# Методы преобразования табличных данных в изображения в задаче выявления аномалий в киберфизических системах

**Евгения Новикова**[1], Марат Бухтияров[2]

[1] Санкт-Петербургский Федеральный Исследоватеьский центр РАН

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»



РусКрипто
Солнечногорск, Россия – Март 21, 2024

# Структура доклада

# Актуальность исследования

- В настоящее время предложено большое число подходов к выявлению аномалий в потоках данных от киберфизических системах на основе методов глубокого обучения [Sun et al., 2024; Wang et al., 2020; Xia et al, 2023; Tushkanova et al., 2023]
  - они выявлять нелинейные пространственные и временные зависимости между анализируемыми признаками
  - применение методов глубокого обучения требовательно к наличию вычислительных ресурсов
- Граничные вычисления: концепция переноса вычислений, связанных с обработкой данных, ближе к устройствам, которые генерируют эти данные
  - предложено федеративное обучение как парадигма МО с сохранением конфиденциальности, которая может быть развернута в IoT
  - устройства Интернета Вещей имеют ограниченные ресурсы вычислительной техники и памяти

# Эффективность модели МО

Ментальная модель эффективности модели МО [Menghani, 2023]

- **Эффективность модели МО во время применения**: Каков размер модели? Сколько параметров имеет модель? Каково потребление оперативной памяти при прогнозе? Какова задержка при прогнозе?
- **Эффективность модели МО во время применения**: Время обучения модели? сколько устройств? каковы их вычислительные возможности? и т.д.

Подходы к построению эффективных модели МО

# Цель и задачи исследования

## Цель

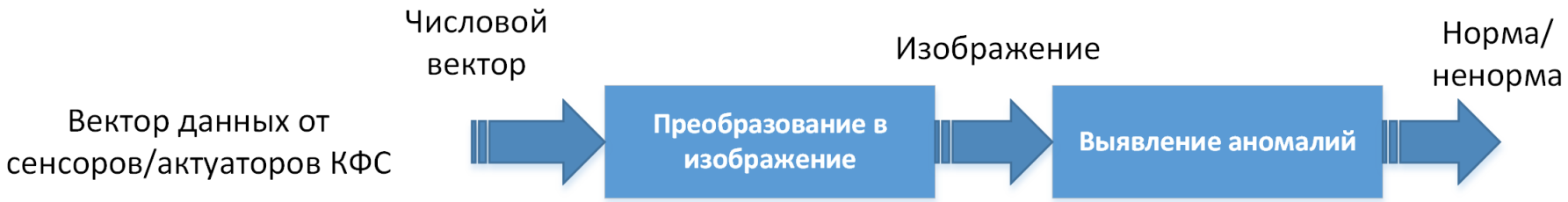
Поиск "легковесных" решений для обнаружения аномалий в многомерных временных рядах путем анализа различных методов предварительной обработки данных и применения сверточных нейронных сетей

**Задачи:**

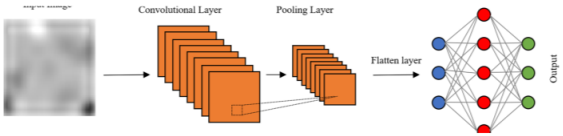
- анализ существующих подходов к построению изображений по табличным данным
- экспериментальная оценка влияния различных подходов к преобразованию на эффективность обнаружения аномалий в киберфизических системах.

# Преобразование табличных данных в изображения

Схема потока данных в процессе выявления аномалий




| Timestamp | FIT101 | LIT101 | MV101 | P101 | P102 |
|---|---|---|---|---|---|
| 28/12/2015 10:00:00 AM | 2,427057 | 522,8467 | 2 | 2 | 1 |
| 28/12/2015 10:00:01 AM | 2,446274 | 522,886 | 2 | 2 | 1 |
| 28/12/2015 10:00:02 AM | 2,489191 | 522,8467 | 2 | 2 | 1 |
| 28/12/2015 10:00:03 AM | 2,53435 | 522,9645 | 2 | 2 | 1 |
| 28/12/2015 10:00:04 AM | 2,56926 | 523,4748 | 2 | 2 | 1 |
| 28/12/2015 10:00:05 AM | 2,609294 | 523,8673 | 2 | 2 | 1 |
| 28/12/2015 10:00:06 AM | 2,637158 | 524,1028 | 2 | 2 | 1 |
| 28/12/2015 10:00:07 AM | 2,652211 | 524,2206 | 2 | 2 | 1 |
| 28/12/2015 10:00:08 AM | 2,655735 | 524,4954 | 2 | 2 | 1 |



