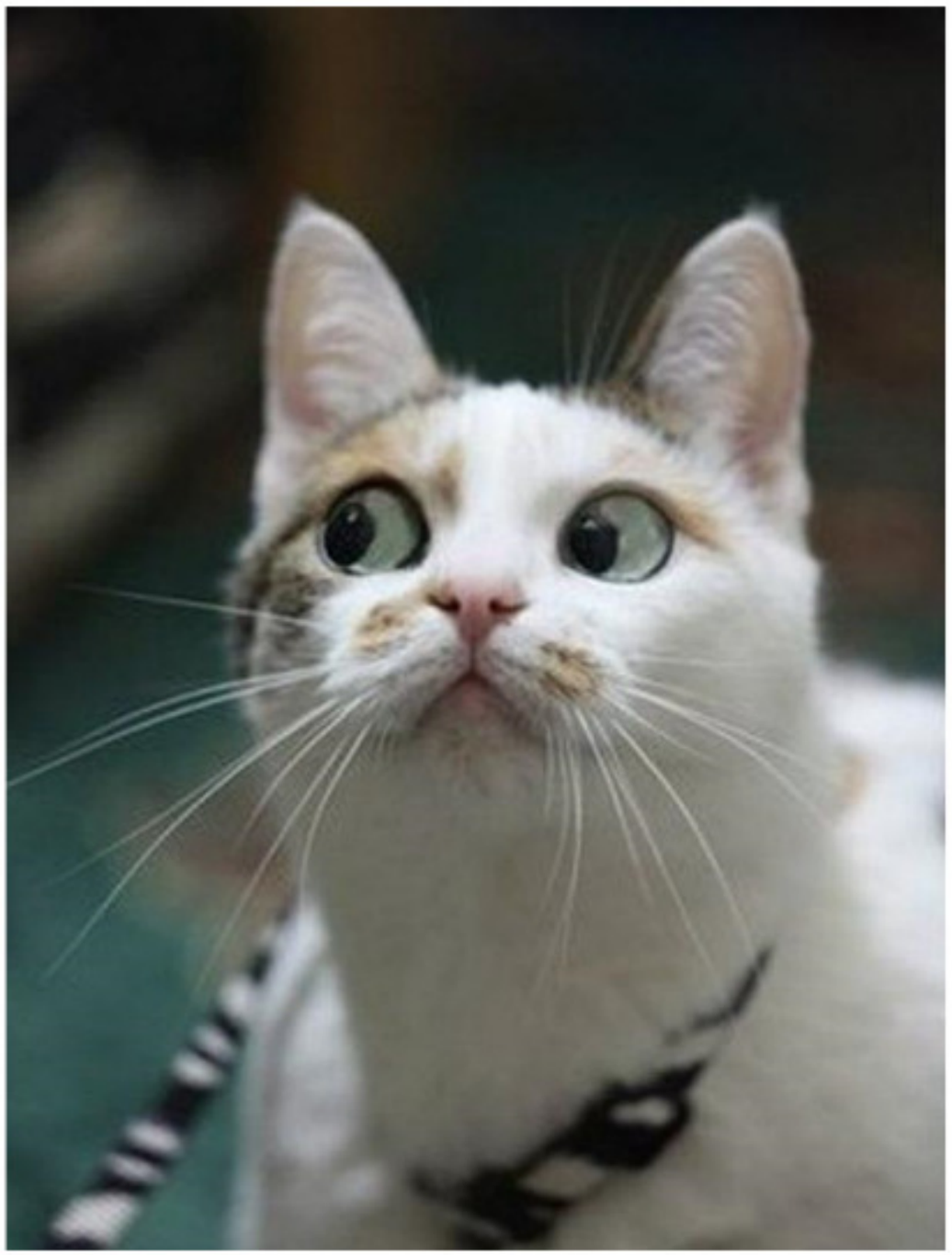
# Теория информационной безопасности и методология

