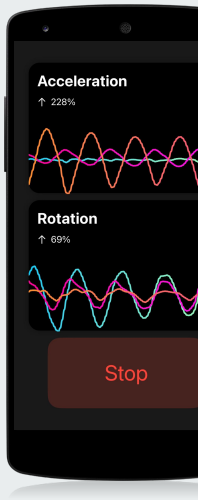
# Исследование и разработка методов статической аутентификации пользователей по данным датчиков движения мобильного устройства

к.ф.-м.н., доцент, Казачук Мария Андреевна
к.ф.-м.н., доцент, Петровский Михаил Игоревич
студент магистратуры, Чикин Олег Павлович




Кафедра ИИТ ВМК МГУ, 2025

# Актуальность задачи (1)

- Проблема **обеспечения конфиденциальности** данных в информационных системах, в том числе **мобильных устройствах (смартфонах)**, актуальна.
- **Аутентификация** – один из основных инструментов обеспечения конфиденциальности.
- Существующие системы аутентификации в смартфонах **уязвимы**:
  - Высокий риск компрометации паролей / отпечатков пальцев и т.д.
- Необходимо разрабатывать **новые** сценарии и алгоритмы **статической** аутентификации пользователей смартфонов.

# Актуальность задачи (2)

- Введение статической аутентификации пользователей смартфонов на основе **анализа жеста**, проделанного со смартфоном в руке:
  - Не требуется наличия **специализированного оборудования;**
  - **Высокая надежность** за счет использования поведенческих биометрических показателей.
- Данные, характеризующие жест пользователя, снимаются с **датчиков движения**, встроенных в смартфон:
  - **Акселерометр** – основной датчик движения, измеряет проекцию кажущегося ускорения (разности между истинным ускорением объекта и гравитационным ускорением).
  - Таким образом, снятые данные представляют собой **временной ряд**.

# Постановка задачи

- **Исследование** существующих и **разработка** собственных алгоритмов **статической аутентификации пользователей** по данным датчиков движения мобильного устройства:
  - Рассматривается **аутентификация** пользователя по **жесту**, выполненному со смартфоном в руке.

# Обзор существующих решений

# Базовое решение

- Был **изучен** имеющийся **задел кафедры ИИТ** по данной тематике:
  - Разработанные решения основаны на анализе показаний **акселерометра**.
- Качество этих решений **превосходит** результаты **существующих** работ, однако **не** является **достаточно высоким**:
  - **Метрика ROC AUC** составляет порядка **0.93**.
- Собранный ранее набор данных **не является** достаточно **репрезентативным**:
  - Включает в себя показания только **7 пользователей**.
- Предлагается:
  - **Улучшить** эти решения путем проведения **обзора** последних работ по данной тематике, **выявления** и **применения** наиболее **перспективных методов**, не рассмотренных ранее, а также **разработки** собственных алгоритмов;
  - Добавить **дополнительный сбор** показаний **гироскопа**, собрать **новый набор** данных и рассмотреть возможность **комбинированной** аутентификации.

# Итоги обзора (1)

- Был проведен **обзор** последних **20 научных статей** по данной тематике.
- Были определены не рассмотренные ранее наиболее перспективные методы **предобработки временного ряда**:
  - Использование фильтров (Баттерворта, Савицкого-Голея), кубического сглаживающего сплайна для удаления шумов;
  - Нормализация данных.
- В качестве элементов **вектора признаков**, зачастую используют:
  - Max-, min-, mean-, median-значения временного ряда, дисперсию, коэффициенты эксцесса и асимметрии, среднее квадратическое и стандартное отклонение, диапазон, длину и магнитуду;
  - Данные показатели рассчитываются как для всего временного ряда (из модулей ускорения или отдельных его компонент), так и для его отдельных участков.

# Итоги обзора (2)

- Были определены перспективные методы **сокращения размерности** пространства признаков:
  - Линейный дискриминантный анализ (LDA);
  - Метод главных компонент (PCA);
  - Выбор признаков на основе корреляции (CFS).
- Среди наиболее перспективных методов **построения модели** пользователя, ранее также показавших высокие результаты, следует отметить следующие:
  - One Class K-Nearest Neighbors (One Class KNN);
  - One Class Support Vector Machine (One Class SVM);
  - Нейронные сети – сверточные, рекуррентные, многослойный персептрон.
- При этом, **метрика ROC AUC** в рассмотренных в ходе **обзора** работах не превышает **0.90–0.92**, используемые **наборы** данных **закрыты** и содержат в среднем образцы жестов по **7–10 пользователям**.

