17 октября 2011

МЕТОДЫ И ИНСТРУМЕНТАРИИ ПРОГНОЗИРОВАНИЯ КАЧЕСТВА И РИСКОВ ДЛЯ УПРАВЛЕНИЯ ЭФФЕКТИВНОСТЬЮ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ

Дтн, проф. А.И. Костогрызов

www.mathmodels.net

(495) 795-85-24, (499) 764-26-58

Цель на ближайшие годы

Согласно «Стратегии развития информационного общества в РФ» от 07.02.2008 г. №Пр-212 целью формирования и развития информационного общества в России является повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления на основе использования информационных и телекоммуникационных технологий

Общее

Сегодня уже действуют стандарты для систем любой области приложения – это ISO 9001 (требования к системе менеджмента качества), ISO/IEC 15288 (первый стандарт по системной инженерии, регламентирует процессы жизненного цикла систем), стандарты ISO серий 14000 (менеджмент экологической безопасности), 18000 (менеджмент охраны труда), 20000 (сервис-менеджмент), 27000 (менеджмент информационной безопасности), 31000 (менеджмент риска) и др.

Новые определения

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

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)

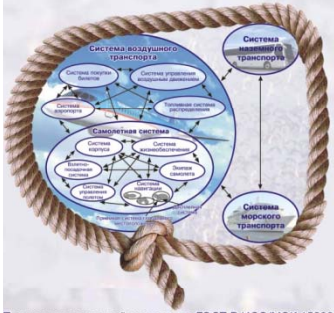
Риск – эффект неопределенности в целях (задачах) (по ISO 31000 - 2009)

Эффект – отклонение от ожидаемого – негативного или позитивного

В чем суть основных системных изменений?

- в разработке и внедрении основ системной инженерии в различные сферы человеческой жизнедеятельности

(что отражает стремление к решению проблем на уровне систем, а не составных компонентов)



Пример транспортной системы из ГОСТ Р ИСО/МЭК 15288

Важные исследования задерживаются из-за того, что в той или иной области неизвестны результаты, уже давно ставшие классическими в смежной области
Н. Винер

Особенность нашего времени – поворот к системной инженерии

Система - комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких целей (ГОСТ Р ИСО/МЭК 15288)

20-й век			21-й век
30-60 гг.	70-80 гг.	90-е гг.	сегодня
Кибернетика и математическое моделирование	Теория вероятностей, основы системного анализа	Теория системной инженерии	

Оценки потоков и вероятностно-временных характеристик

Теория надежности, модели под конкретные системы

Стандарты и др. нормативные документы, базовые модели, методы оценки и процессы обеспечения качества

Бум прошел

Апробированные математические модели, инструментальные средства и технологии их эффективного применения

Инженерия – это применение научных основ, в первую очередь математики, при помощи которых свойства материалов и источники энергии становятся полезными для людей (IEEE Std 610.12)

Системная инженерия – избирательное приложение научно-технических усилий по: преобразованию функциональных потребностей в описание технического облика, который наилучшим образом удовлетворяет этим потребностям по показателям эффективности; обеспечению целостности всех физических, функциональных и программно-технических интерфейсов способами, оптимизирующими проектирование и применение всей системы (SEI)

- в широком применении и развитии «процессного подхода» на уровне стандартов

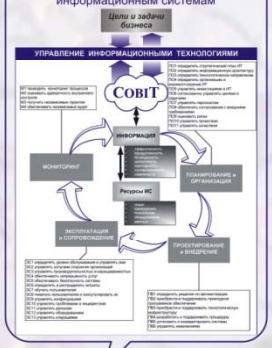
Эволюционное развитие процессного подхода

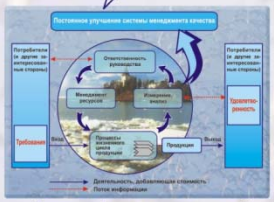
Процессы сбора, обработки, хранения и представления информации в автоматизированных системах

Зарождение процессного подхода на уровне стандартов для автоматизированных систем 34-й серии

80 – 90 г.г.

Пример развития в приложении к информационным системам





Процессный подход для предприятий на уровне ГОСТ Р ИСО 9001 «Системы менеджмента качества. Требования»

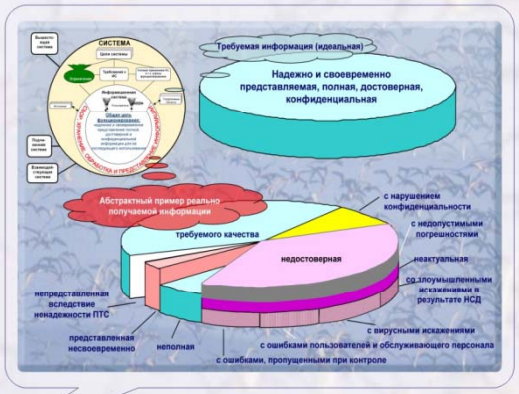
2000 – 2001 г.г.

Пример использования в ГОСТ 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения»

Процессный подход для систем на уровне ГОСТ Р ИСО/МЭК 15288 «Системная инженерия. Процессы жизненного цикла систем», 12207 «Процессы жизненного цикла программных средств», 16085 «Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения» и др.

2002 – 2009 г.г.

- в достижении эффектов, напрямую зависящих от возможностей и уязвимостей применяемых информационных технологий и систем



Пример формализации, используемой для информационных систем (по ГОСТ РВ 51987

Без формализации информационных процессов и вероятностного анализа качества используемой информации эффективность автоматизации непрогнозируема

- в объективных потребностях моделирования процессов и систем на всех стадиях жизненного цикла

(принципиально важным становится непрерывный количественный анализ и обоснование рациональных способов достижения промежуточных и конечных целей при ограничениях на сроки, ресурсы, затраты)

=> Предлагаемые модели и поддерживающие их инструментарии призваны снять практическое противоречие между объективными потребностями в эффективном управлении качеством и рисками и невозможностью удовлетворения этих потребностей в режиме реального времени из-за сложности создания достаточно адекватных и доступных математических моделей, высокой стоимости и сроков их программной реализации!

ГОСТ Р ИСО/МЭК 15288 «Системная инженерия. Процессы жизненного цикла систем»

Процессы жизненного цикла систем

Процессы соглашения

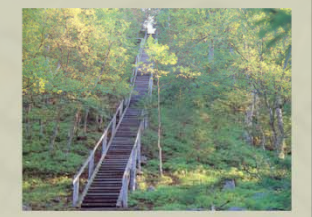
Процесс приобретения
Процесс поставки

Процессы предприятия

Процесс управления средой предприятия
Процесс управления инвестициями
Процесс управления процессами жизненного цикла системы
Процесс управления ресурсами
Процесс управления качеством

Процессы проекта

Процесс планирования проекта
Процесс оценки проекта
Процесс контроля проекта
Процесс принятия решений
Процесс управления рисками
Процесс управленя конфигурацией
Процесс управления информацией



Технические процессы

Процесс определения требований правообладателей
Процесс анализа требований
Процесс проектирования архитектуры
Процесс изготовления
Процесс комплексирования
Процесс верификации
Процесс передачи
Процесс валидации
Процесс функционирования
Процесс обслуживания
Процесс изъятия и списания

Пример процесса управления информацией

Цель процесса управления информацией

своевременное предоставление заинтересованным сторонам необходимой полной, достоверной и, если требуется, конфиденциальной информации в течение и, соответственно, после завершения жизненного цикла системы

Результаты процесса управления информацией

определяется информация, подлежащая управлению;
определяются формы представления информации;
информация преобразуется и распределяется в соответствии с требованиями;
документируется статус информации;
информация является “свежей”, полной и достоверной;
информация становится доступной для уполномоченных сторон

Деятельность в процессе управления информацией

определять содержание, семантику, форматы и средства для представления, хранения, передачи и поиска информации;

Примечание – Информация может появляться и исчезать в любой форме (например, вербальной, текстовой, графической и числовой) и может быть сохранена, обработана, продублирована и передана при помощи любых средств (например, электронных, печатных, магнитных, оптических). Необходимо учитывать ограничения организации, например, инфраструктуру, внутриорганизационные связи, распределенные работы над проектом. Стандарты и соглашения, касающиеся хранения, преобразования, передачи и представления информации, используются в соответствии с политикой организации, соглашениями и ограничениями, указанными в законодательных актах

получать идентифицированные элементы информации;

Примечание – Сюда может относиться формирование информации или ее сбор от соответствующих источников

обслуживать элементы информации и хранящиеся записи этих в соответствии с требованиями к целостности, защите и сохранению тайны;

Примечание – Следует регистрировать статус элементов информации, например описание версий, запись распределения, классификация уровней защиты. Информация должна быть четкой, храниться и аккумулироваться таким образом, чтобы ее можно было легко извлекать из средств, предоставляемых соответствующим окружением, и которые предотвращают разрушение, порчу и потерю информации

определять меры по сопровождению информации;

Примечание – К ним относится анализ статуса хранимой информации в отношении ее целостности, достоверности, доступности и любых потребностей в копировании или переносе на альтернативный носитель. В случае изменения технологии следует рассматривать варианты: либо сохранить инфраструктуру так, чтобы архивные данные могли быть прочитаны; либо осуществить перезапись архивных данных с использованием новой технологии

архивировать заданную информацию в соответствии с целями аудита и сохранения знаний;

Примечание – Необходимо выбирать носители, местоположение хранилищ и способы защиты информации в соответствии с обоснованными в спецификациях периодами хранения и восстановления информации, политикой организации, соглашениями и законодательством

Задачи, решаемые на основе математического моделирования

Анализ качества процессов представления информации
(Надежность, Своевременность)
Анализ качества используемой информации
(Полнота, Актуальность, Безошибочность после контроля, Корректность после обработки, Конфиденциальность)
Анализ безопасности функционирования системы
(Безошибочность действий человека, Защищенность от опасных воздействий, Защищенность от несанкционированного доступа)

