При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение № 14.578.21.0231, уникальный идентификатор соглашения RFMEFI57817X0231).

ФГАОУ ВО «Санкт-Петербургский государственный политехнический университет Петра Великого»

Применение мультифрактальных и вейвлет-эвристик для обнаружения аномалий в сверхвысоких объемах трафика сетевой инфраструктуры цифрового производства

Лаврова Дарья Сергеевна, Штыркина Анна Александровна

Системы цифрового производства

Мониторинг оборудования

Контроль эффективности

Программное управление устройствами

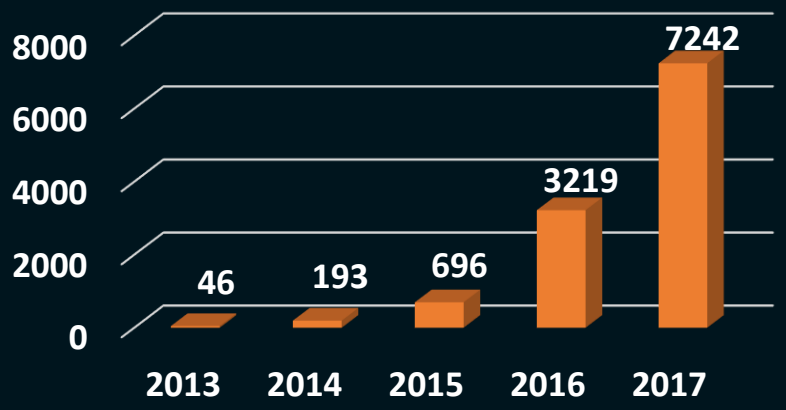
Контроль производства

Управление Умным Домом

Системы ЦП

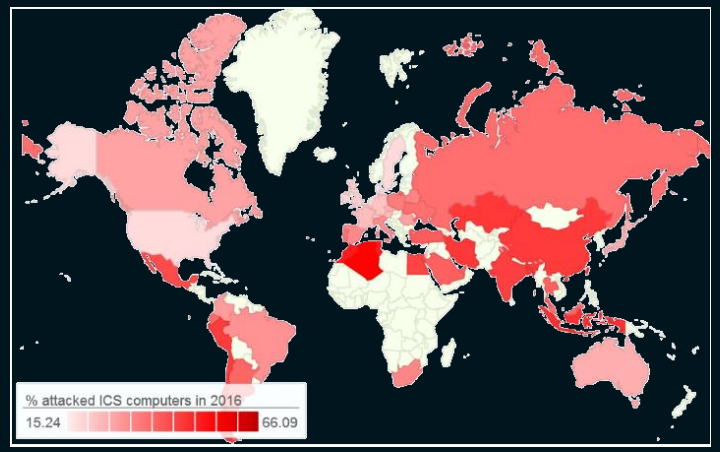
- АСУ ТП
- Интернет Вещей
- MANET/VANET/FANET сети и т.д.

Количество образцов вредоносного ПО для «умных» устройств



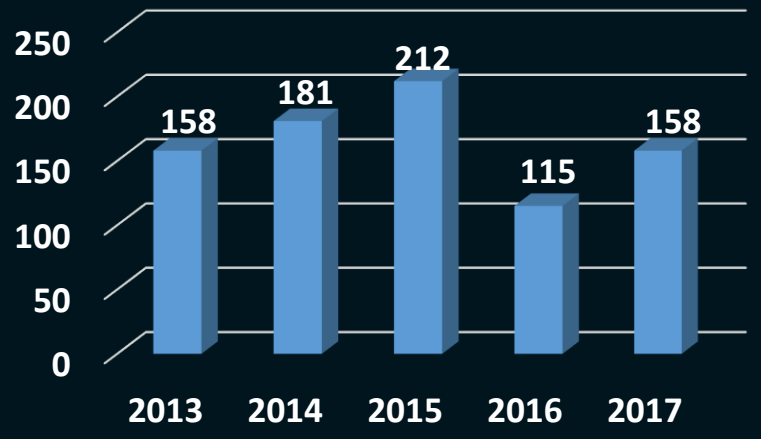
Согласно исследованию Лаборатории Касперского 2017 года