# Исследование и построение решения

# Набор данных (1)

- Используемые в существующих работах **наборы данных** являются **закрытыми** и содержат **в среднем** образцы жестов по **7–10** пользователям.
- Собранный ранее **на кафедре** набор данных содержит данные по **7** пользователям, снятые с акселерометра.
- Был реализован программный прототип системы аутентификации пользователей мобильных устройств, поддерживающий **дополнительный** сбор показаний **гироскопа**, и на его основе был собран **новый набор данных**:
  - Три вида **простых** и **сложных** жестов: “*Звезда*”, “*Бесконечность*”, *слово “Кот”*;
  - Жесты описываются **ускорением** (показания *акселерометра*) и **угловой скоростью** (показания *гироскопа*) смартфона **по трем осям**;
  - **15** пользователей, в среднем по **50** образцов каждого жеста **на пользователя**;
  - Показания **гироскопа** могут **улучшить** точность модели, а **увеличение** числа пользователей сделает набор данных **более репрезентативным**.

# Набор данных (2)

- В базовом решении и самостоятельно реализованном программном прототипе системы аутентификации **сбор данных** осуществляется через **web-сайт**:
  - Возможность осуществлять сбор данных на **основных мобильных платформах** (iOS, Android) **без отдельных реализаций** для каждой из них;
  - Мобильное устройство **не** занимается **тяжелыми вычислениями**, которые могут повлиять на его работу.
- Для проверки **корректности удаленного** сбора данных (отсутствия потерь в качестве данных при их удаленном снятии с датчиков мобильного устройства) было реализовано **локальное приложение** для сбора данных:
  - Для работы на **iOS**, язык программирования **Swift**, 500 строк кода;
  - Проведенные эксперименты показали **идентичность** собранных данных при **удаленном** и **локальном** сборе.

# Распознавание на основе вектора признаков (1)

- Базовое решение основано на использовании:
  - **Вейвлет-преобразования** модулей ускорений с ограничением детализирующих коэффициентов, выделении **статистических** характеристик, последующей **стандартизации** признаков и метода **Fuzzy**.
- **Вейвлет-преобразование** одномерного сигнала – это его представление в виде обобщенного ряда по системе базисных функций, сконструированных из **исходного вейвлета** $\psi$ :

$$\psi_{ab}(t) = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a})$$

где $b$ – параметр, отвечающий за **сдвиг во времени**, $a$ – параметр, отвечающий за изменение **временного масштаба.**

- В дискретном вейвлет-преобразовании сигнал пропускают через **низкочастотный** и **высокочастотный** фильтры и получают **аппроксимирующие** и **детализирующие** коэффициенты, которые прореживают в **2 раза**.

# Распознавание на основе вектора признаков (2)

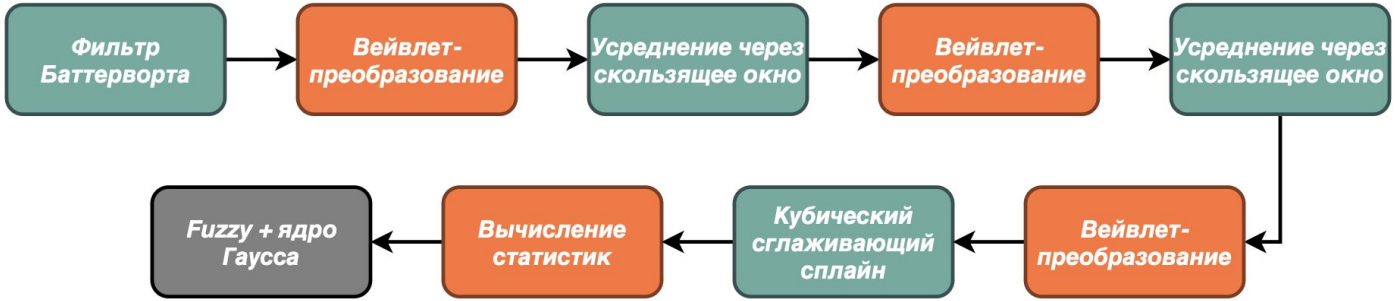
- Базовое решение основано на расчете **вектора признаков** на основе статистик по **аппроксимирующим** и **детализирующим** коэффициентам временного ряда:
  - *Max-*, *min-*, *mean-значения* и *стандартное отклонение* **модулей** ускорений смартфона.
- Для **повышения** точности аутентификации, предлагается:
  - Добавить **статистики** по значениям показаний **гироскопа**;
  - Исследовать **не рассмотренные** ранее перспективные **алгоритмы фильтрации** временного ряда (как отдельно, так и в комбинации с вейвлет-преобразованием);
  - Скорректировать **набор** вычисляемых **статистик**;
  - Рассчитывать статистики **не только** для **модулей** показаний акселерометра и гироскопа, но и для их отдельных **проекций** по трем осям;
  - **Проанализировать** влияние **аппроксимирующих** и **детализирующих** коэффициентов на точность аутентификации;
  - Рассчитывать статистики по **отдельным равномерным частям** временного ряда.

