Московский межотраслевой форум – 16 апреля 2013г.

Прогнозирование рисков и обоснование эффективных упреждающих мер в обеспечение комплексной безопасности

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

Общее

Сегодня в индустрии безопасности и ее приложений действуют Федеральные законы, правила безопасности, системообразующие стандарты – это **ISO 9001** (требования к системе менеджмента качества), **ISO/IEC 15288** (первый стандарт по системной инженерии, регламентирует процессы жизненного цикла систем), стандарты **ISO серий:**

14000 (менеджмент безопасности окружающей среды),
18000 (менеджмент охраны труда), **20000** (сервис-менеджмент),
27000 (менеджмент информационной безопасности),
31000 (менеджмент риска) и др.

Всех их роднит требование системного управления рисками!

Но! Чтобы эффективно управлять – надо уметь количественно прогнозировать риски и обосновывать действенные меры в режиме упреждения!

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

Риск – эффект неопределенности в целях и задачах (по ISO 31000 – 2009)
Эффект – отклонение от ожидаемого – негативного или позитивного

Паспорт

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

1. Перечень потенциально опасных участков объекта

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

2. Модели нарушителей _____

3. Перечень критических элементов объекта

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

[Статья 6](), п. 1
Обеспечение безопасности объектов ТЭК осуществляется субъектами ТЭК !!!

А какой остаточный риск будет иметь место в различных сценариях угроз?
Какой риск допустим?
Что предпринимать, чтобы не превышать допустимых рисков по критериям «эффективность - стоимость»?

5. Организация охраны и защиты объекта

1. Основания установления охраны

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

2. Структура подразделения охраны

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

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

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

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

4. Наличие организационно-распорядительных документов

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

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

5. Организация пропускного и внутриобъектового режимов

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

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

6. Количество действующих контрольно-пропускных пунктов:

Всего _____
Проходных _____
Автотранспортных _____
Железнодорожных _____
Совмещенных _____

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

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

8. Обеспеченность охраны
8.1. Оружием и боеприпасами

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

8.2. Специальными средствами и служебным огнестрельным оружием

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

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

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

8.4. Служебными собаками

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

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

9. Обеспечение сохранности оружия, боеприпасов и специальных средств

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

10. Средний возраст сотрудников охраны

(лет)

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

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

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

(наименование и дата утверждения)

6. Инженерно-технические средства охраны

1. Общая протяженность периметра, подлежащего ограждению

(пог. м)

2. Содержание ограждения

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

3. Освещение охраняемой территории и периметра ограждения

(наличие, краткая характеристика)

4. Охранная сигнализация ограждения

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

5. Сигнализация

(количество лучей)

5.1. Охранная сигнализация

(количество лучей)

5.2. Пожарная сигнализация

(количество лучей)

5.3. Совмещенная охранная и пожарная сигнализация

(количество лучей)

5.4. Тревожная сигнализация

(количество лучей, куда выведены)

5.5. Наличие средств радиосвязи

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

5.6. Наличие средств телефонной связи

(количество постов, оборудованных телефонной связью)

5.7. Наличие средств видеонаблюдения

(тип и количество видеокамер, контролируемые зоны)

6. Техника контрольно-пропускных пунктов

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

7. Наличие иных инженерных сооружений

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

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

(кто обслуживает: специалисты предприятия или подрядной специализированной организации)

8. Оценка антитеррористической защищенности

1. Определение требуемого уровня антитеррористической защищенности критических элементов объекта

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

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

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

3. Оценка эффективности физической защиты критических элементов объекта

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

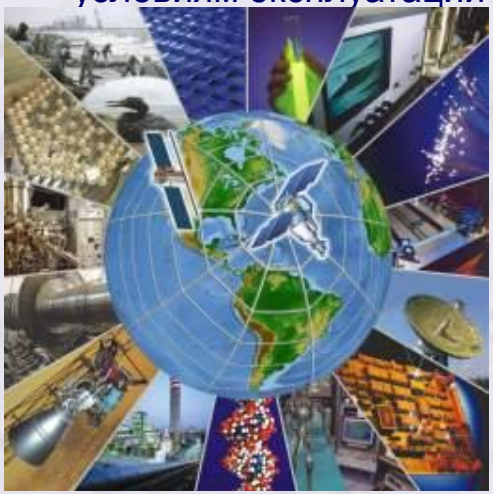
4. Оценка достаточности мероприятий по защите критических элементов объекта

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

ВЫВОДЫ по результатам анализа



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








2. Для иных приложений - в сфере химической, биологической, транспортной, экологической безопасности, безопасности зданий и сооружений, информационной безопасности, в т.ч. в условиях террористических угроз – требования к допустимым рискам задаются преимущественно на качественном уровне в форме требований к выполнению конкретных условий.

Это означает невозможность корректного решения обратных задач управления безопасностью исходя из задаваемого уровня допустимого риска

ВЫВОДЫ по результатам анализа (продолжение)

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

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

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

в) рационального применения мер противодействия рискам

Общее в управлении рисками

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

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

Производственная безопасность

Пожарная безопасность

Радиационная и ядерная безопасность

Экологическая безопасность

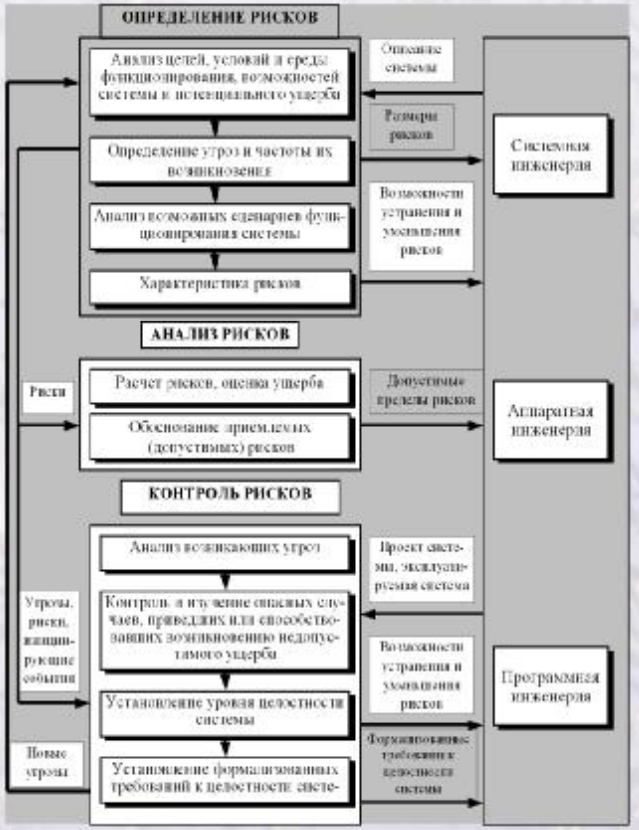
Транспортная безопасность

Авиационная безопасность

Безопасность высотных зданий

Информационная безопасность

и др.



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

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

В какой ситуации предприятия?

Природные и техногенные угрозы неизбежны









Требования безопасности объективны

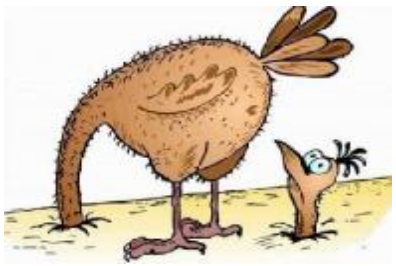


Остаточные риски неминуемы, несмотря на контроль

Методы анализа рисков не направлены на эффективное упреждение!
(за некоторыми исключениями)

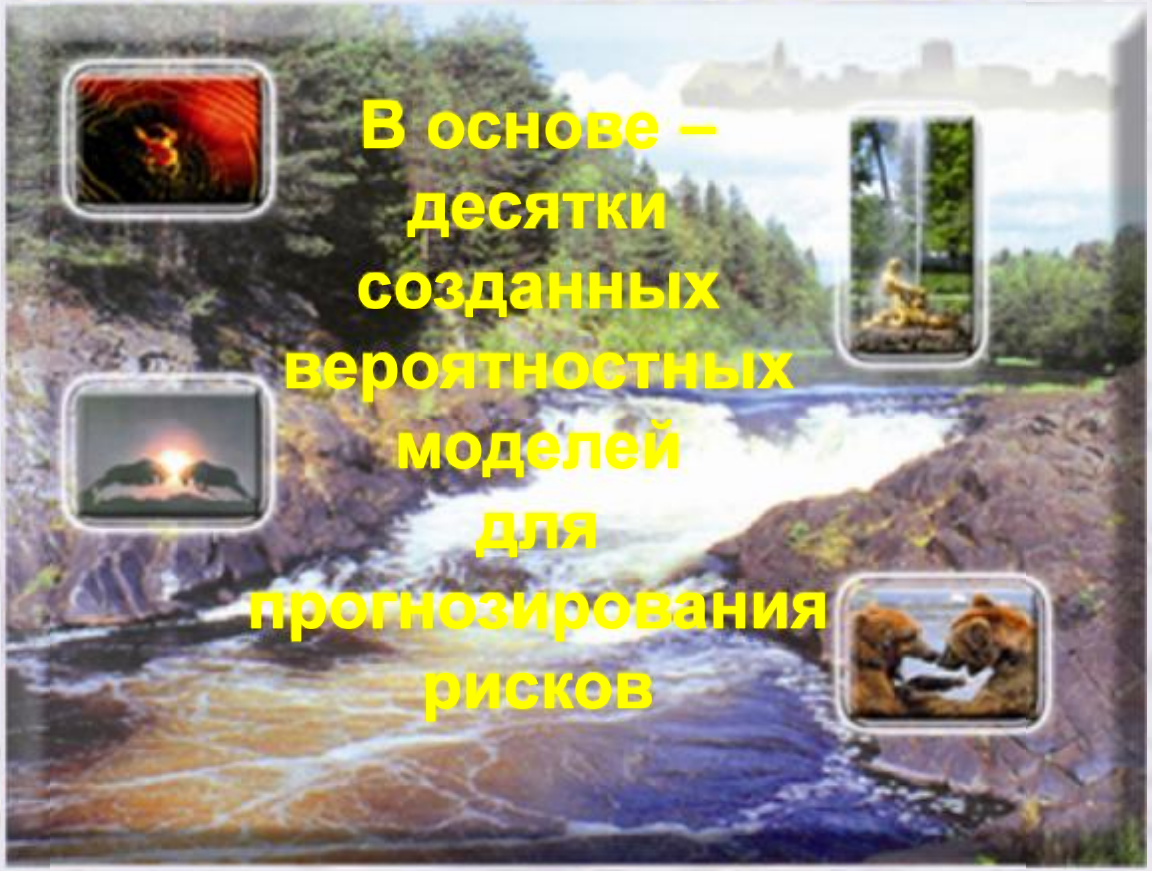
Используемые методы специфичны, результаты несравнимы. В общем случае для различного рода угроз задачи количественного обоснования требований к средствам и системным процессам при ограничениях на ресурсы и допустимые риски – не решаются!

