Профессор, д.т.н. П. Д. Зегжда

ПОДХОДЫ К ОЦЕНКЕ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

Рускрипто 2017

РАЗДЕЛ 1. КИБЕРПРОСТРАНСТВО – НОВЫЙ ВИТОК ЭВОЛЮЦИИ IT СИСТЕМ

ЧЕТВЕРТАЯ ПРОМЫШЛЕННАЯ РЕВОЛЮЦИЯ – INDUSTRY 4.0

- Перманентная информационная революция
- Промышленная компьютеризация
- Интеграция Internet-технологий с АСУ производства, энергетики, транспорта, медицины, банковской сферы, домашних устройств и систем безопасности

Автоматизация → **Информатизация** → **Кибернетизация**

КОНЦЕПЦИЯ ИНТЕРНЕТА ВЕЩЕЙ

Концепция промышленного интернета рассматривает организацию умных сетей как явление, способное перестроить экономические и общественные процессы исключающие из части действий необходимость участия человека.

Кевин Эттон 2009 г. (Proctor & Gambale) предложил теорию Internet of Things.

В общей сложности изменения затронут 2/3 мировой экономики, что соответствует увеличению ВВП на $ 12 трлн. к 2030 г.

РАЗДЕЛ 2. КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ

ПОНЯТИЕ КИБЕРФИЗИЧЕСКОГО ОБЪЕКТА (КФО)

КФО – концептуальная парадигма представления производственных, технологических схем в виде конгломерата средств преобразования различных видов материи и энергии и информационно-телекоммуникационной среды, обеспечивающей как обмен информацией между компонентами так и устойчивое функционирование всей системы в условиях внешних воздействий с помощью автоматизированного управления.

К **КФО** можно отнести:

- Системы управления производством (АСУ ТП, SCADA-системы)
- Интернет вещей (Internet of Things, умный дом, умные вещи).
- Робототехнические системы критического назначения.
- Беспилотные летательные аппараты.
- Беспилотные автомобили.
- Системы военного назначения.

РАЗДЕЛ 3. СИСТЕМАТИЗАЦИЯ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИНТЕРНЕТА ВЕЩЕЙ

Возможны связи двух типов:

- «machine-human»
- «machine-machine» (по большей части будут устанавливаться автоматически)

Объем и вариативность собираемых и обрабатываемых данных существенно возрастут

Ключевые классы устройств:

- средства идентификации
- средства измерения
- средства передачи данных
- средства обработки данных

Неоднородность множества сущностей IoT будет возрастать, его компоненты будут обеспечивать различный функционал в зависимости от контекста их применения

РАЗДЕЛ 4.
ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

КАНАЛЫ ВОЗДЕЙСТВИЯ НА КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ

- Воздействия на подсистему управления
- Воздействия на человеко-машинный интерфейс
- Воздействия на устройства, входящие в состав киберфизических систем
- Воздействия на протоколы взаимодействия и сетевое оборудование

ПОЛУЧИВШИЕ ШИРОКУЮ ОГЛАСКУ ИНЦИДЕНТЫ НАРУШЕНИЯ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Менее 2% от подвергшихся нападению сообщают об инцидентах
(удар по репутации и снижение стоимости акций)

Август 2012: нефтяная компания Saudi Aramco

Крупнейшая нефтяная компания в мире Saudi Aramco стала жертвой направленной атаки на свои офисы. Хакеры получили доступ к сети благодаря атаке на одного из сотрудников компании, через которого смогли получить доступ к 30 000 компьютеров в сети. В какой-то момент хакерам удалось удалить содержимое всех компьютеров, в то время как на экранах показывался горящий американский флаг.

2013: системы Департамента автомобильных дорог и транспорта в США

Были заражены 200 компьютеров Департамента автомобильных дорог и транспорта в округе Кук (штат Иллинойс). Эти системы отвечали за поддержание сотни километров дорог в пригороде Чикаго. В результате атаки пришлось отключать сеть на 9 дней, чтобы вылечить все компьютеры.

Декабрь 2014: металлургический завод в Германии

Используя социальную инженерию, хакеры сумели получить доступ к компьютеру одного сотрудника, с которого они смогли получить доступ к внутренней сети системы управления. В результате этого стало невозможным выключить одну из домен, что нанесло огромный ущерб предприятию.

Декабрь 2015: электросеть Украины

В конце 2015 года Украина подверглась кибер-атаке на свою национальную электросеть, в результате чего свыше 600000 жителей остались без электричества.

Ноябрь 2016: система управления температурой воды и отоплением в Финляндии

Жители многоквартирных домов в финском городе Лаппеэнранта провели неделю без отопления и горячей воды. Причиной стала мощная DDoS-атака на «умную» систему контроля температуры воды и давления в батареях отопления.

РАЗДЕЛ 5. СПЕЦИФИКА ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КФС

ТРУДНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КФС

Традиционные подходы не решают главную задачу

- Цель защиты КФС – обеспечение непрерывности процесса управления в условиях дестабилизирующих воздействий, а цель ИБ – обеспечение конфиденциальности, целостности, доступности данных

Непродуманность КФС с точки зрения безопасности

- Возможность идентификации киберфизических систем и ПО в локальных и глобальных сетях
- применение в современных КФС устаревших аппаратных и программных средств общего назначения
- Слабые средства авторизации и аутентификации («вшитые» в ПО аутентификационные данные по умолчанию, ненадежные алгоритмы и т.д.)
- Отсутствие шифрования в промышленных транспортных протоколах (modbus, s7comm и др.)
- Слабые средства аудита и регистрации событий

Негибкая архитектура КФС и АСУ ТП

- Невозможность внесения существенных изменений в системы
- Отсутствие обновлений операционных систем и приложений или невозможность их применить
- Высокий риск автоблокировки системы при внедрении средств защиты

Человеческий фактор

РАЗДЕЛ 6.
ПОДХОДЫ К ОЦЕНКЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КФС

ЛАБОРАТОРИЯ КАСПЕРСКОГО ПРЕДЛАГАЕТ ДВА ТИПА ОЦЕНКИ БЕЗОПАСНОСТИ СИСТЕМ

Safety (внутренняя безопасность) – свойство системы сохранять работоспособность, не наносить вред окружающей среде и людям при условии ее эксплуатации в соответствии с предопределенными правилами в заданных условиях

Security (внешняя безопасность) – степень устойчивости к внешним угрозам или степень защиты от внешних угроз. Применимо к значимым и уязвимым системам. Безопасность представляет форму защиты, когда создается какое-либо разделение между системой и угрозой

Для CPS значимым является соблюдение обоих условий =
Safety + Security

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.

