МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА КОМ'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Спеціальність 125 «Кібербезпека» | Освітня програма: БІКС

ДИПЛОМНА РОБОТА БАКАЛАВРА

«Проєктування алгоритму моніторингу мережевої поведінки, спрямованого на оперативне виявлення зловмисної активності в масштабованих IoT-середовищах»

Виконав: студент гр. БІКС-22 Муренко Даніїл В'ячеславович

Науковий керівник: Шабала Є.Є.

КНУБА 2026

Мета, об'єкт, предмет, актуальність

Мета роботи	Розробка алгоритму моніторингу мережевої поведінки IoT-пристроїв, що забезпечує оперативне виявлення аномальної та зловмисної активності в масштабованих кіберфізичних середовищах
Об'єкт дослідження	Мережеві взаємодії в IoT-середовищах кіберфізичних систем (на прикладі насосної станції)
Предмет дослідження	Методи та алгоритми виявлення аномальної і зловмисної мережевої активності IoT-пристроїв
Актуальність	Зростання кількості IoT у критичній інфраструктурі (водопостачання, енергетика) підвищує ризик кібератак. Обмежені ресурси вузлів унеможливлюють традиційні засоби захисту — потрібні легковагові поведінкові алгоритми з ненаглядовим навчанням

Основні завдання

1. Провести аналіз особливостей IoT-середовищ та кіберфізичних систем, їх вразливостей
2. Дослідити сучасні підходи до виявлення аномалій: IDS/IPS, машинне навчання
3. Розробити симуляційну модель кіберфізичної системи насосної станції (кіберполігон)
4. Згенерувати датасет нормального трафіку, аномалій та атак (FDI, Replay, DoS, Physical)
5. Спроєктувати 6-компонентний алгоритм моніторингу мережевої поведінки
6. Реалізувати прототип (Python) та провести експериментальну оцінку ефективності