Интенсивность атак на индустриальные компьютеры



Согласно исследованию Лаборатории Касперского (ICS CERT) 2016 года

Общее число уязвимостей АСУ ТП



Согласно исследованию Positive Technologies 2017 года

Обеспечение безопасности систем цифрового производства

Проблемы:

- Разнородность компонентов системы
- Структурная сложность системы
- Высокая интенсивность генерации данных
- Большой объем данных
- Необходимость обнаружения атак и реагирования на них в режиме реального времени

Решение:

АНАЛИЗ СЕТЕВОГО ТРАФИКА

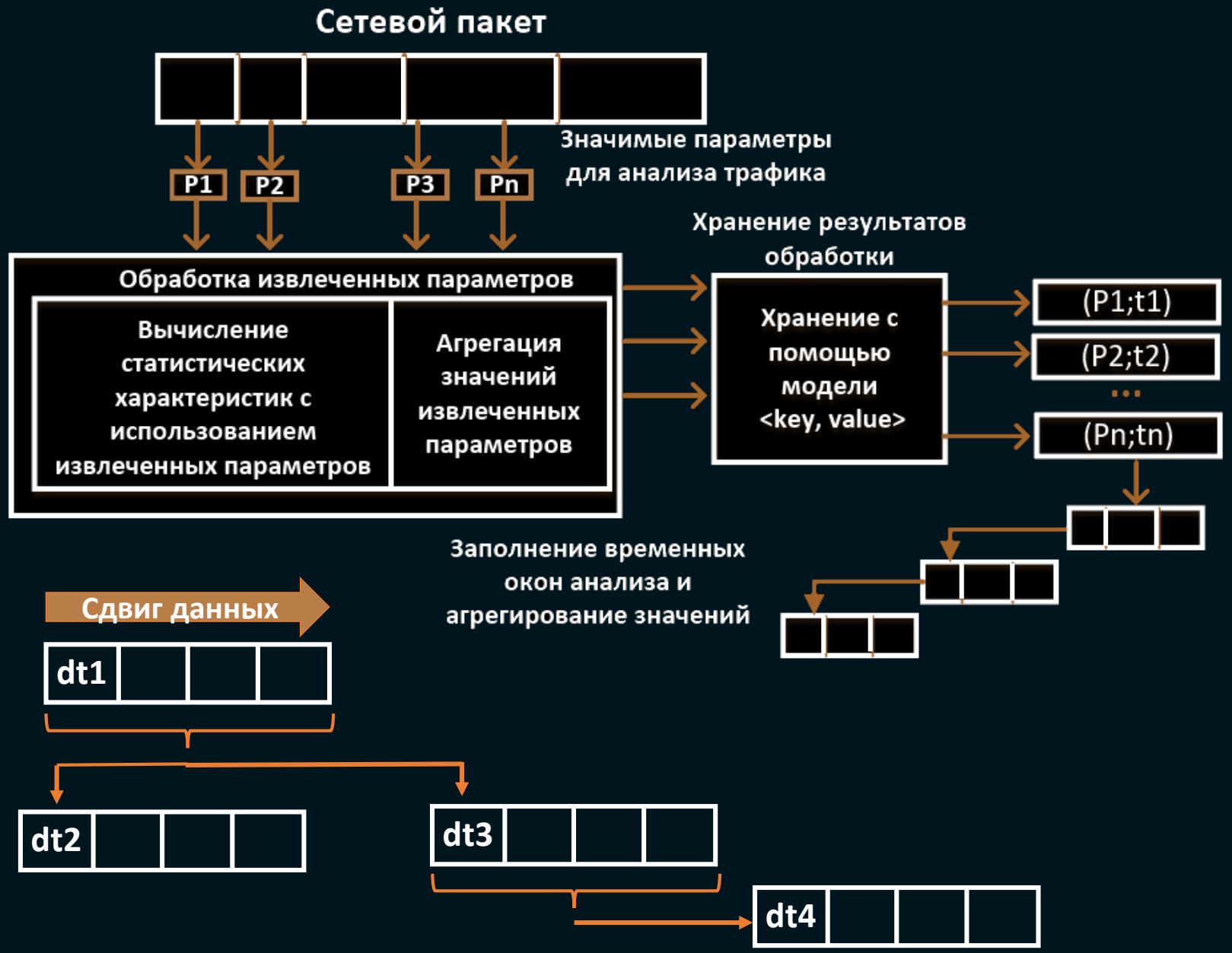
Задачи:

- Сокращение объема данных
- Увеличение скорости обработки информации
- Разработка методов точного обнаружения аномалий сетевой инфраструктуры системы

Оценка мультифрактального спектра Лежандра

Дискретный вейвлет-анализ

Сокращение размерности данных



Извлечение параметров

- Средний размер пакета 1500 байт
- 50 значимых параметров (P)
- 10 байт на параметр (m)
- Итого – сокращение размерности до 66%

Агрегация данных

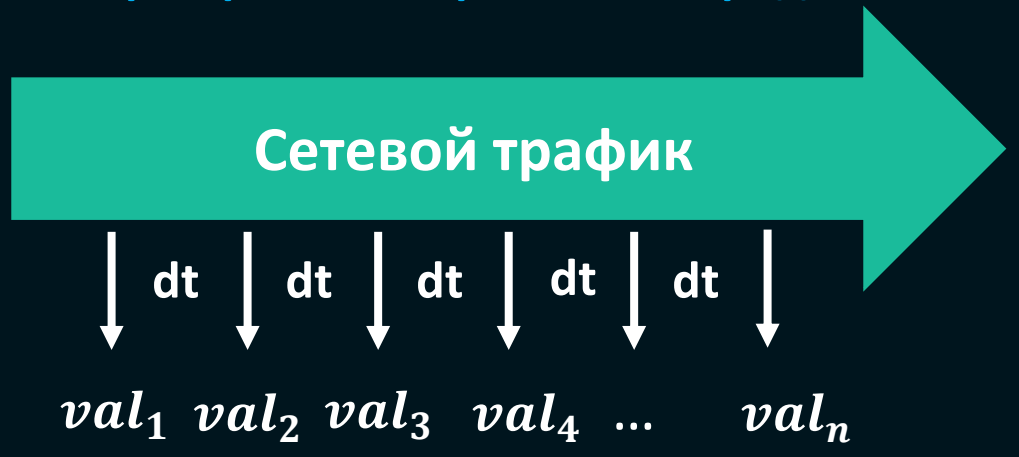
- Агрегирование данных
- Формирование иерархически-зависимых окон
- Пусть число окон $N = 10$, число элементов в ряду $m = 1000$
- Объем $V = N * P * B * m = 4.8$ Мб

Мультифрактальный анализ

Параметры для формирования временных рядов

- IP-адреса отправителя и получателя;
- порты отправителя и получателя;
- временная метка;
- размер сетевого пакета;
- число сетевых пакетов в потоке;
- число сетевых пакетов протоколов каждого типа;
- число исходящих и входящих подключений для хоста;
- число пакетов с флагами SYN, ACK, RST и т. д.
- другие параметры, настраиваемые пользователем

Формирование временного ряда



Оценка мультифрактального спектра

Мелкий масштаб
- Мультифрактальный анализ
- Локальный тренд

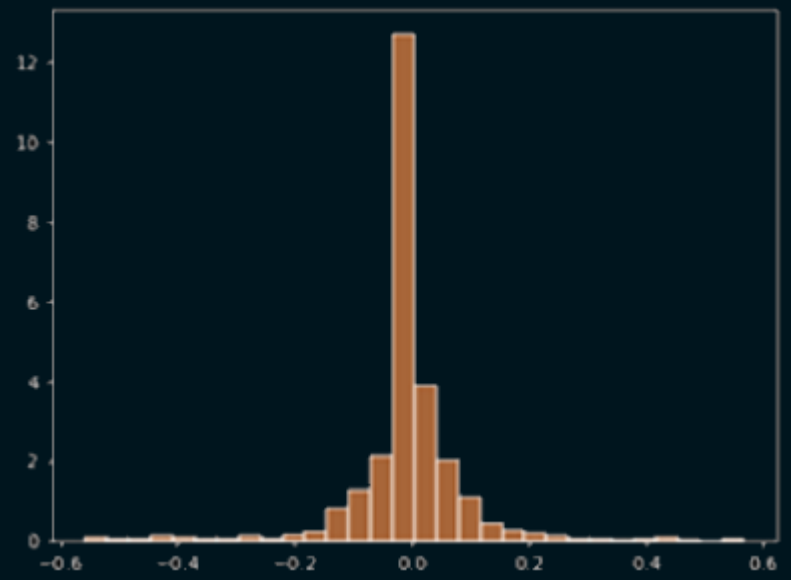
Крупный масштаб
- Фрактальный анализ
- Глобальный тренд