ОТЛИЧИТЕЛЬНЫЕ СВОЙСТВА КФС С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

Модульность	Ориентированность на быстрое внедрение новых отраслей техники	Расширяемость системы за счет распределенной структуры
Гетерогенность. Сочетание информационной и физической составляющих	Автоматизация управления путем интеграции средств вычислении и физических компонентов с целью достижения автономности	Наличие нескольких типов потоков: - Поток данных - Информационно-управляющие потоки - Физические потоки
Децентрализация. Наличие множества центров управления	Синхронизация действий для достижения цели	Система устройств стремящихся к автономному существованию
Интероперабельность. Взаимодействие модулей и оптимизация структуры для сохранения функциональности	Наличие общих протоколов связывающих информационные и физические компоненты	Интерфейсы взаимодействия гетерогенных устройств для сохранения функционирования
Отказоустойчивость стремящаяся к когнитивному поведению	Отсутствие единой точки отказа и саморегуляция, взаимозаменяемость модулей	Обнаружение ошибок, резервирование, адаптивность, гибкость управления
Класс информационных угроз. Жесткая зависимость от информационных компонент	Атаки из Internet. Влияние физических модулей на уязвимости. Интеграция ПО в физические модули. Аппаратные закладки. Утечки незащищенных внутренних интерфейсов	Необходимость защиты от сетевых угроз. Глобальная угроза нарушителя (перехвата) управления. Взаимозависимость безопасности информационных и физических подсистем.

ПРЕДЛАГАЕМАЯ СТРУКТУРА ПОКАЗАТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Аппарат оценки ИБ на основе конфиденциальной доступности, целостность для информационной составляющей включая:
   - *защищенность от атак из сети Internet*
   - *защиту внутренних протоколов*
   - *обнаружение уязвимостей по информационным и физическим компонентам.*
2. Оценка согласованности информационной и физической составляющей с учетом их взаимовлияния, свойств масштабируемости, интероперабельности, модульности на основе кросскорреляционных связей и оценки самоподобия, динамической устойчивости.
3. Оценка влияния информационных атак на систему управления (с учетом адаптивности) и способность к саморегуляции на основе фрактальных показателей устойчивости и способности к гомеостазу.
4. Оценка устойчивости структуры взаимосвязи элементов КФС на основе графовых методов оценки управляемости, масштабируемости, отказоустойчивости и константности функционирования в условиях информационных атак.
5. Разработка специфических критериев обнаружения атак на основе нарушения самоподобия и структурной устойчивости.

РАЗДЕЛ 6.1.
ОЦЕНКА БЕЗОПАСНОСТИ И УПРАВЛЯЕМОСТИ КБС С ИСПОЛЬЗОВАНИЕМ ИЕРАРХИЧЕСКИХ АДАПТИВНЫХ ГРАФОВ

МЕТОДИКА МОДЕЛИРОВАНИЯ АТАК НА БАЗЕ ПОСТРОЕННОЙ МОДЕЛИ

1 ОПРЕДЕЛЕНИЕ ЗЛОУМЫШЛЕННИКА

Задается модель злоумышленника, включающая:
- Доступные ему вершины
- Субъекты
- Средства проведения атак

2 ОПРЕДЕЛЕНИЕ ПЕРЕЧНЯ ВЕРШИН, С КОТОРЫХ МОЖЕТ НАЧАТЬСЯ АТАКА

$$V_{as} = V_a / V_{a-s}, ys_i \in S_a \mid s_i \in v_k \wedge v_k \in V_{a-s} \wedge V_{a-s} \subseteq V_a$$

3 ОПРЕДЕЛЕНИЕ МНОЖЕСТВА ДОСТУПНЫХ ПОЛЬЗОВАТЕЛЮ ВЕРШИН ПО МАРШРУТАМ ТРАНСПОРТНОГО УРОВНЯ

$$V^{attack} = V_{as} \cup V_{ats}$$

4 ОПРЕДЕЛЕНИЕ ВЕРШИН, СТАВШИХ ДОСТУПНЫМИ ЗЛОУМЫШЛЕННИКУ:

$$S_a^+ = \{s_j \in S \mid s_j \in v_k \wedge v_k \in V^{attack}\}$$

$$S_a = S_a \cup S_a^+$$

5 ПРАВИЛА И ЭЛЕМЕНТЫ ПОЛИТИКИ БЕЗОПАСНОСТИ, СТАВШИЕ ДОСТУПНЫМИ ЗЛОУМЫШЛЕННИКУ

$$P_a = P_a \cup \{p_q \mid p_q \in P \wedge p_q \in v_k \wedge v_k \in s_j \in v_k \wedge v_k \in V^{attack}\}$$

