InfoSecurity Russia 2016, 20 сентября 2016г.

АНАЛИТИЧЕСКОЕ ПРОГНОЗИРОВАНИЕ РИСКОВ И ОБОСНОВАНИЕ СБАЛАНСИРОВАННЫХ МЕР УПРЕЖДАЮЩЕГО ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

дтн, проф. Костогрызов А.И.

www.mathmodels.net

План выступления

1. Анализ состояния и перспектив развития
2. Основная идея
3. Генерация вероятностных моделей для сложных структур
4. Оптимизационные задачи
5. Пример реализации и извлечения эффектов

1. Анализ состояния и перспектив развития

Что нас ждет к 2030 году?

Из долгосрочного прогноза научно-технологического развития России до 2030г. (prognoz.hse.ru)

Прогноз в области информационно-коммуникационных технологий (ИКТ)

Глобальные вызовы

- Усиление контроля над информацией в сети Интернет
- Увеличение дисбаланса между требованиями безопасности и личной свободой человека
- Рост киберпреступности и масштаба ее эффектов (технических сбоев и др.)
- Радикальная трансформация рынков ИКТ в условиях смены технологий компонентной базы (прекращение действия закона Мура, развитие новых материалов, фотоники и др.)

Окна возможностей

- Производство и поддержание функционирования суперкомпьютеров
- Работа со сверхбольшими объемами данных (Big Data)
- Создание новых интерфейсов «человек – цифровая среда»
- Конвергенция информационных платформ
- Обеспечение повсеместного высокоскоростного доступа к сетевой инфраструктуре
- Формирование единой управляющей среды
- Новые принципы организации вычислений
- Разработка эффективных форм представления информации, контента и знаний
- Эволюция Интернета («семантический веб», «Интернет вещей»)
- Моделирование человеческого интеллекта, когнитивные модели сознания и поведения
- Разработка биоподобных и антропоморфных робототехнических устройств

2030

Угрозы для России

Ускоренное формирование единого глобального информационного пространства
Обострение «цифрового неравенства»
Неготовность к широкомасштабному предоставлению гражданам медицинских и иных социальных услуг с использованием ИКТ
Возможность использования потенциала ИКТ в целях подрыва национальной безопасности, нарушения государственного и общественного порядка
Необходимость обеспечения эффективного (защищенного) документооборота
Неготовность к массовому применению технологий виртуальной реальности

2030

Представление по годам до 2030

Вывод:

ожидается возрастание неопределенности и сложности на порядки

Трансформация с внедрением «умных» систем

Из промышленного и технологического форсайта РФ на долгосрочную перспективу

<u>Вывод</u>: ожидаются более частые изменения в сложных структурах

Какие перспективные планы в Европе?

Страны, участвующие в реализации Плана и выработанных стратегий: Франция, Германия, Италия, Нидерланды, Испания, Швеция, Швейцария, Великобритания

Выделены основные области:

- умные сети и города / технологии;
- интеллектуальные транспортные системы;
- передовое производство;
- робототехника и автономные системы
- облачные вычисления
- информация общественного сектора, открытые данные и большие данные;
- электронное управление;
- обмен метаданными по интероперабельным активам многократного использования (в электронном управлении);
- основные базы для облегчения разработки интероперабельных решений;
- электронная идентификация и доверительные услуги, включая электронные подписи;
- радиометки (RFID);
- Интернет вещей;
- сетевая и информационная безопасность;
- электронная инфраструктуры для исследовательских данных и науки; интенсивных вычислений;
- широкополосная инфраструктура

ВЫВОД:

ЗАДАЧИ АНАЛИТИЧЕСКОГО ПРОГНОЗИРОВАНИЯ РИСКОВ И ОБОСНОВАНИЕ СБАЛАНСИРОВАННЫХ МЕР УПРЕЖДАЮЩЕГО ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ОСТРО АКТУАЛЬНЫ!

