09 декабря 2010, Санкт-Петербург

Системный прогноз качества и рисков. Технология «Прикоснись и моделируй»

Костогрызов А.И.

www.mathmodels.net

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

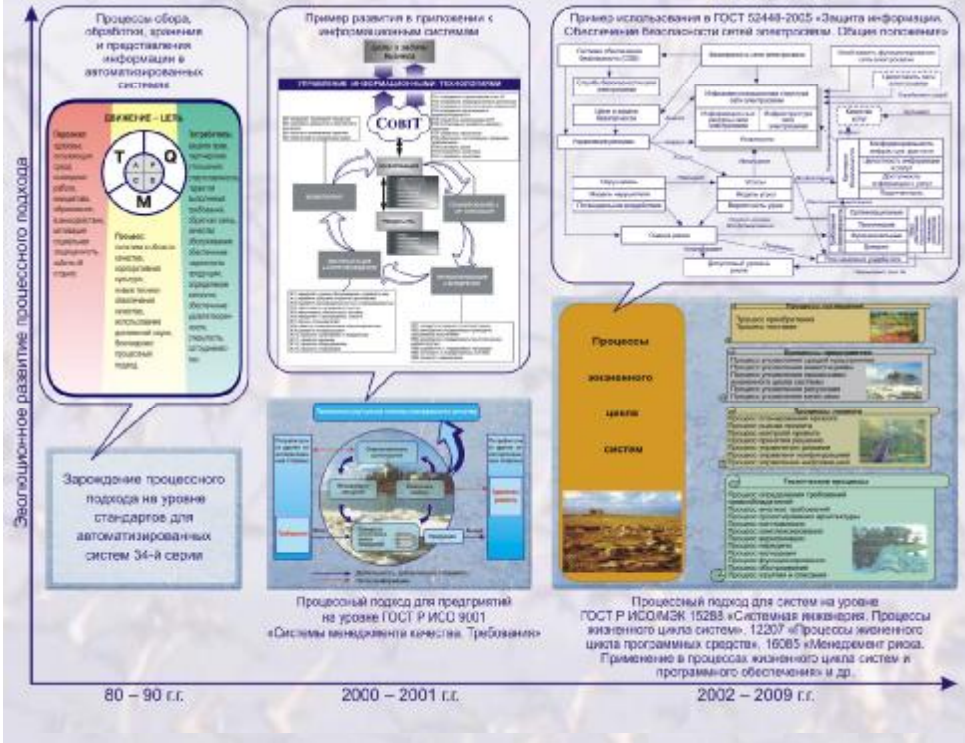
В чем суть основных системных изменений?

- 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

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



- 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!

Общее

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)

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

Пример формализации

Построение и развитие сложных систем базируется на системном анализе

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

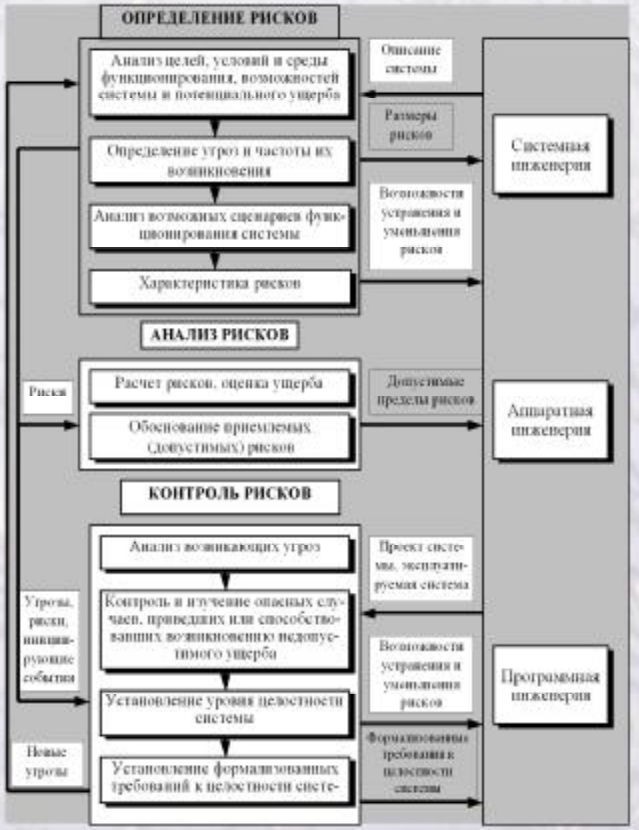
Транспортная безопасность

Авиационная безопасность

Безопасность высотных зданий

Информационная безопасность

и др.



4. **Существующие модели** для анализа рисков в приложении к rприродным 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

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)

Предлагается

Технология «Прикоснись и моделируй»

применяется с 2010г.

- в Институте проблем информатики РАН, НИИ прикладной математики и сертификации, Центре стандартизации, проектирования и разработки информационно-коммуникационных технологий и систем, НИИ Минобороны, РГУ нефти и газа, ОАО «Газавтоматика», Курском и Самарском госуниверситетах и др.

- в Федеральном агенстве по государственным резервам

- в Банке РФ (для оценки эффективности системы инженерного обеспечения)

- в Министерстве информационных технологий и связи Московской области

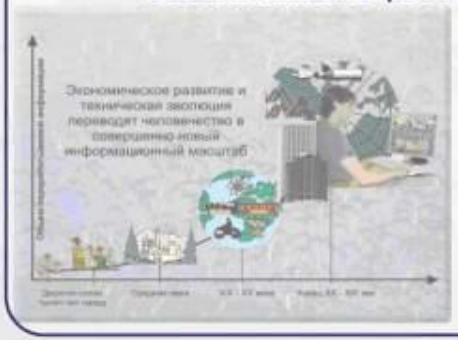
- в Сибирской угольной энергетической компании

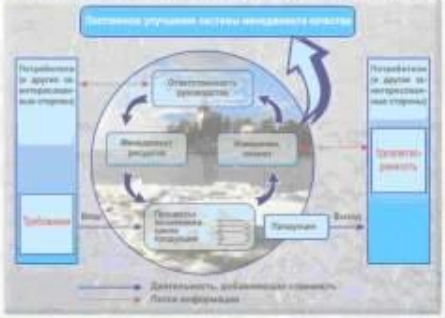
- на месторождении «Заполярное» (ОАО Газпром)

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)

Развитие математических моделей для оценки качества и рисков в соответствии с требованиями системообразующих стандартов

МОНОГРАФИИ

СТАТЬИ И ДОКЛАДЫ НА НАУЧНО-ТЕХНИЧЕСКИХ ФОРУМАХ

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.:

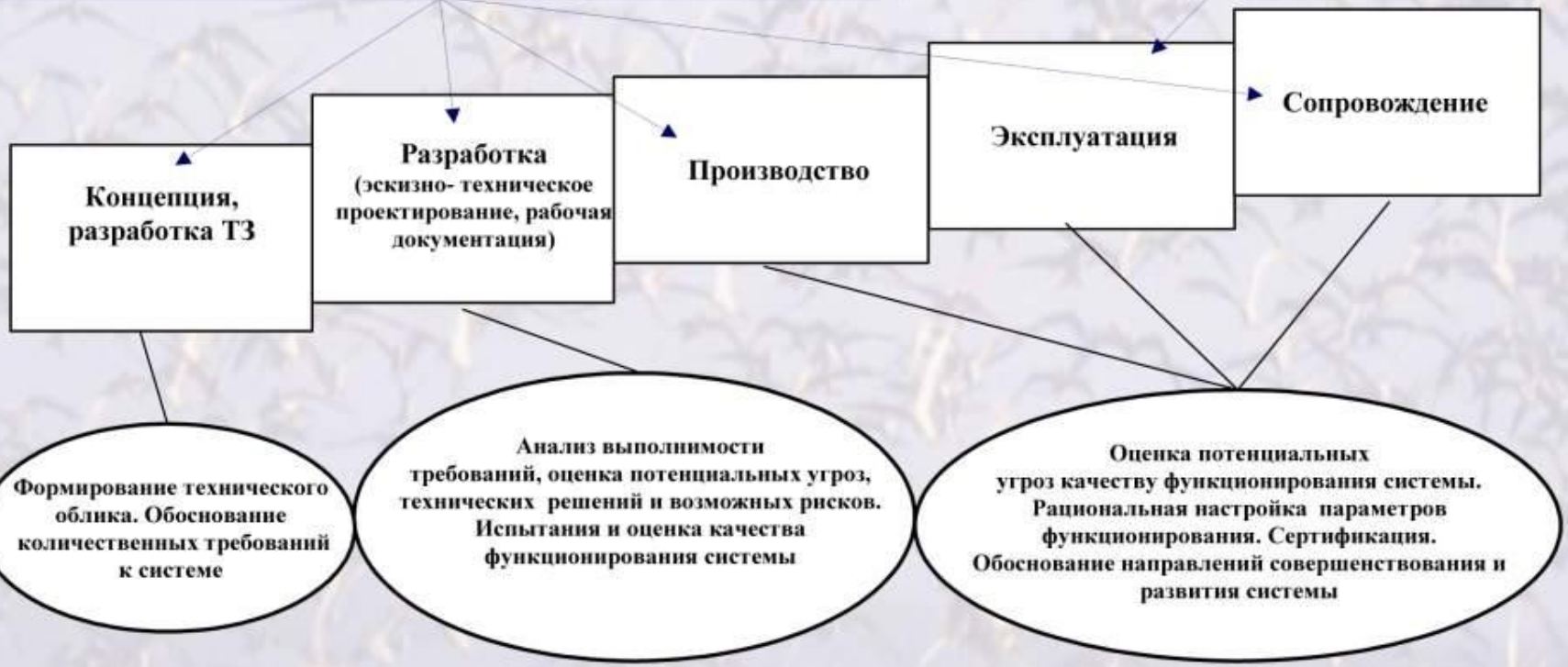
$$Z_{созд.}(Q_{рац.}) = \min_{\text{управляемые параметры A,M}} Z_{созд.}(Q)$$

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.:

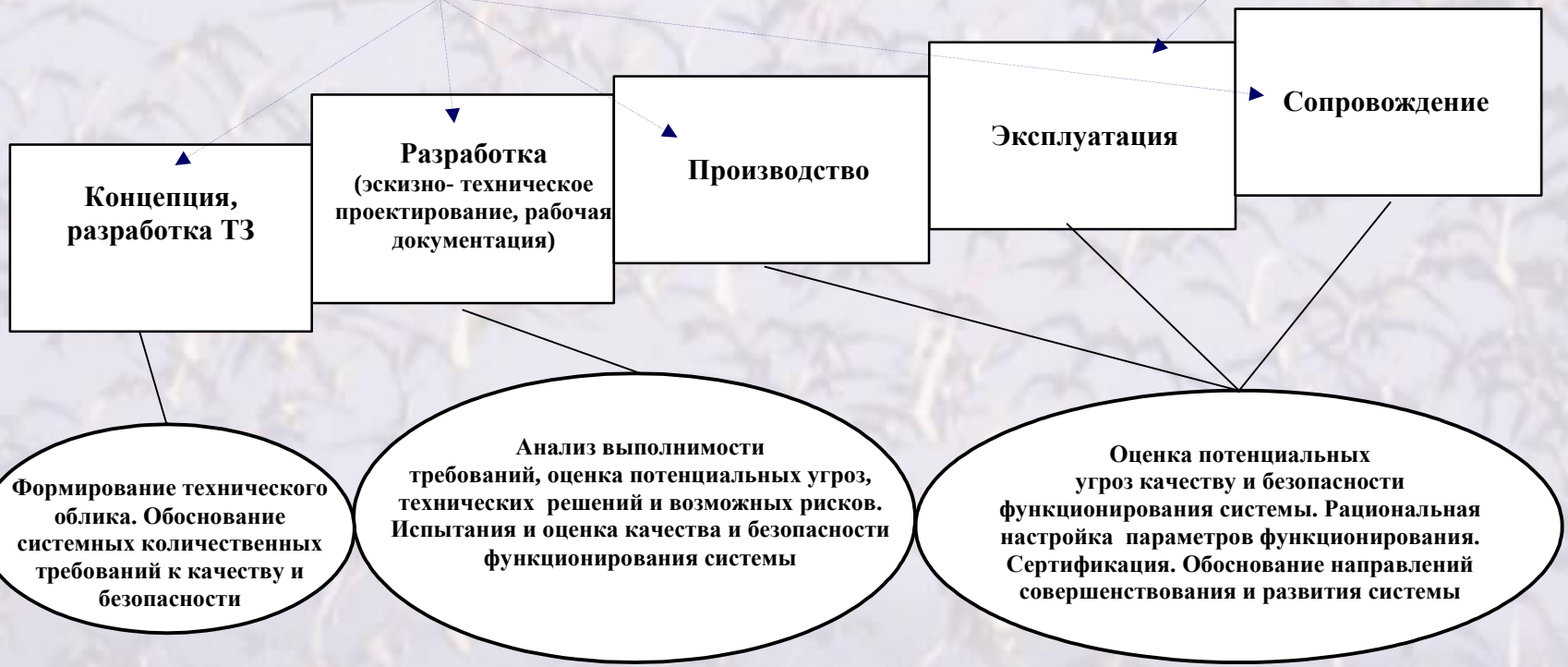
$$Z_{созд.}(Q_{рац.}) = \min_{\text{управляемые параметры A,M}} Z_{созд.}(Q)$$

