Распознавание аномальных режимов на адаптивных нейроалгоритмах

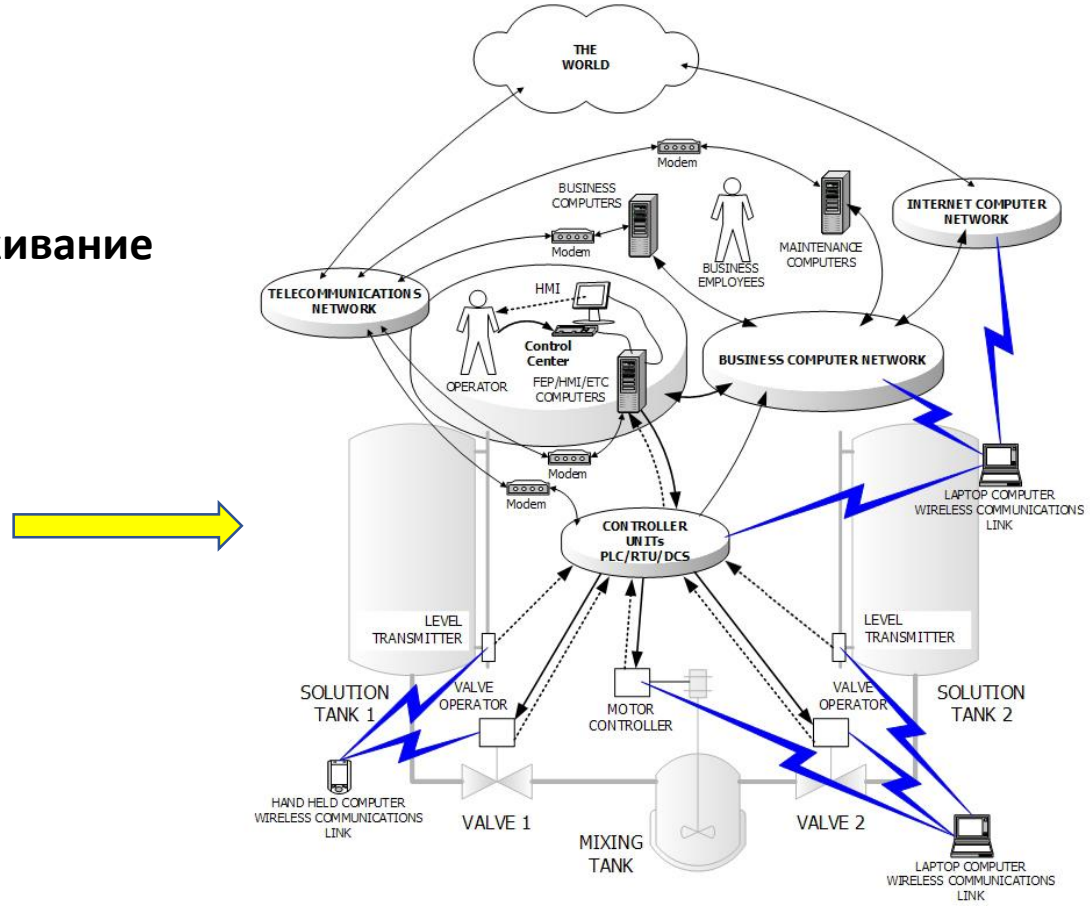
Александр Ларюхин

ООО «Интеллектуальные Сети»

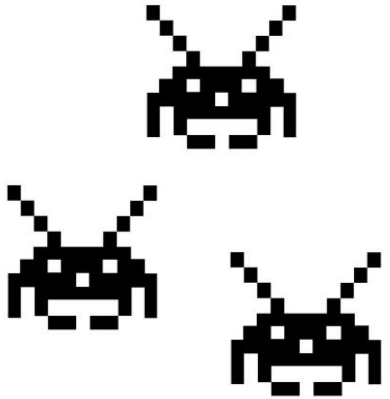
Проблема информатизации

- **Интенсивное развитие сетевой инфраструктуры промышленных сетей**
- **Интеграция информационных систем**

