11 декабря 2019г., МГУ им. М.В. Ломоносова, Москва

ОБ ИСПОЛЬЗОВАНИИ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ И ТЕОРИИ ВЕРОЯТНОСТИ ДЛЯ ПРОГНОЗИРОВАНИЯ РИСКОВ

А.И. Костогрызов

ОБЩЕЕ

Система - комбинация взаимодействующих элементов, организованная для достижения одной или нескольких поставленных целей - по ГОСТ Р ИСО/МЭК 57193-2016, ISO/IEC/IEEE 15288, ISO 9001 - 2008

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

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

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

объединению возможностей всех инженерных дисциплин и специальностей в единое системотехническое достижение

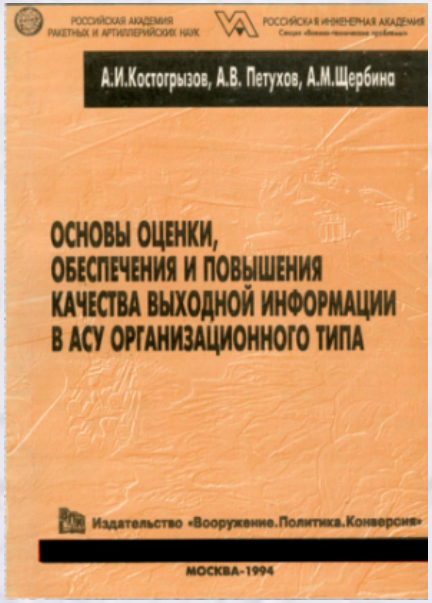
Безопасность – 1) состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз (по ФЗ «О безопасности», ГОСТ Р 22.0.02); 2) отсутствие недопустимого риска (по ГОСТ Р 51898-2002, ГОСТ 1.1-2002); 3) состояние защищённости прав граждан, природных объектов, окружающей среды и материальных ценностей от последствий несчастных случаев, аварий и катастроф на промышленных объектах (ГОСТ Р 12.3.047)

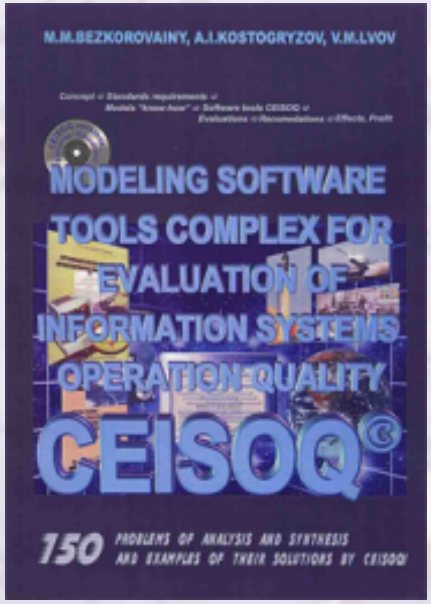
Риск – 1) мера опасности с ее последствиями (по ФЗ «О техническом регулировании», ГОСТ Р 51898-02 «Аспекты безопасности…» и др.)

2) эффект неопределенности в целях и задачах (по ISO 31000 – 2009)

Теоретические основы – 1993-2003гг.

(150 решенных задач анализа и синтеза для различных АСУ)





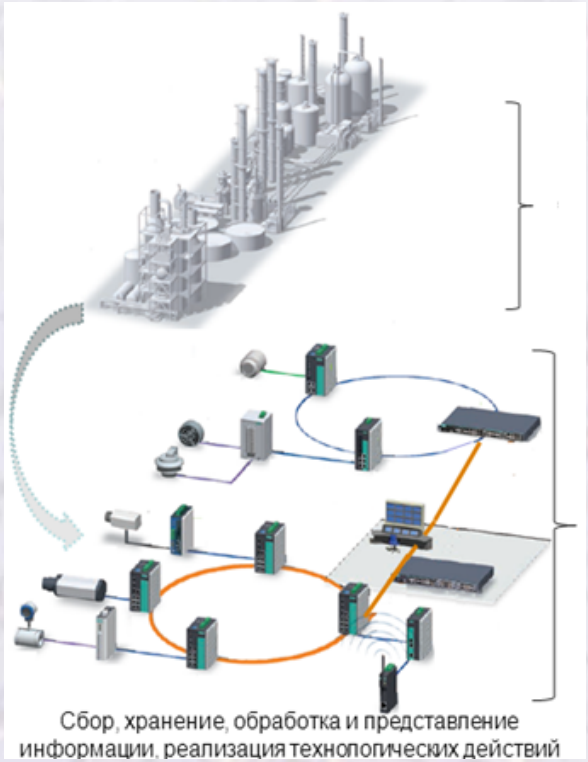
ДЕПЕРСОНИФИКАЦИЯ

- **задача, смежная с задачей анализа рисков для сложных систем: предлагая методы деперсонификации, необходимо понимать степень достижения целей (“highly likely”)**

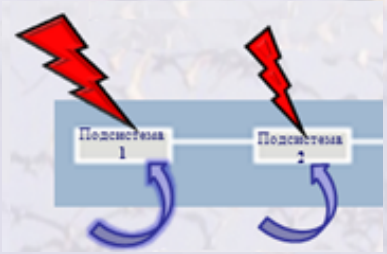
Риск – 1) мера опасности с ее последствиями (по ФЗ «О техническом регулировании», ГОСТ Р ИСО/МЭК 15026-02, ГОСТ Р ИСО/МЭК 16085-07, ГОСТ РВ 51987-02)

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

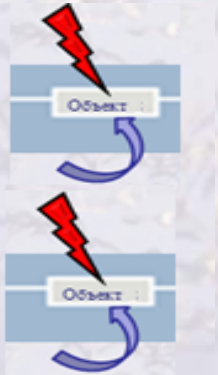
ДЕКОМПОЗИЦИЯ ДО ПОДСИСТЕМ И ОТДЕЛЬНЫХ КРИТИЧНЫХ ЭЛЕМЕНТОВ



Комплексирование функций распределения по алгоритму



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



Риск $R(t) = R_1(t)R_2(t)$

ОЦЕНКА И УПРАВЛЕНИЕ КАЧЕСТВОМ ОПЕРИРУЕМОЙ ИНФОРМАЦИИ

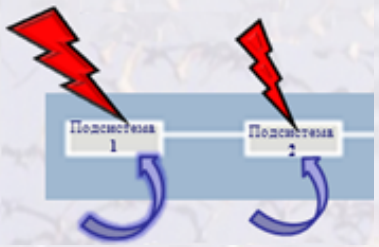
КОМПЛЕКСИРОВАНИЕ ФУНКЦИЙ РАСПРЕДЕЛЕНИЯ ДЛЯ ИНТЕГРИРУЕМЫХ СЛОЖНЫХ АРХИТЕКТУР

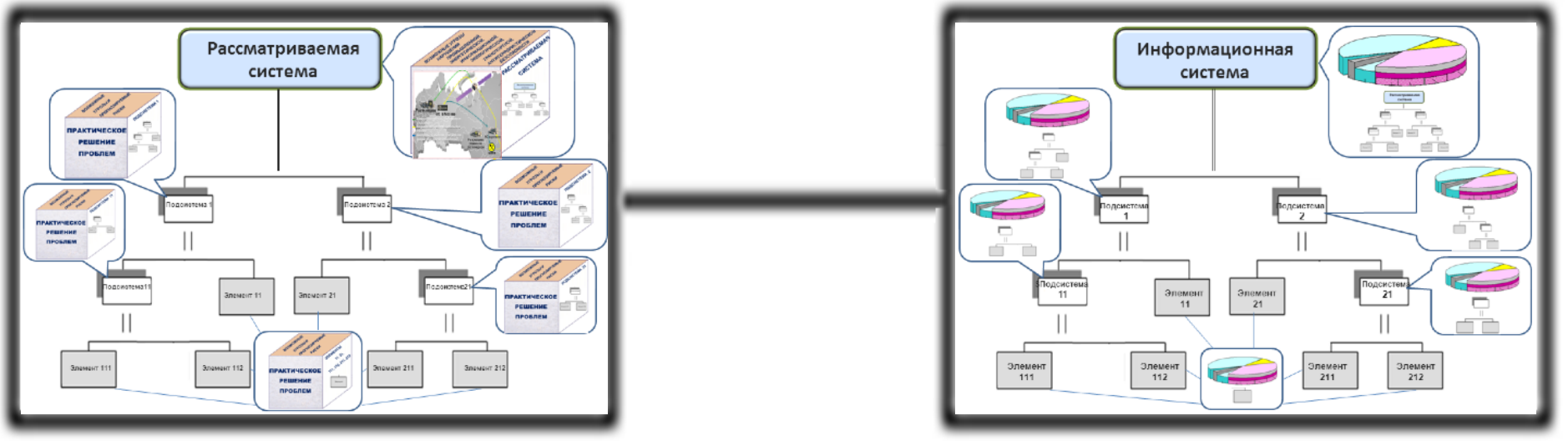
Методы системной инженерии

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

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

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





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

ЧТО ПРЕДЛАГАЕТСЯ?

