

*Международная конференции «Эффективные технологии управления производством»
22 октября 2009г.*

ИННОВАЦИОННОЕ УПРАВЛЕНИЕ КАЧЕСТВОМ И РИСКАМИ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ

(современные стандарты системной инженерии, математические модели и методы анализа системных процессов, доступный прогноз качества и рисков, в т.ч. через Интернет, практические эффекты и рекомендации)

Костогрызов А.И.
(495) 795-85-24, (499) 764-26-58

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)

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

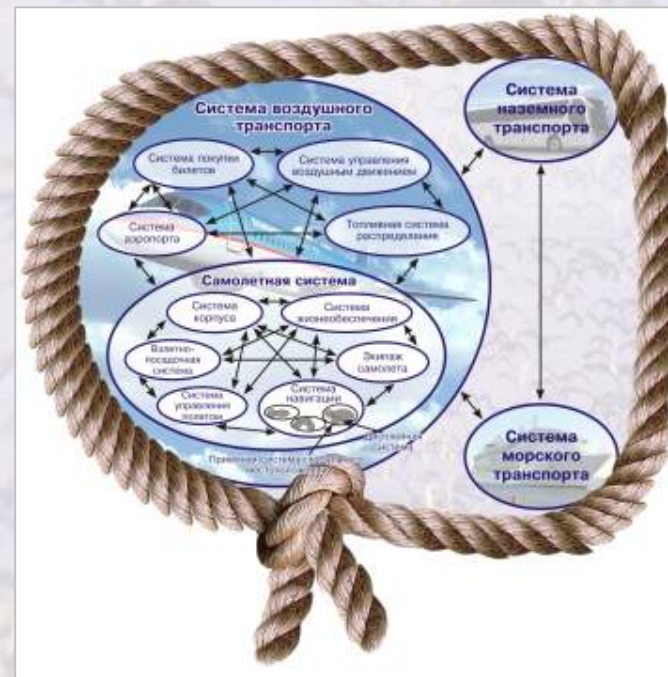
20-й век			21-й век
30-60 гг.	70-80 гг.	90-е гг.	сегодня
<p><u>Кибернетика и математическое моделирование</u></p>  <p>Оценки потоков и вероятностно-временных характеристик</p> <p>Бум прошел</p>	<p>Теория вероятностей, основы системного анализа</p>  <p>Теория надежности, модели под конкретные системы</p> 	<p>Теория системной инженерии</p> <p>Стандарты и др. нормативные документы, базовые модели, методы оценки процессов и обеспечения качества</p> 	<p>Апробированные математические модели, инструментальные средства и технологии их эффективного применения</p> 

Системная инженерия – избирательное приращение 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)

ISO 9001



ISO/IEC 15288



Пример из ISO/IEC 15288

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



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)



**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 управления 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



Цель процесса приобретения

получение продукта или услуги в соответствии с требованиями приобретающей стороны

Результаты процесса приобретения

определяется стратегия приобретения;
выбирается поставщик;
устанавливается связь с поставщиком;
объявляется обоснование для выбора поставщика;
заключается соглашение о приобретении продукта или услуги в соответствии с определенными критериями приемки;
принимается продукт или услуга, соответствующие соглашению;
осуществляется оплата или другие согласованные расчеты

Деятельность в процессе приобретения

утверждать план приобретения;
подготавливать заявку на поставку продукта или услуги;

Примечание – Необходимо обеспечить определение требований к одному или нескольким поставщикам. Если поставщик является внешним по отношению к организации, то заявка может включать правила деловых отношений, которым поставщик будет следовать, а также критерии выбора поставщика

выбирать поставщика;

Примечание – Для конкурсных поставок необходимо оценивать и сравнивать предложения по поставке на соответствие критериям выбора. Если предложения выходят за рамки критериев, они сравниваются друг с другом с целью определения их приоритетности и, как следствие, - предпочтительных поставщиков. Обоснование ранжирования каждого предложения документируется, и поставщики могут быть проинформированы о том, почему они были или не были выбраны

заключать соглашение с поставщиком;

Примечание – В соответствии с принятой формой соглашения в нем устанавливаются требования к системным продуктам или услугам, контрольные сроки разработок и поставок, условия верификации, валидации и приемки, процедуры обработки исключительных ситуаций, процедуры контроля изменений и графики выплат

оценивать выполнение соглашения;

Примечание – Это действие предполагает подтверждение того, что обе стороны выполняют свои обязательства в соответствии с соглашением. Планируемые технические риски, риски по срокам поставки и стоимостные риски должны контролироваться, а влияние на организацию нежелательных результатов регулярно оцениваться. При необходимости согласовываются изменения условий соглашения

Задачи, решаемые на основе математического моделирования

- Анализ технических рисков
- Анализ рисков по срокам поставки
- Оценка стоимостных рисков
- Анализ неудовлетворительных результатов



Цель процесса поставки

обеспечение приобретающей стороны продукцией или услугами, удовлетворяющими согласованным требованиям

Результаты процесса поставки

определяется приобретающая сторона продукта или услуги;
составляется ответ на заявку приобретающей стороны;
заключается соглашение о поставке продукта или услуги в соответствии с определенными критериями приемки;
обеспечивается связь с приобретающей стороной;
в соответствии с согласованными процедурами и условиями поставок поставляется продукт или услуга, удовлетворяющие соглашению;
в порядке, указанном в соглашении, передается ответственность за приобретенный продукт или услугу;
производится оплата или осуществляются другие согласованные взаиморасчеты

Деятельность в процессе поставки

оценивать заявку на поставку продукта или услуги, чтобы определить ее выполнимость и содержание ответа на нее;
готовить предложение по удовлетворению ходатайства;
заключать соглашение с приобретающей стороной;

Примечание – Поставщик подтверждает, что требования, сроки поставки и условия приемки выполнимы, что процедуры обработки исключительных ситуаций и контроля изменений, а также график оплаты приемлемы, и что они являются достаточным основанием для того, чтобы выполнить соглашение без излишних рисков

оценивать выполнение соглашения;

Примечание – Риски, относящиеся к зафиксированной в соглашении стоимости, эксплуатационным характеристикам и срокам, контролируются, а информация о них соответствующим образом сообщается приобретающей стороне. Оценивается воздействие нежелательных результатов на деятельность организации

поставлять продукт или услуги в соответствии с критериями соглашения

Задачи, решаемые на основе математического моделирования

Анализ технических рисков

Анализ рисков по срокам поставки

Оценка стоимостных рисков

Анализ неудовлетворительных результатов



Цель процесса управления средой предприятия

определение и проведение политики и процедур, необходимых для функционирования организации в соответствии с положениями данного стандарта

Результаты процесса управления средой предприятия

реализуется политика и процедуры стратегического управления жизненным циклом системы;
определяется степень ответственности и объем полномочий при осуществлении управления жизненным циклом системы;
реализуется политика усовершенствования процессов жизненного цикла системы

Деятельность в процессе управления средой предприятия

устанавливать планы действий для каждой области деятельности;
подготавливать политику и процедуры управления жизненным циклом системы;
Примечание – Фактические объем операций и степень детализации проекта по осуществлению жизненного цикла систем зависят от сложности работ, используемых технологий, опытности и квалификации персонала, выполняющего работу. Политика и процедуры должны отвечать требованиям проекта. Функции управления риском, управления качеством и управления человеческими ресурсами играют существенную роль при реализации проекта

определять критерии, позволяющие контролировать развитие процессов жизненного цикла;
Примечание – Следует установить критерии принятия решений, относящиеся к началу и окончанию каждой стадии жизненного цикла, а также к другим ключевым событиям

периодически пересматривать используемую при проектировании модель жизненного цикла системы;
Примечание – Следует постоянно подтверждать пригодность, адекватность и результативность моделей жизненного цикла, используемых в каждом проекте, и соответствующим образом совершенствовать их

Задачи, решаемые на основе математического моделирования

Анализ возможных способов выполнения проектов

Сравнительная оценка затрат на выполнение работ

Анализ стратегии в управлении средой предприятия



Цель процесса управления инвестициями

запуск в производство и поддержка обоснованных и успешных проектов, способствующих достижению целей организации

Результаты процесса управления инвестициями

квалифицируются и отбираются инвестиционные возможности или потребности;
определяются и распределяются ресурсы и денежные средства;
определяются полномочия и ответственность при управлении проектом;
поддерживаются проекты, удовлетворяющие условиям соглашения, требованиям правообладателей и организации;
переориентируются или прекращаются проекты, не удовлетворяющие условиям соглашения, требованиям правообладателей или организации

Деятельность в процессе управления инвестициями

находить новые возможности и формы развития в деловой области, заключать новые соглашения, соответствующие стратегическому плану предприятия и планам для каждого из направлений его деятельности;

Примечание – Следует расставлять приоритеты для проектов, которые должны быть начаты, и устанавливать критерии для определения того, какие проекты будут выполняться

оценивать предполагаемые результаты осуществления проектов;
распределять ресурсы для достижения целей проекта;

оценивать текущие проекты с целью подтверждения того, что:

- 1) проекты продвигаются в направлении достижения поставленных целей;
- 2) проекты ведутся согласно соответствующим директивам;
- 3) проекты реализуются в соответствии с планами и процедурами жизненного цикла систем;
- 4) проекты остаются жизнеспособными, что подтверждается, например, постоянной потребностью в услуге, практическим выполнением продукта и приемлемыми доходами от инвестиций

Задачи, решаемые на основе математического моделирования

Анализ перспективности проектов

Анализ предполагаемых результатов осуществления проекта

Рациональное распределение инвестиций

Оценка доходности инвестиций



Цель процесса управления процессами жизненного цикла системы

гарантировать доступность эффективных процессов жизненного цикла для использования организацией

Результаты процесса управления процессами жизненного цикла системы

определяются процессы жизненного цикла системы, которые будут использоваться организацией;
определяется политика применения процессов жизненного цикла системы;
определяется политика адаптации процессов жизненного цикла системы для удовлетворения потребностей отдельных проектов;
определяются критерии оценки результатов применения процессов жизненного цикла системы;
предпринимаются действия по совершенствованию способов определения и применения процессов жизненного цикла системы

Деятельность в процессе управления процессами жизненного цикла системы

устанавливать стандартные наборы процессов жизненного цикла систем для соответствующих стадий жизненного цикла системы;
определять методы и инструментальные средства, которые поддерживают выполнение процессов жизненного цикла системы;
по возможности устанавливать показатели, которые позволяют определять характеристики выполненных стандартных процессов;
контролировать выполнение процесса, сохранять и анализировать показатели процесса и определять тенденции по отношению к критериям предприятия;
определять возможности для усовершенствования стандартных процессов жизненного цикла систем;
совершенствовать имеющиеся процессы, методы и инструментальные средства, используя найденные возможности

Задачи, решаемые на основе математического моделирования

Анализ возможных изменений конкурентоспособности

Анализ организации процессов в жизненном цикле

Анализ возможных улучшений в результате усовершенствований

Оценка политики в управлении жизненным циклом



Цель процесса управления ресурсами

обеспечение проектов необходимыми ресурсами

Результаты процесса управления ресурсами

проекты обеспечиваются необходимыми ресурсами, материалами и обслуживанием;
поддерживается или улучшается квалификация персонала;
разрешаются конфликты, возникающие в результате одновременного осуществления нескольких проектов

Деятельность в процессе управления ресурсами

определять и обеспечивать готовность инфраструктуры ресурсов, и осуществлять поддержку проекта;

Примечание – Проектные планы и потребности будущей деловой деятельности способствуют пониманию необходимой инфраструктуры ресурсов. Физические факторы, такие как оборудование, человеческие факторы, уровень шума и параметры окружающей рабочей среды, считаются определенными

проявлять заботу о персонале, занятом в осуществлении текущих проектов;

Примечание – Сюда относятся: отбор, обучение и удержание персонала, обладающего необходимым уровнем навыков и опыта для того, чтобы проект был должным образом обеспечен кадрами; контроль уровня компетентности персонала в области процессов жизненного цикла систем; обучение и тренировки персонала для совершенствования навыков и обеспечения возможности карьерного роста; оценка работы персонала по таким свойствам, как профессионализм, мотивация, способность работать в команде, необходимость в переобучении, в переводе на другую должность или в другое подразделение организации

Стимулировать персонал, например, посредством предоставления возможности карьерного роста или при помощи системы поощрений;

контролировать области взаимодействия нескольких проектов для разрешения связанных с графиками их реализации конфликтов:

- 1) из-за ограниченных возможностей организационной инфраструктуры, вспомогательных служб и ресурсов при распределении между текущими проектами;
- 2) из-за того, что персонал занят работой над несколькими проектами одновременно

Задачи, решаемые на основе математического моделирования

Анализ инфраструктуры, количества и качества ресурсов

Анализ готовности персонала для осуществления проекта

Анализ временных задержек при работе над несколькими проектами



Цель процесса управления качеством

обеспечить уровень качества продукции, услуг и реализации процессов жизненного цикла, соответствующий целям предприятия в области качества и удовлетворяющий заказчика

Результаты процесса управления качеством

определяются политика организации и процедуры в области управления качеством;
определяются цели и задачи организации в области управления качеством;
определяется отчетность и полномочия для управления качеством;
контролируется степень удовлетворенности заказчика;
предпринимаются необходимые меры в случае, если цели в области управления качеством не достигнуты

Деятельность в процессе управления качеством

устанавливать политику, стандарты и процедуры в области управления качеством;

устанавливать цели организации в области управления качеством, основанные на стратегии, направленной на обеспечение удовлетворенности заказчика;

выполнять оценку и составлять отчеты о степени удовлетворенности заказчика;

проводить периодическую переоценку планов обеспечения качества проектов;

Примечание – Необходимо убедиться, что для каждого проекта установлены цели в области управления качеством, основанные на требованиях правообладателя

контролировать состояние совершенствования качества продукции и услуг

Задачи, решаемые на основе математического моделирования

Анализ эффективности работы службы качества

Анализ степени удовлетворенности заказчика

Оценка политики в управлении качеством



Цель процесса планирования

доведение до заинтересованных сторон
эффективного и выполнимого плана проекта

Результаты процесса планирования

обеспечивается доступ к проектным планам;
определяются роли, ответственность и полномочия;
делается официальный запрос на ресурсы и услуги, необходимые
для осуществления проекта;
определяются показатели для характеристик проекта;
штат проекта ориентируется в соответствии с проектным планом

Деятельность в процессе планирования проекта

определять проектные цели и ограничения;

Примечание – Цели и ограничения включают рабочие характеристики и иные аспекты качества, затраты, сроки и показатели удовлетворенности правообладателей. Каждая цель определяется с той степенью детализации, которая позволяет выбирать, настраивать и реализовывать соответствующие процессы и действия

определять границы проекта в соответствии с соглашением. Устанавливать декомпозицию работ, основанную на развивающейся системной архитектуре. Определять и поддерживать графики работ в рамках проекта, основываясь на целях проекта и оценках выполнимости работ;

Примечание – Сюда относится определение продолжительности, взаимосвязей, зависимостей и последовательности мероприятий проекта, достижение контрольных точек его выполнения, используемые ресурсы и регулярно проводимый анализ (ревизии), необходимые для своевременного завершения проекта

определять критерии достижения результатов проекта для схем принятия решений на стадиях жизненного цикла, сроков поставок и основных зависимостей от внешних входов и выходов;

Примечание – Интервалы времени между моментами внутренних ревизий проекта определяются в соответствии с политикой организации в отношении таких вопросов, как бизнес и критичность системы, графики работ и технические риски

определять расходы на проект и планировать бюджет;

Примечание – Расходы зависят от проектных графиков, оценок объемов работ, затрат на инфраструктуру, приобретаемые комплектующие, получение услуг, а также от затрат на обеспечивающие системы и резервов бюджета для управления рисками

определять проектные показатели, которые должны быть сформированы, и связанные с ними данные, которые должны быть собраны, подвергнуты валидации и анализу;

Примечание – К этому действию относится определение источников проектных данных, их получателей и назначение соответствующих сроков

составлять планы по обеспечению качества проект

Задачи, решаемые на основе математического моделирования

Анализ достижимого качества

Определение границ проекта

Оценка затрат и условий выполнимости задач
проекта



Цель процесса оценки проекта

Определение статуса проекта

Результаты процесса оценки проекта

становятся доступными показатели или результаты оценки рабочих характеристик проекта;
оценивается адекватность ролей, обязанностей и полномочий;
оценивается адекватность ресурсов и услуг, необходимых для реализации проекта;
анализируются отклонения от планируемых значений показателей рабочих характеристик проекта;
заинтересованные стороны информируются о статусе проекта

Деятельность в процессе оценки проекта

оценивать статус проекта относительно соответствующих проектных планов для определения отклонений в затратах, сроках и качестве;

оценивать результативность структуры проектной команды, распределение ролей и обязанностей;

Примечание – Данное действие включает оценку компетентности членов команды для адекватного выполнения проектных ролей и задач проекта. Везде, где возможно, применяются объективные показатели, например такие, как эффективность использования ресурсов, степень достижения целей проекта

