

**Комитет Торгово-промышленной палаты Российской Федерации  
по промышленной безопасности – заседание 14.10.2020**

# **Вопросы подготовки и публичного обсуждения стандартов по системной инженерии и защите информации**

**Дтн, проф. 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

**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)



# ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем» (ISO/IEC/IEEE 15288 )

## Процессы жизненного цикла систем



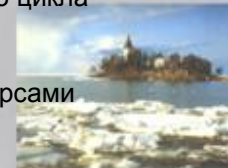
### Процессы соглашения

процесс приобретения  
процесс поставки



### Процессы организационного обеспечения проекта

процесс управления моделью жизненного цикла  
процесс управления инфраструктурой  
процесс управления портфелем  
процесс управления человеческими ресурсами  
процесс управления качеством  
процесс управления знаниями



### Процессы технического управления

процесс планирования проекта  
процесс оценки и контроля проекта  
процесс управления решениями  
процесс управления рисками  
процесс управления конфигурацией  
процесс управления информацией  
процесс измерений  
процесс гарантии качества



### Технические процессы

процесс анализа бизнеса или назначения  
процесс определения потребностей и требований заинтересованной стороны  
процесс определения системных требований  
процесс определения архитектуры  
процесс определения проекта  
процесс системного анализа  
процесс реализации  
процесс комплексирования  
процесс верификации  
процесс передачи  
процесс валидации  
процесс функционирования  
процесс сопровождения  
процесс изъятия и списания





# ПРИМЕРЫ КРИТИЧЕСКИ ВАЖНЫХ СИСТЕМ

## Гидроэнергетика



## Атомная промышленность



## Нефте- и газодобыча



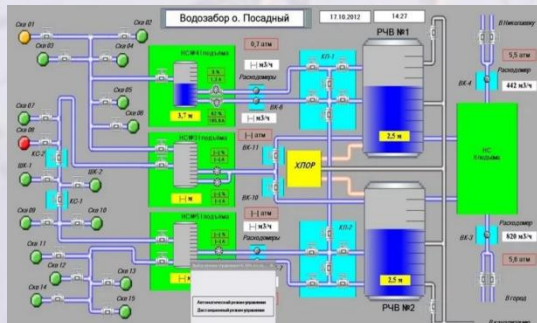
## Обработка, транспортировка нефти и газа



## Нефтехимическая промышленность



## ЖКХ



## Управление транспортом



## Военные приложения

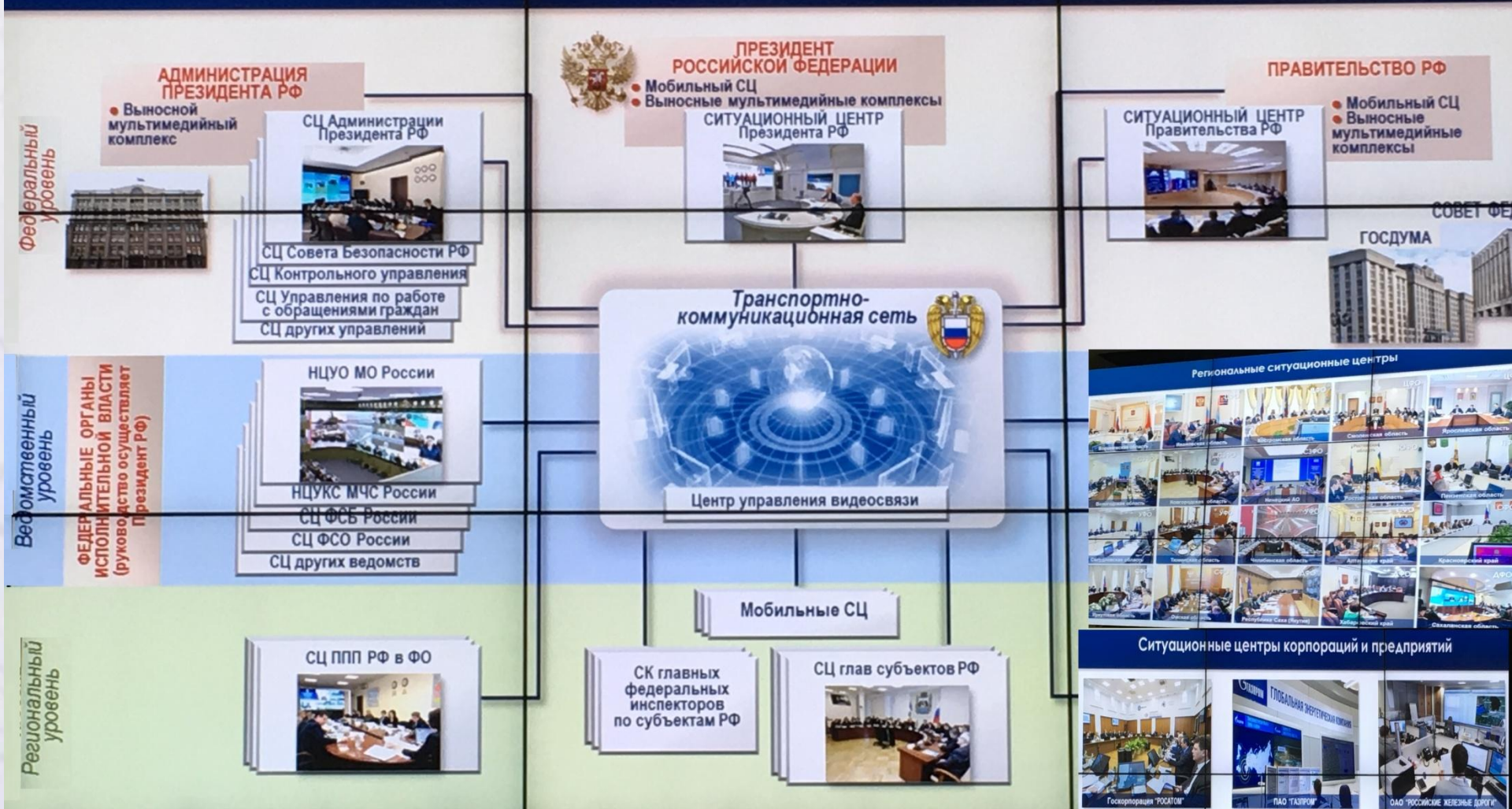


и др.