В итоге интерес предприятия сводится к получению «галочки»



Но при реализации рисков ответственность – лишь на предприятиях!

Вместе с тем, все предприятия заинтересованы в выявлении скрытых возможностей и эффектов, приводящих к снижению затрат, ущербов и увеличению доходности!



Это достижимо путем обоснования выбора средств и упреждающих мер контроля, мониторинга и восстановления нарушаемой целостности в результате количественного прогнозирования рисков! – Надо лишь подобрать методы…

Предлагаемые стандарты, идеи, методы и программные инструментарии для прогнозирования рисков и обоснования системных требований

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

Процессы жизненного цикла систем

Процессы соглашения

Процесс приобретения
Процесс поставки

Процессы предприятия

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

Процессы проекта

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

Технические процессы

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

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

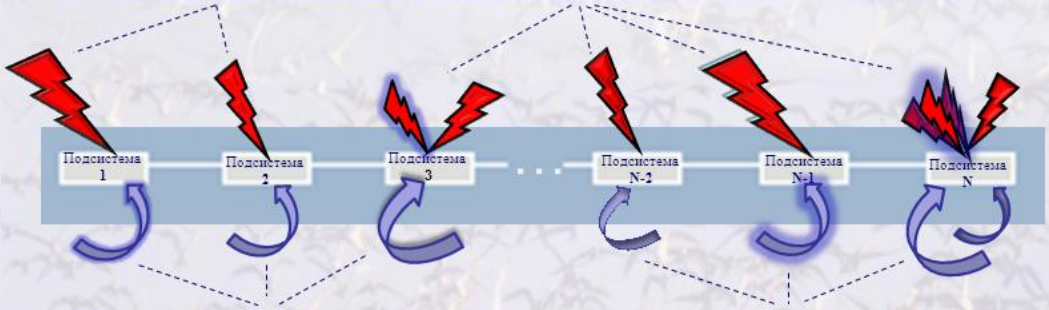
Содержание программных комплексов в поддержку системообразующих стандартов

Объективные потребности в оценке качества и рисков в жизненном цикле систем

Имеет место логическая общность в процессах реализации различного рода угроз, мер контроля, мониторинга и восстановления целостности

для сложной системы

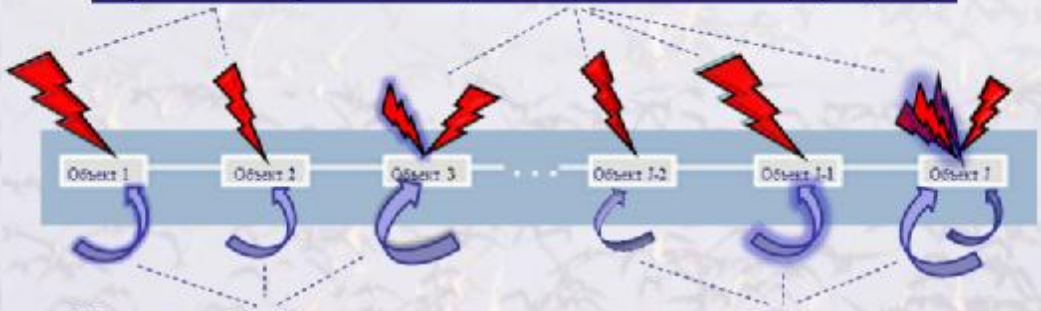
Угрозы и их проявления для каждой из подсистем 1, 2, …, N-1, N



Меры контроля, мониторинга и восстановления целостности для каждой из подсистем 1, 2, …, N-1, N оцениваемого объекта

для совокупности объектов

Угрозы и их проявления для каждого объекта 1, 2, …, J-1, J



Меры контроля, мониторинга и восстановления целостности для каждого из объектов 1, 2, …, J-1, J оцениваемой совокупности (ассоциации) объектов

Общие исходные данные по составным элементам:

- частота возникновения угроз
- среднее время развития кризисной ситуации с момента возникновения угрозы
- период между моментами контроля
- средняя длительность контроля
- средняя наработка на ошибку средств мониторинга (если таковой имеет место)
- среднее время восстановления нарушенной целостности

Единые расчетные показатели:

- риск нарушения безопасности функционирования элемента в течение периода прогноза
- риск нарушения комплексной безопасности в течение периода прогноза

Применение для построения системы противоаварийной устойчивости

Дестабилизирующие факторы (угрозы)

Человеческие факторы

- квалификация персонала организация подготовки и переподготовки кадров
- организацию производственного контроля
- влияние руководителей на исполнителей работ
- состояние здоровья, возрастной фактор
- удовлетворенность работой на предприятии

Факторы, определяемые состоянием основных фондов

- техническое состояние основных систем производственных процессов, в т.ч. состояние горных выработок, техническое состояние оборудования, оборудования подготовительных работ, очистных работ, конвейерного транспорта, вспомогательного транспорта, технологических комплексов погрузки и обогащения руды
- техническое состояние систем жизнеобеспечения шахт, в т.ч. систем вентиляции, дегазации, водоотлива и водоотведения, испарения и пылеподавления, противопожарной защиты и газодинамической безопасности, электроснабжения, обеспечения пожарной обороны
- техническое состояние транспортных систем
- техническое состояние систем ТГК-13

Организационно-производственные факторы

- факторы, определяющие эффективность функционирования основных систем производственных процессов
- факторы, определяющие эффективность технологических процессов жизнеобеспечения шахты
- факторы, определяющие эффективность функционирования транспортных систем
- факторы, определяющие эффективность функционирования систем ТГК-13

Факторы, не зависящие от производственной деятельности

- стихийные бедствия
- аварии на других предприятиях, являющихся поставщиками
- горногеологические факторы
- внешнее энергоснабжение, водоснабжение, транспорт
- экологические факторы
- демографические факторы

Причины дестабилизации

УЯЗВИМОСТИ
(состояние предприятия и системы обеспечения его противоаварийной устойчивости, допускающее возможность реализации дестабилизирующих воздействий в его деятельность.)

Дестабилизация

Предупреждение негативного воздействия дестабилизирующих факторов

Предотвращение появления аварийных ситуаций

Локализация развития аварийных ситуаций в начальный период их возникновения, ликвидация последствий аварий и катастроф, обеспечение восстановления нарушенного производства в короткие сроки

Меры по нейтрализации угроз и противодействию рискам

Организационные меры:

- соблюдение требований законов РФ и нормативно-правовых документов
- разработка и реализация технической политики
- разработка и внедрение руководств и положений по обеспечению противоаварийной устойчивости, введение ответственных
- организация производственного контроля
- обеспечение безопасности персонала и окружающей среды
- планирование и организация устойчивого функционирования предприятия
- подготовка и повышения квалификации кадров
- организация контроля состояния здоровья персонала, анализа степени удовлетворенности работой на предприятии

Технические и технологические меры:

- контроль технического состояния и, при необходимости, восстановление требуемой целостности основных систем производственных процессов, систем жизнеобеспечения шахт, транспортных систем и систем ТГК-13
- периодический контроль и мониторинг целостности, восстановление нарушенной целостности и рациональное управление при функционировании основных систем производственных процессов
- периодический контроль и мониторинг целостности, восстановление нарушенной целостности и рациональное управление технологическими процессами жизнеобеспечения шахты
- периодический контроль и мониторинг целостности, восстановление нарушенной целостности и рациональное управление при функционировании транспортных систем
- периодический контроль и мониторинг целостности, восстановление нарушенной целостности и рациональное управление при функционировании систем ТГК-13

Методические и информационные меры:

- обеспечение качества информационных процессов
- сбор и анализ статистики по результатам периодического контроля и мониторинга целостности и восстановлении нарушенной целостности систем
- сравнительный анализ, прогноз рисков и обоснование допустимых рисков для различных объектов и процессов
- обоснование эффективных мер по нейтрализации угроз и противодействию рискам
- разработка, внедрение и поддержание в рабочем состоянии системы менеджмента риска
- разработка и внедрение эффективной системы обучения и повышения квалификации персонала по противоаварийной устойчивости предприятий

