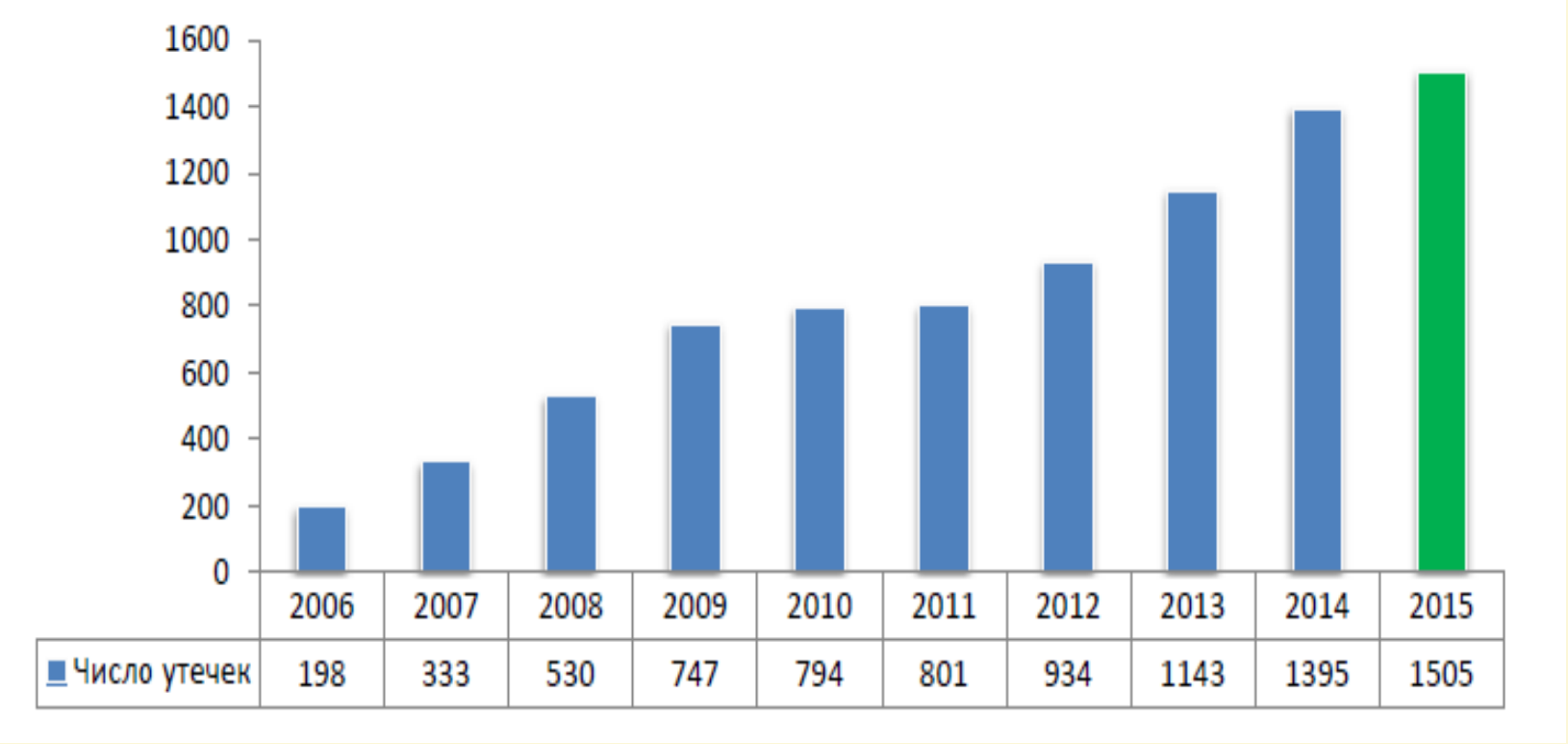


КЛАССИФИКАЦИЯ ПОМЕХ В ВИДЕ СЕТЕВЫХ АТАК
(ПО ЛАПОНИНОЙ О.Р.)