# ПРИМЕРЫ СИСТЕМ ПРИНЯТИЯ РЕШЕНИЙ

## Система распределённых ситуационных центров



Пример статистики



Фрагменты - из выступления Н.И. Ильина на 5-й Всероссийской научно-практической конференции «Аналитика развития и безопасности России: Культура, инфраструктура и интеллектуальные технологии государственного управления», 15 ноября 2018г., Москва

# ПО ЗАКАЗУ РОССТАНДАРТА – СОЗДАНЫ ПРОЕКТЫ

## Информационная безопасность (состояние защищенности)

**общие** - ISO/IEC 27000:2018(3), ISO/IEC 27002:2013(2), стандарты системной инженерии,  
**сетевая безопасность** -ISO/IEC 27033-2:2012(4), ISO/IEC 27033:2014(5), ISO/IEC 21878:2018(13),ISO/IEC 27033-5:2016(23), ISO/IEC 27033-6:2016(24), **безопасность приложений** - ISO/IEC 27034-2:2015(10), ISO/IEC 27034-3:2018(25), ISO/IEC 27034-5:2017(26), ISO/IEC 27034-5-1:2018(27), ISO/IEC 27034-6:2016(28),  
**биометрия** - ISO/IEC 19792:2009(12), **оценка** - ISO/IEC TR 27008:2019(15), ISO/IEC 27034-7:2018(29),  
**управление** - ISO/IEC 27010:2015(16), **экономика** - ISO/IEC TR 27016:2014(18),  
**кибербезопасность** -ISO/IEC 27032:2012(22), ISO/IEC 27039:2015(30), **хранение** - ISO/IEC 27040:2015(31),  
**расследование** - ISO/IEC 27041:2015(32), ISO/IEC 27042:2015(33), ISO/IEC 27043:2015(34)

## Большие данные

## З а щ и т а                      и н ф о р м а ц и о н н ы х                      т е х н о л о г и й

**Специальные приложения:** в энергетике-ISO/IEC 27019:2017(20), **функциональная безопасность машин**-IEC TR63074:2019(21), IEC TR 63069:2019(60), IEC TR 61511-4:2020(64)

**Общие:** стандарты системной инженерии, **с поставщиками** -ISO/IEC 27036-1:2014(6), ISO/IEC 27036-2:2014(7), ISO/IEC 27036-3:2013(8), **ISO/IEC 27036-4:2016(9)**, **архитектура** - ISO/IEC DIS 20547-4(17), **защита биометрии** - ISO/IEC 24745:2011(14),

### Облачные и туманные

ISO/IEC 27017:2015(1), **ISO/IEC 27036-4:2016(9)**,  
перс.ISO/IEC19086-4:2019(11),  
ISO/IEC27018: 2019(19),  
стандарты системной инженерии

### Квантовые

- стандарты  
системной  
инженерии

### Виртуальной и дополненной реальности

- стандарты  
системной  
инженерии

### Искусствен- ного интеллекта

- стандарты  
системной  
инженерии



## Для процессов приобретения и поставки

35. Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы



## Для процессов организационного обеспечения проекта

36. Системная инженерия. Защита информации в процессе управления инфраструктурой системы

37. Системная инженерия. Защита информации в процессе управления моделью жизненного цикла системы



40. Системная инженерия. Защита информации в процессе управления качеством системы

41. Системная инженерия. Защита информации в процессе управления знаниями о системе

## Для процессов технического управления

42. Системная инженерия. Защита информации в процессе планирования проекта

43. Системная инженерия. Защита информации в процессе оценки и контроля проекта

44. Системная инженерия. Защита информации в процессе управления решениями

45. Системная инженерия. Защита информации в процессе управления рисками для системы

46. Системная инженерия. Защита информации в процессе управления конфигурацией системы

47. Системная инженерия. Защита информации в процессе управления информацией системы

48. Системная инженерия. Защита информации в процессе измерений системы



## Для технических процессов

49. Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы

50. Системная инженерия. Защита информации в процессе определения потребностей и требований заинтересованной стороны для системы

51. Системная и программная инженерия. Защита информации в процессе определения системных требований

52. Системная и программная инженерия. Защита информации в процессе определения архитектуры системы

53. Системная инженерия. Защита информации в процессе определения проекта

54. Системная и программная инженерия. Защита информации в процессе реализации системы

55. Системная инженерия. Защита информации в процессе сопровождения системы

56. Системная и программная инженерия. Защита информации в процессе гарантии качества для системы

57. Системная инженерия. Защита информации в процессе системного анализа

58. Системная инженерия. Защита информации в процессе верификации системы

59. Системная и программная инженерия. Защита информации в процессе функционирования системы

61. Системная инженерия. Защита информации в процессе комплексирования системы

63. Системная инженерия. Защита информации в процессе передачи системы

64. Системная и программная инженерия. Защита информации в процессе аттестации (валидации) системы

