Профессор, д.т.н. П. Д. Зегжда
Профессор, д.т.н. Д. П. Зегжда

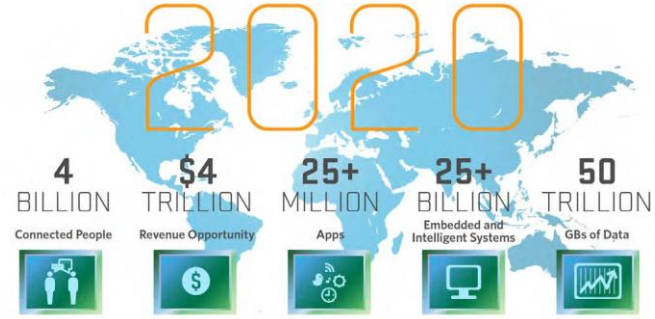
ПОДХОД К ОЦЕНКЕ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ФРАКТАЛЬНЫХ МЕТОДОВ

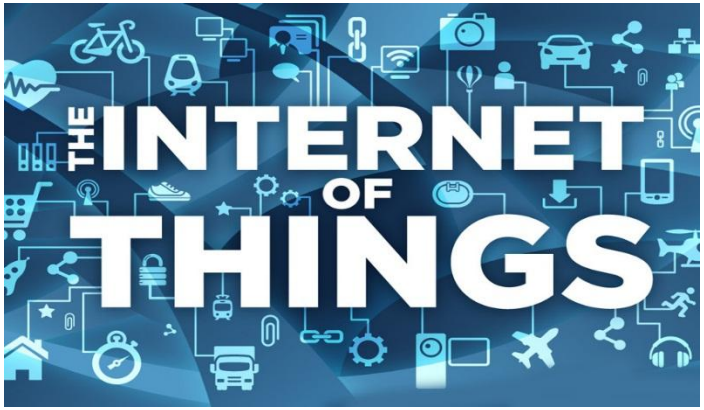
САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

Раздел 1. Киберпространство – новый виток эволюции IT систем

Экспансия компьютеризации принесла с собой всю остроту проблем информационной безопасности состоящую в зависимости работоспособности современного производства от целенаправленных и случайных компьютерных воздействий, приводящих к скрытому, удаленному и труднообнаруживаемому воздействию, которое может вызвать катастрофические последствия.

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ВЕЩЕЙ





Развитие Интернета Вещей в совокупности с отсутствием единых стандартов безопасности

По результатам исследований HP на 2015 год:

- **60%** устройств обладают уязвимым веб-интерфейсом
- **70%** наиболее часто используемых «умных» приборов, имеющих выход в сеть, уязвимы
- **80%** устройств подвержены утечке информации в той или иной степени и когда-то «выдавали» личную информацию о своих владельцах
- **90%** устройств собирают ту или иную персональную информацию о владельце без его ведома

Атаки не на «компьютерные» системы, а на «реальные» (кардиостимуляторы, бытовые устройства, автотранспорт и т.д.)

Раздел 2. Киберугрозы и задачи кибербезопасности

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ КИБЕРПРОСТРАНСТВА

- Информационная безопасность в новых условиях отличается расширенным пониманием объекта защиты как критической информационной среды, исследованием уязвимостей как основной характеристики компонентов критической информационной среды и динамический (нестабильный, «плавающий») характер оценки области допустимой безопасности критической информационной среды.
- Уровень безопасности не может быть оценен только внедряемым комплексом средств защиты ввиду сложного взаимовлияния при котором выполнение функций защиты непредсказуемо. Необходимость введения функциональной целостности.
- Для гетерогенных сложных систем с размытым периметром оценки безопасности отдельных узлов не согласуются друг с другом ввиду чего невозможно построить единую шкалу.
- Использование различных моделей оценки рисков.