оценивать адекватность и готовность инфраструктуры, обеспечивающей выполнение проекта;

Примечание – К этим работам относится также подтверждение выполнения обязательств внутри организации

оценивать развитие проекта, используя измеренные достижения и результаты выполнения проекта в промежуточных контрольных точках;

Примечание – Необходимо в запланированные сроки собирать и оценивать фактические или прогнозируемые затраты на персонал, ресурсы и выполняемые работы, осуществлять сравнение с заданными проектными показателями достижения целей проекта. Сюда относится также проведение оценок результативности для определения адекватности развития системы относительно предъявляемых требований. Кроме того, сюда входит оценка готовности обеспечивающих систем поставлять необходимые услуги

проводить требуемые управленческий и технический анализ, аудит и проверки для определения готовности к переходу на следующую стадию жизненного цикла системы или на следующий этап осуществления проекта;

отслеживать критические процессы и новые технологии;

анализировать данные и показатели для выявления значимых отклонений или изменений по отношению к запланированным показателям и давать соответствующие рекомендации для корректировки;

Примечание – Там, где возможно, эти работы включают статистический анализ показателей, которые выявляют тенденции, например, плотность неисправностей характеризует качество выходных результатов, вероятностное распределение измеренных параметров позволяет выявить воспроизводимость процесса

Задачи, решаемые на основе математического моделирования

Анализ ожидаемого качества

Анализ команды

Анализ развития проекта

Анализ эффективности проверок, аудитов и инспекций

Анализ критических условий

Обоснование рекомендаций по корректировке



Цель процесса контроля проекта

организация исполнения плана проекта и обеспечение гарантий реализации в соответствии с планами и графиками в пределах проектного бюджета, и техническими целями

Результаты процесса контроля проекта

определяются и совершаются корректирующие действия, если результаты проекта не соответствуют запланированным заданиям; инициируется перепланирование проекта, если цели проекта или ограничения изменились или допущения, сделанные при планировании, оказались неверными; санкционируются действия по переходу от одного запланированного этапа или события к следующему (при условии успешной реализации предыдущего этапа или события); достигаются цели проекта

Деятельность в процессе контроля проекта

управлять проектными требованиями и изменениями требований в соответствии с проектными планами;
при нарушении допустимых или заранее определенных пределов инициировать корректирующие действия, необходимые для достижения целей и получения результатов решения задач проекта;
Примечание – В случае обнаружения несоответствий или неготовности в состав корректирующих действий может входить перераспределение или переназначение персонала, инструментальных средств и активов инфраструктуры проекта

инициировать превентивные меры для обеспечения достижения целей и результатов проекта;
инициировать действия по разрешению проблем для коррекции несоответствий;
Примечание – Они включают выполнение корректирующих действий по отношению к этапам внедрения и реализации процессов жизненного цикла, если несоответствия прослеживаются к этим этапам. Действия документируются и оцениваются для подтверждения их адекватности и своевременности

разворачивать во времени содержание, определение и соответствующую декомпозицию работ, которые должны быть выполнены в рамках проекта вследствие принятых решений о корректирующих действиях и оцененных изменений, которые эти действия вносят;
инициировать действия по изменениям, связанным с изменениями предусмотренных договором затрат, сроков или качества, произошедшими по инициативе приобретающей стороны или поставщика;

Задачи, решаемые на основе математического моделирования

- Выявление несоответствий
- Обоснование параметров управления проектными требованиями и планами
- Анализ эффективности корректирующих действий



Цель процесса принятия решения

выбор из существующих альтернатив наиболее предпочтительного направления проектных действий

Результаты процесса принятия решения

определяется стратегия принятия решений;
определяются альтернативные направления действий;
выбирается наиболее предпочтительное направление действий;
объявляется и фиксируется само решение, его обоснование и допущения

Деятельность в процессе контроля проекта

определять стратегию принятия решений;

Примечание – К этому действию относится определение категорий решений, схем установления приоритетов и идентификация ответственных сторон. Также определяются лица, принимающие решения, им предоставляются полномочия по принятию решений, и они несут ответственность за принятие решений. Необходимость в принятии решений может возникать вследствие оценки результативности, технического компромисса, наличия проблемы, требующей решения, необходимости реагировать на риски, когда их уровень выходит за допустимые пределы, новые возможности или переход проекта на следующую стадию жизненного цикла. Стратегия принятия решений включает в себя установление и распределение ответственности и полномочий по принятию решений

выбирать и объявлять стратегию принятия решений для каждой ситуации, в которой необходимо принимать решение. Определять желаемые результаты и критерии успешного разрешения проблемы;

оценивать баланс последствий альтернативных действий, используя утвержденную стратегию принятия решений, с целью оптимизации или улучшения ситуации принятия решений;

документировать, отслеживать, оценивать и сообщать о результатах принятия решения для подтверждения того, что проблемы были решены эффективно, отрицательные тенденции были устранены и были получены возможные преимущества

Задачи, решаемые на основе математического моделирования

Обоснование требований к характеристикам

сбора информации

Оценки успешности разрешения проблемы

Анализ стратегии принятия решений



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



Цель процесса управления конфигурацией

установление и поддержание целостности всех идентифицированных выходных результатов проекта или процесса обеспечения доступа к ним любой заинтересованной стороны

Результаты процесса управления конфигурацией

определяется стратегия управления конфигурацией;
определяются элементы, нуждающиеся в управлении конфигурацией;
устанавливается базовая линия конфигурации;
контролируются изменения элементов, нуждающихся в управлении конфигурацией;
контролируется конфигурация выделенных элементов;
становится доступным на протяжении всего жизненного цикла статус элементов конфигурации, на которые распространяется управление

Деятельность в процессе управления конфигурацией

определять стратегию управления конфигурацией;

Примечание – Сюда относится определение полномочий на запрет или разрешение доступа, реализацию и контроль изменений элементов конфигурации, определение места и условий их хранения, включая требования к окружающей среде, и, в случае информации, хранение носителей с назначенным уровнем целостности, защищенности и безопасности, определение критериев или событий, определяющих начало контроля конфигурации и управления базовой линией в процессе эволюции конфигурации, а также в определении стратегии аудита и ответственности за гарантии непрерывной целостности и безопасности информации; определение стратегии аудита и обязанностей по обеспечению постоянной целостности и безопасности информации, описывающей конфигурацию. Деятельность по управлению конфигурацией должна быть совместима с руководством

поддерживать информацию о конфигурации на приемлемом уровне целостности и защищенности;

гарантировать, что изменения базовой линии конфигурации тщательно идентифицируются, записываются, оцениваются, утверждаются, проводятся и верифицируются

Примечание – Эти действия также могут включать объединение в процессе развития конфигурации состояний ее элементов для формирования документированной базовой линии на определенный момент времени или при определенных обстоятельствах, Регистрировать этапы конфигурации, обоснования для базовой линии и связанные с этим данные о соответствующих разрешениях. Поддерживать записи о конфигурации в течение жизненного цикла и архивировать их в соответствии с соглашениями, законами или наилучшей производственной практикой. Управлять выполнением записей, изменениями и утверждениями текущего статуса конфигурации и статуса всех предыдущих конфигураций для подтверждения корректности, своевременности, целостности и защищенности информации. Проводить аудит для проверки соответствия базовой линии чертежам, документам по контролю интерфейсов и другим требованиям, указанным в соглашении

Задачи, решаемые на основе математического моделирования

Обоснование параметров стратегии управления конфигурации

Оценка качества конфигурационной информации



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 накапливаться 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)



Цель определения требований заказчиков (правообладателей)

выявление требований к системе, выполнение которых может обеспечить функциональные возможности, необходимые пользователям системы и иным заинтересованным лицам в заданной эксплуатационной среде

Результаты процесса определения требований

задаются требуемые характеристики и условия использования функциональных возможностей системы;
определяются ограничения для системных решений;
достигается возможность текущего отслеживания связей между требованиями правообладателей и самими правообладателями и их потребностями;
описывается основа для определения системных требований;
определяется основа для валидации соответствия функциональных возможностей системы;
формируется основа для ведения переговоров и заключения соглашения о поставке продукции или услуг

Деятельность в процессе определения требований

определять ограничения системных решений, которые являются неизбежным следствием существующих соглашений, управленческих или технических решений;
определять представительный набор последовательных действий для идентификации всех требуемых функциональных возможностей, которые отвечают предполагаемым сценариям и средам функционирования и сопровождения;

Примечание – Сценарии используются для анализа функционирования системы в заданной среде с целью установления требований, которые формально не были заданы ни одним из правообладателей, например, юридические, регулирующие и социальные обязательства. Определяются и анализируются условия использования системы. Содержательному анализу подлежат мероприятия, которые осуществляют пользователи для достижения целей системы, а также основные характеристики конечных пользователей системы (например, предполагаемая квалификация, степень выносливости), характеристики физической среды (например, уровень освещенности, температура), а также любое используемое оборудование (например, защитное оборудование или аппаратура связи). Также анализируются социальное воздействие и воздействие организации на пользователей, которые могут повлиять на применение системы или сдерживать процесс проектирования системы

устанавливать и специфицировать экологические, медицинские требования, требования безопасности и другие требования правообладателей, имеющие отношение к критическим показателям;
анализировать полное множество выявленных требований;

Примечание – Анализ включает идентификацию противоречивых, пропущенных, неполных, неоднозначных, нелогичных или непроверяемых требований и расстановку приоритетов

разрешать проблемы, возникающие в связи с определением требований;

Примечание – Сюда относятся требования, которые не могут быть реализованы или которые нецелесообразно реализовывать

доводить результаты анализа требований до сведения соответствующих правообладателей для гарантии того, что их потребности и ожидания были правильно поняты и выражены;

Примечание – Необходимо путем разъяснения достигать соглашения по решениям, касающимся противоречивых, нецелесообразных и неосуществимых требований

поддерживать взаимное соответствие между требованиями правообладателей и потребностями заинтересованных лиц

Задачи, решаемые на основе математического моделирования

- Определение требований к интегральному качеству
- Определение допустимых условий создания
- Определение характеристик среды функционирования
- Определение характеристик взаимодействия пользователей с системой
- Определение системотехнических ограничений в эксплуатации
- Определение требований к удовлетворенности заказчика



Цель процесса анализа требований

преобразование требований правообладателя, выраженных в виде его представлений о желаемых функциональных возможностях, в техническое видение требуемого продукта, способного предоставить такие функциональные возможности

Результаты процесса анализа требований

задаются требуемые характеристики, свойства, функциональные и эксплуатационные требования к техническим решениям;
задаются ограничения, влияющие на архитектурное проектирование системы, а также на средства по его реализации;
определяются способы, с помощью которых обеспечивается целостность системных требований, требований правообладателей и взаимное соответствие между ними;
определяется основа для верификации системных требований

Деятельность в процессе анализа требований

определять функциональные границы системы в терминах ее поведения и предусмотренных свойств;
Примечание – К ним относятся входные воздействия на систему, а также реакция системы на действия пользователя и поведение внешней среды, анализ и описание взаимодействий между системой и средой относительно интерфейсных ограничений, например, механических, электрических, весовых, температурных, а также ограничений материальных и информационных потоков. Таким образом, устанавливается ожидаемое поведение системы, выраженное в количественных показателях, а также границы их допустимых значений

определять каждую функцию, которую должна выполнять система, насколько хорошо система, включая операторов, будет выполнять требуемую функцию, условия, при которых система способна выполнять эту функцию, а также условия, при которой система начинает и прекращает выполнение данной функции;
определять технические показатели и показатели качества при использовании, позволяющие оценивать технические достижения;

Примечание – При этом оцениваются критические параметры функционирования системы, связанные с каждым показателем результативности, соответствующим принятым требованиям правообладателей. Критические показатели функционирования анализируются и проверяются для подтверждения удовлетворения требований заказчика и для определения стоимости проекта, проектных графиков или эксплуатационных рисков, связанных с любыми несоответствиями

задавать системные требования и функции, в соответствии с которыми определяются риски и критические параметры системы, связанные с такими критическими показателями, как здоровье, безопасность, защищенность, безотказность, готовность и обслуживаемость;

анализировать целостность системных требований для обеспечения уверенности в том, что каждое требование, пары требований или наборы требований обладают системной целостностью;

демонстрировать связь между системными требованиями и требованиями правообладателей;

на протяжении всего жизненного цикла вести учет совокупности системных требований вместе с их обоснованиями, связанными решениями и допущениями

Задачи, решаемые на основе математического моделирования

Анализ выполнимости требований к интегральному качеству системы

Анализ выполнимости требований к взаимодействию пользователей с системой

Анализ выполнимости требований к условиям эксплуатации

Анализ выполнимости требований к удовлетворенности заказчика



Цель процесса проектирования архитектуры

синтез решения, которое бы удовлетворяло системным требованиям

Результаты процесса проектирования архитектуры

устанавливается порядок, в соответствии с которым выполняется проектирование архитектуры;
задается реализуемый набор описаний системных элементов, которые удовлетворяют требованиям, предъявляемым к системе;
включаются в решение по проектированию архитектуры требования к интерфейсу;
устанавливается связь между проектированием архитектуры и системными требованиями;
определяется основа для верификации системных элементов;
устанавливается основа комплексирования системных элементов

Деятельность в процессе проектирования архитектуры

определять приемлемые проекты логической архитектуры;

Примечание – Данное действие включает идентификацию и определение производных требований для описания функциональных и эксплуатационных требований, функциональных возможностей и свойств, требований к своевременности, к потокам данных и т.д. в соответствии с логической архитектурой

выполнять декомпозицию функций системы, определенных в процессе анализа требований и поставить им в соответствие элементы архитектуры системы, сформировать производные требования, необходимые для такого сопоставления;

анализировать итоговый проект архитектуры с целью установления проектных критериев для каждого элемента;

Примечание – Проектные критерии включают физические, эксплуатационные, поведенческие характеристики, характеристики надежности и устойчивости

определять, какие системные требования должны выполняться операторами;

оценивать альтернативные проектные решения, моделируя их с той степенью детализации, которая позволяет сравнивать спецификации, выраженные в системных требованиях, с эксплуатационными характеристиками, стоимостными и временными показателями и рисками, выраженными в требованиях правообладателей;

Примечание – Сюда относятся:

- 1) оценка и сообщение о появлении неблагоприятных свойств системы, обусловленных взаимодействием потенциальных системных элементов или в результате изменений в элементах системы;
- 2) гарантии того, что ограничения обеспечивающих систем приняты в расчет в данном проекте;
- 3) проведение оценок результативности, анализа компромиссных решений, анализа рисков, которые приводят к тому, что разрабатывается выполнимый, эффективный, стабильный и оптимизированный проект

поддерживать взаимосвязь и взаимозависимость между архитектурой и системными требованиями

Задачи, решаемые на основе математического моделирования

Анализ проекта архитектурного построения системы

Анализ функциональных компонентов (как систем с функциями массового обслуживания, сбора, контроля, анализа, мониторинга, противодействия угрозам)



Цель процесса изготовления

создание заданных (специфицированных) элементов системы

Результаты процесса изготовления

определяется стратегия изготовления;
определяются технологические ограничения, связанные с конструкцией системного элемента;
изготавливается системный элемент;
системный элемент упаковывается и хранится в соответствии с соглашением о его поставке

Деятельность в процессе изготовления

разрабатывать стратегию изготовления;

Примечание – В нее включаются процедуры изготовления, процессы производства, инструменты и оборудование, допущения при изготовлении и неопределенности при верификации. В случае многократного изготовления системного элемента, например при массовом производстве, использовании взаимозаменяемых системных элементов и т.п., процедуры изготовления и процессы производства должны задаваться таким образом, чтобы обеспечить достижение последовательного и устойчивого воспроизводства

реализовывать или адаптировать системные элементы, используя обеспечивающие системы и определенные материалы в соответствии с заданными процедурами изготовления для производства технических средств, создания программных средств и (или) для обучения операторов;

вести регистрацию доказательств соответствия элементов системы соглашениям с поставщиками, законодательству и политике организации;

Примечание – Сюда входит обеспечение объективных доказательств того, что требования проектирования архитектуры были реализованы в системных элементах. Доказательства предоставляются в соответствии с соглашениями о поставке, законодательством и политикой организации

Задачи, решаемые на основе математического моделирования

Анализ влияния факторов неопределенности

Анализ стратегии реализации



Цель процесса комплексирования

сборка системы согласно архитектурному проекту

Результаты процесса комплексирования

определяется стратегия комплексирования системы;
определяются неизбежные ограничения, связанные с процессом комплексирования, которые влияют на системные требования;
компонуются и комплексировается система, допускающая верификацию на соответствие требованиям, заданным архитектурным проектом;
ведется документальный учет несоответствий, возникших в процессе комплексирования

Деятельность в процессе комплексирования

определять последовательность и стратегию сборки системы, которые минимизируют риски в процессе комплексирования;