6 ОТМЕНА ПРАВИЛ P_a

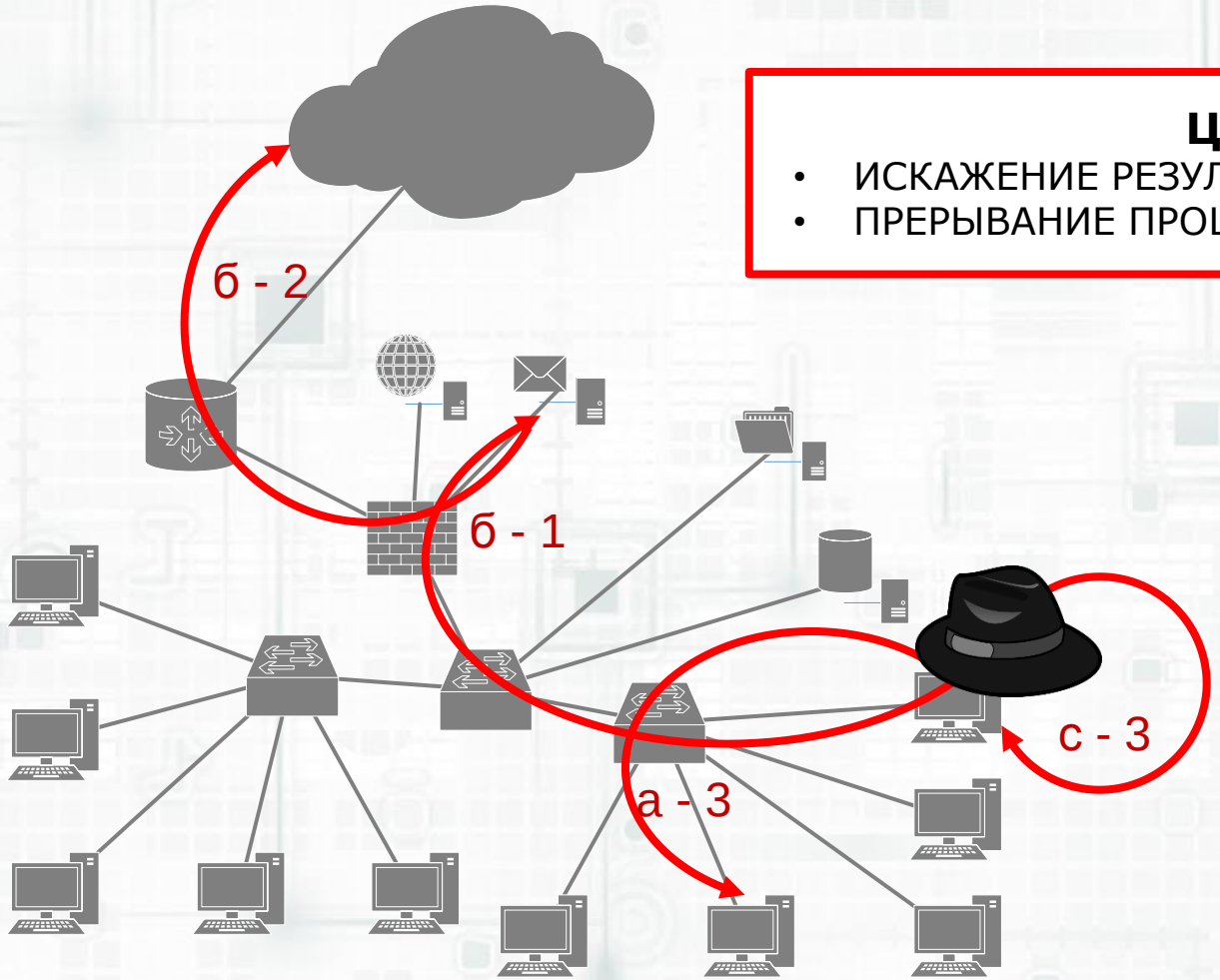
ОПРЕДЕЛЕНИЕ ВЕРШИН, СТАВШИХ ДОСТУПНЫМИ ЗЛОУМЫШЛЕННИКУ ПОСЛЕ ОТМЕНЫ ПРАВИЛ

7 ЕСЛИ ЦЕЛЕВАЯ ВЕРШИНА ДОСТИГНУТА – КОНЕЦ ЭТАПА, ИНАЧЕ:

Если множество S_a^+ не пусто – переход к шагу 3

Если множество S_a^+ пусто – конец этапа, злоумышленник не достиг цели

ПРИМЕР ОПИСАНИЯ АТАКИ В ТЕРМИНАХ РАЗРАБОТАННОЙ МОДЕЛИ



ЦЕЛЕВЫЕ АТАКИ

- ИСКАЖЕНИЕ РЕЗУЛЬТАТОВ (И/ИЛИ ПОРЯДКА) ПРОЦЕССА
- ПРЕРЫВАНИЕ ПРОЦЕССА

ВОЗМОЖНОСТИ НАРУШИТЕЛЯ В КАЖДОЙ ВЕРШИНЕ

- ВНОСИТЬ ИЗМЕНЕНИЯ В СЕМАНТИЧЕСКУЮ СЕТЬ ВЕРШИНЫ G_{H_i}
- ИСПОЛЬЗОВАТЬ ДЛЯ ДАЛЬНЕЙШЕЙ АВТОРИЗАЦИИ СУБЪЕКТЫ S_i, ОПРЕДЕЛЕННЫЕ НА ВЕРШИНЕ V_i
- ИЗМЕНЯТЬ ПРАВИЛА И ПАРАМЕТРЫ ПОЛИТИКИ БЕЗОПАСНОСТИ, ОПРЕДЕЛЕННЫЕ НА ВЕРШИНЕ V_i

МАТЕМАТИЧЕСКИЙ АППАРАТ ДЛЯ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Графы малых миров
Безмасштабные графы
Классические
случайные графы

Обеспечение связности в условиях агрессивного воздействия за счет избыточного числа связей

Звезда
Звезда из звезд

Связность в условиях агрессивного воздействия не обеспечивается

- Использование топологии с малой фиксированной степенью вершин
- Использование методов восстановления нарушенных связей

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ: МОДЕЛИРОВАНИЕ АТАКИ НА СЕГМЕНТ ИНТЕРНЕТА ВЕЩЕЙ

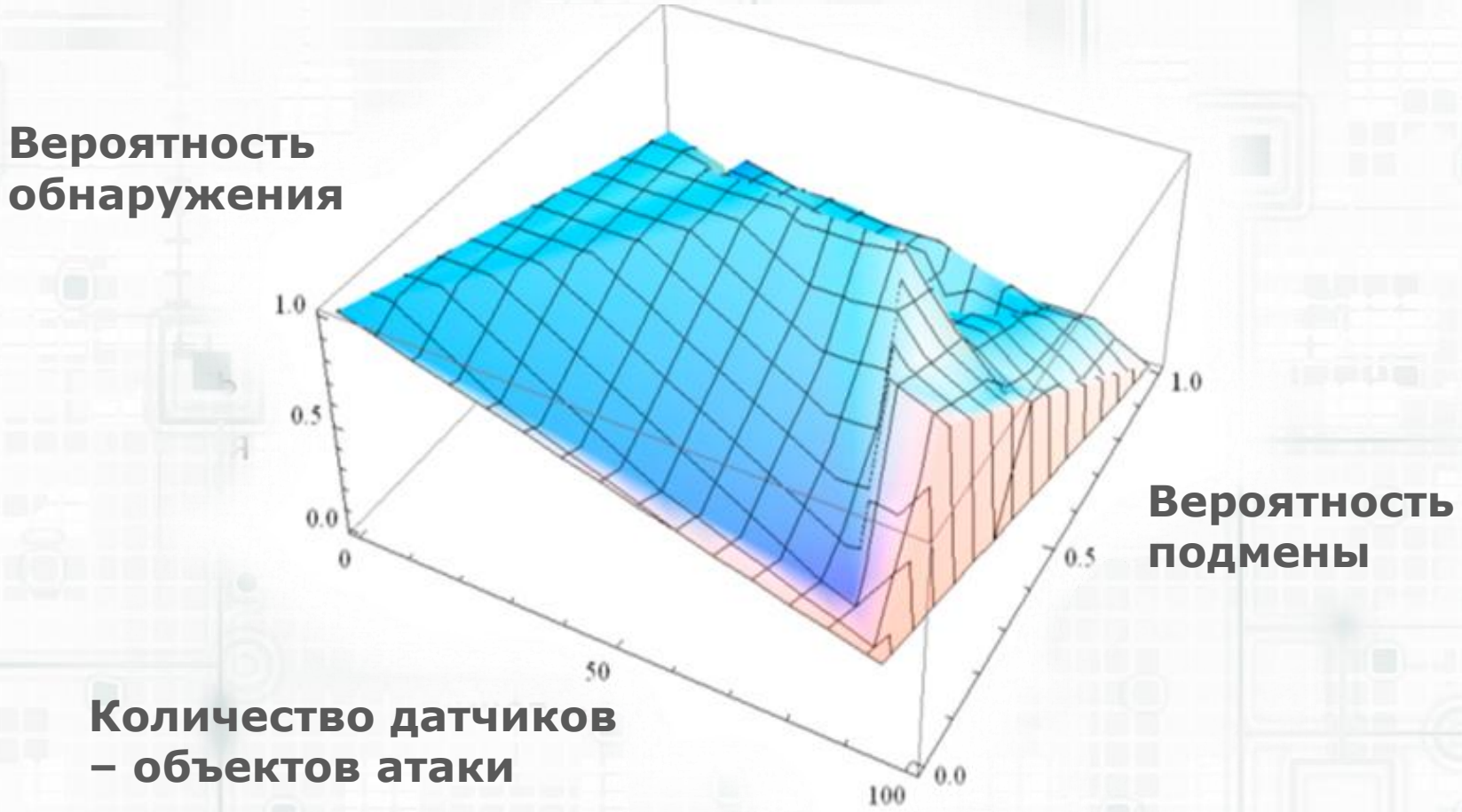
Обзор и анализ совокупности данных с внешнего периметра системы (sensor fusion), раскрытие конфиденциальных особенностей бизнес-процесса (в логистических цепях)