65. Системная инженерия. Защита информации в процессе изъятия и списания системы



# **РЕАЛИЗОВАН ПОДХОД**

**от частного к общему  
+ обратная связь на  
современном уровне  
понимания и возможностей**

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



**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**

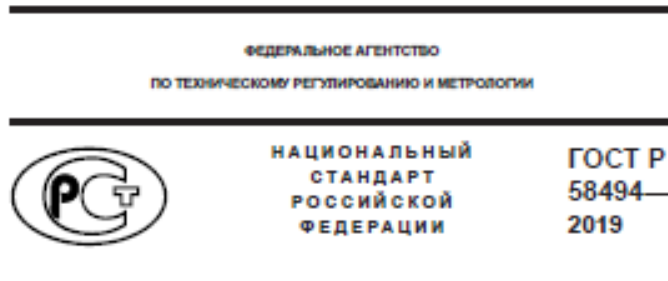
<b>П Е Р Е Ч Е Н Ь</b>			
<b>видов федерального государственного контроля (надзора), в отношении которых применяется риск-ориентированный подход</b>			
1.	Федеральный государственный пожарный надзор		
2.	Федеральный государственный санитарно-эпидемиологический надзор, осуществляемый Федеральной службой 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

<b>П Е Р Е Ч Е Н Ь</b>	
<b>видов регионального государственного контроля (надзора), при организации которых риск-ориентированный подход применяется в обязательном порядке</b>	
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".

**ЭТО – ТЕНДЕНЦИЯ!**

# ЧАСТНОЕ - ПОЛОЖИТЕЛЬНЫЙ ПРИМЕР – ГОСТ Р 58494-2019



*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*

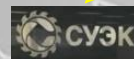


# Пример - система дистанционного контроля

Общая идея для использования методов системной инженерии

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

Ростехнадзор



АО в Москве

Направление сигнала обобщенного состояния

Направление предупредительного сигнала

Контроль за выполнением мер для устранения причин отклонений

Региональное управление Ростехнадзора

АС в регионе

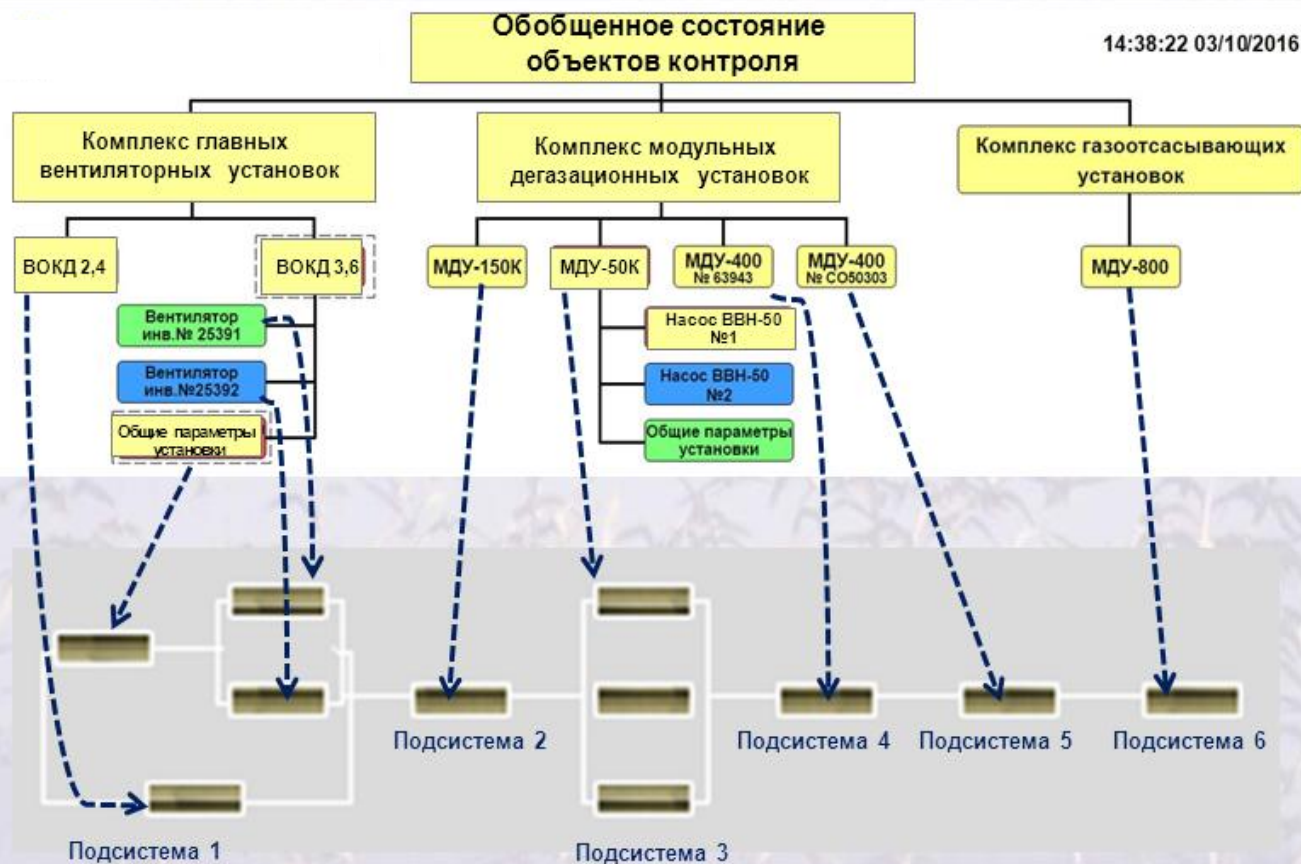
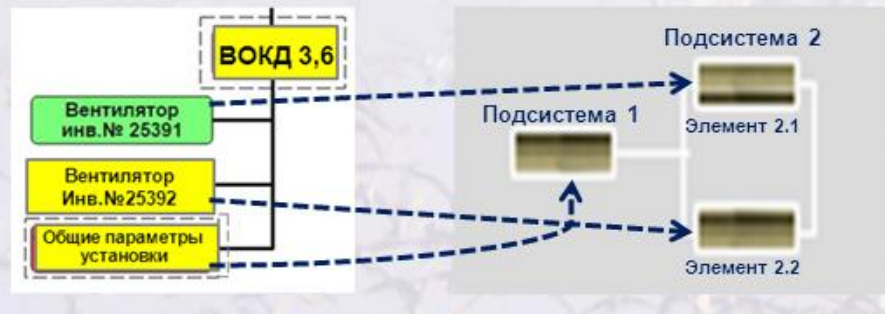