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



Контроль и оптимизация

Место и суть виртуального моделирования 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-листовый 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

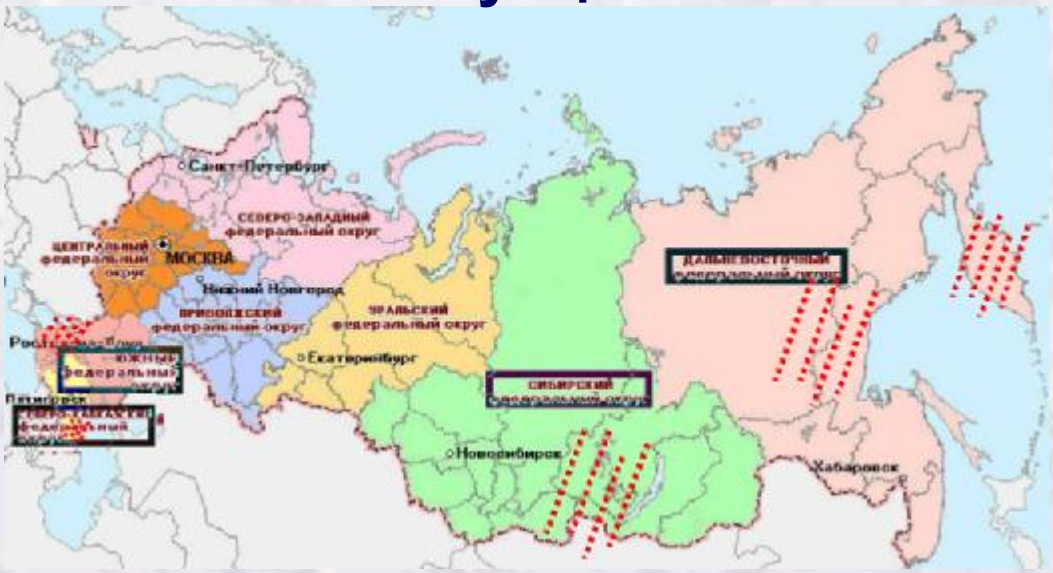
Итог

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)

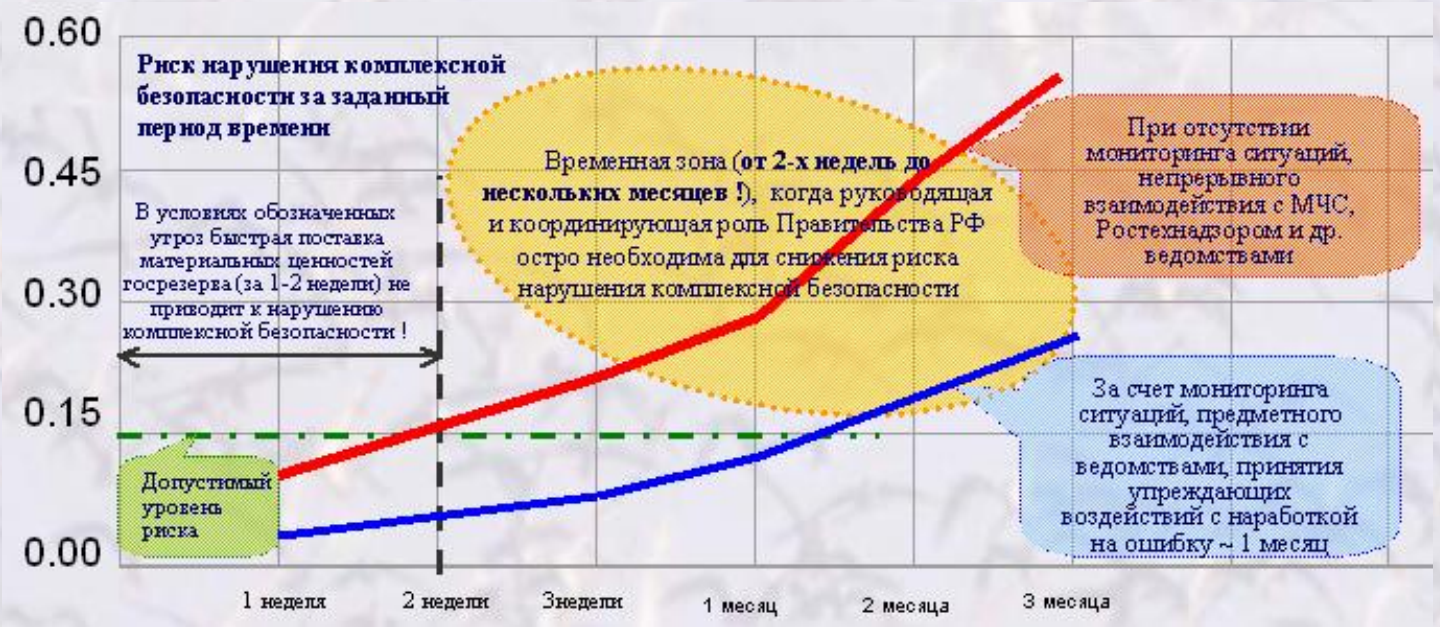
Примеры

Прогноз риска нарушения комплексной безопасности в условиях чрезвычайных ситуаций

«Прикоснись»



«Моделируй»



Методический подход к оценке рисков в опасном производстве

Руководством должны осуществляться:

целенаправленный сбор и обработка оперативной информации

мониторинг и контроль ситуации

реализация мер противодействия рискам для всех идентифицированных типов опасностей

Последовательность методических шагов

1. Анализ частного риска неполучения необходимой информации на момент принятия решения – R1
2. Анализ частного риска нераспознавания потенциальной опасности в режиме реального времени – R2
3. Анализ частного риска неконтролируемого развития критичных ситуаций в течение задаваемого периода времени – R3
4. Анализ частного риска возникновения аварийной ситуации в течение задаваемого периода времени вопреки принятым мерам противодействия – R4

5. Анализ интегрального риска аварии в течение задаваемого периода времени – R5

Изначальные положения для создания методики:

в силу случайного характера влияние опасных факторов и условий описывается в терминах случайных ...