1. **Штатный информационный поток между абонентами (отправитель-получатель);**
2. **Пассивная атака – простой съем информации;**
3. **Активная атака – отказ в обслуживании (DoS-атака, Denial of Service);**
4. **Активная атака – модификация потока данных (man in the middle);**
5. **Активная атака – создание ложного потока данных (фальсификация).**

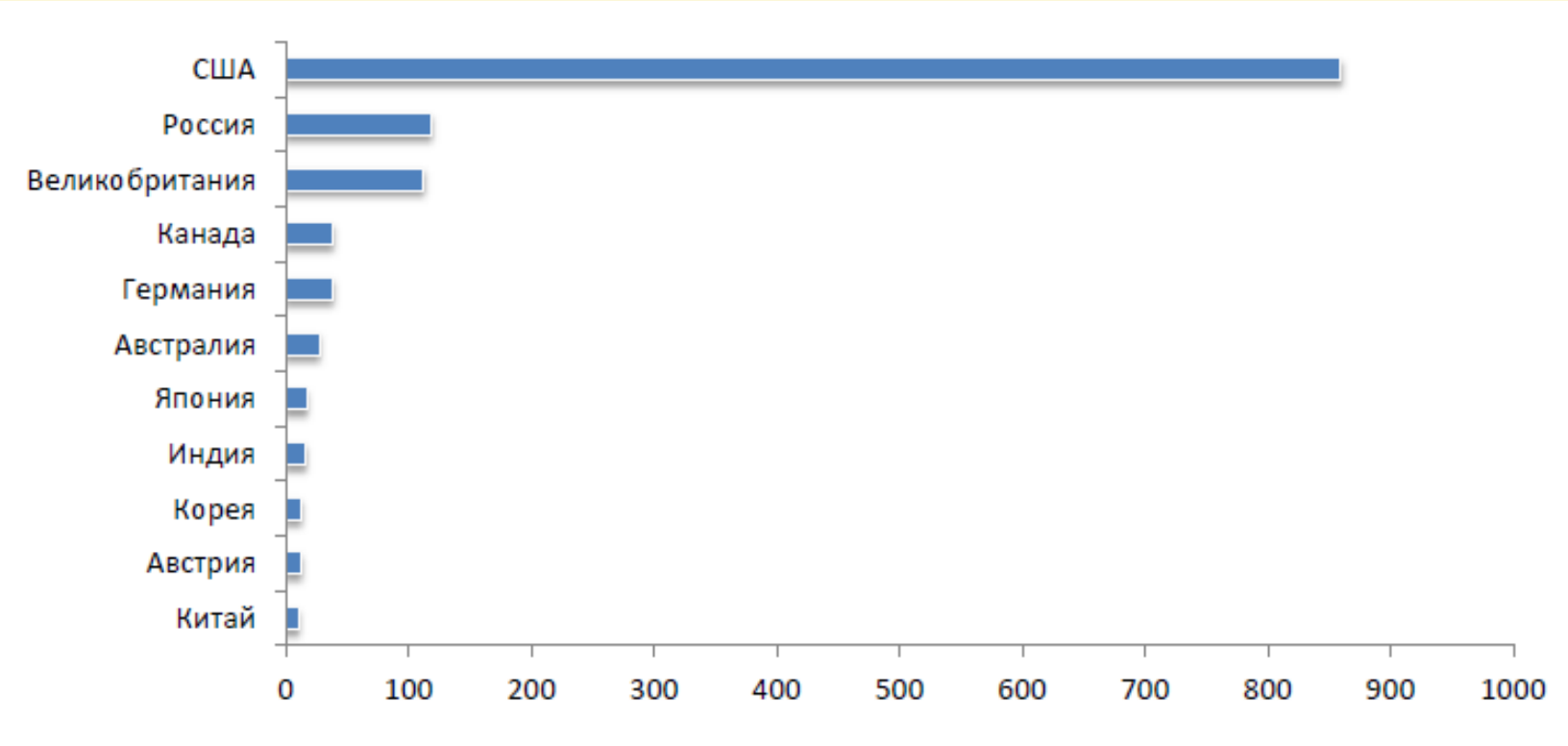
ЧИСЛО ЗАРЕГИСТРИРОВАННЫХ УТЕЧЕК ИНФОРМАЦИИ, 2006 -2015 ГГ.



	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Число утечек	198	333	530	747	794	801	934	1143	1395	1505

По данным Аналитического центра InfoWatch

РАСПРЕДЕЛЕНИЕ ЧИСЛА УТЕЧЕК ПО СТРАНАМ В 2015 ГГ.



По данным Аналитического центра InfoWatch

Пример

КОМПРОМЕТАЦИЯ ЛИЧНЫХ ДАННЫХ 154 МЛН. АМЕРИКАНСКИХ ИЗБИРАТЕЛЕЙ

июнь 2016 г.