Примечание – Такая стратегия позволяет осуществлять верификацию при помощи последовательности наращиваемых конфигураций системных элементов. Она зависит от степени готовности системных элементов и согласуется с локализацией последствий ошибок и стратегией оценки ситуации. По возможности скомплексированная конфигурация включает в свой состав людей-операторов. Последовательное применение процессов комплексирования и верификации, а в случае необходимости и процесса валидации повторяется для систем на каждом из последующих уровней до тех пор, пока рассматриваемая система не будет создана

идентифицировать ограничения на конструктивные решения, возникающие в результате следования стратегии комплексирования;

гарантировать, что системные элементы были верифицированы на соответствие критериям приемки, указанным в соглашении;

Примечание – Системные элементы, не прошедшие верификацию, идентифицируются в качестве таковых и обрабатываются в соответствии с установленными процедурами

комплексировать системные элементы в соответствии с применяемыми описаниями контроля интерфейсов и установленными процедурами сборки, используя заданные средства интеграции;

вести учет информации, касающейся комплексирования в соответствующей базе данных
Примечание – Сюда относятся записи о решении проблем, обнаруженных благодаря стратегии комплексирования и системам, обеспечивающим комплексирование, или допущенным ошибкам сборки. Данные анализируются для проведения мероприятий по корректировке или улучшению стратегии комплексирования и ее осуществления

Задачи, решаемые на основе математического моделирования

Анализ влияния факторов неопределенности

Анализ стратегии комплексирования



Цель процесса верификации

подтверждение того, что заданные (специфицированные) требования проекта полностью реализованы в системе

Результаты процесса верификации

определяется стратегия верификации;
в качестве входных данных используются ограничения, накладываемые на верификацию.
получаются отчетные данные, являющиеся источником для совершения корректирующих действий;
предоставляются объективные доказательства того, что реализованная продукция удовлетворяет системным требованиям и требованиям архитектурного проекта

Результаты процесса верификации

определять стратегию верификации систем в течение жизненного цикла;

Примечание – Эта стратегия касается системы и ее описаний, например требований, проектных определений. Она включает содержание и цели для каждого объекта верификации, например, при верификации проекта проверяется способность корректно осуществлять проектирование, способность к воспроизведению системы, возможность корректировать возникающие ошибки, способность прогнозировать отказы. Верификация демонстрирует посредством оценки продукта, что система создана "правильно", то есть система является реализацией того проекта, по которому и должен быть создан продукт. В ходе верификации, если есть возможность, в систему включается человек-оператор. Содержание и масштаб процесса верификации, например, пересмотр, инспекция, аудит, сравнение, статические испытания, динамические испытания, демонстрация (или комбинация этих видов верификации) зависят от того, что подвергается верификации: модель, прототип или реальный продукт и от возможных рисков, например, по безопасности, критичности с коммерческой точки зрения

определять план верификации, основываясь на системных требованиях;
идентифицировать и сообщать о потенциальных ограничениях на проектные решения;
осуществлять верификацию для демонстрации соответствия заданным проектным требованиям;
формировать доступные верификационные данные о системе;
анализировать, вести учет и докладывать информацию о верификации, отклонениях и корректирующих действиях

Примечание – В соответствии с условиями соглашений, касающимися целей организации, необходимо проводить верификацию таким образом, чтобы изолировать ту часть системы, которая вызывает появление несоответствий. Проводится оперативная диагностика с такой степенью разрешения, которая обеспечивает экономическую оправданность действий по устранению недостатков, в том числе последующее исправление дефектов и (или) совершенствование организационных аспектов. Верификационные данные собираются, классифицируются и упорядочиваются в соответствии с критериями, определенными стратегией верификации. Таким образом, осуществляется классификация несоответствий согласно их источникам, корректирующим воздействиям и владельцам. Верификационные данные анализируются с целью обнаружения таких существенных признаков, как тенденции и условия отказов, доказательства ошибок проектирования и возникающих угроз функциональным возможностям системы

Задачи, решаемые на основе математического моделирования

- Анализ степени влияния «подыгрывающих» компонентов и условий
- Анализ степени соответствия
- Анализ качества верификации
- Анализ стратегии верификации



Цель процесса передачи

достижение способности обеспечивать услуги в среде функционирования согласно заданным требованиям правообладателей

Результаты процесса передачи

определяется стратегия передачи;
система приводится в рабочее состояние на месте ее применения;
в процессе работы система способна выполнять свои функции;
конфигурация приведенной в рабочее состояние системы документируется;
регистрируются отчеты о корректирующих действиях;
обеспечивающими системами предоставляются необходимые услуги

Деятельность в процессе передачи

определять стратегию передачи;

Примечание – Стратегия передачи включает в себя установку и ввод в действие системы в соответствии с соглашениями. По возможности передача осуществляется с привлечением операторов

продемонстрировать, что система подготовлена к работе надлежащим образом;

Примечание – Приемочные испытания, указанные в соглашении о поставке, могут продемонстрировать правильность установки. Если точное место размещения или среда функционирования недоступны, производится репрезентативная выборка

продемонстрировать способность установленной системы выполнять требуемые функции;

Примечание – Приемочные испытания, указанные в соглашениях, могут определять критерии, которые демонстрируют, что системный объект обладает способностью выполнять требуемые функции после того, как система приведена в рабочее состояние на своем рабочем месте и обслуживается штатными операторами

вести документированный учет данных по установке, включая рабочую конфигурацию, обнаруженные отклонения, предпринятые действия и извлеченные уроки

Примечание – Отчет по итогам установки системы должен включать наряду с техническими сведениями сведения о недостаточности и неполноте системных требований. В случае обнаружения несоответствий в интерфейсе между системой, заданной средой функционирования и любыми системами, обеспечивающими стабильность использования системы, необходимо проводить корректирующие действия и (или) осуществлять изменения требований

Задачи, решаемые на основе математического моделирования

Анализ способности операторов к эксплуатации

Анализ реальных возможностей системы на основе результатов выборочных испытаний



Цель процесса валидации

получение объективных доказательств того, что функции, обеспечиваемые системой при ее использовании, соответствуют требованиям правообладателей

Результаты процесса валидации

определяется стратегия валидации;
подтверждается готовность к выполнению функций, требуемых правообладателями;
предоставляются данные валидации;
составляется отчет по данным валидации, на основании которых можно осуществить корректирующие действия

Деятельность в процессе валидации

определять стратегию валидации реализуемых системой функций в среде функционирования при условии достижения удовлетворенности правообладателей;

Примечание – Посредством оценки функциональных возможностей, представляемых правообладателям, валидация демонстрирует, что создан “правильный объект” системы, то есть он соответствует цели и удовлетворяет потребителя. Валидация проводится, начиная с самых ранних этапов жизненного цикла. Например, бумажные прототипы, имитационные модели или макеты системы, находящейся в разработке в соответствующем представлении окружающей среды, могут быть использованы для валидации на стадии формирования концепции будущей системы. Содержание и масштаб процесса валидации зависят от того, подвергается ли валидации модель, прототип или реальная система, от рисков (например, новизна, безопасность, факторы технической и коммерческой критичности), от соглашений и организационных ограничений и от требований правообладателей. Валидацию созданного продукта могут проводить поставщик, приобретающая сторона или ее представитель. Ответственность сторон устанавливается в соглашении

подготавливать план валидации;
проводить валидацию для демонстрации соответствия функциональных возможностей системы требованиям правообладателей;

Примечание – При выполнении валидации минимизируются организационные ограничения такие как, неопределенность воспроизведения повторных действий по валидации, условий и полученных результатов. Необходимо объективно отражать и утверждать валидационные мероприятия и результаты. Валидация также может проводиться для подтверждения того, что система не только удовлетворяет всем эксплуатационным и функциональным требованиям и требованиям к удобству и простоте использования, но также удовлетворяет требованиям заказчика, которые зачастую выражены менее формально и бывают субъективными, но являются для него более существенными, и значимыми

анализировать, регистрировать и составлять отчеты по валидационным данным в соответствии с критериями, определенными стратегией валидации

Примечание – При выполнении этого действия несоответствия классифицируются по их источнику и собственнику корректирующего действия. Валидационные данные анализируются для обнаружения таких важных признаков, как тенденции и условия отказов, доказательства ошибок проектирования и возникновения угроз функциональным возможностям системы

Задачи, решаемые на основе математического моделирования

Анализ возможностей системы при выполнении требований заказчика

Сравнительная оценка затрат и прибыли от внедрения системы



Цель процесса функционирования

использование системы для выполнения заданных функций

Результаты процесса функционирования

определяется стратегия функционирования;
поставляются услуги, удовлетворяющие требованиям правообладателей;
успешно выполняются заявки на принятые корректирующие действия;
поддерживается удовлетворенность правообладателей

Деятельность в процессе функционирования

контролировать функционирование системы для подтверждения того, что система управляется в соответствии с планами работы, в безопасном режиме и в соответствии с законодательными актами, касающимися охраны труда и окружающей среды;
осуществлять мониторинг функционирования системы для подтверждения того, что показатели выполнения функций находятся в пределах допустимых значений;
Примечание – Система может показывать неприемлемые эксплуатационные характеристики, если ее элементы, входящие в технические средства, имеют превышения сроков годности или рабочая среда системы негативно воздействует на оперативный и обслуживающий персонал (включая текучесть кадров, стрессы и утомление операторов)

осуществлять действия по обнаружению отказов при появлении несоответствий в выполняемых функциях;
определять приемлемое направление действий, если требуется проведение корректирующих мероприятий для устранения ошибок, появившихся в результате изменений в потребностях;
Примечание – Приемлемое направление действий может состоять из проведения небольших адаптаций программных или технических средств, модификации действий оператора, изменений требований правообладателей, изменений в конструкции и (или) в реализации системы, допущения ограничений предоставляемых услуг

вводить необходимые изменения в порядок эксплуатации, среду функционирования, интерфейсы “человек-машина” и в обучение операторов, если ошибки человека приводят к отказам;
постоянно или регулярно общаться с пользователями для определения степени, с которой предоставляемые услуги удовлетворяют их потребности

Задачи, решаемые на основе математического моделирования

- Анализ достигаемого уровня качества
- Анализ достигаемого уровня взаимодействия пользователей с системой
- Анализ выполнения системотехнических ограничений
- Анализ степени удовлетворенности заказчика



Цель процесса обслуживания

поддержание способности системы выполнять заданные функции

Результаты процесса обслуживания

разрабатывается стратегия обслуживания;
ограничения процесса обслуживания применяются в качестве исходных данных при формировании системных требований;
становятся доступными системные элементы, используемые для замены;
осуществляется поддержка услуг, удовлетворяющих требования правообладателей;
в отчетах сообщается о необходимости корректирующих проектных изменений;
ведется документальный учет данных об отказах и сроках службы

Деятельность в процессе обслуживания

подготавливать стратегию обслуживания;

Примечание – При подготовке стратегии определяются графики и ресурсы, необходимые для выполнения корректирующего и превентивного обслуживания в соответствии с требованиями эксплуатационной готовности

определять ограничения системных требований, являющиеся неизбежным следствием реализации стратегии обслуживания;

подтверждать, что мероприятия по материально-техническому обеспечению удовлетворяют требуемым уровням пополнения запасов, в результате чего хранящиеся на складе системные элементы удовлетворяют требованиям по интенсивности восстановлений и запланированным срокам проведения технического обслуживания и ремонта;

Примечание – Необходимо контролировать качество и готовность элементов замены, транспортирование и целостность во время хранения, а также нанимать, обучать и аккредитовывать персонал для поддержания численности и навыков операторов

выполнять действия по идентификации отказов при появлении любых несоответствий в системе;

поддерживать составление отчетов, содержащих историю проблемы, выполненные корректирующие действия и обнаруженные тенденции для информирования операторов и персонала технического обслуживания и ремонта, а также лиц, занятых в других проектах, в которых создаются или используются подобные системные элементы

Задачи, решаемые на основе математического моделирования

- Обоснование параметров сопровождения
- Анализ стратегии сопровождения



Цель процесса изъятия и списания

прекращение существования системного объекта

Результаты процесса изъятия и списания

определяется стратегия изъятия и списания;
ограничения по изъятию и списанию предоставляются в качестве входных данных для требований;
системные элементы уничтожаются, сохраняются, перерабатываются или восстанавливаются;
среда возвращается к своему первоначальному или согласованному (с заинтересованными сторонами) состоянию;
обеспечивается доступ к записям о действиях по изъятию и списанию и результатам анализа долгосрочных угроз

Деятельность в процессе изъятия и списания

определять средства для хранения, места хранения, критерии для инспекций и периоды хранения, если система подлежит хранению;

подтверждать, что после изъятия и списания не существует факторов, наносящих вред здоровью, безопасности, защите и окружающей среде

Задачи, решаемые на основе математического моделирования

Оценка возможных отрицательных последствий
Анализ стратегии снятия системы с эксплуатации



Объективные потребности в оценке качества и рисков в жизненном цикле систем



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 электронной цифровой подписи»,
«Об информации, информационных технологиях и защите информации»,
Доктрина информационной безопасности
и др.

Безопасность – это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз

Производственная безопасность - объективно существующая возможность негативного воздействия на объект или процесс, в результате которого может быть причинен какой-либо ущерб, вред, ухудшающий состояние, придающий развитию нежелательные динамику или параметры (характер, темпы, формы и т.д.)

Система обеспечения пожарной безопасности - совокупность сил и средств, а также мер правового, организационного, экономического, социального и научно-технического характера, направленных на борьбу с пожарами. Пожар – это неконтролируемое горение, причиняющее материальный ущерб, вред...

Радиационная безопасность – это соблюдение допустимых пределов радиационного влияния на персонал, население и окружающую природную среду, установленных пределами,

правилами и стандартами безопасности. **Ядерная безопасность** - соблюдение норм, правил, стандартов и условий использования ядерных материалов, обеспечивающих радиационную безопасность (свойство реакторной установки и атомной станции с определенной вероятностью предотвращать возникновение ядерной аварии – ПБУ)

Транспортная безопасность - состояние защищенности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства. Актом незаконного вмешательства - противоправное действие (бездействие), в том числе террористический акт, угрожающее безопасной деятельности транспортного комплекса, повлекшее за собой причинение вреда, материальный ущерб либо создавшее угрозу наступления таких последствий

Авиационная безопасность – состояние защищенности авиации от незаконного вмешательства в деятельность в области авиации

Информационная безопасность РФ - состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

Безопасность информации - состояние защищенности информации от различных угроз

Сравнительный анализ нормативно-правовой базы

Закон РФ «О промышленной безопасности опасных производствен- ных объектов»

Системные требования изложены в:

ГОСТ 12.2.044-80 ССБТ. Машины и оборудование для транспортирования нефти. Требования безопасности. ГОСТ 17410-78. Контроль неразрушающий. Трубы металлические бесшовные цилиндрические. Методы ультразвуковой дефектоскопии; ПБ 03-585-03 Правила устройства и безопасной эксплуатации технологических трубопроводов; ПБ 03-591-03. Правила безопасной эксплуатации факельных систем; ПБ 08-624-03 Правила безопасности в нефтяной и газовой промышленности; РД 08-284-99. Методические рекомендации по идентификации опасных производственных объектов резервуаров магистральных нефтепроводов и нефтебаз; РД 153-39 4-087-01 Автоматизация и телемеханизация магистральных нефтепроводов. Основные положения; РД 39-132-94 Правила по эксплуатации, ревизии, ремонту и отбраковке нефтепромысловых трубопроводов; РД 39-5-1227 Норматив обменного фонда оборудования и нормы расхода запасных частей и материалов на техническое обслуживание систем измерения количества нефти и трубопоршневых установок; РД 51-4-2.003-97 Методические рекомендации по расчетам конструктивной надежности магистральных газопроводов; РД-03-131-97. Правила организации и проведения акустико-эмиссионного контроля сосудов, аппаратов, котлов, технологических трубопроводов; РДБТ 39-0147171-003-88 Требования к установке датчиков стационарных газосигнализаторов в производственных помещениях и на наружных площадках нефтяной и газовой промышленности; СНИП 2.05.06-85 Магистральные трубопроводы. СНИП 2.11.03-93 Склады нефти и нефтепродуктов. Противопожарные нормы; ГОСТ 12.0.006-2002 ССБТ. Общие требования к управлению охраной труда в организации и др.

Резюме. Нормативные требования задаются количественно, в т.ч. на вероятностном уровне.