2. ОСНОВНАЯ ИДЕЯ – ПОВОРОТ К СИСТЕМНОЙ ИНЖЕНЕРИИ

Определения

Система - комбинация взаимодействующих элементов, организованная для достижения одной или нескольких поставленных целей (по ГОСТ Р ИСО/МЭК 15288-05, 9001 - 2008)

Системная инженерия – это избирательное приложение научно-технических усилий по:

преобразованию функциональных потребностей в описание системной конфигурации, которая наилучшим образом удовлетворяет этим потребностям по показателям эффективности;

объединению связанных технических параметров и обеспечению совместимости всех физических, функциональных и программно-технических интерфейсов способом, оптимизирующим в целом определение и проектирование всей системы;

объединению возможностей всех инженерных дисциплин и специальностей в единое системотехническое достижение

Риск - мера опасности с ее последствиями (по ФЗ «О техническом регулировании», ГОСТ Р ИСО/МЭК 15026-02, ГОСТ Р ИСО/МЭК 16085-07, ГОСТ РВ 51987-02)

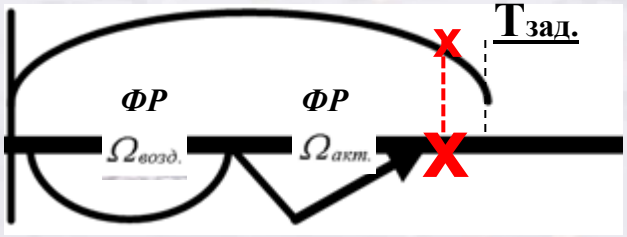
Риск – эффект неопределенности в целях (задачах) (по ISO 31000 - 2009)

Эффект – отклонение от ожидаемого – негативного или позитивного

ОСНОВНАЯ ИДЕЯ ОЦЕНКИ КАЧЕСТВА ИНФОРМАЦИИ

СУТЬ ПРОГНОЗИРОВАНИЯ В ТЕРМИНАХ ФУНКЦИИ РАСПРЕДЕЛЕНИЯ ВРЕМЕНИ ДО НАРУШЕНИЯ БЕЗОПАСНОСТИ (в теории вероятности это - ВСЕ!)

В общем случае «черного ящика» (без контроля и восстановления)



функция распределения времени до нарушения (ФР) определяется так:

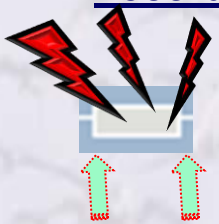
$$R(T_{зад.}) = P(\tau_{возн.} + \tau_{развития\ угрозы} \le T_{зад.})$$

$\tau_{возн.}$ – время между возникновениями угрозы, ФР = $\Omega_{возд.}$

$\tau_{развития\ угрозы}$ – время активизации угрозы, ФР = $\Omega_{акт.}$

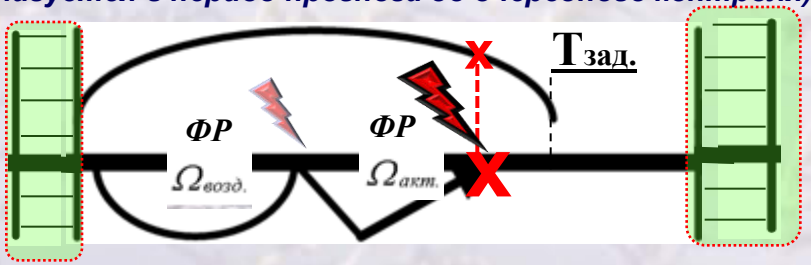
При экспоненциальной аппроксимации ФР Ωвозд.,Ωакт. достаточно знать частоту возникновения и среднее время развития угроз

Созданы аналитические модели для расчета ФР, учитывающие периодический контроль (с восстановлением после нарушений) и возможности мониторинга между контролями:



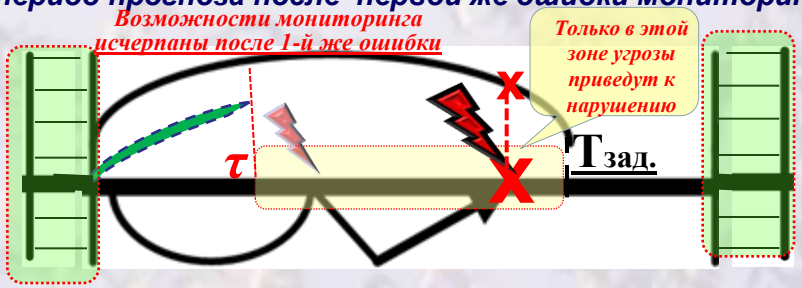
- реализуется периодический контроль (без непрерывного мониторинга)