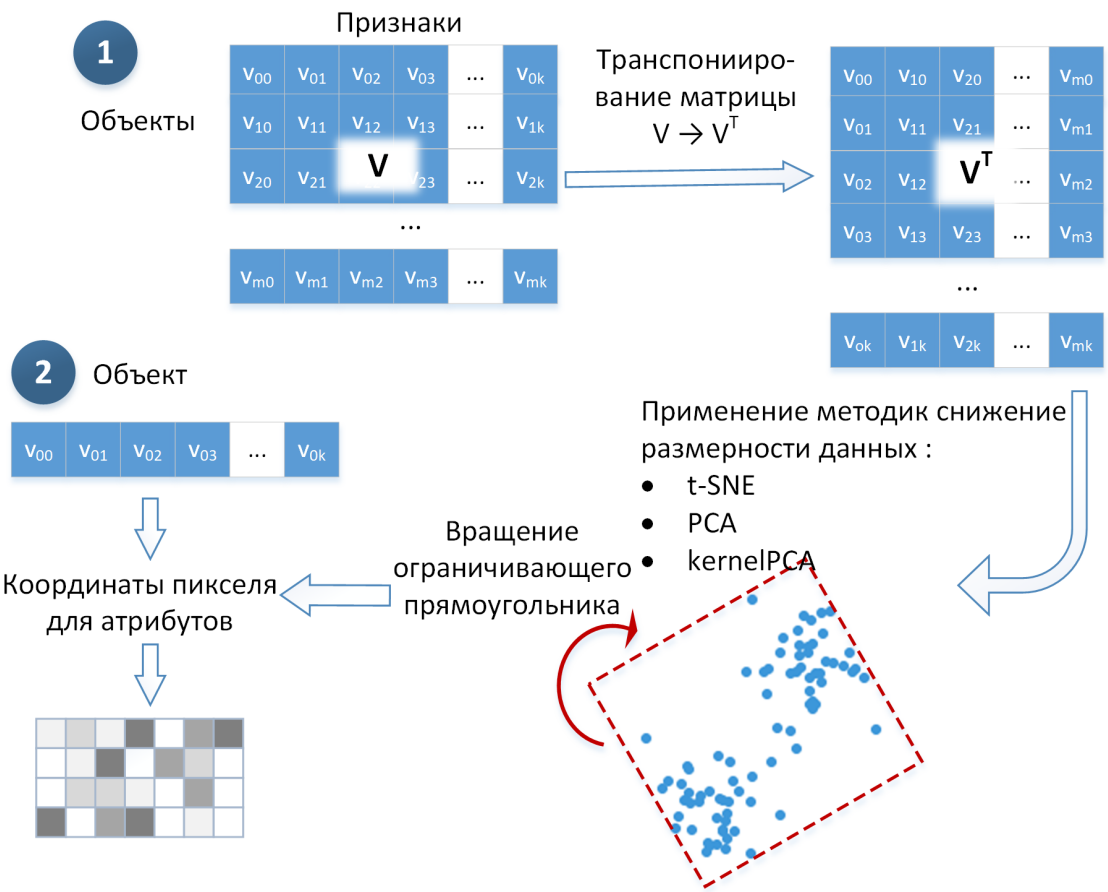

**Требования к входным данным:**
- входной вектор - числовой вектор;
- обучающая выборка представлена таблицей с объектами и метками;

**Методы преобразования:**
- прямое построение изображения
- нелинейное преобразование DeepInsight
- преобразование на основе оценки подобия IGDT