# Распознавание на основе вектора признаков (3)

- В качестве **постобработки** вектора признаков, в базовом решении используется алгоритм **стандартизации**:
  - Предлагается рассмотреть влияние **нормализации** и **стандартизации** признаков на качество аутентификации.
- Предлагается рассмотреть не исследованные ранее алгоритмы **сокращения размерности пространства признаков**.
- Рассматриваемая задача является задачей **поиска исключений**:
  - **Исключения** – объекты, которые **не соответствуют** или **сильно отличаются** от остальных объектов в хранилище или базе данных.
- Для построения модели пользователя базовое решение использует **нечеткий метод поиска исключений** с использованием потенциальных функций (Fuzzy):
  - Предлагается продолжить **исследование** применимости данного алгоритма вместе с алгоритмами **One Class KNN** и **One Class SVM**.

# Распознавание на основе вектора признаков (4)

- В ходе **исследования** была получена следующая **модификация** базового решения:




- Данная модификация включает в себя:
  - Добавление показаний **гироскопа**;
  - Добавление **проекций** показаний датчиков (*по 3-ем осям*);
  - Добавление **новых статистик** (*коэффициент эксцесса*, *коэффициент асимметрии*, *87-й процентиль*, *межквартильный размах*, *стандартная ошибка*);
  - **Многократное** применение **вейвлет-преобразования** (*к аппроксимирующим коэффициентам*);
  - Применение **новых фильтров** (*Баттерворта*, *кубического сплайна*).

# Беспризнаковое распознавание (1)

- Базовое решение основано на использовании:
  - Метода **фильтрации** последовательностей ускорений смартфона по трем осям – **скользящего окна**, метода **динамической трансформации временных рядов** (DTW) и метода **Fuzzy** (с DTW-ядром Гаусса).
- Для **повышения** точности аутентификации, предлагается:
  - При вычислении метрики DTW использовать **не только** показания **акселерометра**, но и показания **гироскопа**;
  - Рассматривать не только **показания** датчиков смартфонов **по трем осям**, но и **модули** соответствующих величин;
  - Использовать предварительную **вейвлет-параметризацию** временного ряда перед вычислением метрики **DTW**, а также предварительное **применение** других перспективных **фильтров**, выявленных на этапе обзора.

# Беспризнаковое распознавание (2)

- В ходе **исследования** была получена следующая **модификация** базового решения:


- Данная модификация включает в себя:
  - Добавление показаний **гироскопа**;
  - Добавление **модулей** показаний датчиков;
  - **Многократное** применение **вейвлет-преобразования** (*к аппроксимирующим коэффициентам*);
  - Применение **новых фильтров** (*Баттерворта*, *кубического сплайна*).

