


# Математические основы информационной безопасности

Груздев Дмитрий Николаевич

# Искусственный интеллект

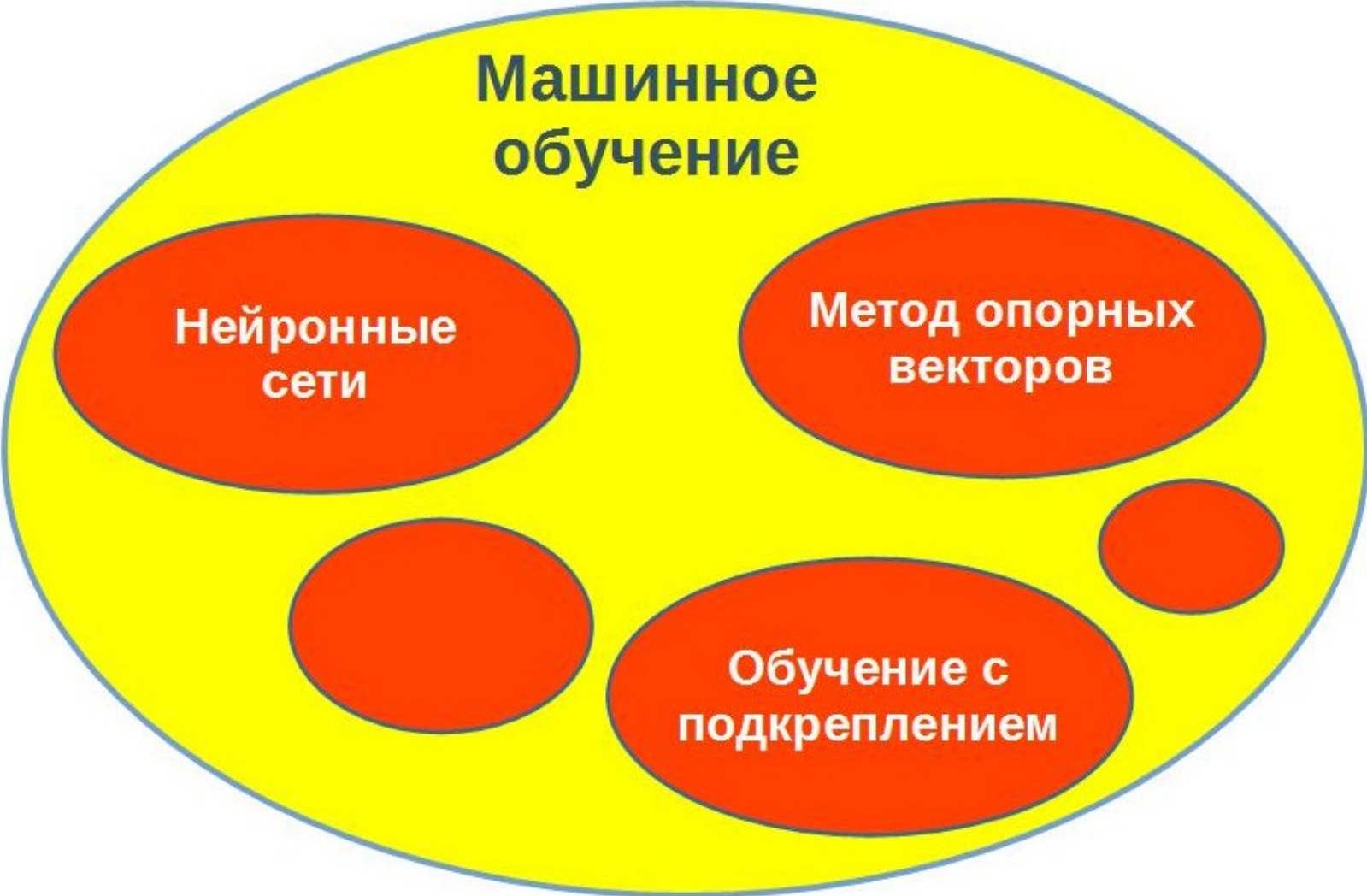
A diagram showing the components of Artificial Intelligence. A large blue oval contains the title 'Искусственный интеллект' at the top. Inside this oval are five yellow ovals: 'Машинное обучение' (top left), 'Экспертные системы' (top right), 'Сеть знаний' (bottom center), and two smaller unlabeled yellow ovals (bottom left and bottom right).

Машинное  
обучение

Экспертные  
системы

Сеть  
знаний

# Машинное обучение



A diagram illustrating the components of Machine Learning. A large yellow oval contains the title 'Машинное обучение' at the top. Inside this oval are five red ovals: 'Нейронные сети' (top left), 'Метод опорных векторов' (top right), 'Обучение с подкреплением' (bottom right), and two unlabeled red ovals (bottom left and middle right).

Нейронные  
сети

Метод опорных  
векторов

Обучение с  
подкреплением

# Машинное обучение

В 1962 г. Артур Самуэль написал самообучающуюся программу игры в шашки, которая обыграла чемпиона штата Коннектикут.