- **Диагностика и обслуживание**

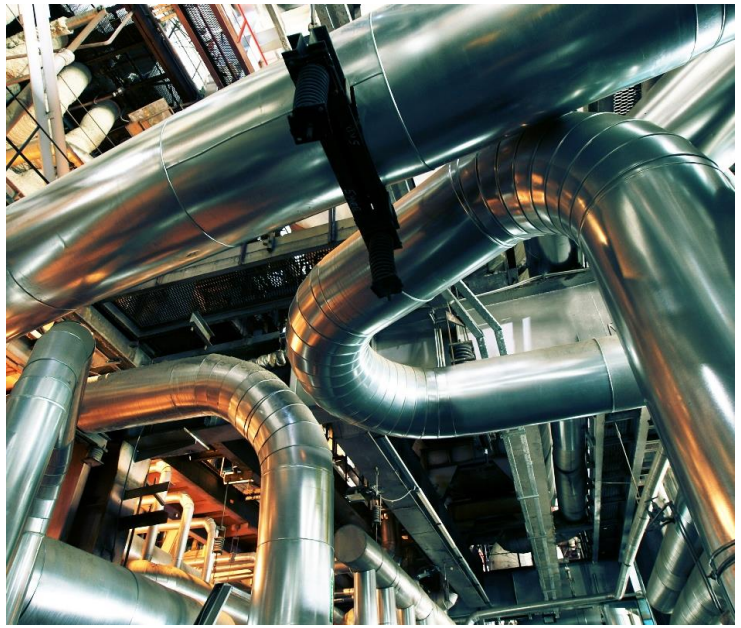


- **Уязвимость к вторжениям**



iGrids интеллектуальные сети

Проблема информатизации



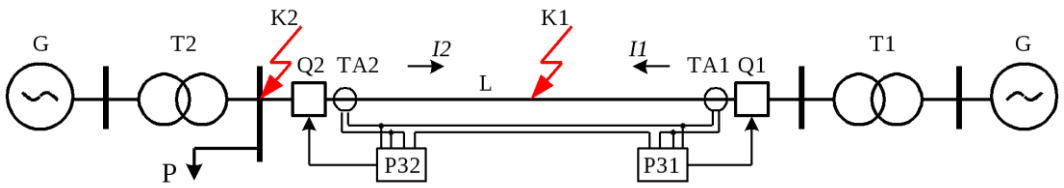
Различие подхода в обеспечении ИБ в корпоративных и промышленных сетях

- **Высокая пропускная способность**
- **Исполнение в режиме реального времени**
- **Недопустимость ожидания ответа на интерактивный запрос со стороны механизмов безопасности**

- **Непрозрачность процессов в промышленных сетях**
- **Отсутствие единообразия в алгоритмах**

iGrids интеллектуальные сети

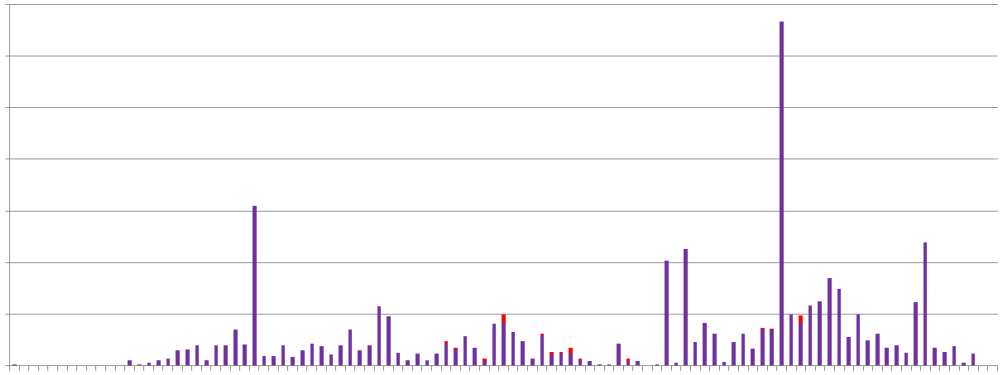
Поиск аномалий



Примеры аномалий:

- **Избыточное срабатывание защит**
- **Несрабатывание защит**
- **Отказ устройств**