Раздел 3. Безопасность киберфизических систем

ПОНЯТИЕ КИБЕРФИЗИЧЕСКОГО ОБЪЕКТА (СИСТЕМЫ КАК СОВОКУПНОСТИ ОБЪЕКТОВ) (КФО)

КФО – концептуальная парадигма представления производственных, технологических схем в виде интеграции информационно-телекоммуникационной среды и систем преобразования различных видов энергии, обеспечивающей обмен информацией между компонентами и устойчивое функционирование всей системы с помощью автоматизированного управления, защиты от внешних воздействий, мониторинга состояния.

К КФО можно отнести:

- Системы управления производством. SCADA.
- Системы IoT, включающей центр управления.
- Робото-технические системы критического назначения.
- Беспилотные летательные аппараты.
- Беспилотные автомобили.
- Системы военного назначения.

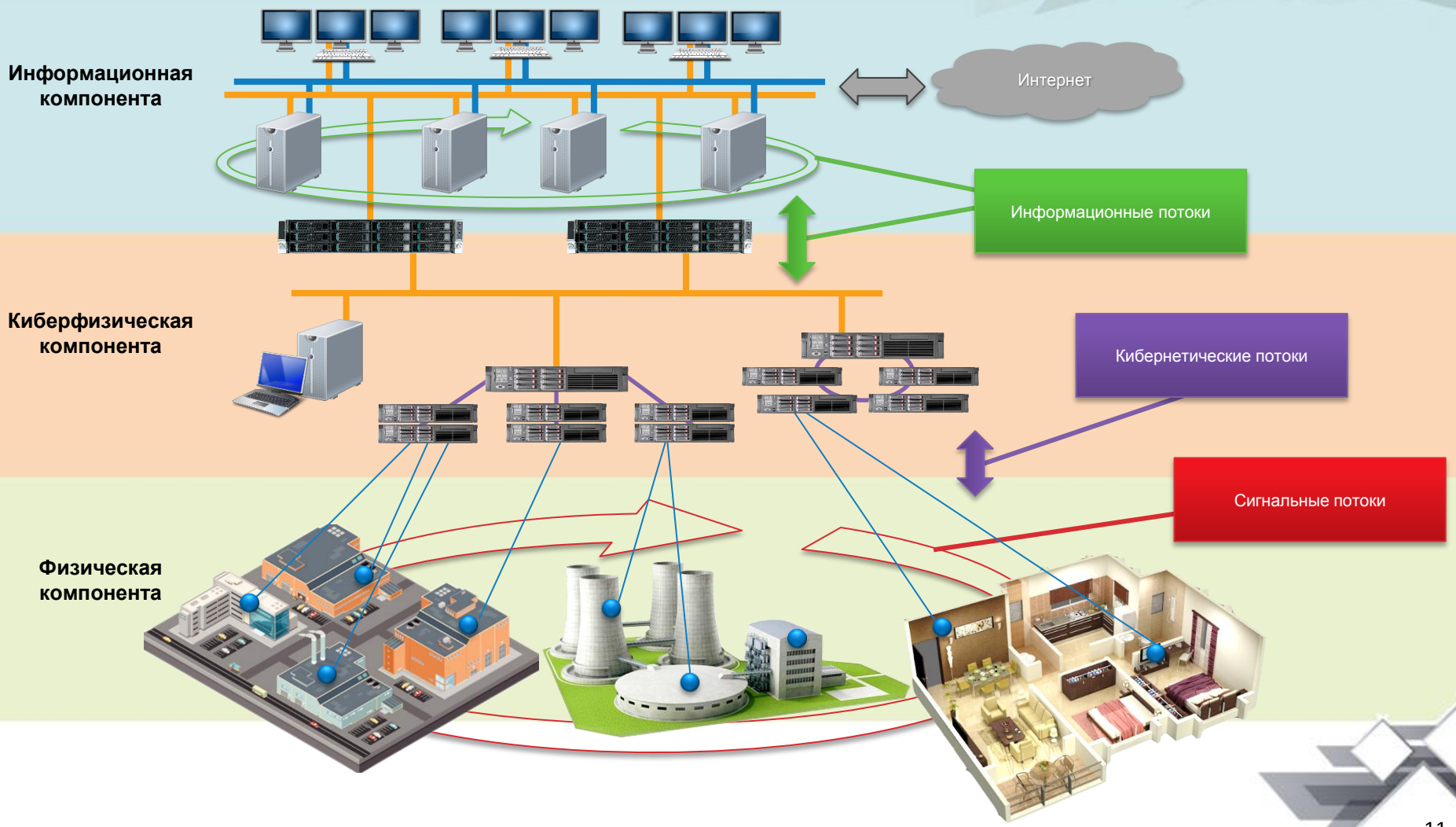
ОТЛИЧИТЕЛЬНЫЕ ПРИЗНАКИ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ

- Высокая степень компьютеризации системы, постоянный телекоммуникационный контакт (обмен информацией) с аналогичными системами и взаимодействие с глобальной сетью Internet.
- Наличие центра (подсистемы) автоматического управления функционированием системы и обеспечение ее устойчивой работоспособности при наличии различных возмущающих воздействий.
- Наличие единой информационной среды или киберпространства, представляющего собой совокупность программно-аппаратных средств обработки и передачи информации, обмен внутри системы и с окружающей средой, системы автоматического управления физическими компонентами посредством логически программируемых контроллеров и поддержание заданного сценария работы с возможностью адаптивного управления, а так же средства обеспечения защиты информации, в виде криптосерверов, межсетевых экранов, антивирусов и т.д.
- Наличие интеллектуализации управления путем построения сценариев работы на основе автопрогноза и адаптационного управления, что обеспечивает устойчивость систем.

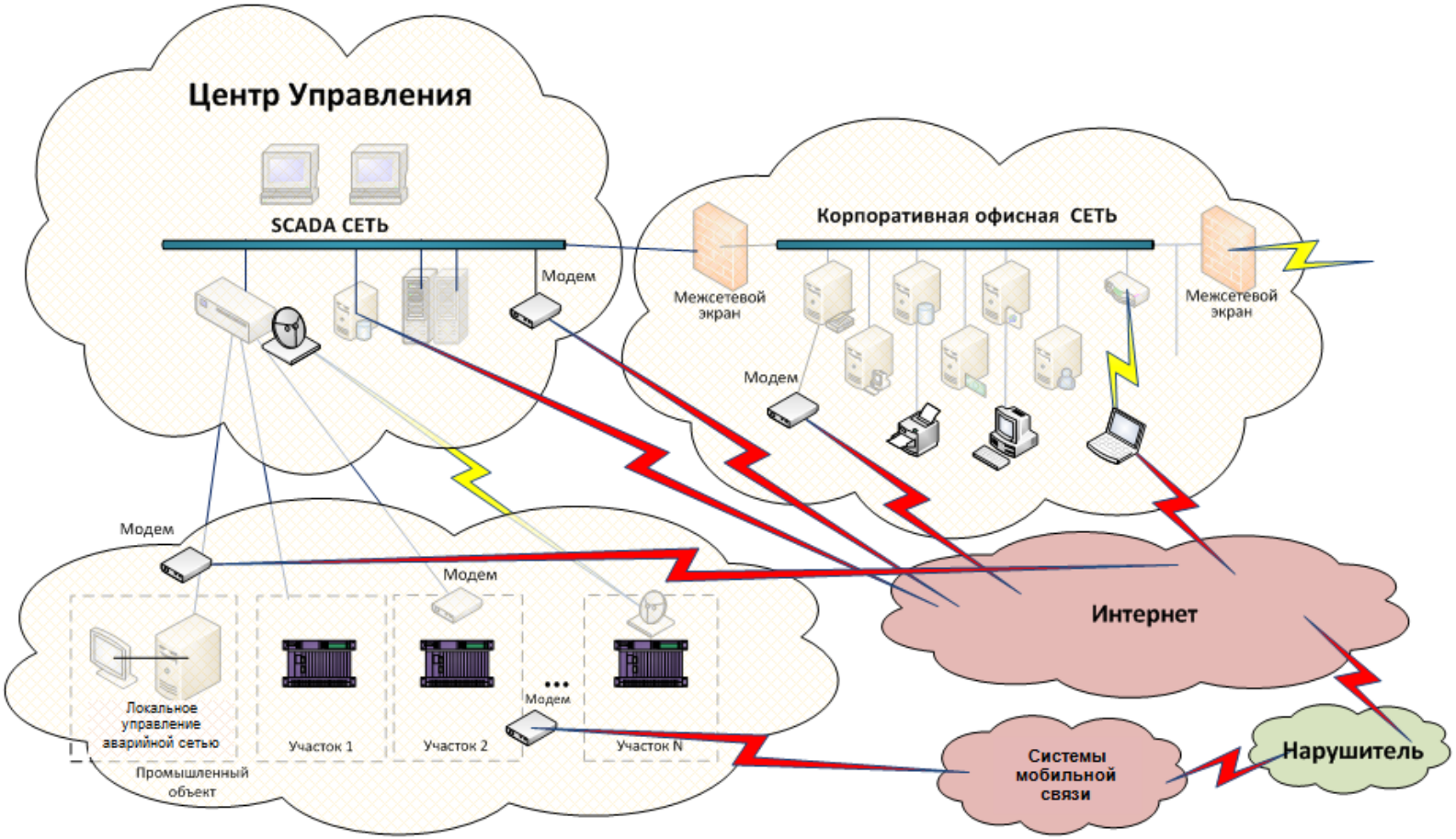
ЛОГИЧЕСКАЯ КОНЦЕПТУАЛЬНАЯ СХЕМА КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ

- Набор взаимосвязанных физических компонент, реализующих технологический процесс.
- Набор взаимосвязанных информационных компонент, осуществляющих управление процессом в разной степени автоматизации.
- Коммуникационную среду, обеспечивающую обмен информации внутри системы и с окружающей средой и передачи управляющих команд через ПЛК исполнительным механизмом.

АРХИТЕКТУРА КИБЕРФИЗИЧЕСКИХ СИСТЕМ



СОЗДАНИЕ ЕДИНОЙ ИНФОРМАЦИОННОЙ СЕТИ ПРЕДПРИЯТИЯ И ТОЧКИ ВНЕШНИХ ВОЗДЕЙСТВИЙ



Раздел 4. Нормативная база кибербезопасности. Международные стандарты

НОРМАТИВНЫЕ ДОКУМЕНТЫ

ГЕОГРАФИЯ	НАИМЕНОВАНИЕ ДОКУМЕНТА
США	National Security Presidential Directive 54/Homeland Security Presidential Directive 23, 2008
Великобритания	The UK Cyber Security Strategy, 2011
Канада	Canada's Cyber Security Strategy, 2010
Германия	Cyber Security Strategy for Germany, 2011
Австралия	Cyber Security Strategy, 2009
Новая Зеландия	New Zealand Cyber Security Strategy, 2011
Нидерланды	The National Cyber Security Strategy, 2011
Индия	Discussion draft on National Cyber Security Policy, 2011
ITU	ITU-T Recommendation Rec. ITU-T X.1205 (X.cso), 2008
ISO/IEC	ISO/IEC 27032 Guidelines for Cybersecurity (DRAFT), 2011
Европейский Союз	Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2013
Российская Федерация	Концепция национальной стратегии кибербезопасности Российской Федерации. Проект. 2013

- **Киберпространство –** принципиально новая среда противоборства конкурирующих государств, не является географическим в общепринятом смысле, но в полной мере является международным
- Кибервойна в виртуальном киберпространстве – реальность
- Кибервооружения нацелены на объекты жизнеобеспечения и промышленности
- Неясно, что значит «вести действия в виртуальном киберпространстве»
- Частный и промышленный сектор подвержены наибольшему риску кибернетического воздействия
- Не существует общепринятых стандартных определений терминов в сфере кибербезопасности

Раздел 5. Безопасность киберфизических систем и свойство гомеостаза.