- **Спектр** $D_q = \frac{\tau(q)}{q-1}$, где $\tau(q)$ **- скейлинговая функция**
- **Применяем преобразование Лежандра**
- $f_L(\alpha) = \inf_{q \in R}(\alpha q - \tau(q))$ **- мультифрактальный спектр Лежандра**
- **Ширина спектра** $width = \alpha_{max} - \alpha_{min}$

Вейвлет-анализ

Дискретное вейвлет-преобразование:

$$dwt(t_i) = \sum a_{m,k}\,\varphi_{m,k}\,(t_i) + \sum\sum d_{m,k}\psi_{m,k}(t_i)$$



$DWT(X(t)$

Коэффициенты детализации
- Локальные изменения
- Нормальный закон распределения

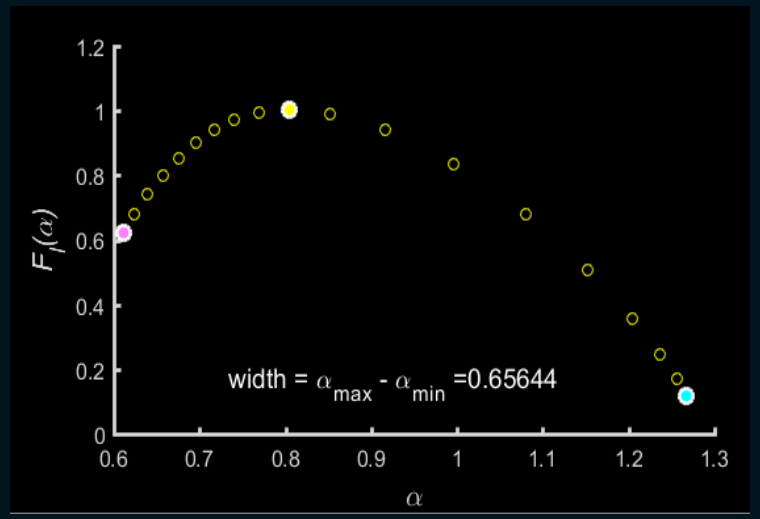
Коэффициенты аппроксимации
- Глобальные изменения
- Экспоненциальный закон распределения

- **Задача анализа – поиск разладки во временном ряду, образованном коэффициентами детализации**
- **Метод поиска – Байесовский онлайн метод поиска разладки**

$P(r_t, |x_{1:t}) = \frac{P(r_t, x_{1:t})}{P(x_{1:t})}$ – апостериорное распределение случайной величины r_t

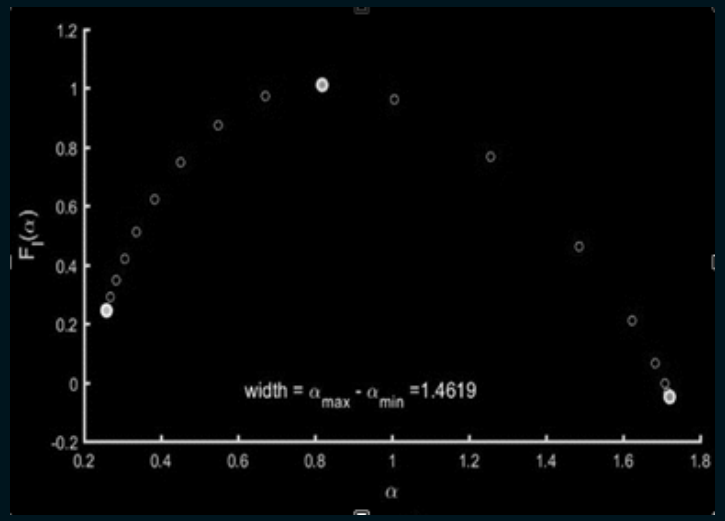
Экспериментальные результаты (1)