- **корректное прогнозирование рисков и обоснование упреждающих мер**

(в т.ч. идеи, методы и технологии системной инженерии в обеспечение качества и безопасности, стандарты)

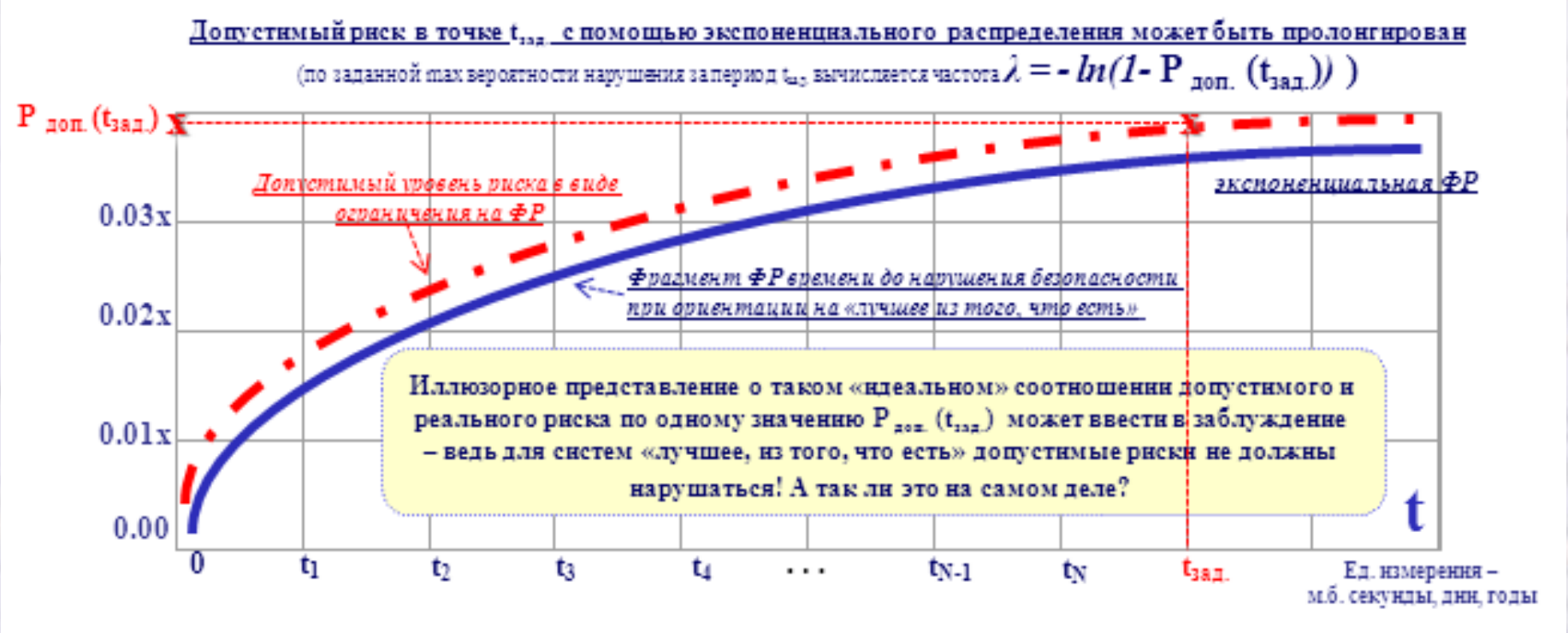
Риск – 1) мера опасности с ее последствиями (по ФЗ «О техническом регулировании», ГОСТ Р ИСО/МЭК 15026-02, ГОСТ Р ИСО/МЭК 16085-07, ГОСТ РВ 51987-02)

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

Подразумеваемое формальное представление при задании требований

Например, частота – показатель риска по РБ «Методика анализа риска аварий на сухопутных объектах нефтегазодобычи и промысловых трубопроводах»

экспоненциальное – для ФР времени наработки на нарушение целостности (безопасности)

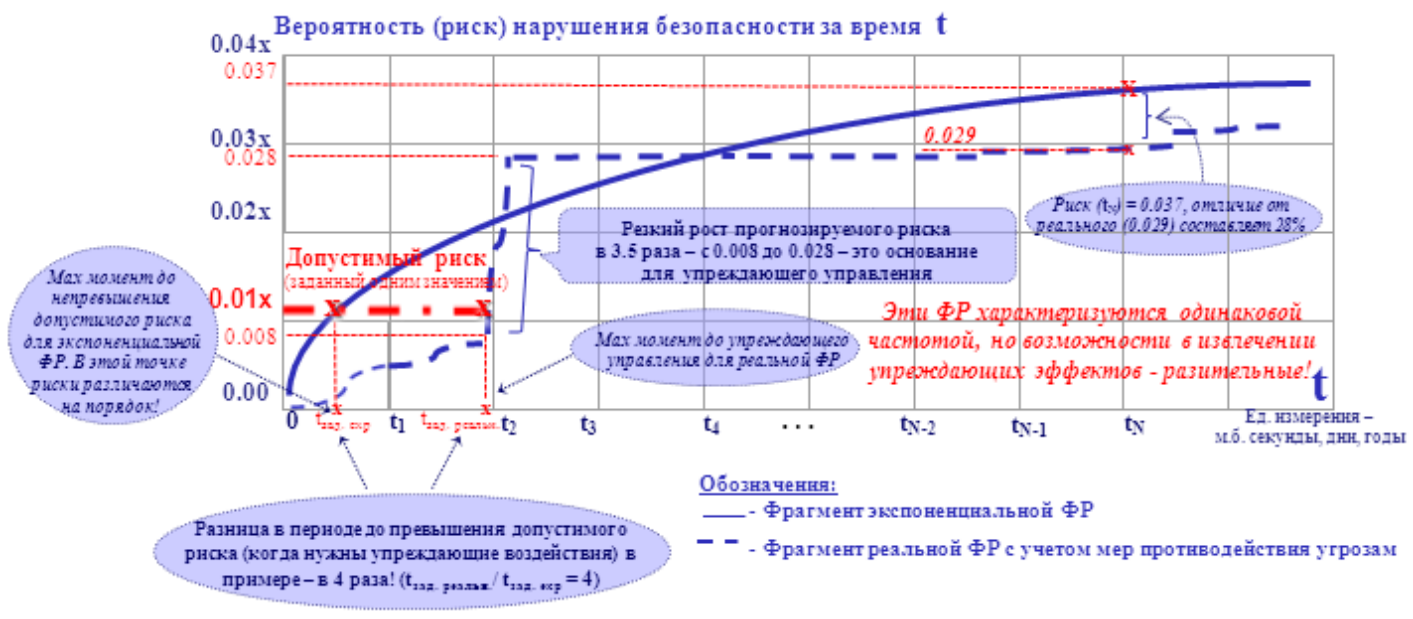


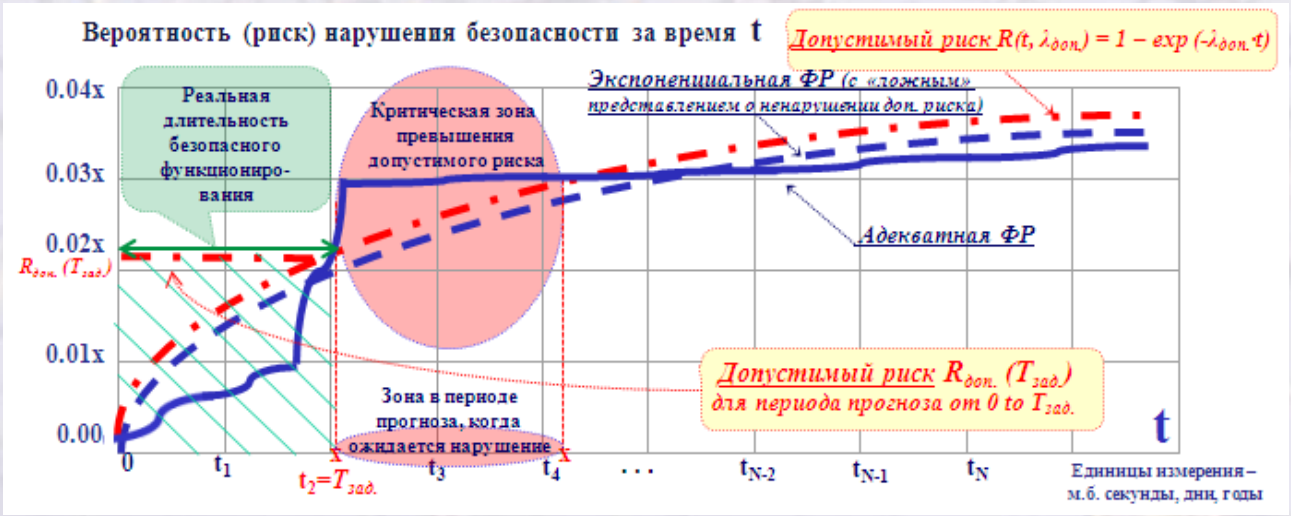
Подобные упрощенные представления - это начальные подходы 30-летней давности!

Заблуждения приводят к ошибкам (но к каким?)

ОШИБКИ – МНОГОКРАТНЫЕ !

Пример 1:
-разница во времени до требуемой реакции – в 4 раза;
- в ошибке роста риска – в 3.5 раза;
- в риске за заданный период прогноза -28%.





Пример 2:
ошибки в определении пределов реальной длительности безопасного функционирования – могут быть сотни, тысячи процентов!

Вывод: при существующем подходе аргументы для выработки эффективных упреждающих мер – отсутствуют или ошибочны!

ПОЯСНЕНИЕ СУТИ МОДЕЛИРУЕМЫХ ПРОЦЕССОВ РЕАЛИЗАЦИИ УГРОЗ И ПРОТИВОДЕЙСТВИЯ УГРОЗАМ

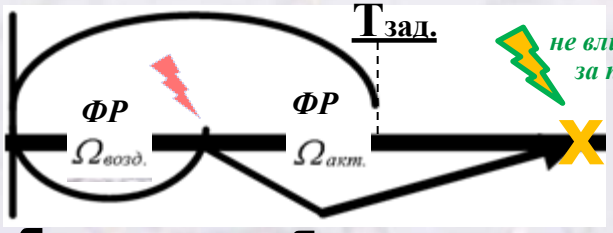
1. Проявление угроз без каких-либо мер контроля

(т.е. первая же угроза, если реализуется до истечения периода прогноза Тзад., приведет к нарушению)

Вероятность отсутствия нарушения $P(T_{зад.}) = 1 - R(T_{зад.})$

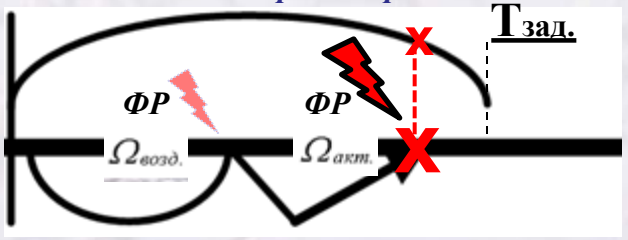
Риск нарушения целостности $R(T_{зад.}) = \Omega_{возд.} * \Omega_{акт.}(T_{зад.})$

Пример события «отсутствие нарушения целостности» в течение периода прогноза Тзад.