“Компьютерная программа обучается на основе опыта  $E$  по отношению к некоторому классу задач  $T$  и меры качества  $R$ , если **качество решения задач из  $T$ , измеренное на основе  $R$ , улучшается с приобретением опыта  $E$ .**”

Том Митчел

# Анализ данных

- область математики и информатики, занимающаяся построением и исследованием методов и алгоритмов извлечения знаний из экспериментальных данных
- процесс исследования, фильтрации, преобразования и моделирования данных с целью извлечения информации и принятия решений

## Виды анализа данных:

- Описательный – определение основных характеристик данных
- Разведочный – построение графиков, диаграмм
- Индуктивный – расчет статистик, проверка статистических гипотез
- Прогностический – применение экстраполирующих алгоритмов
- Казуальный – определение взаимозависимостей в данных на логическом уровне
- Механистический – глубокое понимание работы системы

# Аналитик данных

- Сбор данных (организует сам или получает задачу).
- Определение параметров набора данных.
- Проведение предварительной обработки.
- Интерпретация данных и решение задачи.
- Выводы и рекомендации для бизнеса.
- Визуализация результатов .



# Признаки объекта

## **Вопрос о выдаче кредита:**

Объект: человек

**Признаки:** пол, возраст, зарплата, количество детей, **размер обуви**

## **Задача об оценке квартиры:**

Объект: квартира

**Признаки:** площадь, этаж, расстояние до метро, наличие школы, кондиционера, **цвет обоев**

## **Анкета на сайте знакомств:**

Объект: человек

**Признаки:** пол, возраст, увлечения, любимые книги, фильмы



# Объекты и признаки

$x_1, x_2, \dots, x_m$  – набор объектов

$x_j^{(1)}, x_j^{(2)}, \dots, x_j^{(n)}$  – признаки  $j$ -го объекта

$x_i = (x_i^{(1)}, x_i^{(2)}, \dots, x_i^{(n)})$

Матрица “объекты-признаки” ( $m = 26, n = 4$ )

Цветок (лепесток)	Длина $x^{(1)}$	Ширина $x^{(2)}$	Цвет $x^{(3)}$	Гладкость $x^{(4)}$
1	12.5	3.2	белый	-
2	8.3	2.4	синий	+
...				
26	9.1	3.3	синий	-

$x_2 = (8.3, 2.4, \text{белый}, +)$

# Объекты и ответы

$x_1, x_2, \dots, x_m$  – набор объектов

$y_1, y_2, \dots, y_m$  – набор ответов (признаки для прогнозирования)

$(x_1, y_1), \dots, (x_m, y_m)$  – пары объект-ответ

Квартира (объект)	Площадь $x^{(1)}$	Этаж $x^{(2)}$	До метро $x^{(3)}$	Школа $x^{(4)}$	Кондиционер $x^{(5)}$	Цена $y$
1	32.5	4	550	-	-	7.2
2	118.3	1	750	+	+	21.5
...						
33	65.1	12	1100	-	+	12.4

# Виды машинного обучения

Алгоритмы машинного обучения:

- Обучение с учителем
- Обучение без учителя

Другие: обучение с подкреплением, системы рекомендаций.

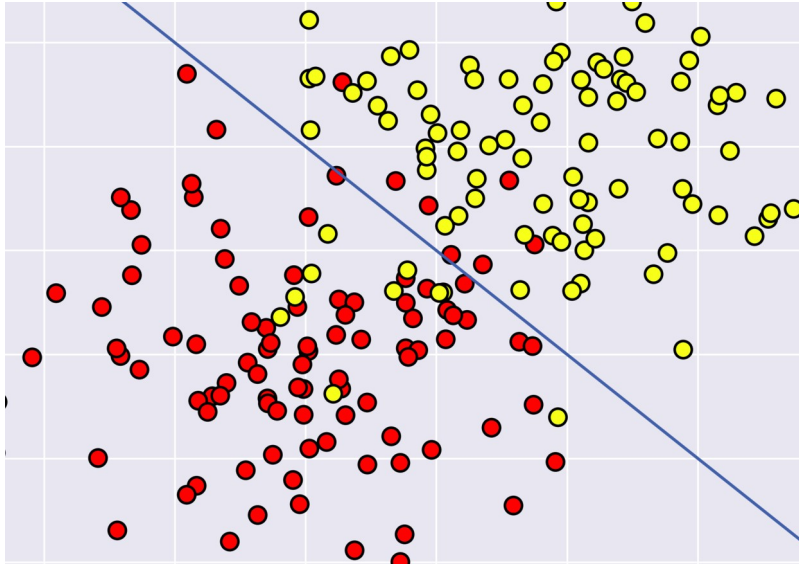
# Обучение с учителем

Построение функциональной зависимости по прецедентам “объект-ответ”. Возможность вычислять ответ для любого объекта.

Задачи:

- классификации
- регрессии
- ранжирования
- прогнозирования

# Классификация

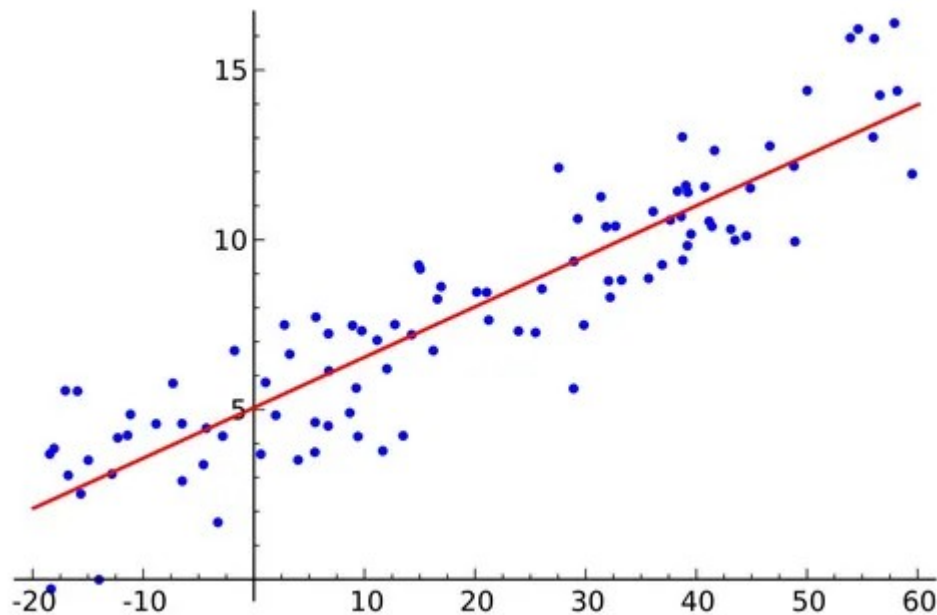


Множество допустимых ответов конечно.

Допустимые ответы называются метками классов.

Класс – множество объектов с одинаковой меткой.

# Регрессия





Допустимым ответом является число или числовой вектор.


# Ранжирование


**Яндекс**  Найти Будьте в Плюсе



Поиск Картинки Видео Карты Маркет Новости Переводчик Эфир Коллекции Кью Услуги Ещё

 **Учение – свет! - Достижение - World of Warcraft**  
[ru.wowhead.com](#) > ?achievement=1956 ▾   
Учение – свет! Прочтите тома "Школы тайной магии", перечисленные ниже. Критерий.  
Школы тайной магии – Введение. Школы тайной магии... [Читать ещё >](#)

**Нашлось 2 млн результатов**  
32 тыс. показов в месяц  
[Дать объявление](#) [Показать все](#)

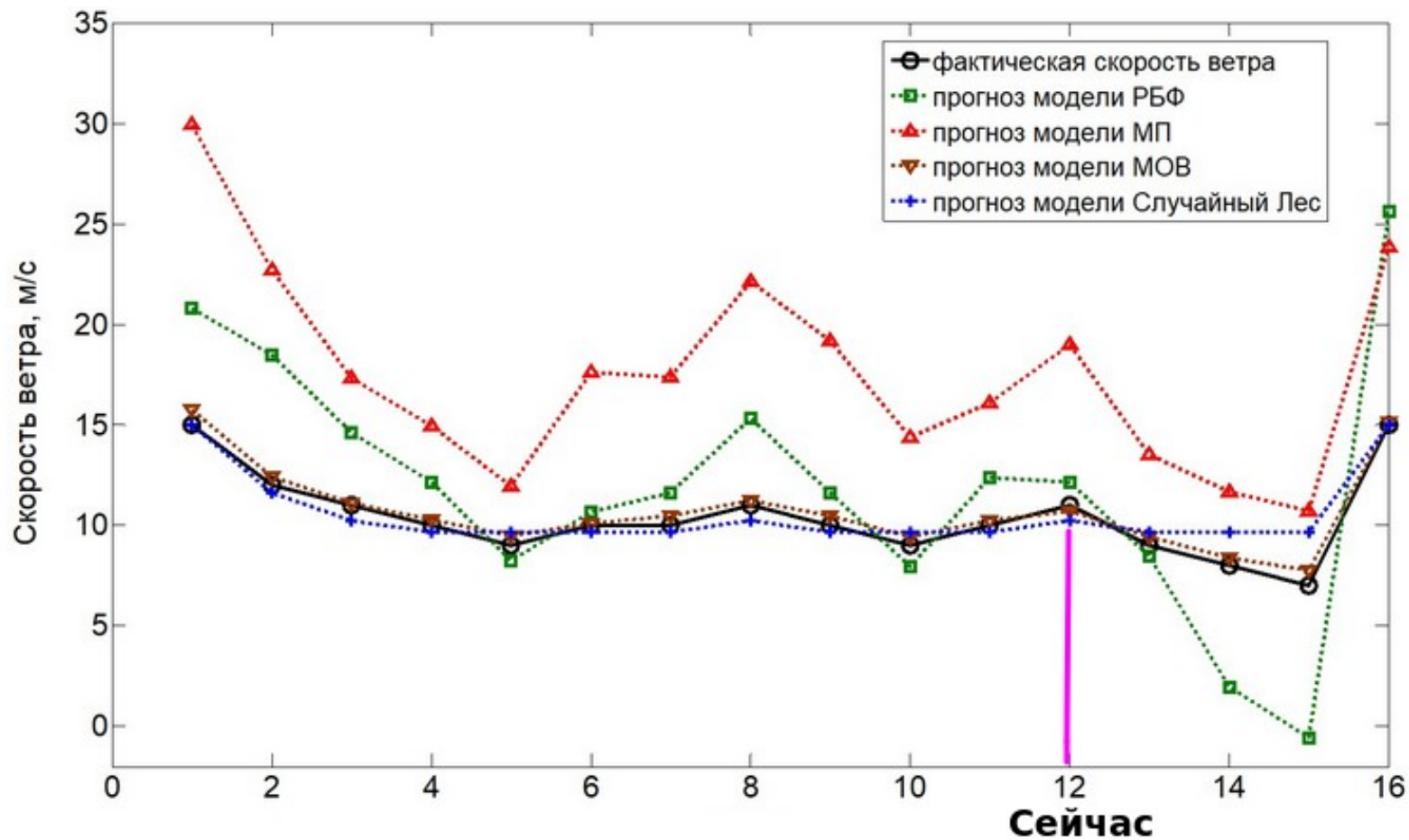
 **«Учение - свет, а неученье - тьма!». Как появи...**  
[zen.yandex.ru](#) > Яндекс.Дзен > id... ▾  
Фразу часто используют в назидание или в шутку, когда хотят подчеркнуть роль образования и пользу знаний. [Читать ещё >](#)