Подмена данных датчика (угон машины, «накрутка» показателей устройства smart grid)

Виртуальные и физические устройства Интернета вещей оснащённые GPS-датчиками и сенсорами освещенности (~1000 устройств)

РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТА

В моделируемом примере задается множество вершин, подверженных такой атаке подмены с заданной вероятностью, и оценивается вероятность обнаружения этих атак на основе проверки наличия семантических противоречий на графе сети (т.е. проверки консистентности семантической сети)



НАБОР ИНДИКАТОРОВ УСТОЙЧИВОСТИ «СЕТИ ВЕЩЕЙ»

Управляемость

Вероятность существования пути от устройства до координирующего центра, время передачи сообщения по этому пути не превышает *t*

Масштабируемость

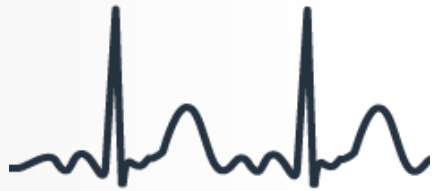
Дисперсия значений остальных индикаторов для системы от k до n узлов

Отказоустойчивость

Уровень нестабильности системы, при котором управляемость стремится к нулю

Константность функционирования

Скорость потребления ресурсов в зависимости от уровня нестабильности системы



РАЗДЕЛ 6.2. ОЦЕНКА АВТОНОМНОСТИ И УСТОЙЧИВОСТИ КБС. САМОПОДОБИЕ КФС

ВОЗМОЖНЫЕ ПОКАЗАТЕЛИ СОХРАНЕНИЯ УСТОЙЧИВОСТИ КИБЕРСИСТЕМ

Анализ динамической устойчивости

Использование статистических показателей:

- автокорреляционная функция;
- сохранение закона распределения;
- построение метрик, отличие состояния.

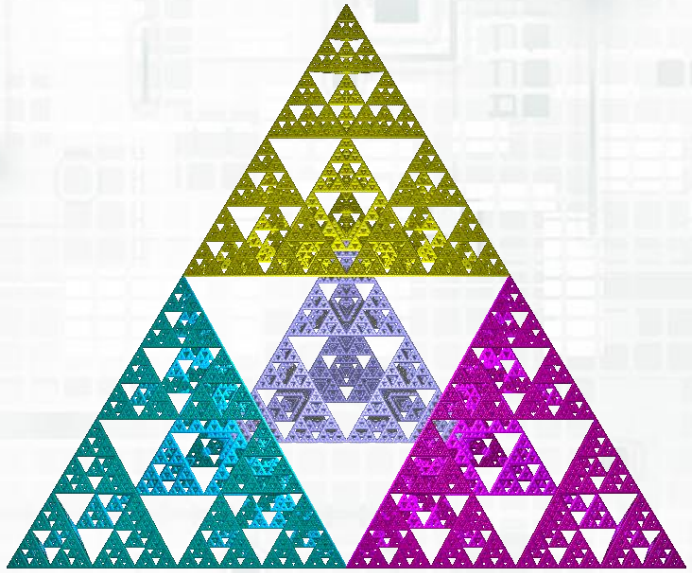
Обобщенная мера устойчивости в виде гомеостаза – по аналогии со свойствами живого организма.

САМОПОДОБИЕ

Самоподобие – инвариантность относительно изменения масштаба

Свойство протяженной зависимости

Самоподобная система сохраняет неизменными свои основные свойства, независимо от определённых преобразований, факторов или условий



РАЗДЕЛ 6.2.1. ФРАКТАЛЬНЫЕ ОЦЕНКИ УСТОЙЧИВОСТИ К КИБЕРУГРОЗАМ

ПОКАЗАТЕЛЬ ХЁРСТА И ФАКТОР ФАНО

Показатель Хёрста H– характеризует «степень» случайного процесса:

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

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

Индекс разброса дисперсии – Фактор Фано:

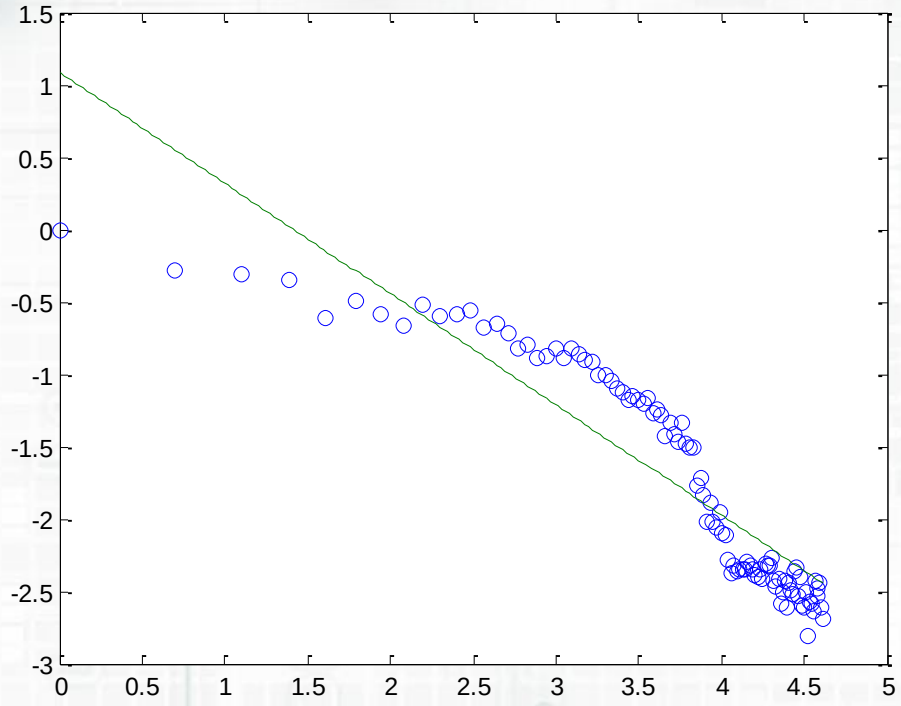
$$\Phi(n) = \frac{\sigma^2(n)}{m(n)}, \text{где } \sigma^2(n) - \text{дисперсия}, m(n) - \text{математическое ожидание}$$

Если процесс самоподобен, то выполняется :

