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 о предоставлении субсидии № 14.575.21.0100 от 14.11.2014, уникальный идентификатор RFMEFI57514X0100).

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

SIEM-СИСТЕМА ДЛЯ ВЫЯВЛЕНИЯ И АНАЛИЗА ИНЦИДЕНТОВ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ВЕЩЕЙ

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

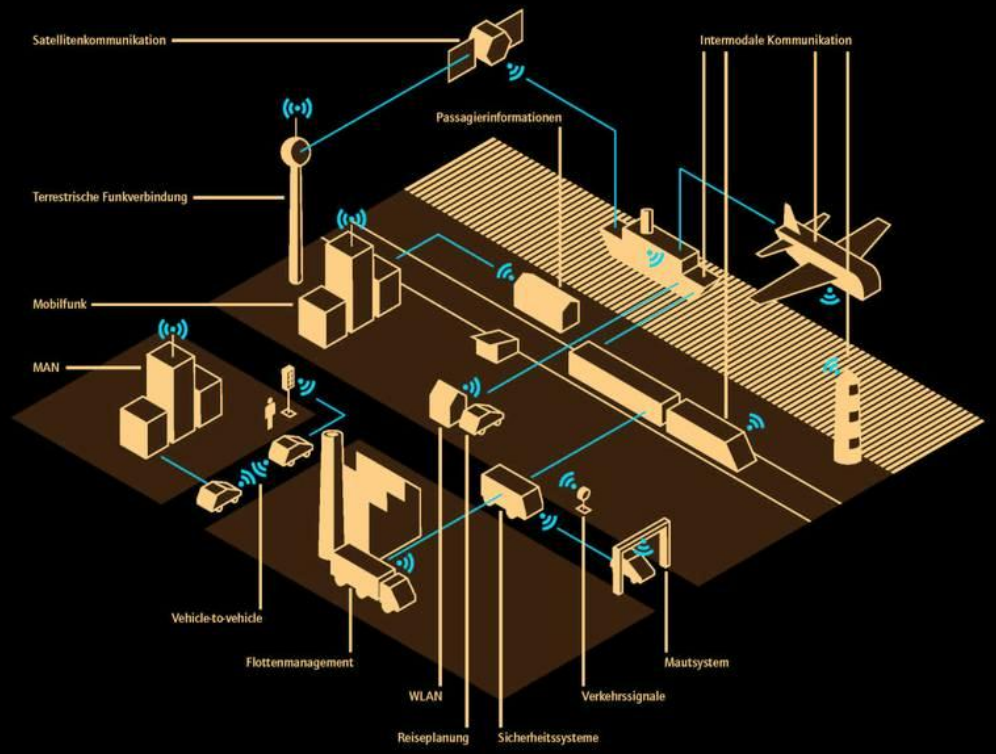
Лаврова Дарья Сергеевна

Интернет Вещей и киберфизические системы

Концепция Интернета Вещей (ИВ) предполагает:

- ✓ **Зависимость протекания физических процессов от информационных**
- ✓ **Отсутствие человека как управляющей функциональной единицы**
- ✓ **Наличие собственной подсистемы управления, способной восстанавливать и поддерживать корректность функционирования системы при наличии воздействий**

Системы, реализующие концепцию ИВ – киберфизические системы (КбФС)



Нарушение корректности работы КбФС способно нанести вред жизни людей

Малая мощность большой части устройств Интернета Вещей

Высокая вариативность устройств в составе Интернета Вещей

Необходимость обработки больших массивов гетерогенных данных

Сложность и актуальность задачи обеспечения безопасности ИВ

Угрозы безопасности Интернета Вещей

ИНТЕРНЕТ ВЕЩЕЙ

Подсистема физических устройств

«УМНЫЕ» ФИЗИЧЕСКИЕ УСТРОЙСТВА

- Несанкционированное физическое воздействие на устройство
- Реализация уязвимостей устройства и внедрение ВПО
- Воздействие с использованием специализированных аппаратных устройств (микрозондирование)

Коммуникационная подсистема

СЕТЕВЫЕ ПРОТОКОЛЫ И ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ

RFID

6LOWPAN

СЕТЕВОЕ КОММУНИКАЦИОННОЕ ОБОРУДОВАНИЕ

- Перехват, подмена, модификация, удаление, анализ данных
- Реализация уязвимостей сетевых протоколов
- Криптографический анализ зашифрованных данных
- Сетевое воздействие на устройства

Подсистема управления

СЕРВЕРЫ И КОМПОНЕНТЫ УПРАВЛЕНИЯ

СЕРВЕРА ОБРАБОТКИ, БАЗ ДАННЫХ, ВЕБ-СЕРВЕРА

- Манипуляция параметрами управления и настройками устройств
- Установка ВПО
- Манипуляция внешней информацией
- Нарушение целевой функции системы