применяемые способы снижения опасности направлены на своевременное вскрытие опасности, устранение или замедление ее развития и снижение ущербов;

средства, технологии и меры противодействия рискам с формальной точки зрения представляют собой последовательность защитных преград развитию аварийных ситуаций. Чем они эффективнее, тем меньше риск аварии и размеры возможных ущербов

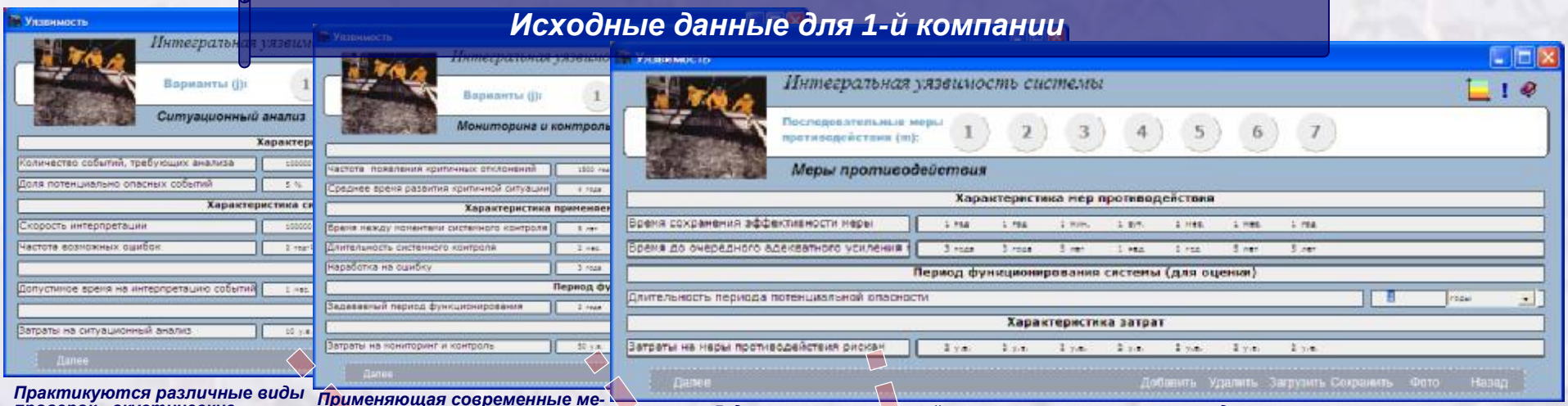
$$R_5 = 1 - [(1- R_{21})\,(1- R_{31})(1- R_{41})] \ldots [(1- R_{2i})\,(1- R_{3i})(1- R_{4i})] \ldots,\ i=1,\ldots,I,$$

I – количество составных участков объекта,
если детализации до отдельных участков не производится, то I=1

Существующие модели и программные инструментарии для расчетов

Интегральная оценка рисков, затрат и математического ожидания ущербов

Исходные данные для 1-й компании



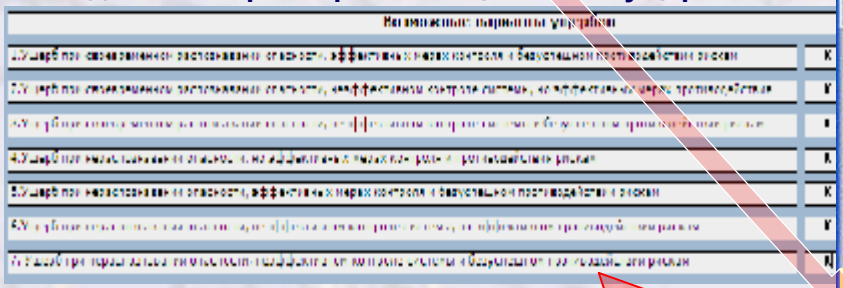
Практикуются различные виды проверок - акустические, магнитные, оптические, с проникающими веществами, радиационные, радиоволновые, тепловые и электромагнитные

Применяющая современные методы мониторинга и контроля, включая комбинацию дистанционного зондирования интегральных и локальных методов инспекции, методов внутритрубной инспекции

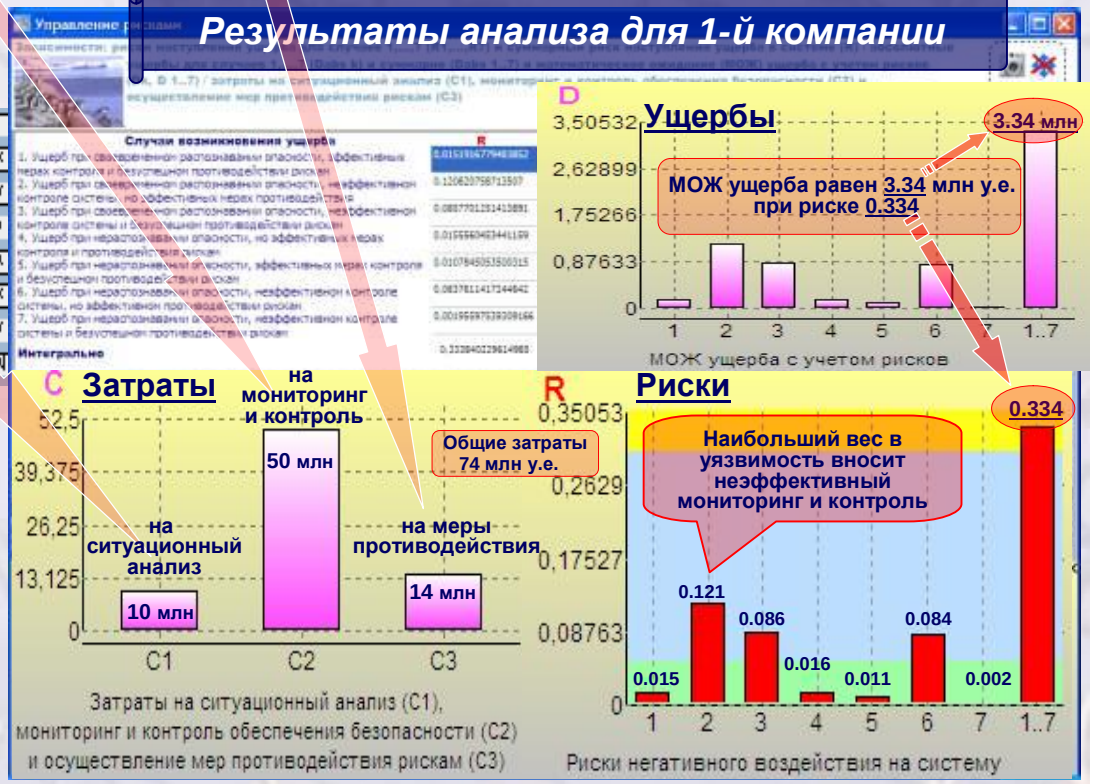
В дополнение к мерам 2-й компании применяются методы неразрушающего контроля и дистанционное зондирование (космический мониторинг и авиационная съемка)