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

НАХОЖДЕНИЕ ФАКТОРА ФАНО

Аппроксимация методом наименьших квадратов

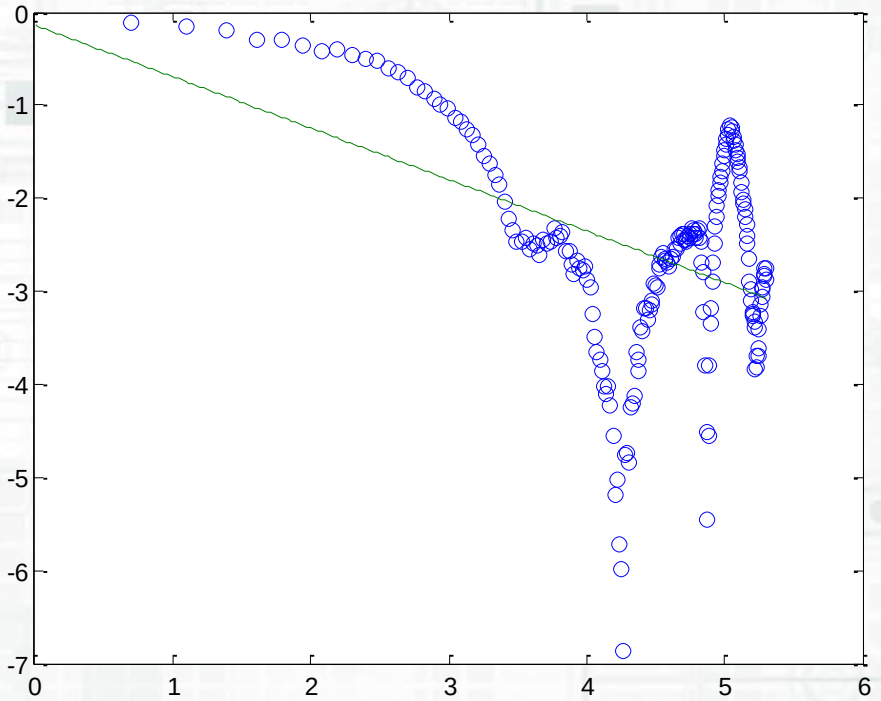


Стабильная выборка

$F = 0.764467$

Выборка с нарушением

$F = 0.553055$



РАЗДЕЛ 6.2.2
УСТОЙЧИВОСТЬ НА ОСНОВЕ СТОХАСТИЧЕСКОЙ ДИНАМИКИ

СТОХАСТИЧЕСКИЕ ФРАКТАЛЬНЫЕ ПРОЦЕССЫ

В отсутствии возмущений стационарное состояние киберфизической системы может быть формализовано следующим образом.

Пусть ρ – стационарное состояние, а ε - малый замкнутый контур вокруг ρ.

Состояние *S* называется устойчивым, если для любого заданного ε всегда можно найти $\delta(\varepsilon)$, такое, что любая траектория движения, находящаяся внутри , не достигнет границы ε.

В общем виде для *N*-мерной системы динамические уравнения системы имеют вид:

$$\frac{dx_i}{dt} = f_1(x_i, \ \dots \ , x_N , \vec{Q})$$

где $i \in \overline{1 , N}$, $\vec{Q}$ - вектор параметров системы.

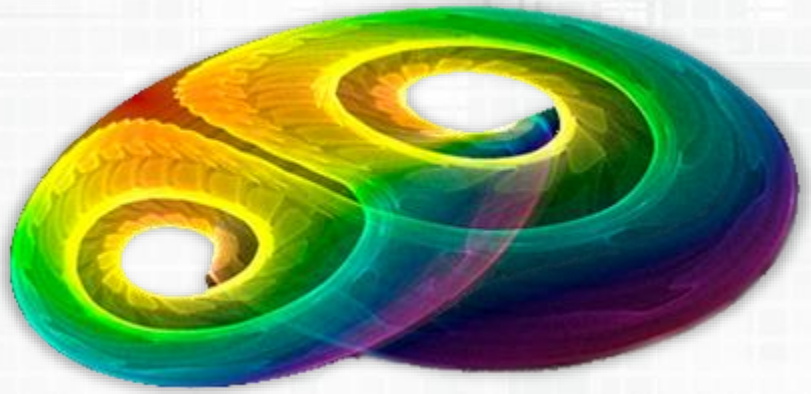
Анализ стационарности такой системы приводит к понятию **аттрактора**

ПОКАЗАТЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КИБЕРФИЗИЧЕСКИХ СИСТЕМ С УЧЕТОМ ДИНАМИЧЕСКИХ ХАРАКТЕРИСТИК

Аттрактор – область фазового пространства, в котором оказываются все траектории системы с течением времени, из которой в стабильном состоянии система не выходит.

В первом приближении можно считать, что стабильное нахождение системы в области аттрактора выражает условие гомеостаза.

Развитие или эволюция системы, т.е. необратимый переход на другую траекторию описывается самоподобной фрактальной структурой – странным аттрактором, что применительно к задаче безопасности означает необратимые изменения в системе, возникшие вследствие стихийной чрезвычайной ситуации либо кибератаки.