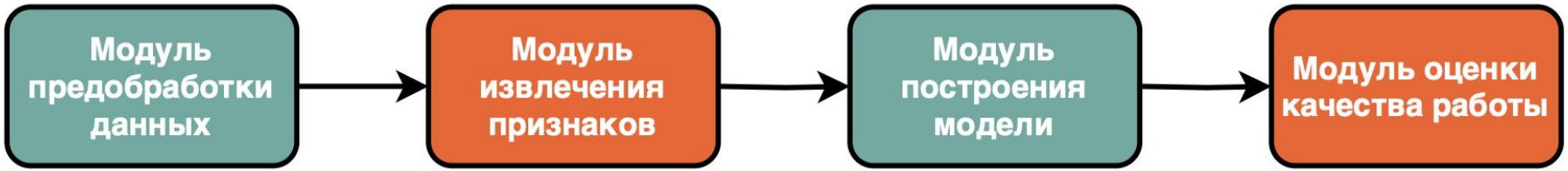
# Экспериментальное исследование

| *Исследуемый подход* | *Mean ROC AUC* | *Median ROC AUC* | *Interquartile Range* | *FRR* | *FAR* | *ERR* |
|---|---|---|---|---|---|---|
| ***Беспризнаковое распознавание (предложенное решение)*** | ***0.99*** | ***0.99*** | ***0.0008*** | ***0.001*** | ***0.007*** | ***0.004*** |
| ***Распознавание на основе вектора признаков (предложенное решение)*** | ***0.98*** | ***0.99*** | ***0.0065*** | ***0.013*** | ***0.018*** | ***0.016*** |
| Беспризнаковое распознавание (базовое решение) | 0.93 | 0.95 | 0.0087 | 0.016 | 0.017 | 0.017 |
| Yanna 2021 | 0.92 | 0.91 | 0.0163 | 0.025 | 0.024 | 0.025 |
| Huang 2022 | 0.90 | 0.90 | 0.0256 | 0.049 | 0.050 | 0.056 |
| Распознавание на основе вектора признаков (базовое решение) | 0.87 | 0.86 | 0.0358 | 0.078 | 0.081 | 0.080 |
| Shen 2020 | 0.87 | 0.85 | 0.0405 | 0.082 | 0.084 | 0.091 |
| Liu 2009 | 0.85 | 0.84 | 0.0515 | 0.093 | 0.085 | 0.095 |

По результатам экспериментальных исследований предложенные решения превзошли по качеству работы существующие и могут активно применяться на практике.

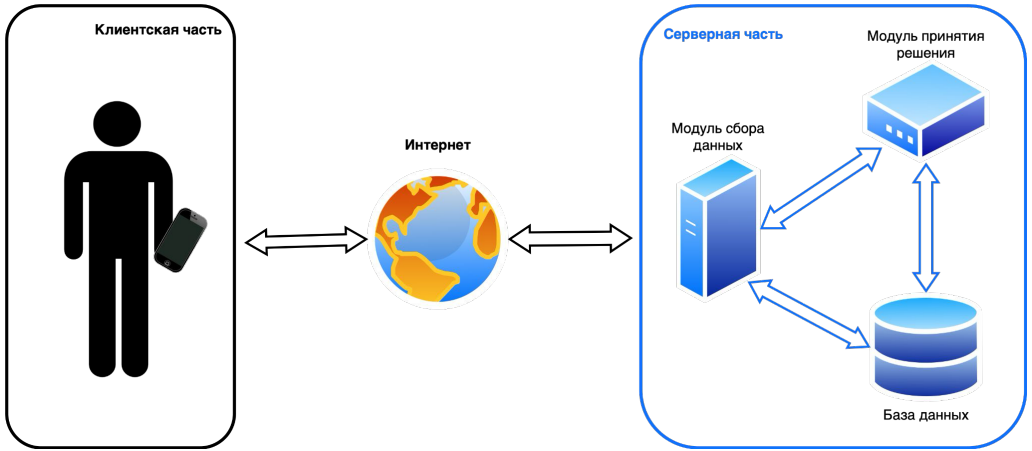
# Программная реализация

- В ходе работы, были **реализованы**:
  - **Экспериментальный стенд** для проведения исследований (~850 строк на Python3);
  - **Приложение** для **локального** сбора данных с акселерометра и гироскопа смартфона (~500 строк на Swift);
  - **Программный прототип кроссплатформенной системы аутентификации** пользователей мобильных устройств (~1700 строк на Python3, JS, CSS, HTML).



# Программный прототип системы аутентификации (1)

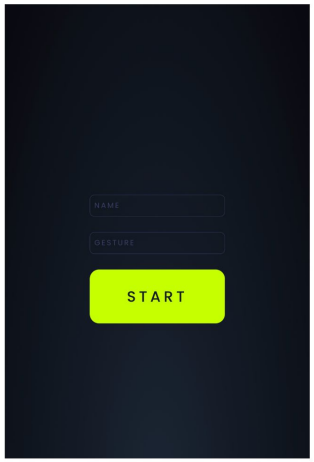
- Общая архитектура:

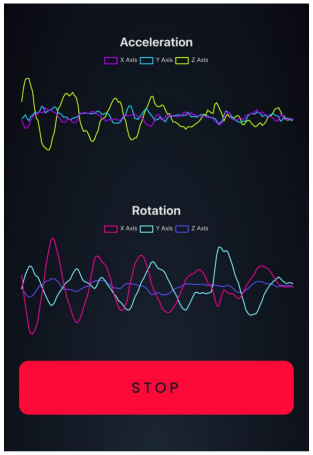


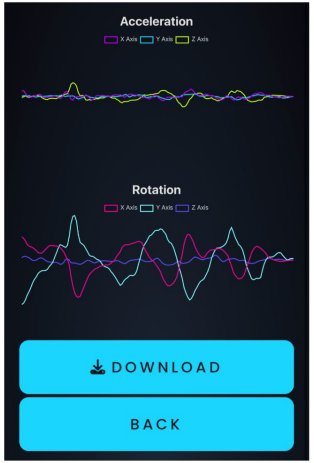

- Клиент сбора для мобильного устройства реализован в виде веб-страницы с помощью **HTML**, **JS** и фреймворка **jQuery Mobile** (~600 строк кода);
- Взаимодействия между клиентом и сервером происходят поверх соединения, защищенного **SSL**;
- В качестве хранилища данных используется реляционная СУБД **PostgreSQL**;
- Для реализации серверной части использовались язык **Python3** и фреймворк **Django** (~1000 строк кода).

# Программный прототип системы аутентификации (2)

- **Клиентская часть** системы аутентификации была протестирована на **iOS** (версий 16 и 17) и **Android** (версий 16 и 17), **серверная часть** тестировалась на **Linux** (Ubuntu 22.04.3 LTS):
  - Предобработка данных и извлечение признаков: **64 мс** для 40 временных рядов;
  - Обучение модели: **89 мс**;
  - Применение модели: **1.6 мс**.
- Аппаратные **характеристики сервера**: 4-х ядерный Intel Xeon (Icelake) с частотой 2000 МГц и 4 Гб RAM.



# Результаты

- Были **предложены модификации** базового решения, основанного на вейвлет-преобразовании и вычислении признаков на основе статистик:
  - Это позволило значительно увеличить показания Mean ROC AUC (с **0.87** до **0.98**).
- Были **предложены модификации** базового решения, основанного на DTW-преобразовании и применении классификатора с DTW-ядром Гаусса:
  - Это позволило значительно увеличить показания Mean ROC AUC (с **0.93** до **0.99**).
- Были **разработаны экспериментальный стенд** для проведения исследований, а также **приложение для локального сбора данных**, подтвердившее идентичность удаленно и локально собранных данных.
- Был **разработан программный прототип системы аутентификации** пользователей мобильных устройств и **собран новый набор данных** для проведения исследований:
  - Данный прототип может быть использован для построения перспективных систем ИБ, включающих в себя анализ жестов, проделанных с мобильным устройством в руке.

# Спасибо за внимание!

# Алгоритм DTW

Рассмотрим 2 временных ряда:

$Q = q_1, q_2, \ldots, q_i, \ldots, q_n;$

$C = c_1, c_2, \ldots, c_j, \ldots, c_m;$

где $q_i = [p_{i,x}, p_{i,y}, p_{i,z}], c_j = [p_{j,x}, p_{j,y}, p_{j,z}]$

1. Строим матрицу *d* порядка *n x m:*

$$d(q_i, c_j) = \sqrt{(p_{i,x} - p_{j,x})^2 + (p_{i,y} - p_{j,y})^2 + (p_{i,z} - p_{j,z})^2}$$