Результаты анализа для 1-й компании

Задаваемые размеры потенциальных ущербов

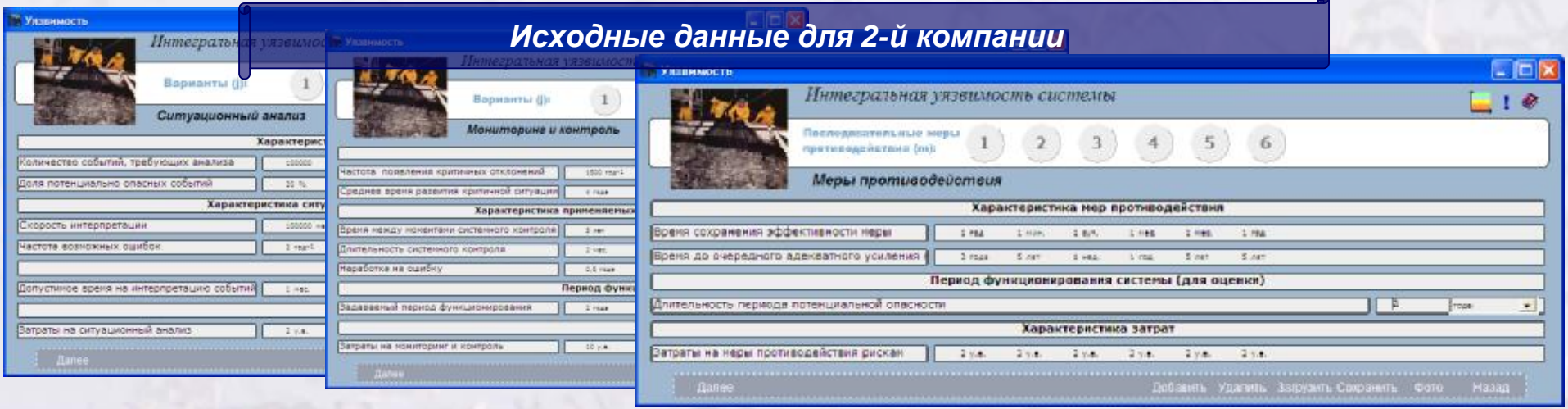


Полное множество вариантов возникновения возможных ущербов из-за неэффективного ситуационного анализа и/или мониторинга и контроля и/или мер противодействия

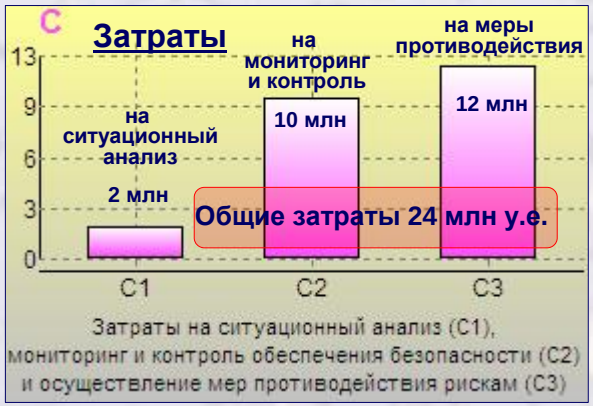


Интегральная оценка рисков, затрат и математического ожидания ущербов

Исходные данные для 2-й компании



Результаты анализа для 2-й компании



Окончательный вывод:

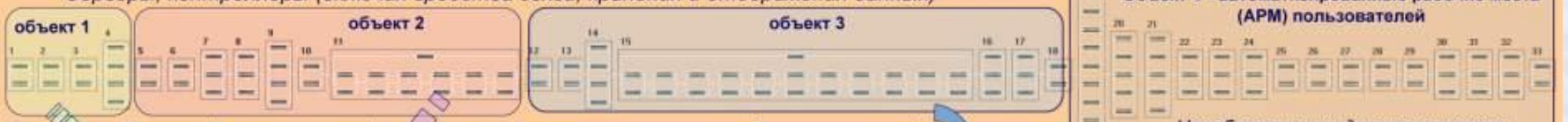
Несмотря на существенно меньшие расходы 2-й компании МОЖ ущерба 9.92 млн у.е. в три раза превышает МОЖ ущерба 1-й компании. Риск 0.992 свидетельствует о неизбежности реализации потенциальных угроз, что отрицательно скажется на качестве и конкурентоспособности продукции и услуг компании, т.е. техническая политика 2-й компании неэффективна.

Для 1-й компании суммарные затраты на ситуационный анализ, мониторинг, контроль и меры противодействия рискам равны 74 млн у.е., риск негативного воздействия на компанию за 2 года равен 0.334, а МОЖ ущерба – 3.34 млн у.е. Такой риск может восприниматься как ориентир эффективной технической политики

Анализ качества - 1

Логическая структура системы для расчетов с использованием модели «Анализ проекта архитектурного построения системы» комплекса «ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ»

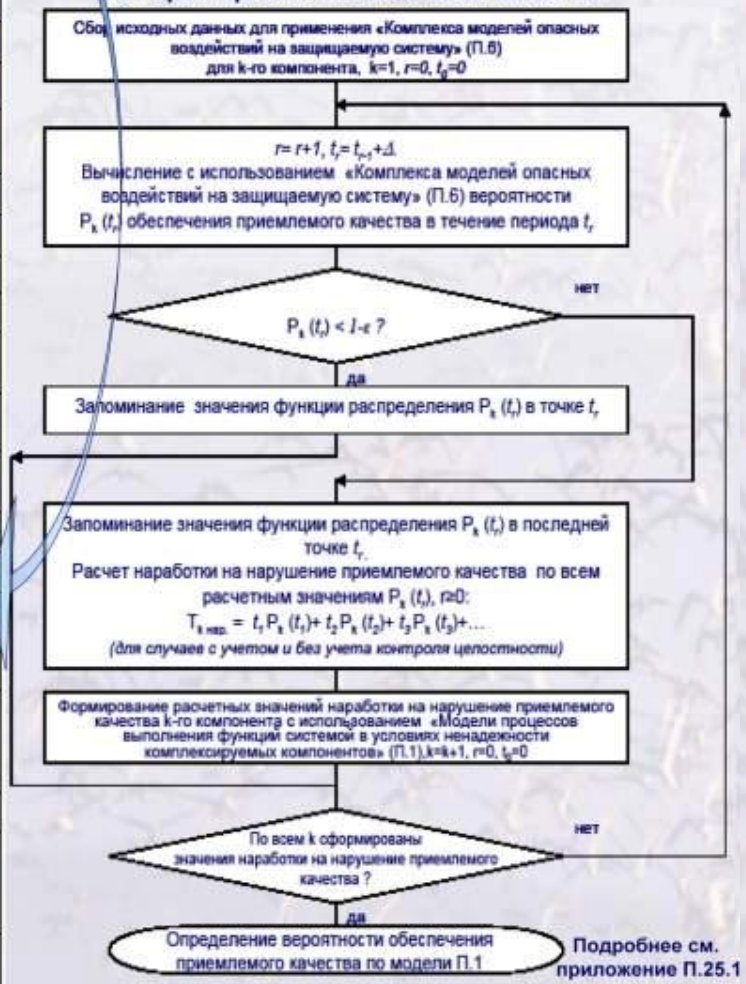
Серверы, контроллеры (включая средства связи, хранения и отображения данных)