Система дистанционного контроля (СДК ПБ) – это автоматизированная система, осуществляющая дистанционный мониторинг параметров и процессов, расчет и представление в режиме реального времени показателей состояния промышленной безопасности, информационно-аналитическую поддержку ответственных лиц для обеспечения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

## ДЕКОМПОЗИЦИЯ

# Примеры формирования логической структуры

Формальное представление сложной структуры для прогнозирования рисков нарушения ПБ



### Исходные данные для расчетов риска:

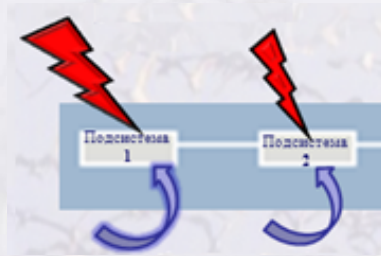
- частота возникновения угроз;
- среднее время развития угроз с момента их возникновения до достижения критического уровня целостности;
- время между окончанием предыдущей и началом очередной диагностики целостности системы;
- длительность диагностики, включая восстановление целостности системы;
- длительность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



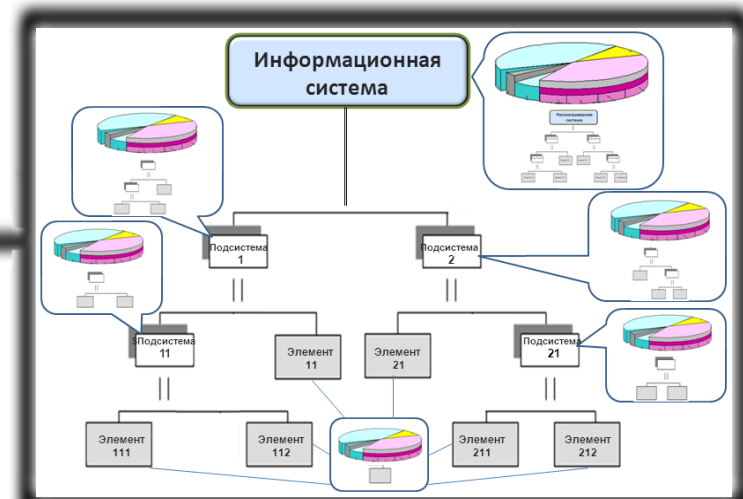
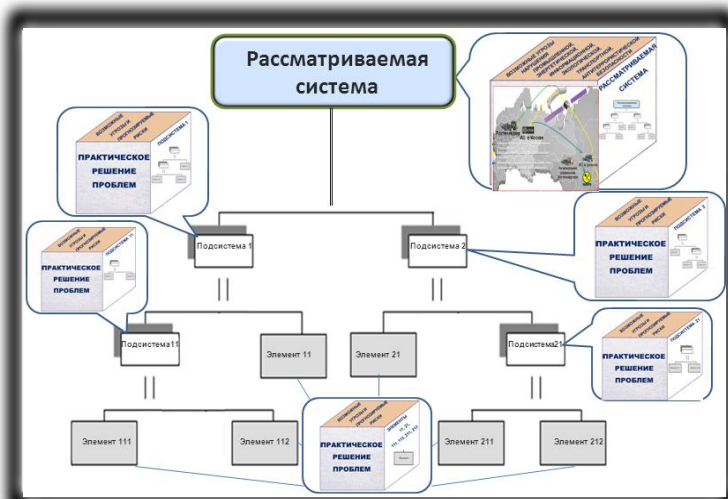
# КОМПЛЕКСИРОВАНИЕ ФУНКЦИЙ РАСПРЕДЕЛЕНИЯ ДЛЯ ИНТЕГРИРУЕМЫХ СЛОЖНЫХ АРХИТЕКТУР

(при расчетах время  $t$  пробегает все значения от 0 до  $\infty$ )