Пример процесса управления рисками

Цель процесса управления рисками

снижение последствий отрицательного воздействия вероятных событий, которые могут явиться причиной изменений качества, затрат, сроков или ухудшения технических характеристик

Результаты процесса управления рисками

определяются и классифицируются риски;
количественно оцениваются вероятности и последствия осуществления рисков;
устанавливается стратегия реакции на каждый из рисков;
определяется и объявляется статус риска;
принимаются соответствующие меры в случае, если риск вышел за пределы приемлемых значений

Деятельность в процессе управления рисками

налаживать систематический подход к определению рисков, их оценке и выработке соответствующей реакции;

Примечание – К данному действию относится определение событий, которые негативно влияют на систему, проект или организацию. Также сюда может входить классификация рисков. В пределах качества, затрат, сроков или технических характеристик определяют способ выражения рисков в соответствующих терминах, включая показатели там, где это возможно

идентифицировать и определять риски;

определять вероятности событий, связанных с рисками, используя установленные критерии;

оценивать риски в терминах возможных последствий, используя установленные критерии;

определять градации рисков по их вероятности и последствиям;

определять стратегии реакции на риски;

Примечание – К этому действию относятся:

1) предупреждение риска путем принятия решения об уклонении от вовлечения в опасную ситуацию, либо выхода из нее;

2) оптимизация риска (включая его уменьшение), нацеленная на снижение негативных последствий риска и соответствующих вероятностей. Оптимизация риска зависит от критериев риска, в том числе затрат и официальных требований;

3) передача риска путем разделения ответственности за несение ущерба с другой стороной;

4) удержание риска в границах приемлемого ущерба

определять допустимые значения для каждого установленного риска;

устанавливать меры по обработке рисков в случае, если допустимые границы нарушены;

Примечание – Для рисков с тяжелыми последствиями необходимо составлять чрезвычайные планы, которые будут реализовываться в случае, если меры по уменьшению риска не привели к приемлемым результатам

вести учет рисков в течение всего жизненного цикла

Примечание – Учет включает определение текущего понимания рисков и отношения к мерам и ресурсам, связанным с реакцией на риски. Такой учет позволяет отслеживать историю рисков, что помогает при принятии решений и может оказаться примером для проектирования будущих систем

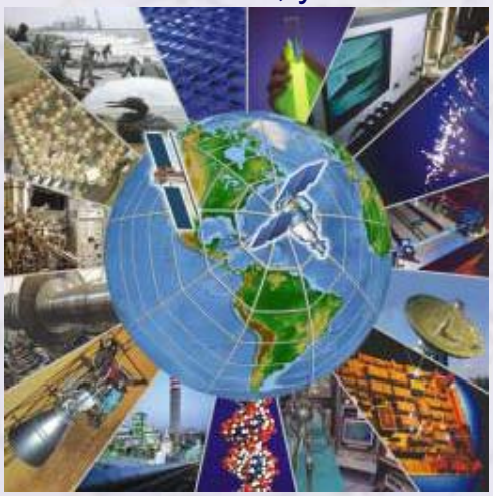
Задачи, решаемые на основе математического моделирования

Анализ риска неадекватной интерпретации событий
Анализ риска неконтролируемого развития ситуаций
Анализ эффективности мер противодействия рискам
Оценка стоимости удержания рисков
Обоснование параметров стратегии управления рисками

ВЫВОДЫ по результатам анализа



1. Для приложений, в которых уже были многочисленные факты трагедий с гибелью людей - **в сфере промышленной, пожарной, радиационной, ядерной, авиационной безопасности - требования к допустимым рискам выражены количественно на вероятностном уровне** и на уровне необходимых требований к исходным материалам, используемым ресурсам, технологиям, начальным состояниям, условиям эксплуатации








2. Для иных приложений - **в сфере химической, биологической, транспортной, экологической безопасности, безопасности зданий и сооружений, информационной безопасности, в т.ч. в условиях террористических угроз – требования к допустимым рискам задаются преимущественно на качественном уровне** в форме требований к выполнению конкретных условий. Это означает невозможность корректного решения обратных задач управления безопасностью исходя из задаваемого уровня допустимого риска

ВЫВОДЫ по результатам анализа (продолжение)

3. Во всех случаях **эффективное управление рисками** для любого рода систем при штатных начальных состояниях **возможно и целесообразно** на основе:

а) использования исходных ресурсов и защитных технологий с более лучшими характеристиками с точки зрения безопасности, в т.ч. для восстановления целостности;

б) рационального применения адекватной системы **ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности;**

в) рационального применения мер противодействия рискам

Общее в управлении рисками

Риск *– это "…вероятность причинения вреда… с учетом тяжести этого вреда"* - № 184-ФЗ от 27.12.2002г.,ст.2

Риск - *мера опасности, характеризующая вероятность возникновения возможных аварий и тяжесть их последствий* - Методические рекомендации РД 03-357-00

Производственная безопасность

Пожарная безопасность

Радиационная и ядерная безопасность

Экологическая безопасность

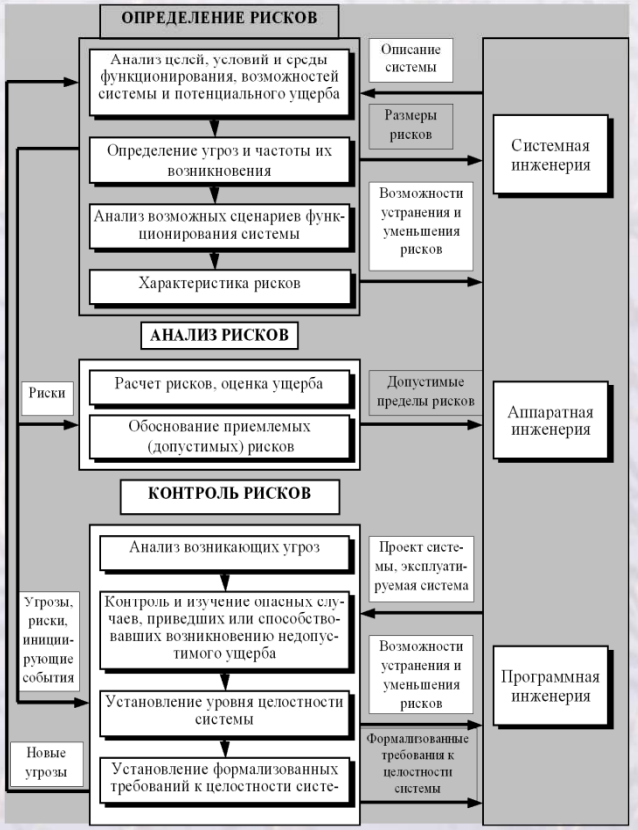
Транспортная безопасность

Авиационная безопасность

Безопасность высотных зданий

Информационная безопасность

и др.



4. **Существующие модели** для анализа рисков в приложении к гприродным и техногенным ситуациям **Неидентичны** *(поэтому понятие допустимых рисков логически не сравнимо),* они **не позволяют решать обратные задачи обоснования** требований к системам сбора и анализа информации, параметрам контроля и мониторинга и мер противодействия при ограничениях на выделяемые средства и допустимые риски.

А это не позволяет утверждать об эффективности упреждающего решения проблем безопасности!

Объективные потребности в оценке качества и рисков в жизненном цикле систем

Предлагаемые методы и инструментарии прогнозирования

Математические модели для оценки качества и рисков в соответствии с требованиями системообразующих стандартов

Анализ правовых документов

Законы РФ

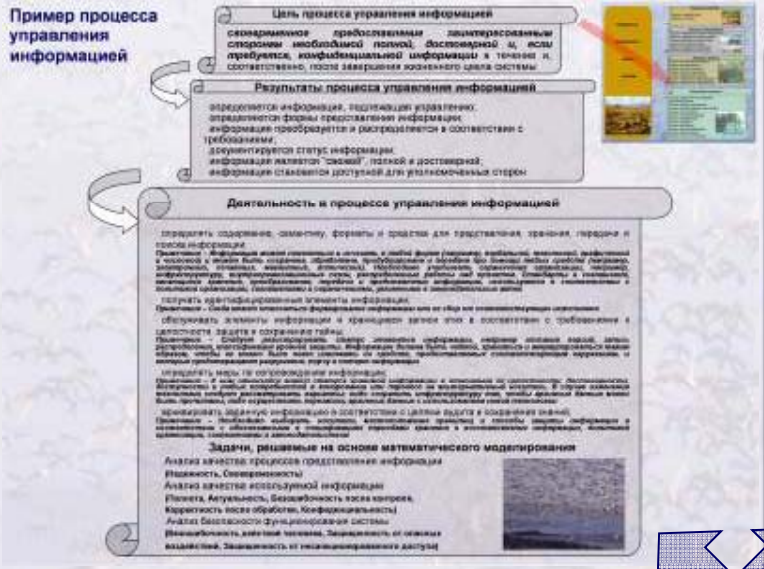
"О безопасности", «О промышленной безопасности опасных производственных объектов», «О пожарной безопасности», «Об использовании атомной энергии», «О радиационной безопасности населения», «О транспортной безопасности», Воздушный кодекс Российской Федерации (в части авиационной безопасности), «О связи» (в части защиты и управления), «О противодействии терроризму», «Концепция безопасности Москвы», «О государственной тайне», «О коммерческой тайне», «Об информации, информационных технологиях и защите информации», Доктрина информационной безопасности и др.

и др.