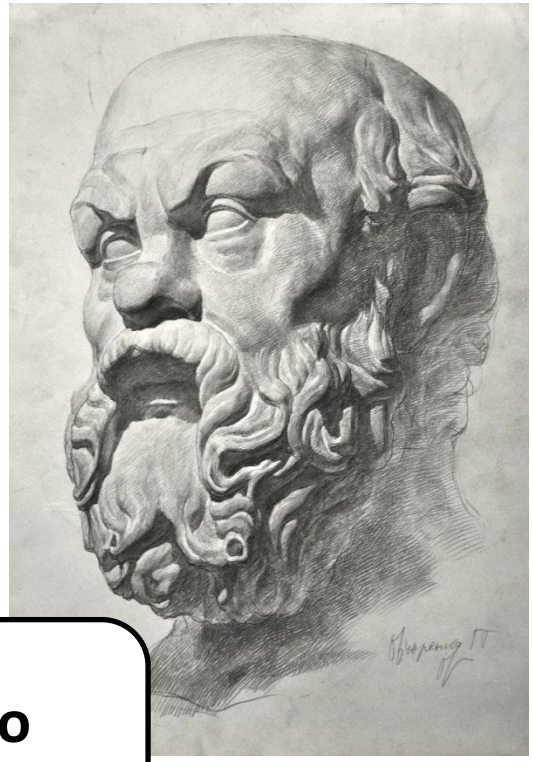
По данным РБК:

Утечку обнаружил тот же исследователь Крис Викери (Chris Vickery) из MacKeeper, что и в декабре 2015 г. На одном из серверов в облаке Google была обнаружена некорректно настроенная база CouchDB.

В открытом доступе оказались личные данные 154 миллионов американских избирателей. База содержала имена, адреса проживания, телефоны, email-адреса, возраст, пол, политические предпочтения, информацию о владении оружием, национальность, информацию об участии в предыдущих выборах и ссылку на профиль в Facebook.

Исследователи предположили, что утечка могла произойти по вине компании **L2**, специализирующейся на утилизации подобных данных. Викери связался с представителями этой компании и сообщил им об утечке. Через несколько часов доступ к базе данных был закрыт.

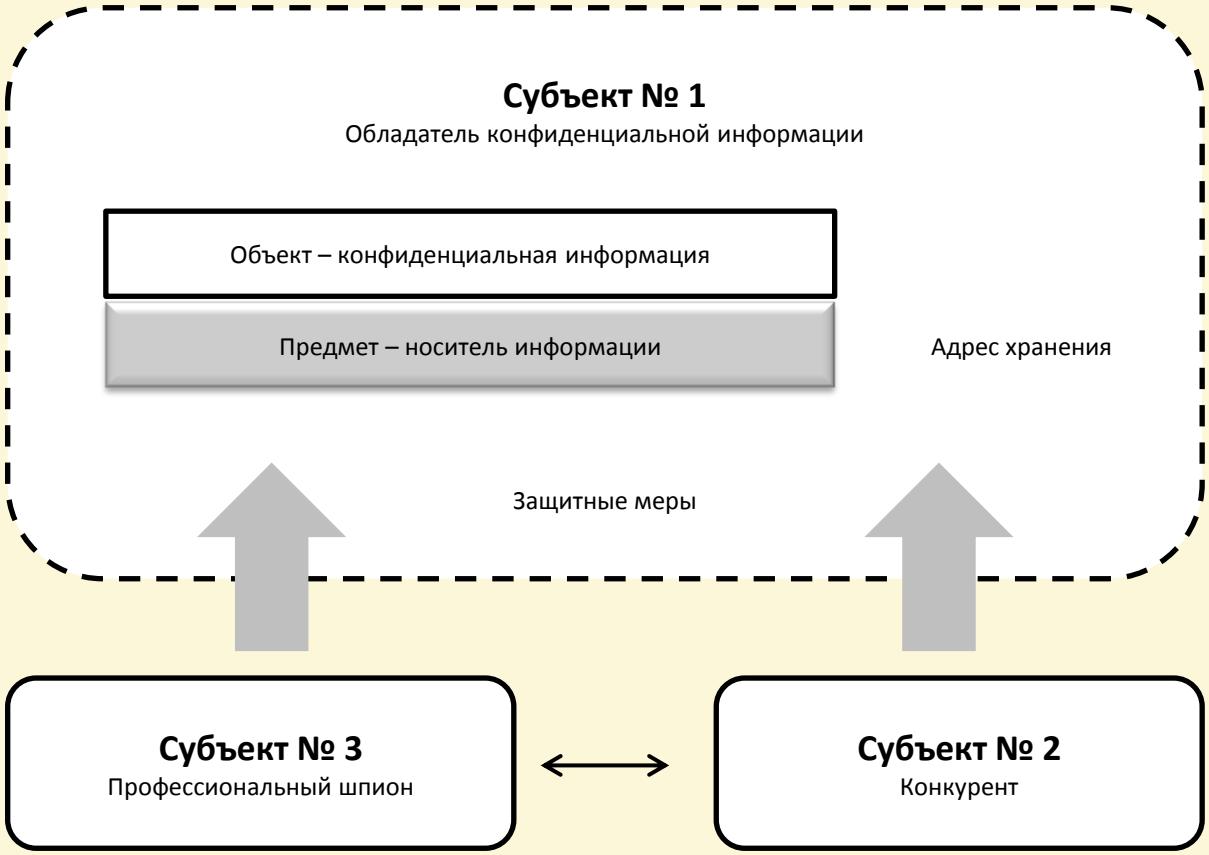
В настоящий момент неизвестно, кто именно допустил утечку и кто, кроме Викери, заполучил доступ к этим данным.