Методы  
системной  
инженерии



$$\text{Риск } R(t) = 1 - [1 - R_1(t)][1 - R_2(t)]$$

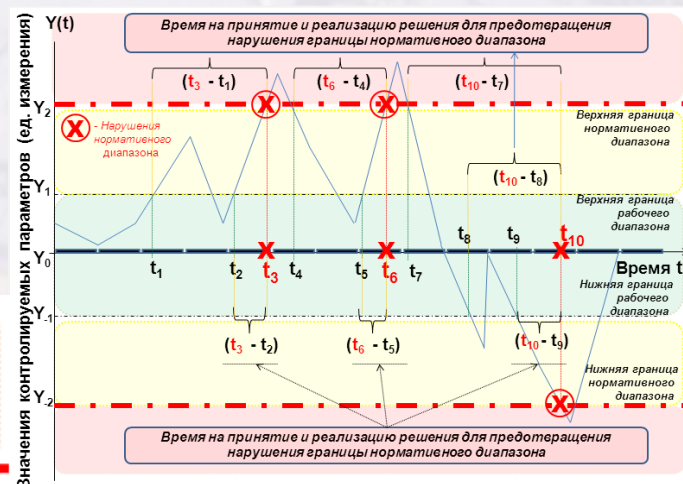
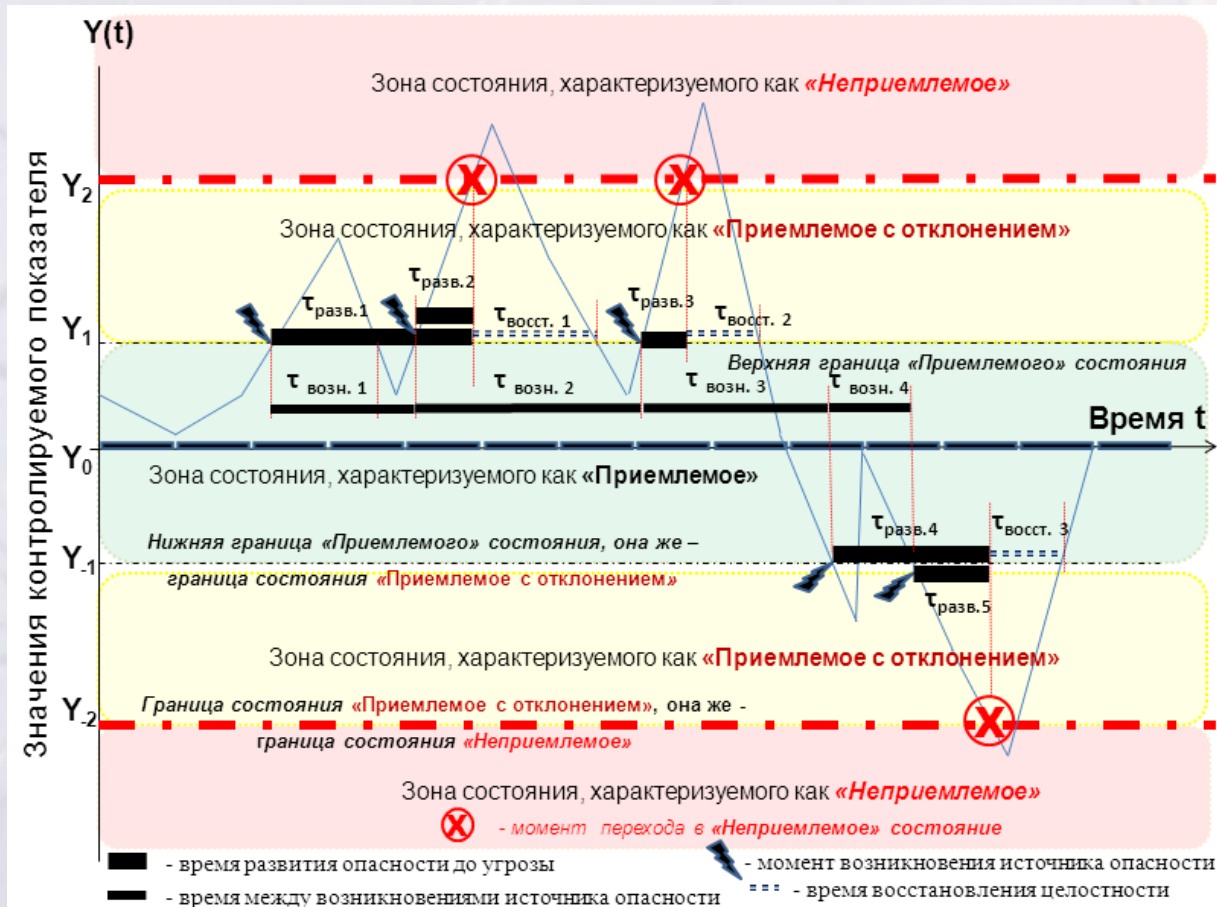


**Логическая интерпретация элементарных состояний: интегрированная система находится в состоянии «отсутствия нарушений целостности», если «И» система слева, «И» система справа находятся в состоянии «отсутствия нарушений целостности»**

# ОТ ЧАСТНОГО — К ОБЩЕМУ

Для  
оборудования

Для общего случая



Эта модель применима  
для любого показателя!



# Пример из Доктрины энергетической безопасности

Цель обеспечения энергетической безопасности (по п.22 Доктрины) – поддержание защищенности экономики и населения страны от угроз на уровне, соответствующем требованиям законодательства РФ, касающимся подпунктов а)-о):

22а) 22б) 22в) 22г) 22д) 22е) 22ж) 22з) 22и) 22к) 22л) 22м) 22н) 22о)

Возможные критерии (для выработки рациональных упреждающих мер)

<p><b>КВ1 - Удержание интегрального и/или частных рисков в допустимых пределах в течение задаваемого прогнозного периода времени при ограничениях на эксплуатационные условия и ресурсы</b></p> <p>В условиях внешнеэкономических, внешнеполитических, внутренних и трансграничных вызовов и угроз с учетом последствий (по пп. 8-21), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24-29)</p>	<p><b>КВ2 - Минимизация затрат при ограничениях на допустимый уровень интегрального и/или частных рисков в течение задаваемого прогнозного периода времени, эксплуатационные условия и ресурсы</b></p> <p>В условиях внешнеэкономических, внешнеполитических, внутренних и трансграничных вызовов и угроз с учетом последствий (по пп. 8-21), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24-29)</p>	<p><b>КВ3 - Минимизация интегрального риска при ограничениях на допустимый уровень частных рисков в течение задаваемого прогнозного периода времени, эксплуатационные условия и ресурсы</b></p> <p>В условиях внешнеэкономических, внешнеполитических, внутренних и трансграничных вызовов и угроз с учетом последствий (по пп. 8-21), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24-29)</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Планы по мерам упреждающего реагирования на высокий риск реализации угроз