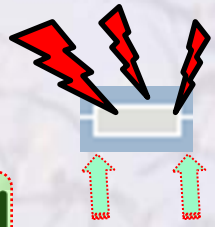
$\tau_{возникновения}$ $\tau_{развития\ угрозы}$

Пример события «нарушение целостности» в течение периода прогноза Тзад.



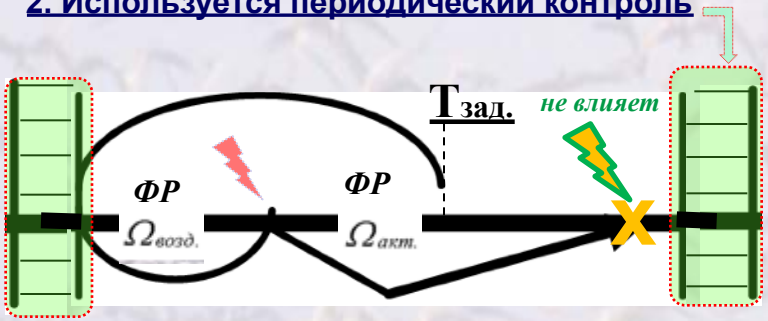
$$R = P(\tau_{возни.} + \tau_{развития\ угрозы} \leq T_{зад.})$$

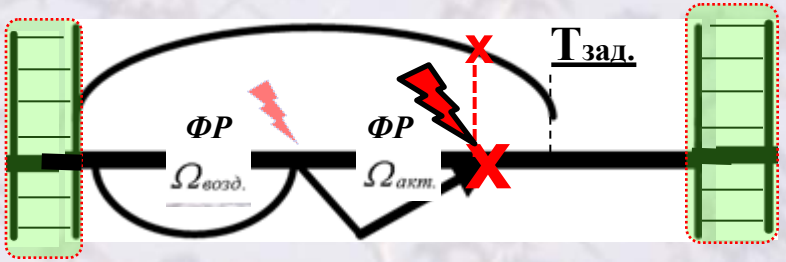
2. Используется периодический контроль



периодический контроль (без мониторинга)

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



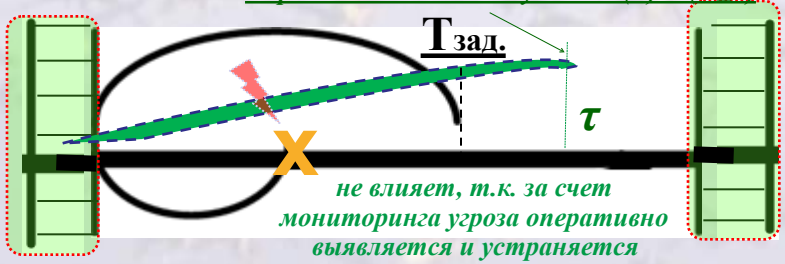


3. Внутри между моментами контроля используется мониторинг с оперативным восстановлением

мониторинг между контролями

(т.е. угроза приводит к нарушению, если реализуется в период прогноза после отказа средств мониторинга)

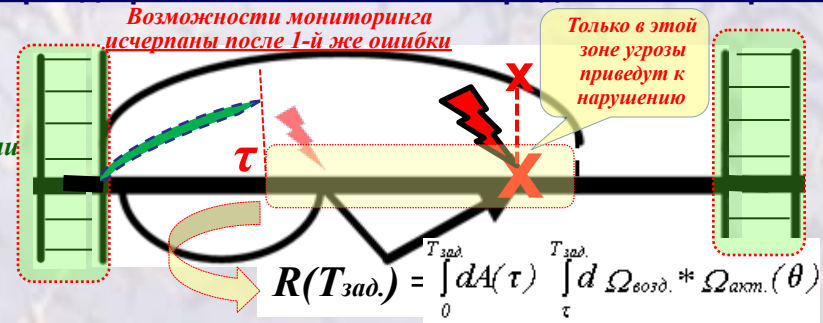
Наработка τ на ошибку с ФР A(T)=P(τ ≤T)



не влияет, т.к. за счет мониторинга угроза оперативно выявляется и устраняется

Возможности мониторинга исчерпаны после 1-й же ошибки

Только в этой зоне угрозы приведут к нарушению



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

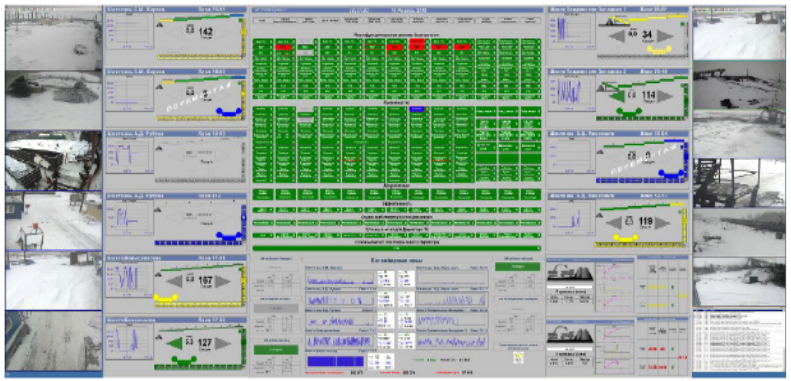
КАК РАБОТАЕТ ДЛЯ ОПАСНОГО ПРОИЗВОДСТВА?

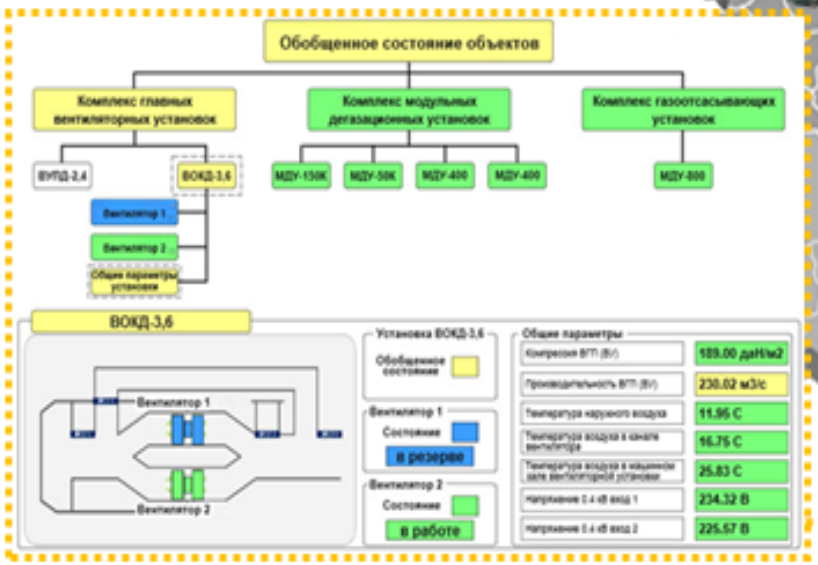
- задача, смежная с задачей деперсонификации

Риск – 1) 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)

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

ПРИМЕРЫ КОНТРОЛЯ И УПРАВЛЕНИЯ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

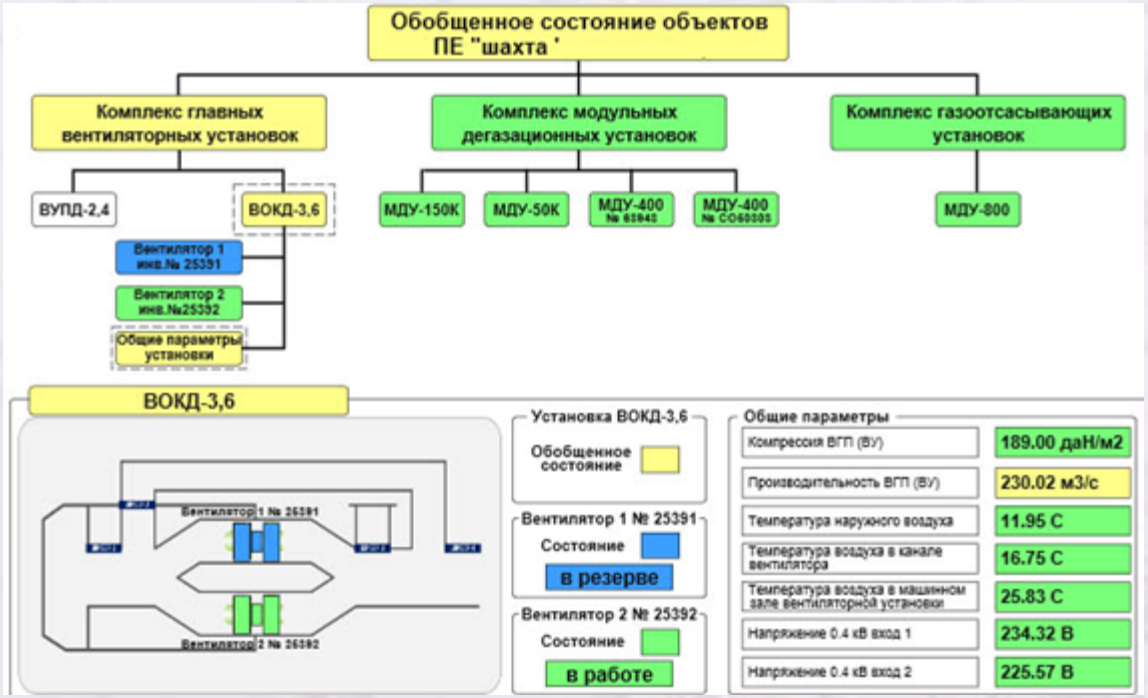




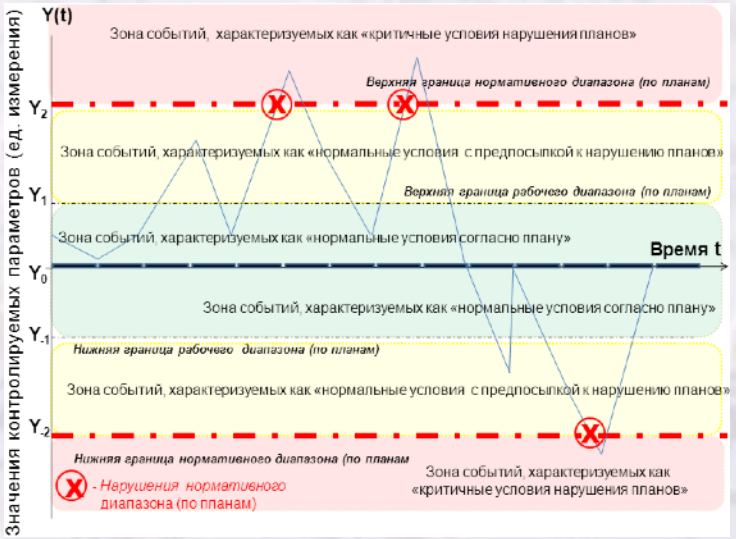
Общая идея для использования методов системной инженерии