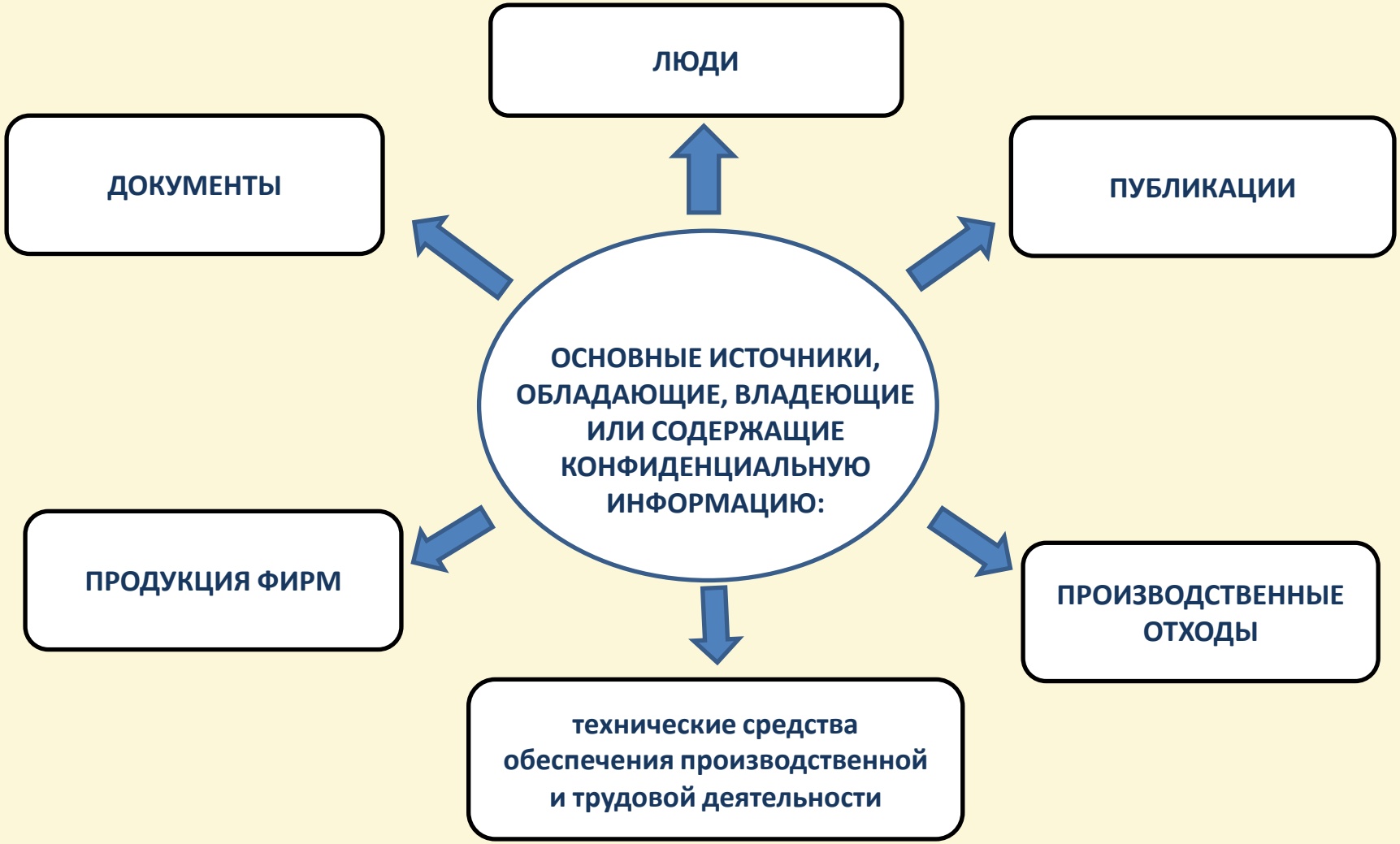
Сократ, мудрец

Угроза осуществления промышленного шпионажа

Промышленный шпионаж — это форма недобросовестной конкуренции, базирующаяся на незаконном получении, использовании и разглашении данных, которые составляют коммерческую, служебную или другую охраняемую законом тайну с целью получения преимуществ для осуществления предпринимательской деятельности.



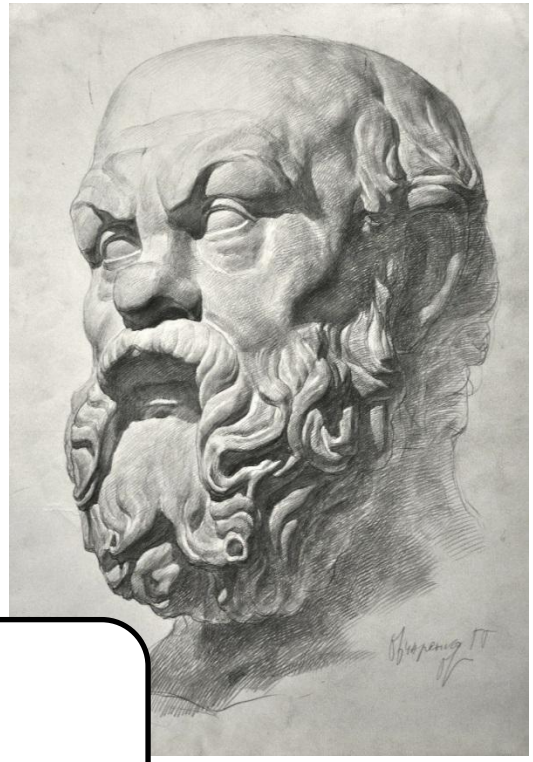
Принципиальная схема промышленного шпионажа



Опрос, проведенный Американским Сообществом Промышленной Безопасности среди 138 компаний, продемонстрировал, что за 2014 год только они потеряли 53 млрд. долларов из-за утечек информации. При этом кражи осуществлялись *БЕЗ ПРИВЛЕЧЕНИЯ ХАКЕРОВ И ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ.*

ОСНОВНЫЕ СПОСОБЫ ПРОМЫШЛЕННОГО ШПИОНАЖА

- 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.