КИБЕРБЕЗОПАСНОСТЬ VS ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОДОЛЖЕНИЕ ТАБЛИЦЫ

Свойства	Информационная безопасность	Кибербезопасность
Меры безопасности	Организационно Криптографически Защита от НСД Надежность	Но кроме перечисленных для ИТКС – аварийная защита физического процесса.
Мониторинг	Наличие внутренних критериев безопасности	–Внутренние критерии не формулируются –Оценивается выполнение конечной функции
Средства безопасности	СКЗИ, НСД, AV, МЭ, СОВ и др.	Поддержание самоподобного процесса на основе саморегуляции
Анализ безопасности	Аттестация Сертификация Pen Testing	Анализ устойчивости Метрики Самоподобие

ВОЗМОЖНЫЕ ПОДХОДЫ К ПОСТРОЕНИЮ ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ КИБЕРСИСТЕМ

1) Нормативные по существующим стандартам - отсутствует единый подход и методы оценки.
2) Введение группы показателей для информационных и физических компонент.
3) Задание показателей, характеризующих состояние системы в целом. Регулярность поведения системы в условиях деструктивных воздействий.

ВОЗМОЖНЫЕ ПОКАЗАТЕЛИ СОХРАНЕНИЯ УСТОЙЧИВОСТИ КИБЕРСИСТЕМ

- Анализ динамической устойчивости
- Использование статистических показателей:
    - автокорреляционная функция;
    - сохранение закона распределения;
    - построение метрик, отличие состояния.
  – Обобщенная мера устойчивости в виде гомеостаза – по аналогии со свойствами живого организма.

ПОНЯТИЕ ГОМЕОСТАЗА

Гомеостаз (*по-гречески одинаковый, подобный*) – способность открытой системы сохранять постоянство своего внутреннего состояния посредством скоординированных частей системы, направленных на поддержание динамического равновесия, стремление системы восстановить утраченное равновесие, преодолевать воздействия внешней среды.

Уолтер Кеннон (Walter B. Cannon)

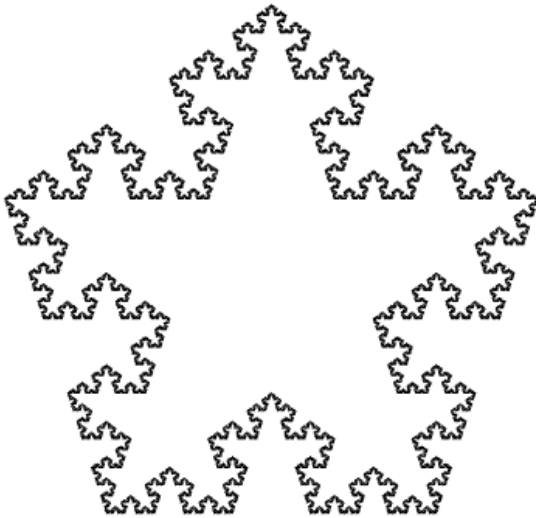
The Wisdom of the Body

Раздел 6. Фрактальные методы оценки безопасности КФС

ФРАКТАЛЫ

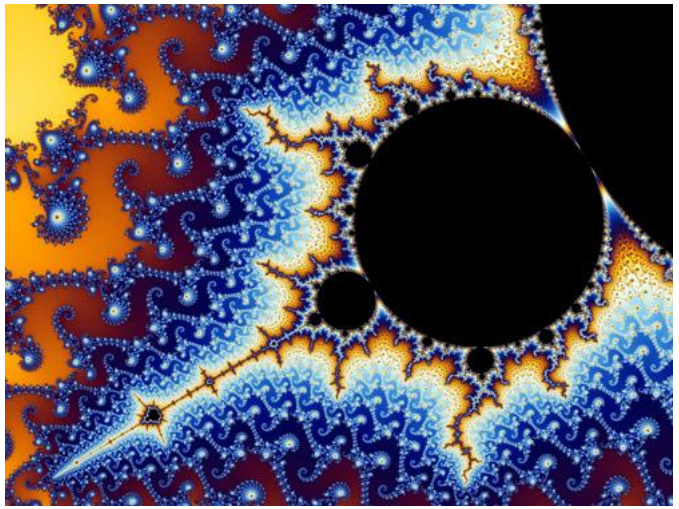
- Фрактал – геометрический объект с дробной размерностью
- Виды фракталов:

Геометрические



Кривая Коха

Алгебраические



Множество Мандельброта

Фракталы обладают свойством самоподобия

САМОПОДОБИЕ

- Самоподобие – инвариантность относительно изменения масштаба
- Свойство протяженной зависимости
- Самоподобная система сохраняет неизменными свои основные свойства, независимо от определённых преобразований, факторов или условий

САМОПОДОБНЫЕ СИСТЕМЫ

Подходы к оценке самоподобия временных рядов:

– DFA (Detrended Fluctuation Analysis)

– Фактор Фано

– Вычисление показателя Хёрста

DETRENDED FLUCTUATION ANALYSIS

1. Построение случайного блуждания:

$$y(k) = \sum_{i=1}^{k} (F_i - \langle F \rangle)$$

2. Разбиение ряда значение *y(k)* на отрезки длиной *n*. В каждом из отрезков методом наименьших квадратов определяется уравнение прямой аппроксимирующей последовательность
3. Вычисление среднеквадратичной ошибки:

$$D(n) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y(k) - y_n(k))^2}$$

Если $D(n) \sim n^{\alpha}$, или $\ln(D(n)) \sim \alpha \ln(n)$, можно говорить о существовании скейлинга:

- $0 < \alpha < 0.5$ – анти-корреляции
- $\alpha = 0.5$ - некоррелированное поведение
- $0.5 < \alpha < 1$ – коррелированная динамика, ряд можно назвать

ПОКАЗАТЕЛЬ ХЁРСТА И ФАКТОР ФАНО

- Показатель Хёрста H– характеризует «степень» случайного процесса:

$$\frac{R_n}{S_n} = (\frac{n}{2})^H, \quad R_n - \text{размах первых } n \text{ значений ряда},$$

$$S_n \ - \text{выборочная дисперсия}$$

Если процесс самоподобен, то выполняется: $0.5 < H < 1$

- Фактор Фано:

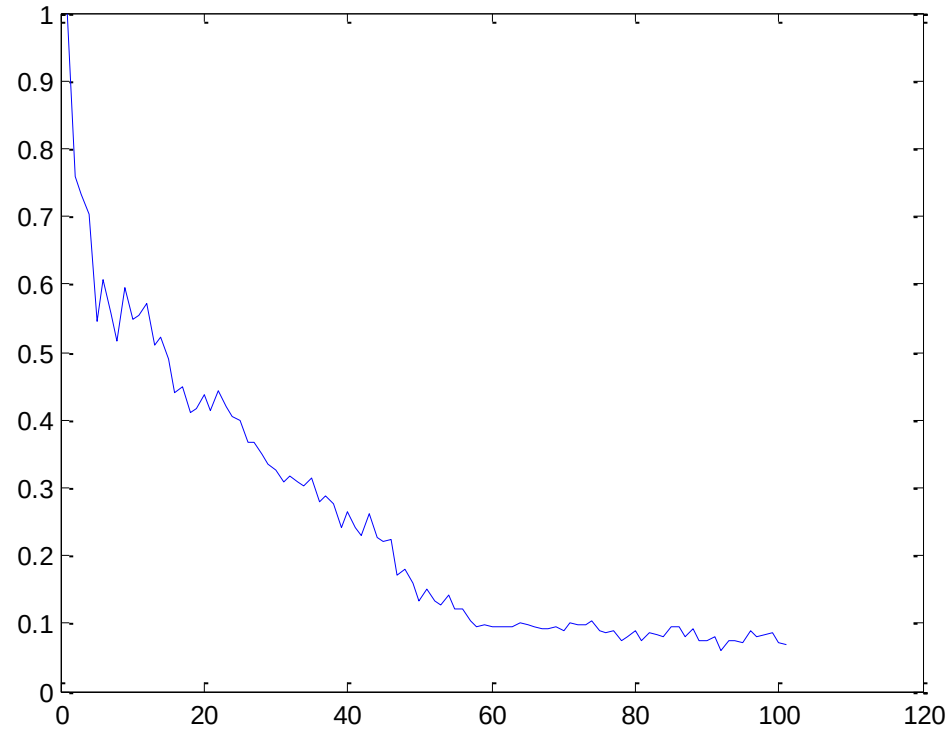
$$\Phi(n) = \frac{\sigma^2(n)}{m(n)}, \text{где } \sigma^2(n) - \text{дисперсия}, m(n) - \text{математическое ожидание}$$