РАЗДЕЛ 6.3.
ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ГОМЕОСТАЗА

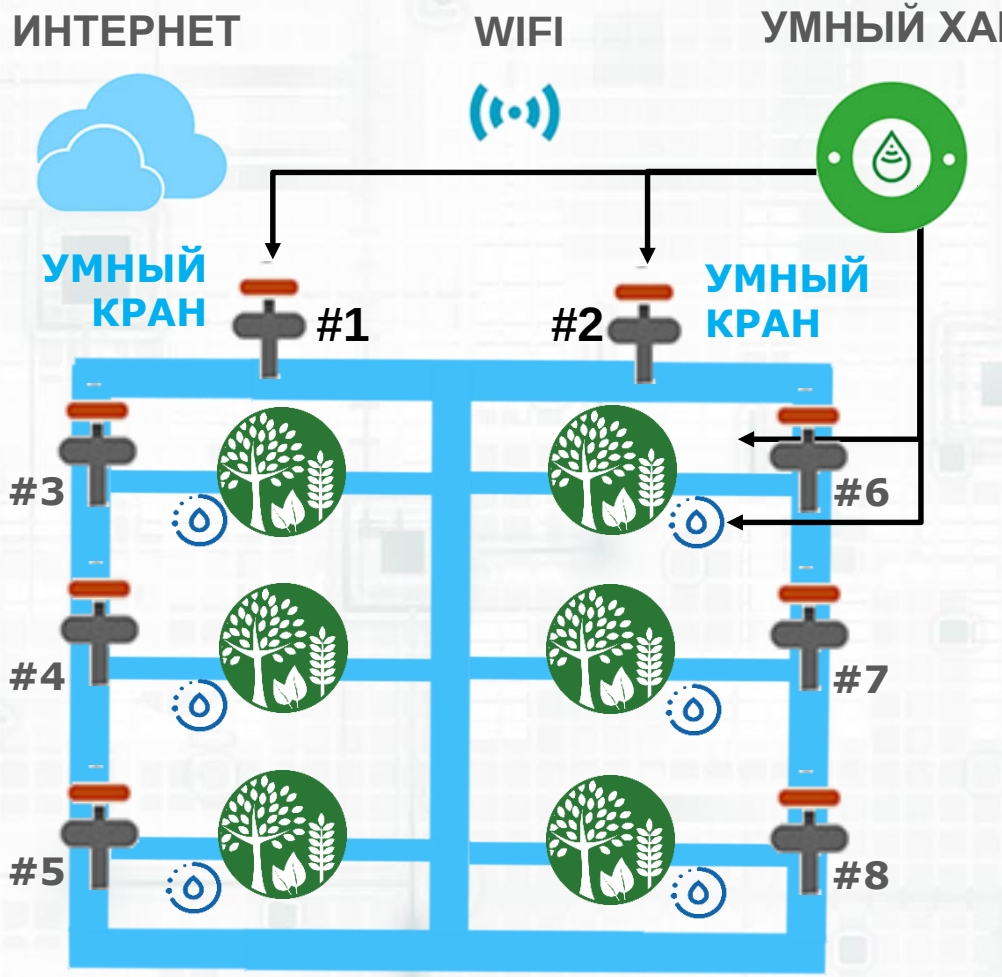
ПОНЯТИЕ ГОМЕОСТАЗА

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

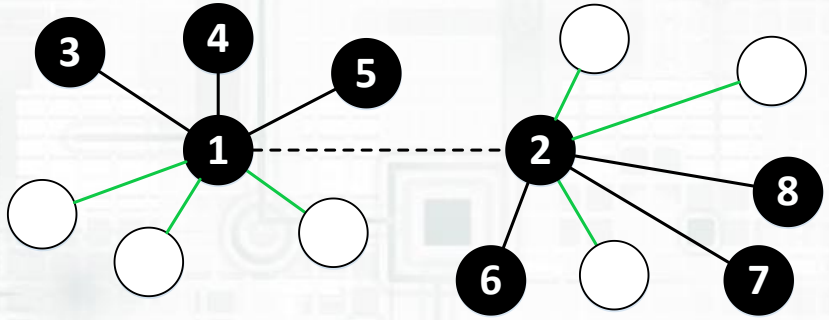
ГОМЕОСТАЗ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ПРИМЕРЕ СТАТИЧЕСКОЙ УМНОЙ СИСТЕМЫ ПОЛИВА РАСТЕНИЙ

СХЕМА УМНОЙ СИСТЕМЫ ПОЛИВА

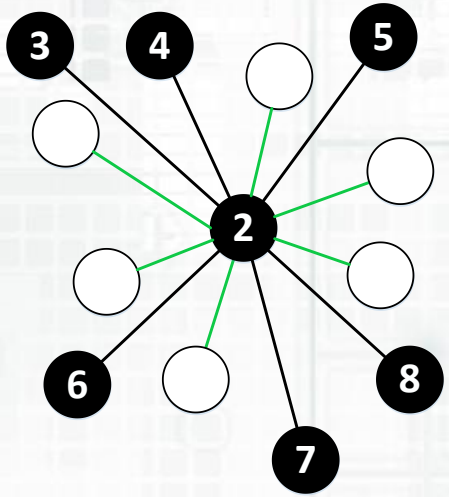


ГОМЕОСТАЗ С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА #2

НОРМАЛЬНОЕ ФУНКЦИОНИРОВАНИЕ



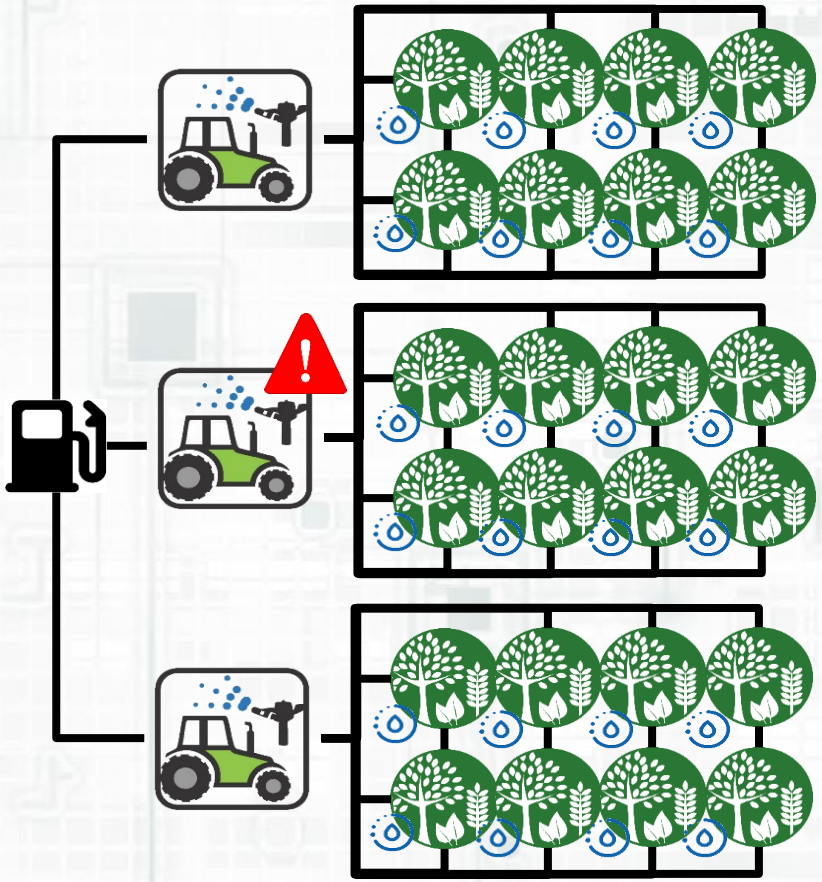
ВЫХОД ИЗ СТРОЯ УМНОГО КРАНА #1



ИЗОЛЯЦИЯ УМНОГО КРАНА #1 И ПЕРЕНОС ЛОГИКИ НА УМНЫЙ КРАН #2

ГОМЕОСТАЗ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ПРИМЕРЕ ДИНАМИЧЕСКОЙ УМНОЙ СИСТЕМЫ ОРОШЕНИЯ ПОЛЕЙ (2)

СХЕМА УМНОЙ СИСТЕМЫ ОРОШЕНИЯ

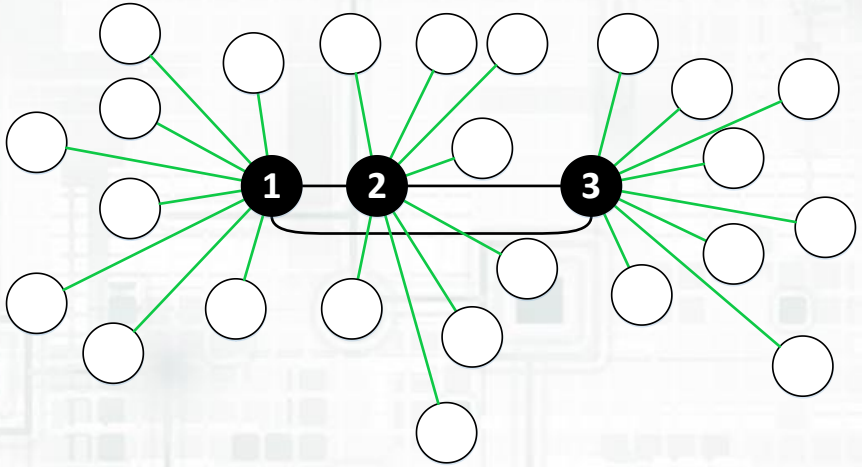


ВЫБОР МАШИНОЙ УЧАСТКА ПОЛИВА ОСНОВАН НА ВЫЧИСЛЕНИИ РАССТОЯНИЙ:

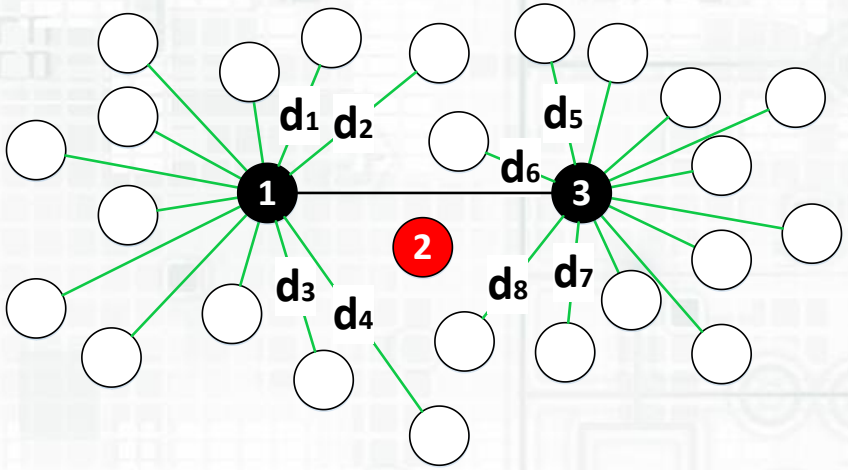
$d_1, d_2, \dots, d_8$ - КРАТЧАЙШИЕ РАССТОЯНИЯ ОТ МАШИН ДО УЧАСТКОВ ПОЛИВА

ГОМЕОСТАЗ С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА #2

ВЫХОД ИЗ СТРОЯ ПОЛИВАЛЬНОЙ МАШИНЫ #2



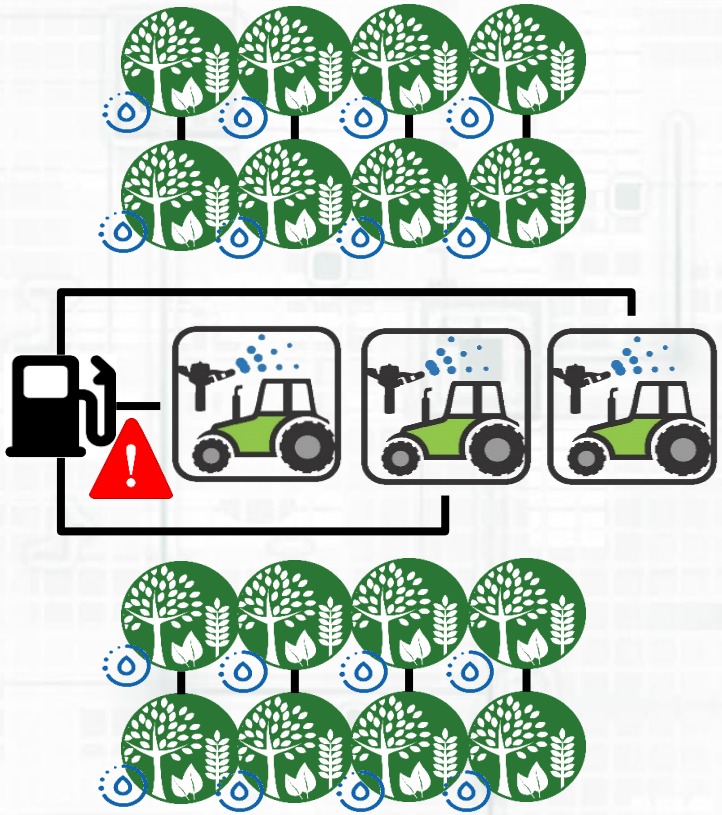
РАСПРЕДЕЛЕНИЕ ЗАДАЧ МЕЖДУ МАШИНАМИ #1 И #3



ГОМЕОСТАЗ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА ПРИМЕРЕ ДИНАМИЧЕСКОЙ УМНОЙ СИСТЕМЫ ОРОШЕНИЯ ПОЛЕЙ (3)

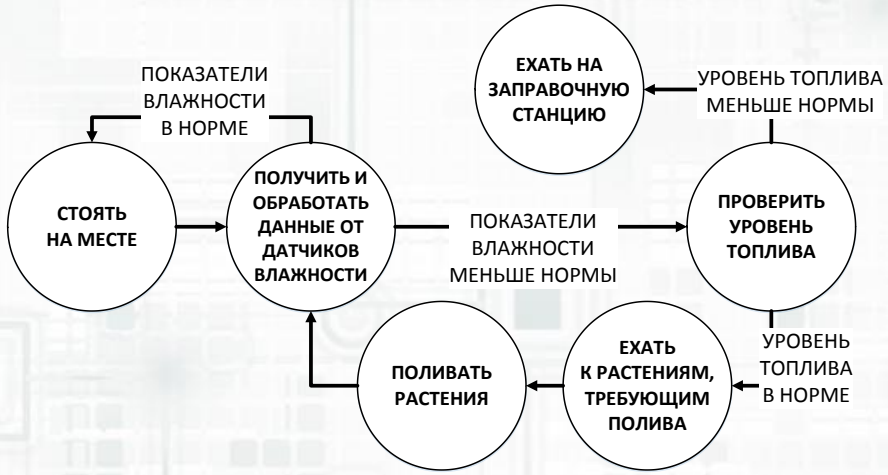
СХЕМА УМНОЙ СИСТЕМЫ ОРОШЕНИЯ

ВОЗНИКНОВЕНИЕ ПРОСТОЯ В РАБОТЕ СИСТЕМЫ ИЗ-ЗА ТОГО, ЧТО У МАШИН ОДНОВРЕМЕННО ЗАКОНЧИЛОСЬ ТОПЛИВО, ОРГАНИЗОВАЛАСЬ ОЧЕРЕДЬ

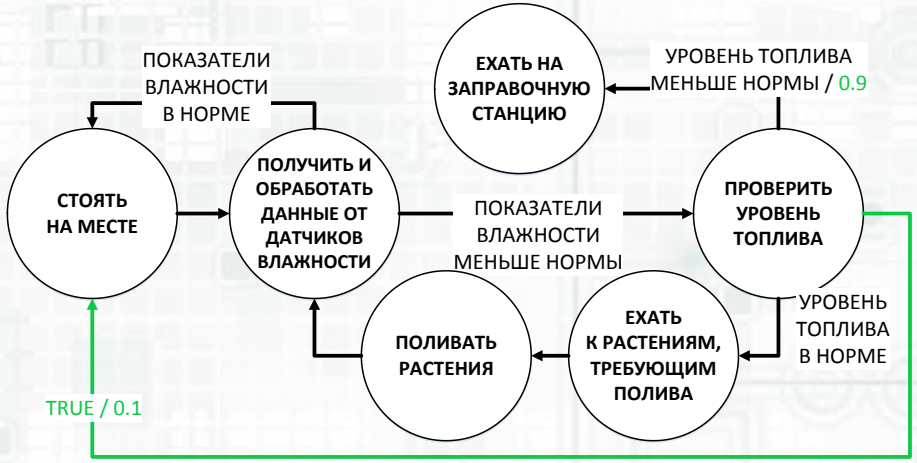


ГОМЕОСТАЗ С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА #3

КОНЕЧНЫЙ АВТОМАТ КАЖДОЙ ПОЛИВАЛЬНОЙ МАШИНЫ



ДОБАВЛЕНИЕ ВЕРОЯТНОСТЕЙ ПЕРЕХОДОВ В КОНЕЧНЫЙ АВТОМАТ КАЖДОЙ ПОЛИВАЛЬНОЙ МАШИНЫ



РАЗДЕЛ 7.
ОБЩАЯ СХЕМА ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАЗЛИЧНЫХ КЛАССОВ КФС