Эффективное управление рисками возможно и целесообразно на основе:

- использования исходных материалов, различного рода ресурсов и защитных технологий с более лучшими характеристиками с точки зрения безопасности;
- рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности составных компонентов, объектов или системы;
- рационального применения мер противодействия рискам (включая избегание рисков ситуаций)

Законы РФ «О пожарной безопасности», «Технический регламент о требованиях пожарной безопасности»

Системные требования изложены в:

ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность. Общие требования; ГОСТ 12.1.018-93 ССБТ. Пожаровзрывобезопасность статического электричества. Общие требования; ГОСТ 12.2.037-78 ССБТ. Техника пожарная. Требования безопасности; ГОСТ Р 52436-2005 «Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний»; ГОСТ Р 50862-2005 «Сейфы, сейфовые комнаты и хранилища. Требования и методы испытаний на устойчивость к взлому и огнестойкость»; НПБ 75-2000 «Приборы приемно-контрольные пожарные. Приборы управления пожарные. Общие требования. Методы испытаний»; НПБ 88-2001 «Установки пожаротушения и сигнализации. Нормы и правила проектирования»; НПБ 104-03 «Проектирование систем оповещения людей о пожаре в зданиях и сооружениях»; НПБ 105-03 «Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности»; НПБ 110-03 «Перечень зданий, сооружений, помещений и оборудования, подлежащих защите автоматическими установками пожаротушения и автоматической пожарной сигнализацией»; СНИП 21-01-97 «Пожарная безопасность зданий и сооружений»; СНИП 2.04.09-84 «Пожарная автоматика зданий и сооружений» и др.

Резюме. Для технологических процессов, блоков, помещений, зданий, наружных установок осуществляются установленные на законодательном уровне оценки взрывопожароопасности (для определения возможных разрушительных воздействий). Требования к исходным материалам, различного рода ресурсам, технологиям и начальным состояниям пожароопасных элементов, а также к мерам обеспечения пожарной безопасности регламентированы нормативными документами, в том числе по вероятностным показателям на уровне норм пожарной безопасности!

Эффективное управление рисками возможно и целесообразно на основе применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления нарушенной целостности

Законы РФ «Об использовании атомной энергии», «О радиационной безопасности населения»

Системные требования изложены в:

ОПБ-88/97 «Общие положения обеспечения безопасности атомных станций при проектировании, сооружении и эксплуатации» (в т.ч. вероятность предельного аварийного выброса реактора за год не должна превышать 10⁻⁷); ПБУ РУ АС-89 «Правила ядерной безопасности реакторных установок атомных станций»; СП АС-88 «Санитарные правила проектирования и эксплуатации атомных станций»; INSAG-12. Basic safety principles for nuclear power plants (риск оценивается математическим ожиданием ущерба); IEC 61508 "Функциональная безопасность электрических / электронных / программируемых электронных систем, относящихся к безопасности"; IEC 61513 "(АЭС. Информационно-управляющие системы, важные для безопасности. Общие требования к системам); IEC 60880 "Программное обеспечение для компьютеров в системах, важных для безопасности атомных электростанций"; IEC 60987 "Программируемые цифровые компьютеры, важные для безопасности атомных электростанций"; ОПБ ИР-88 «Общие положения обеспечения безопасности исследовательских реакторов при проектировании, сооружении и эксплуатации»; СП – АС-79 «Общие положения по обеспечению радиационной безопасности населения»; ПБЯ РУ АС-89 «Правила ядерной безопасности реакторных установок атомных станций»; ТС ТОб АС-85 «Типовое содержание технического обоснования безопасности атомных станций»; ТС ТОб РУ-87 «Типовое содержание технического обоснования безопасности реакторных установок»; ПНАЭ Г-5-006-87 «Нормы проектирования сейсмостойких атомных станций»; ПНАЭ Г-7-013-89 «Правила устройства и безопасной эксплуатации исполнительных механизмов органов воздействия на реактивность»; ПНАЭ Г-10-021-90 «Правила устройства и эксплуатации локализирующих систем безопасности атомных станций» и др.

Резюме. Требования к исходным материалам, конструктивным решениям, различного рода сооружениям, физическим барьерам и уровням защиты, к предельным уровням аварийного выброса реактора и радиационного воздействия на население, а также к локализирующим системам регламентированы нормативными документами, в том числе в вероятностном выражении на уровне норм радиационной и ядерной безопасности

Эффективное управление рисками для особого рода воздействий с высокой степенью неопределенности возможно и целесообразно на основе:

- рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности составных компонентов и системы в целом;
- рационального применения мер противодействия рискам с использованием эффективных физических барьеров и организационно-технических уровней защиты и способов избегания рисков ситуаций

Женевский протокол от 1925 года, Конвенции, Положения, Постановления Правительства РФ

Системные требования изложены в:

Женевском протоколе от 1925 года о запрещении применения на войне удушливых, ядовитых или других подобных газов и бактериологических средств, Конвенции о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничтожении (1972 г.), Конвенции о биологическом разнообразии (1992 г.), «Положении об осуществлении контроля за внешнеэкономической деятельностью в отношении возбудителей заболеваний (патогенов) человека, животных и растений, генетически измененных микроорганизмов, токсинов, оборудования и технологий», утвержденное Постановлением Правительства РФ от 29.08.2001г. № 634, Концепции федеральной целевой программы "Национальная система химической и биологической безопасности Российской Федерации (2009 - 2013 годы)", утвержденной распоряжением Правительства РФ от 28.01.2008 г. № 74-р

Резюме. В общем случае нормативные количественные требования к допустимым уровням рисков и безопасности на сегодня не выработаны. Для обеспечения химической и биологической безопасности объективно необходимо развитие критериев и методической базы по определению и категорированию уровней опасности объектов, территорий и природных явлений, обоснование нормативов

Эффективное управление рисками возможно и целесообразно на основе:

- рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности составных компонентов и системы в целом (включая население и другие объекты биосферы, техносферу);
- рационального применения мер избегания рисков ситуаций и противодействия рискам с использованием эффективных мер, направленных на своевременное выявление угроз, повышение надежности функционирования опасных объектов и технического оборудования, модернизацию систем контроля, управления (в том числе автоматической противоаварийной защиты технологических процессов и обеспечения физической защиты опасных объектов), предупреждение возникновения источников и очагов химического и биологического поражения (заражения), нейтрализации воздействия источников химической и биологической опасности, а также применение комплексных средств индивидуальной и коллективной защиты людей и средств спасения в условиях чрезвычайной опасности

Сравнительный анализ нормативно-правовой базы (продолжение)

Международные конвенции и кодексы, документы ИКАО, Закон РФ «О транспортной безопасности», Воздушный кодекс РФ

Системные требования изложены в:

Международной конвенции по охране человеческой жизни на море (МК СОЛАС-74) и Международном кодексе по охране судов и портовых средств (Кодекс ОСПС), Regulation (EC) N 725/2004 и Directive 2005/65/EC, документах Международной организации гражданской авиации ИКАО (Требования к личному составу гражданской авиации при выдаче свидетельства, Правила полетов, Метеорологическое обеспечение международной авиации, Аэронавигационные карты, Единичные измерения, подлежащие использованию в воздушных и наземных операциях, Эксплуатация воздушных судов, Государственные и регистрационные знаки воздушных судов, Летная годность воздушных судов, Упрощение формальностей при международных воздушных перевозках, Авиационная электросвязь, Обслуживание воздушного движения, Поиск и спасение, Расследование летных происшествий, Аэродромы, Службы аэронавигационной информации, Охрана окружающей среды, Защита Международной гражданской авиации от актов незаконного вторжения, Безопасная перевозка опасных грузов по воздуху), документах Воздушного кодекса РФ и Федеральной системы обеспечения защиты деятельности гражданской авиации от актов незаконного вмешательства (в т.ч. «Руководства по досмотру членов экипажей, обслуживающего персонала, пассажиров, ручной клади и багажа, грузов, бортовых пасов», «Положения о пропуском и внутриобъектовом режиме в аэропортах, авиапредприятиях, организациях и учреждениях гражданской авиации», «Типового положения о службе авиационной безопасности аэропортов» и «Типового положения о службе авиационной безопасности эксплуатантов и организаций гражданской авиации», «Памяти экипажу воздушного судна по действиям в чрезвычайной обстановке» и др.)

Резюме. Сформированное множество угроз нарушения авиационной безопасности является основой для принятия конкретных мер по снижению рисков, это множество расширяется исходя из практического опыта и актов незаконного вмешательства. В отличие от устоявшегося множества опасных производственных факторов в промышленности множество угроз и сценариев нарушения транспортной безопасности на количественном уровне окончательно не сформировано. В общем случае нормативные количественные требования к допустимым уровням рисков и безопасности на сегодня не выработаны

Эффективное управление рисками возможно и целесообразно на основе: рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности; рационального применения мер противодействия рискам (включая избегание рисков ситуаций)

Закон РФ «О противодействии терроризму», «Концепция безопасности Москвы» и др.

Системные требования изложены в:

ГОСТ Р 22.1.12-2005 «Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений»; МГСН 1.01-99 «Нормы и правила проектирования планировки и застройки г. Москвы», МГСН 1.04-2005 «Временные нормы и правила проектирования планировки и застройки участков территории высотных зданий-комплексов, высотных градостроительных комплексов в городе Москве», МГСН 4.04-94 «Многофункциональные здания и комплексы», МГСН 4.19-2005 «Временные нормы и правил проектирования многофункциональных высотных зданий и зданий-комплексов в г. Москве», СП 11-107-98 «Порядок разработки и состав раздела "Инженерно-технические мероприятия гражданской обороны. Мероприятия по предупреждению чрезвычайных ситуаций" проектов строительства»; СНиП 2.01.51-90 «Инженерно-технические мероприятия гражданской обороны»; СНиП 2.08.02-89 «Общественные здания и сооружения», СНиП 31-01-2003 «Здания жилые многоквартирные», СНиП 31-03-2001 «Производственные здания», СНиП 31-05-2003 «Общественные здания административного назначения», СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование», СНиП 23-01-99 Строительная климатология; СНиП II-3-79 Строительная теплотехника; ПБ 12-529-03 «Правила безопасности систем газораспределения и газопотребления», СанПиН 2.1.2.1002-00 «Санитарно-эпидемиологические требования к жилым зданиям и помещениям», «Методики оценки систем безопасности и жизнеобеспечения на потенциально опасных объектах, зданиях и сооружениях» и др.

Резюме. В общем случае нормативные количественные требования к допустимым рискам формулируются в косвенной форме выполнения конкретных условий. Нормативные количественные требования к допустимым рискам в вероятностном выражении на сегодня не выработаны.

Эффективное управление рисками возможно и целесообразно на основе: выполнения задаваемых нормативных требований и условий; рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности важных объектов; рационального применения мер противодействия рискам (включая избегание рисков ситуаций)

Законы РФ «Об охране окружающей среды», «О гидrometeorологической службе», «Об охране атмосферного воздуха», «О животном мире», «О недрах», «Об экологической экспертизе» и др.

Системные требования изложены в:

Земельном кодексе, Водном кодексе, Градостроительном кодексе РФ, Федеральных законах РФ, ГОСТ 2874-82 «Показатели санитарного состояния природных вод», ГОСТ 17.1.3-07-82 «Охрана природы. Гидросфера. Правила контроля качества воды водоемов и водотоков», ГОСТ 17.1.3-08-82 «Охрана природы. Гидросфера. Правила контроля качества морских вод», ГОСТ 17.2.3.01-86 «Охрана природы. Гидросфера. Правила контроля качества воздуха населенных пунктов», РД 39-018-90 «Временная инструкция о порядке проведения оценки воздействия на окружающую среду при разработке проектов обустройства морских месторождений углеводородов», РД 52.04.167-88 «Руководство по контролю загрязнения атмосферы», РД 52.04.576-97 «Положение о методическом руководстве наблюдениями за состоянием и загрязнением окружающей природной среды. Общие требования», «Положение о порядке осуществления государственного мониторинга состояния недр. МПР РФ. М: 2001», СП 11-102-97 «Инженерно-экологические изыскания для строительства» и др.

Резюме. В общем случае нормативные количественные требования к допустимым рискам формулируются чаще всего в косвенной форме выполнения конкретных условий, в количественном виде – на уровне частоты наступления потенциально опасных событий. Нормативные количественные требования к допустимым рискам в вероятностном выражении на сегодня не выработаны

Эффективное управление рисками возможно и целесообразно на основе: выполнения задаваемых условий обращения с природой; рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности природной среды; рационального применения мер противодействия рискам (включая избегание рисков ситуаций)

Законы РФ «О государственной тайне», «Об информации, информационных технологиях и защите информации», «О коммерческой тайне», «О связи», Доктрина информационной безопасности и др.

Системные требования изложены в:

ГОСТ Р 51275 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества», ГОСТ 28147-1989 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования, ГОСТ Р 50739-95 «СВТ. Защита от НСД. Общие технические требования», ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство», ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения», ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования», РД Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации» – 1992, РД Гостехкомиссии России «СВТ. Межсетевые экраны» – 1997, нормативные документы ФСТЭК и др.; ГОСТ Р ИСО/МЭК 13335 «Информационная технология - Методы и средства обеспечения безопасности», ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью», ISO/IEC 21827 «Информационная технология – Инженерия безопасности систем – Модель функциональной завершенности», ISO/IEC TR 15443-2002 «Информационная технология – Методики обеспечения безопасности – Основы гарантий безопасности информационных технологий» ISO/IEC TR 15947-2002 «Информационная технология – Методики обеспечения безопасности – Основы обнаружения вторжений в области информационных технологий» и др.

Резюме. В отличие от промышленной безопасности в общем случае требования к допустимым рискам формулируются в форме требований к выполнению конкретных условий. Количественные требования к допустимым рискам в вероятностном выражении на сегодня не выработаны (за исключением вероятностных требований по стандарту ГОСТ РВ 51987)

Эффективное управление рисками возможно и целесообразно на основе: рационального применения адекватной системы ситуационного анализа потенциально опасных событий, эффективных способов контроля и мониторинга состояний и оперативного восстановления целостности компонентов, объекта и системы; рационального применения мер противодействия рискам (включая избегание рисков ситуаций)

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

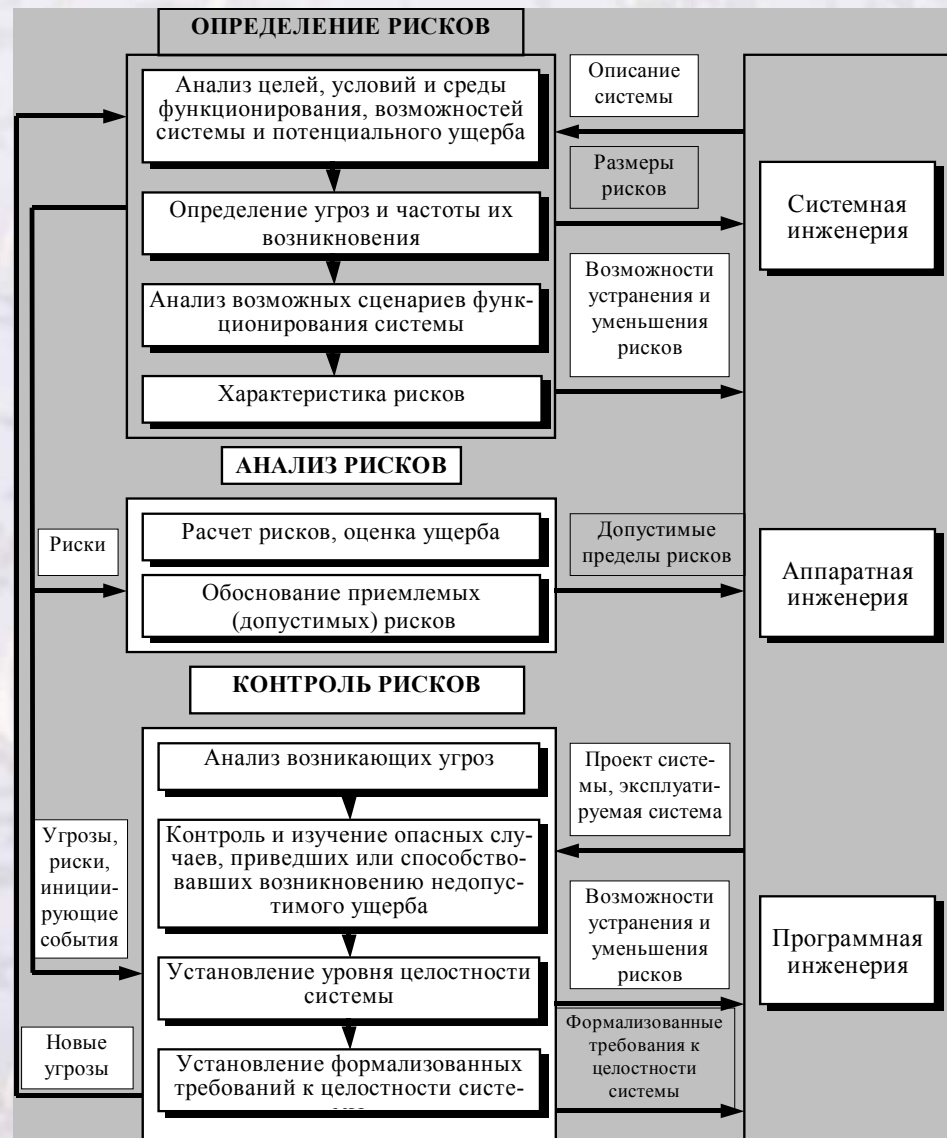
Транспортная безопасность

Авиационная безопасность

**Безопасность высотных
зданий**

**Информационная
безопасность**

и др.