Огляд методів виявлення аномалій та обґрунтування вибору

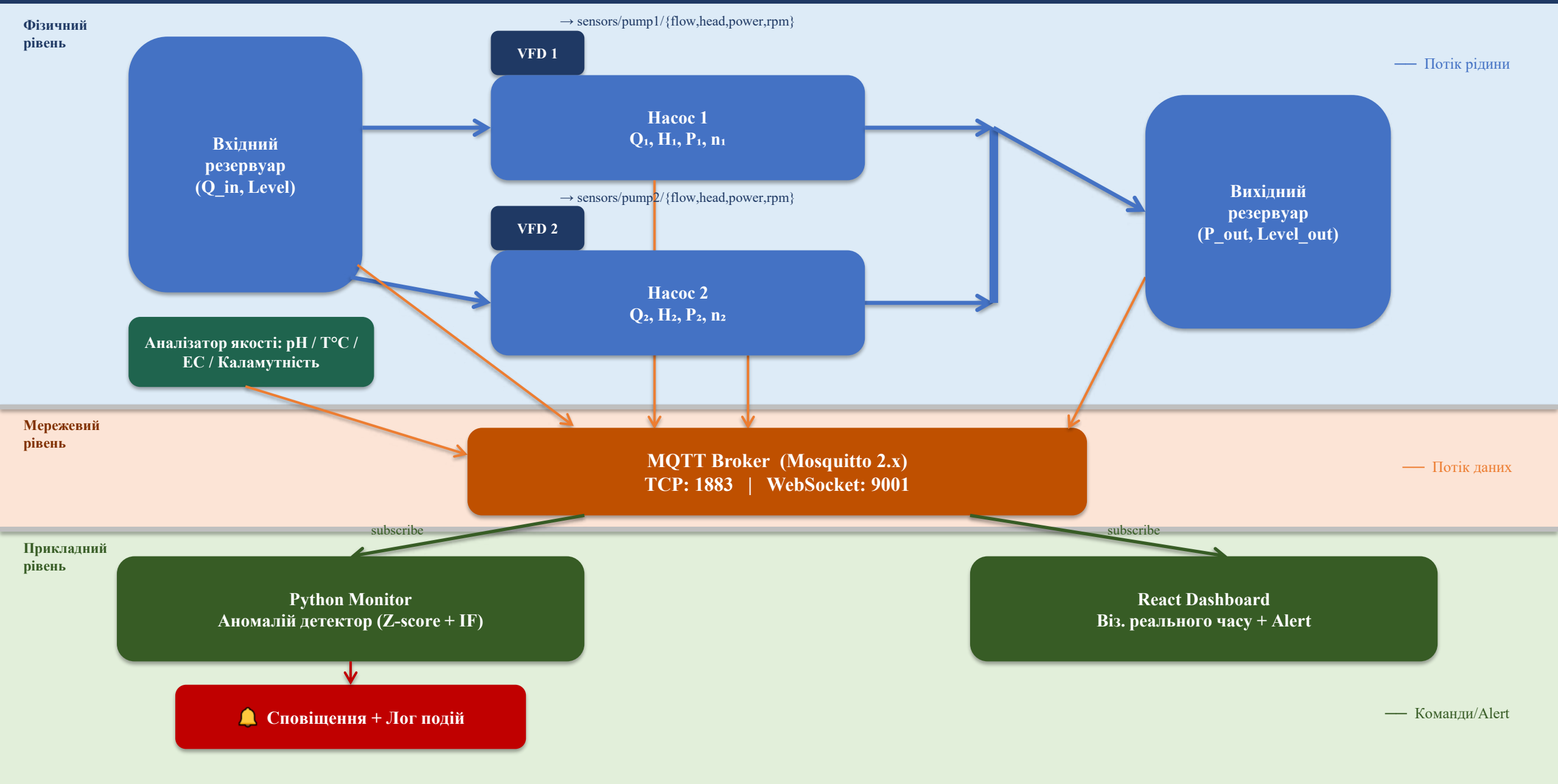
Статистичні (Z-score)	Сигнатурні (IDS/IPS)	Isolation Forest	OCSVM
Аналіз відхилень від рухомого середн. μ та σ. Швидкий, не потребує навчання.	Зіставлення з базою сигнатур. Висока точність для відомих атак, нові атаки не виявляє.	Ізолює аномалії випадковими деревами. Ненагляд., ефективний для багатовим. даних.	One-Class SVM. Найвищий AUC=0,977 серед одиночних детекторів у тестуванні.

Обраний підхід: Гібридний детектор = Z-score + Isolation Forest (ненаглядоване навчання)