Содержание программных комплексов в поддержку системообразующих стандартов

Качество функционирования информационных систем по ГОСТ 34.602, ГОСТ РВ 51987, ГОСТ Р ИСО/МЭК 15288

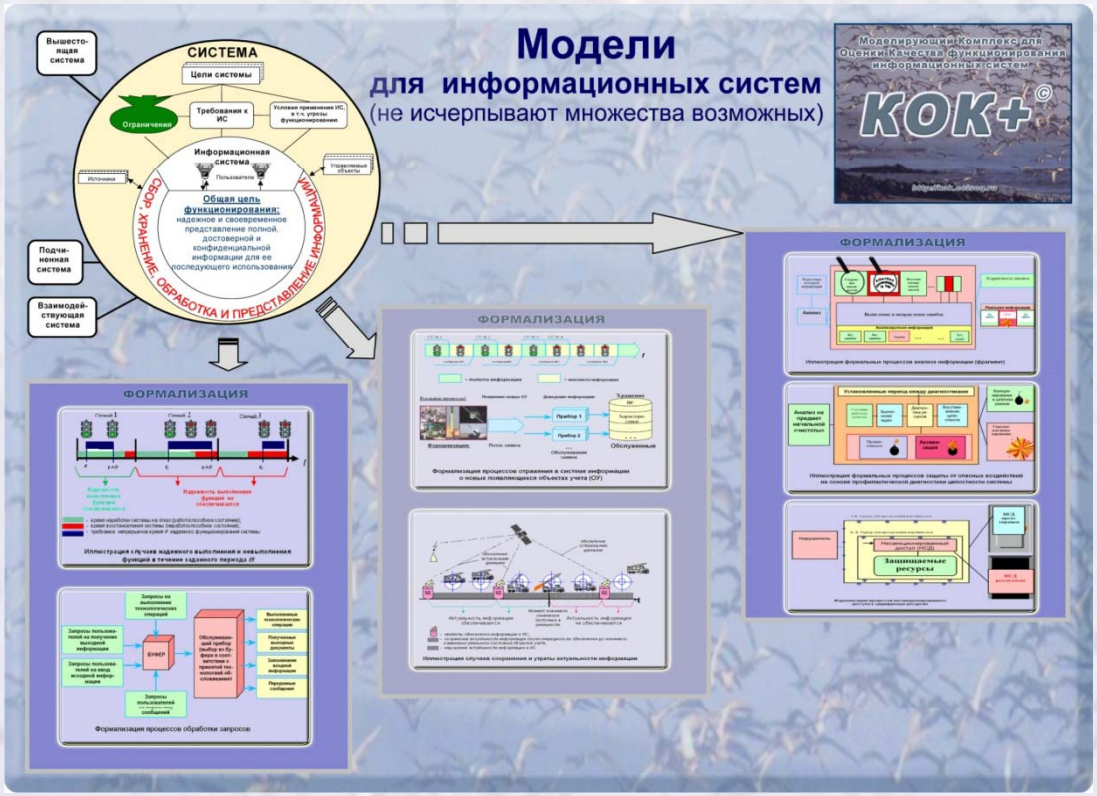
Пример процесса управления информацией



Пример формализации

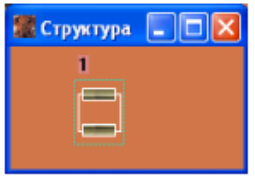
Построение и развитие сложных систем базируется на системном анализе

Модели
для информационных систем
(не исчерпывают множества возможных)

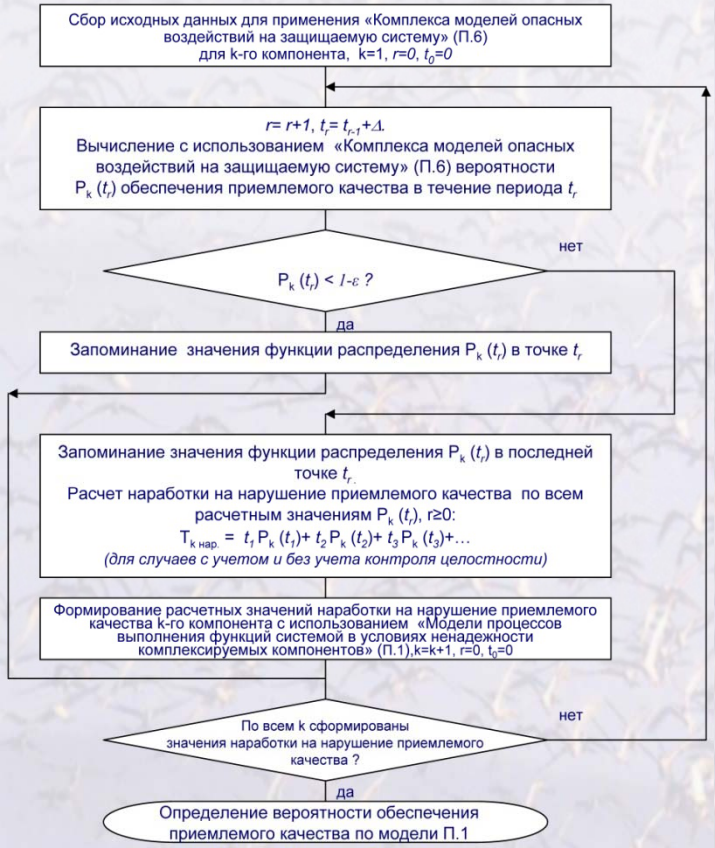


Сворачивание элементов и комбинация моделей

ФР времени наработки на отказ $B(t) = 1 - [1 - B_1(t)][1 - B_2(t)]$



ФР времени наработки на отказ $B(t) = B_1(t)B_2(t)$



Примеры моделирующих комплексов

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.:

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

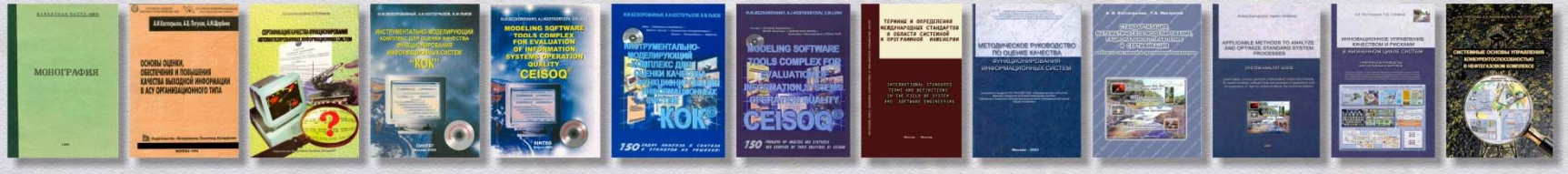
при ограничениях $R \le R_{доп.}$ и $С_{экспл.} \le С_{доп.}$ и, возможно, ограничениях на допустимые значения других показателей, отнесенных к критичным

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

МОНОГРАФИИ



СТАТЬИ И ДОКЛАДЫ НА НАУЧНО-ТЕХНИЧЕСКИХ ФОРУМАХ

Возможные пути обеспечения и повышения эффективности:

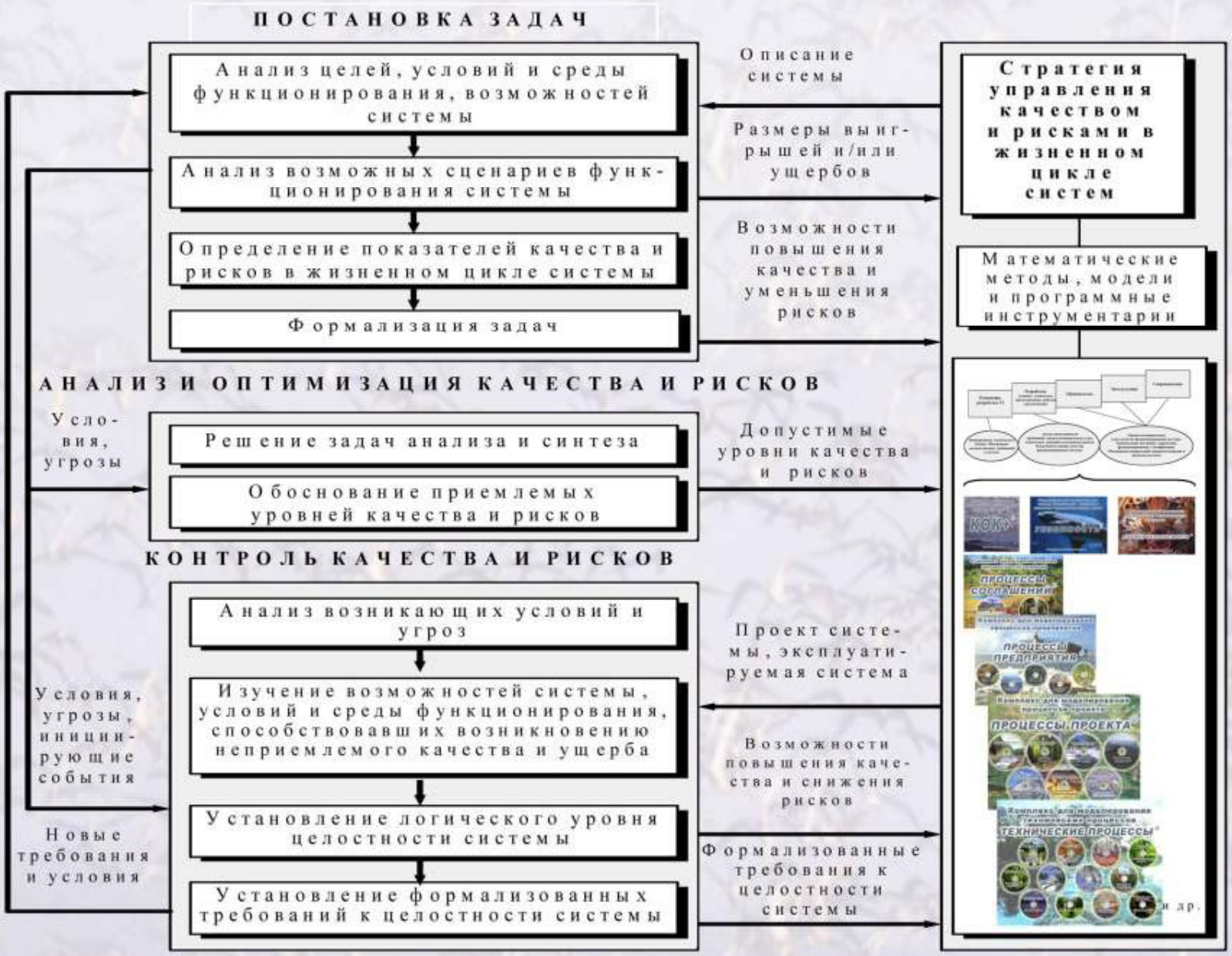
1- традиционный – прагматическая фильтрация информации