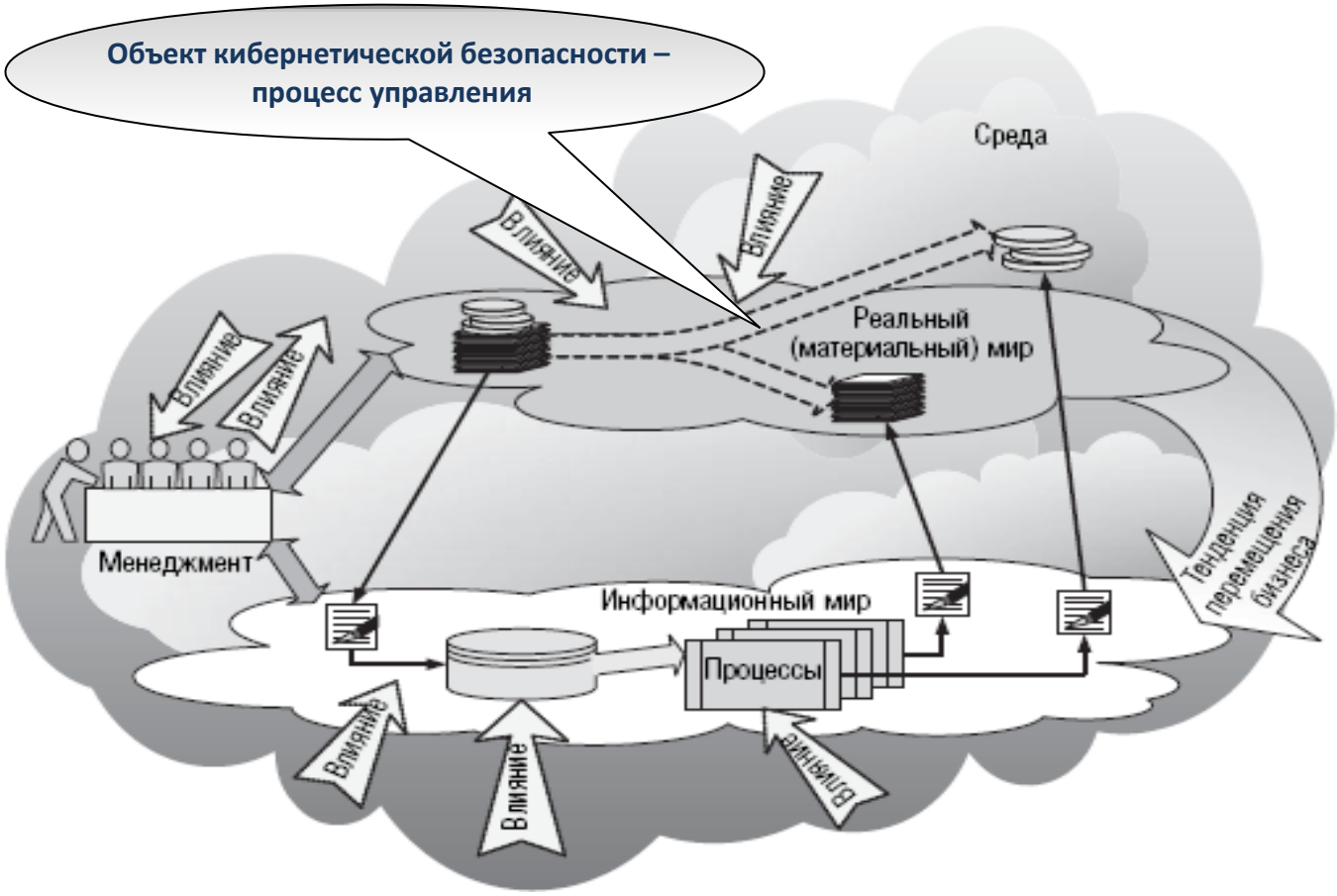


Сократ, мудрец

Угроза нарушения нормальной жизнедеятельности предприятия

КИБЕРНЕТИЧЕСКИЕ УГРОЗЫ

явления, деяния, условия, факторы, представляющие опасность для информации управления, инфраструктуры управления, субъектов управления и порядка управления.



Деформация бизнеса через инциденты в информационной сфере

ПОНЯТИЕ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

Основные объекты воздействия информационно-ударных группировок сил и средств информационного противоборства

- Программное и информационное обеспечение
- Программно-аппаратные, телекоммуникационные и другие средства информации и управления
- Каналы связи, обеспечивающие циркуляцию информационных потоков и интеграцию системы управления
- Интеллект человека и массовое сознание