Атака SYN-flood



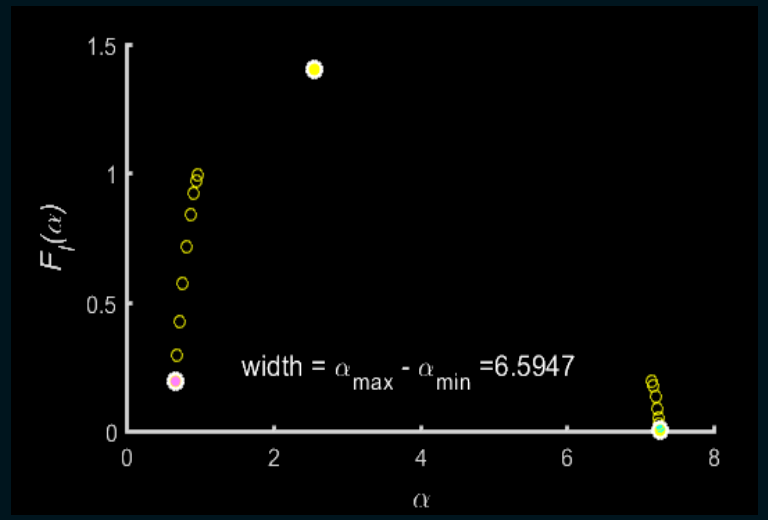
Нет атаки

Атака smurf

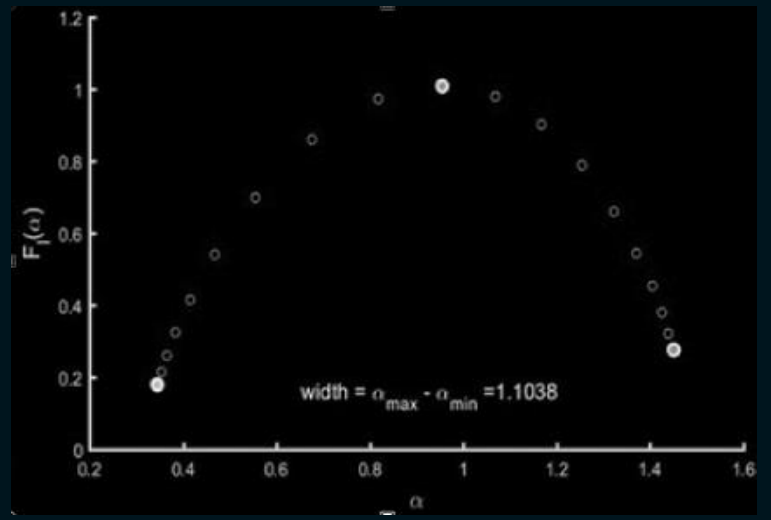


Нет атаки