ПОКАЗАТЕЛИ УСТОЙЧИВОСТИ ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

ВОЗМОЖНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

- НА ИНФОРМАЦИОННЫЕ УЗЛЫ
- НА СИСТЕМУ УПРАВЛЕНИЯ
- НА МЕХАНИЧЕСКИЕ УЗЛЫ

ПОКАЗАТЕЛИ УСТОЙЧИВОСТИ ДЛЯ РАЗНЫХ ТИПОВ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

ДЛЯ СЛАБОСВЯЗАННЫХ СИСТЕМ (УМНЫЙ ДОМ, ИНТЕРНЕТ ВЕЩЕЙ)

АНАЛИЗ СТАТИСТИЧЕСКИХ ПОКАЗАТЕЛЕЙ

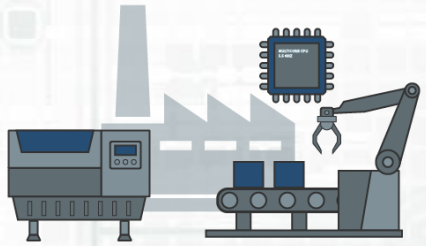
- ОЦЕНКА САМОПОДОБИЯ
- ОЦЕНКА СОГЛАСОВАННОСТИ ДИНАМИКИ ИЗМЕНЕНИЯ ДАННЫХ ОТ УСТРОЙСТВ
- АНАЛИЗ ВРЕМЕННЫХ РЯДОВ

ДЛЯ СИСТЕМ С АДАПТИВНЫМ УПРАВЛЕНИЕМ

АНАЛИЗ ПОТОКОВ УПРАВЛЕНИЯ

- ПОКАЗАТЕЛИ УПРАВЛЯЕМОСТИ, ОТКАЗОУСТОЙЧИВОСТИ, МАСШТАБИРУЕМОСТИ ФУНКЦИОНИРОВАНИЯ ПО СТРУКТУРЕ ГРАФА
- МЕТОД АТТРАКТОРОВ
- АДАПТИВНЫЕ ГРАФЫ

ДЛЯ СИЛЬНОСВЯЗАННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ



АНАЛИЗ СОХРАНЕНИЯ СВОЙСТВА ГОМЕОСТАЗА

- СПОСОБНОСТЬ К ГОМЕОСТАЗУ И ЭВОЛЮЦИИ

Показатели безопасности КФС (1)

	Интернет вещей	Многоагентные		SCADA, Системы в энергетике, медицине, производстве, обслуживание	Системы беспилотных движущихся средств	Интеллектуальные роботы
	Встроенные системы; WSN; RFID; NFS, M2M, Iot умный дом, Iot промышленный, виртуализированные системы	**Биоинспирированные системы**	**Реконфигурируемые системы (гибкие)**			
	Интернет ориентированные Человекоориентированные Семантикоориентированные			АСУ топологии производства; Удаленно управляемые агрегаты (эл. станции)	Дроны, беспилотные авто, системы видеокамер, спутники, средства разведки	Системы спутников, летательные станции, работы для чрезвычайных ситуаций, военные системы
Связь и механизмы взаимодействия	пассивная односторонняя двусторонняя наличие центра (ов) управления интернет подобия	Обмен со средой	Полный двусторонний обмен друг с другом	Взаимосвязи для выполнения технологических операций Использование модели механических исполнительных механизмов Согласованное управление информационной и исполнительной части в динамике Наличие центра мониторинга	Обмен со средой и с центром управления создание общего центра мониторинга и управления Полная двусторонняя связь друг с другом и центром управления	Автономные интеллектуальные системы, способные принимать решения без участия человека. Взаимодействие с внешним миром, другими комплексами Способность к самосохранению война роботов

Показатели безопасности КФС (2)

	Интернет вещей	Многоагентные		SCADA, Системы в энергетике, медицине, производстве, обслуживание	Системы беспилотных движущихся средств	Интеллектуальные роботы
	Встроенные системы; WSN; RFID; NFS, M2M, Iot умный дом, Iot промышленный, виртуализированные системы	**Биоинспирированные системы**	**Реконфигурируемые системы (гибкие)**			
Угрозы	▪ Атки на подсистему физических устройств для съема информации и хищения ресурсов, нарушения сети коммуникаций ▪ Атаки на протокол и технологии, сетевое оборудование, на RFID, Glowpan ▪ Атаки на сервер обработки, базы данных, веб-серверы, web-интерфейс			APT атаки на системы управления, исполнительные механизмы системы взаимодействия с использованием вывода из строя оборудования, отключение защитной автоматики	Атаки на сеть управления, на центр управления, доступ к системам и перехват управления через уязвимости wel-интерфейса и приложения	Информацион-ное противоборство
Системы управления КБС	Работа по заданной программе при минимальной обратной связи пассивный обмен, отсутствие мониторинга	Наличие системы мониторинга и обратной связи на параметрическом управлении Самоорганизация путем перенастройки и переконфигурации, самовосстановление	Обратная связь на параметрическом и сетевом уровне (переконфигурация) Наличие мониторинга и защиты Самооптимизация и проактивное восстановление	Адаптивное управление с несколькими уровнями обратной связи, мониторинг состояния, наличие активной аварийной защиты для медицинских систем Интеллектуальный мониторинг и управление роботами Контроль устойчивости исполнительных механизмов	Несколько уровней обратной связи, адаптивное управление приспособленной к окружающей среде программирования управления, использование гибкой системы коммуникации с управляемой архитектурой	Обеспечение гомеостаза на всех уровнях взаимодействия. Самосохранение Способность к рассуждению и антиципации (прогнозу)

Показатели безопасности КФС (3)

	Интернет вещей	Многоагентные		SCADA, Системы в энергетике, медицине, производстве, обслуживание	Системы беспилотных движущихся средств	Интеллектуальные роботы
	Встроенные системы; WSN; RFID; NFS, M2M, Iot умный дом, Iot промышленный, виртуализированные системы	Биоинспирированные системы	Реконфигурируемые системы (гибкие)			
Математическое аппаратное моделирование	Графические и структурные модели	Адаптивные графы, Семантические сети Потоковые модели	Иерархические случайные графы семиотические модели	Стохастические динамические модели Фрактальные модели фазовые и информационные протрет Самотестирование	Модели теории обслуживания динамические графы Сети автоматов Отказоустойчивость и оптимизация	Теорию Гироматов интеллектуальные управляющие системы Когнитивные сценарии
Показатели устойчивости	Вычисление статистических инвариантов	Статистические и фрактальные показатели самоподобия и самоорганизации	Показатели управляемости, отказоустойчивости, масштабируемости, константности функционирования по структуре графа	Показатели динамической устойчивости Показатели Ляпунова Метод аттракторов Фрактальные методы	Динамические показатели устойчивости топологии, адаптивные случайные графы -параллельные графы	Способность к гомеостазу и эволюции

Кафедра ИБКС
ФГБОУ ВПО «СПбГПУ»

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

Тел: +7 (812) 552-64-89
+7 (812) 552-76-32

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