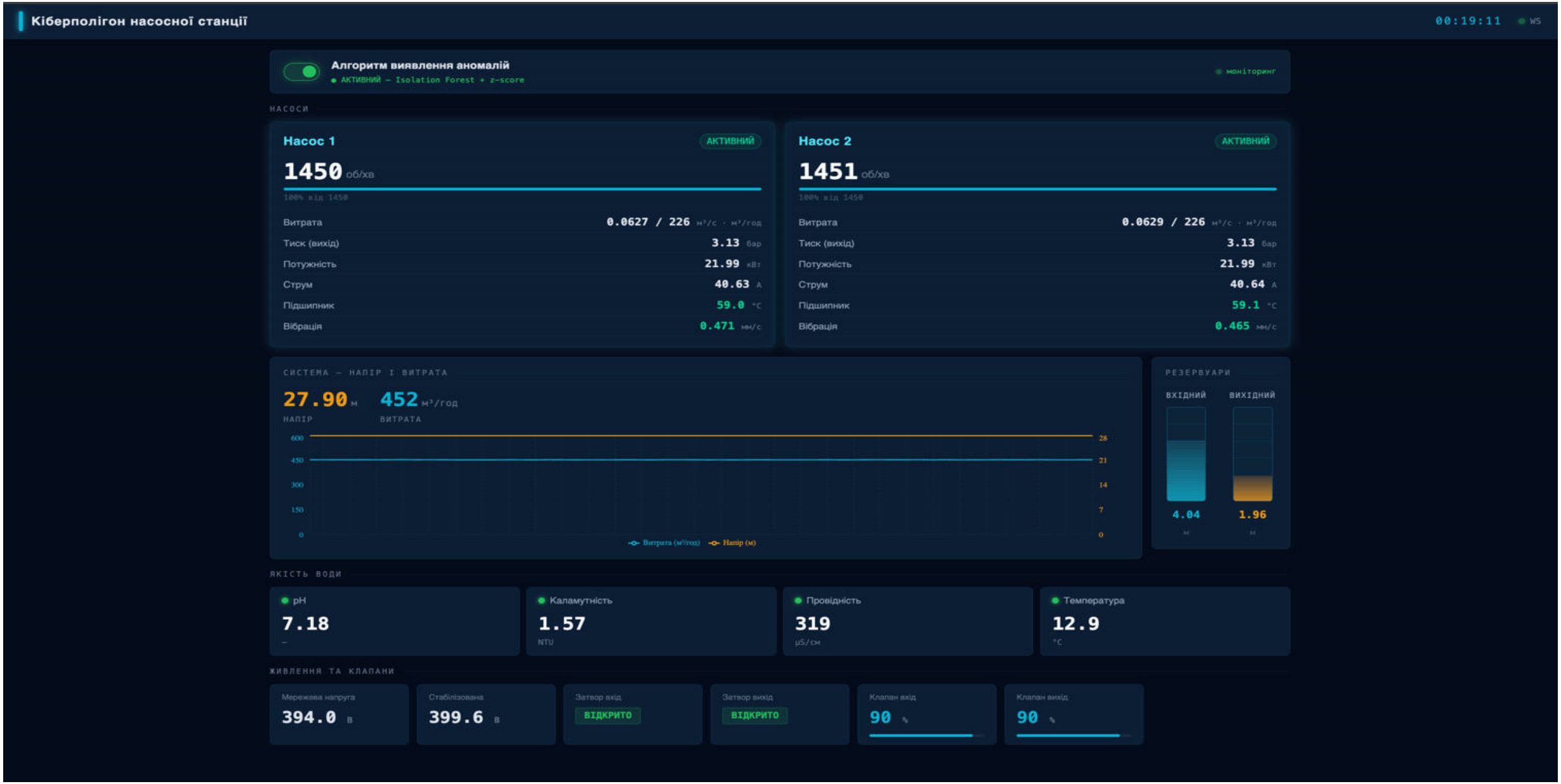
Метод	Тип навчання	Точність	Повнота	AUC (тест)	F1-міра	Роль у конвеєрі
Z-score	Без учителя	—	—	—	—	Виявляє FDI, DoS, Replay (через head_residual)
Isolation Forest	Без учителя	0,906	0,509	0,899	0,652	Підвищує Precision у комбінації
OCSVM	Без учителя	0,655	1,000	0,977	0,792	Порівняльний базовий детектор
Комбінований ✓	**Без учителя**	**0,950**	**0,991**	**0,997**	**0,970**	**P=0,950 R=0,991 F1=0,970 — обрано**