Атака

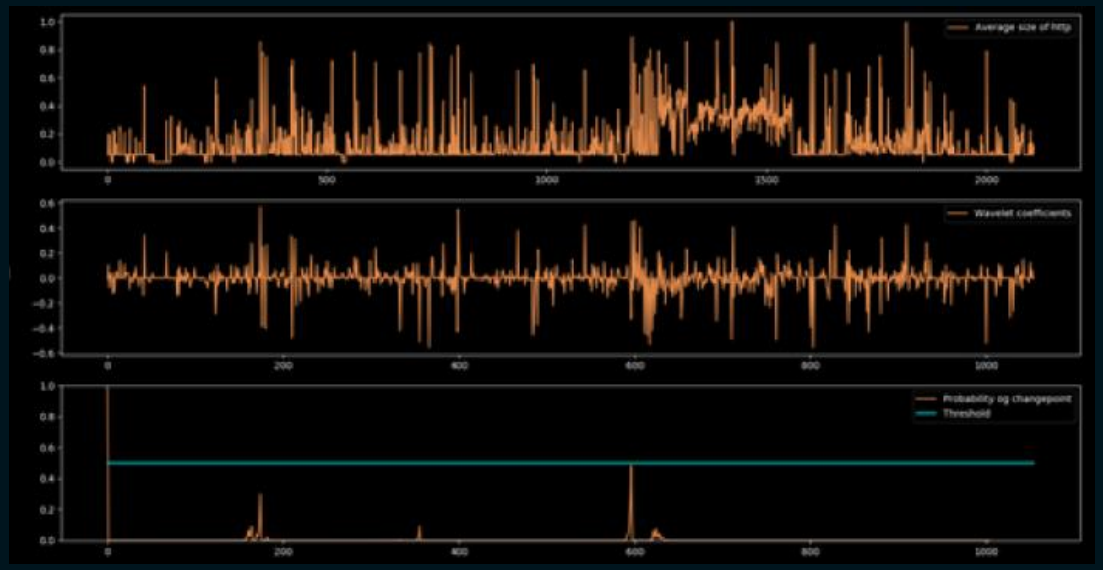


Атака

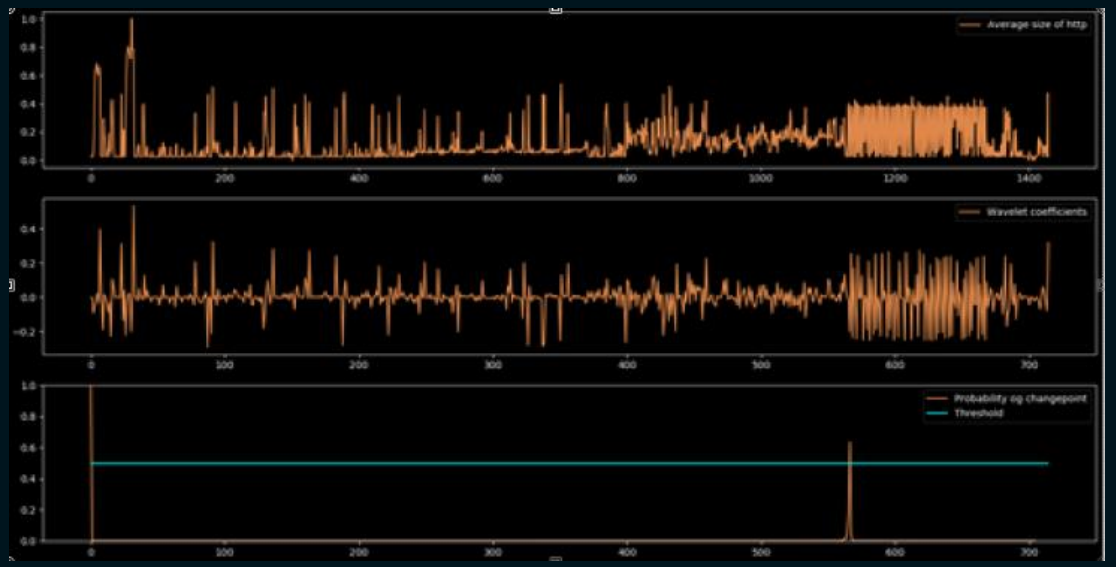


Экспериментальные результаты (2)