Если процесс самоподобен, то выполняется :

$$\Phi(n) \sim n^{2H-1}$$

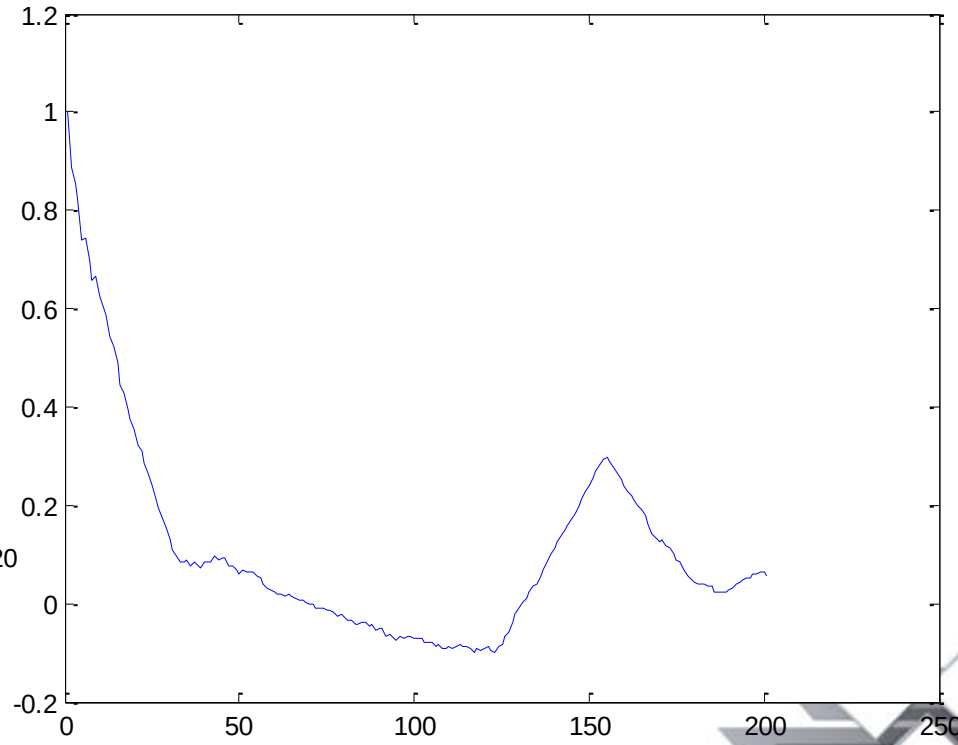
НАХОЖДЕНИЕ ФАКТОРА ФАНО

Автокорреляционная функция



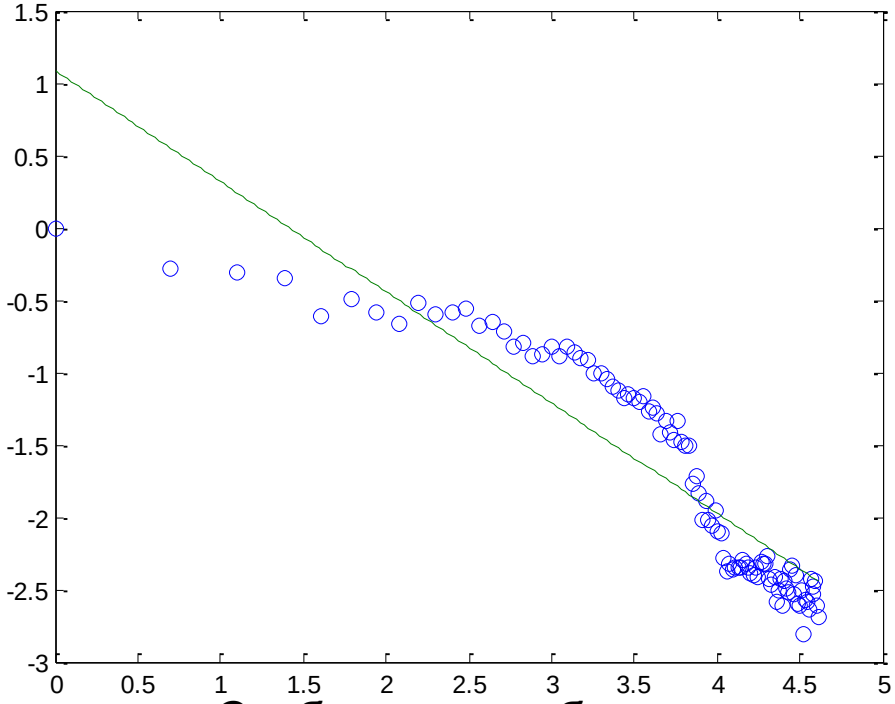
Стабильная выборка

Выборка с нарушением



НАХОЖДЕНИЕ ФАКТОРА ФАНО

Аппроксимация методом наименьших квадратов