для прогнозного периода от нескольких недель до полугодя	для прогнозного периода от полугодя до 3-х лет	для прогнозного периода от четырех лет и более
Краткосрочные планы	Среднесрочные планы	Долгосрочные планы

**Цель 22б) - надежное и устойчивое обеспечение российских потребителей энергоресурсами стандартного качества и услугами в сфере энергетики**

**Риск 22б)-Р17ж) - 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 – те же:**

- 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 восстановления целостности системы;
- длительность прогнозного периода времени

0-й ярус (корень)

i-й Федеральный округ

1-й ярус - цели

22а) 22б) 22в) 22г) 22д) 22е) 22ж) 22з) 22и) 22к) 22л) 22м) 22н) 22о)

2-й ярус - направления деятельности

22б)-НД24а) 22б)-НД24б) 22б)-НД24в) 22б)-НД24г) 22б)-НД24д) 22б)-НД24е) 22б)-НД24ж) 22б)-НД24з) 22б)-НД24и) 22б)-НД24к) 22б)-НД24л) 22б)-НД24м) 22б)-НД24н) 22б)-НД24о)

3-й ярус - решаемые задачи

22а)-НД24д)-329а) 22а)-НД24д)-329б) 22а)-НД24д)-329в) 22а)-НД24д)-329г) 22а)-НД24д)-329д) 22а)-НД24д)-329е)

4-й ярус - риски для достижения цели

22б)-Р17а) 22б)-Р17б) 22б)-Р17в) 22б)-Р17г) 22б)-Р17д) 22б)-Р17е)

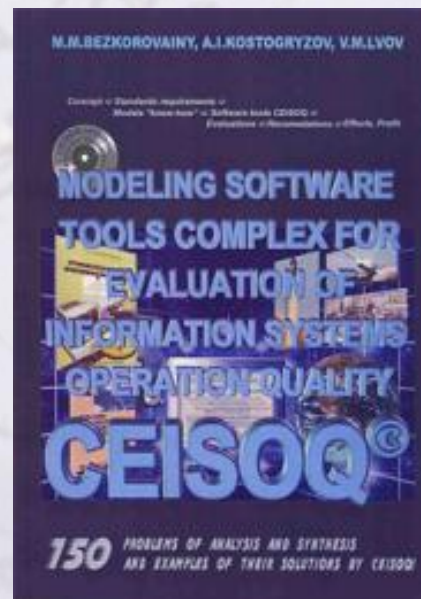
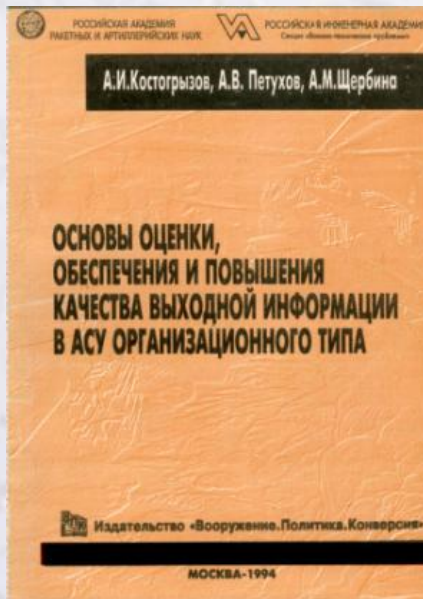
5-й ярус - угрозы, определяющие риски

22б)-Р17ж)-БнВ-У15а) 22б)-Р17ж)-БнВ-У15б) 22б)-Р17ж)-БнВ-У15г) 22б)-Р17ж)-ТрансУ15а)

6-й ярус - характеристики угроз для моделирования  
(по частным показателям, УВМП и регламенту контроля состояния энергетической безопасности)

# Теоретические основы – 1993-2003гг.

(150 решенных задач анализа и синтеза для различных АСУ)





# 2005

**100 МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ,  
35 ПРОГРАММНЫХ КОМПЛЕКСОВ**  
ДЛЯ МОДЕЛИРОВАНИЯ, АНАЛИЗА, КОНСАЛТИНГА  
И СЕРТИФИКАЦИИ СЛОЖНЫХ СИСТЕМ  
В КОНТЕКСТЕ СТАНДАРТОВ:

- ISO/IEC 15288:2002 Системы инженерии. Процесс жизненного цикла систем
- ГОСТ Р ISO 9001:2001 Системы менеджмента качества. Требования к качеству
- ISO 13407 Проектирование требований к системе
- ГОСТ Р 51987:2002 Информационная технология. Комплекс стандартов на автоматизированные системы
- ГОСТ Р 51987:2002 Информационная технология. Комплекс стандартов на автоматизированные системы
- ГОСТ Р 51987:2002 Информационная технология. Комплекс стандартов на автоматизированные системы

**СТАНДАРТИЗАЦИЯ,  
МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ,  
РАЦИОНАЛЬНОЕ УПРАВЛЕНИЕ  
И СЕРТИФИКАЦИЯ**  
в области системной и программной инженерии

**80 стандартов ISO, IEC,  
IEEE, IEC, ANSI, ГОСТ Р**  
**100 универсальных  
математических моделей**  
**35 доступных программных  
комплексов**  
**50 примеров решения  
задач анализа и синтеза**

2001 - 2005

<http://mathmodels.net>

# 2007

**ANDREY KOSTOGRYZOV**  
Dr. of Science (Eng.), Professor, Honored Science Worker of Russian Federation, Director of the Research Institute of Applied Mathematics and Certification, the Main Designer of the International Center for Informatics and Electronics, Professor of the Gubkin Russian State University of Oil and Gas  
[www.mathmodels.net](http://www.mathmodels.net)