Человеко-машинный интерфейс

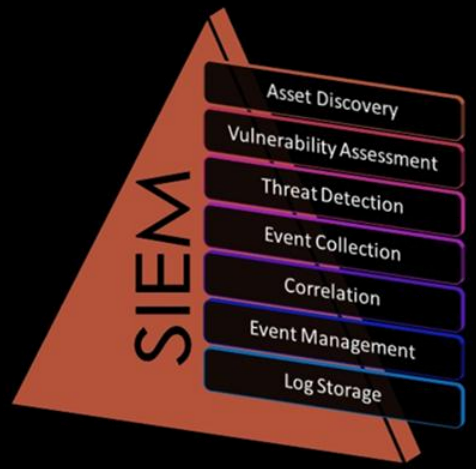
ВЕБ-ИНТЕРФЕЙС И ПРИЛОЖЕНИЯ

ПОТРЕБИТЕЛИ УСЛУГ

- Реализация уязвимостей интерфейса
- Сбор и анализ пользовательских данных (нарушение приватности)
- Получение несанкционированных данных с использованием социальной инженерии

SIEM-система для Интернета Вещей

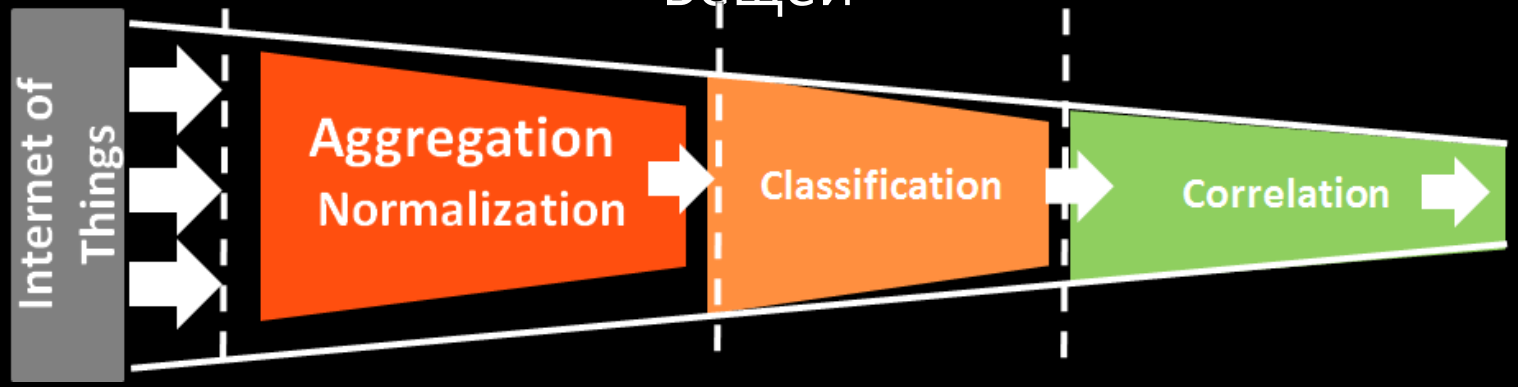
Подход к анализу безопасности Больших Данных в Интернете Вещей



Основные задачи при разработке SIEM системы для ИВ

- ✓ Сбор и агрегация данных от устройств
- ✓ Нормализация данных
- ✓ Обучение системы
- ✓ Анализ данных для обнаружения и расследования инцидентов безопасности
- ✓ Визуализация результатов анализа

Предобработка данных от устройств Интернета Вещей



Миллион сообщений Тысячи сообщений Десятки событий

Способы сбора данных

- ✓ Сбор данных напрямую с конечных устройств
- ✓ Сбор данных через шлюз
- ✓ Использование сервера для сбора данных

Архитектура SIEM-системы для Интернета Вещей

СБОР РАЗНОРОДНЫХ ДАННЫХ ОТ БОЛЬШОГО ЧИСЛА УСТРОЙСТВ

ПРЕДВАРИТЕЛЬНАЯ ОБРАБОТКА ДАННЫХ

- АГРЕГАЦИЯ ДАННЫХ ОТ УСТРОЙСТВ ПО ВРЕМЕНИ
- НОРМАЛИЗАЦИЯ ДАННЫХ ОТ УСТРОЙСТВ
- АГРЕГАЦИЯ ДАННЫХ ОТ УСТРОЙСТВ ПО ОБЪЕКТУ
- ФОРМИРОВАНИЕ СПРАВОЧНИКОВ МЕТАДАННЫХ
- ТРАНСФОРМАЦИЯ ДАННЫХ В СОБЫТИЯ