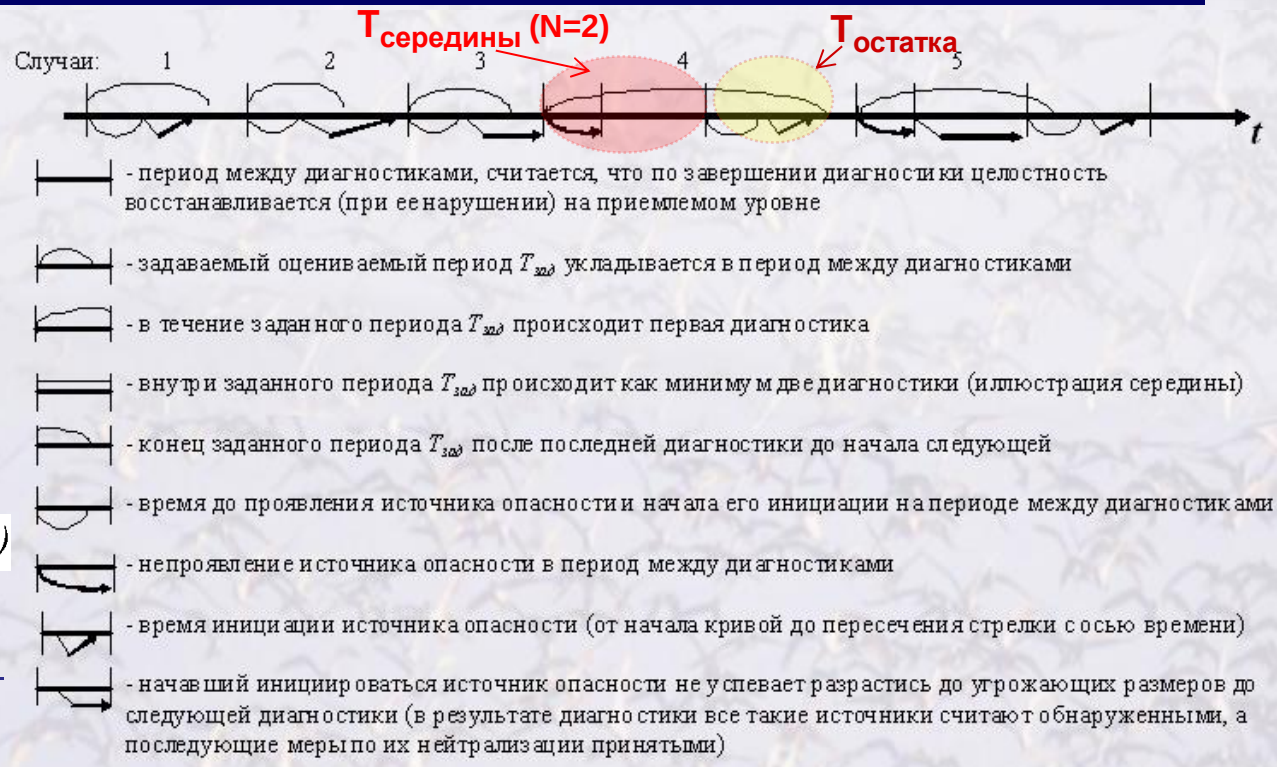
Анализ угроз в обеспечение информационной безопасности

Прогноз качества функционирования информационных систем базируется на определении общей цели и степени ее достижения в условиях различных угроз

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

Некоторые базовые модели (см. также ГОСТ РВ 51987)

Иллюстрация событий для модели 1 периодического контроля



Для варианта 1, когда $T_{зад} < T_{меж} + T_{диаг}$

модель 1 :

$$P_{возд.(1)}(T_{зад.}) = 1 - \Omega_{возд.} * \Omega_{акт.}(T_{зад.})$$

модель 2 (+мониторинг между контролями):

$$P_{возд.(1)}(T_{зад.}) = 1 - \int_0^{T_{зад.}} dA(\tau) \int_0^{T_{зад.}-\tau} d\,\Omega_{возд.} * \Omega_{акт.}(\theta)$$

где * – знак свертки,

$\Omega_{возд.}(t)$ – ФР времени между возникновениями источника опасности, в инструментариях $\Omega_{возд.}(t)=1-exp(-\sigma t)$, σ – частота возникновения источника опасности,

$\Omega_{акт.}(t)$ – ФР времени инициации источника опасности до угрожающих размеров, приводящих к нарушению целостности объекта, в инструментариях $\Omega_{акт.}(t) = 1-exp(-t/\beta)$, β – среднее время инициации,

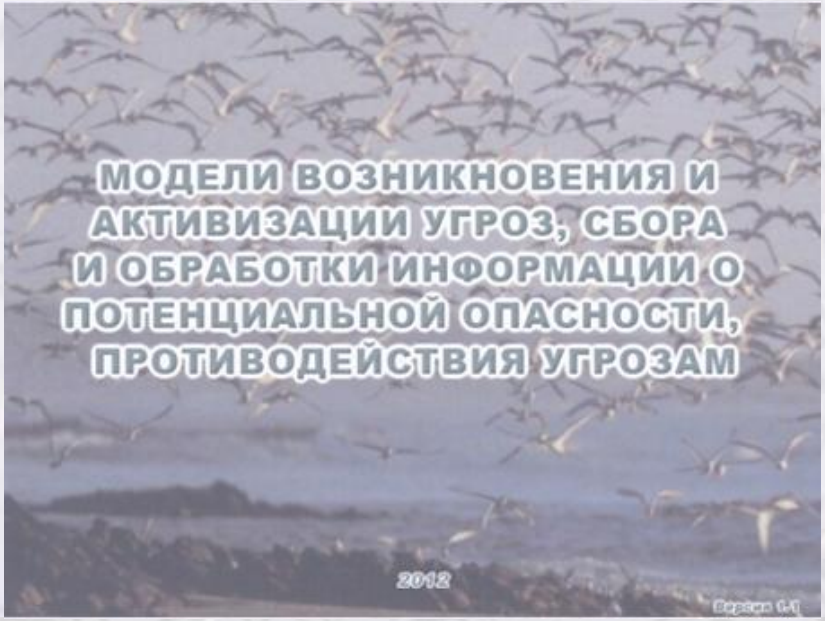
$A(t)$ – ФР времени наработки оператора на ошибку, в инструментариях $A(t)=1-e^{-t/T_{нар.}}$, $T_{нар.}$ – среднее.

Для варианта 2 (когда $T_{зад} \geq T_{меж} + T_{диаг}$) :

$$P_{возд} = P_{серед} + P_{кон},$$

$$P_{серед} = \frac{N(T_{меж}+T_{диаг})}{T_{зад}} \cdot P^{N}_{возд(1)}(\ldots, T_{меж}+T_{диаг}) \quad P_{кон} = \frac{T_{ост}}{T_{зад}} \cdot P_{возд(1)}(\ldots, T_{ост})$$

Примеры моделирующих комплексов



ОЦЕНКА ФУНКЦИОНИРОВАНИЯ ЭЛЕМЕНТОВ

1 Оценка качества процессов представления информации

2 Оценка качества используемой информации

3 Прогноз безопасности функционирования элемента

4 Оценка рисков

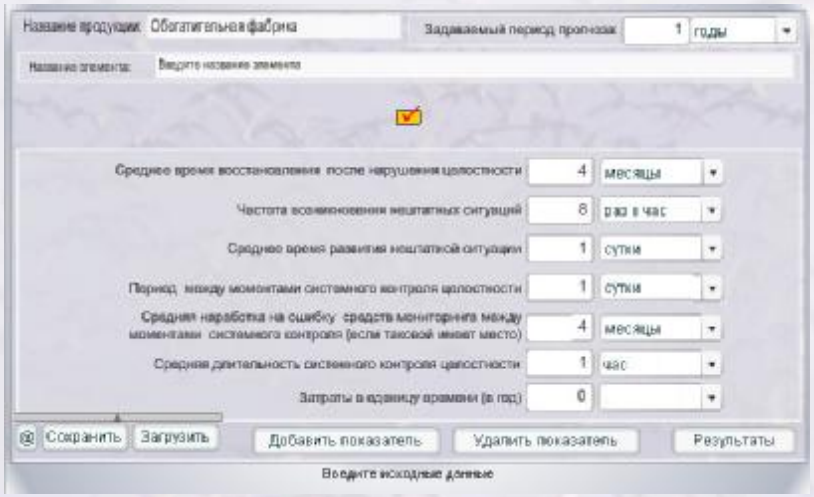
КОМПЛЕКСНАЯ ОЦЕНКА ПРОЦЕССОВ

5 Прогноз комплексного качества

6 Прогноз комплексной безопасности

7 Прогноз рисков в непрерывном производстве

Ввод исходных данных

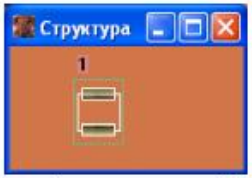


Построение сложных архитектур

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

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

Параллельное объединение - «ИЛИ»