(т.е. угроза приводит к нарушению, если только реализуется в период прогноза до очередного контроля)



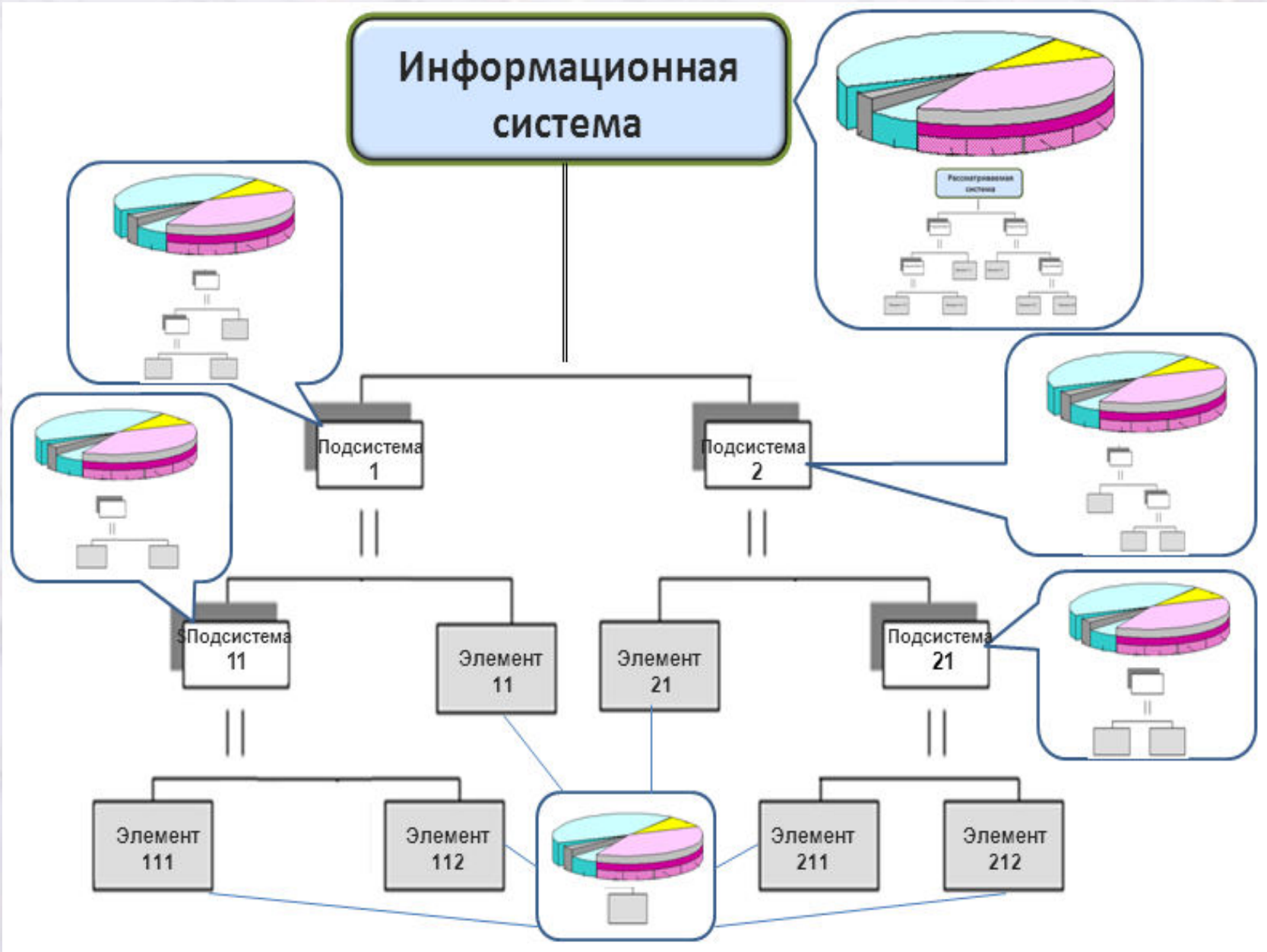
- между моментами контроля осуществляется мониторинг состояния