БАЗА ЗНАНИЙ

АВТОМАТИЧЕСКОЕ ПОСТРОЕНИЕ ОНТОЛОГИЙ

ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ

- АНАЛИЗ ЗНАЧЕНИЙ ПАРАМЕТРОВ УСТРОЙСТВ
- АНАЛИЗ КОММУНИКАЦИОННЫХ СВЯЗЕЙ
- АНАЛИЗ ЗАВИСИМОСТЕЙ В ДАННЫХ

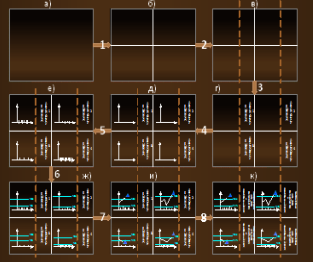
ОБУЧЕНИЕ SIEM-СИСТЕМЫ

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ

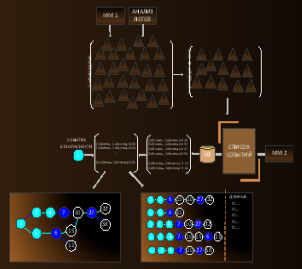
ПОСТРОЕНИЕ НАБОРОВ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ВЗАИМОСВЯЗАННЫХ СОБЫТИЙ

ВИЗУАЛИЗАЦИЯ РЕЗУЛЬТАТОВ АНАЛИЗА

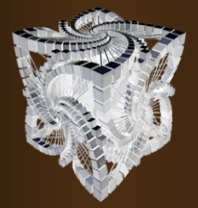
ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ



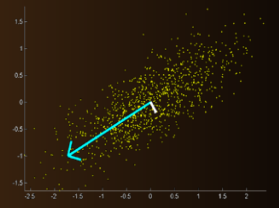
РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ



ОБЩАЯ ОЦЕНКА УРОВНЯ БЕЗОПАСНОСТИ



ФРАКТАЛЬНЫЕ МЕТОДЫ



МЕТОД ГЛАВНЫХ КОМПОНЕНТ

Процесс преобразования и загрузки данных в SIEM-системе ИВ

Двухэтапная агрегация данных от устройств Интернета Вещей

Процесс преобразования и загрузки данных в интернете вещей

Выбор и анализ параметров для SIEM-системы Интернета Вещей

Основные задачи:

- ✓ **Выбор параметров Интернета Вещей для последующего анализа безопасности**
- ✓ **Подходы к анализу выбранных параметров**

Выбор параметров Интернета Вещей

- ❑ Устройства:
  - ❖ Тип устройства
  - ❖ Параметры устройства
  - ❖ Значения параметров
- ❑ Коммуникационные связи:
  - ❖ Направление связи
  - ❖ Наличие/отсутствие связи
  - ❖ Время
- ❑ Зависимости между данными, характеризующие протекание физического процесса

Подходы к анализу выбранных параметров

Мониторинг значений параметров каждого устройства:

- ❑ Корреляция событий на основе правил (rule-based event correlation)
- ❑ Корреляция событий на основе статистики (statistic event correlation)

Анализ коммуникационных связей:

- ❑ Мониторинг наличия/отсутствия связей
- ❑ Анализ характеристик связей

- ❑ Анализ схожести событий на основе метрик и весовых коэффициентов
- ❑ Выявление и мониторинг нелинейных зависимостей между данными

Выявление инцидентов безопасности в Интернете Вещей

Корреляция на основе правил

Априорно небезопасные события, характеризующиеся

- Отсутствием данных от устройства
- Сообщениями об ошибке
- Соединением с IP-адресами из black-list
- Событиями неизвестного типа

Корреляция на основе статистики

Потенциально небезопасные события, характеризующиеся

- Количеством событий
- Значениями параметров событий
- Временными параметрами

Автокорреляция

Потенциально небезопасные события, характеризующиеся значениями параметров событий

Выявление зависимостей между данными

По N наблюдениям от показателей y_i $(i = 1,2,3, \dots, N)$, имеющимся в распоряжении исследователя, можно построить степенную функцию $(N-1)$-й степени

$$\widehat{y_i} = a_0 + a_1 i + a_2 i^2 + a_3 i^3 + \cdots + a_{N-1} i^{N-1}$$

Этот полином так опишет исходный ряд наблюдений $\{y_i\}$, что его расчётные значения $\widehat{y_i}$ в каждой i-й точке в точности будут соответствовать фактическим значениям y_i

Коэффициент согласия в динамике $k_s = \dfrac{\sum_i \overline{\Delta}^i y \, \overline{\Delta}^i x}{\sqrt{\sum_i (\overline{\Delta}^i y)^2 \sum_i (\overline{\Delta}^i x)^2}}$

- Одновременная близость коэффициентов корреляции и согласия в динамике к единице говорит о сильной линейной взаимосвязи
- Близость коэффициента согласия в динамике к единице при значении коэффициента корреляции, не близком к единице, говорит о возможной нелинейной взаимосвязи или линейной с лагами

Расследование инцидентов безопасности в Интернете Вещей

GU Zhaojun, Yong LI. Research of Security Event Correlation based on Attribute Similarity. International Journal of Digital Content Technology and its Applications. Volume 5, Number 6, June 2011