Лекция 2

к.т.н., доцент факультета БИТ
Коржук Виктория Михайловна
vmkorzhuk@itmo.ru

весенний семестр
2023

# Предыдущая лекция



- Информационная безопасность
- Конфиденциальность, целостность, доступность
- Уязвимости, угрозы, атаки
- Виды информации ограниченного доступа
- Субъекты и объекты
- Несанкционированный доступ
- Нарушитель ИБ, потенциал нарушителя

https://www.youtube.com/embed/MDDoAEHd8o4

# Пример хакерской атаки

Вспомните/найдите в интернете еще один пример хакерской атаки

Instructions

Collaborate Board

## Пример хакерской атаки

# Задача оценки угроз

1. обоснование структуры и содержания системы показателей уязвимости информации;

2. обоснование структуры и содержания параметров, влияющих на показатели;

3. разработка комплексов моделей зависимости показателей от параметров, позволяющих определять значения всех необходимых показателей во всех состояниях и условиях системы;

4. разработка методологии использования моделей при исследованиях и практическом решении различных вопросов защиты, или иначе — разработка методологии оценки уязвимости информации.

# Система показателей уязвимости информации

Как вы считаете, что включают в себя "показатели уязвимости информации"?

Collaborate!

Система показателей уязвимости информации

# Показатели уязвимости информации

=

количество угроз

+

количество нарушителей

+

количество компонентов системы

| | |
|---|---|
| экстремальный | самый слабый к[illegible] самая [illegible]троза, [illegible]мый сильный [illegible] |
| | компонента при однократном проявлении одной угрозы со стороны одного злоумышленника |

# Matching Pairs

# Показатели уязвимости информации

Подумайте и приведите пример одного из показателей уязвимости информации

Collaborate!

Показатели уязвимости информации

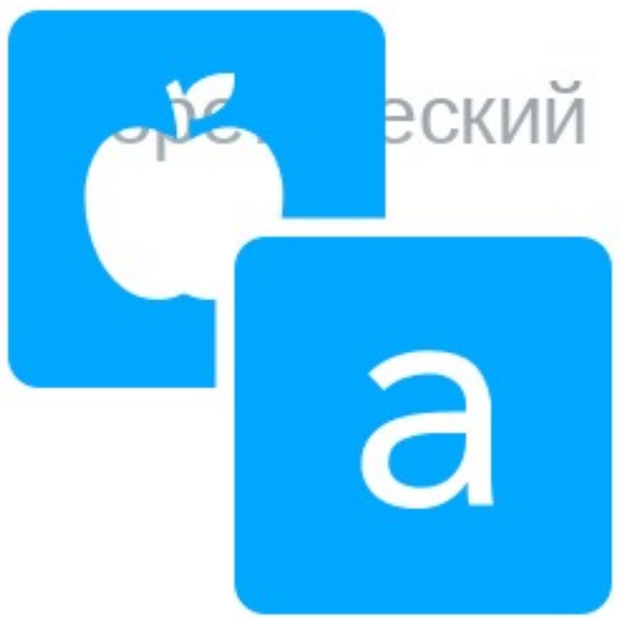
# Подходы к оценке уязвимости информации

1. эмпирический

2. теоретический

3. теоретико-эмпирический

длительный сбор и обработка данных о реальных атаках



законов распределения для построения строгих зависимостей

# Matching Pairs

# Определение требований по защите информации

## Вероятность защищенности информации

должна быть выше или равна

требуемому уровню защищенности.

# Poll

Как вы считаете, какой фактор является наиболее важным при определении требований к защите?