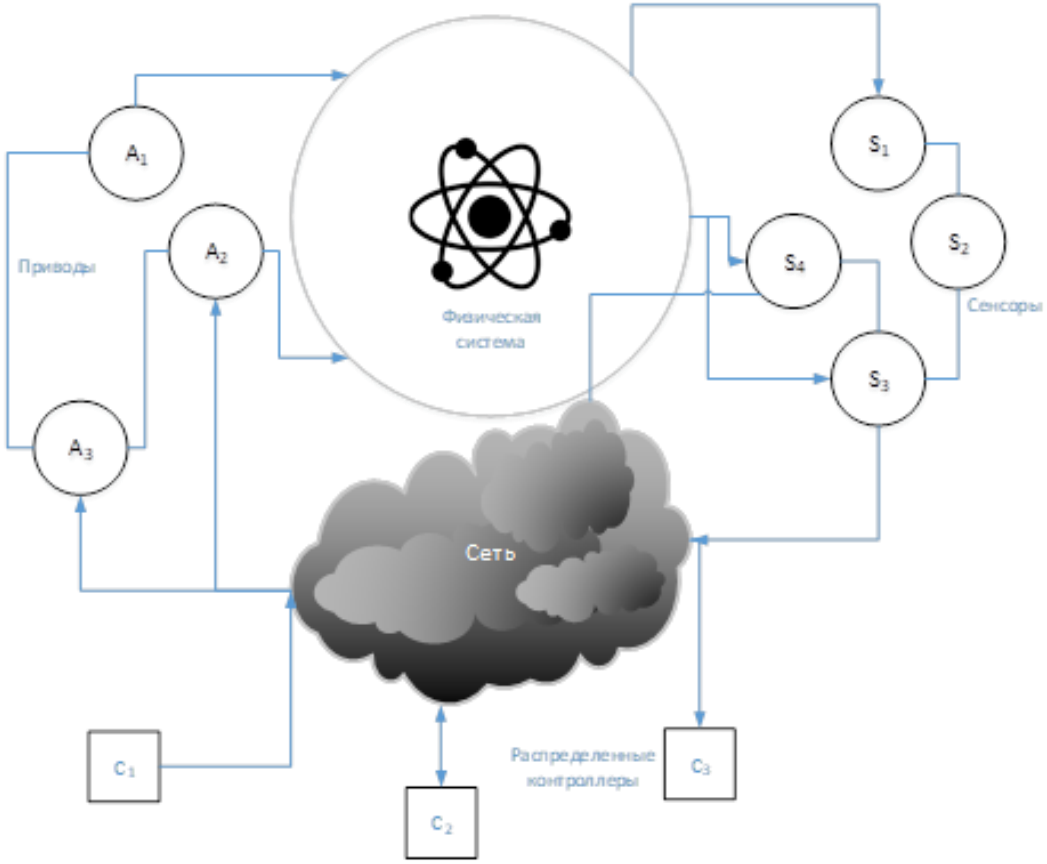
Статические выбросы – один из «нормальных режимов»



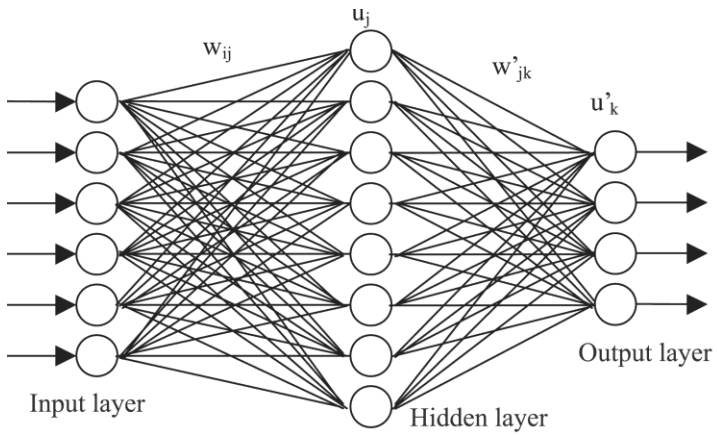
iGrids интеллектуальные сети

Поиск аномалий

Коллективные и контекстуальные аномалии:
Неадекватное режиму поведение устройств



Перспективный подход: Методы интеллектуального анализа данных - искусственная нейронная сеть