 **Учение-свет**  
[sites.google.com](#) > site/ucenesvet/ ▾   
Учение-свет. Поиск по сайту. Главная страница.

Ответ задачи – конечное упорядоченное множество.

# Прогнозирование





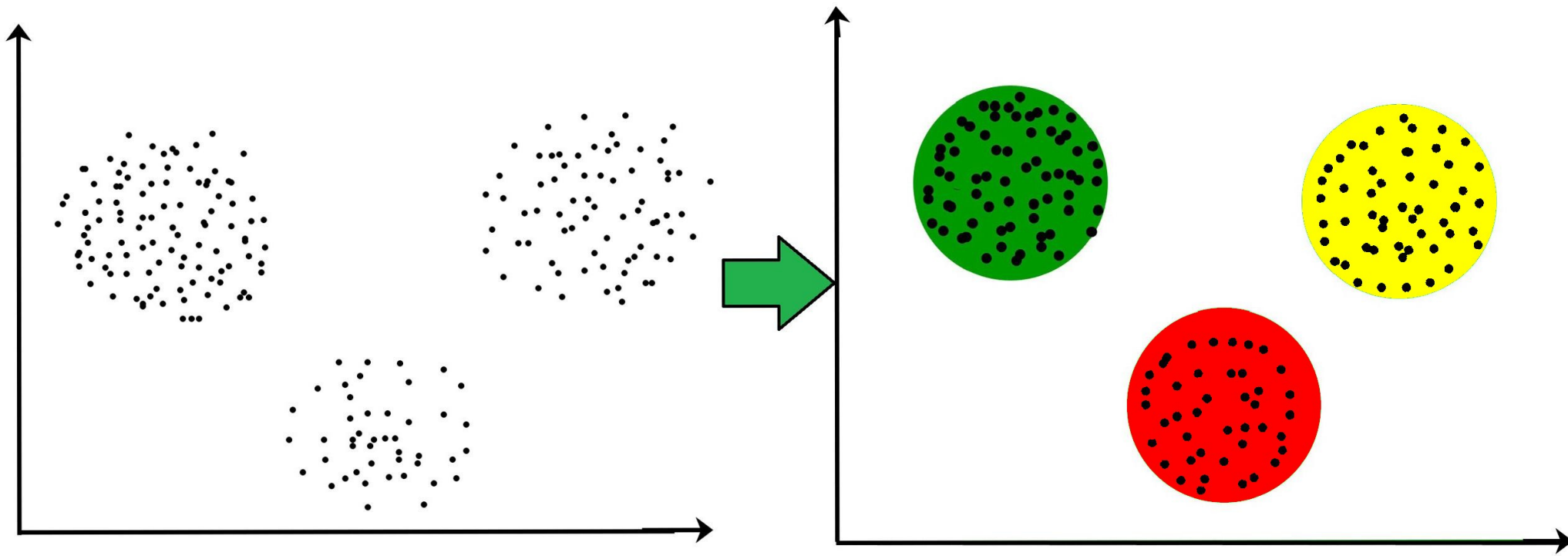
# Обучение без учителя

В данных присутствуют объекты без ответов. Требуется установить зависимости между объектами.

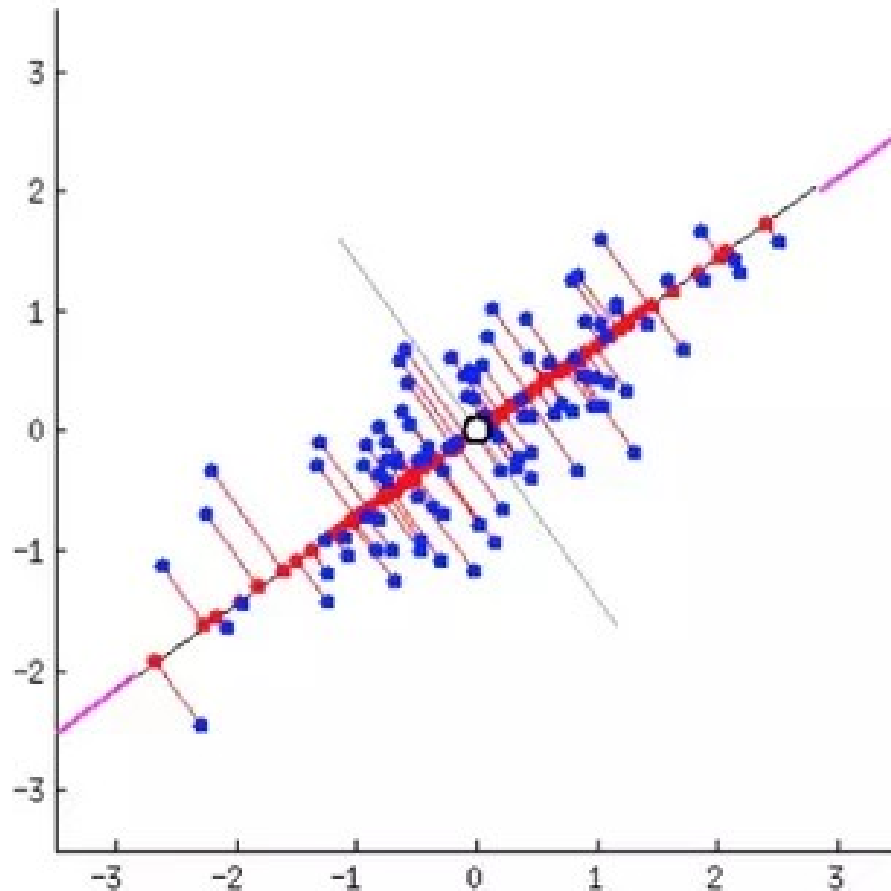
Задачи:

- кластеризация
- снижение размерности
- фильтрация выбросов

# Кластеризация



# Снижение размерности



# Линейная зависимость

Квартира (объект)	Площадь $x^{(1)}$	Этаж $x^{(2)}$	До метро $x^{(3)}$	Школа $x^{(4)}$	Кондиционер $x^{(5)}$	Цена $y$
1	32.5	4	550	-	-	7.2
2	118.3	1	750	+	+	21.5
...						
33	65.1	12	1100	-	+	12.4

$$h_{\Theta}(x_i) = \Theta_0 + \Theta_1 x_j^{(1)} + \Theta_2 x_j^{(2)} + \dots + \Theta_n x_j^{(n)}$$

$$x_j(0) = 1$$

$$h_{\Theta}(x_j) = \Theta x_j, \quad \Theta = ?$$

# Функция ошибки

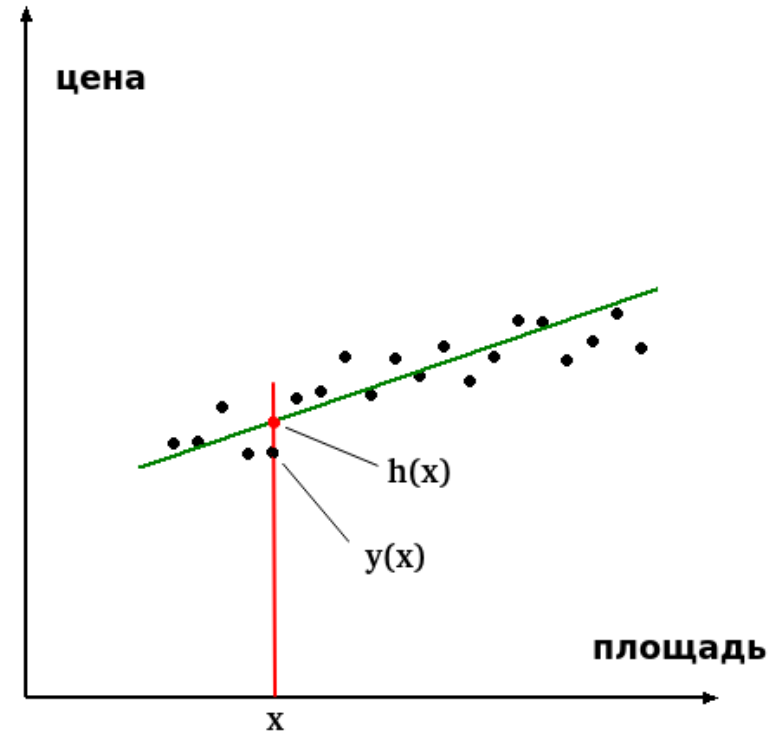
Площадь	Цена
32.5	7.2
118.3	21.5
...	
65.1	12.4

$$h_{\Theta}(x_j) = \Theta_0 + \Theta_1 x_j^{(1)}$$

$$E_{\Theta} = \sum |y_j - h_{\Theta}(x_j)| \text{ - линейная}$$

$$E_{\Theta} = \frac{1}{2} * \sum (y_j - h_{\Theta}(x_j))^2 \text{ - квадратичная}$$

Задача: минимизировать  $E_{\Theta}$ .



# Градиентный спуск

$$E_{\Theta} = \frac{1}{2} * \sum (h_{\Theta}(x^{(i)}) - y^{(i)})^2 - \min$$

$$E_{\Theta^{(0)}} = \frac{1}{2} * (h(x^{(0)}) - y^{(0)})^2 - \min$$

$h(x^{(0)}) > y^{(0)} \Rightarrow$  немного уменьшить  $h(x^{(0)})$

$h(x^{(0)}) < y^{(0)} \Rightarrow$  немного увеличить  $h(x^{(0)})$

Направление изменения  $h(x^{(0)})$  совпадает с  $-dE_{\Theta^{(0)}}/dh(x^{(0)}) = -(h(x^{(0)}) - y^{(0)})$