# Прямое преобразование данных

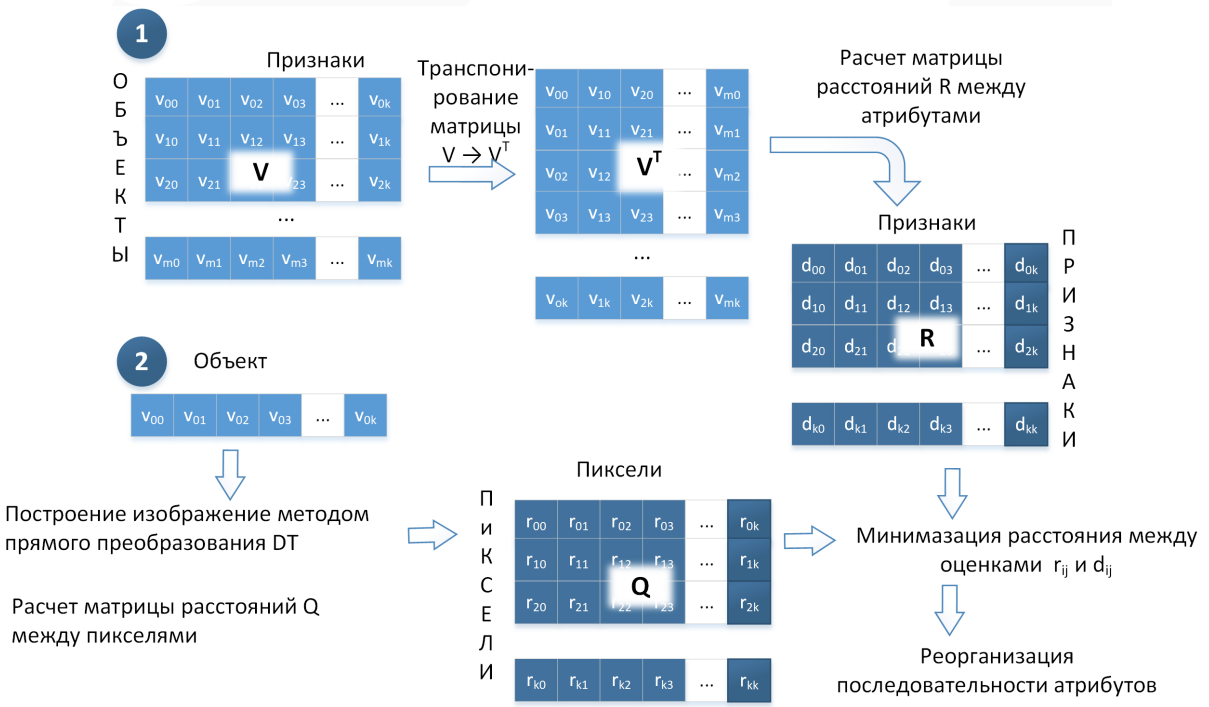

- Положение параметра (пикселя) определяется его положением в векторе и размером изображения;
- размер изображения определяется как $W_{image} = ceil((N + M)/2)$ для квадратных изображений;
- отсутствует корреляция между ближайшими пикселями

# Нелинейное преобразование




- DeepInsight[Sharma et al., 2019], REFINED [Bazgir et al., 2020];
- на основе проекции многомерных данных на двумерную плоскость;
- генерируемые изображение слишком разрежены $\longrightarrow$ их необходимо переобредилить размер ;
- в измененных изображениях один пиксель может отражать усредненное значения перекрывающихся признаков.

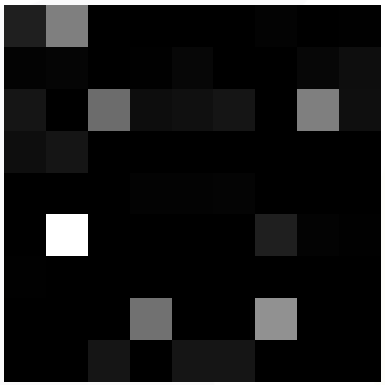
# Преобразование на основе оценки подобия признаков