ВЫВОДЫ по результатам анализа нормативно-правовых документов по безопасности

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
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

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

Пример процесса управления информацией

- Цель процесса управления информацией**
своевременное предоставление заинтересованным сторонам необходимой полной, достоверной и, если требуется, конфиденциальной информации в точной 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 "своей", 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 (аналоговой, цифровой, графической и т.д.) и может быть сохранена, обработана, преобразована и передана при помощи любых средств (персонального компьютера, мобильного устройства, оптического). Необходимо учитывать ограничения конфиденциальности, например, инфраструктуру, организационные аспекты, распределение работы над проектом. События и события, касающиеся критичной, преобразованной, переданной и предоставленной информации, используются в соответствии с политикой организации, соответствующими и/или законодательными требованиями и/или стандартами.

получать идентифицированные элементы информации;
Примечание - События относятся к формированию информации или ее сбору от соответствующих источников; обслуживать элементы информации и хранящиеся записи этих в соответствии с требованиями к целостности, защите и сохранению тайны.

определять меры по сохранению информации;
Примечание - К ним относятся анализ статуса критичной информации и отклонения от целостности, достоверности, доступности и любых потребностей в информации или передаче ее инфраструктурной поддержке. В случае изменения технологии следует рассмотреть варианты: либо сохранить инфраструктуру так, чтобы данные были доступны, либо "мгновенно" скопировать информацию в другую инфраструктуру, либо использовать другие методы.

аудитировать заданную информацию в соответствии с целями аудита и сохранения знаний;
Примечание - Необходимо выбирать методы, инструменты, критерии и способы защиты информации в соответствии с обоснованными и стандартизированными периодами хранения и восстановления информации, политикой организации, соответствующими и/или законодательными требованиями.

Задачи, решаемые на основе математического моделирования
 Анализ качества процессов представления информации (Надежность, Своевременность)
 Анализ качества используемой информации (Полнота, Актуальность, Безопасность после контроля, Корректность после обработки, Конфиденциальность)
 Анализ безопасности функционирования системы (Безопасность действий человека, Защищенность от внешних воздействий, Защищенность от несанкционированного доступа)



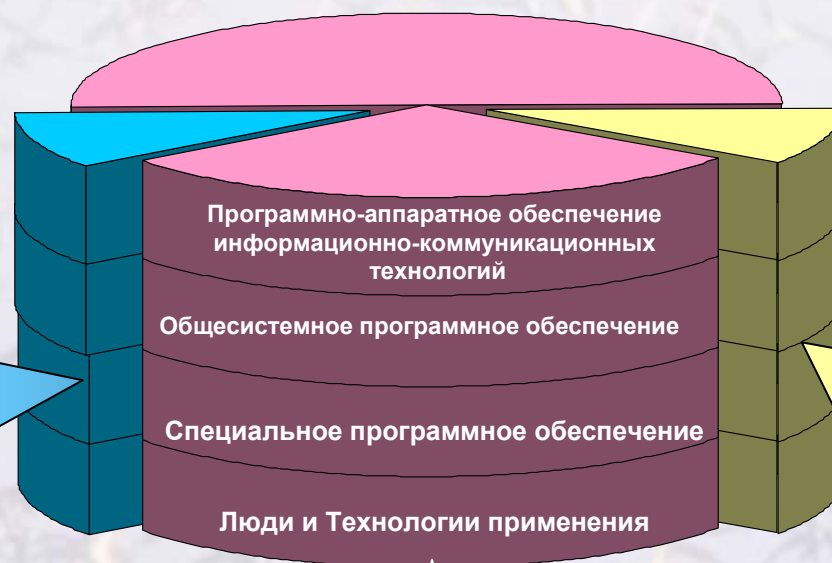
Пример формализации



Построение и развитие сложных систем базируется на системном анализе

Что реально делается и что не делается для информационных систем ?

Надёжные и временные характеристики задаются и оцениваются Главными конструкторами количественно



Степень безопасности информации оценивается на качественном уровне Испытательными лабораториями ФСБ, ФСТЭК, Минобороны РФ (количественно НЕ оценивается)

Затраты на качество и безопасность



Как количественно обосновать

$P=?$? $R=?$

Источник поисковых идей – в результатах применения комплексов КОК, КОК+, «Управление рисками» и др.



Модели и инструментари являются методологической основой деятельности ряда НИИ и испытательных лабораторий (НИИПМС, ИПИ РАН, АНО «Инфостандарт», 3 ЦНИИ Минобороны, Международного центра по информатике и электронике, ЦИТИС, РАРАН, РГУ нефти и газа им. И.М. Губкина и др.)

С 2000г. применение позволило существенно сократить риски и неоправданные затраты и повысить степень научной обоснованности технических решений

Развитие математических моделей 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.

Системное улучшение системы менеджмента качества

Процессы жизненного цикла систем

Процессы	Инициация Целевые требования Планирование
жизненного	Планирование Процессы управления качеством Процессы управления рисками Процессы управления проектами Процессы управления ресурсами Процессы управления финансами Процессы управления персоналом Процессы управления информацией
цикла	Планирование проекта Процессы организационного управления Процессы управления качеством Процессы управления рисками Процессы управления проектами Процессы управления ресурсами Процессы управления финансами Процессы управления персоналом Процессы управления информацией
систем	Планирование проекта Процессы организационного управления Процессы управления качеством Процессы управления рисками Процессы управления проектами Процессы управления ресурсами Процессы управления финансами Процессы управления персоналом Процессы управления информацией

Основная идея оценки информационных систем по ГОСТ РВ 51987
 «Требования и оценка качества функционирования информационных систем»

и др.



ПРОГРАММНЫЕ КОМПЛЕКСЫ

100 МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ПРОЦЕССОВ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ



Содержание программных комплексов в поддержку системообразующих стандартов



2004 - 2008

ПРИОБРЕТЕНИЕ	ПОСТАВКА	ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ	УПРАВЛЕНИЕ ПРОЕКТОМ	УПРАВЛЕНИЕ РИСКАМИ	УПРАВЛЕНИЕ КАЧЕСТВОМ	УПРАВЛЕНИЕ КОММУНИКАЦИЕЙ	УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ
ПЛАНИРОВАНИЕ ПРОЕКТА	ОЦЕНКА ПРОЕКТА	КОНТРОЛЬ ПРОЕКТА	ПРИНЯТИЕ РЕШЕНИЯ	УПРАВЛЕНИЕ РИСКАМИ	УПРАВЛЕНИЕ КАЧЕСТВОМ	УПРАВЛЕНИЕ КОММУНИКАЦИЕЙ	УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ
ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ ЗАКАЗЧИКА	АНАЛИЗ ТРЕБОВАНИЙ ЗАКАЗЧИКА	ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ	ЧЕЛОВЕЧЕСКИЙ ФАКТОР	РЕАЛИЗАЦИЯ ПРОЕКТА	ИНТЕГРАЦИЯ	ВЕРИФИКАЦИЯ	ПЕРЕДАЧА ЗАКАЗЧИКУ
ВЕРИФИКАЦИЯ	ПЕРЕДАЧА ЗАКАЗЧИКУ	ВАЛИДАЦИЯ	ФУНКЦИОНИРОВАНИЕ	ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ	СПИСАНИЕ	ВЕРИФИКАЦИЯ	ПЕРЕДАЧА ЗАКАЗЧИКУ

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 $T_{зад.}$, если на них достигается минимум затрат на создание системы $Z_{созд.}$ при ограничениях на приемлемый уровень качества $R_{доп.}$ и допустимый уровень затрат при эксплуатации $S_{доп.}$:

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

управляемые
параметры A, M

при ограничениях $R_{кач.} \geq R_{доп.}$ и $S_{экспл.} \leq S_{доп.}$ и, возможно, ограничениях на допустимые значения других показателей, отнесенных к критичным

Управляемые параметры процесса $Q(A, M)$ признаются наиболее рациональными для заданного периода эксплуатации $T_{зад.}$, если на них достигается максимум качества функционирования системы $R_{кач.}$.

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

управляемые
параметры A, M

при ограничениях $S_{экспл.} \leq S_{доп.}$ 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 Tзад., если на них достигается минимум затрат на создание системы Zсозд. при ограничениях на приемлемый уровень риска Rдоп и допустимый уровень затрат при эксплуатации Cдоп.:

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

управляемые
параметры A,M

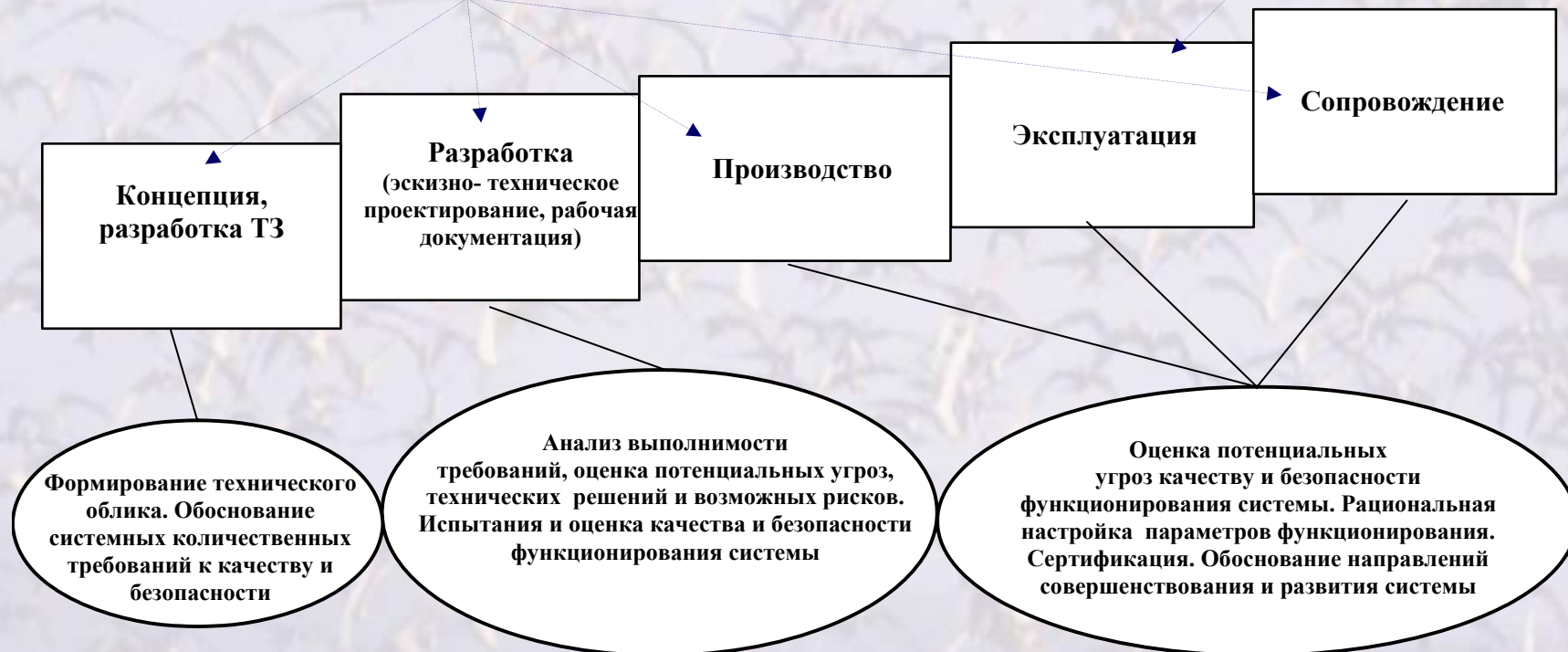
при ограничениях $R \leq R_{\text{доп.}}$ и $C_{\text{экспл.}} \leq C_{\text{доп.}}$ и, возможно, ограничениях на допустимые значения других показателей, отнесенных к критичным

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

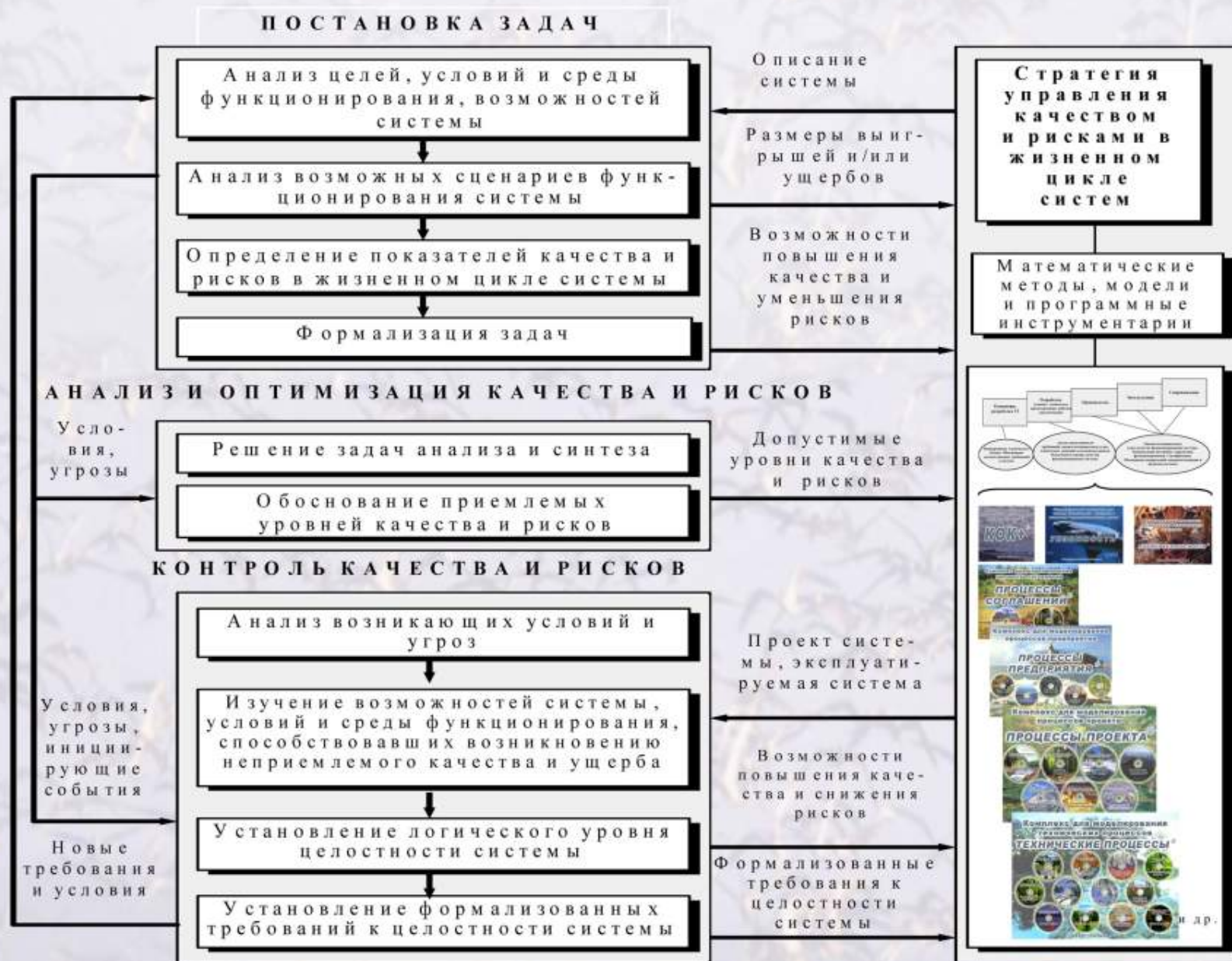
$$R(Q_{\text{рац.}}) = \min_{\text{управляемые параметры A,M}} R(Q)$$

управляемые
параметры A,M

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



Контроль и оптимизация

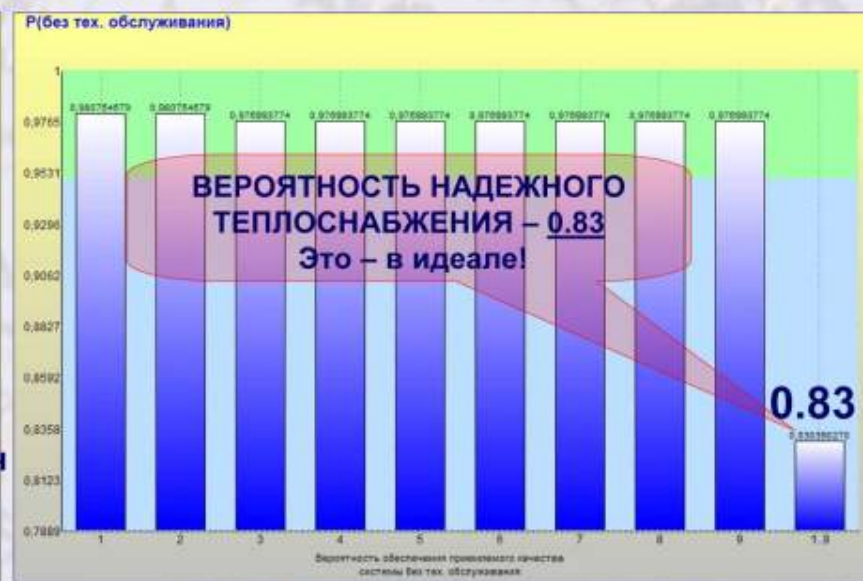


A large number of birds, possibly terns, are captured in flight against a pale, clear sky. The birds are scattered across the entire frame, creating a sense of a massive flock. The word "Примеры" is overlaid in the center in a bold, dark blue font with a subtle drop shadow.