Телеметрия системы дистанционного контроля – это источник исходных данных для прогнозирования рисков в режиме реального времени

Система дистанционного контроля (СДК ПБ) – это автоматизированная система, осуществляющая дистанционный мониторинг параметров и процессов, расчет и представление в режиме реального времени показателей состояния промышленной безопасности, информационно-аналитическую поддержку ответственных лиц для обеспечения нормальных условий функционирования объекта

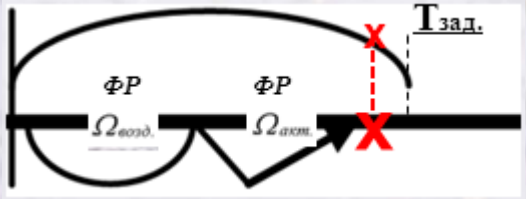


Методы системной инженерии



Значения параметров – это исходные данные для вероятностного моделирования

В общем случае «черного ящика» без контроля – от поломки до поломки



функция распределения (ФР) времени до нарушения определяется так:

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

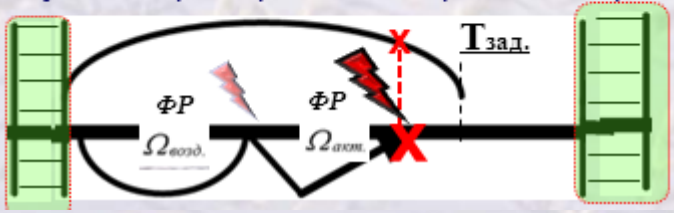
$\tau_{возн.}$ – время между возникновениями угрозы, ФР = $\Omega_{возд.}$

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

В случае периодического контроля – с упреждением

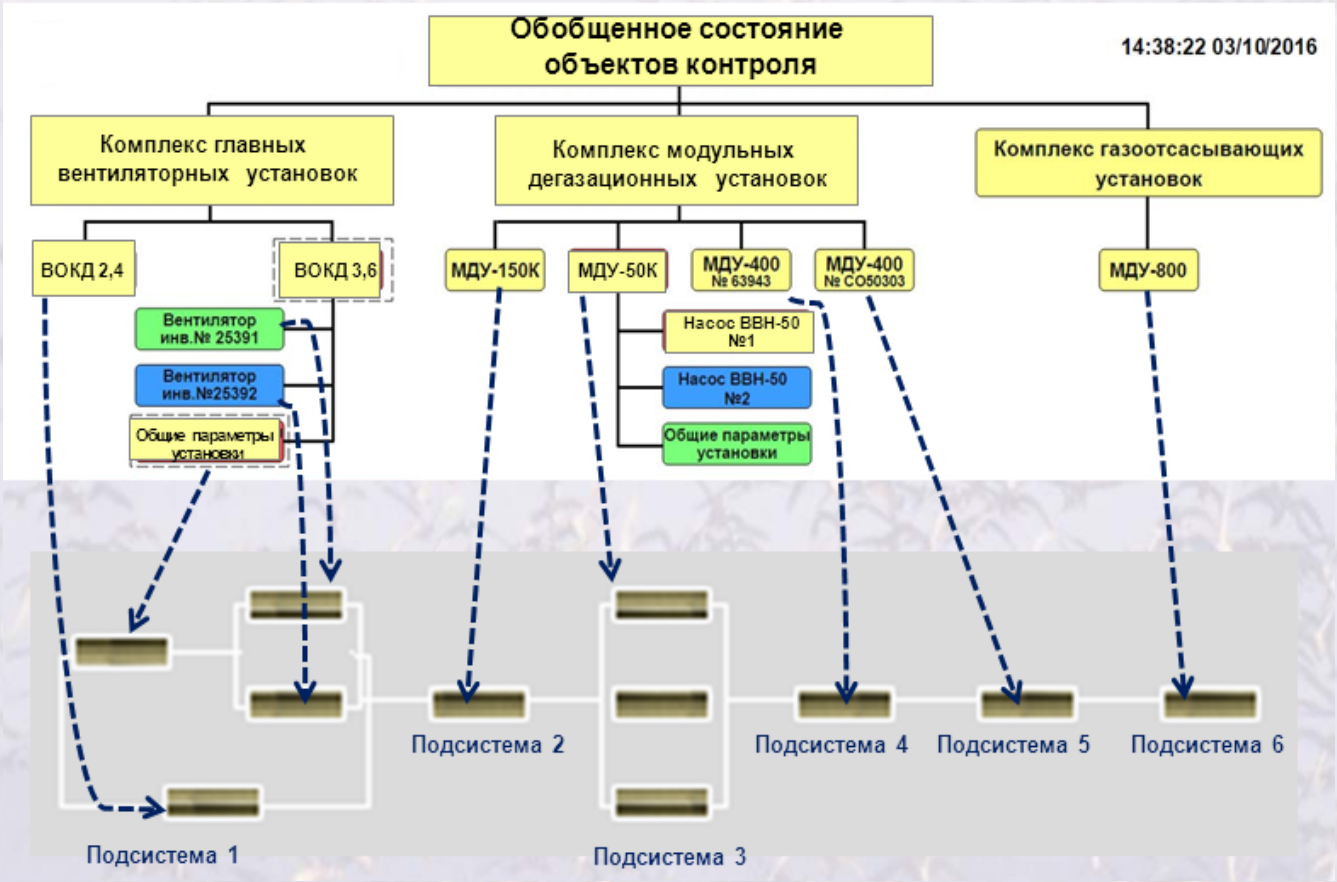
- реализуется периодический контроль

- угроза приводит к нарушению, если только она реализуется в период прогноза до очередного контроля



Методы системной инженерии

Примеры формирования логической структуры

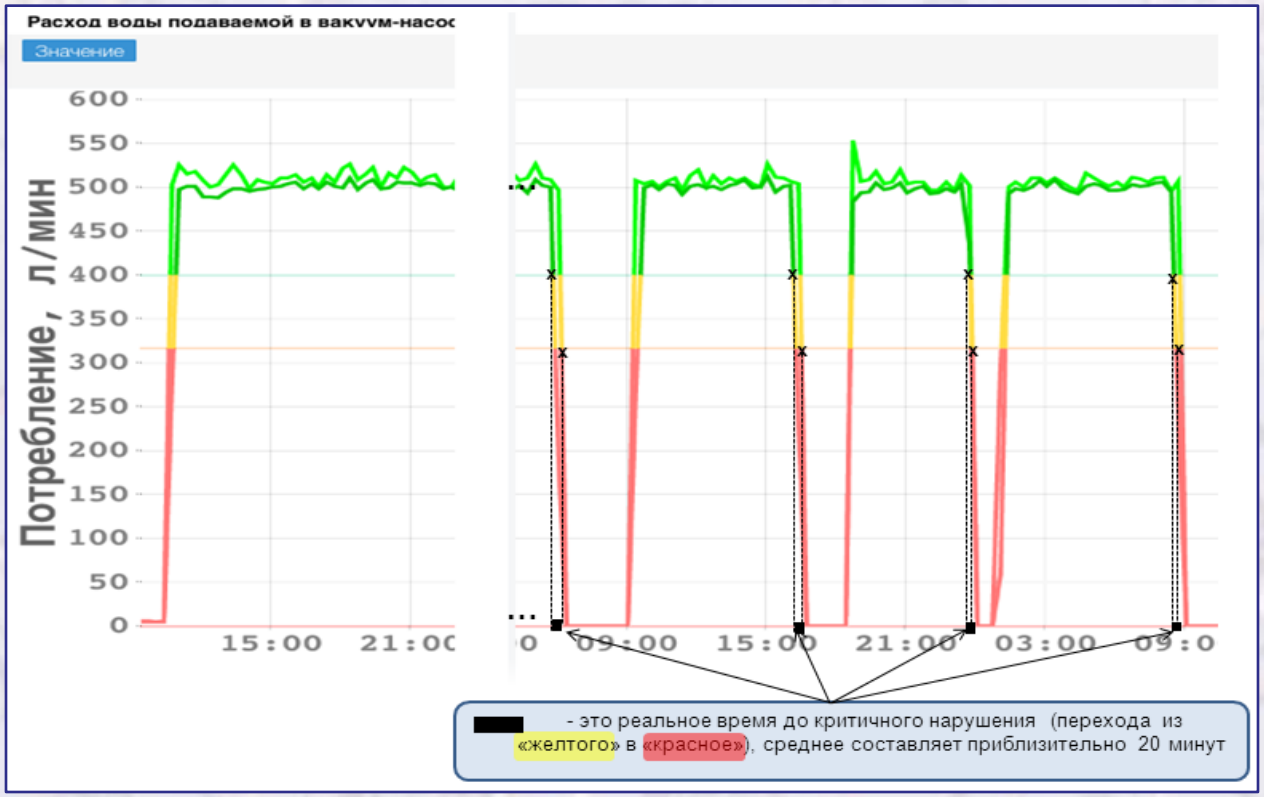


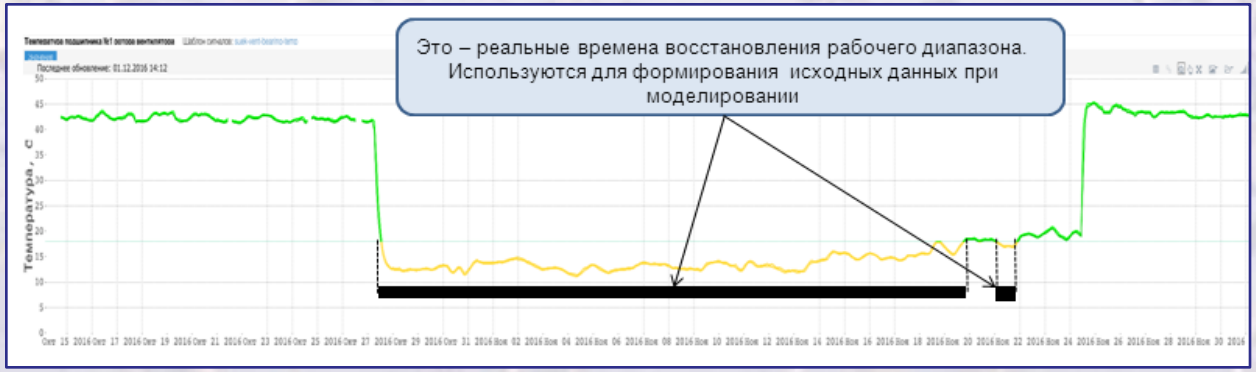
Исходные данные для расчетов риска:

– частота возникновения угроз;
– среднее время развития угроз с момента их возникновения до достижения критического уровня целостности;
– время между окончанием предыдущей и началом очередной диагностики целостности системы;
– длительность диагностики, включая восстановление целостности системы;
– длительность прогнозного периода времени

Пример формирования исходных данных для прогнозирования рисков (из статистики по одному параметру)

Методы системной инженерии





Алгоритм интеграции рисков (для разнородных угроз)

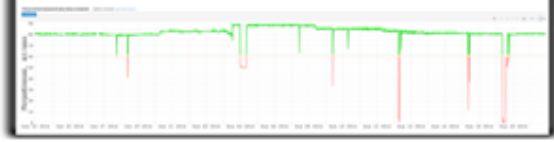
Методы системной инженерии

ИНТЕГРАЦИЯ РИСКОВ (на примере 2-х разнородных характеристик)

1. Определение «критичного нарушения»

«В системе в течение периода прогноза Тзад. будет хотя бы одно критичное нарушение, если за этот период ИЛИ в подсистеме 1 расход метано-воздушной смеси выйдет за пределы нормы, ИЛИ в подсистеме 2 температура подшипника выйдет за пределы нормы»

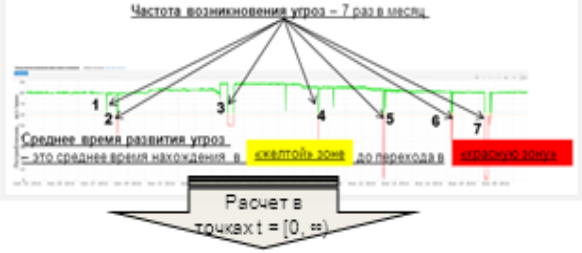
Подсистема 1) – характеристика расхода метано-воздушной смеси перед установкой



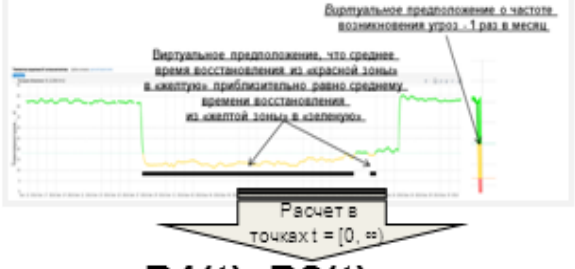
Подсистема 2) – характеристика температуры подшипника ротора вентилятора

2. Формирование исходных данных для расчетов рисков R1(t), R2(t)

1) Исходные данные по характеристике «расход метано-воздушной смеси перед установкой»



2) Исходные данные по характеристике «температура подшипника ротора вентилятора»



3. Расчет рисков «критичного нарушения» R1(t), R2(t) по моделям

На выходе - две вероятностные функции распределения (в точках t от 0 до ∞):

R1(t) – риск того, что за время t расход метано-воздушной смеси выйдет за пределы нормы;

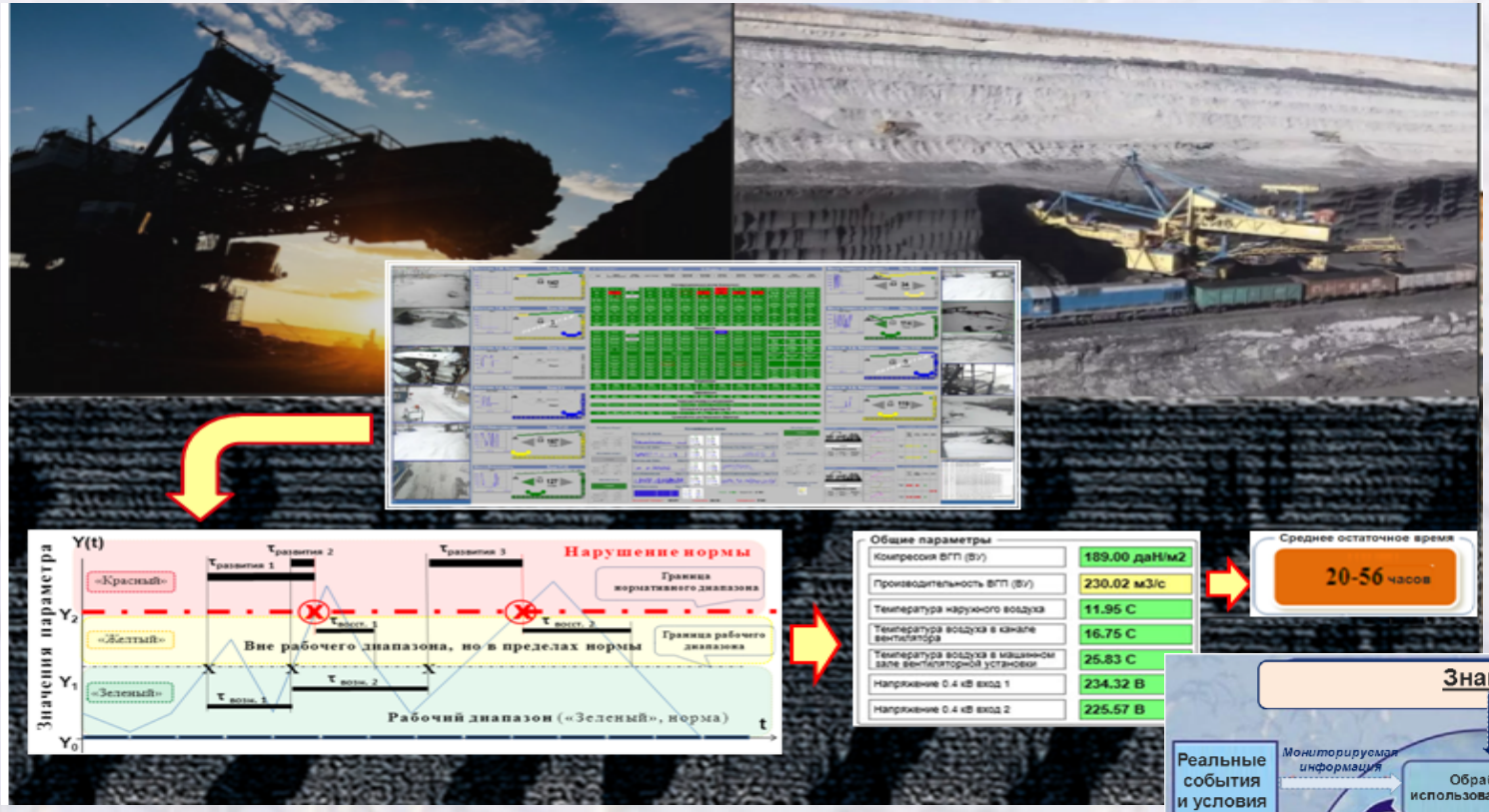
R2(t) – риск того, что за время t температура подшипника выйдет за пределы нормы.

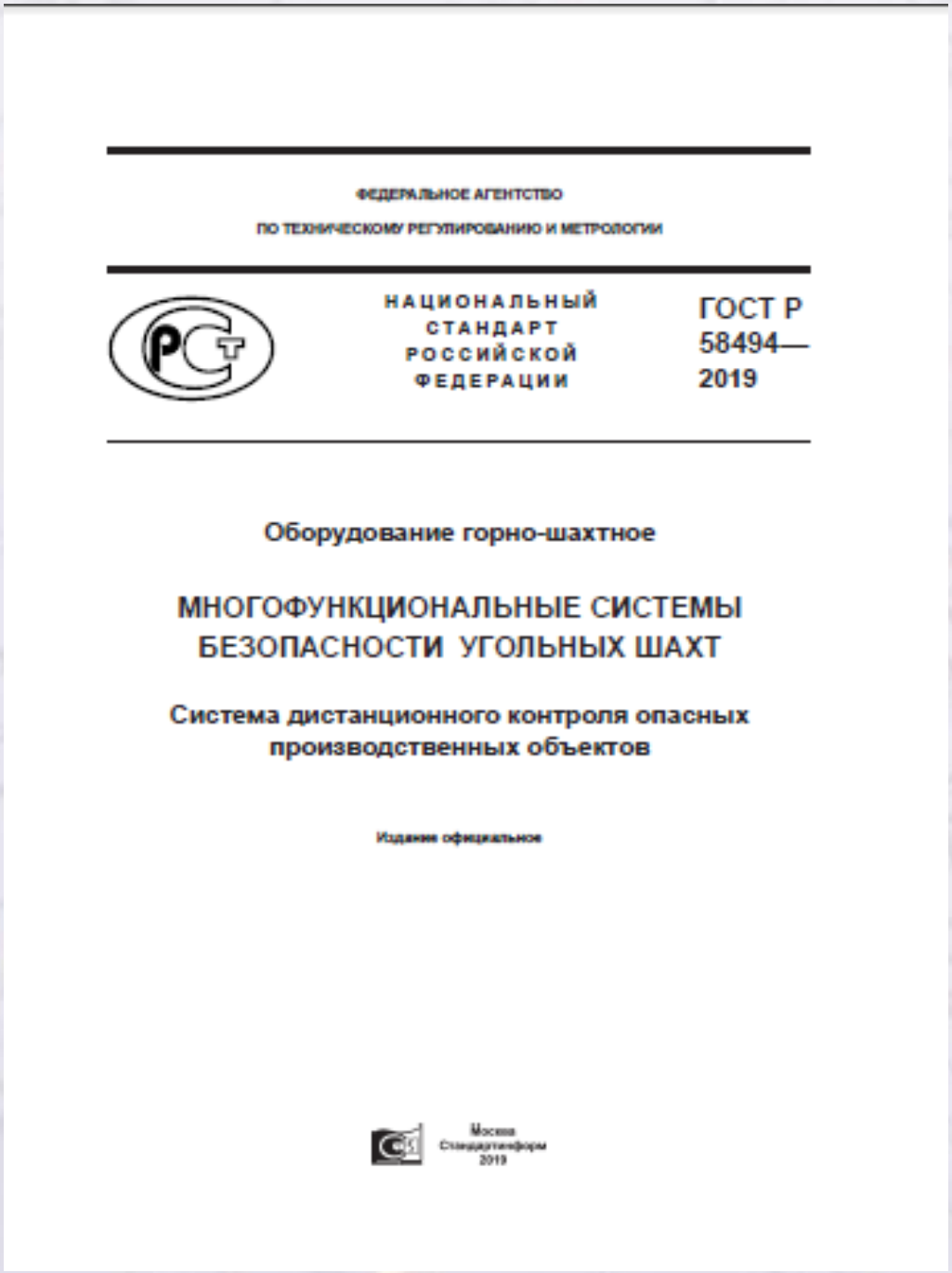
Эти функции зависят от частоты и среднего времени развития угроз, периода между моментами системной диагностики и длительности диагностики, времени восстановления целостности, наработки на ошибку (отказ) средств мониторинга.