(т.е. угроза приводит к нарушению, если только реализуется в период прогноза после первой же ошибки мониторинга)



В итоге – возможно рассчитать ФР нарушения безопасности для Тзад. с учетом мер противодействия рискам (контроля, мониторинга, восстановления)

ДЕКОМПОЗИЦИЯ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ



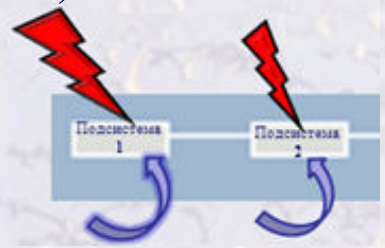
3. Генерация вероятностных моделей для сложных структур

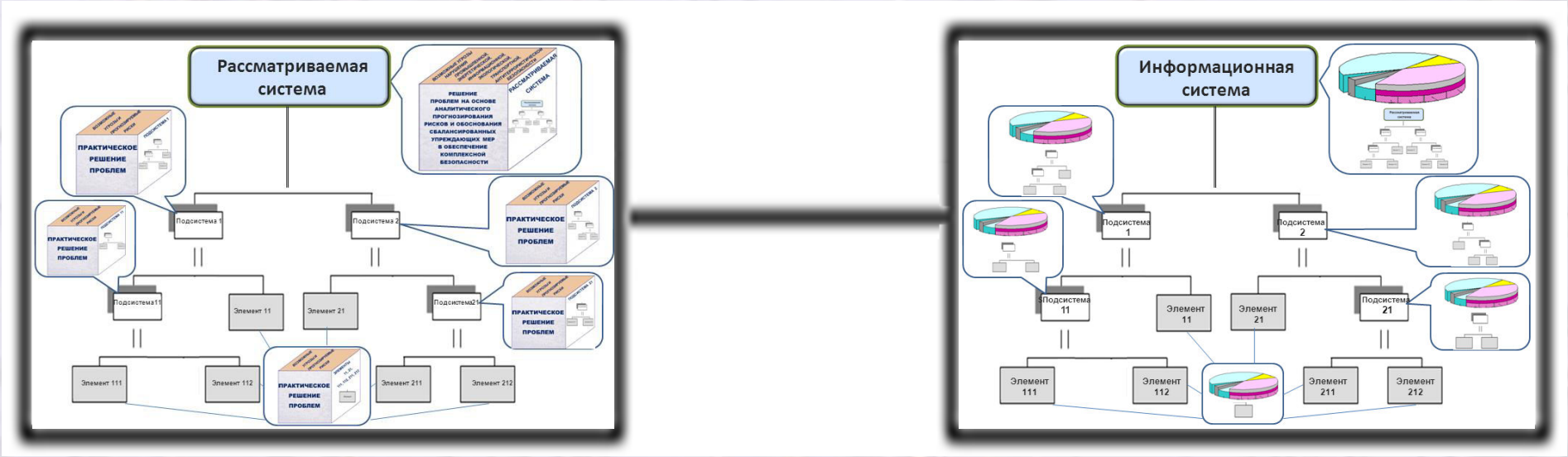
Комплексирование функций распределения для интегрируемых сложных архитектур

(при расчетах время t пробегает все значения от 0 до ∞)

Последовательное объединение - «И» 1-я «И» 2-я подсистемы

Риск $R(t) = 1 - [1 - R_1(t)][1 - R_2(t)]$





Логическая интерпретация элементарных состояний: интегрированная система находится в состоянии «отсутствия нарушений целостности», если «И» система слева, «И» система справа находятся в состоянии «отсутствия нарушений целостности»