Исходные данные для расчетов (ежемесячный контроль с техн. обслуживанием)

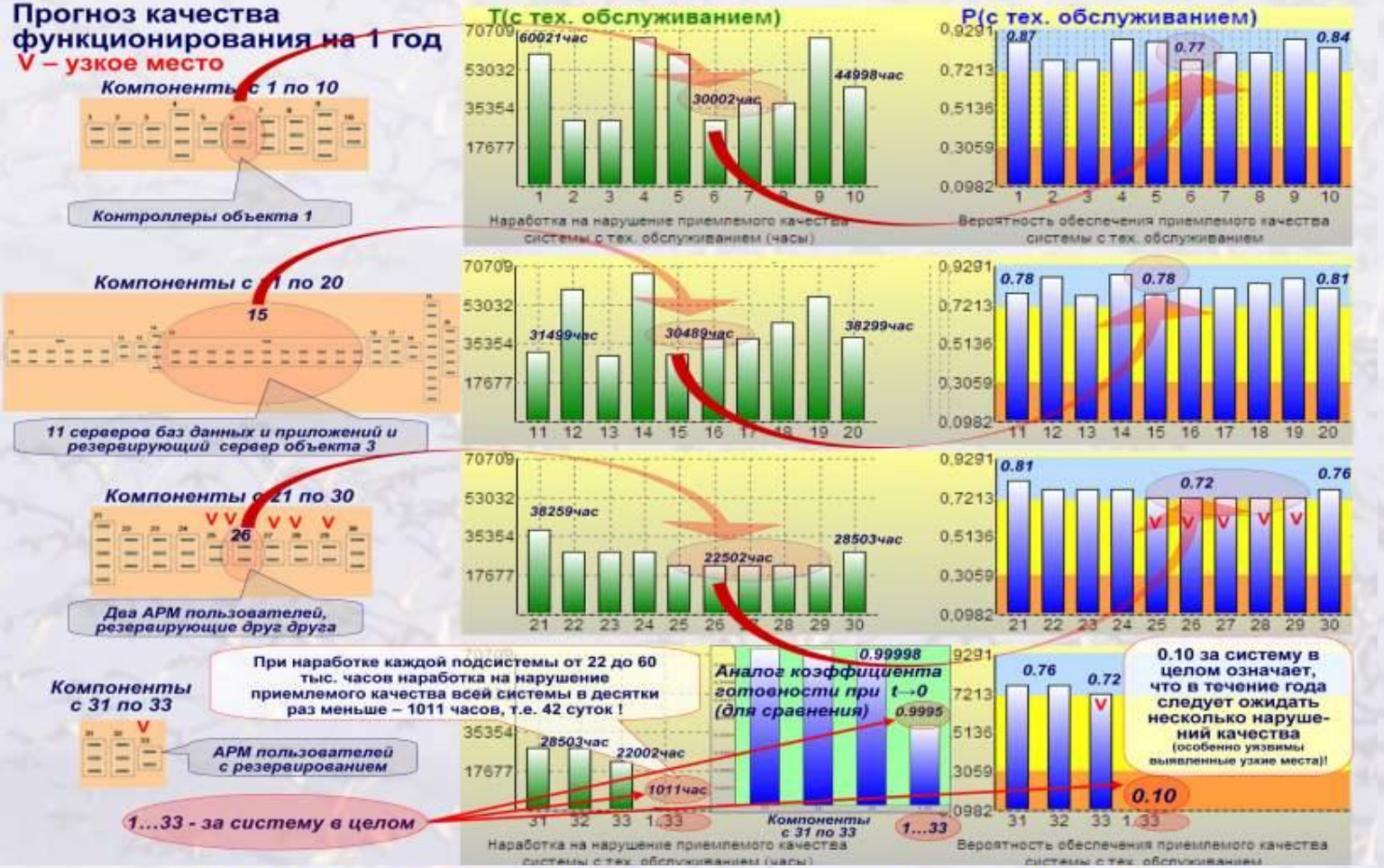
Сервер	Блок	Подсистема в схеме	Наработка на ухудшение качества*, час
Главный сервер объекта 1	Узел 1 кластера главного сервера Резервирующий узел 2	1 1	40000 каждый
Контроллер	Контроллер 1 Резервирующий контроллер 2	2 2	20000 каждый
Сервер терминального доступа	Сервер терминального доступа 1 Резервирующий сервер	3 3	20000 каждый
Сервер системы управления	Узел 1 кластера сервера системы управления Резервирующие узлы 2,3,4	4 4	30000 каждый
Главный сервер объекта 2	Узел 1 кластера главного сервера Резервирующий узел 2	5 5	40000 каждый
Контроллер	Контроллер 1 Резервирующий контроллер 2	6 6	20000 каждый
Серверы терминального доступа объекта 21	Основной и резервирующие серверы 1-3	7	20000
Серверы терминального доступа объекта 22	Основной и резервирующие серверы 1-3	8	20000
Серверы системы управления	Узел 1 кластера сервера системы управления Резервирующие узлы 2,3,4	9 9	30000 каждый
Сервер документооборота	Узел 1 кластера сервера документооборота Резервирующий узел 2	10 10	30000 каждый
6 серверов баз данных и приложений	Узел 1 кластера каждого сервера баз данных и приложений Резервирующий узел 2	11 11	30000 каждый
Резервирующий сервер баз данных и приложений	Резервирующий сервер	11	30000
Главный сервер объекта 3	Узел 1 кластера главного сервера Резервирующий узел 2	12 12	40000 каждый
Контроллер	Контроллер 1 Резервирующий контроллер 2	13 13	20000 каждый
Сервер системы управления	Узел 1 кластера сервера системы управления Резервирующие узлы 2,3,4	14 14	30000 каждый
11 серверов баз данных и приложений Резервирующий сервер баз данных и приложений	Узел 1 кластера каждого сервера баз данных и приложений Резервирующий узел 2 Резервирующий сервер	15 15 15	30000 каждый
Серверы терминального доступа объекта 31	Основной и резервирующие серверы 1-3	16	20000
Серверы терминального доступа объекта 32	Основной и резервирующие серверы 1-3	17	20000 каждый
Сервер терминального доступа 4	Сервер терминального доступа 4	17	
Сервер терминального доступа 5	Сервер терминального доступа 5	17	
Сервер терминального доступа 6	Сервер терминального доступа 6	17	
Сервер документооборота	Узел 1 кластера сервера документооборота Резервирующий узел 2	18 18	30000 каждый