Последовательность действий

1. В зависимости от типа инцидента, который обнаруживается, назначить весовые коэффициенту каждому типу параметров событий
2. Задать порог, который будет означать, что если функция схожести принимает значения больше данного порога, то события с достаточной степенью силы взаимосвязаны между собой
3. Используя функцию схожести, вычислить корреляцию между событиями
4. Сравнить полученное значение с пороговым значением
5. Группировать взаимосвязанные события

$$event = \{source, destination, action, time\}$$

Получение меры схожести между двумя типами атрибутов

- ❑ корреляция символьных параметров
- ❑ корреляция числовых параметров

Функция схожести символьных параметров

$$Sim_{cha}(event_i, event_j) = \sum_{k=1}^{p} \frac{\varphi(value_{ik}, value_{jk})}{p}$$

Функция схожести числовых параметров

$$Sim_{num}(event_i, event_j) = \frac{\sum_{f=1}^{n} \omega_f Sim_f(event_i, event_j)}{\sum_{f=1}^{n} \omega_f}$$

$$Sim(event_i, event_j) = \mu Sim_{cha}(event_i, event_j) + (1-\mu) Sim_{num}(event_i, event_j)$$

Общая оценка уровня безопасности в Интернете Вещей

Анализ устойчивости (самоподобия) системы фрактальными методами

1. Анализ периодичности многомерных временных рядов с использованием автокорреляционной функции
2. Вычисление фактора самоподобия (фактора Фано)

Сокращение размерности пространства методом главных компонент (МГК)

1. Построение ковариационной матрицы
2. Поиск главных компонент
3. Анализ влияния изменений показателей на значение главной компоненты

Используется фрагмент системы Интернета Вещей для выращивания растений

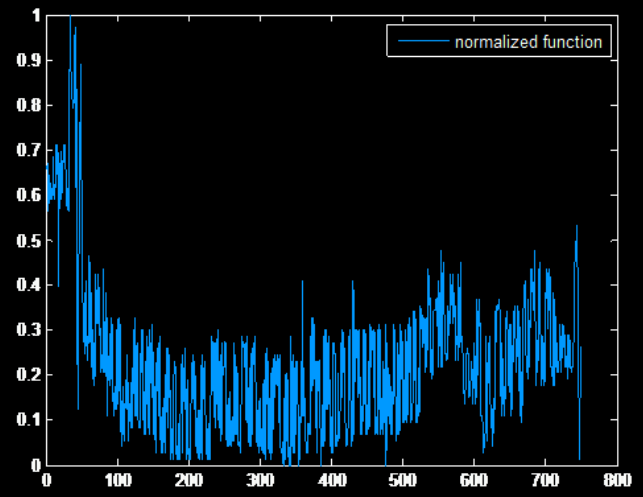
Анализ показаний:

- ❑ температурных данных
- ❑ данных освещенности
- ❑ данных влажности воздуха

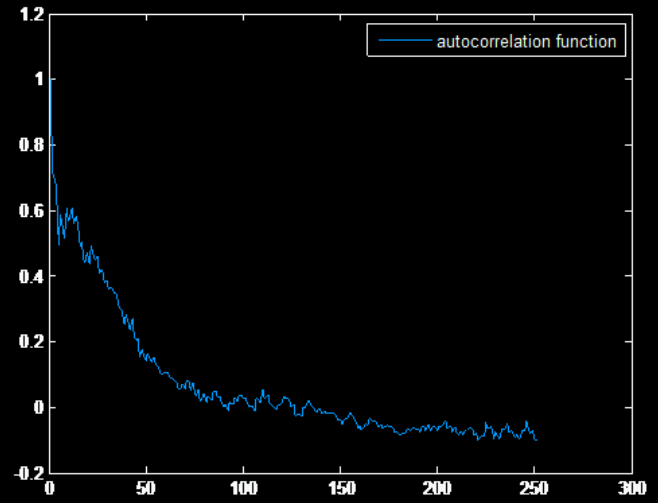
Проведенные экспериментальные исследования