$h(x^{(0)}) = \Theta_0 + \Theta_1 x_1 + \dots + \Theta_n x_n$  — увеличить

$x_1 > 0 \Rightarrow$  немного увеличить  $\Theta_1$

$x_1 < 0 \Rightarrow$  немного уменьшить  $\Theta_1$

Направление изменения  $\Theta_1$  совпадает с  $x_1 = dh(x^{(0)})/d\Theta_1$

Аналогично, для случая когда  $h(x^{(0)})$  необходимо уменьшить

Направление изменения  $\Theta_1$  совпадает с  $-dE_{\Theta^{(0)}}/d\Theta_1 = -dE_{\Theta^{(0)}}/dh(x^{(0)}) * dh(x^{(0)})/d\Theta_1$

Направление изменения  $\Theta_j$  совпадает с  $-dE_{\Theta}/d\Theta_j$

# Градиентный спуск

$$\Theta_i := \Theta_i - \alpha * dE_{\Theta} / d\Theta_i, \alpha > 0$$

$$\Delta\Theta_i = -\alpha * dE_{\Theta} / d\Theta_i$$

Алгоритм настройки параметров  $\Theta$ :

повторять

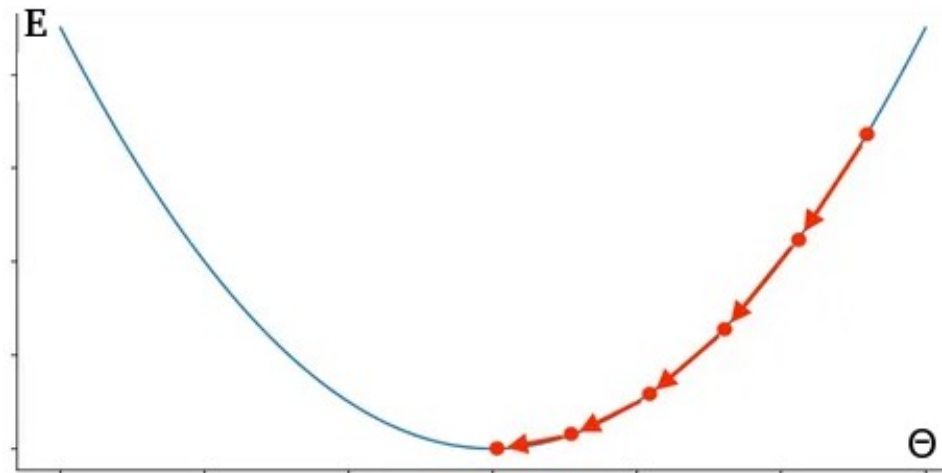
    для  $i = 1..n$

$$\Theta_i := \Theta_i - \alpha * dE_{\Theta} / d\Theta_i$$

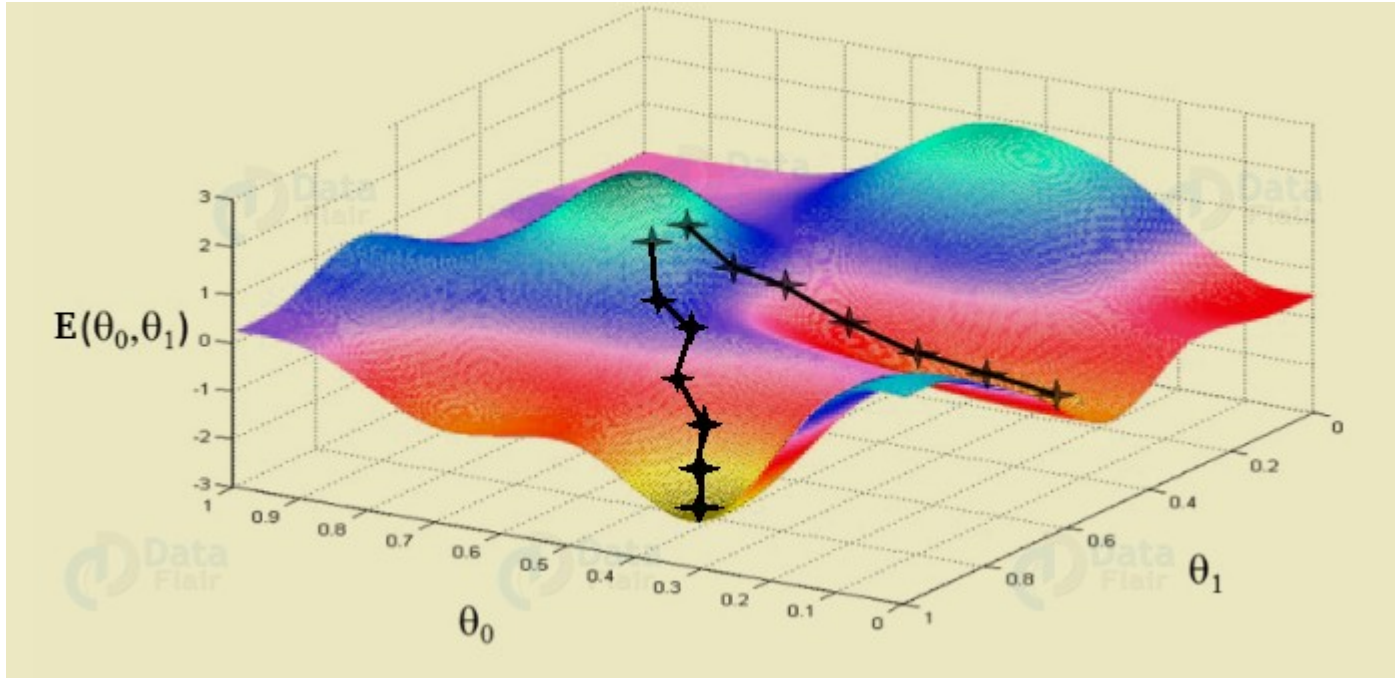
пока  $E$  убывает

Задаваемые параметры:

- начальное значение  $\Theta$
- значение  $\alpha$  – скорость обучения



# Начальное значение $\Theta$



Начальные значения  $\Theta_i$  обычно задаются случайными небольшими числами.