4. Интегральный риск R(Тзад.) того, что за период прогноза Тзад. будет хотя бы одно критичное нарушение при соответствующем ущербе, равен

$$R(Тзад.) = 1 - [1 - R1(Тзад.)][1 - R2(Тзад.)]$$

Пример: прогнозирование остаточного времени





ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58494— 2019

Оборудование горно-шахтное

МНОГОФУНКЦИОНАЛЬНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ УГОЛЬНЫХ ШАХТ

Система дистанционного контроля опасных производственных объектов

Издание официальное

Москва
Стандартинформ
2019

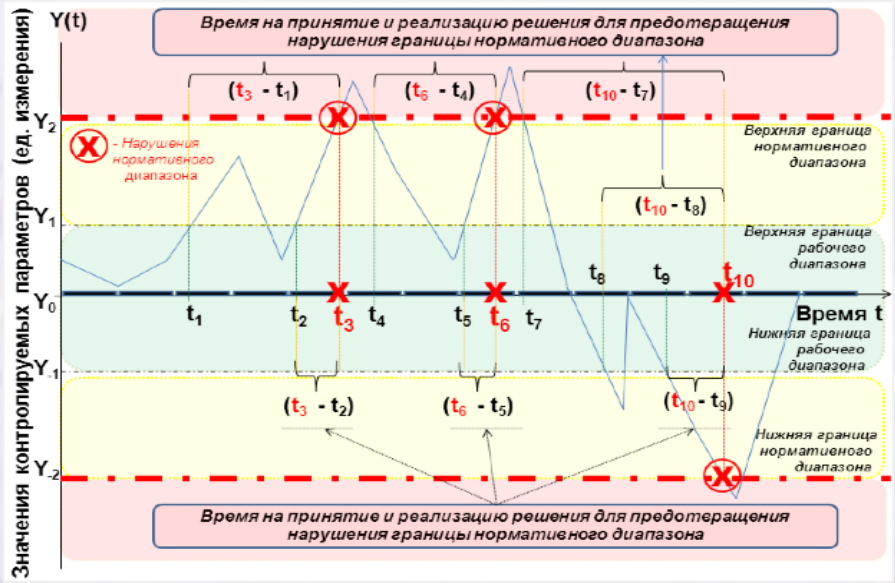
Применение стандарта при создании (модернизации, развитии) и эксплуатации СДК промышленной безопасности (ПБ) ОПО обеспечивает:

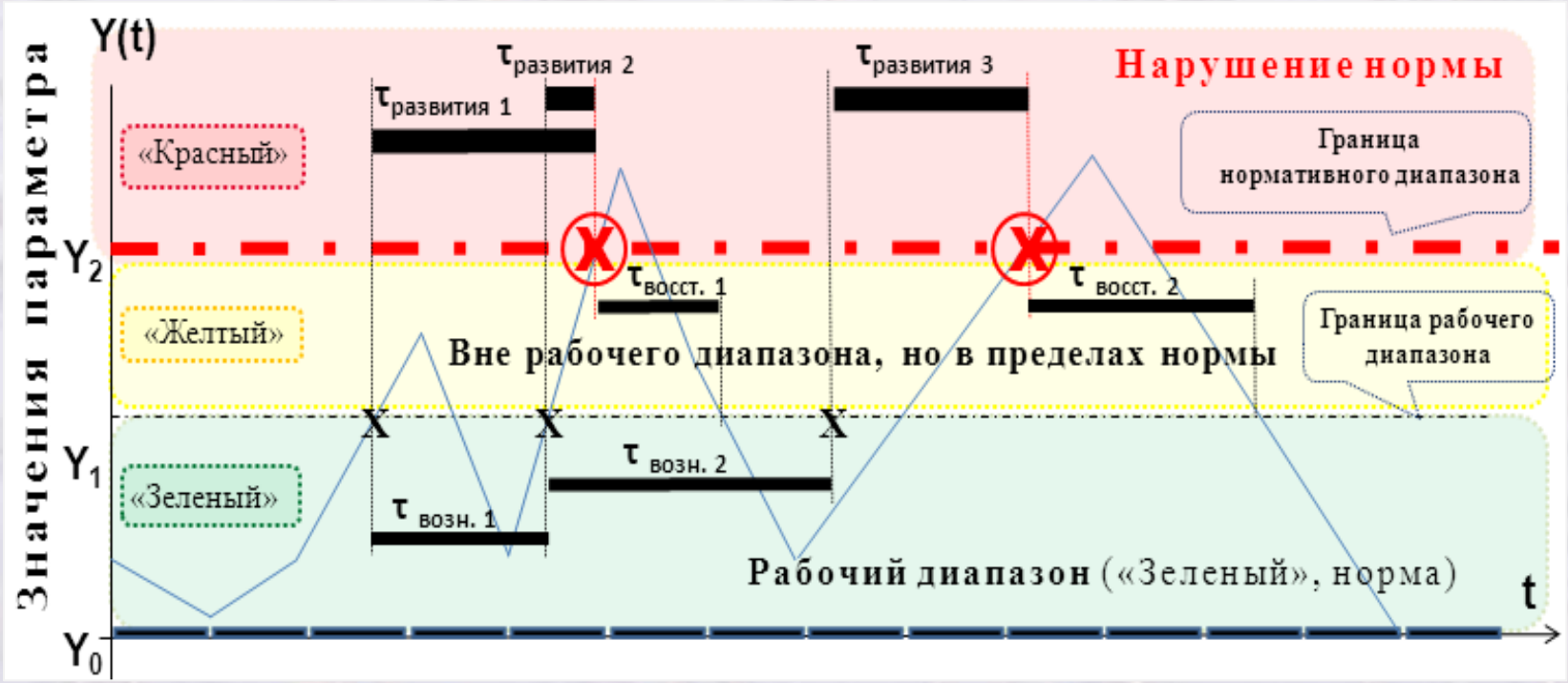
- раннее распознавание и оценку развития предпосылок к инцидентам и нарушению нормальных условий функционирования ОПО;
- прогнозирование рисков, выявление явных и скрытых недостатков и угроз, поддержку принятия решений по предотвращению в режиме реального времени возникновения на ОПО предаварийных и аварийных условий функционирования;
- определение сбалансированных мер обеспечения промышленной безопасности при средне- и долгосрочном планировании на ОПО;
- обоснование предложений по совершенствованию и развитию многофункциональных систем безопасности угольных шахт по результатам системного анализа информации СДК ПБ ОПО

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 4
4 Основные положения по созданию и применению 6
5 Общие требования 8
6 Специальные требования к количественным показателям состояния промышленной безопасности 15
7 Требования к качеству функционирования 17
8 Требования к системному анализу получаемой информации 18
Приложение А (справочное) Пример перечня оборудования, контролируемого СДК ПБ ОПО 22
Приложение Б (справочное) Пример перечня параметров оборудования, контролируемых СДК ПБ ОПО 23
Приложение В (справочное) Пример классификации событий 26
Приложение Г (справочное) Примеры задания нормативных и рабочих диапазонов контролируемых параметров оборудования 28
Приложение Д (справочное) Типовая номенклатура показателей 30
Приложение Е (справочное) Типовые методы и модели для системного анализа 32
Приложение Ж (справочное) Типовые модели для оценки качества функционирования. 50
Приложение И (обязательное) Типовые допустимые значения для показателей качества функционирования. 57
Приложение К (справочное) Примерный перечень методик системного анализа 59
Библиография 60