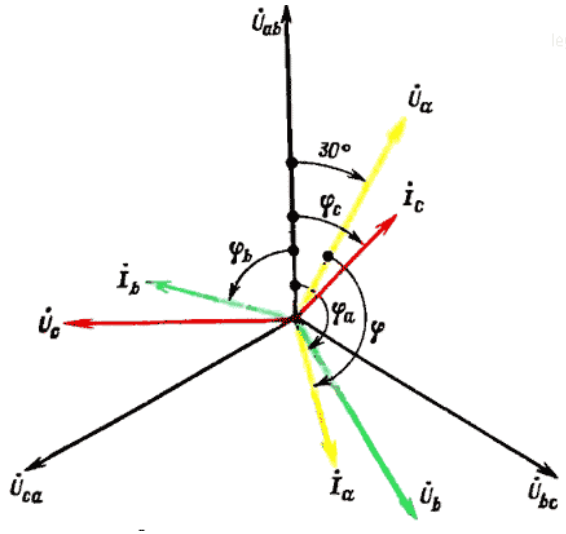


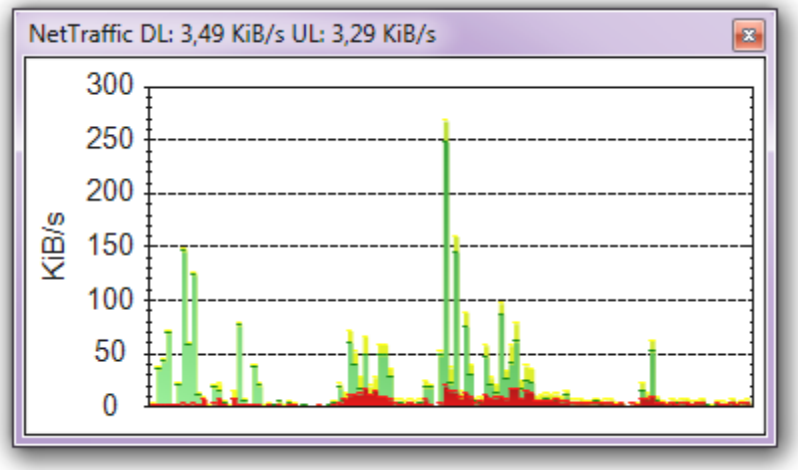
iGrids интеллектуальные сети

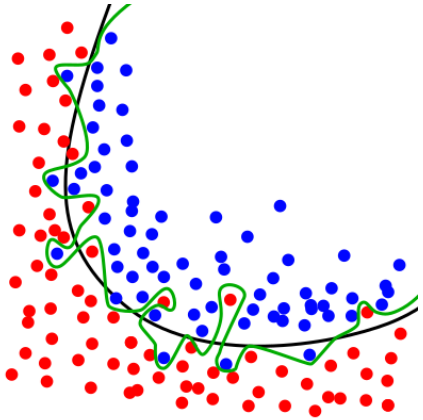
Концепция применения ИНС

В качестве основных данных для обучения выбраны:

- **Токи и напряжения**
- **Сетевой трафик**
- **Поведение защит**



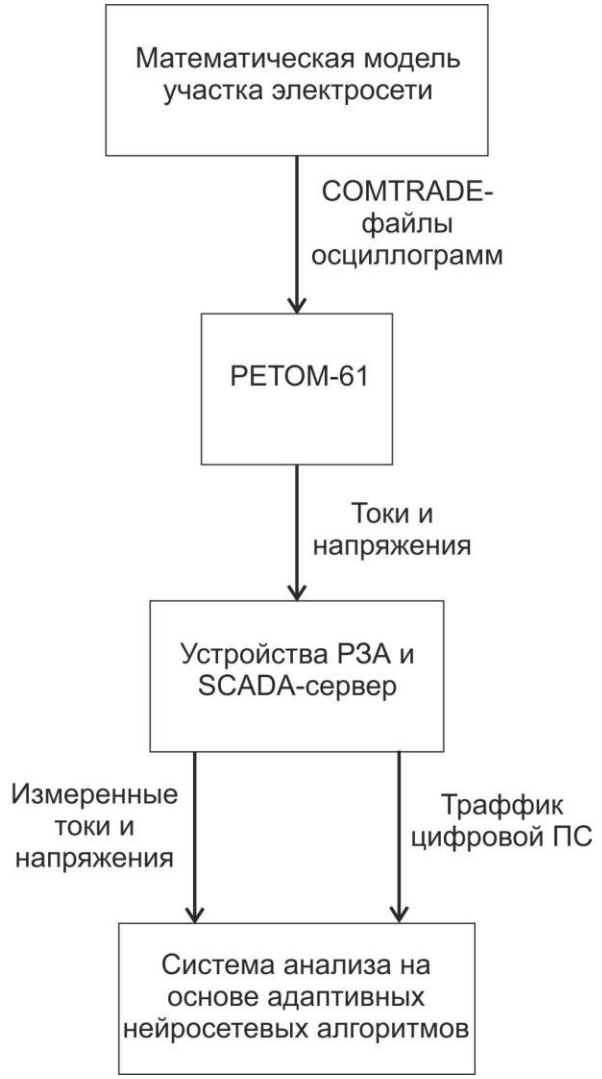




Проблема переобучения ИНС:
Необходимо выбирать данные и величины, не находящиеся в прямо зависимости