# Скорость обучения $\alpha$

Маленькая **скорость обучения** заставляет алгоритм сходиться очень долго, слишком большая — расходиться



Работа алгоритма градиентного спуска на параболе из точки  $(-1.2, 1.42)$ . Вариатны скорости обучения: 0.03, 0.2, 1.05

# Градиентный спуск для линейной регрессии

$$h_{\Theta}(x) = \Theta_0 + \Theta_1 x^{(1)} + \Theta_2 x^{(2)} + \dots + \Theta_n x^{(n)}$$

$$E_{\Theta} = \frac{1}{2} * \sum (y_j - h_{\Theta}(x_j))^2$$

$$\Delta \Theta_i = -\alpha * dE_{\Theta} / d\Theta_i = -\alpha * \sum (y_j - h_{\Theta}(x_j)) * x_j^{(i)}$$

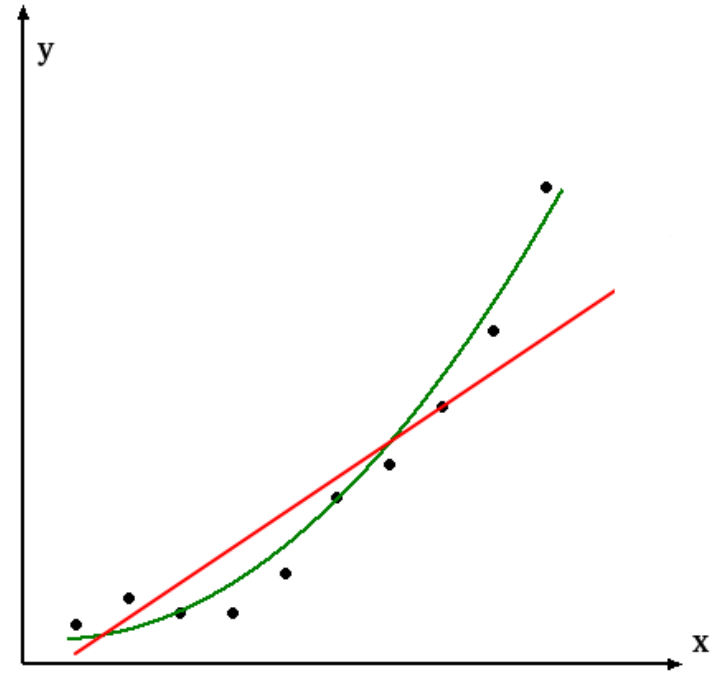
# Добавление новых признаков

Сжатие $x^{(1)}$	Высота $y$
2.5	17.5
0.3	0.3
...	
1.7	9.3

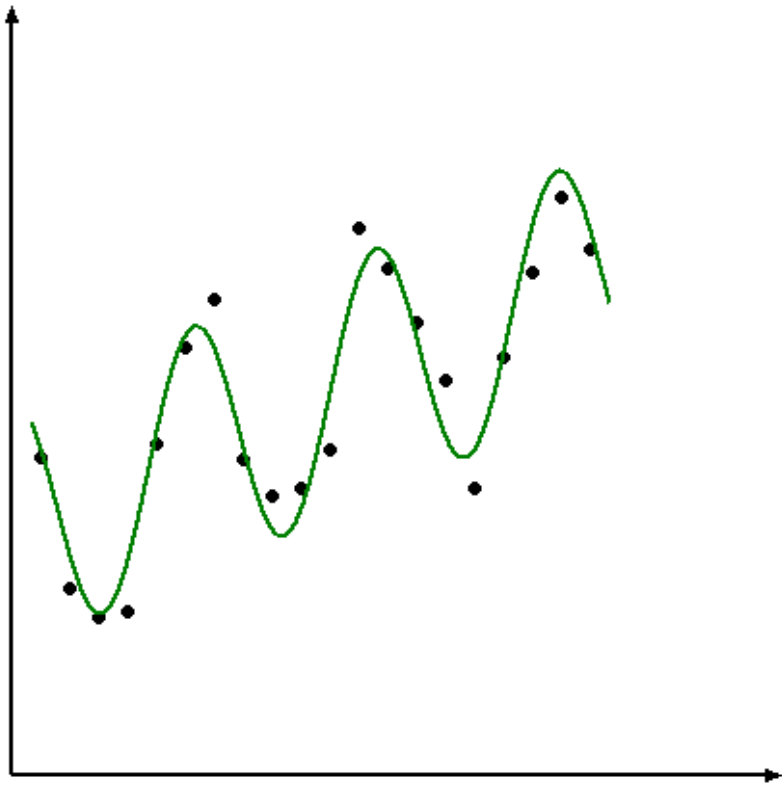
$$h_{\Theta}(x) = \Theta_0 + \Theta_1 x^{(1)}$$