Алгоритм расчета показателей качества



Подробнее см. приложение П.25.1

Анализ качества - 2



Узкие места в результате прогнозирования качества

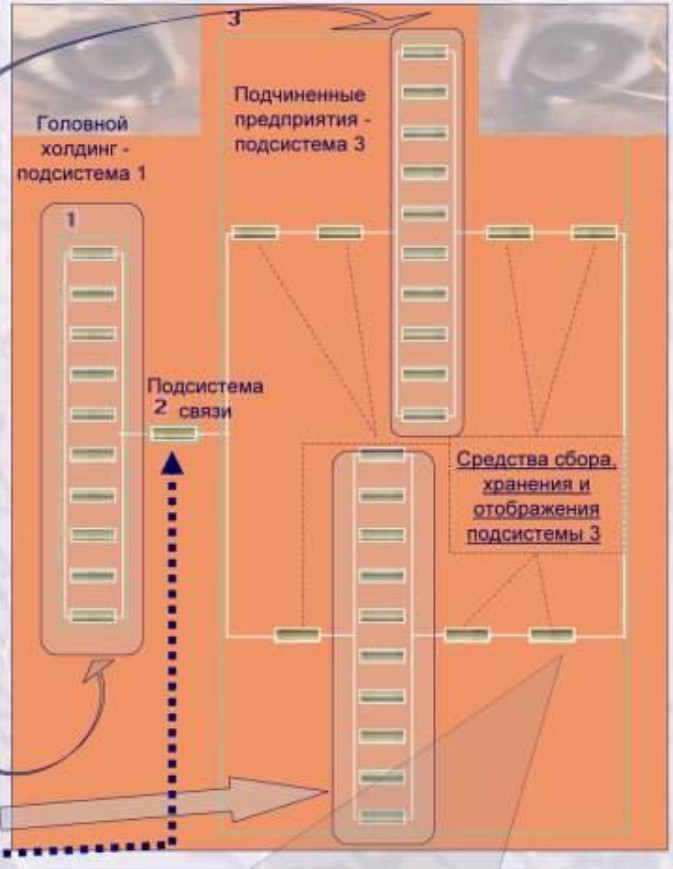
Особенно уязвимые компоненты системы – АРМ пользователей с двукратным резервированием. Риск потери качества в подсистемах 25-29, 33 на 16.7% - 21.5% выше, чем для остальных подсистем

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

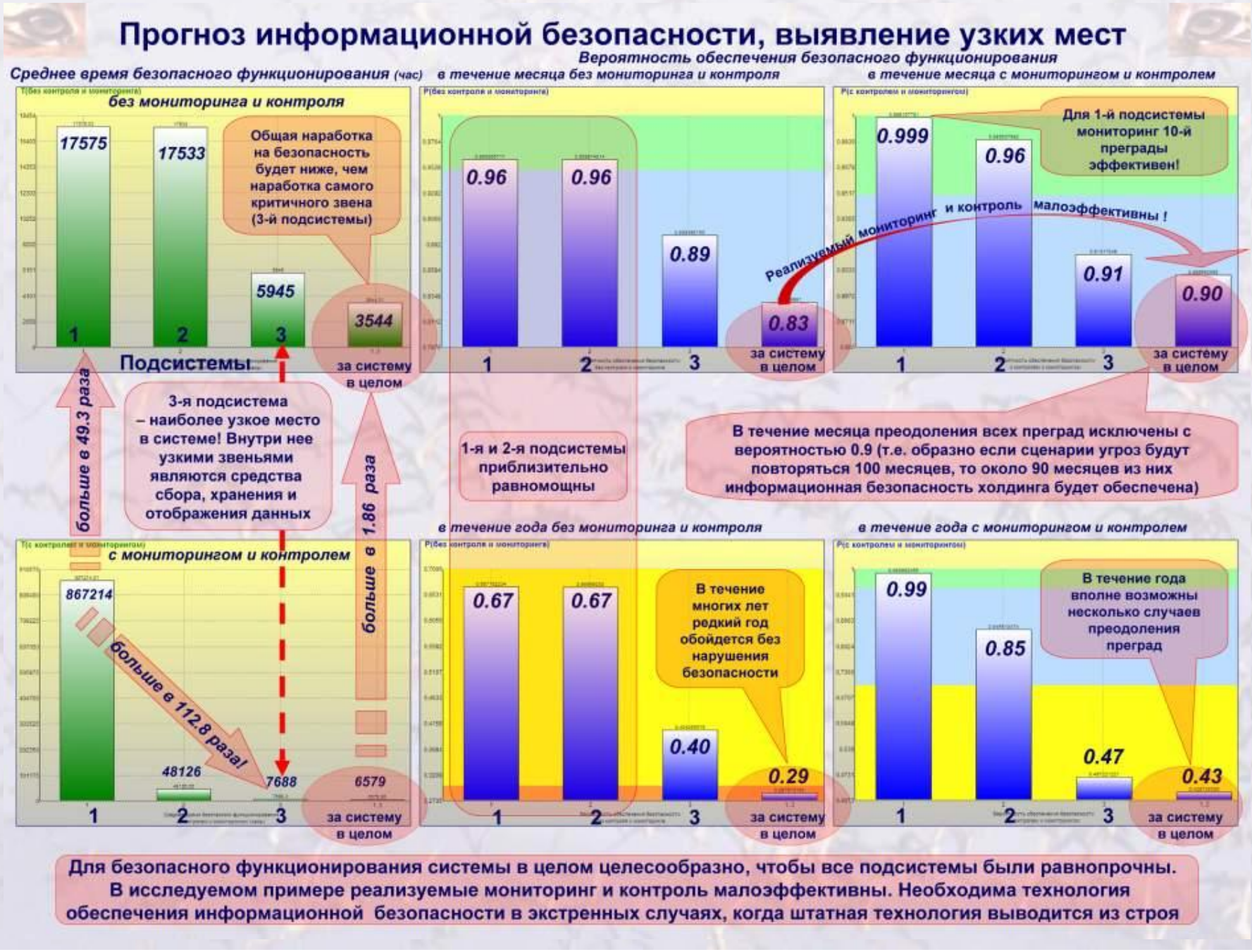
Стойкость меры (компонента) в условиях реализации угроз	2	годы
Наработка на ошибку средств мониторинга (без мониторинга = 1 мсек.)	1	мсек.
Период между системными контролями целостности	1	месяцы