iGrids интеллектуальные сети

Обучение ИНС

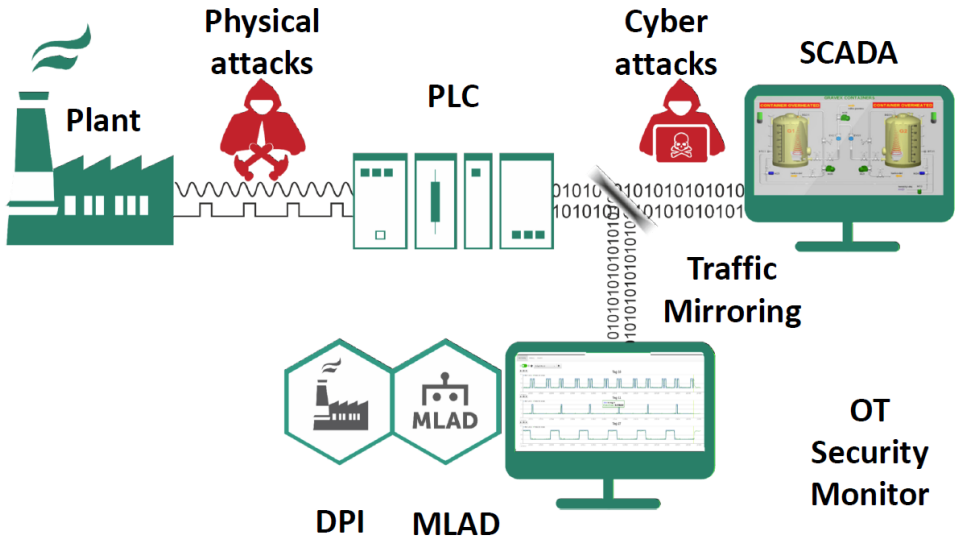


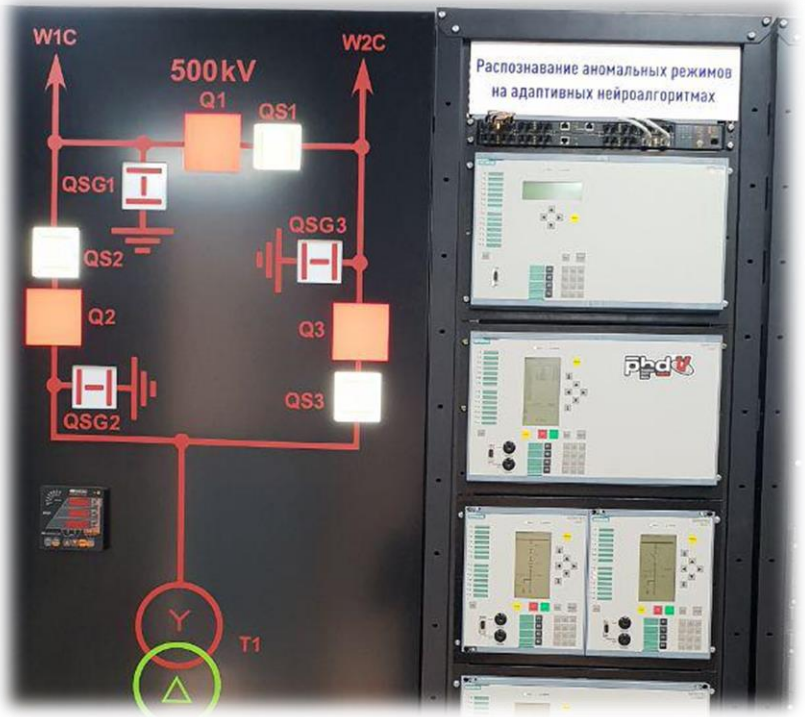
испытательная лаборатория
в городе Чебоксары

iGrids
интеллектуальные сети

Выводы и перспективы

MLAD - Machine Learning for Anomaly Detection





Спасибо за внимание!

Александр Ларюхин
ООО «Интеллектуальные Сети»
laruhin@igrids.ru