(собственный опыт, качественный анализ, ориентация на стандарты)

2 – инновационный – генерация обоснованных идей и эффективных решений

(внедрение основ системной инженерии по требованиям международных и отечественных стандартов)

Контроль и оптимизация



Виртуальное моделирование
(в т.ч. через Интернет)

НИИ, (моделирующие стенды)

ВУЗы (свои и приобретенные модели)

Существующий подход к моделированию процессов

(каждый решает свои проблемы, как может)

Нынешнее состояние

1. Все организации нуждаются в количественных оценках, но лишь малая часть довольствуется результатами расчётов на моделирующих стендах.
2. Используемые модели являются узкоспециализированными, расчётные показатели привязаны к специфике систем и не ориентированы на комплекс требований системообразующих стандартов.
3. Создание моделирующих стендов весьма затратно, осуществляется в рамках конкретных ОКР и под конкретные системы

Итог

1. Анализ качества и рисков и независимые количественные оценки в требуемой степени практически не осуществляются или осуществляются в исключительных случаях по заданию конкретного заказчика (например, по требованиям ядерной безопасности).
2. Уровень качества и безопасности систем в жизненном цикле не прогнозируется
3. Обучение расчетам не проводится

НИИ (моделирующие стенды)

Услуги через Internet

Виртуальный анализ качества и рисков (через несколько минут – 70-листовой аналитический отчет)

ВУЗы, Центры повышения квалификации, Инкубаторы …

Предлагаемый подход к моделированию процессов через Интернет

Отличительные черты

- ориентация на требования системообразующих стандартов с полнотой охвата типовых процессов;
- универсальность показателей и математических моделей, позволяющих оценку и прогноз;
- доступность и понятность для применения;
- возможность поддержки принятия решений через Интернет

Реализация предлагаемых возможностей

1. Через Интернет все организации получают доступ к универсальным моделям для количественного анализа качества и рисков в жизненном цикле систем различного приложения.
2. Расчётные показатели и используемые математические модели отвечают требованиям системообразующих стандартов, построены на теории случайных процессов и на этой основе носят универсальных характер

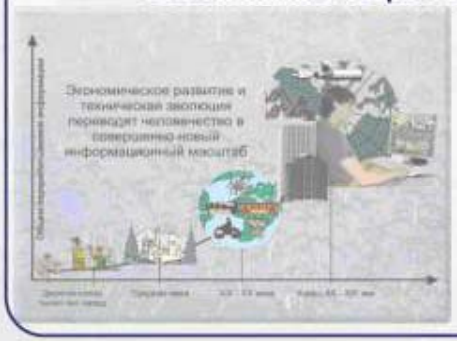
Итог

1. Все организации получают возможность эффективного управления качеством и рисками в соответствии с требованиями международных стандартов
2. Обучение основам системного анализа через Интернет доступно для всех подключенных (в т.ч. студентов)

Суть инновационного подхода к управлению качеством и рисками

От прагматической фильтрации информации ⇨ к генерации обоснованных идей и эффективных решений

Объективные потребности и предпосылки для совершенствования управления качеством и рисками (1)



Научно-методическая и инструментально-моделирующая основа (2)

Инновационный подход к управлению качеством и рисками в жизненном цикле систем

Примеры применения в различных приложениях(3)

Расчеты через Интернет (4)

Приложения для управления эффективностью

Пример по ISO 9001. Внутренние нормативные документы:

РК 1-01-2010 «СМК. Руководство по качеству».

СТО 2-01-2010 «СМК. Управление документацией».

СТО 3-01-2010 «СМК. Управление записями».

СТО 4-01-2010 «СМК. Управление работами, не соответствующими установленным требованиям».

СТО 5-01-2010 «СМК. Внутренние проверки».

СТО 6-01-2010 «СМК. Корректирующие действия».

СТО 7-01-2010 «СМК Предупреждающие действия».

СТО 8-01-2010 «СМК. Метрологическое обеспечение испытательной лаборатории».

СТО 9-01-2010 «СМК. Подготовка и аттестация персонала».

СТО 10-01-2010 «СМК. Обеспечение конфиденциальности информации и прав собственности заказчика».

СТО 11-01-2010 «СМК. Урегулирование претензий со стороны заказчика и других сторон».

СТО 12-01-2010 «СМК. Анализ со стороны руководства».

СТО 13-01-2010 «СМК. Управление субподрядами».

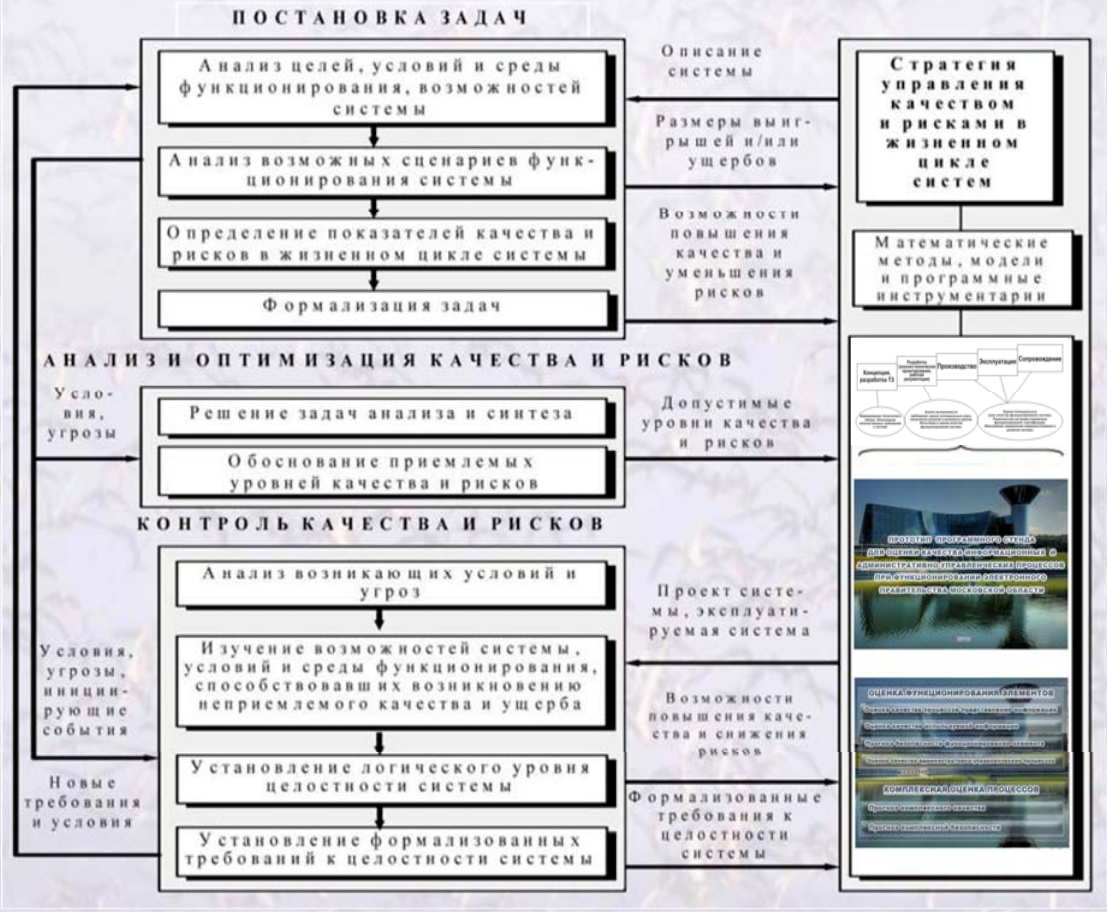
П 1-2010 «Положение о руководителе СМК и представителе руководства по качеству».