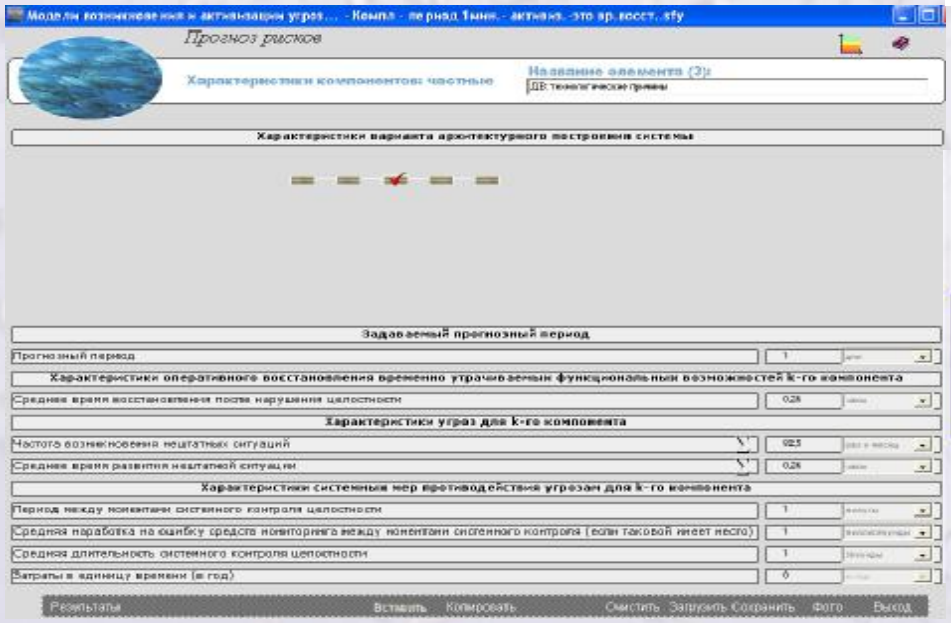


ФР времени наработки на отказ $B(t) = B_1(t)B_2(t)$

Пример логического объединения различных угроз

Исходные данные, связанные с простоями на предприятии непрерывного производства

Исходные данные	Механические причины (1)	Электрические и КИПиА причины (2)	Технологические причины (3)	Отсутствие транспорта (4)	Другие причины (5)
Частота дестабилизирующих воздействий	15 раз/месяц	13.5 раз/месяц	82.5 раз/месяц	1.5 раз/месяц	1.5 раз/месяц
Средние время восстановления	3.13 часа	0.32 часа	0.26 часа	0.11 часа	0.11 часа
Оценка среднего времени развития нештатной ситуации	3.13 часа	0.32 часа	0.26 часа	0.11 часа	0.11 часа



Численный алгоритмический расчет рисков в точках прогноза от 0 до ∞

Оптимизационные задачи для управления рисками в «процессном» подходе

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

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

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

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

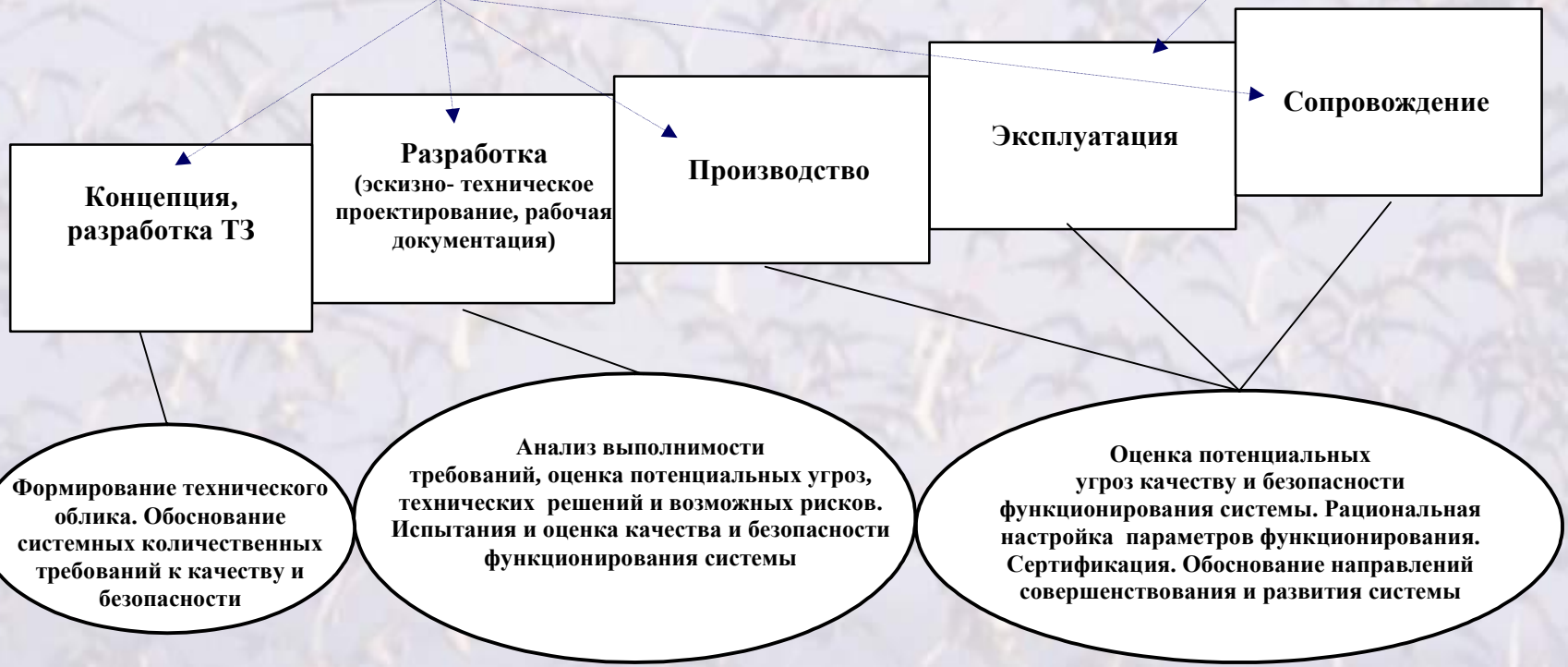
$$Z_{созд.}(Q_{рац.}) = \min_{\text{управляемые параметры A,M}} Z_{созд.}(Q)$$

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

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

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

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



Приложения для рационального управления безопасностью и эффективностью

Задачи в обеспечение эффективности системы противоаварийной устойчивости предприятий

Направления функционального приложения системы	Характеристика эффективности системы	
	Задача №1 - предотвращение реализации дестабилизирующих воздействий	Задача №2 - защита от получения недопустимых ущербов в условиях реализации дестабилизирующих воздействий (ДВ)
Предупреждение негативного воздействия дестабилизирующих факторов	Степень защищенности от возникновения негативного воздействия	-
Предотвращение появления аварийных ситуаций	Степень защищенности от возникновения аварийных ситуаций	Степень защищенности от получения недопустимых ущербов в условиях реализации ДВ
Локализация развития аварийных ситуаций в начальный период их возникновения	-	Способность локализовать развитие аварийных ситуаций за период времени, за который возможный ущерб от развития аварийной ситуации не превысит допустимые пределы
Ликвидация последствия аварий и катастроф в короткие сроки	-	Способность ликвидировать последствия аварий и катастроф за период времени, за который экономические потери не превысят допустимых пределов
Восстановления нарушенного производства в короткие сроки	-	Способность восстановления нарушенного производства за период времени, за который возможные экономические потери не превысят допустимых пределов

ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ РЕГЛАМЕНТОМ ПЛАНОВОГО РЕМОНТА В НЕПРЕРЫВНОМ ПРОИЗВОДСТВЕ (НА ПРИМЕРЕ ОБОГАТИТЕЛЬНОЙ ФАБРИКИ)

Шаг 1 Определение логической структуры системы и модели угроз

Предприятие (система) находится в состоянии целостности (т.е. экономически приемлемого производственного процесса) если каждое из дестабилизирующих воздействий (механических, электрических и КИПиА, технологических, транспортных и иных) не приводит к выходу за допустимые уровни, признаваемые приемлемыми по «прецедентному принципу»

Нарушения по механическим причинам -1 | Нарушения по электрическим и КИПиА причинам - 2 | Нарушения по технологическим причинам - 3 | Нарушения по причинам отсутствия транспорта - 4 | Нарушения по иным причинам - 5

Шаг 2.1 Формирование исходных данных для модели 1

Исходные данные по каждой причине:
- частота возникновения простоев;
- средняя длительность текущего ремонта, экономически приемлемая для производственного процесса;
- период между моментами диагностики;
- средняя длительность диагностики

Применение модели 1 – чтобы учесть текущие ремонты

Данные из статистики предприятия за месяц («по прецеденту» признаны приемлемыми)

Исходные данные	Механические причины (1)	Электрические и КИПиА причины (2)	Технологические причины (3)	Отсутствие транспорта (4)	Другие причины (5)
Частота дестабилизирующих воздействий	15 раз/месяц	13.5 раз/месяц	82.5 раз/месяц	1.5 раз/месяц	1.5 раз/месяц
Среднее время восстановления	3.13 часа	0.32 часа	0.26 часа	0.11 часа	0.11 часа
Оценка среднего времени развития нештатной ситуации	3.13 часа	0.32 часа	0.26 часа	0.11 часа	0.11 часа

Шаг 3.1 Поэлементный расчет

По каждой причине строится ФР времени на нарушение целостности по точкам для $T_{зад} = (0, \infty)$:

$$R_{наруш.} = 1 - P_{возд} \qquad (2.2.1)$$

$$P_{возд(1)} = \begin{cases} \left(\sigma - \beta^{-1}\right)^{-1}\left(\sigma e^{-\sigma T} - \beta^{-1} e^{-\beta T}\right), & \text{если } \sigma \neq \beta^{-1}, \\ e^{-\sigma T}\left[1 + \sigma T_{зад}\right], & \text{если } \sigma = \beta^{-1}. \end{cases} \quad (2.2.2)\text{-}(2.2.5)$$