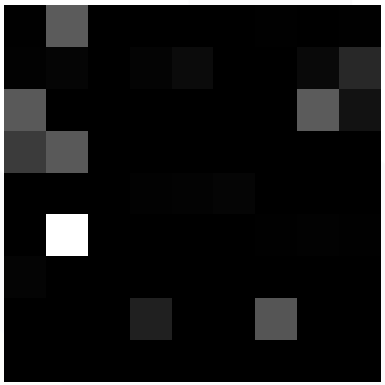

- IGDT ( Image Generator for Tabular Data) [Zhu et al 2021];
- оценивает расстояние между признаками и перестраивает пиксели на изображении

# Методы преобразования данных: пример

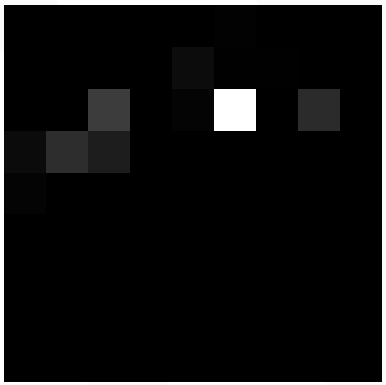
Изображения построенные для одного объекта



прямое преобразования



преобразование на основе оценки подобия IGDT



нелинейное преобразование DeepInsight (t-SNE)

# Сценарий эксперимента

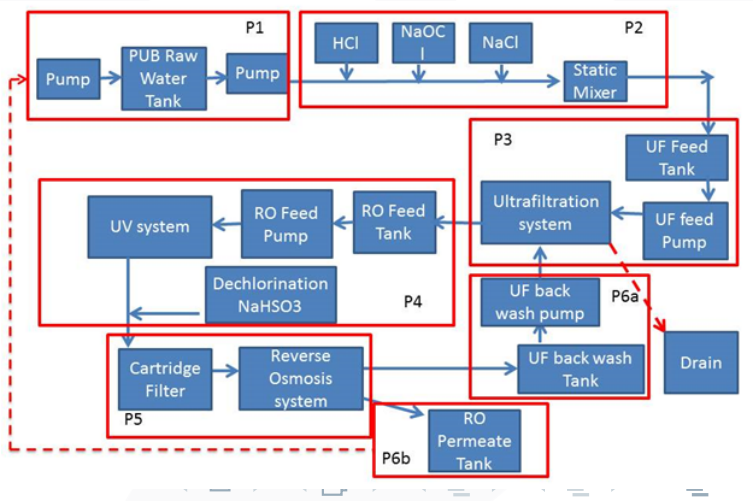
- Бинарный классификатор: CNN с 2 сверточными слоями
- Цель: оценить влияние методов преобразования данных на эффективности выявления аномалий .
- Метрики оценки эффективности:
  - полнота (recall) , точность(precision),и F1-мера,
  - число параметров и время прогноза

# Информация о тестовом наборе данных

**Набор данных SWAT**:
- доступен в двух форматах: PCAP (сетевой трафика) и CSV (данные от физических датчиков) ;
- описывает 5 дней функционирования системы водоочистных сооружений (физическая уменьшенная копия);
- используется во многих исследованиях [Sun et al., 2024; Wang et al., 2020; Xia et al, 2023; Tushkanova et al., 2023]

**Распределение атак по процессам в SWAT**

| Тип записи | Число атакуемых процессов | Атакуемые процессы | Число записей |
|---|---|---|---|
| НОрма | 0 | 0 | 399157 |
| Ненорма | 1 | P1 | 4053 |
| | 1 | P2 | 1809 |
| | 1 | P3 | 37860 |
| | 1 | P4 | 1700 |
| | 1 | P5 | 1044 |
| | 2 | P3, P4 | 1691 |
| | 2 | P1, P3 | 1445 |
| | 2 | P3, P6 | 697 |
| | 2 | P4, P5 | 463 |



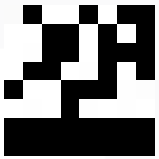
# Результаты эксперимента

## Эффективность обнаружения аномалий

| Подход | Точность | Полнота | f1-мера | Число параметров | Время прогноза |
|---|---|---|---|---|---|
| CNN+DT | 0.98 | **0.96** | **0.97** | 10 561 | $2.07 * 10^{-5}$ сек |
| CNN+DeepInsight with t-SNE | 0.98 | 0.92 | 0.95 | 10 561 | $2.07 * 10^{-5}$ сек |
| DeepSVDD** | 0.95 | 0.68 | 0.82 | 11 648 | $2.21 * 10^{-5}$ сек |
| LSTM** | 0.98 | 0.71 | 0.82 | 66 035 | $5.32 * 10^{-5}$ сек |
| MTS-DVGAN** [Sun et al., 2024] | **0.99** | 0.67 | 0.78 | - | - |
| CAN** [Xie et al., 2023] | 0.91 | 0.94 | 0.92 | - | - |