Контроль и оптимизация

4. Оптимизационные задачи

Оптимизационные задачи для управления качеством в «процессном» подходе

Вариант реализации процесса Q(A,M) характеризуется параметрами:

сценарием критичных изменений среды реализации процесса и/или ресурсов и/или достигаемого качества выходных результатов процесса на заданном множестве потенциальных угроз (A - множество параметров сценария);

осуществляемыми мерами упреждения и реакции с учетом их стоимости для обеспечения целостности процесса (M - множество параметров, характеризующих эти меры)

Управляемые параметры процесса Q(A,M) признаются наиболее рациональными для заданного периода эксплуатации Тзад., если на них достигается минимум затрат на создание системы Zсозд. при ограничениях на приемлемый уровень качества Рдоп и допустимый уровень затрат при эксплуатации Сдоп.:

$$Z_{созд.}(Q_{рац.}) = \min_{\text{управляемые параметры A,M}} Z_{созд.}(Q)$$

при ограничениях Ркач. ≥ Рдоп. и Сэкспл. ≤ Сдоп. и, возможно, ограничениях на допустимые значения других показателей, отнесенных к критичным

Управляемые параметры процесса Q(A,M) признаются наиболее рациональными для заданного периода эксплуатации Тзад., если на них достигается максимум качества функционирования системы Ркач.

$$Р_{кач.}(Q_{рац.}) = \max_{\text{управляемые параметры A,M}} Р_{кач.}(Q)$$

при ограничениях Сэкспл. ≤ Сдоп. и, возможно, ограничениях на допустимые значения других показателей, отнесенных к критичным

Оптимизационные задачи для управления рисками в «процессном» подходе

Вариант реализации процесса Q(A,M) характеризуется параметрами:

сценарием критичных изменений среды реализации процесса и/или ресурсов и/или достигаемой безопасности на заданном множестве потенциальных угроз (A - множество параметров сценария);

осуществляемыми мерами упреждения и реакции с учетом их стоимости для обеспечения целостности процесса (M - множество параметров, характеризующих эти меры)

Управляемые параметры процесса Q(A,M) признаются наиболее рациональными для заданного периода эксплуатации Тзад., если на них достигается минимум затрат на создание системы Zсозд. при ограничениях на приемлемый уровень риска Rдоп и допустимый уровень затрат при эксплуатации Сдоп.:

$$Z_{созд.}(Q_{рац.}) = \min_{\text{управляемые параметры A,M}} Z_{созд.}(Q)$$

при ограничениях $R \le R_{доп.}$ и $С_{экспл.} \le С_{доп.}$ и, возможно, ограничениях на допустимые значения других показателей, отнесенных к критичным

Управляемые параметры процесса Q(A,M) признаются наиболее рациональными для заданного периода эксплуатации Тзад., если на них достигается минимум риска нарушения безопасности функционирования системы R

$$R(Q_{рац.}) = \min_{\text{управляемые параметры A,M}} R(Q)$$

при ограничениях $С_{экспл.} \le С_{доп.}$ и, возможно, ограничениях на допустимые значения других показателей, отнесенных к критичным

5. ПРИМЕР РЕАЛИЗАЦИИ И ИЗВЛЕЧЕНИЯ ЭФФЕКТОВ

из прогнозирования техногенных рисков для обеспечения информационной и промышленной безопасности критически важных объектов нефтегазовой отрасли

(удостоена премии Правительства РФ в области науки и техники за 2014г.)

СУТЬ РЕАЛИЗАЦИИ

Потребители углеводородов:
Административные области, регионы
Хранилища углеводородов
Предприятия и организации
Жилые дома и строения

Основные угрозы:
Разрушение трубопроводов
Возгорание углеводородов
Взрывы
Отключения потребителей из-за нарушений техногенной безопасности

ВОЗНИКНОВЕНИЕ, РАЗВИТИЕ, КОНТРОЛЬ И НЕЙТРАЛИЗАЦИЯ ВОЗМОЖНЫХ УГРОЗ

Научно-техническая и технологическая проблема:

• интеллектуальной поддержки принятия эффективных решений по предупреждению чрезвычайных ситуаций природного и техногенного характера и смягчению негативных последствий на основе многофакторного мониторинга ситуаций, прогнозирования рисков и рационального управления системными процессами

Цель:

• создание функциональных возможностей по раннему выявлению и распознаванию разнородных угроз, прогнозированию развития нештатных ситуаций, обоснованию и реализации целенаправленных упреждающих мер, оптимизации параметров газораспределения, предупреждению и устранению предаварийных и аварийных ситуаций

Совершенствование существующей Концепции управления рисками на основе реализации идей

Недостатки

(в общем случае применения Концепции)

Не осуществляется накопления и целенаправленной обработки информации для системного обоснования рациональных мер контроля, монито-ринга и восстано-вления нарушаемой целостности «умных» элементов

Используемые методы расчета рисков специфичны, результаты несравнимы

Для различного рода угроз задачи количественного обоснования требований к средствам и системным процессам при ограничениях на ресурсы и допустимые риски – не решаются

Системная инженерия

Описание системы

Размеры рисков

Возможности устранения и уменьшения рисков

Допустимые пределы рисков

Проект систе-мы, эксплуати-руемая система

Возможности устранения и уменьшения рисков

Формализованные требования к целостности системы

Основные задачи замысла, получившие научно-теоретическое и практическое разрешение в работе

Создание и совершенствование математических моделей для исследований путей решения проблемы

Комбинация и автоматическая генерация новых моделей

Опытные образцы базы знаний и информационных технологий

Варианты решения типовых производственных задач для управления рисками

РЕАЛИЗАЦИЯ

ОБЩИЙ ВИД ПЕРИФЕРИЙНОГО ПОСТА

ПЕРИФЕРИЙНАЯ ПОДСИСТЕМА

ТЕХНИЧЕСКОЕ РЕШЕНИЕ

НОВИЗНА

1. Функции обеспечения техногенной безопасности внедрены в технологические процессы газораспределения, включая контроль и мониторинг окружающей среды

2. Обеспечены:

- выявление и распознавание разнородных угроз

- раннее прогнозирование развития нештатных ситуаций и загрязнения окружающей среды

- обоснование и реализация целенаправленных управляющих мер предотвращения ущерба

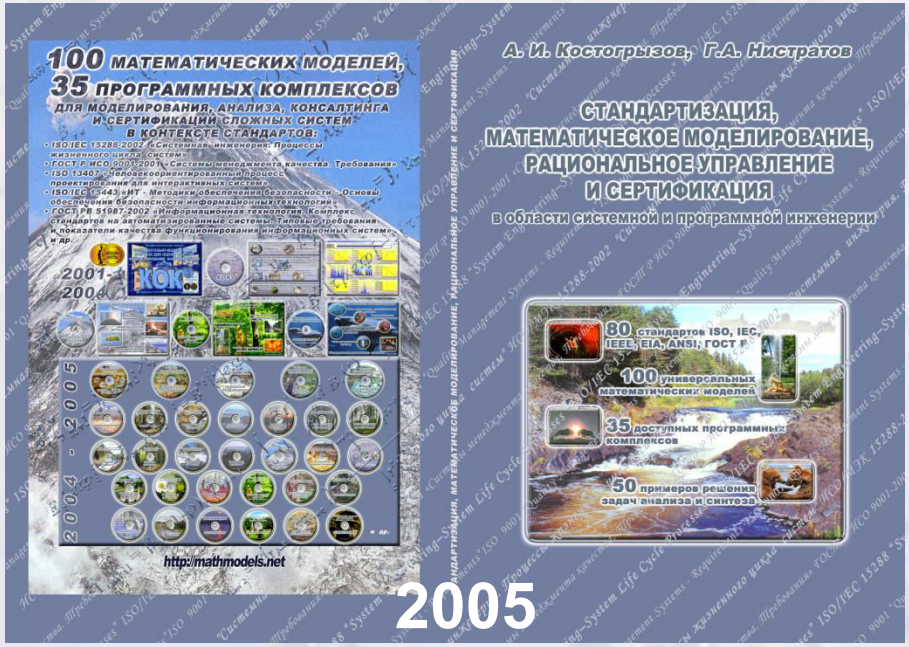
Оптимизация параметров газораспределения в жизненном цикле объектов обеспечивает предупреждение и устранение предаварийных и аварийных ситуаций