Шаг 4.1 Прогнозирование рисков (чтобы определить среднюю наработку на нарушение целостности с т. зр. экономической приемлемости)

По всем причинам строится ФР времени на нарушение целостности по точкам для $T_{зад} = (0, \infty)$:

$$R(t) = 1 - [1 - R_1(t)][1 - R_{i+1}(t)] \quad (2.3.1)$$

с использованием методов 1-3 и (2.3.2) – (2.3.5)

По построенным ФР для всех причин численными методами вычисляются средние времена наработки на нарушение целостности $T_{нар.}$, $T_{нар.i}$ (они характеризуют наработку на ошибку при мониторинге между плановыми ремонтами)

Шаги 3.2 и 4.2 Поэлементный расчет и прогнозирование рисков по модели 2

По каждой причине строится ФР времени на нарушение целостности по точкам для $T_{зад} = (0, \infty)$:

$$R_{наруш.} = 1 - P_{возд} \qquad (2.2.1)$$

$$P_{возд.(1)}(T_{зад.}) = 1 - \int_0^{T_{зад}} dM(\tau) \int_c^{T_{зад}} d\,\Omega_{возд.} * \Omega_{авт.}(\theta) \quad (2.2.6)\text{-}(2.2.7)$$

По всем причинам строится ФР времени на нарушение целостности по точкам для $T_{зад} = (0, \infty)$ с использованием методов 1-3 и формул (2.3.1) – (2.3.5)

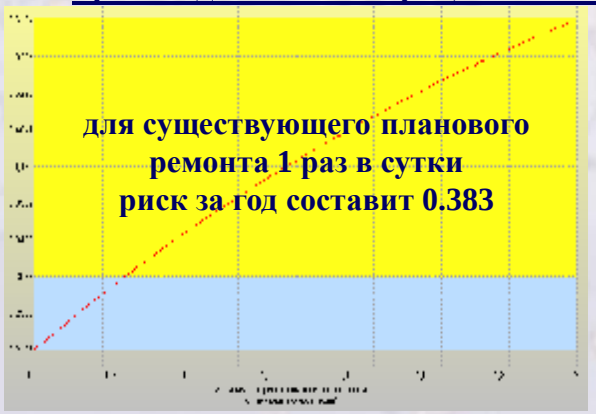
Применение модели 2 учитывает уже и текущие, и плановые ремонты

Шаг 2.2 Формирование исх. данных для модели 2

Исходные данные для модели 2 по каждой причине:
- частота возникновения простоев;
- средняя длительность текущего ремонта, экономически приемлемая для производственного процесса;
- период между моментами планового ремонта;
- средняя длительность планового ремонта;
- время наработки на ошибку при мониторинге

Шаг 5 Сравнительный анализ системных процессов, извлечение закономерностей, обоснование рекомендаций для выработки рациональных организационно-технических решений

Риски нарушения экономически приемлемого производственного процесса в течение периода 0.5 – 2 года

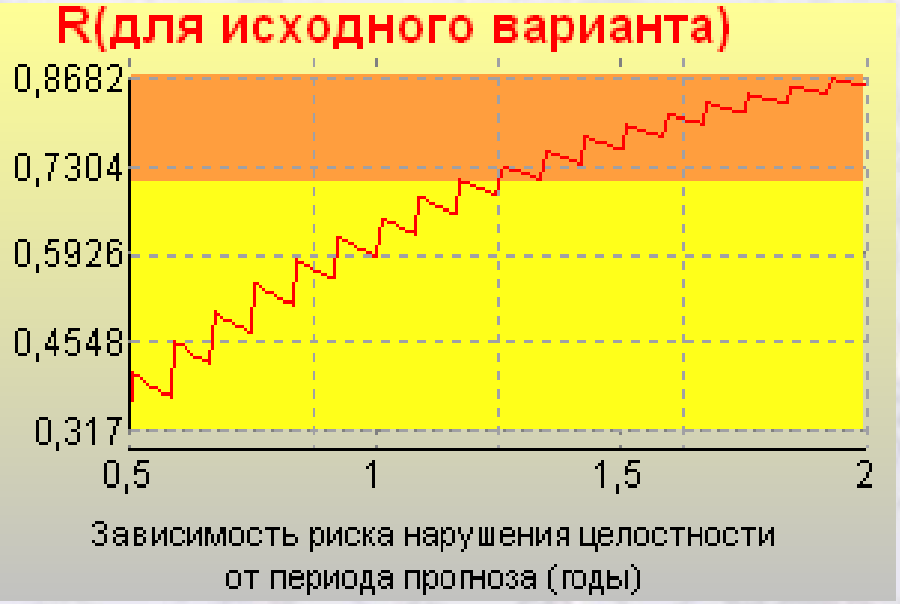


Выявленная закономерность

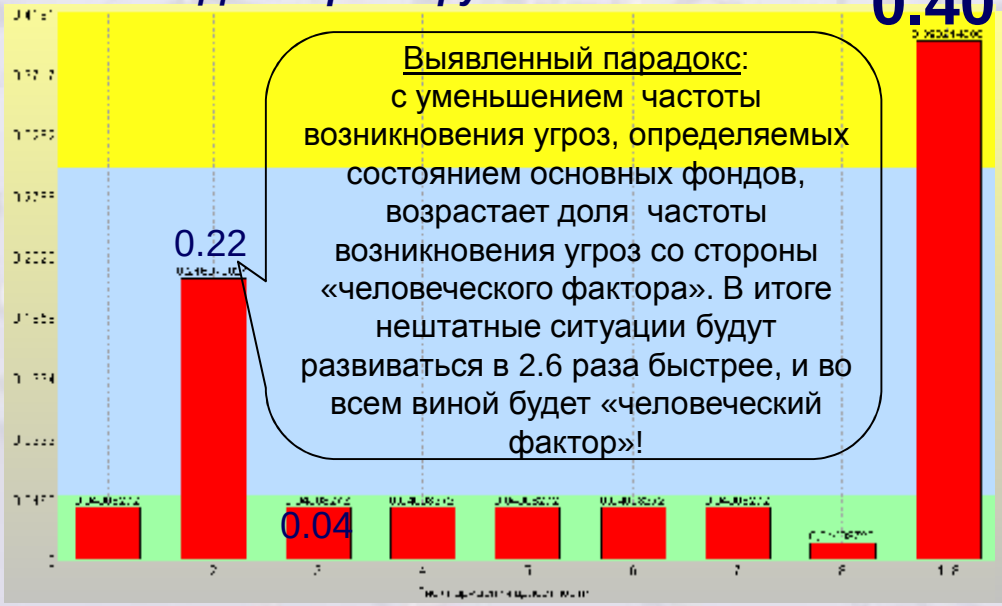
По сравнению с существующим вариантом при реализации планового ремонта 2 раза в сутки средняя наработка предприятия возрастает на 71.3%, а риск нарушения экономически приемлемого производственного процесса за год снизится с уровня 0.383 до 0.057, т.е. сократится в 6.7 раза

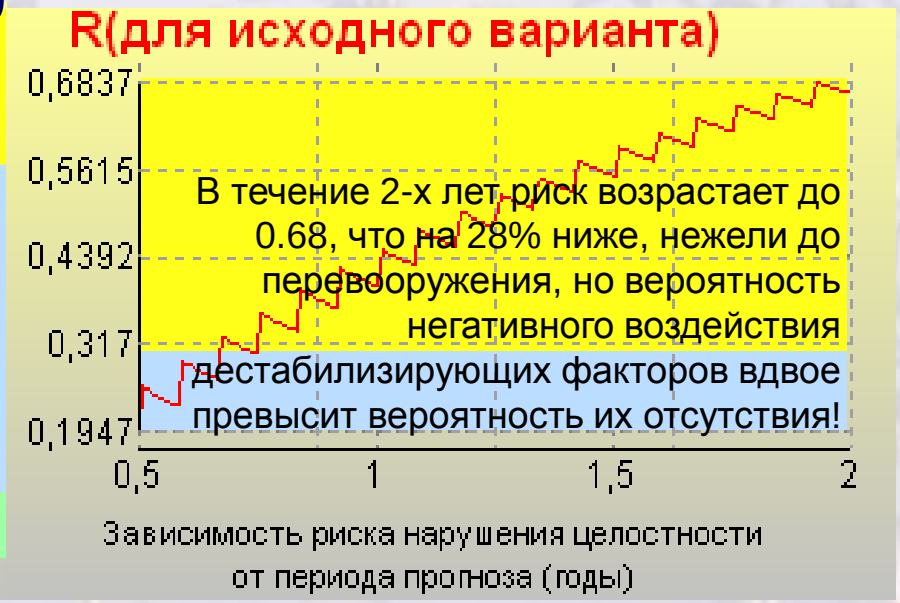
Анализ нарушения целостности в течение года функционирования системы вентиляции, аспирации и пылеподавления

Для существующей системы



Для перевооружаемой системы





Анализ безопасности

Исходные данные:

подсистема 1 – линейная часть, включая отводы и лупинги, запорную арматуру, переходы через естественные и искусственные препятствия, узлы пуска и приема очистных устройств и дефектоскопов, узлы сбора и хранения конденсата, устройства для ввода метанола в газопровод, перемычки;

подсистема 2 - линии электропередачи, предназначенные для обслуживания трубопроводов и устройств электроснабжения и дистанционного управления запорной арматурой и установками электрохимической защиты трубопроводов;

подсистема 3 – технические станции, включая компрессорные станции и узлы подключения, газораспределительные станции, подземные хранилища газа, станции охлаждения, газа, узлы редуцирования газа, газоизмерительные станции;

подсистема 4 – совокупность остальных составных частей, включая установки электрохимической защиты трубопроводов от коррозии, линии и сооружения технологической связи, средства телемеханики трубопроводов, противопожарные средства, здания и сооружения линейной службы эксплуатации трубопроводов, емкости для сбора, хранения и резгазирования газового конденсата, постоянные дороги и вертолетные площадки вдоль трассы газопроводов, указатели и предупредительные знаки, вспомогательные объекты (в т.ч. базы производственного обслуживания, технического обеспечения и комплектации оборудования, автотранспортные и ремонтно-строительные подразделения, цехи технологического транспорта и спецтехники, склады взрывчатых материалов и пр.), а также эксплуатационный и ремонтный персонал.