М 1-01-2010 «СМК. Методы и модели для выполнения работ. Методические положения по оценке качества и рисков на базе прототипа программного инструментально-аналитического стенда»

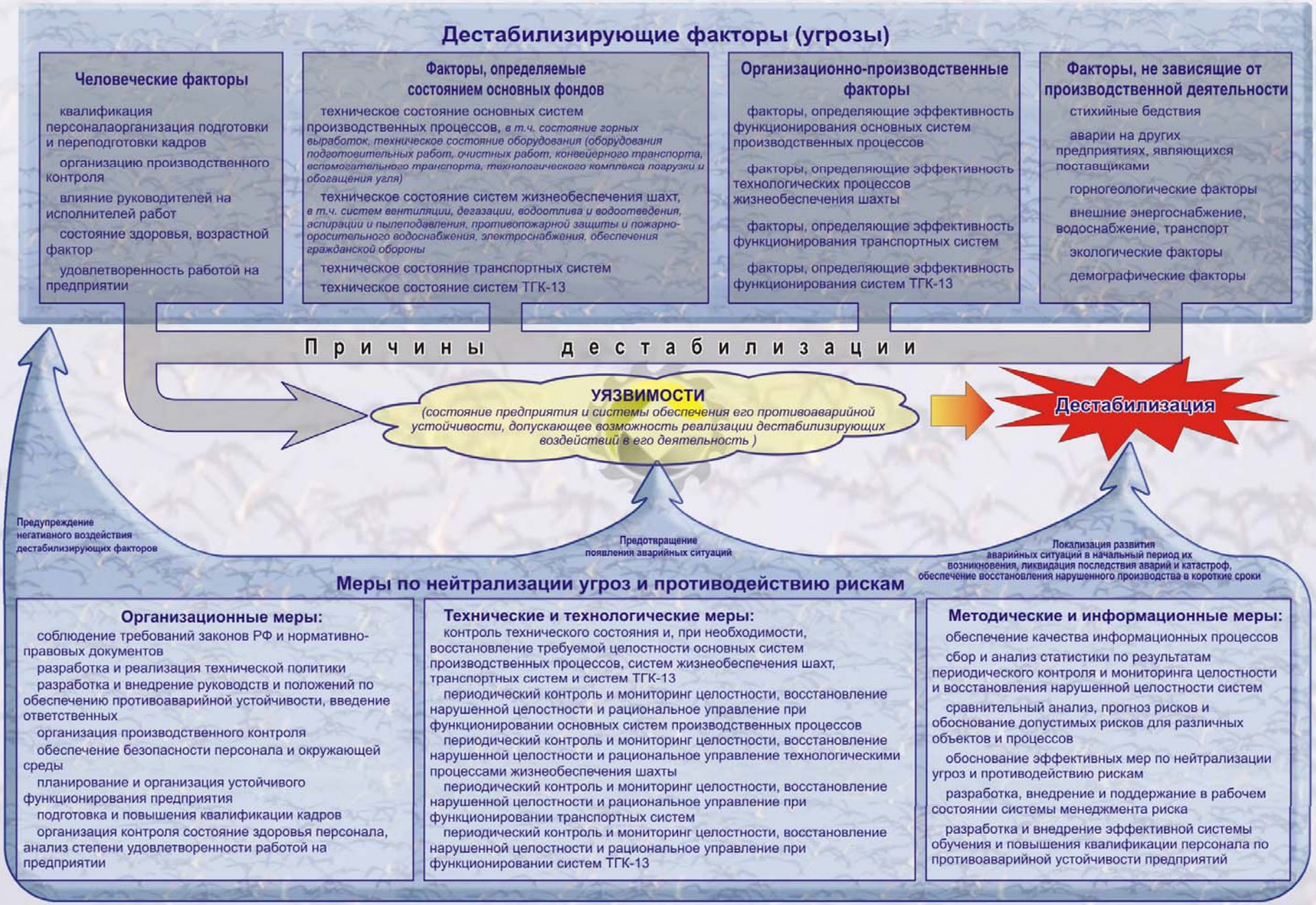
Управление качеством и рисками

Анализ взаимовлияния

Алгоритм рационального управления



Применение для построения системы противоаварийной устойчивости



Принципиальные положения ФЗ «О безопасности объектов ТЭК» №256-ФЗ от 21.07.2011

Статья 6, п. 1 Обеспечение безопасности объектов ТЭК осуществляется субъектами ТЭК … п.4 Контроль – за ФОИВ

Статья 7, п.1 Требования …определяются Правительством РФ; п.3 Субъекты ТЭК на стадиях проектирования и строительства объектов ТЭК обязаны предусматривать осуществление комплекса специальных мер по безопасному функционированию таких объектов, локализации и уменьшению последствий чрезвычайных ситуаций

2. Паспорт безопасности объекта ТЭК составляется на основании результатов категорирования объекта в зависимости от степени его потенциальной опасности,
а также на основании оценки достаточности инженерно-технических мероприятий, мероприятий по физической защите и охране объекта при террористических угрозах согласно требованиям Правительства РФ (по статье 7)

Паспорт

2. Анализ уязвимости производственно-технологического процесса и выявление критических элементов объекта

1. Перечень потенциально опасных участков объекта

№ п/п	Наименование производственно-технологического процесса	Наименование потенциально опасного участка объекта	Количество работающих, человек	Конструктивные и технологические элементы	Характер возможной аварийной (чрезвычайной) ситуации
1	2	3	4	5	6

2. Модели нарушителей _____

3. Перечень критических элементов объекта

№ п/п	Наименование критического элемента объекта	Базовые угрозы	Тип нарушителя	Оценка времени террористического акта	Влияние на обстановку на иных критических элементах объекта
1	2	3	4	5	6

Статья 6, п. 1

Обеспечение безопасности объектов ТЭК осуществляется субъектами ТЭК !!!

А какой остаточный риск будет иметь место в различных сценариях угроз?

5. Организация охраны и защиты объекта

1. Основания установления охраны

(номер распоряжения об установлении охраны, Ф.И.О., должность его подписавших, наличие акта региональной комиссии, дата его утверждения)

2. Структура подразделения охраны

(положение о подразделении охраны, вид подразделения: команда, группа с указанием их подчиненности и другие;

принадлежность охраны: ведомственная, вневедомственная, смешанная (ведомственная, вневедомственная), частные охранные организации, служба безопасности)

3. Штат подразделения охраны (перечисляются должности по штатному расписанию)

№ п/п	Наименование должности	Количество единиц
1	2	3
	Итого:	

4. Наличие организационно-распорядительных документов

(план и схема охраны, инструкция по организации и несению караульной службы, должностные инструкции,

план проверки технического состояния и работоспособности инженерно-технических средств охраны и прочее)

5. Организация пропускного и внутриобъектового режимов

(наличие инструкций, кем установлены пропускной и внутриобъектовый режимы, дата введения,

порядок хранения постоянных, разовых, временных и материальных пропусков, образцы подписей должностных лиц, наличие помещений для бюро пропусков, хранения личных вещей, комнат досмотра)

6. Количество действующих контрольно-пропускных пунктов:

Всего _____

Проходных _____

Автотранспортных _____

Железнодорожных _____

Совмещенных _____

7. Состав суточного наряда охраны отдельно по его принадлежности и виду

Вид поста	Количество	
	единиц	человек
Караулов		
Внешних постов		
Внутренних постов		
Суточных постов		
12-часовых постов		
8-часовых постов		
Всего		

8. Обеспеченность охраны

8.1. Оружием и боеприпасами

(наименование и количество единиц боевого ручного стрелкового оружия и патронов к нему — отдельно по каждому виду, типу, модели)

8.2. Специальными средствами и служебным огнестрельным оружием

(количество единиц специальных средств — отдельно по каждому виду, типу, модели; количество единиц служебного огнестрельного оружия и патронов к нему — отдельно по каждому виду, типу, модели)

8.3. Служебным авто-, мото- и авиатранспортом и водным транспортом

(нормы положенности авто-, мото- и авиатранспорта и водного транспорта, его наличие, марка, год выпуска, назначение — отдельно по каждой единице)

8.4. Служебными собаками

(наличие питомника, вольеров и их количество для содержания служебных собак — отдельно договорных и балансовых собак;

количество караульных собак, количество блокпостов, постов глухой привязи, свободного окарауливания)

9. Обеспечение сохранности оружия, боеприпасов и специальных средств

(характеристика помещения для хранения оружия, боеприпасов и специальных средств, установленные средства охранной и пожарной сигнализации, куда выведены)

10. Средний возраст сотрудников охраны

(лет)

11. Уровень подготовки органов управления и персонала, участвующих в обеспечении мероприятий по физической защите и охране

(наличие программы подготовки и переподготовки сотрудников охраны и органов управления предприятия, кем утверждена, порядок ее реализации, сведения о проводимых учениях, тренировках, проверках несения службы)

12. Наличие совместных (с органами внутренних дел и другими организациями) планов действий личного состава и администрации объекта при возникновении чрезвычайных ситуаций, включая акты незаконного вмешательства, стихийные бедствия и прочее; периодичность проведения совместных тренировок и учений, наличие оперативного штаба и специальных формирований, в том числе из штата предприятия

(наименование и дата утверждения)

6. Инженерно-технические средства охраны

1. Общая протяженность периметра, подлежащего ограждению

(пог. м)

2. Содержание ограждения

(характеристика ограждений: капитальные, деревянные, из колючей проволоки, сетчатые и другие, протяженность в пог. м каждого участка, состояние ограждения)

3. Освещение охраняемой территории и периметра ограждения

(наличие, краткая характеристика)

4. Охранная сигнализация ограждения

(перечислить территории, ограждение которых заблокировано сигнализацией, указать суммарную протяженность заблокированного ограждения в пог. м, тип и количество приборов сигнализации, установленных по периметру ограждения)

5. Сигнализация

(количество лучей)

5.1. Охранная сигнализация

(количество лучей)

5.2. Пожарная сигнализация

(количество лучей)

5.3. Совмещенная охранная и пожарная сигнализация

(количество лучей)

5.4. Тревожная сигнализация

(количество лучей, куда выведены)

5.5. Наличие средств радиосвязи

(количество постов, оборудованных радиосвязью, тип и количество радиостанций)

5.6. Наличие средств телефонной связи

(количество постов, оборудованных телефонной связью)

5.7. Наличие средств видеонаблюдения

(тип и количество видеокамер, контролируемые зоны)

6. Техника контрольно-пропускных пунктов

(тип и количество обычных турникетов, кабинно-турникетных систем, автоматизированных систем пропуска и табельного учета, механизированных ворот, применяемых средств принудительной остановки транспорта и иных специальных средств)

7. Наличие иных инженерных сооружений

(количество и содержание наблюдательных вышек, запретных зон, контрольно-следовых полос, специальных сооружений и других)

8. Эксплуатационно-техническое обслуживание средств охраны и пожарно-технической продукции

(кто обслуживает: специалисты предприятия или подрядной специализированной организации)

8. Оценка антитеррористической защищенности

1. Определение требуемого уровня антитеррористической защищенности критических элементов объекта

№ п/п	Наименование критического элемента объекта	Категория критического элемента объекта по потенциальной опасности	Привлекательность для совершения террористического акта	Модель нарушителя	Требуемый уровень защищенности
1	2	3	4	5	6

2. Анализ выполнения задач физической защиты для обеспечения защищенности критических элементов объекта

№ п/п	Наименование критического элемента объекта	Организация охраны наблюдения	Рубежи обнаружения	Рубежи задержания	Условия доступа	Оценка выполнения задачи физической защиты
1	2	3	4	5	6	7

3. Оценка эффективности физической защиты критических элементов объекта

№ п/п	Наименование критического элемента объекта	Способ предотвращения террористического акта	Модель нарушителя	Оценка времени действий охраны, мин	Оценка времени действий нарушителя, мин	Вывод о выполнении задачи по пресечению террористического акта
1	2	3	4	5	6	7

4. Оценка достаточности мероприятий по защите критических элементов объекта

№ п/п	Наименование критического элемента объекта	Выполнение установленных требований	Выполнение задачи по физической защите	Выполнение задачи по предотвращению террористического акта	Вывод о достаточности мероприятий по защите	Компенсационные мероприятия
1	2	3	4	5	6	7

Условия возникновения и реализации террористических угроз и защиты от них описываются в терминах случайных процессов

Анализ результативности действий ФБР показал: риск ошибочных аналитических выводов из собранной оперативной информации и, как следствие, непринятия вовсе или принятия неадекватных мер противодействия выше 0.998 (!)