- характер обрабатываемой информации
- объем обрабатываемой информации
- продолжительность прибывания информации в системе
- структура системы
- вид защищаемой информации
- технология обработки информации
- организационные установки в системе
- этап жизненного цикла системы

# Рекомендации по предъявлению требований к защите информации

Конкр ебования к защите, обусловленные спецификой автом ботки информации, определяются совокупностью сл

*ваемой информации;*
*ой информации;*
*ребывания информации в АСОД;*

*ормации;*
*ки информации;*
*мационно-воспитательного процесса в АСОД;*
*го цикла АСОД.*

***По*** (с точки зрения требуемой защиты) информацию можно разделить на **общедоступную, конфиденциальную, служебную, секретную и совершенно секретную.**

Соответствующие рекомендации по предъявлению требований к защите могут быть



защиты от несанкционированного доступа не требуется.

2.Требования к защите **конфиденциальной** информации определяет пользователь, устанавливающий статус конфиденциальности.

3.При обработке **служебной** информации к ней должен быть обеспечен

# Оценка защищаемой информации

ресурс

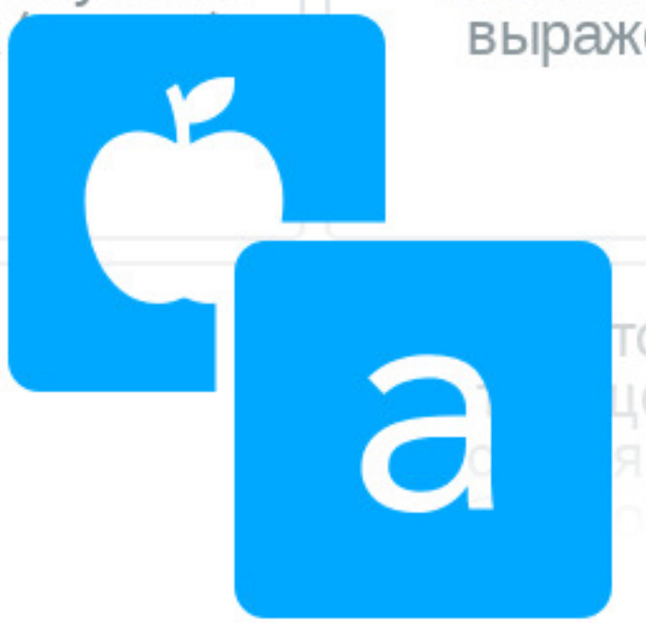
объект труда

толерантность

данных ненужных данных

абсолютном выражении

удобства восприятия и использования ее в процессе решения задач



# Matching Pairs

# Информация как объект труда

Подумайте и опишите, в какой ситуации информация последовательно представляет собой сырье, затем полуфабрикат и, в итоге, продукт обработки

Instructions

Collaborate Board

## Информация как объект труда

https://www.youtube.com/embed/VHfTyBPW4yM

# Про оценку важности

важность решаемой задачи

важность информации для решения задачи

# Пример оценки важности информации

**Оцените важность информации на двух примерах из литературы**

Collaborate Board

Пример оценки важности информации

# Про оценку полноты и релевантности

Полнота - достаточность информации для решения задачи

Релевантность - соответствие нуждам для решения задачи

# Quiz

Соответствие информации потребностям решаемой задачи - это...

- важность
- релевантность
- адекватность
- актуальность
- полнота

Показатель достаточности информации для решения какой-либо задачи - это...

- важность
- полнота
- актуальность
- толерантность

Какой показатель оценивается объективностью генерирования информации с учетом времени?

- чистота
- актуальность
- адекватность
- полнота
- важность

Какие коэффициенты важности входят в оценку важности информации?

- задач
- информации для эффективного решения задач
- информации с точки зрения потерь при нарушении КЦД
- информации с точки зрения восстановления ее КЦД
- рисков

Отсутствие шумов среди необходимых данных - это...

- чистота
- ясность
- достоверность
- адекватность

Форма представления информации с точки зрения удобства и использования - это...

- релевантность
- толерантность
- важность
- достоверность
- целостность

Что вы запомнили? Что нужно будет повторить на следующей лекции? Понятен ли материал?

## Collaborate!

# Exit ticket