Частота возникновения угроз 5 раз в год. Время восстановления системы - 3 суток. Длительность оцениваемого периода – от 1 до 10 лет

Основные результаты:

для подсистемы 1 – 0.52-0.63 за год с возрастанием до 0.91-0.94 за 10 лет;
для подсистемы 2 – 0.36-0.57 за год с возрастанием до 0.85-0.93 за 10 лет;
для подсистемы 3 – 0.51-0.66 за год с возрастанием до 0.91-0.95 за 10 лет;
для подсистемы 4 – 0.02-0.27 за год с возрастанием до 0.18-0.79 за 10 лет

Выводы:

Подсистемы 1-3, включающие в свой состав технические средства, в условиях повышенной сложности контроля и мониторинга состояний являются наиболее уязвимыми звеньями магистральных трубопроводов

Подсистема 4, во многом допускающая эффективный контроль со стороны человека, за счет ежемесячного контроля целостности и непрерывного мониторинга состояния критичных средств подсистемы ответственными руководителями и персоналом, соблюдения функциональных обязанностей и правил техники безопасности является сегодня почти на порядок менее уязвимым звеном магистральных трубопроводов

Продолжение примера. **Поиск путей эффективного использования средств системного контроля и непрерывного мониторинга**

Для подсистемы 1 реализация мониторинга связана с использованием перспективных интеллектуальных трубопроводов с мониторирующими датчиками,

для подсистемы 2 - с использованием спутниковых систем контроля состояния,

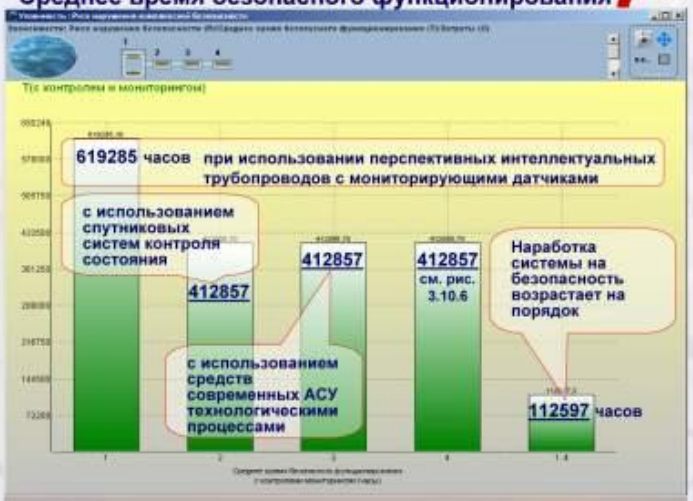
для подсистемы 3 - с использованием средств современных АСУ технологическими процессами.

Для подсистемы 4 мониторинг осуществляется непосредственно ответственными руководителями и персоналом путем соблюдения функциональных обязанностей и правил техники безопасности (с учетом оперативного устранения выявленных нарушений).

Т.е. с точки зрения возможностей мониторинга первые три подсистемы усовершенствуются как минимум до уровня 4-й подсистемы

До какого уровня возможно снижение рисков и при каких условиях ?

Среднее время безопасного функционирования



Снижение рисков достижимо за счет применения эффективных мер мониторинга, контроля и поддержания целостности системы, основанных на использовании:

интеллектуальных трубопроводов с мониторирующими датчиками, позволяющими охватить 100% эксплуатируемых магистральных трубопроводов;

спутниковых систем непрерывного контроля состояния составных компонентов, позволяющих контролировать состояния наземных и воздушных элементов магистральных трубопроводов и обеспечивающих выполнение следующего требования;

средств современных АСУ технологическими процессами, осуществляющими мониторинг функционирования головных и промежуточных перекачивающих и наливных насосных станций, резервуарных парков.

При этом должно обеспечиваться выполнение следующего технического требования - наработка средств мониторинга на ошибку должна быть не менее полугода

Прогноз

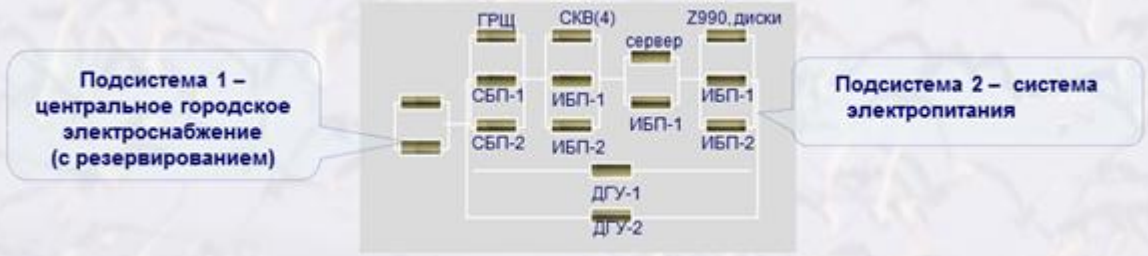
Условия возникновения и реализации террористических угроз и защиты от них описываются в терминах случайных процессов




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

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

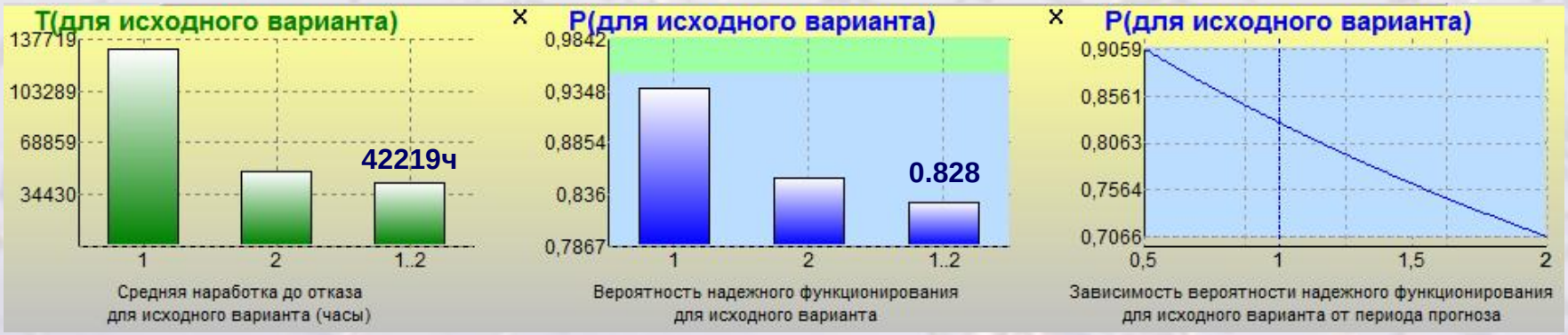
Оценка безопасности функционирования системы инженерного обеспечения - 1



До автоматизации

Наработка системы электропитания на отказ составит 16196 часов, а вероятность надежного функционирования системы в течение года равна 0.649

После автоматизации



При реализуемой технологии контроля, мониторинга и восстановления целостности наработка на отказ 42219 часов (выше в 2.44 раза), а вероятность надежного функционирования в течение года 0.828, (выше в 1.26 раза)

Оценка безопасности функционирования системы инженерного обеспечения - 2

До автоматизации

После автоматизации

Оценка безопасности функционирования системы инженерного обеспечения - 3

До автоматизации

После автоматизации

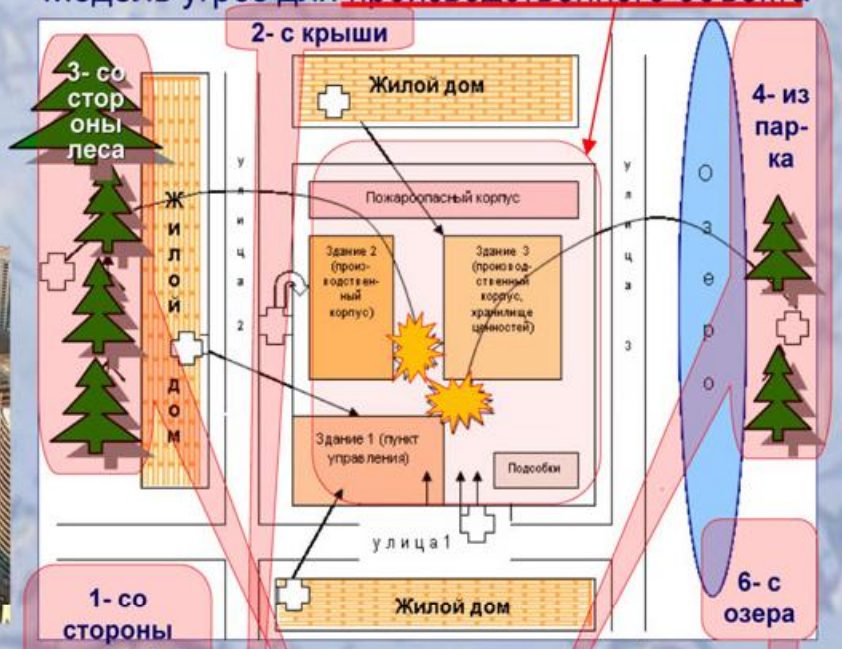
Риск нарушения электроснабжения в 1.7-7 раз ниже!