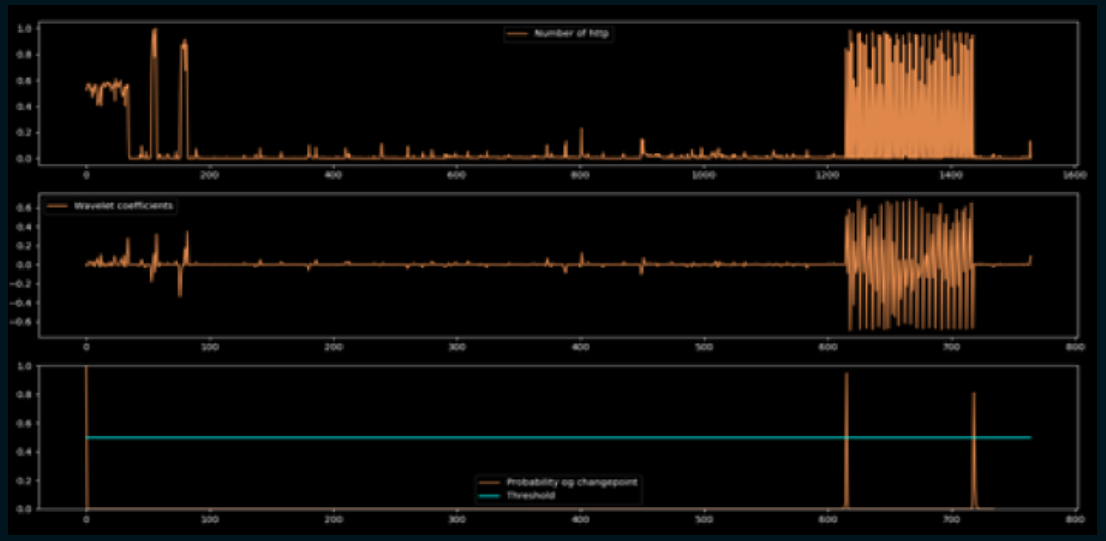
Нет атаки



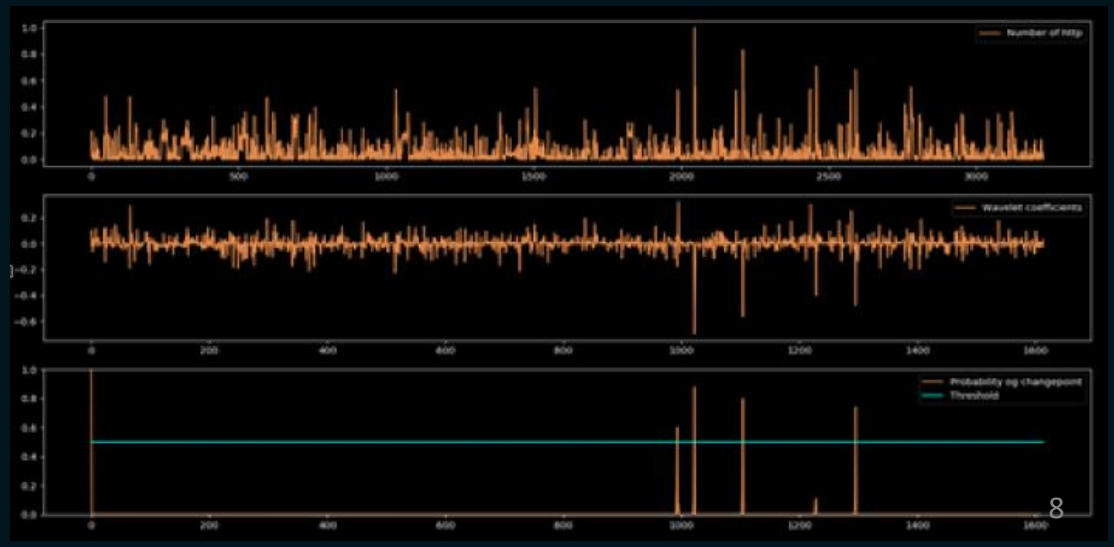
Атака HTTP-Flood



Атака Slowloris



Атака smurf



Выводы

Сокращение размерности данных

- На этапе извлечения значимых параметров размерность данных сокращается на 66%
- Результирующий объем данных после второго этапа не зависит от первоначального объема

Мультифрактальный анализ трафика

- Вычисление ширины мультифрактального спектра Лежандра позволяет исследовать структуру анализируемых данных, а также оценить характер проходящей атаки

Дискретный вейвлет-анализ трафика

- Вейвлет-анализ в совокупности в байесовским методом обнаружения разладки позволяет обнаруживать момент времени, советующий началу атакующих воздействий

Дальнейшие направления исследований

- Оценка порогового изменения значения ширины мультифрактального спектра для более точного обнаружения атак
- Эффективная реализация метода поиска мультифрактального спектра
- Исследование других методов поиска разладки во временных рядах, сравнение с байесовским методом
- Анализ глобального тренда трафика для выявления атак

СПАСИБО ЗА ВНИМАНИЕ!