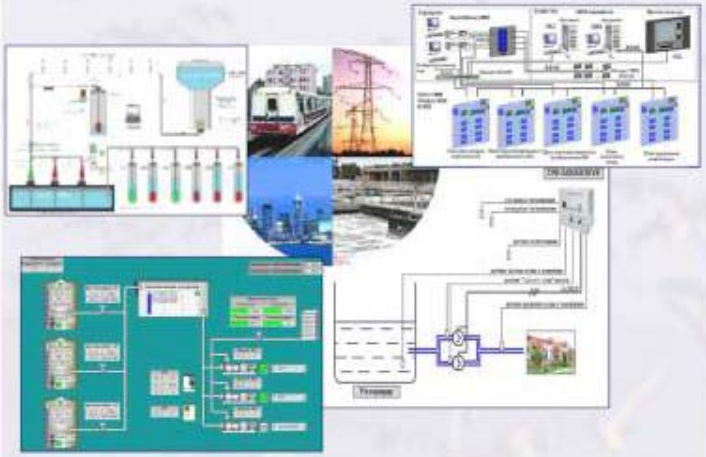
Вывод: ***превентивным образом предупредить сегодня реализацию террористических актов без целенаправленной работы по коренному снижению рисков практически невозможно. Необходима глубоко продуманная. Основой является МОДЕЛИРОВАНИЕ***

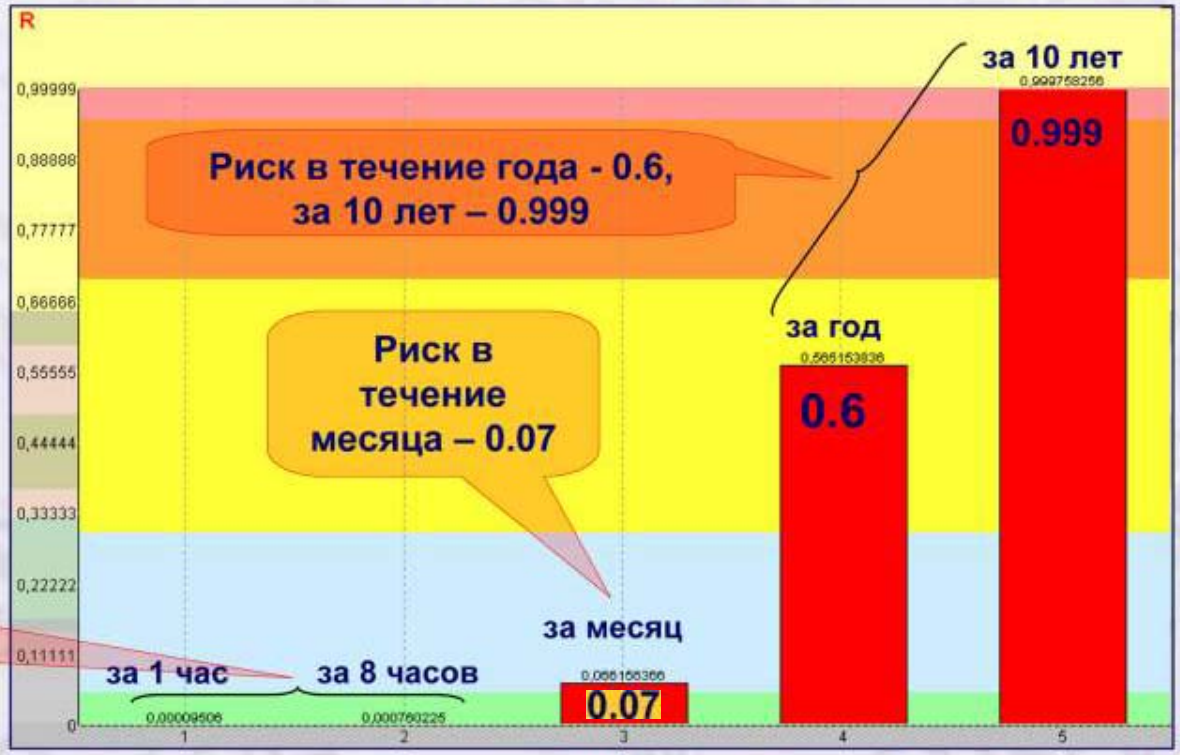
Примеры

Оценка риска неадекватной интерпретации событий диспетчером

за 1 час, 8 часов (одну смену), 1 месяц, 1 год и 10 лет функционирования SCADA-системы

<u>Исходные данные:</u> поток существенных событий - до 100 условных событий в час, содержащий не более 1% потенциально опасных событий. Скорость смысловой интерпретации события составляет около 30 секунд. Частота ошибок диспетчерского персонала и сбоев программно-технических средств SCADA-системы - 1 ошибка в год





Риск в течение 1 часа – не выше 0.0001, в течение рабочей смены диспетчера – 0.0008

Такие риски для SCADA –систем могут быть охарактеризованы как допустимые

Сравнение:
результаты моделирования способов совершенствования системы контроля Росрезерва

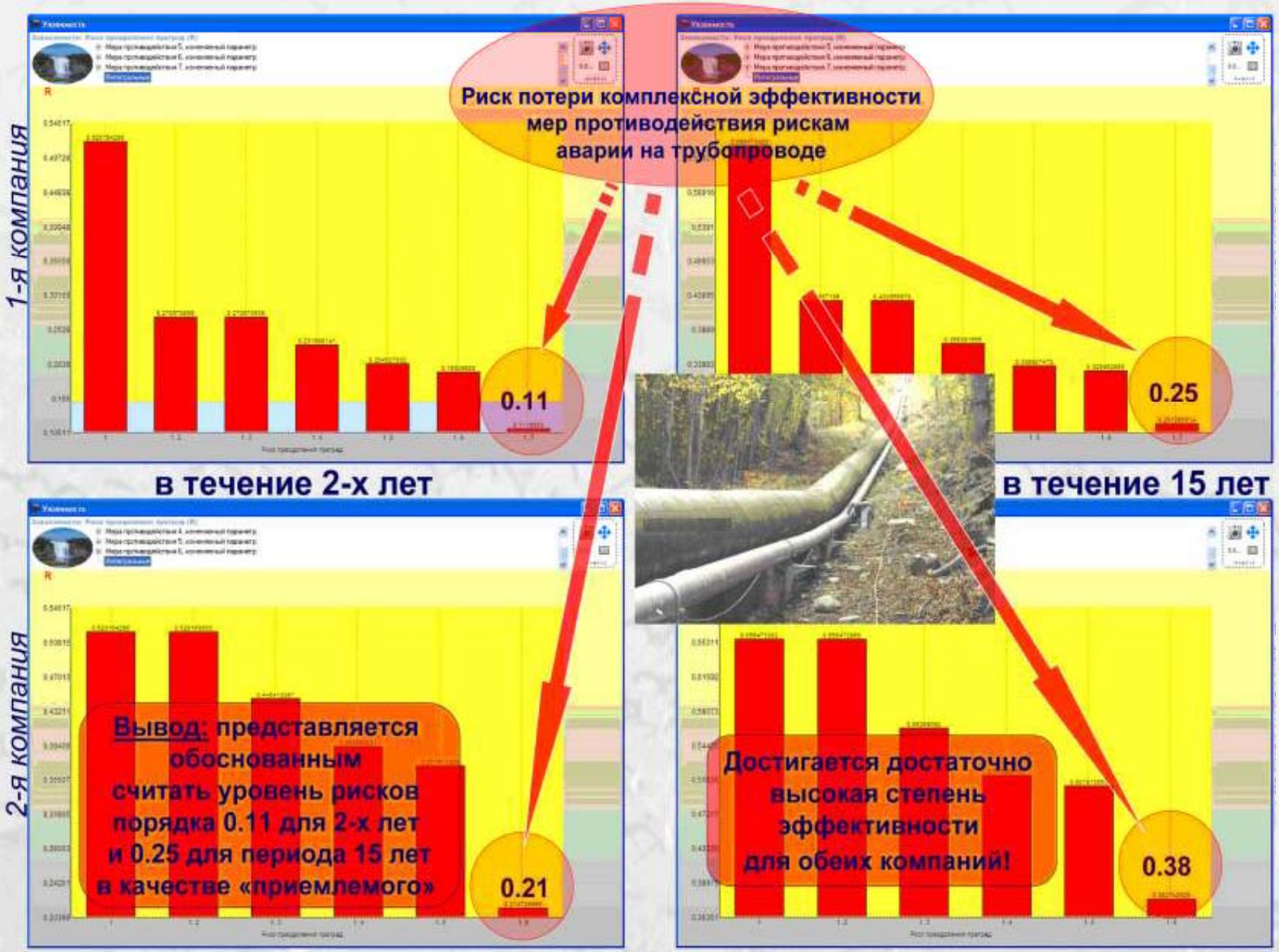
По результатам контроля качества производства, контроля доставки и входного контроля на комбинатах доля невыявленного брака сократилась в 100 раз и составляет 0.01% (!)