ДОСТИГНУТЫЕ ЭФФЕКТЫ

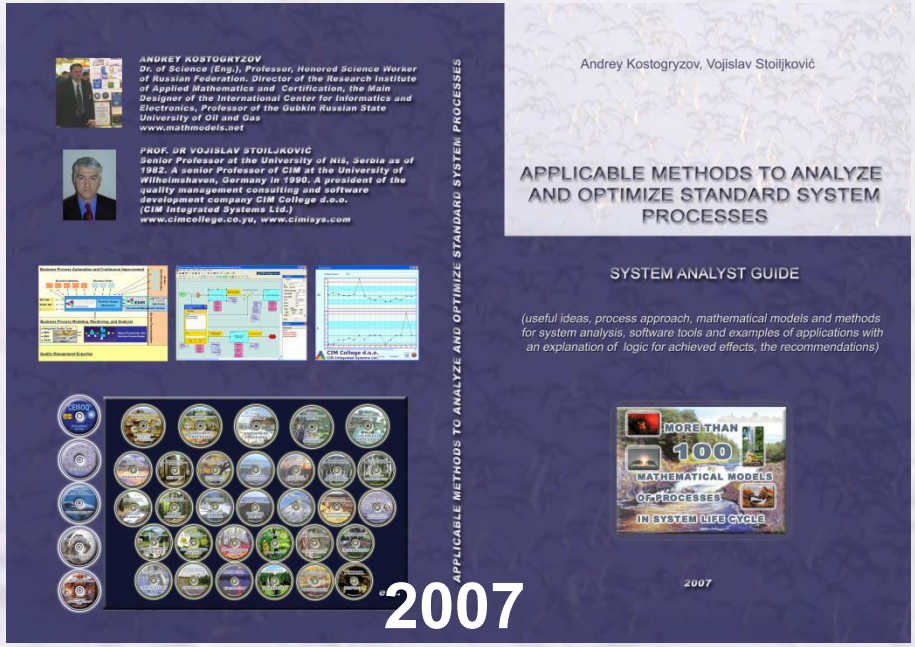
Реализованные функции	Достигнутые эффекты в решении практических проблем
1. Автоматизация процессов контроля режимов газоснабжения	Энергосбережение за счет оптимизации управления процессами
2. Мониторинг состояния технологического оборудования, распознавание и идентификация ситуаций (текущее состояние контролируемых объектов), раннее распознавание и прогнозирование развития предаварийных ситуаций	Сокращение затрат на ремонт, обеспечена оперативная реакция признаки предаварийных ситуаций для предотвращения нарушений техногенной безопасности
3. Сбор и обработка информации о расходе газопродукции	Возможность планирования расхода энергоресурсов, оперативного перераспределения газопотребления в соответствии с текущей техногенной и экологической ситуацией
4.Оперативное дистанционное управление	Энергосбережение, уменьшение финансовых затрат за счет снижения количества бригад, неплановых выездов на места, предотвращения нарушений техногенной безопасности
5. Обобщение поступающей информации, технический аудит, архивирование и документирование данных	Оперативное обнаружение источников нарушения безопасности и определение путей обеспечения потребителей продукции за счет своевременного принятия и реализации управленческих решений
6. Безопасность эксплуатации, в т.ч. функции доступа	Предупреждение преднамеренного вмешательства в технологический процесс (в т.ч. защита от «человеческого фактора»), предупреждение хищений и порчи оборудования за счет «антивандальной реализации» в различных природных условиях (в т.ч. для условий п-ва Ямал и в Арктики)

Применение Комплекса в период 2009-2014гг. **уже обеспечило возможность экономии 8,5 млрд рублей, что достигнуто за счет эффективного внедрения функций обеспечения техногенной безопасности** в технологические процессы контроля и мониторинга газораспределения

Монографии 2005-2010



2005



2007

2008

2010

Монографии 2012-2015