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

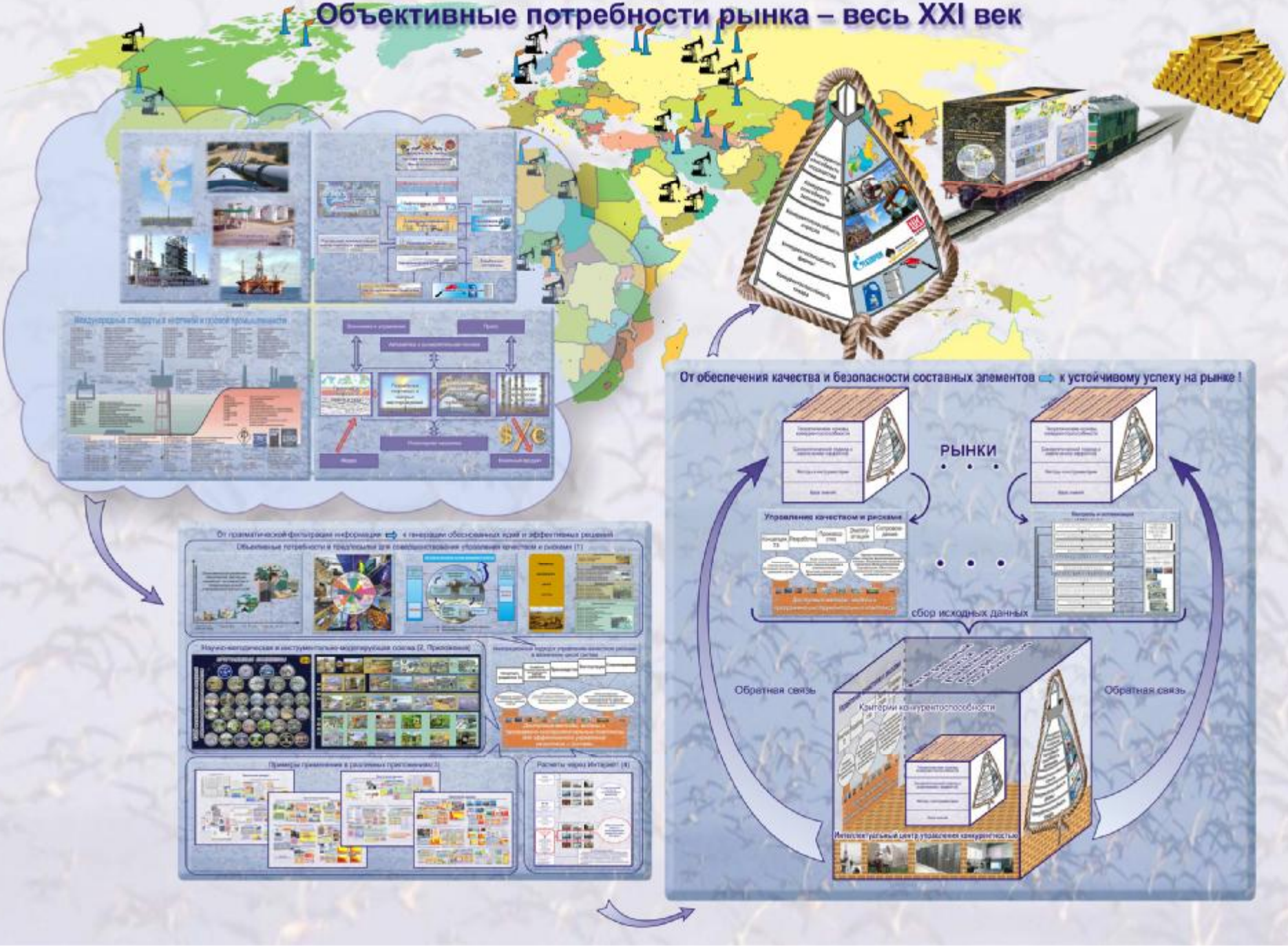
Требуется количественно спрогнозировать на месяц и год уровень информационной безопасности и выявить узкие места. Используется комплекс *«АНАЛИЗ БЕЗОПАСНОСТИ»*©

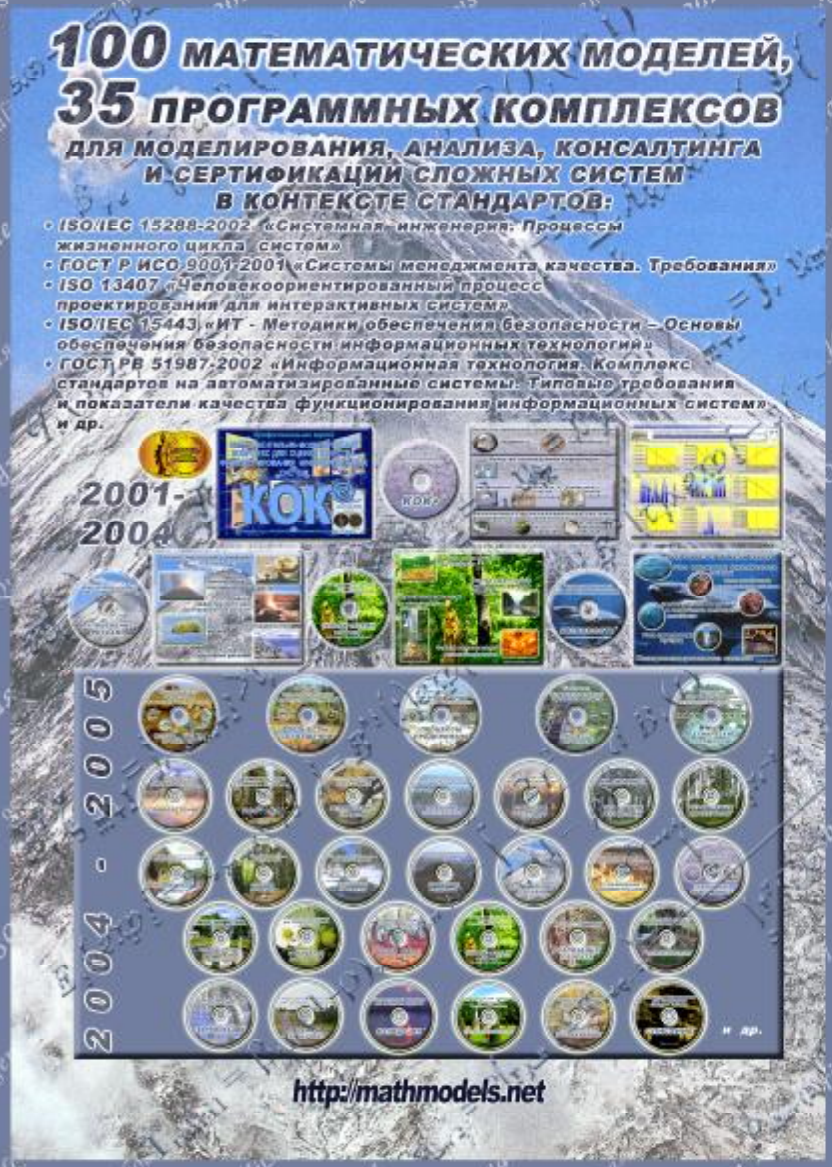
Анализ информационной безопасности - 2



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

Объективные потребности рынка – весь XXI век





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.

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

СИСТЕМНЫЕ ОСНОВЫ УПРАВЛЕНИЯ КОНКУРЕНТОСПОСОБНОСТЬЮ В НЕФТЕГАЗОВОМ КОМПЛЕКСЕ

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

Москва-2010