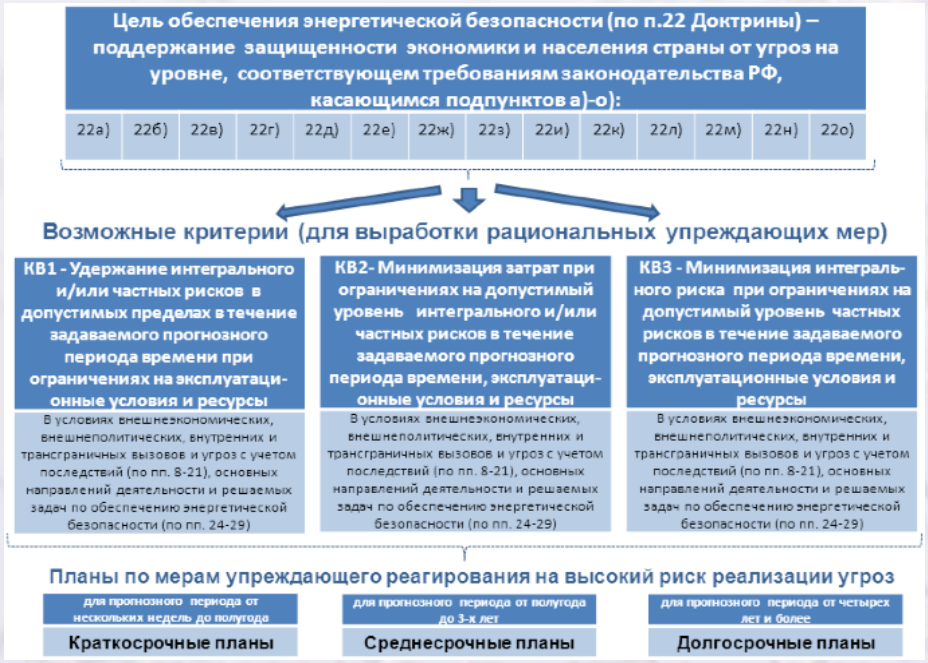
ОТ ЧАСТНОГО – К ОБЩЕМУ

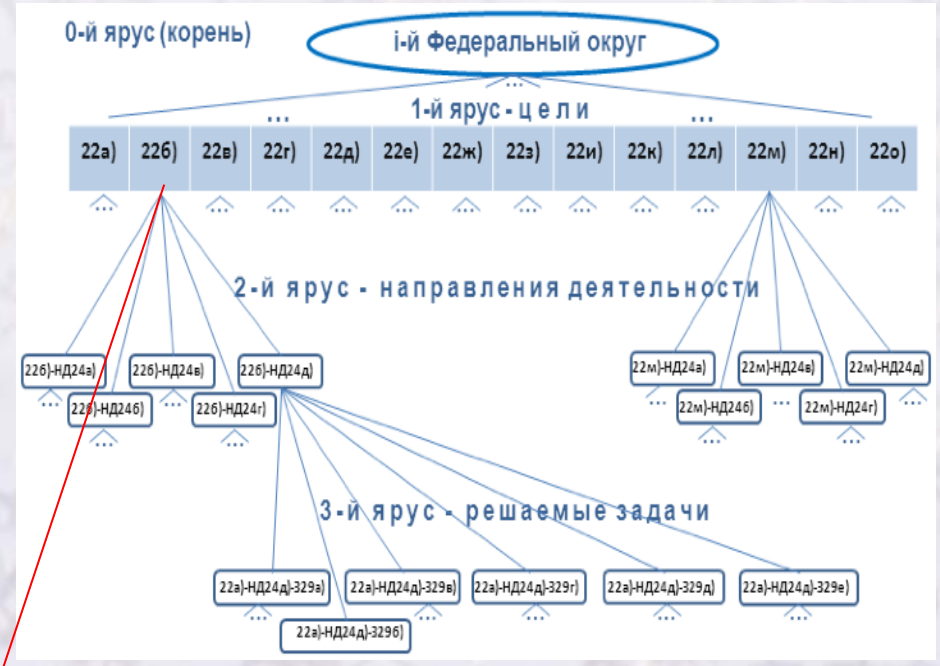




Пример: высококвалифицированный (робот) и средний уровень исполнения

из Доктрины энергетической безопасности





<u>Цель 22б)</u> - надежное и устойчивое обеспечение российских потребителей энергоресурсами стандартного качества и услугами в сфере энергетики

<u>Риск 22б)-Р17ж)</u> - риск высокого уровня износа основных производственных фондов организаций ТЭК, низкая эффективность использования и недостаточные темпы обновления этих фондов для достижения цели

Исходные данные для расчетов риска:

– частота возникновения угроз;
– среднее время развития угроз с момента их возникновения до достижения критического уровня;
– время между окончанием предыдущей и началом очередной диагностики целостности системы;
– длительности диагностики и восстановление целостности системы;
– длительность прогнозного периода времени

65 стандартов по информационной безопасности – в 2020 (1-18)

ИТ. Методы и средства обеспечения безопасности. Свод правил по управлению информационной безопасностью на основе ISO/IEC 27002 для облачных сервисов
ИТ. Методы и средства обеспечения безопасности. Свод норм и правил по управлению информационной безопасностью Взамен ГОСТ Р ИСО/МЭК 27002-2012
ИТ. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ИТ. Методы и средства обеспечения безопасности. Сетевая безопасность.. Часть 2. Руководящие указания по проектированию и реализации сетевой безопасности
Сетевая безопасность. Часть 4. Обеспечение ИТ. Методы и средства обеспечения безопасности. безопасности межсетевого взаимодействия с использованием шлюзов безопасности
ИТ. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 1. Обзор и основные понятия
ИТ. Информационная безопасность во взаимоотношениях с поставщиками. Часть 2. Требования
ИТ. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Руководящие указания по безопасности цепи поставок информационных и коммуникационных технологий
ИТ. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 4. Руководящие указания по безопасности облачных услуг
ИТ. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 2. Основы нормативного регулирования для организации
Облачные вычисления. Основы соглашения для уровня услуг. Часть 4. Компоненты безопасности и защиты персональной информации
ИТ. Методы и средства обеспечения безопасности. Оценка безопасности биометрии
ИТ. Методы и средства обеспечения безопасности. Руководящие указания по обеспечению безопасности при проектировании и реализации виртуализированных серверов
ИТ. Методы и средства обеспечения безопасности. Защита биометрической информации
ВЗАМЕН ГОСТ Р 56045-2014/ISO/IEC TR 27008:2011 ИТ. Методы и средства обеспечения безопасности. Руководящие указания по оценке средств управления информационной безопасностью
ИТ. Методы и средства обеспечения безопасности. Управление информационной безопасностью для связи между секторами и организациями
ИТ. Эталонная архитектура больших данных. Часть 4. Безопасность и конфиденциальность
ИТ. Методы и средства обеспечения безопасности. Управление информационной безопасностью. Экономика организации

65 стандартов по информационной безопасности – в 2020 (19-39)

ИТ. Методы и средства обеспечения безопасности. Свод правил для защиты персональных данных (ПДн) в публичных облаках, используемых для обработки ПДн
Безопасность машин. Вопросы защиты информации, связанные с функциональной безопасностью систем управления, связанных с безопасностью
ИТ. Методы и средства обеспечения безопасности. Руководящие указания по кибербезопасности
Сетевая безопасность. Часть 5. Обеспечение безопасности межсетевого взаимодействия с использованием виртуальных частных сетей (ВЧС)
ИТ. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 6. Защита сетевого доступа к беспроводной IP-сети
ИТ. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 3. Процесс управления безопасностью приложений
ИТ. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5. Структура данных протоколов и средств управления
ИТ. Безопасность приложений. Часть 5. Структура данных протоколов и средств управления. XML-схемы
ИТ. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 6. Практические примеры
ИТ. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 7. Основы прогнозирования гарантий безопасности
ИТ. Методы и средства обеспечения безопасности. Выбор, применение и эксплуатация систем обнаружения и предотвращения вторжений
ИТ. Методы и средства обеспечения безопасности. Безопасность хранения
ИТ. Методы и средства обеспечения безопасности. Руководство по обеспечению пригодности и адекватности метода расследования инцидентов
ИТ. Методы и средства обеспечения безопасности. Руководство по анализу и интерпретации цифровых доказательств
ИТ. Методы и средства обеспечения безопасности. Основные принципы и процессы расследования инцидентов
Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы
Системная инженерия. Защита информации в процессе управления инфраструктурой системы
Системная инженерия. Защита информации в процессе управления моделью жизненного цикла системы
Системная инженерия. Защита информации в процессе управления портфелем проектов
Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы

65 стандартов по информационной безопасности – в 2020 (40-65)

Системная инженерия. Защита информации в процессе управления качеством системы
Системная инженерия. Защита информации в процессе управления знаниями о системе
Системная инженерия. Защита информации в процессе планирования проекта
Системная инженерия. Защита информации в процессе оценки и контроля проекта
Системная инженерия. Защита информации в процессе управления решениями
Системная инженерия. Защита информации в процессе управления рисками для системы
Системная инженерия. Защита информации в процессе управления конфигурацией системы
Системная инженерия. Защита информации в процессе управления информацией системы
Системная инженерия. Защита информации в процессе измерений системы
Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы
Системная инженерия. Защита информации в процессе определения потребностей и требований заинтересованной стороны для системы
Системная и программная инженерия. Защита информации в процессе определения системных требований
Системная и программная инженерия. Защита информации в процессе определения архитектуры системы
Системная инженерия. Защита информации в процессе определения проекта
Системная и программная инженерия. Защита информации в процессе реализации системы
Системная инженерия. Защита информации в процессе сопровождения системы
Системная и программная инженерия. Защита информации в процессе гарантии качества для системы
Системная инженерия. Защита информации в процессе системного анализа
Системная инженерия. Защита информации в процессе верификации системы
Системная и программная инженерия. Защита информации в процессе функционирования системы
Измерение, управление и автоматизация промышленного процесса. Основные принципы обеспечения функциональной безопасности и защиты информации
Системная инженерия. Защита информации в процессе комплексирования системы
Системная инженерия. Защита информации в процессе передачи системы
Системная и программная инженерия. Защита информации в процессе аттестации (валидации) системы
Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 4. Объяснения и обоснования изменений, внесенных в редакцию 2 МЭК 61511-1
Системная инженерия. Защита информации в процессе изъятия и списания системы

Из Постановления Правительства РФ от 21.03.2019г № 289, существенно расширившего применение риск-ориентированного подхода на различные сферы федерального и регионального государственного контроля и надзора

ПЕРЕЧЕНЬ

видов федерального государственного контроля (надзора), в отношении которых применяется риск-ориентированный подход

1. Федеральный государственный пожарный надзор
2. Федеральный государственный санитарно-эпидемиологический надзор, осуществляемый Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека и Федеральным медико-биологическим агентством
3. Федеральный государственный надзор в области связи
4. Федеральный государственный надзор за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права
5. Федеральный государственный контроль (надзор) в сфере миграции
6. Федеральный государственный надзор в области безопасности дорожного движения
7. Федеральный государственный экологический надзор
8. Государственный земельный надзор
9. Государственный карантинный фитосанитарный контроль (надзор)
10. Федеральный государственный транспортный надзор
11. Федеральный государственный контроль (надзор) в области транспортной безопасности
12. Федеральный государственный надзор в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера
13. Государственный надзор в области гражданской обороны
14. Государственный надзор во внутренних водах и в территориальном море Российской Федерации за маломерными судами, используемыми в некоммерческих целях, и базами (сооружениями) для их стоянок
15. Государственный контроль качества и безопасности медицинской деятельности
16. Федеральный государственный надзор в сфере обращения лекарственных средств
17. Государственный контроль за обращением медицинских изделий
18. Федеральный государственный надзор в области защиты прав потребителей
19. Федеральный государственный энергетический надзор
20. Государственный контроль за соблюдением антимонопольного законодательства Российской Федерации
21. Контроль за соблюдением законодательства Российской Федерации и иных нормативных правовых актов о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, осуществляемый Федеральной антимонопольной службой
22. Государственный контроль (надзор) в сфере государственного оборонного заказа
23. Федеральный государственный метрологический надзор, осуществляемый Федеральным агентством по техническому регулированию и метрологии
24. Федеральный государственный ветеринарный надзор

ПЕРЕЧЕНЬ

видов регионального государственного контроля (надзора), при организации которых риск-ориентированный подход применяется в обязательном порядке

1. Региональный государственный экологический надзор
2. Региональный государственный строительный надзор
3. Государственный жилищный надзор
4. Региональный государственный надзор в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера
5. Государственный надзор за обеспечением сохранности автомобильных дорог регионального и межмуниципального значений
6. Государственный контроль (надзор) в области регулируемых государством цен (тарифов)
7. Региональный государственный ветеринарный надзор".