Сжатие $x^{(1)}$	$(x^{(1)})^2$ $x^{(2)}$	Высота $y$
2.5	6.25	17.5
0.3	0.09	0.3
...		
1.7	2.89	9.3

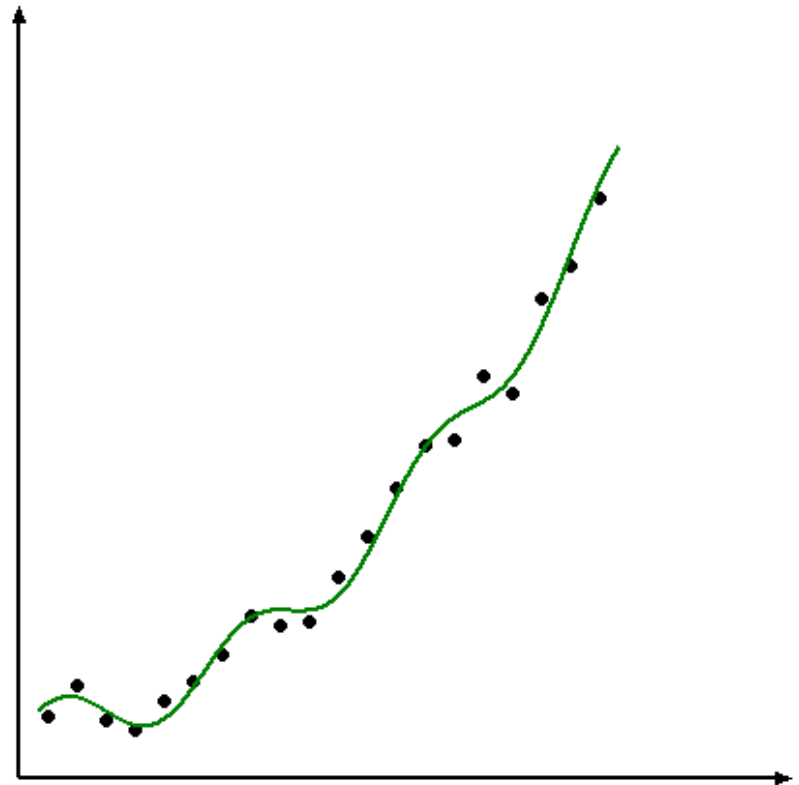
$$h_{\Theta}(x) = \Theta_0 + \Theta_1 x^{(1)} + \Theta_2 x^{(2)}$$



# Добавление новых признаков

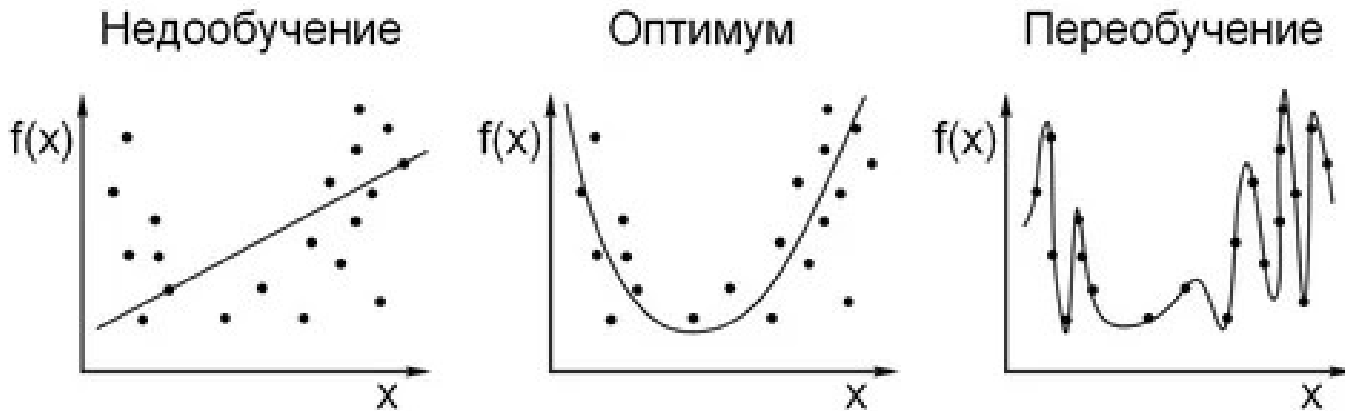


$$x_0 = 1, x_1 = x, x_2 = \cos(x)$$



$$x_0 = 1, x_1 = x, x_2 = x^2, x_3 = \sin(x)$$

# Переобучение



**Переобучение** - явление, когда построенная модель хорошо объясняет примеры из обучающей выборки, но относительно плохо работает на примерах, не участвовавших в обучении (на примерах из тестовой выборки).

# Проверка эффективности

Данные делятся:

- обучающая выборка – для настройки параметров алгоритма;
- контрольная выборка – объекты не участвуют в обучении, используются для оценки эффективности алгоритма.

Варианты:

- На отложенных данных – данные делятся на обучающую и контрольную выборки один раз.
- Оценка скользящего контроля - данные делятся на обучающую и контрольную выборки несколько раз. Результат усредняется.

<https://sesc-infosec.github.io/>