Примеры

Анализ надежности теплоснабжения - 1

Оценки идеальной системы
централизованного теплоснабжения
в течение отопительного сезона



1-й КОМПОНЕНТ – ИДЕАЛЬНЫЕ КОТЕЛЬНЫЕ, 2-й –ЦЕНТРАЛЬНЫЙ ТЕПЛОВЫЙ ПУНКТ И НАДЗЕМНЫЕ БОЙЛЕРНЫЕ УСТАНОВКИ; КОМПОНЕНТЫ С 3-ГО ПО 8-Й - ЭТО С 1-ГО ПО 7-Й ЛУЧИ ТЕПЛОТРАССЫ, 9-Й КОМПОНЕНТ ХАРАКТЕРИЗУЕТ НАРАБОТКУ НА ПОВРЕЖДЕНИЕ ВСЕЙ СЕТИ ТЕПЛОСНАБЖЕНИЯ

Анализ надежности теплоснабжения - 2

Оценки существующей системы централизованного теплоснабжения БЕЗ РЕЗЕРВИРОВАНИЯ ЛУЧЕЙ ТЕПЛОСЕТИ



С РЕЗЕРВИРОВАНИЕМ ЛУЧЕЙ ТЕПЛОСЕТИ

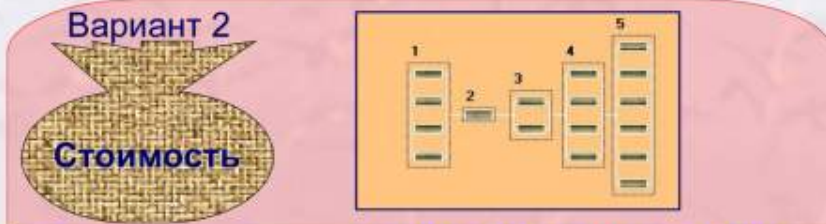
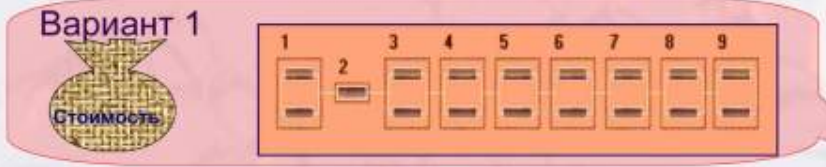


1-й КОМПОНЕНТ – ИДЕАЛЬНЫЕ КОТЕЛЬНЫЕ, 2-й –ЦЕНТРАЛЬНЫЙ ТЕПЛОВЫЙ ПУНКТ И НАДЗЕМНЫЕ БОЙЛЕРНЫЕ УСТАНОВКИ; КОМПОНЕНТЫ С 3-ГО ПО 8-Й - ЭТО С 1-ГО ПО 7-Й ЛУЧИ ТЕПЛОТРАССЫ, 9-Й КОМПОНЕНТ ХАРАКТЕРИЗУЕТ НАРАБОТКУ НА ПОВРЕЖДЕНИЕ ВСЕЙ СЕТИ ТЕПЛОСНАБЖЕНИЯ

Анализ надежности теплоснабжения - 3

Сравнительная оценка вариантов модернизации системы теплоснабжения

1- МОДЕРНИЗИРОВАННАЯ КОТЕЛНЯЯ «ТЕПЛОЦЕНТРАЛЬ» И НОВАЯ КОТЕЛНЯЯ;
 2- МОДЕРНИЗИРОВАННЫЕ ЦТП И НАДЗЕМНЫЕ БОЙЛЕРНЫЕ УСТАНОВКИ; С 3-ГО ПО 9-Й -
 ХАРАКТЕРИЗУЮТ С 1-ГО ПО 7-Й ЛУЧИ ТЕПЛОТРАССЫ (С УЧЕТОМ МОДЕРНИЗАЦИИ НАИБОЛЕЕ
 СТАРЫХ УЧАСТКОВ); 1.9 - ВСЯ СЕТЬ



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



Изначальные положения для создания методики: в силу случайного характера влияние опасных факторов и условий описывается в терминах случайных процессов. Применяемые способы снижения опасности направлены на своевременное вскрытие опасности, устранение или замедление ее развития и снижение ущерба; 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

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

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

Существующие модели и программные инструментари для расчетов

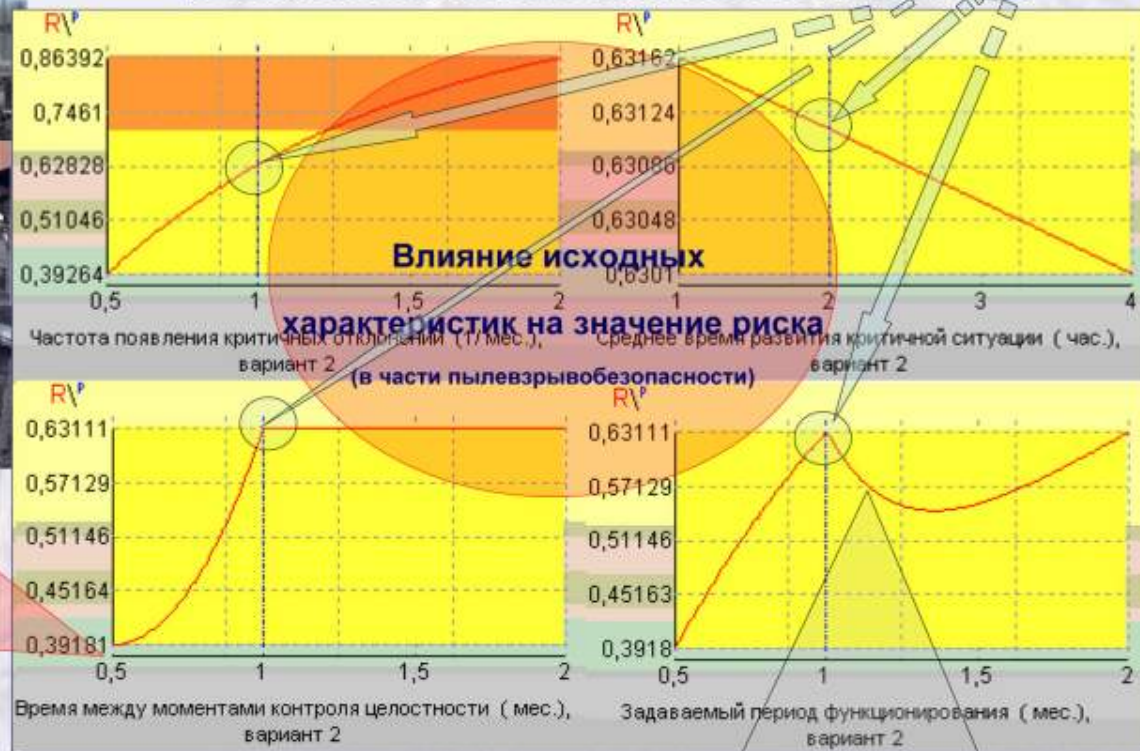


Анализ рисков в опасном производстве

Оценка частного риска неконтролируемого развития критических ситуаций



При сложившейся технологии мониторинга и контроля, проверок на местах и анализа данных на диспетчерском пункте управления риск неконтролируемого развития в течение месяца критических ситуаций, связанных с пылевзрывоопасностью, составляет **0.63**



При сокращении периода времени между моментами контроля за интенсивностью пылеотложения с месяца до двух недель риск неконтролируемого развития критических ситуаций в течение месяца существенно сократится - с 0.63 до 0.39, это - резервы управления (!)

Падение риска связано с тем, что диагностика проводится 1 раз в месяц. Сразу после диагностики целостность восстанавливается, что выражается в снижении риска

Прогнозные выводы: практически ежемесячно на шахте должны возникать (и скорее всего возникали) аварийные проблемы с кабельной сетью и электрооборудованием (риск до 0.983), обрушением пород (риск до 0.81), и нарушением допустимых условий обеспечения пылевзрывобезопасности (риск – 0.63)

Интегральная оценка рисков, затрат и математического ожидания ущерба

Исходные данные для 1-й компании

Уязвимость

Интегральная уязвимость

Варианты (j): 1

Ситуационный анализ

Характеристика системы

Количество событий, требующих анализа: 100000

Доля потенциально опасных событий: 5%

Скорость интерпретации: 100000

Частота возможных ошибок: 2 года

Допустимое время на интерпретацию событий: 1 мес.

Затраты на ситуационный анализ: 10 у.е.

Уязвимость

Интегральная уязвимость

Варианты (j): 1

Мониторинг и контроль

Частота появления критичных отклонений: 1500 год

Среднее время развития критичной ситуации: 4 года

Время между моментами системного контроля: 5 лет

Длительность системного контроля: 2 мес.

Наработка на ошибку: 3 года

Задаваемый период функционирования: 2 года

Затраты на мониторинг и контроль: 50 у.е.

Уязвимость

Интегральная уязвимость системы

Последовательные меры противодействия (m): 1 2 3 4 5 6 7

Меры противодействия

Характеристика мер противодействия

Время сохранения эффективности меры: 1 год 1 год 1 мин. 1 сут. 1 мес. 1 мес. 1 год

Время до очередного адекватного усиления: 3 года 3 года 5 лет 1 нед. 1 год 5 лет 5 лет

Период функционирования системы (для оценки):

Длительность периода потенциальной опасности: 2 года

Характеристика затрат

Затраты на меры противодействия рискам: 2 у.е. 2 у.е. 2 у.е. 2 у.е. 2 у.е. 2 у.е. 2 у.е.

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

Применяются 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)

Задаваемые размеры потенциальных ущербов

Возможные варианты ущербов	
1. Ущерб при своевременном распознавании опасности, эффективных мерах контроля и безуспешном противодействии рискам	10
2. Ущерб при своевременном распознавании опасности, неэффективном контроле системы, но эффективных мерах противодействия	10
3. Ущерб при своевременном распознавании опасности, неэффективном контроле системы и безуспешном противодействии рискам	10
4. Ущерб при нераспознавании опасности, но эффективных мерах контроля и противодействия рискам	10
5. Ущерб при нераспознавании опасности, эффективных мерах контроля и безуспешном противодействии рискам	10
6. Ущерб при нераспознавании опасности, неэффективном контроле системы, но эффективном противодействии рискам	10
7. Ущерб при нераспознавании опасности, неэффективном контроле системы и безуспешном противодействии рискам	10



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

Результаты анализа для 1-й компании

Управление рисками

Случаи возникновения ущерба

1. Ущерб при своевременном распознавании опасности, эффективных мерах контроля и безуспешном противодействии рискам	0.0151916779483852
2. Ущерб при своевременном распознавании опасности, неэффективном контроле системы, но эффективных мерах противодействия	0.120820758713507
3. Ущерб при своевременном распознавании опасности, неэффективном контроле системы и безуспешном противодействии рискам	0.0857701251413891
4. Ущерб при нераспознавании опасности, но эффективных мерах контроля и противодействия рискам	0.01555660493441159
5. Ущерб при нераспознавании опасности, эффективных мерах контроля и безуспешном противодействии рискам	0.01078450535000315
6. Ущерб при нераспознавании опасности, неэффективном контроле системы, но эффективном противодействии рискам	0.0837611417244642
7. Ущерб при нераспознавании опасности, неэффективном контроле системы и безуспешном противодействии рискам	0.00195597539309166
Интегрально	0.3338400229614985

Ущерб

МОЖ ущерба равен 3.34 млн у.е. при риске 0.334

Затраты

Общие затраты 74 млн у.е.

Риски

Наибольший вес в уязвимость вносит неэффективный мониторинг и контроль

Затраты на ситуационный анализ (C1), мониторинг и контроль обеспечения безопасности (C2) и осуществление мер противодействия рискам (C3)

Риски негативного воздействия на систему

Интегральная оценка рисков, затрат и математического ожидания ущерба

Исходные данные для 2-й компании

Уязвимость

Интегральная уязвимость

Варианты (j): 1

Ситуационный анализ

Характеристика ситуации

Количество событий, требующих анализа: 100000

Доля потенциально опасных событий: 20 %

Характеристика применяемых мер

Скорость интерпретации: 100000 мс

Частота возможных ошибок: 2 год⁻¹

Допустимое время на интерпретацию событий: 1 мес.

Затраты на ситуационный анализ: 2 у.е.

Далее

Уязвимость

Интегральная уязвимость

Варианты (j): 1

Мониторинг и контроль

Характеристика применяемых мер

Частота появления критических отклонений: 1500 год⁻¹

Среднее время развития критической ситуации: 4 года

Характеристика применяемых мер

Время между моментами системного контроля: 5 лет

Длительность системного контроля: 2 мес.

Наработка на ошибку: 0,5 года

Период функционирования

Задаваемый период функционирования: 2 года

Затраты на мониторинг и контроль: 10 у.е.

Далее

Уязвимость

Интегральная уязвимость системы

Последовательные меры противодействия (m): 1 2 3 4 5 6

Меры противодействия

Характеристика мер противодействия

Время сохранения эффективности меры: 1 год 1 мин. 1 сут. 1 мес. 1 год

Время до очередного адекватного усиления: 3 года 5 лет 1 нед. 1 год 5 лет 5 лет

Период функционирования системы (для оценки)

Длительность периода потенциальной опасности: 2 года

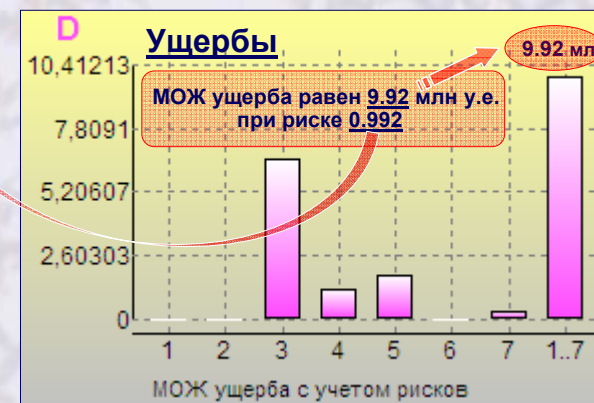
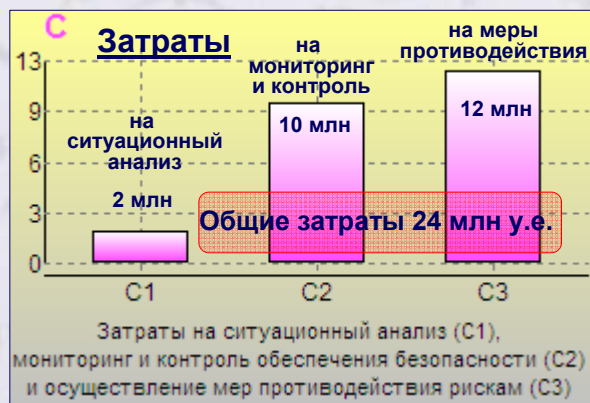
Характеристика затрат

Затраты на меры противодействия рискам: 2 у.е. 2 у.е. 2 у.е. 2 у.е. 2 у.е. 2 у.е.