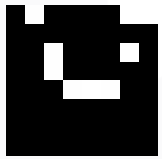
** - trained on GPU-equipped computational cluster

Изображения для нормы и не нормы



Прямое преобразование (норма)

DeepInsight (t-SNE) (норма)



Прямое преобразование (ненорма)

DeepInsight (t-SNE) (ненорма)

# Результаты и направление будущих исследований

## Результаты

- Использование специальных методов предварительной обработки (формирования анализируемых признаков) позволяет использовать эффективные архитектуры нейронных сетей для обнаружения аномалий
- Точность алгоритма классификации , используемого для обнаружения аномалий, зависит от того, насколько точно метод проекции данных отражает сходство между признаками..
- Более точная проекция точек данных, более устойчивый к новым и невидимым аномалиям обученный классификатор.

**Направление будущих исследований**

- Разработка подходов, основанных на сходстве признаков, для построения изображений для подмножетсва объектов (для формирование временного контекста ).
- Применение методов объяснения МО , разработанных для сверточных сетей, для обнаружения аномальных датчиков

# Литература


Zhu et al., 2021 — Zhu, Y., Brettin, T., Xia, F., Partin, A., Shukla, M., Yoo, H., Evrard, Y.A., Doroshow, J.H., Stevens, R.L.: Converting tabular data into images for deep learning with convolutional neural networks. Scientific Reports (2021). https://doi.org/10.1038/s41598-021-90923-y

Sharma et al.,2019 — Sharma, A., Vans, E., Shigemizu, D., Boroevich, K.A., Tsunoda, T.: Deepinsight: A methodology to transform a non-image data to an image for convolution neural network architecture. Scientific Reports (2019). https://doi.org/10.1038/s41598-019-47765-6

Bazgir et al., 2020 — Bazgir, O., Zhang, R., Dhruba, S.R., Rahman, R., Ghosh, S., Pal, R.: Rep resentation of features as images with neighborhood dependencies for compatibility with convolutional neural networks. Nature communications (2020).https://doi.org/10.1038/s41467-020-18197-y trusion detection. International Journal of Intelligent Computing Research (IJICR) 12, 087–1095 (2021)

Menghani, 2023 — Menghani G.: Efficient Deep Learning: A Survey on Making Deep Learning Models Smaller, Faster, and Better. ACM Comput. Surv. 55, 12, Article 259 (December 2023), 37 pages. https://doi.org/10.1145/3578938

Sun et al., 2024 — Sun H, Huang Y., Han L., Fu C., Liu H., Long X.: MTS-DVGAN: Anomaly detection in cyber-physical systems using a dual variational generative adversarial network. Computers & Security, Vol. 139, 2024, 103570, https://doi.org/10.1016/j.cose.2023.103570.

Wang et al., 2020 — Wang, C., Wang, B., Liu, H., Qu, H.: Anomaly detection for industrial control system based on autoencoder neural network. Wirel. Commun. Mob. Comput. 2020, 8897926–1889792610 (2020)

Xia et al, 2023 — Xia F., Chen X., Yu S, Hou M., Liu M. and You L.: Coupled Attention Networks for Multivariate Time Series Anomaly Detection. IEEE Transactions on Emerging Topics in Computing, doi: 10.1109/TETC.2023.3280577.

Tushkanova et al., 2023 — Tushkanova, O.; Levshun, D.; Branitskiy, A.; Fedorchenko, E.; Novikova, E.; Kotenko, I. Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. Algorithms 2023, 16, 85. https://doi.org/10.3390/a16020085

# *Спасибо за внимание!*
# *Вопросы?*

Контакты:
Евгения Новикова novikova@comsec.spb.ru