Результаты моделирования процессов освежения запасов

Вероятность сохранения качества запасов молока цельного сгущенного с сахаром при строгом соблюдении регламента равна 0.68, рыбных консервов - 0.67, мясных консервов - 0.65, бензина - 0.66, металлических конструкций - 0.64

При увеличении вдвое реального срока хранения качество хранимых резервов на момент выпуска повышается на 21%-23%

Прогноз эффективности мер противодействия рискам на 2 года и 15 лет при производстве трубопродукции в процессе эксплуатации трубопроводов



Исходные данные:

1-я мера – СМК на предприятии –поставщике с гарантией качества выпускаемой продукции в течение года и совершенствованием раз в 3 года;

2-я мера - проверка качества продукции всеми рекомендованными видами и методами неразрушающего контроля в течение года и совершенствованием раз в 3 года;

3-я мера – контрольная информация SCADA-системы, обновляющая данные 1 раз в минуту с техническим совершенствованием 1 раз в 5 лет;

4-я мера - дистанционное зондирование с сохранением эффективности в течение суток, осуществляемое раз в неделю;

5-я мера - ежегодные локальные инспекции с сохранением эффективности в течение месяца;

6-я мера - интегральные инспекции 1 раз в 5 лет с сохранением эффективности в течение месяца;

7-я мера - установки электрохимической защиты трубопроводов от коррозии и средства телемеха-ники трубопроводов с сохранением эффективности в течение года и обновлением 1 раз в 5 лет

1-я мера – СМК на предприятии –поставщике с гарантией качества выпускаемой продукции в течение года и совершенствованием раз в 3 года;

2-я мера – контрольная информация SCADA-системы, обновляющая текущие данные 1 раз в минуту с техническим совершенствованием 1 раз в 5 лет;

3-я мера – вертолетное обследование и регулярные рентгенографические методы анализа с сохранением эффективности в течение суток, осуществляемые раз в неделю;

4-я мера - ежегодные локальные инспекции с сохранением эффективности в течение месяца;

5-я мера - интегральные инспекции 1 раз в 5 лет с сохранением эффективности в течение месяца;

6-я мера - установки электрохимической защиты трубопроводов от коррозии и средства телемеханики трубопроводов с сохранением эффективности в течение года и обновлением 1 раз в 5 лет

Вводные понятия

Условное разделение систем инженерного обеспечения (СИО):

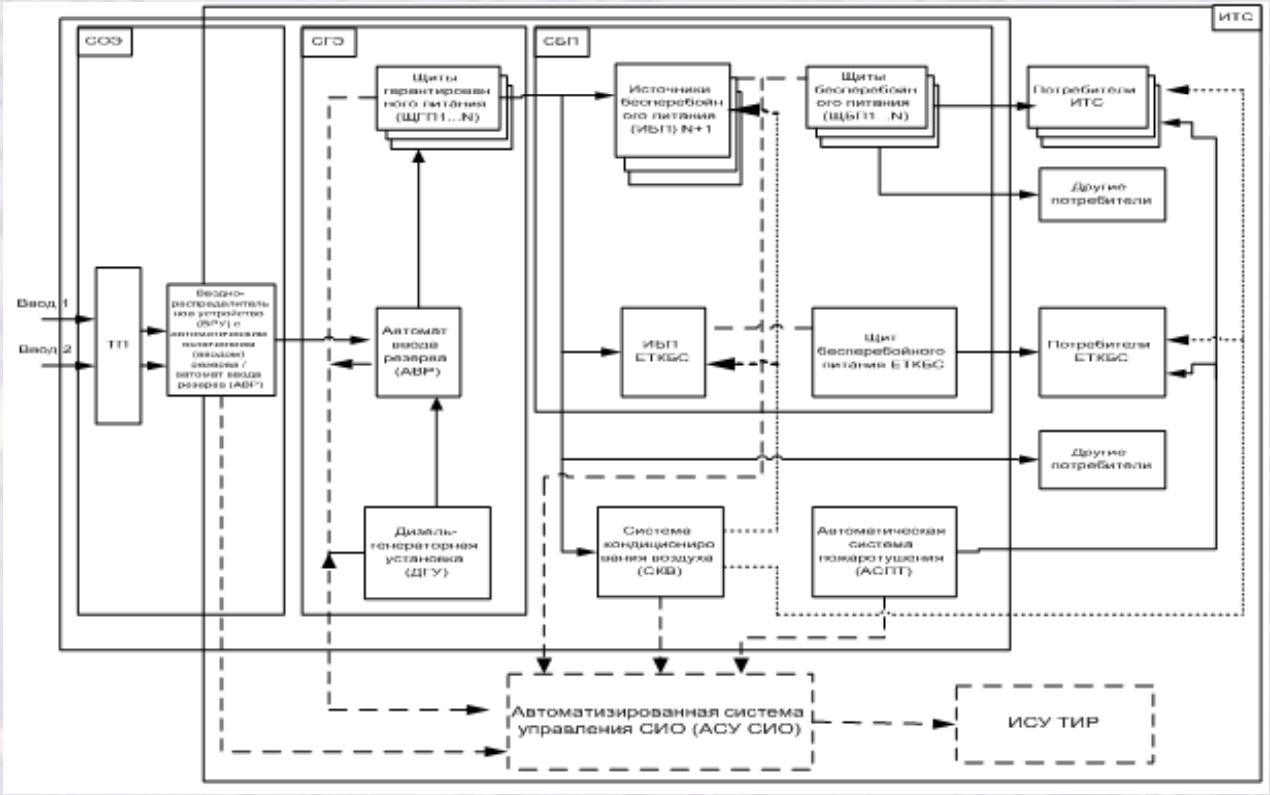
СИО, обеспечивающие условия функционирования информационно-телекоммуникационных систем (ИТС)

системы общего электроснабжения (СОЭ), гарантированного электроснабжения (СГЭ), бесперебойного электропитания (СБП), кондиционирования воздуха (СКВ), автоматического пожаротушения (САП или АСПТ) и др.

СИО, обеспечивающие условия жизнедеятельности персонала

системы электроснабжения общего назначения, водоснабжения и канализации, охранной сигнализации и контроля доступа, подъемных и лифтовых механизмов и др.

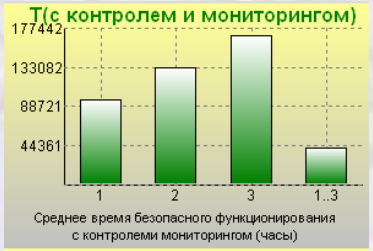
Структурная схема СИО ИТС



Оценка безопасности функционирования системы инженерного обеспечения

Наработка на безопасность

Разница несущественна - 1.3%. Это объясняется тем, что ИБП и ДГУ используются, главным образом, для кратковременного поддержания электропитания при выходе из строя основных средств

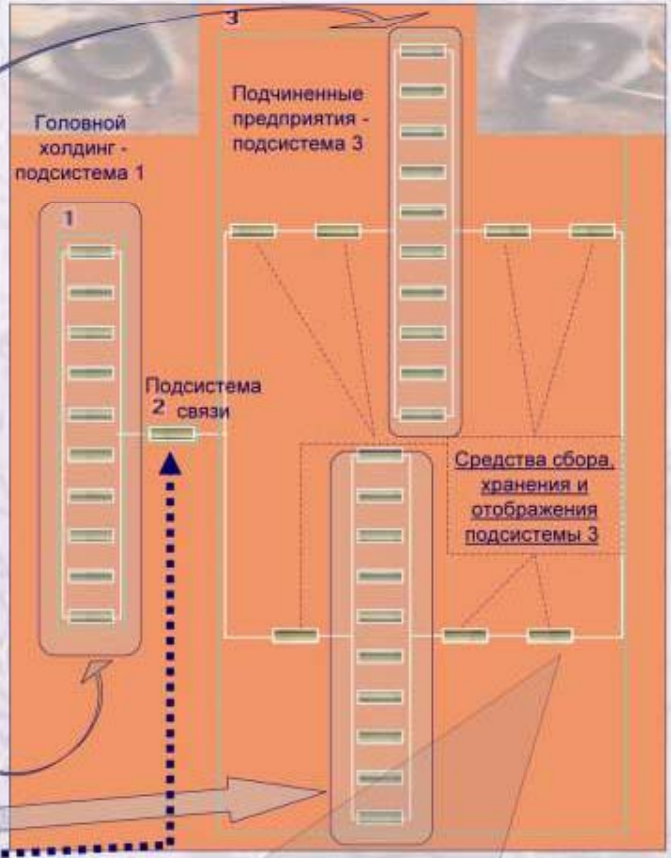


Анализ информационной безопасности - 1

Модель нарушителя и преграды НСД для системы сложной структуры

см. табл. 3.4.1 из примера 3.4.9

Преграда	Частота смены значения параметра преграды	Среднее время преодоления преграды нарушителем	Возможный способ преодоления преграды
1. Охраняемая территория со сменой охраны	через 2 часа	30 мин.	Скрытое проникновение на территорию
2. Пропускная система в здание, где располагается ИС и рабочие места пользователей со сменой службы контроля	через 1 сутки	10 мин.	Подделка документов, сговор, обман
3. Электронный ключ для включения компьютера	через 5 лет (наработка до замены)	1 неделя	Кража, принудительное изъятие ключа, сговор
4. Пароль для входа в систему	через 1 мес.	1 мес.	Подсматривание, принудительное выпытывание, сговор, подбор пароля
5. Пароль для доступа к программным средствам	через 1 мес.	10 суток	—□□—
6. Пароль для доступа к требуемой информации	через 1 мес.	10 суток	—□□—
7. Зарегистрированный внешний носитель информации для записи	через 1 год	1 сутки	Кража, принудительная регистрация, сговор
8. Подтверждение подлинности пользователя в процессе сеанса	через 1 мес.	1 сутки	Подсматривание, принудительное выпытывание, сговор
9. Телемониторинг помещений	через 5 лет (наработка до замены)	2 суток	Имитация неисправности, ложные ролики, маскировка под персонал, сговор
10. Шифрование информации со сменой ключей	через 1 мес.	2 года	Расшифровка, сговор