Далее

Добавить Удалить Загрузить Сохранить Фото Назад

Результаты анализа для 2-й компании



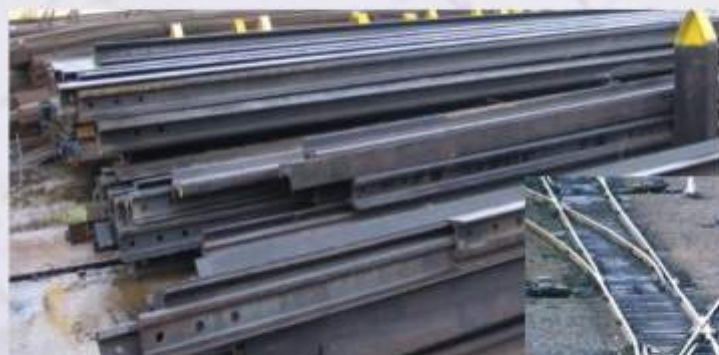
Окончательный вывод:

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

Примеры объектов неразрушающего контроля и диагностирования



Сравнение эффективности систем мониторинга состояний трубопровода



Интегральные результаты расчетов

Исходные данные
Риск скрытого внедрения и воздействия источников опасности

Варианты: 1 2 3 4 5 6

Мониторинг и контроль

Характеристики угрозы

Частота появления критических отклонений	1500 раз/г	1500 раз/г	1500 раз/г	1500 раз/г	1500 раз/г	1500 раз/г
Среднее время развития критической ситуации	2 года	2 года	2 года	2 года	2 года	2 года

Характеристика применяемых технологий мониторинга доступности

Время между моментами системного контроля	2 лет	3 лет	3 лет	3 лет	3 лет	3 лет
Длительность системного контроля	2 мес.	2 мес.	2 мес.	2 мес.	2 мес.	2 мес.
Нарастание на ошибку	0.5 года	0.5 года	0.5 года	0.5 года	0.5 года	0.5 года

Период функционирования системы (для оценки)

Задаваемый период функционирования	2 года	5 лет	10 лет	2 года	5 лет	10 лет
------------------------------------	--------	-------	--------	--------	-------	--------



При увеличении частоты регламентной системной диагностики каждого из проблемных участков с 1 до 2-х раз за 5 лет риск воздействия источника опасности в течение 5 лет снижается

для 1-й компании с 0.42 до 0.16,

для 2-й компании – с 0.67 до 0.39

Увеличение вдвое количества скрытых дефектов принципиально не повлияет на значение риска

При сокращении вдвое среднего времени развития критической ситуации риск воздействия источника опасности в течение 5 лет возрастет для 1-й компании с уровня 0.42 до 0.60, а для 2-й компании – с уровня 0.67 до 0.89

Оценка экологической безопасности региона



Расчетные риски нарушения экологической безопасности региона в течение 5 лет (станции наблюдения: 1-й категории, 2-й категории)

Уязвимость

Риск

Варианты (1-8)

Мониторинг и контроль

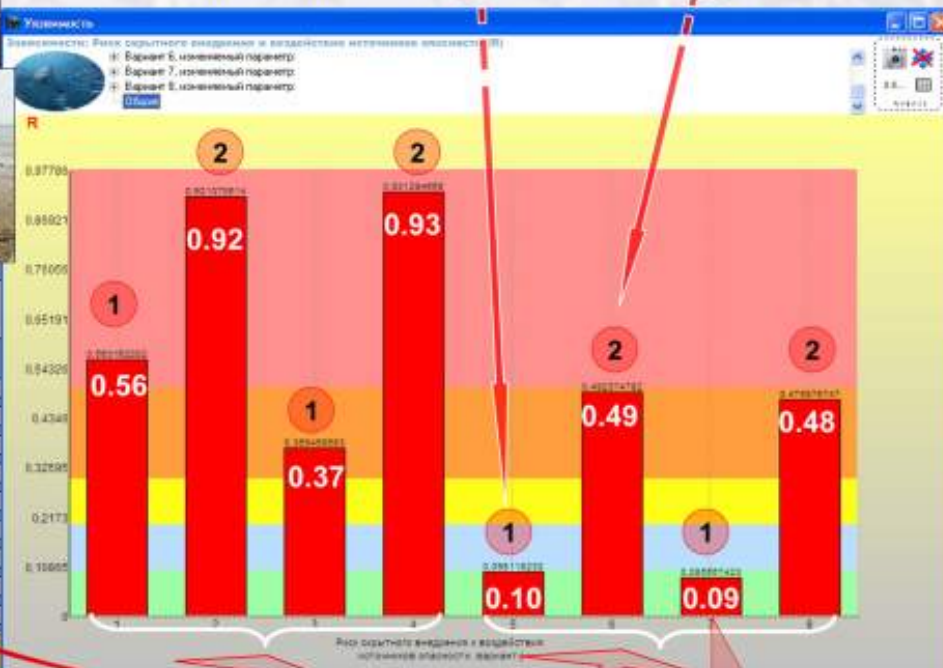
Характеристика угрозы	1-я технология (устаревшая)	2-я технология (современная)
Частота появления критичных отклонений	0.5 мес ⁻¹	1 мес ⁻¹
Среднее время развития критичной ситуации	3 мес	1 год
Характеристика применяемых технологий мониторинга: доступности и целостности		
Время между моментами системного контроля	10 сут	10 сут
Длительность системного контроля	10 сут	10 сут
Наработка на ошибку	0.5 года	0.5 года

Период функционирования системы (для оценки)

Задаваемый период функционирования	1 год	1 год	1 год	1 год	1 год	1 год	1 год
1 год	1 год	1 год	1 год	1 год	1 год	1 год	1 год

Увеличение частоты угроз вдвое увеличивает риск с 0.5 до 0.6

Длительность контроля от 0.5 до 2-х суток влияет незначительно!



Рекомендуется более частый контроль качества морских вод - до частоты контроля станциями 1-й категории (риск снижается с 0.5 до 0.3 и более)

Рекомендуется увеличение наработки на ошибку (риск снижается с 0.5 до 0.28 и более)

Эффективность работы станций 1-й категории при современной технологии мониторинга высока: риск не более 0.1 (!)

Анализ уязвимости нефтегазовых платформ - 1



Принципиальная особенность:

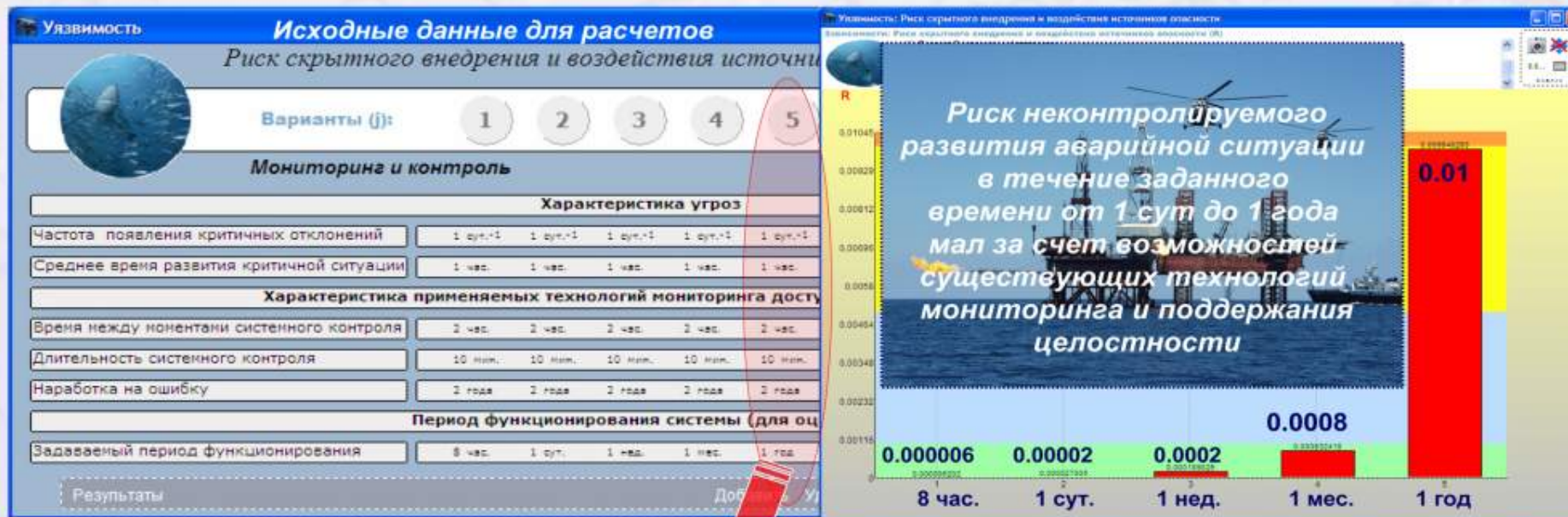
в отличие от суши проблемы безопасности должны разрешаться своими силами непосредственно в море, поскольку удаленность от берега и, возможно, ледовые условия для северных районов исключают помощь извне

Типовой состав НГС

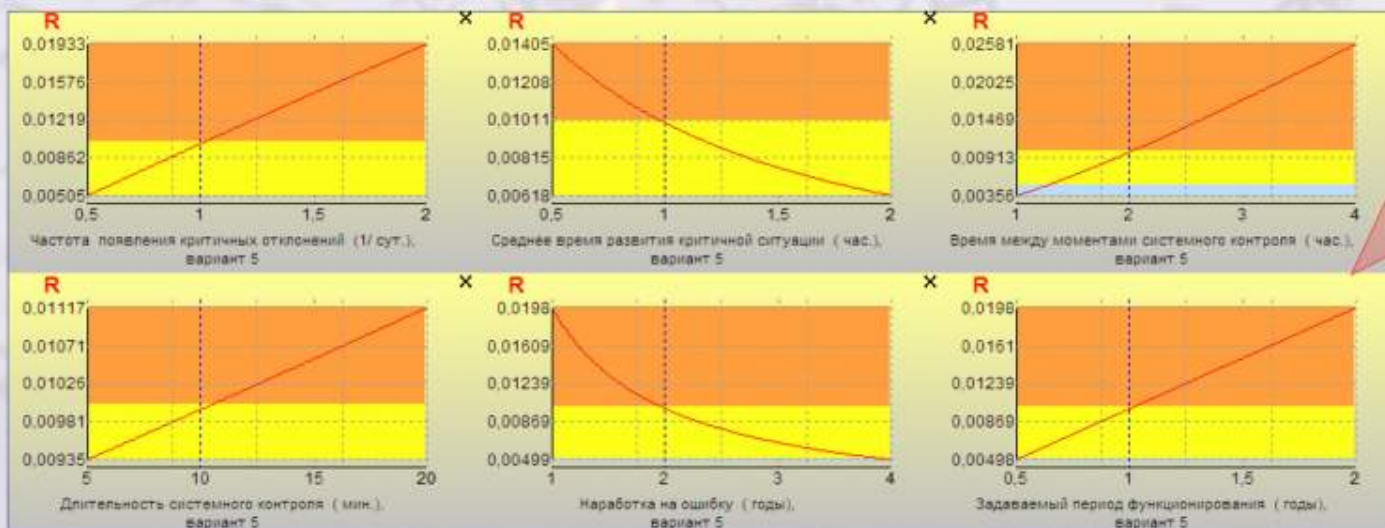


Анализ уязвимости нефтегазовых платформ - 3

Анализ существующих систем обеспечения аварийной безопасности



Зависимость риска неконтролируемого развития аварийной ситуации в течение года от изменения исходных данных

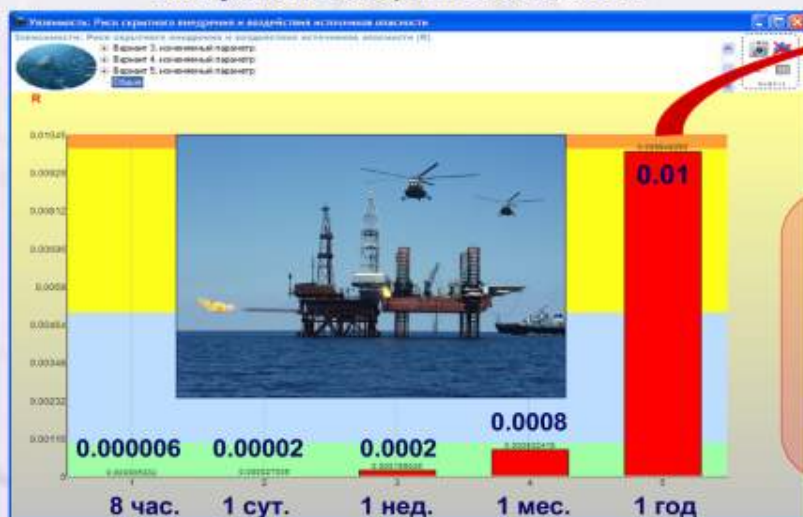


Достаточно высокая степень устойчивости: при изменении исходных данных в диапазоне -50% + 100% риск развития аварийной ситуации в течение года не превысит 0.026 (и то лишь в случае, если период между системными контролями будет увеличен с 2-х до 4-х часов)

Анализ уязвимости нефтегазовых платформ - 4

Анализ развития террористической опасности во внешних условиях, аналогичных характеристикам аварийной опасности

Риск неконтролируемого развития ситуации для условий аварийной опасности



Риск неконтролируемого развития ситуации для условий террористической опасности



Риски возрастают с 0.01 до 0.9998 вследствие недостаточной степени распознавания террористических угроз

Зависимость риска неконтролируемого развития ситуации в условиях террористических угроз в течение недели от изменения исходных данных



При изменении исходных данных в диапазоне -50% +100% риск неконтролируемого развития аварийной ситуации в течение недели колеблется в диапазоне 0.22 - 0.70

Резюме: ожидаются несоизмеримо более высокие риски неконтролируемого развития ситуаций, что означает явную уязвимость НГС в условиях террористических угроз

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. Ограждаемая территория со сменной охраной	через 2 часа	30 мин.	Скрытое проникновение на территорию
2. Пропускная система в здании, где располагается ИС и рабочие места пользователей со сменной 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 сменной 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»©

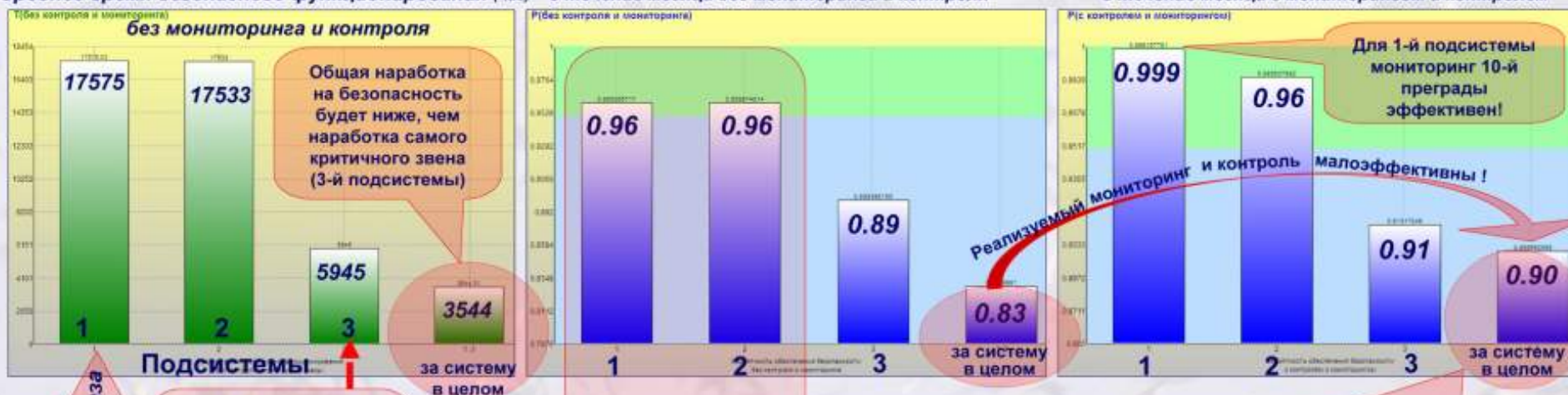


Прогноз информационной безопасности, выявление узких мест

Вероятность обеспечения безопасного функционирования

Среднее время безопасного функционирования (час) в течение месяца без мониторинга и контроля

в течение месяца с мониторингом и контролем



Общая наработка на безопасность будет ниже, чем наработка самого критичного звена (3-й подсистемы)

Для 1-й подсистемы мониторинг 10-й преграды эффективен!

Реализуемый мониторинг и контроль малоэффективны!