Данные освещенности при нормальном функционировании системы

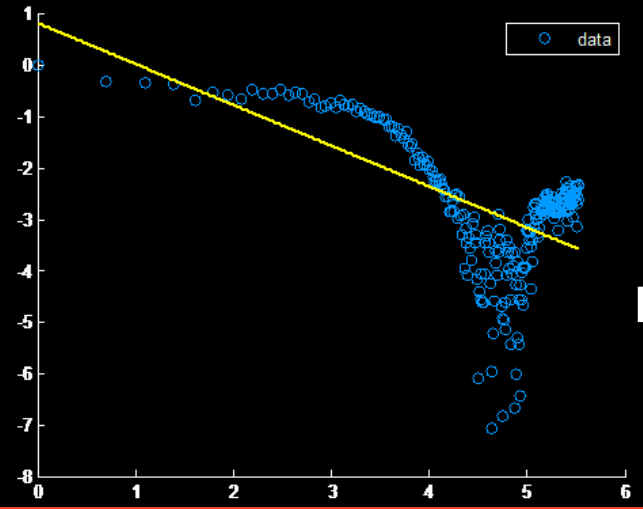
Нормированная функция



Автокорреляционная функция

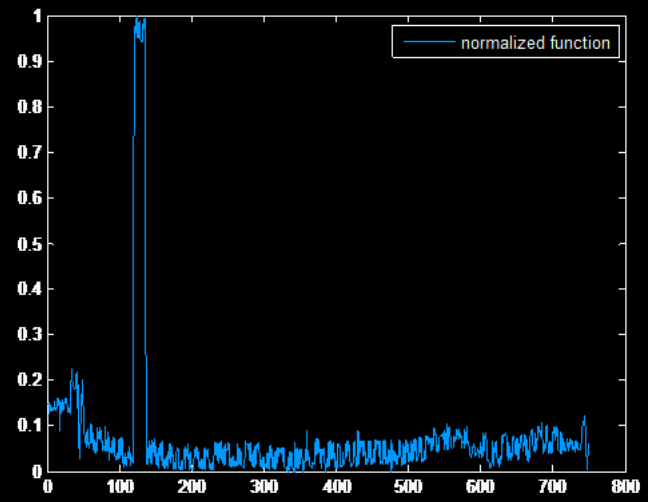


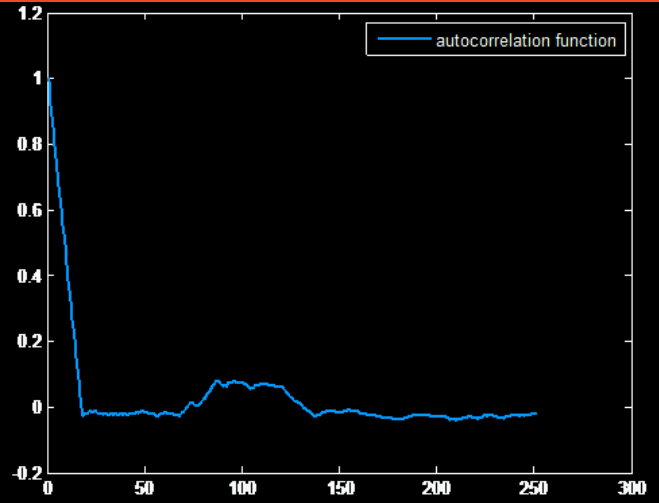
Вычисление фактора Фано

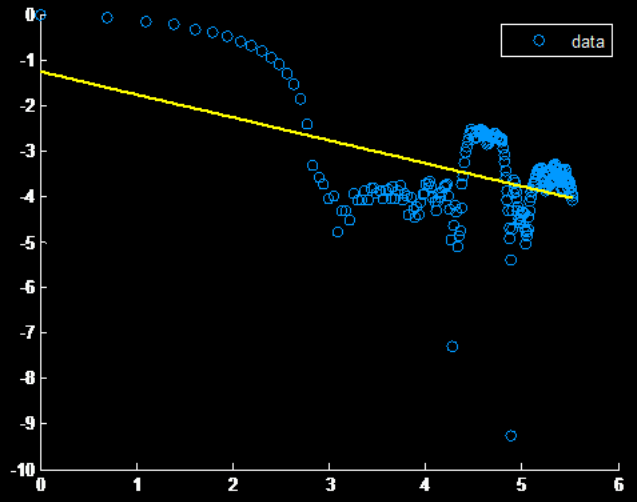


F = 0.792922

Данные освещенности, содержащие резкий скачок значений





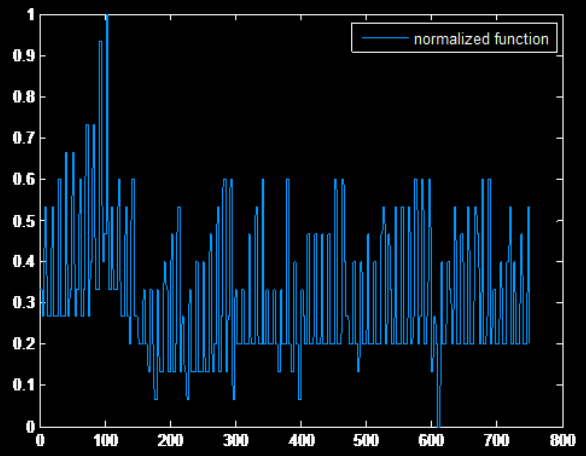


F = 0.503528

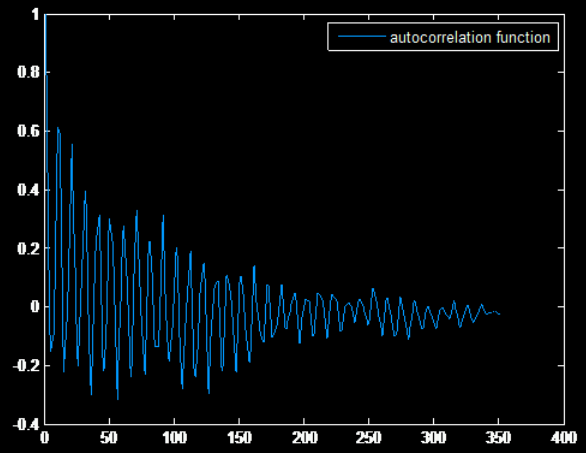
Проведенные экспериментальные исследования (2)