* Z-score — детерміністичний детектор, AUC не обчислюється

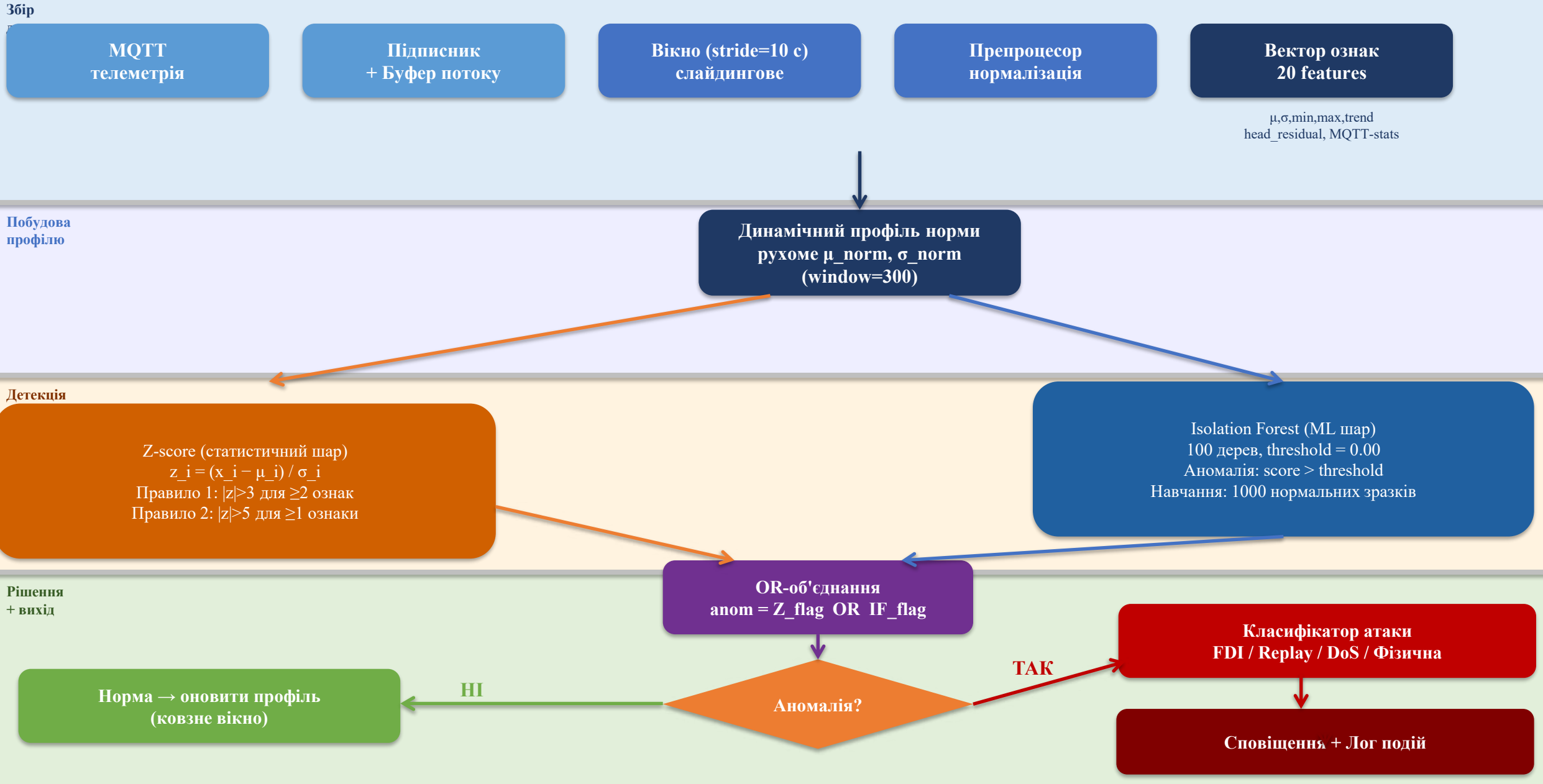
Структурна схема кіберполігону насосної станції



Симуляційна модель кіберполігону — деталі реалізації



Алгоритм виявлення аномалій — блок-схема



Вектор ознак та гібридний детектор

Вектор ознак $x \in \mathbb{R}^{20}$: по 5 статистик (μ, σ, min, max, trend) для кожного з 4 каналів + head_residual + MQTT_interval + MQTT_burst

Канал 1: Flow
(Q, м³/год)

μ σ min max trend

Канал 2: Head
(H, м)

μ σ min max trend

Канал 3: Power
(P, кВт)

μ σ min max trend

Канал 4: RPM
(n, об/хв)

μ σ min max trend

Фізичний залишок напору $\Delta h = H_{вим} - H_{модель}$

Ключова ознака Replay-атаки: $\Delta h \approx 4–6$ м = 28–43σ
(заморожений flow від 1450 rpm при 1000 rpm)