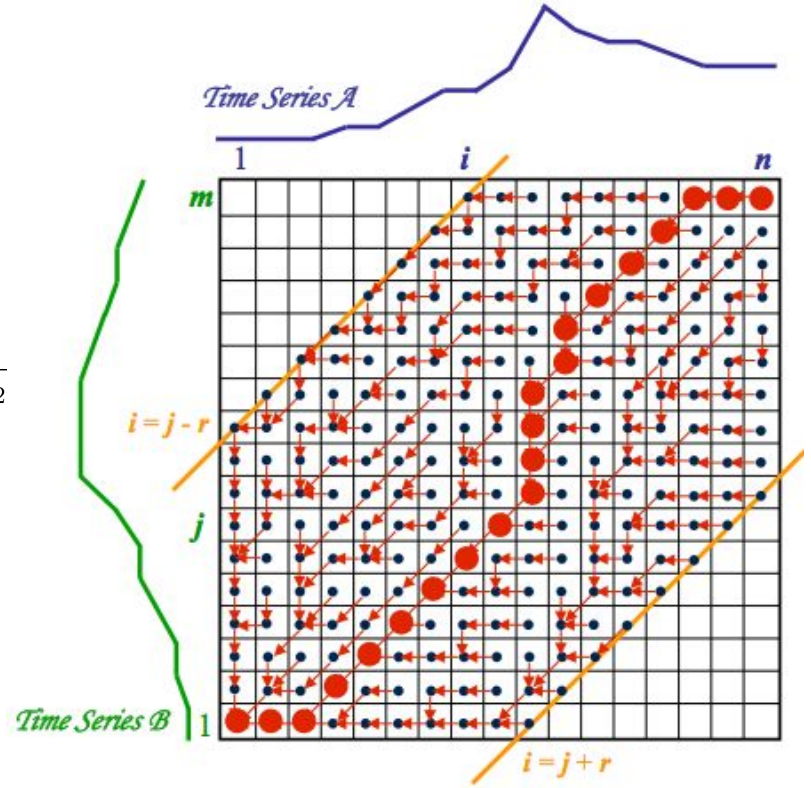
2. Строим матрицу трансформаций $D$, каждый элемент которой:

$$D_{i,j} = d_{ij} + \min(D_{i-1,j}, D_{i,j-1}, D_{i-1,j-1})$$

3. Строим оптимальный путь трансформации $W$ и *DTW-расстояние*:

$$W = w_1, w_2, \ldots, w_K; \max(n, m) \le K \le m + n$$

$$DTW(Q, C) = \min\left(\frac{\sum_{k=1}^{K} d(w_k)}{K}\right)$$



# Нечеткий метод поиска исключений (1)

*Идея выявления исключений*:

- С помощью **потенциальной функции** строится отображение исходного множества анализируемых объектов в **пространство характеристик**;
- **Вместо гиперсферы**, содержащей образы анализируемых объектов, в пространстве характеристик строится один общий **нечеткий кластер**, содержащий **все образы** анализируемых объектов;
- **Степень принадлежности** образа анализируемого объекта этому кластеру интерпретируется как **мера “типичности”**.

# Нечеткий метод поиска исключений (2)

- Метод формально приводит к задаче **минимизации функционала**:

$$\min_{U,a,\eta} J(U,a,\eta) = \sum_{i=1}^{N} u_i^m (\varphi(x_i) - a)^2 + \eta \sum_{i=1}^{N} (1-u_i)^m$$

где $a$ – центр нечеткого кластера в пространстве характеристик; $N$ – число анализируемых объектов; $U$ – вектор значений, где $u_i \in [0,1]$ – степень типичности $i$-го объекта; $m > 1$ – степень нечеткости и $\eta > 0$ – параметр, контролирующий размер или радиус нечеткого кластера в пространстве признаков высокой размерности.

- На основе итерационного метода, минимизирующего функционал $J(U,a,\eta)$, для каждого анализируемого объекта $z$ находится значение его меры типичности:

$$u(z) = \left[ 1 + \left( \frac{\sum_{j=1}^{N} u_j^m \sum_{i=1}^{N} u_i^m K(x_i,x_j)}{\eta \left( \sum_{i=1}^{N} u_i^m \right)^2} - 2\frac{\sum_{i=1}^{N} u_i^m K(z,x_i)}{\eta \sum_{i=1}^{N} u_i^m} + \frac{K(z,z)}{\eta} \right)^{\frac{1}{m-1}} \right]^{-1}$$

где $K$ – используемая ядровая (потенциальная) функция.

# Потенциальные функции

Для методов, в которых можно осуществить ***kernel trick*** (способ **классификации**, позволяющий работать в **новом** пространстве признаков, **не вычисляя координаты** данных в пространстве **более высокой** размерности), необходимо выбрать способ расчета потенциальной функции. В качестве таковых могут выступать:

- *DTW-ядро Гаусса*:

$$K(x,y) = exp\left(-\frac{DTW(x,y)}{2\sigma^2}\right)$$

- *Ядро Гаусса*:

$$K(x,y) = exp\left(-\frac{\|x-y\|^2}{2\sigma^2}\right)$$

где $\sigma$ – ширина используемого ядра (параметр алгоритма).