АКТУАЛЬНЫЕ ТИПЫ КИБЕРУГРОЗ

ИЗМЕНЕНИЯ СРЕДЫ ВЕДЕНИЯ БИЗНЕСА

Мобильность

Совместная работа

Виртуализация и облака

Причины появления новых угроз

ЭВОЛЮЦИЯ КИБЕРУГРОЗ

ЭВОЛЮЦИЯ ТАКТИКИ РЕАЛИЗАЦИИ КИБЕРУГРОЗ

СМЕНА ЛАНДШАФТА КИБЕРУГРОЗ

УГРОЗЫ СЕГОДНЯ

Устойчивые, сложные, мутирующие

Каждый экземпляр атаки может отличаться от другого

Домены меняются ежедневно, даже ежечасно

Контент мутирует и маскируется под легальный трафик

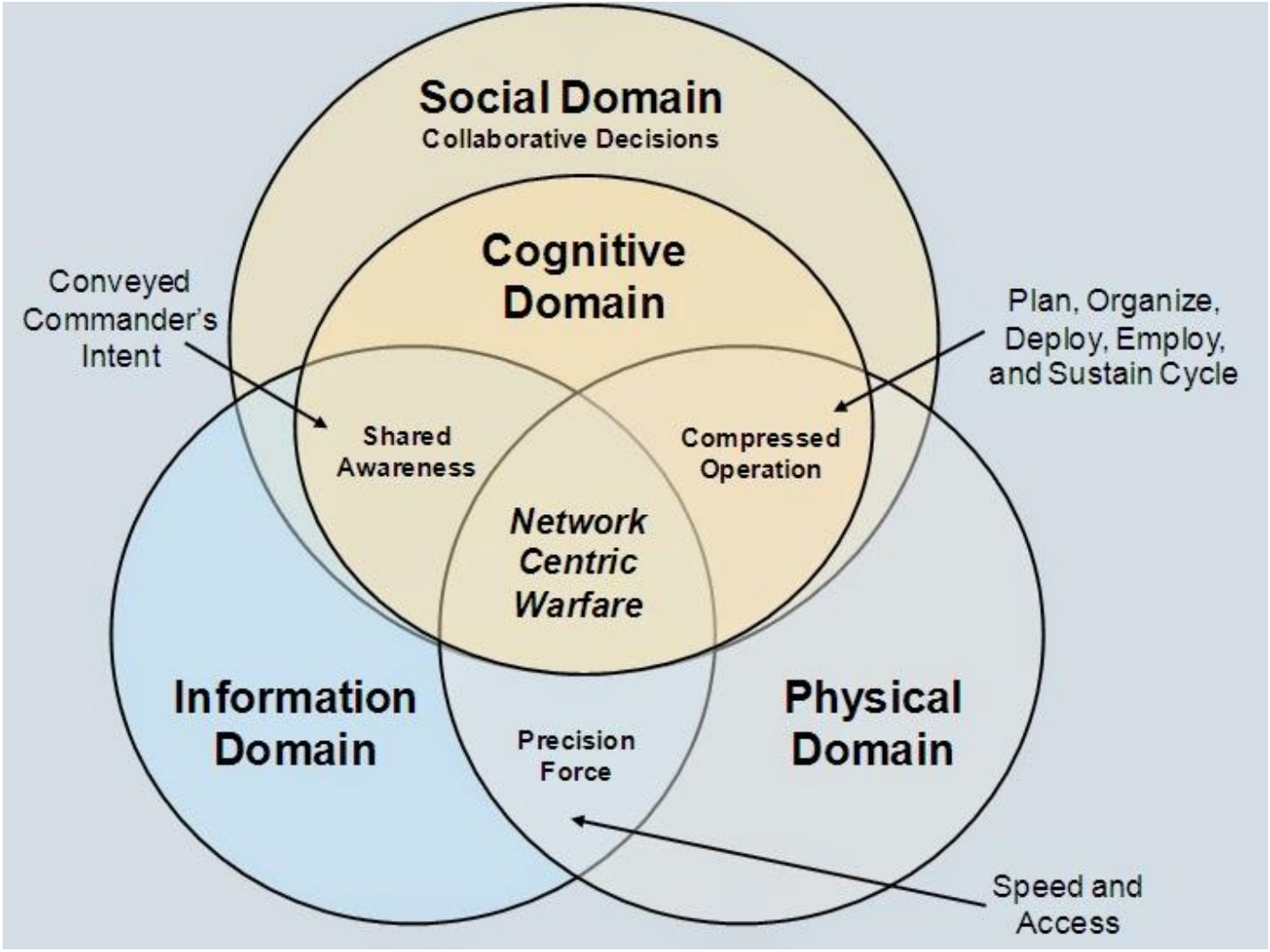
80% спама исходит от инцифицированных клиентов

70% «зомби» используют динамические IP-адреса

Угрозы из легальных доменов растут на сотни процентов в год

Спам составляет более 180 миллиардов сообщений в день

ОСНОВНЫЕ СОСТАВЛЯЮЩИЕ СЕТЕЦЕНТРИЧЕСКОГО ПРОТИВОБОРСТВА



Пример

КИБЕРАТАКИ В ДОБЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ

В апреле и мае 2015 года канадская золотодобывающая компания Detour Gold Corp. подверглась атаке хакерской группировки, которая называла себя Angels_Of_Truth. В результате злоумышленниками было украдено более 100 Гб ценной информации. При этом 18 Гб из этих данных были размещены на торрент-трекере.