Из Постановления Правительства РФ от 21.03.2019г № 289, существенно расширившего применение риск-ориентированного подхода на различные сферы федерального и регионального государственного контроля и надзора

ПЕРЕЧЕНЬ

видов федерального государственного контроля (надзора), в отношении которых применяется риск-ориентированный подход

1. Федеральный государственный пожарный надзор
2. Федеральный государственный санитарно-эпидемиологический надзор, осуществляемый Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека и Федеральным медико-биологическим агентством
3. Федеральный государственный надзор в области связи
4. Федеральный государственный надзор за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права
5. Федеральный государственный контроль (надзор) в сфере миграции
6. Федеральный государственный надзор в области безопасности дорожного движения
7. Федеральный государственный экологический надзор
8. Государственный земельный надзор
9. Государственный карантинный фитосанитарный контроль (надзор)
10. Федеральный государственный транспортный надзор
11. Федеральный государственный контроль (надзор) в области транспортной безопасности
12. Федеральный государственный надзор в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера
13. Государственный надзор в области гражданской обороны
14. Государственный надзор во внутренних водах и в территориальном море Российской Федерации за маломерными судами, используемыми в некоммерческих целях, и базами (сооружениями) для их стоянок
15. Государственный контроль качества и безопасности медицинской деятельности
16. Федеральный государственный надзор в сфере обращения лекарственных средств
17. Государственный контроль за обращением медицинских изделий
18. Федеральный государственный надзор в области защиты прав потребителей
19. Федеральный государственный энергетический надзор
20. Государственный контроль за соблюдением антимонопольного законодательства Российской Федерации
21. Контроль за соблюдением законодательства Российской Федерации и иных нормативных правовых актов о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, осуществляемый Федеральной антимонопольной службой
22. Государственный контроль (надзор) в сфере государственного оборонного заказа
23. Федеральный государственный метрологический надзор, осуществляемый Федеральным агентством по техническому регулированию и метрологии
24. Федеральный государственный ветеринарный надзор

ПЕРЕЧЕНЬ

видов регионального государственного контроля (надзора), при организации которых риск-ориентированный подход применяется в обязательном порядке

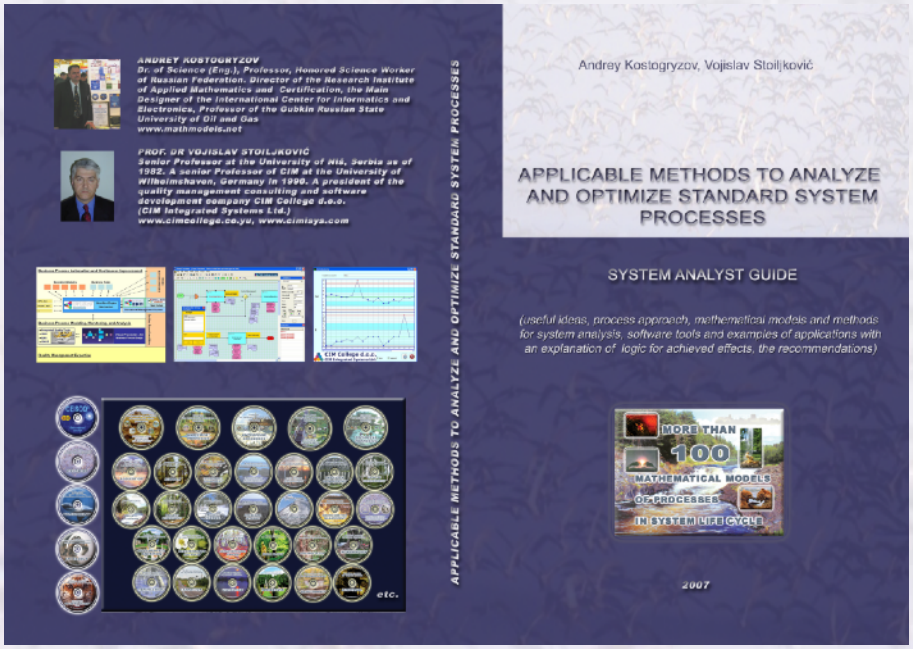
1. Региональный государственный экологический надзор
2. Региональный государственный строительный надзор
3. Государственный жилищный надзор
4. Региональный государственный надзор в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера
5. Государственный надзор за обеспечением сохранности автомобильных дорог регионального и межмуниципального значений
6. Государственный контроль (надзор) в области регулируемых государством цен (тарифов)
7. Региональный государственный ветеринарный надзор".

ПРЕДЛОЖЕНИЕ

- продолжать целенаправленное внедрение предложенного подхода в решение проблем информационной безопасности

2005

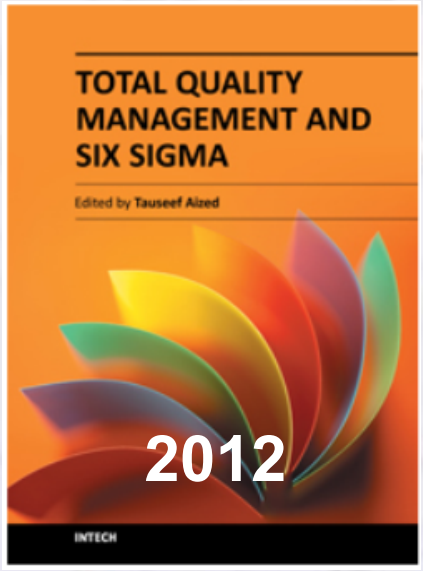
2007

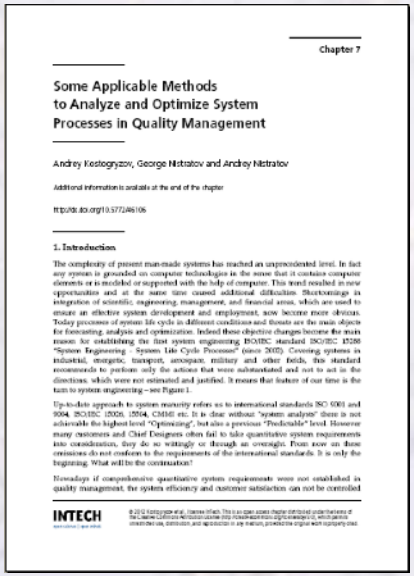


2008

2010

Монографии 2012-2015




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

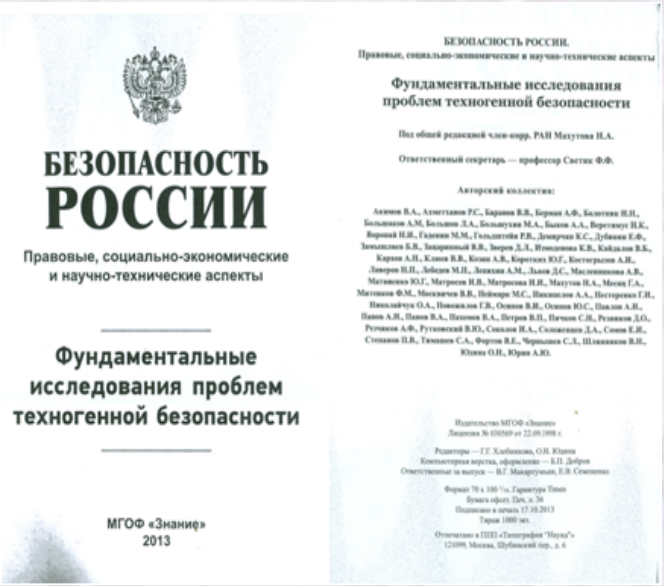
1. Introduction

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 modelled or supported with the help of computer. This trend reached 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 substandardized 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 analysis" 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

INTECH


БЕЗОПАСНОСТЬ
РОССИИ

Правовые, социально-экономические и научно-технические аспекты

Фундаментальные исследования проблем техногенной безопасности

МГОФ «Знание»
2013

БЕЗОПАСНОСТЬ РОССИИ.
Правовые, социально-экономические и научно-технические аспекты

Фундаментальные исследования проблем техногенной безопасности

Под общей редакцией член-корр. РАН Макутова Н.А.

Ответственный секретарь — профессор Светик Ф.Ф.

Авторский коллектив:


БЕЗОПАСНОСТЬ
РОССИИ

Правовые, социально-экономические и научно-технические аспекты

Тематический блок
«НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ»

Научные основы техногенной безопасности

МГОФ «Знание»

БЕЗОПАСНОСТЬ РОССИИ
Правовые, социально-экономические и научно-технические аспекты

Тематический блок
«НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ»

Научные основы техногенной безопасности

Авторский коллектив:

2015, 2017гг. – раздел «ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ РИСКАМИ НА ОСНОВЕ ПРОГНОЗНОГО МОДЕЛИРОВАНИЯ СИСТЕМНЫХ ПРОЦЕССОВ»