больше в 49.3 раза

3-я подсистема – наиболее узкое место в системе! Внутри нее узкими звеньями являются средства сбора, хранения и отображения данных

больше в 1.86 раза

1-я и 2-я подсистемы приблизительно равнозначны

В течение месяца преодоления всех преград исключены с вероятностью 0.9 (т.е. образно если сценарии угроз будут повторяться 100 месяцев, то около 90 месяцев из них информационная безопасность холдинга будет обеспечена)



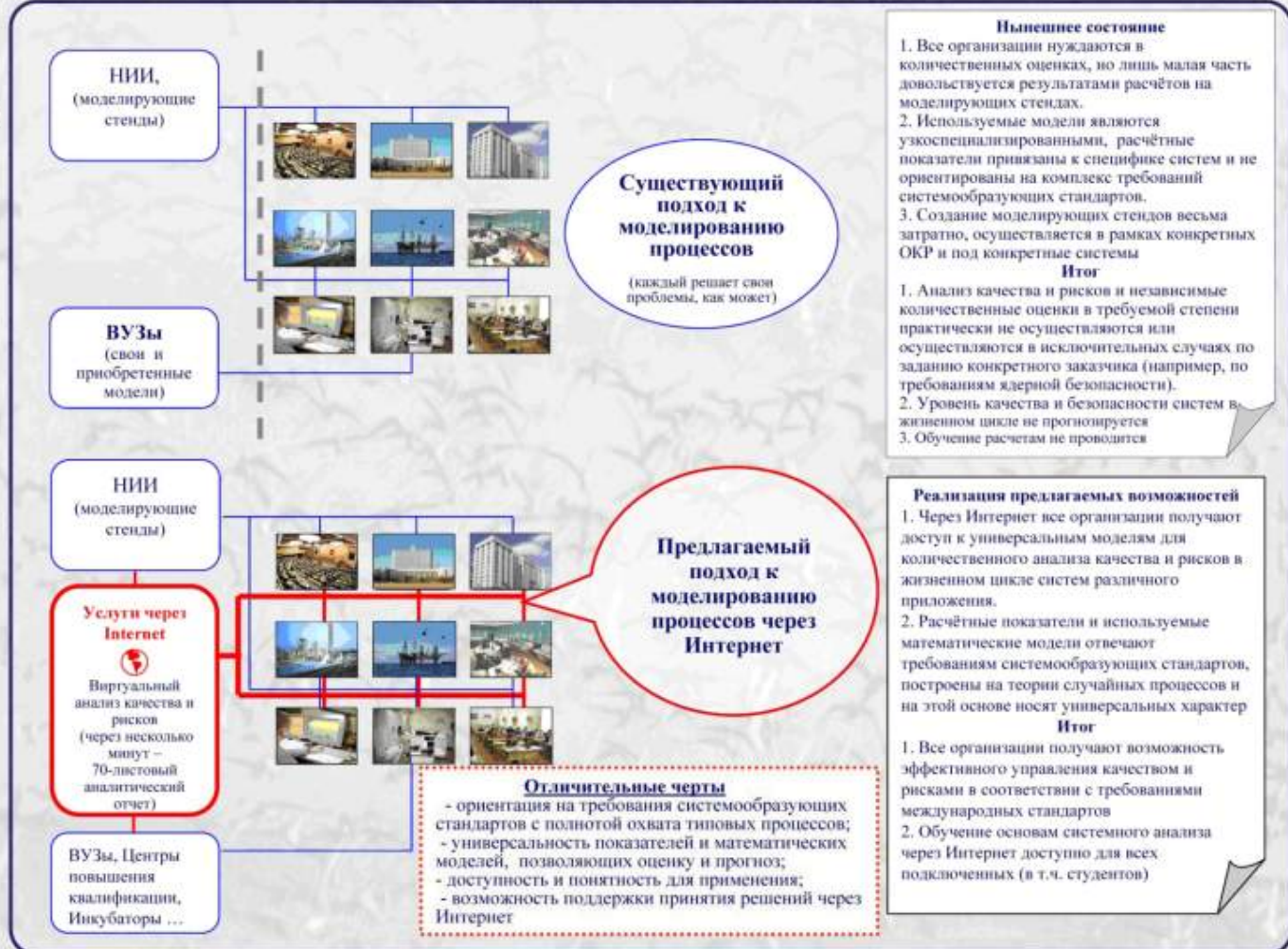
В течение многих лет редкий год обойдется без нарушения безопасности

В течение года вполне возможны несколько случаев преодоления преград

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



Место и суть виртуального моделирования через Интернет



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 расчётам не проводится

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 несут универсальный 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)

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

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



КОСТОГРЫЗОВ АНДРЕЙ ИВАНОВИЧ
заслуженный деятель науки РФ, доктор технических наук,
профессор, член-корреспондент РАН и РАЕН, действительный
член Академии информатизации образования



СТЕПАНОВ ПАВЕЛ ВЛАДИМИРОВИЧ
доктор технических наук, профессор, действительный член
Академии проблем качества, гранд-доктор философии, профессор
европейской академии



АВТОРСКИЕ ПУБЛИКАЦИИ,
ПОДЪЯВЛЕННЫЕ В ОБЛАСТИ
ПРЕДВАГАЕМЫХ
ИННОВАЦИИ

ИННОВАЦИОННОЕ УПРАВЛЕНИЕ КАЧЕСТВОМ И РИСКАМИ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ

А.И. Костогрызов, П.В. Степанов



ИННОВАЦИОННОЕ УПРАВЛЕНИЕ КАЧЕСТВОМ И РИСКАМИ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО
ДЛЯ СИСТЕМНЫХ АНАЛИТИКОВ

(современные стандарты и идеи системной инженерии, математические модели, методы, методики и программно-инструментальные комплексы для системного анализа, в т.ч. доступные на уровне высокоэффективной Интернет-технологии, примеры приложений с объяснением логики достигаемых результатов, полезные практические рекомендации)

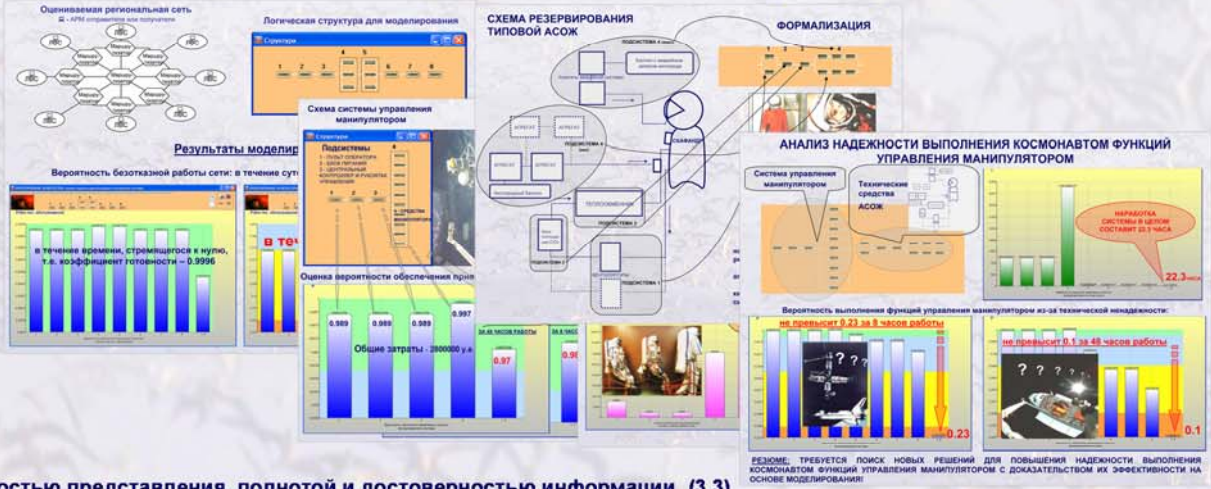


Схема решения задач (3.1)

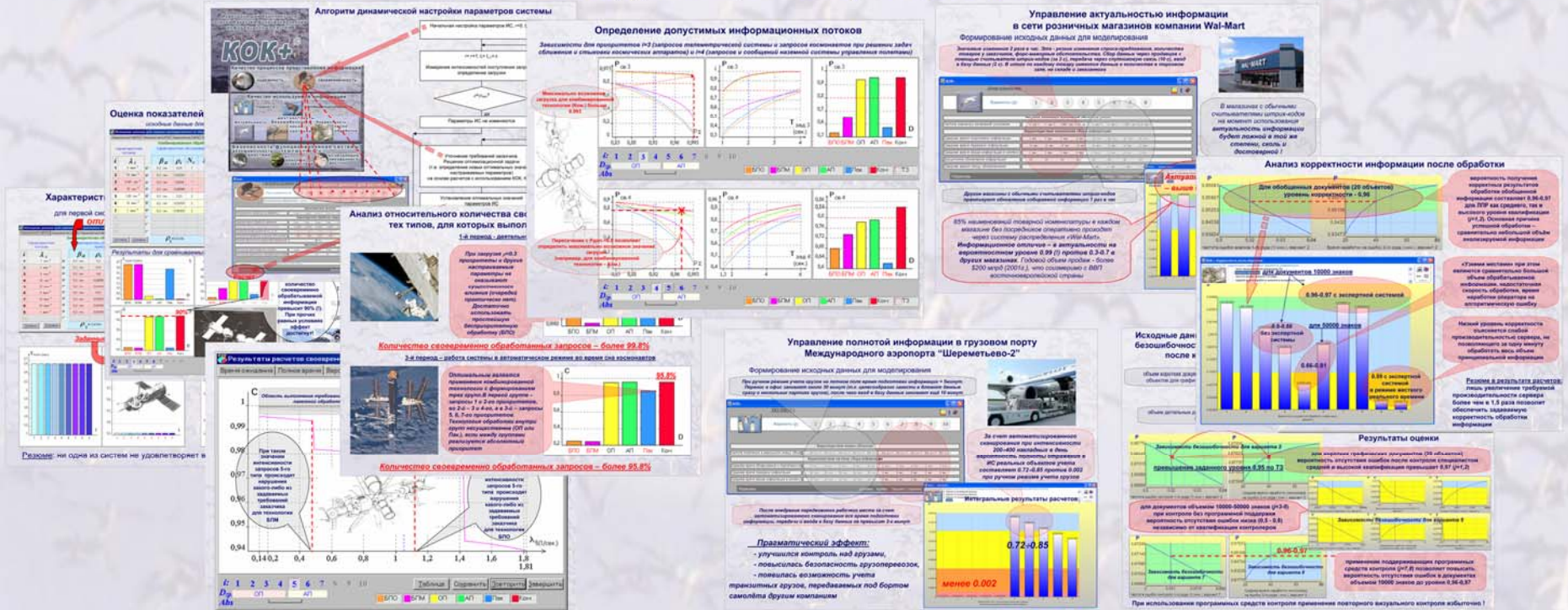


Практические примеры

Примеры анализа безотказности функционирования (3.2)



Примеры управления своевременностью представления, полнотой и достоверностью информации (3.3)



Практические примеры

Примеры сравнения защищенности информации в открытой и закрытой сетях (3.4)

Исходные данные

Исходные потоки и времена обработки	Исходные потоки	Время обработки
1	1000	1.0
2	2000	2.0
3	3000	3.0
4	4000	4.0
5	5000	5.0
6	6000	6.0
7	7000	7.0
8	8000	8.0
9	9000	9.0
10	10000	10.0

Результаты атаки

Обоснование требований к сложности шифра для обеспечения перехода карантина судов в период Второй мировой в

Оценка защищенности от НСД и сохранения конфиденциальности информации

Обоснование максимально допустимого периода объём при 97 разрядности шифрования по эмпирической шкале

Вероятность обеспечения защищенности от НСД

Адекватный учет периода обкатки и информационных ресурсов на сис

Необходимый успешный период РС-17 был в требуемая расшифровки месяцев, т.е. 1.4

Математическое моделирование

Достижимые вероятностно-временные

Для обеспечения максимальной защищенности в режиме P_пред = 0.90

Среднее время обработки

Требуются средние время прохождения трафика на уровне 14 - 27 лет

32 месяца

Модель нарушителя и преграды НСД для системы сложной структуры

табл. 3.4.1 и 3.4.2

Параметры	Число элементов системы	Число связей	Число уровней	Число узлов	Число каналов	Число точек доступа	Число точек контроля	Число точек защиты	Число точек обнаружения	Число точек реагирования	Число точек восстановления
1	1000	1000	10	1000	1000	1000	1000	1000	1000	1000	1000
2	2000	2000	20	2000	2000	2000	2000	2000	2000	2000	2000
3	3000	3000	30	3000	3000	3000	3000	3000	3000	3000	3000
4	4000	4000	40	4000	4000	4000	4000	4000	4000	4000	4000
5	5000	5000	50	5000	5000	5000	5000	5000	5000	5000	5000
6	6000	6000	60	6000	6000	6000	6000	6000	6000	6000	6000
7	7000	7000	70	7000	7000	7000	7000	7000	7000	7000	7000
8	8000	8000	80	8000	8000	8000	8000	8000	8000	8000	8000
9	9000	9000	90	9000	9000	9000	9000	9000	9000	9000	9000
10	10000	10000	100	10000	10000	10000	10000	10000	10000	10000	10000

Прогноз информационной безопасности, выявление узких мест

Среднее время выполнения функциональных задач

Вероятность обеспечения безопасности функциональных задач

Системные до

А если ключи менять ежемесячно?

Эффект вылета по сравнению с 97-разрядным шифрованием по эмпирической шкале - обесценивание конфиденциальности с вероятностью 0.9999 против 0.995. Максимально допустимый период обкатки информационной защищенности - не менее 2 месяцев!

Для обеспечения функциональных систем и защиты информации, чтобы не подвергались бы разрывам. В исследуемых системах требуется мониторинг и контроль многоуровневый. Необходимо усиление обеспечения информационной безопасности в открытых сетях, когда нету технологии вычисления из стран

Примеры оценки эффективности технологий выявления закладок (3.5)

Примеры программных закладок

Идентификация, классификация, анализ

Идентификация, классификация, анализ

Оценка степени доверия к результатам проверки программы на закладки

Определение максимального объема исходных текстов программ для эффективного анализа без специальных инструментов

Определение максимального количества закладок (пока вероятность их гарантированного выявления будет не ниже 0.9)

Определение времени для гарантированного выявления закладок

Варианты 1-5 и 6-10 приблизительно равноэффективны. Срок проверки более 1 недели нецелесообразен, все проверки будут завершены в течение нескольких суток. Доля закладок от 0.1% до 1% также не оказывает влияния на эффективность, практически все закладки будут выявлены

Вывод: на практике эффективный анализ без специальных инструментов объемом в несколько тысяч функциональных пред

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

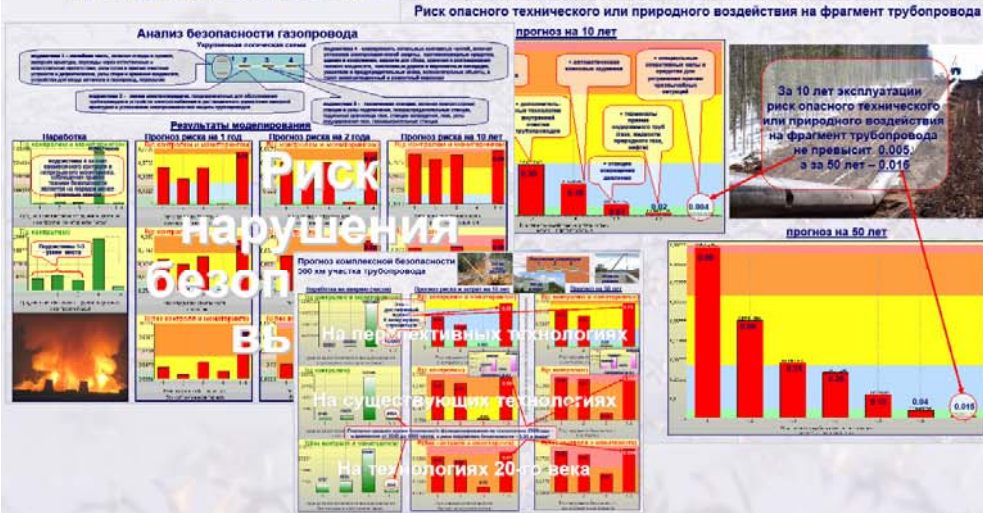
Варианты (n)	1	2	3	4	5	6
Объем проверяемой программы от 1000 до 2000 функций	1000	2000	3000	4000	5000	6000
Срок проверки	1 мин	2 мин	3 мин	4 мин	5 мин	6 мин
Доля закладок	0.1%	0.2%	0.3%	0.4%	0.5%	0.6%
Вероятность выявления	0.99	0.99	0.99	0.99	0.99	0.99

Исходные данные

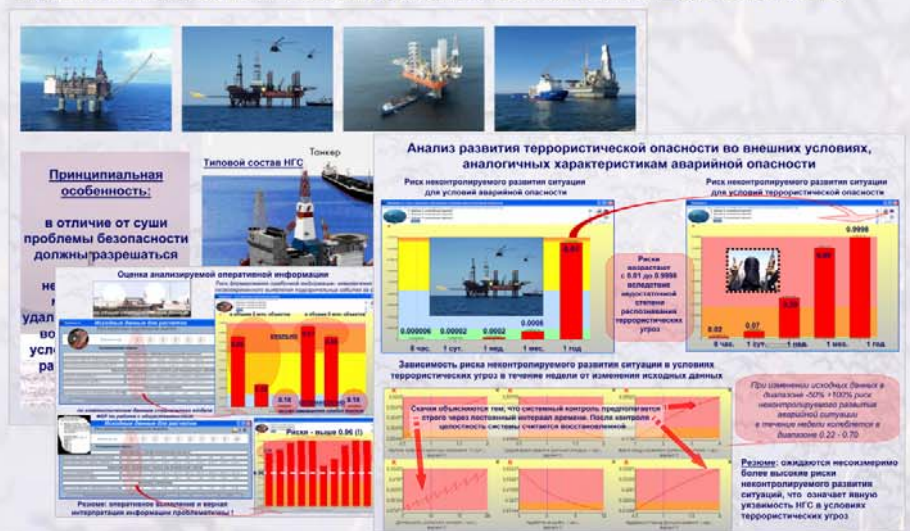
Варианты (n)	1	2	3	4	5	6
--------------	---	---	---	---	---	---

Практические примеры

Примеры прогнозирования безопасности функционирования трубопроводов (3.13)



Примеры анализа уязвимости морских нефтегазодобывающих систем (3.14)



Примеры выработка рекомендаций по повышению защищенности объектов (3.15)



Примеры исследования мер повышения безопасности авиapolетов (3.16)



Примеры анализа выборных технологий и ... защищенности политических лидеров... (3.17)



Исследования эффективности системы мер противодействия коррупции (3.18)