В апреле 2016 года в канадской золотодобывающей компании Gold Corp. произошла крупная утечка данных. Злоумышленники обнародовали 14.8 Гб данных, разместив соответствующий документ на Pastebin, популярном сайте для хранения и общего использования данных, с ссылкой на его скачивание. Архив содержал персональные данные работников и финансовую информацию.

Кибератаки в промышленности совершаются, в основном, для получения определенных технических знаний в достижении конкурентного преимущества, ослабления экономики другого государства, получения определённых данных (личную информацию (PII), финансовую составляющую или учетные записи) или даже с целью протеста против компаний, как источника загрязнения окружающей среды. Они не только могут быть причиной потерь из-за простоев на производстве, но оказать негативное влияние на стоимость акций компании, нанести ущерб экономике страны или региона, если она зависит от подобного предприятия.

Кейс

ФАЛЬШИВЫЙ ТВИТ О РАНЕНИИ Б.ОБАМЫ

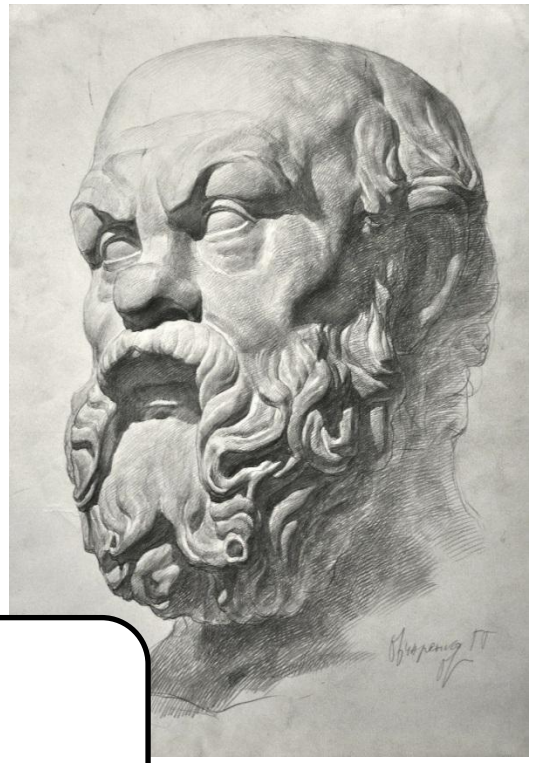
23 апреля 2013 г. сирийские хакеры взломали **Twitter-аккаунт** агентства **Associated Press** и сообщили об атаке на Белый дом, в результате которой оказалась в опасности жизнь президента США. Опровержение последовало через несколько минут, но новость успели подхватить многие новостные медиа.

В результате действий хакеров фондовый рынок США кратковременно зафиксировал потерю около 1,5% своей капитализации. В абсолютном выражении для компаний, входящих в широкий индекс ***S&P 500***, это означало падение рыночной стоимости на сумму около 136,5 млрд долл.

Ответственность за резкое проседание рынка участники биржи возложили на автоматизированные системы ведения торгов, которые подчинялись алгоритмам, и начали экстренную распродажу активов. В настоящее время пересмотрены правила автоматизированной торговли с точки зрения скорости ведения электронных торгов.

Вопрос: *возможна ли такая реакция на информацию в технологических системах*.

Библиография



Сократ, мудрец

Основная литература

1. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Безопасность предпринимательской деятельности. М.: Издательство «Юрайт», 2016;
2. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Пособие для обучения на майноре. (на начальном этапе)

Дополнительная литература

1. Обеспечение информационной безопасности бизнеса. *Под редакцией Курило А.П.* М.: Альпина, 2011. ;
2. Хэл Абельсон и др. Атака битов: твоя жизнь, свобода и благополучие в цифровую эпоху. С-П, «Символ-Плюс», 2009;
3. Глобальное исследование утечек конфиденциальной информации в 2015 году. Аналитический центр InfoWatch, www.infowatch.ru/analytics

Нормативные акты

ФЗ от 27 июля 2006 г. 149-ФЗ «Об информации, информационных технологиях и о защите информации».