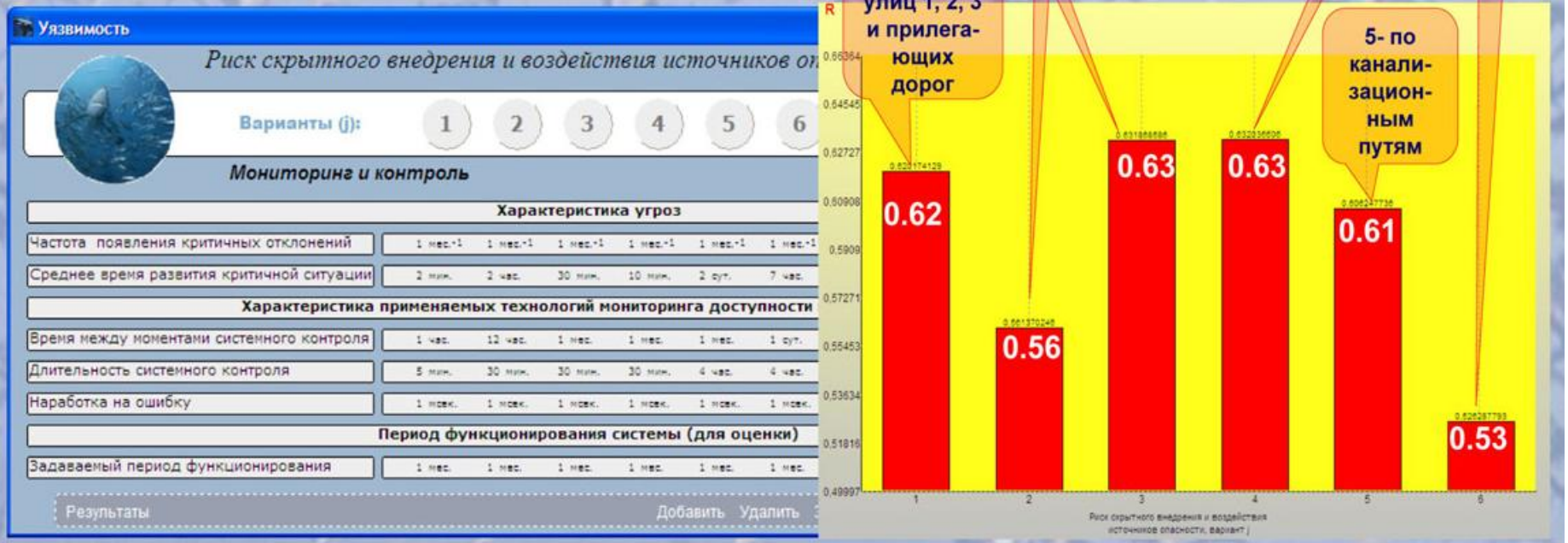
Уменьшение надежности – всего 0.02, что соизмеримо с вкладом от добавления двух ИБП и ДГУ. Последнее означает, что с увеличением состава соответствующее снижение надежности электроснабжения может быть компенсировано наличием в резерве дополнительно двух ИБП и одного-двух ДГУ!

Анализ уязвимости важных наземных объектов

Возможные объекты террористического воздействия

Модель угроз для производственного объекта





Сравнение вариантов обеспечения безопасности объекта

Данные: по ситуационному анализу

Характеристика событий потенциальной опасности	
Количество событий, требующих анализа	100
Доля потенциально опасных событий	100 %
Характеристика интерпретации событий	
Скорость интерпретации	3 сек.-1
Частота возможных ошибок	1 чел.-1
Временные ограничения	
Допустимое время на интерпретацию событий	0.5 мин.
Характеристика затрат	
Затраты на ситуационный анализ	1000000

по мониторингу и контролю

Характеристика критичных ситуаций	
Частота появления критичных ситуаций	1 чел.-1
Среднее время развития критичной ситуации	1 час.
Характеристика технологий мониторинга	
Время между моментами системного контроля	1 час.
Длительность системного контроля	5 мин.
Наработка на ошибку	8 час.
Период функционирования системы (для оценки)	
Задаваемый период функционирования	1 год.
Характеристика затрат	
Затраты на мониторинг и контроль	1000000

по мерам противодействия

Характеристика мер противодействия						
Время сохранения эффективности меры	1 сут.	1 сут.	1 сут.	1 год	10 год	1 сут.
Время до очередного адекватного усиления	1 сут.	1 сут.	1 сут.	1 год	5 лет	1 сут.
Период функционирования системы (для оценки)						
Длительность периода потенциальной опасности	1	месяцы				
Характеристика затрат						
Затраты на меры противодействия рискам	100	100	100	1000	100000	100

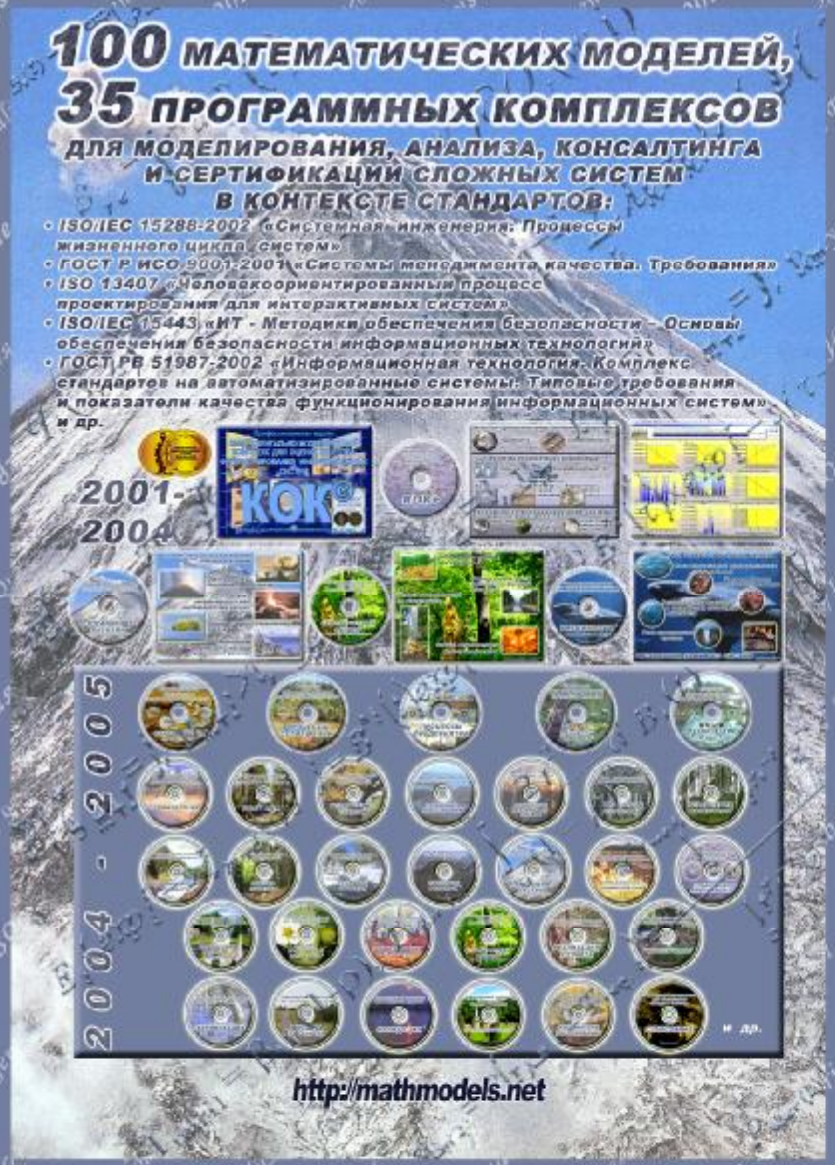
1-е направление - комплексное предотвращение ущерба

1. Ущерб при нераспознавании опасности, эффективных мерах контроля и безуспешном противодействии рискам	500
2.Ущерб при нераспознавании опасных ситуаций, эффективных мерах обеспечения целостности и противодействия рискам	10000
3.Ущерб при своевременном распознавании опасных ситуаций, нарушениях целостности при эффективных мерах противодействия рис	800
4.Ущерб при нераспознавании опасных ситуаций, нарушениях целостности системы при эффективных мерах противодействия рискам	2000
5.Ущерб при своевременном распознавании опасных ситуаций, нарушениях целостности при опасном воздействии на систему	5000
6.Ущерб при своевременном распознавании опасности, эффективных мерах контроля и безуспешном противодействии рискам	100000
7.Ущерб при нераспознавании опасности, неэффективном контроле системы и безуспешном противодействии рискам	100000