MQTT-метрики: interval + burst

Міжпакетний інтервал та кількість пакетів у вікні
Ключові ознаки DoS-атаки (різке зростання burst)

Z-score правила детекції

Правило 1: ≥2 ознак з $|z_i| > 3\sigma$ → аномалія

Правило 2: ≥1 ознака з $|z_i| > 5\sigma$ → аномалія (Replay)

Isolation Forest параметри

n_estimators=100, max_samples='auto'

threshold=0.00 (відкалібровано; було 0.10 → 90% FP)

Навчальна вибірка: 1000 нормальних зразків

Сценарії атак у кіберполігоні

FDI (False Data Injection)

- Підміна показань датчиків на фіксоване фальшиве значення
- Детекція: різке відхилення μ та σ ознак від профілю (Z-score)
- Результат: Detection Rate = 100%

Replay Attack

- Зловмисник відтворює легітимний трафік з іншої точки навантаження
- Детекція: фізичний залишок $\Delta h = H_{вим} - H_{модель} \approx 28–43\sigma$
- Результат: Detection Rate = 100%

DoS / MQTT Flooding

- Перевантаження MQTT-брокера потоком фальшивих повідомлень
- Детекція: різке зростання burst та зменшення interval
- Результат: виявляється через критичне падіння message_rate

Фізичні несправності

- Деградація насоса: зростання P при незмінному H і Q
- Детекція: відхилення у power_ratio та head_residual
- Результат: Detection Rate = 95,5% (21/22)

Датасет (тест): 184 зр. | FDI: 43 | Replay: 49 | Фіз.: 22 | Норм.: 70 | IF навч.: 6 959 норм. зразків | n_est=100, thresh=0.00 | Z-score: k=2/3σ; k=1/5σ | Stride: 10 с | QoS: 0

Результати тестування та метрики ефективності

Precision
0,950
9,5/10 виявлень — справжні

Recall
0,991
99,1% реальних атак виявлено

F1-score
0,970
Збалансована точність

AUC-ROC
0,997
≈ ідеальне розділення класів

Деталізація по типах атак

Тип атаки	Виявлено/Всього	Recall	FP Rate
FDI	43/43	100%	0%
Replay	49/49	100%	0%
Фізична аномалія	21/22	95,5%	—
Всього	113/114	99,1%	—

Порівняння детекторів: IF AUC=0,899 | OCSVM AUC=0,977 → Комбінований (Z-score OR IF) AUC=0,997

Обчислювальна ефективність: 7,3 мс/цикл · 5,8 МБ ОЗП · Stride 10 с · 1 Гц · Edge-ready без хмарних ресурсів

Час відгуку: 7,3 мс < 100 мс ✓ | ОЗП: 5,8 МБ < 50 МБ ✓ | Хмарна залежність: відсутня ✓ | Навчання: ненаглядоване ✓

Висновки

1. Проведено аналіз IoT-середовищ та CPS: визначено ключові вразливості, обґрунтовано поведінковий підхід з ненаглядовим навчанням
2. Розроблено симуляційну модель кіберполігону насосної станції (2 насоси + VFD + аналізатор + MQTT) — фізично взаємозалежні параметри в реал. часі
3. Спроєктовано 6-компонентний алгоритм моніторингу з гібридним детектором (Z-score + IF) та вектором із 20 flow-характеристик
4. Комбінований конвеєр: Recall=0,991, Precision=0,950, F1=0,970, AUC=0,997; FDI та Replay виявляються зі 100% повнотою
5. Підтверджено обчислювальну ефективність: 7,3 мс/цикл, 5,8 МБ ОЗП — придатний для edge-computing без хмарних ресурсів
6. Кіберполігон може слугувати основою для подальших досліджень у галузі виявлення загроз в ICS/SCADA-системах

ДЯКУЮ ЗА УВАГУ!

Муренко Данііл В'ячеславович | БІКС-22 | КНУБА 2026

«Проєктування алгоритму моніторингу мережевої поведінки,
спрямованого на оперативне виявлення зловмисної активності
в масштабованих IoT-середовищах»