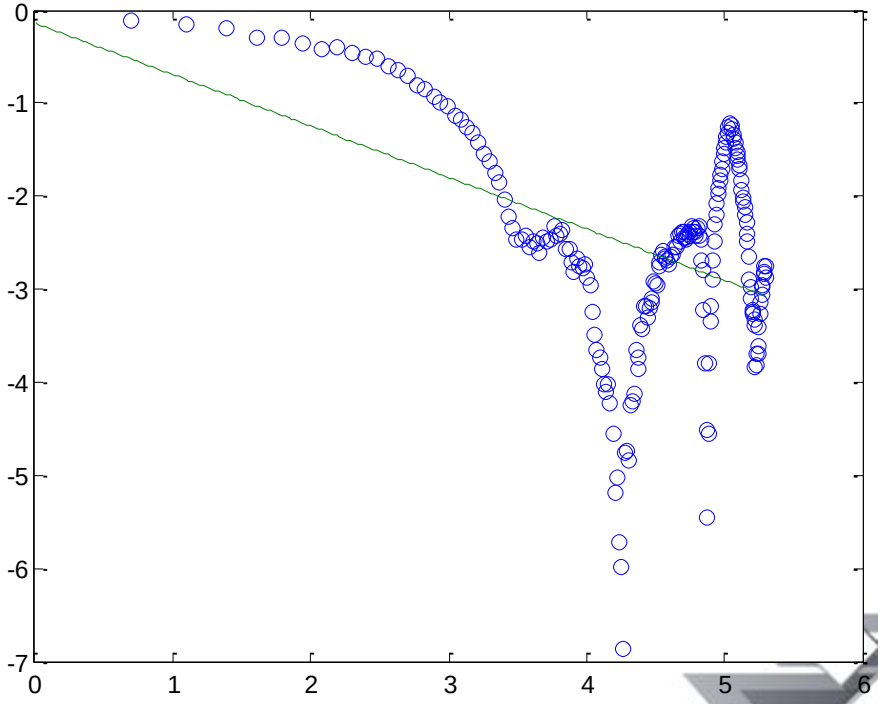


Стабильная выборка

$F = 0.764467$

Выборка с нарушением

$F = 0.553055$



Кафедра ИБКС
ФГБОУ ВПО «СПбГПУ»

Главный учебный корпус, к. 173
Политехническая ул., 29,
Санкт-Петербург
195251

Тел: +7 (812) 552-64-89, 552-76-32

Web: http://ibks.ftk.spbstu.ru
E-mail: Zeg@ibks.ftk.spbstu.ru