Данные влажности воздуха при нормальном функционировании системы

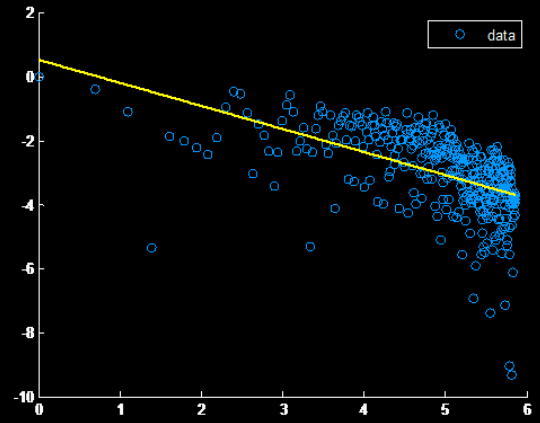
Нормированная функция



Автокорреляционная функция

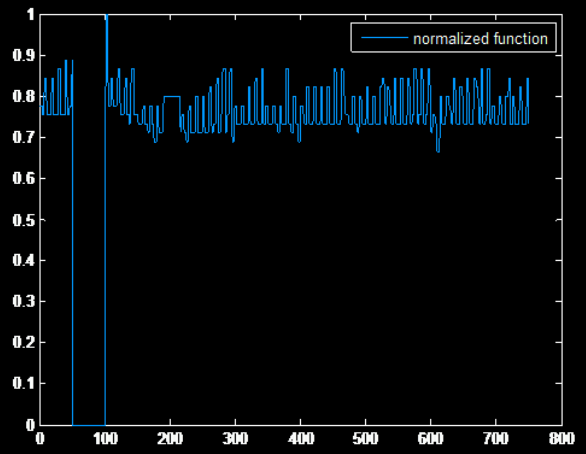


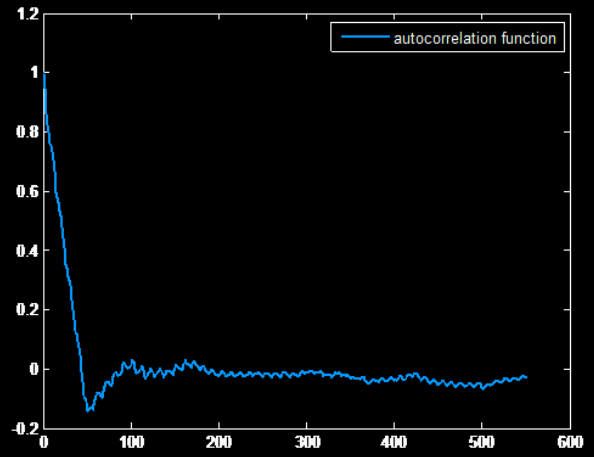
Вычисление фактора Фано

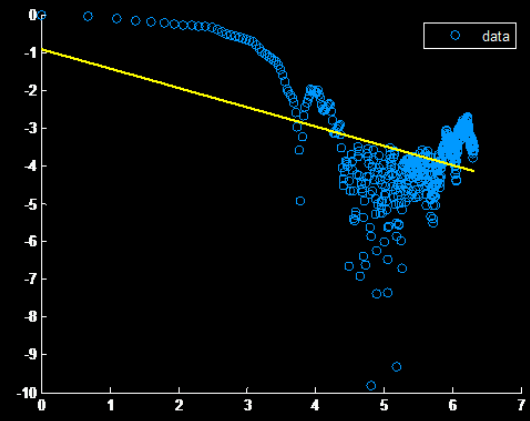


F = 0.719106

Данные влажности воздуха при прекращении поступления данных от устройств





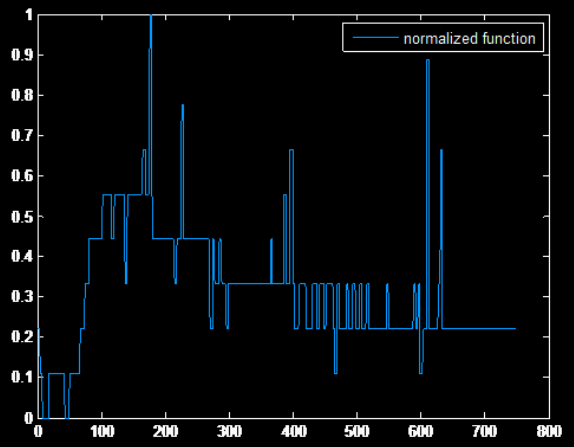


F = 0.511200

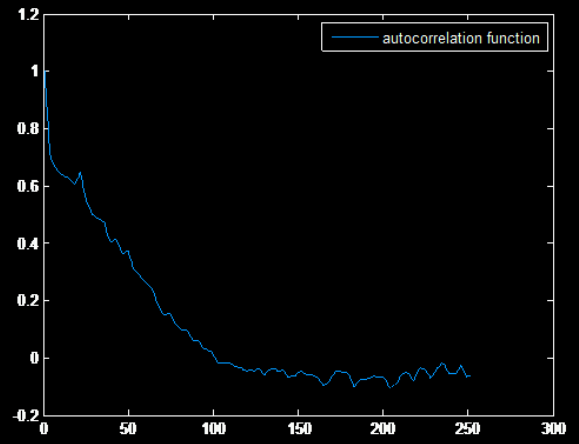
Проведенные экспериментальные исследования (3)