Системные данные

Время восстановления (среднее)	0,5	часы
Длительность периода	1	месяцы
Частота возникновения угроз	1	раз в час

Характеристики средств сбора, хранения и отображения данных

Стойкость меры (компонента) в условиях реализации угроз	2	годы
Наработка на ошибку средств мониторинга (без мониторинга = 1 мсек.)	1	мсек.
Период между системными контролями целостности	1	месяцы

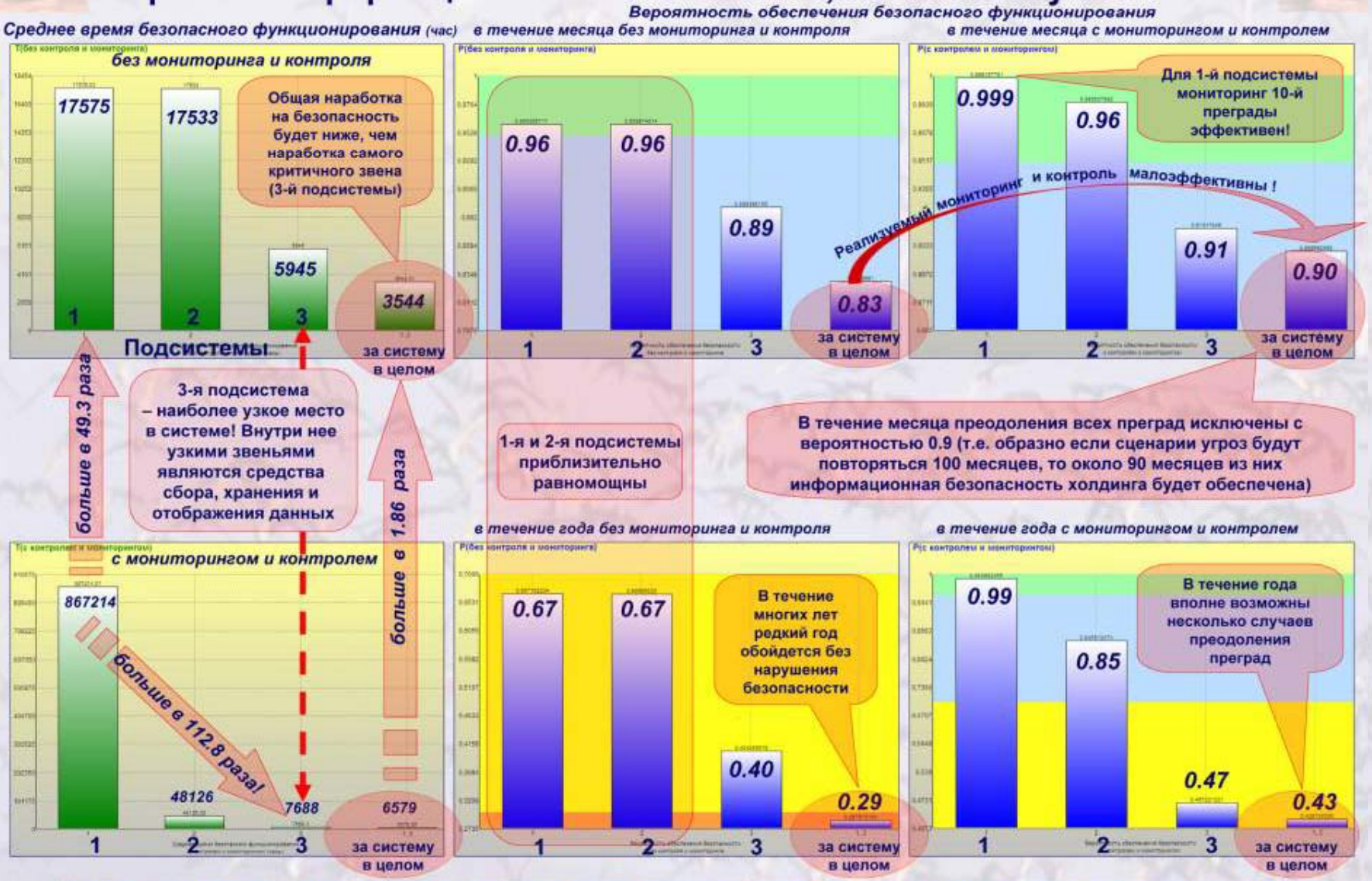
Характеристики подсистемы связи

Стойкость меры (компонента) в условиях реализации угроз	2	годы
Наработка на ошибку средств мониторинга (без мониторинга = 1 мсек.)	1	месяцы
Период между системными контролями целостности	1	месяцы

Требуется количественно спрогнозировать на месяц и год уровень информационной безопасности и выявить узкие места. Используется комплекс *«АНАЛИЗ БЕЗОПАСНОСТИ»*©

Анализ информационной безопасности - 3

Прогноз информационной безопасности, выявление узких мест



Для безопасного функционирования системы в целом целесообразно, чтобы все подсистемы были равнопрочны. В исследуемом примере реализуемые мониторинг и контроль малоэффективны. Необходима технология обеспечения информационной безопасности в экстренных случаях, когда штатная технология выводится из строя

Достижение уровней совершенства для традиционного и инновационного подходов

Что сегодня на практике оценивается для информационных систем?

Качество используемой информации количественно НЕ оценивается (!), что не отвечает системному подходу

Инновационный подход к управлению качеством и рисками в жизненном цикле систем

Что достижимо при традиционном подходе ?

Не оценены количественно риски (в т.ч. приемлемые), степени уязвимости систем, зависимости достигаемой безопасности от моделей нарушителей. Нет возможностей для решения обратных задач оптимизации усилий и затрат!

Что достижимо при предлагаемом подходе ?

А. И. Костогрызов, Г.А. Нистратов

СТАНДАРТИЗАЦИЯ, МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, РАЦИОНАЛЬНОЕ УПРАВЛЕНИЕ И СЕРТИФИКАЦИЯ

в области системной и программной инженерии

СТАНДАРТИЗАЦИЯ, МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, РАЦИОНАЛЬНОЕ УПРАВЛЕНИЕ И СЕРТИФИКАЦИЯ

Более 70 практических примеров управления качеством и рисками для информационных, промышленных, транспортных, нефтегазовых систем, анализ «человеческого фактора» и др.

ГРИГОРЬЕВ ЛЕОНИД ИВАНОВИЧ
доктор технических наук, профессор. Заведующий кафедрой "Автоматизированные системы управления" РГУ нефти и газа им. И.М.Губкина. Почетный работник газовой промышленности, высшего профессионального образования, топливно-энергетического комплекса России

КЕРШЕНБАУМ ВСЕВОЛОД ЯКОВЛЕВИЧ
заслуженный деятель науки РФ, доктор технических наук, профессор. Генеральный директор Национального института нефти и газа, заведующий кафедрой «Управление качеством, стандартизация и сертификация» РГУ нефти и газа им. И.М.Губкина. Вице-президент Российской инженерной академии, лауреат Премии Правительства России

КОСТОГРЫЗОВ АНДРЕЙ ИВАНОВИЧ
заслуженный деятель науки РФ, доктор технических наук, профессор. Генеральный директор Центра стандартизации, проектирования и разработки информационно-коммуникационных технологий и систем, научный руководитель НИИ прикладной математики и сертификации

СИСТЕМНЫЕ ОСНОВЫ УПРАВЛЕНИЯ КОНКУРЕНТОСПОСОБНОСТЬЮ В НЕФТЕГАЗОВОМ КОМПЛЕКСЕ

Л.И. ГРИГОРЬЕВ, В.Я. КЕРШЕНБАУМ, А.И. КОСТОГРЫЗОВ

СИСТЕМНЫЕ ОСНОВЫ УПРАВЛЕНИЯ КОНКУРЕНТОСПОСОБНОСТЬЮ В НЕФТЕГАЗОВОМ КОМПЛЕКСЕ

Москва-2010

ПРЕДЛАГАЕТСЯ:

► поставка, наладка, адаптация, разработка на заказ и сопровождение программных инструментариев и информационных технологий, выполнение НИОКР

► разработка на заказ баз знаний, методов и программных инструментариев для ситуационных центров, систем поддержки принятия решений

► количественное обоснование технического облика сложных комплексов и системных требований к характеристикам составных компонентов, планируемым технологиям и квалификации работников, разработка проектов технических заданий

► независимая оценка выполнимости системных требований, количественная экспертиза эффективности технических решений по проектированию систем, выявление «узких мест» на всех этапах жизненного цикла

► математическое моделирование процессов в различных сценариях потенциальных угроз, сравнение вариантов защиты по критериям «эффективность - стоимость»

► разработка методик, поддерживающих программных инструментариев, анализ рисков (технологических, информационных, организационно-производственных, связанных с человеческим фактором, политических, финансово-экономических, террористических и др.), оценка качества и безопасности, в т.ч. в процессе испытаний и эксплуатации

► обоснование эксплуатационных условий эффективного использования систем и рациональных значений настраиваемых параметров

► обучение системным основам управления качеством, рисками, конкурентоспособностью