2-е направление - построение упрощенной системы противодействия

МОНОГРАФИИ

СТАТЬИ И ДОКЛАДЫ НА НАУЧНО-ТЕХНИЧЕСКИХ ФОРУМАХ



СТАНДАРТИЗАЦИЯ, МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, РАЦИОНАЛЬНОЕ УПРАВЛЕНИЕ И СЕРТИФИКАЦИЯ

А. И. Костогрызов, Г.А. Нистратов

СТАНДАРТИЗАЦИЯ, МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, РАЦИОНАЛЬНОЕ УПРАВЛЕНИЕ И СЕРТИФИКАЦИЯ

в области системной и программной инженерии

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

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

СИСТЕМНЫЕ ОСНОВЫ УПРАВЛЕНИЯ КОНКУРЕНТОСПОСОБНОСТЬЮ В НЕФТЕГАЗОВОМ КОМПЛЕКСЕ

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

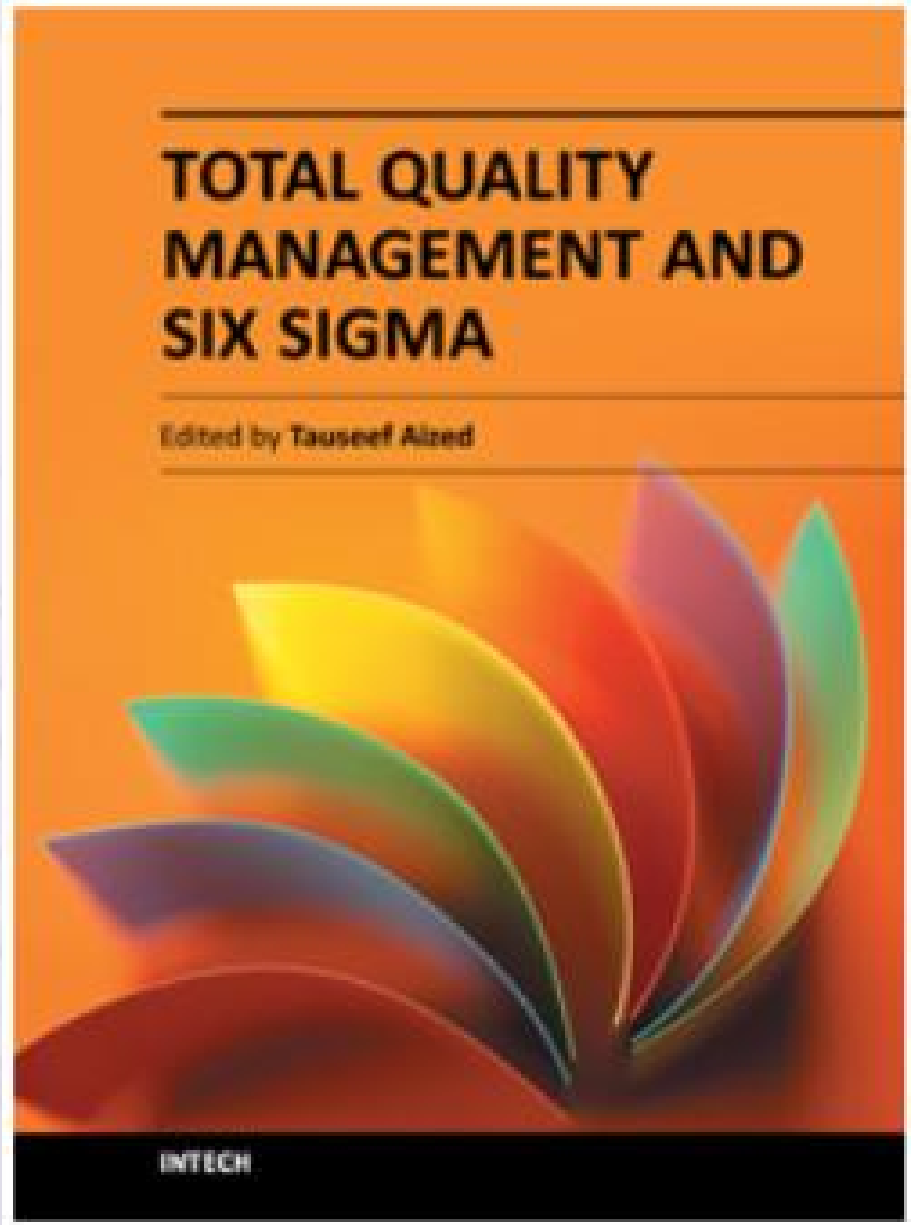
КЕРШЕНБАУМ ВСЕВОЛОД ЯКОВЛЕВИЧ
заслуженный деятель науки РФ, доктор технических наук, профессор. Генеральный директор Национального института нефти и газа, заведующий кафедрой «Управление качеством, стандартизация и сертификация» РГУ нефти и газа им. И.М.Губкина. Вице-президент Российской инженерной академии,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

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

Москва-2010

СИСТЕМНЫЕ ОСНОВЫ УПРАВЛЕНИЯ КОНКУРЕНТОСПОСОБНОСТЬЮ В НЕФТЕГАЗОВОМ КОМПЛЕКСЕ

Глава 7 - 70 страниц в монографии изд-ва InTech



Chapter 7

Some Applicable Methods to Analyze and Optimize System Processes in Quality Management

Andrey Kostogryzov, George Nistratov and Andrey Nistratov

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/46106

1. Introduction

The complexity of present man-made systems has reached an unprecedented level. In fact any system is grounded on computer technologies in the sense that it contains computer elements or is modeled or supported with the help of computer. This trend resulted in new opportunities and at the same time caused additional difficulties. Shortcomings in integration of scientific, engineering, management, and financial areas, which are used to ensure an effective system development and employment, now become more obvious. Today processes of system life cycle in different conditions and threats are the main objects for forecasting, analysis and optimization. Indeed these objective changes become the main reason for establishing the first system engineering ISO/IEC standard ISO/IEC 15288 "System Engineering - System Life Cycle Processes" (since 2002). Covering systems in industrial, energetic, transport, aerospace, military and other fields, this standard recommends to perform only the actions that were substantiated and not to act in the directions, which were not estimated and justified. It means that feature of our time is the turn to system engineering – see Figure 1.

Up-to-date approach to system maturity refers us to international standards ISO 9001 and 9004, ISO/IEC 15026, 15504, CMMI etc. It is clear without "system analysts" there is not achievable the highest level "Optimizing", but also a previous "Predictable" level. However many customers and Chief Designers often fail to take quantitative system requirements into consideration, they do so wittingly or through an oversight. From now on these omissions do not conform to the requirements of the international standards. It is only the beginning. What will be the continuation?

Nowadays if comprehensive quantitative system requirements were not established in quality management, the system efficiency and customer satisfaction can not be controlled

Заказчики, Потребители:

Банк Российской Федерации
3 ЦНИИ Минобороны РФ
Центр информационных технологий и систем органов исполнительной власти
Международный центр по информатике и электронике
Центр стандартизации, проектирования и разработки информационно-коммуникационных технологий и систем
ОАО «Газавтоматика», ОАО «Газпромавтоматизация» ОАО «Газпром»
ООО "Газпром добыча Ямбург", ООО «Нормет»
Сибирская угольная энергетическая компания (СУЭК)
ООО “Информ ТБ Уголь +”
ОАО «ICL-КПО ВС»
ЗАО «ИНГРАС-М»
Институт проблем информатики Российской академии наук
Российская академия ракетных и артиллерийских наук
Российский гуманитарный научный фонд
РГУ нефти и газа им. И.М.Губкина
Юго-Западный государственный университет (ЮЗГУ)
Самарский государственный аэрокосмический университет им. академика С.П. Королева
Консорциум «ИНТЕГРА-С»
CIM College, Сербия и др.

www.mathmodels.net

Предложения в проект решения:

1. В интересах органов государственной власти, министерств и ведомств, государственных и частных хозяйствующих субъектов в критичных областях приложения признать наиболее приоритетными следующие наукоемкие направления работ для обеспечения промышленной безопасности:

- формирование современной научно-технической политики по обеспечению комплексной безопасности критически и стратегически важных объектов промышленной инфраструктуры в РФ с учётом изменяющейся природной, техногенной среды и социальной обстановки;
- развитие и широкое внедрение научно-методического обеспечения для эффективного применения в отечественной практике положений современных международных и отечественных стандартов в области системной инженерии;
- создание и реализацию методов прогнозирования и управления рисками (техническими, технологическими, информационными и др.) для целенаправленного повышения безопасности в жизненном цикле различного рода систем;
- разработку и внедрение моделирующих инструментально-технологических комплексов и инновационных технологий для анализа и обоснования эффективных путей повышения качества и безопасности функционирования предприятий, формирование и ведение банка данных для характеристики допустимых рисков по прецедентному принципу;
- обучение в области методов прогнозирования и управления рисками, обеспечения безопасности для систем различного функционального приложения

2. Рекомендовать Совету Безопасности Российской Федерации поставить работу по созданию «Концепции комплексной безопасности критически и стратегически важных объектов промышленной инфраструктуры РФ», предусматривающую объединение отдельных отраслевых, ведомственных, региональных центров и систем, занимающихся обеспечением отраслевой безопасности (радиационной, экологической, энергетической, информационной, антитеррористической, транспортной и др.) в Едином Государственном Центре Комплексной Безопасности (ЕГЦКБ) при Совете Безопасности РФ