Данные температуры при нормальном функционировании системы

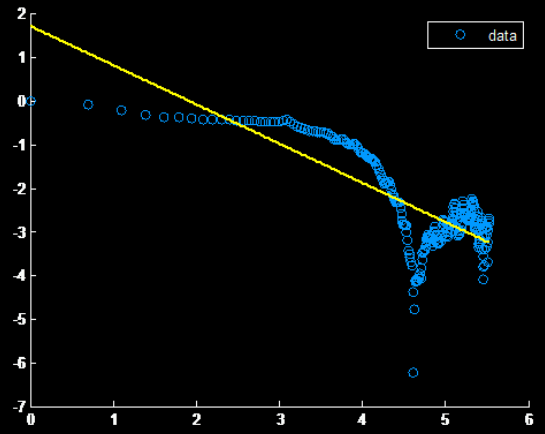
Нормированная функция



Автокорреляционная функция

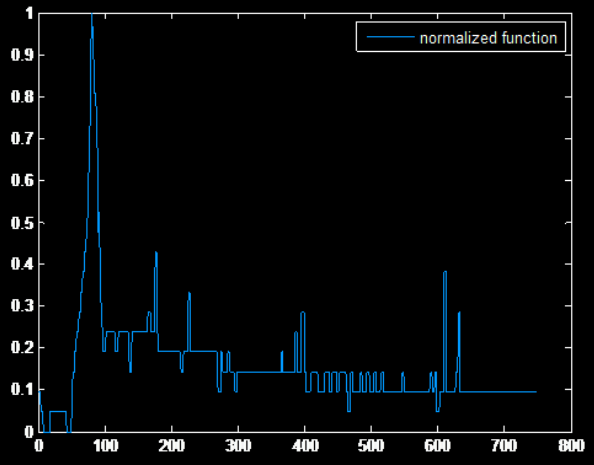


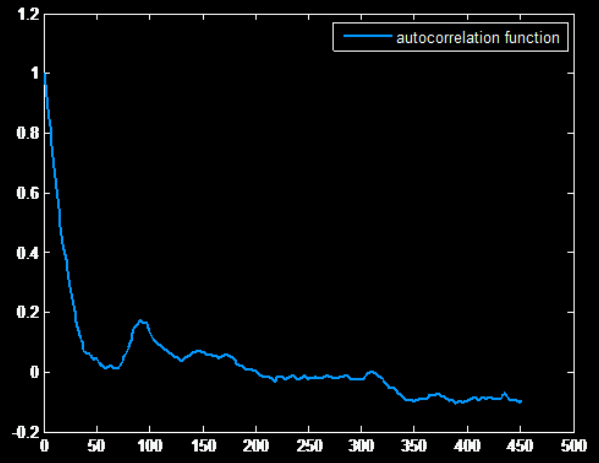
Вычисление фактора Фано

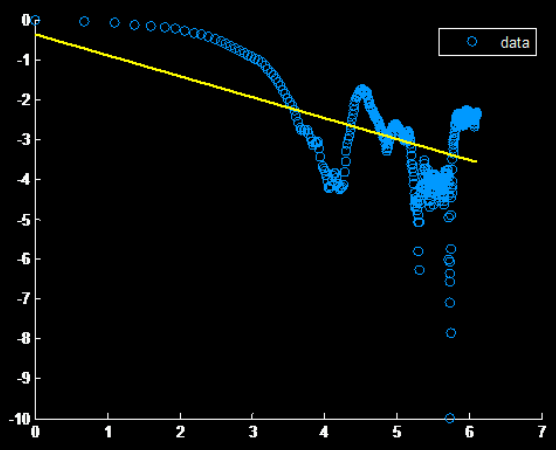


F = 0.896760

Данные температуры при плавном целенаправленном изменении



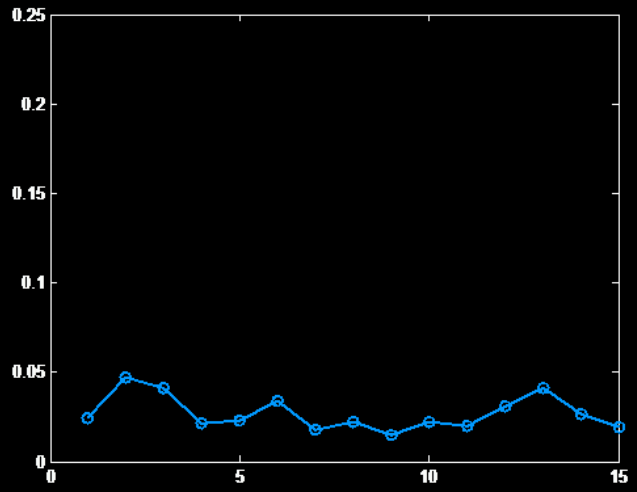




F = 0.525045

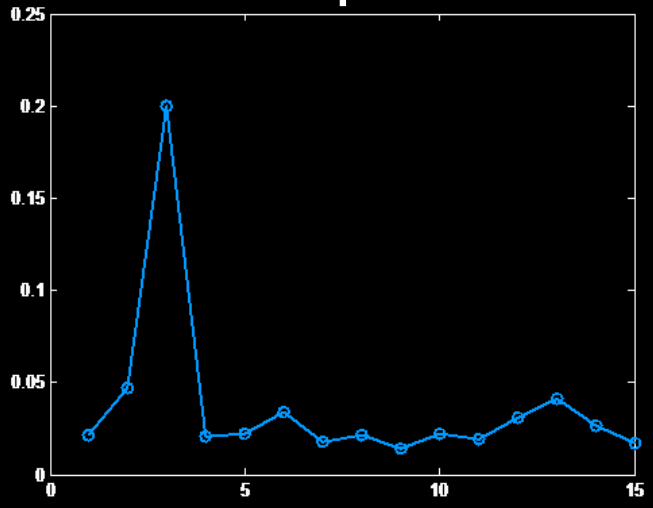
Проведенные экспериментальные исследования (4)

Метод главных компонент

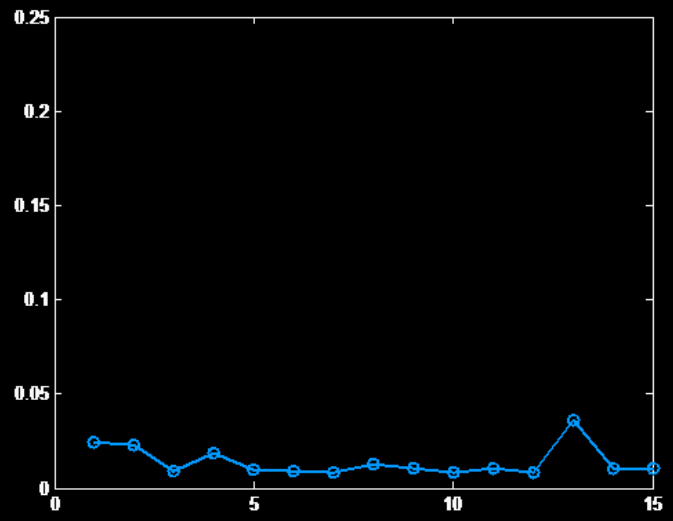


Значение главной компоненты при нормальном функционировании системы

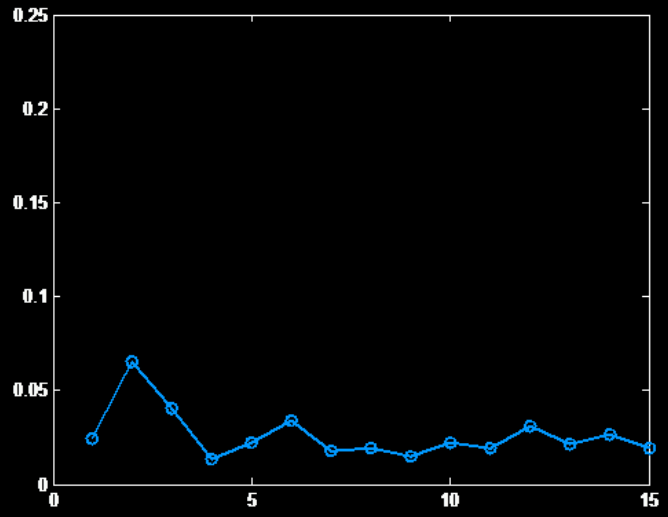
Скачок значений данных освещенности



Прекращение поступления данных влажности



Плавное целенаправленное изменение значений температуры



Результаты и дальнейшее направление исследований

Результаты

1. Предложен подход к анализу безопасности Интернета Вещей, базирующийся на концепции SIEM-системы
2. Предложены подходы к выявлению и расследованию инцидентов безопасности в Интернете Вещей:
   - Мониторинг значений параметров устройств
   - Мониторинг коммуникационных связей между устройствами
   - Выявление и мониторинг зависимостей в данных
   - Анализ взаимосвязи событий
3. Рассмотрены подходы к общей оценке уровня безопасности Интернета Вещей

Направление работ

- Проведение экспериментальных исследований на многомерных временных рядах
- Разработка методов вычисления пороговых значений, определяющих допустимое отклонение фактора самоподобия
- Применение методов выявления разладки процесса наблюдений

СПАСИБО ЗА ВНИМАНИЕ!