**PROF. DR VOJISLAV STOILJKOVIC**  
Senior Professor at the University of Nis, Serbia as of 1982, A senior Professor of CIM at the University of Wittenhaaven, Germany in 1990, A president of the quality management consulting and software development company CIM College d.o.o. (CIM Integrated Systems Ltd.),  
[www.cimcollege.co.rs](http://www.cimcollege.co.rs), [www.cimsys.com](http://www.cimsys.com)

**APPLICABLE METHODS TO ANALYZE AND OPTIMIZE STANDARD SYSTEM PROCESSES**

**SYSTEM ANALYST GUIDE**

(useful ideas, process approach, mathematical models and methods for system analysis, software tools and examples of applications with an explanation of logic for achieved effects, the recommendations)

**MORE THAN 100  
MATHEMATICAL MODELS  
OF PROCESSES  
IN SYSTEM LIFE CYCLE**

2007

# 2008

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

**СТЕПАНОВ ПАВЕЛ ВЛАДИМИРОВИЧ**  
доктор технических наук, профессор, действительный член Академии проблем качества, доктор философии, профессор европейского колледжа

**ИННОВАЦИОННОЕ УПРАВЛЕНИЕ КАЧЕСТВОМ И РИСКАМИ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ**

**ИННОВАЦИОННОЕ УПРАВЛЕНИЕ КАЧЕСТВОМ И РИСКАМИ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ**

**ПРАКТИЧЕСКОЕ РУКОВОДСТВО  
ДЛЯ СИСТЕМНЫХ АНАЛИТИКОВ**

(современные стандарты и идеи системной инженерии, математические модели, методы, алгоритмы и программно-инструментальные средства для системного анализа и синтеза, доступные уровни высокопроизводительной имитационной модели, примеры приложений с объяснением логики достигнутых результатов, полезные практические рекомендации)

**ОБЪЕКТНО-ОРИЕНТИРОВАННОЕ ПОДХОД К СИСТЕМНОМУ АНАЛИЗУ**

# 2010

**ГРИГОРЬЕВ ЛЕОНИД ИВАНОВИЧ**  
доктор технических наук, профессор, член-корреспондент РАН и РАЕН, действительный член Академии информатизации управления, член-корреспондент РАН и РАЕН, действительный член Академии проблем качества, доктор философии, профессор европейского колледжа

**КЕРШЕНБАУМ ВСЕВОЛОД ЯКОВЛЕВИЧ**  
доктор технических наук, профессор, член-корреспондент РАН и РАЕН, действительный член Академии информатизации управления, член-корреспондент РАН и РАЕН, действительный член Академии проблем качества, доктор философии, профессор европейского колледжа

**КОСТОГРЫЗОВ АНДРЕЙ ИВАНОВИЧ**  
заслуженный деятель науки РФ, доктор технических наук, профессор, член-корреспондент РАН и РАЕН, действительный член Академии информатизации управления, член-корреспондент РАН и РАЕН, действительный член Академии проблем качества, доктор философии, профессор европейского колледжа

**СИСТЕМНЫЕ ОСНОВЫ УПРАВЛЕНИЯ КОНКУРЕНТОСПОСОБНОСТЬЮ В НЕФТЕГАЗОВОМ КОМПЛЕКСЕ**

**СИСТЕМНЫЕ ОСНОВЫ УПРАВЛЕНИЯ КОНКУРЕНТОСПОСОБНОСТЬЮ В НЕФТЕГАЗОВОМ КОМПЛЕКСЕ**

**СИСТЕМНЫЕ ОСНОВЫ УПРАВЛЕНИЯ КОНКУРЕНТОСПОСОБНОСТЬЮ В НЕФТЕГАЗОВОМ КОМПЛЕКСЕ**







2017, 2018гг.



# БЕЗОПАСНОСТЬ РОССИИ



# БЕЗОПАСНОСТЬ РОССИИ

Правовые, социально-экономические  
и научно-технические аспекты

## Фундаментальные и прикладные проблемы комплексной безопасности

МГОФ «Знание»  
2017

### БЕЗОПАСНОСТЬ РОССИИ

Правовые, социально-экономические и научно-технические аспекты

Тематический блок

«НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ»

Фундаментальные и прикладные  
проблемы комплексной безопасности

Авторский коллектив:

Абросимов Н.В., Агеев А.Н., Алужкин В.В., Акимов В.А., Алексин А.В., Алексин Н.П.,  
Асмолов В.Г., Афиногенов Д.А., Азметдинов Р.С., Балаждин Д.В., Баранов В.В.,  
Барин Н.В., Барышев С.Н., Белов П.Г., Белозеров А.С., Белкин П.Н., Берили А.Ф.,  
Белоткин Н.Н., Болышкин А.М., Болышев Л.А., Болышутин М.А., Ботанин Л.Г.,  
Быков А.А., Веретинский Н.К., Власов С.В., Воробьев Ю.Л., Вороний Н.Н.,  
Гаджиев М.М., Галлямов В.А., Гетилин А.Ф., Гольдштейн Р.В., Горюхины Н.В.,  
Гражданский А.П., Гринев В.А., Дедушкин Ф.М., Демурин К.С., Драгунов Ю.Г.,  
Дубинин Е.Ф., Ерохин К.Н., Жукин С.А., Захарович В.В., Зарев Д.Л.,  
Иванов В.В., Ивлев В.Н., Игнатьев К.В., Илюшин Д.А., Кайдалов В.В.,  
Карлов А.Н., Клавят Е.В., Клеин В.В., Ковалевич О.М., Козин А.В., Короткий Ю.Г.,  
Корчагин А.Д., Косов В.С., Костогризов А.Н., Костюков В.Н., Котельников В.С.,  
Кузнец Н.Р., Кузнецов В.В., Кулик Б.Н., Лавров Н.П., Лебедев М.П., Леонкин А.М.,  
Лисков М.В., Лисин Ю.В., Масляковский А.В., Матвеев Ю.Г., Матросов Н.В.,  
Матросов Н.Н., Мазуров Н.А., Матвеев Ф.М., Матрофеев А.В., Москатов В.В.,  
Надин В.А., Назаров В.П., Назолин А.Л., Найзер М.С., Насинов А.Д.,  
Никишилов А.А., Нестеренко Г.Н., Николайчук О.А., Новикова Г.В., Осипов В.Н.,  
Осипов Ю.С., Павлов А.Н., Павлов А.Н., Павлов В.А., Павлов В.А., Переход В.Н.,  
Петров Ю.К., Петров В.П., Петровский А.С., Пичков С.Н., Полонин В.Н.,  
Пурменов С.В., Пучков В.А., Радченко С.Г., Раузиновский Н.А., Раузи В.С.,  
Резниченко Д.О., Резниченко А.Ф., Рамзанов А.Н., Рутковский В.Ю., Рабичкин Н.А.,  
Секляков А.М., Секляков Н.А., Селезнев Е.Д., Соколов Е.Н., Соколовский Л.А.,  
Скляков В.М., Степанов П.В., Суриков А.Н., Таракан А.А., Тимашев С.А.,  
Титов Е.Ю., Тутунов А.А., Филев М.Н., Федота В.Н., Фелин Б.Н., Фертон В.Е.,  
Харбев В.Г., Харюновский В.В., Харьков С.А., Цалков Р.Х., Цыганков С.А.,  
Червопелков А.Н., Чернышев С.Л., Чернышевский А.О., Чернышевский О.Ф.,  
Чернов А.П., Чернов А.Г., Шляхников В.Н., Шейгу С.К., Юсупов О.Н., Юрков А.Ю.

Издательство МГОФ «Знание». Лицензия № 030569 от 22.09.1998 г.

Издательско-просветительский проект «Безопасность России»

Директор проекта — Макарушкин В.Г.

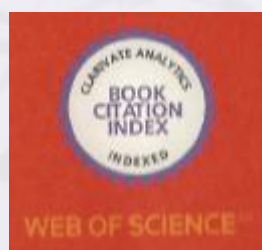
Редакторы — Хлебникова Г.Г., Юдина О.Н.

Компьютерная верстка, оформление — Барыкин А.Н.

Координатор проекта — Семенов Е.В.

Формат 70 x 100 1/16. Гарнитура Times  
Печать офсет. Усл. печ. л. 48,8. Тираж 1000 экз.  
Подписано в печать 28.05.2015

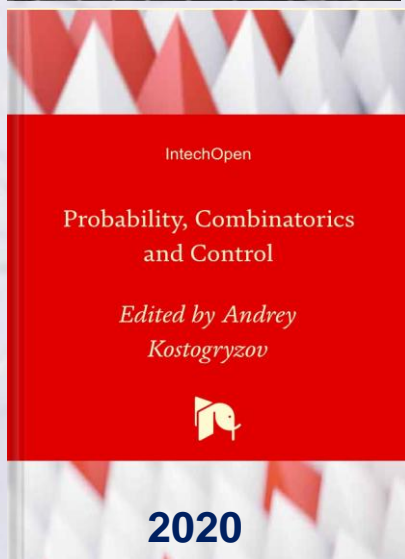
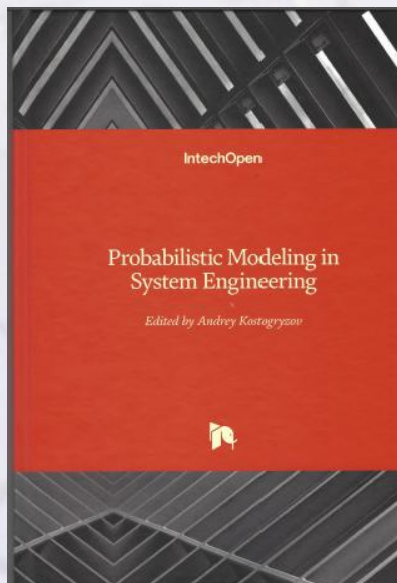
Отпечатано в ИПИ «Гипограф» «Нарва»  
121099, Москва, Шубинский пер., д. 6



# 2018- публикация InTech (Лондон) книги «Вероятностное моделирование в системной инженерии».

Книга в открытом доступе - может списать любой желающий (бесплатно)

<http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering>



This book consists of 12 chapters from the following authors:

## Chapter 1

Probabilistic Modelling in Solving Analytical Problems of System Engineering

by Anatoly Lepikhin, Vladimir Moskvichev and Nikolay Machutov

## Chapter 2

Probabilistic Methods and Technologies of Risk Prediction and Rationale of Preventive Measures by Using "Smart Systems": Applications to Coal Branch for Increasing Industrial Safety of Enterprises

by Vladimir Artemyev, Jury Rudenko and George Nistratov

## Chapter 3

Probabilistic Modeling Processes for Oil and Gas

by Vsevolod Kershenbaum, Leonid Grigoriev, Petr Kanygin and Andrey Nistratov

## Chapter 4

Probabilistic Analysis of Transportation Systems for Oil and Natural Gas

by Yuriy V. Lisin, Nikolay A. Makhutov, Vladimir A. Nadein and Dmitriy A. Neganov

## Chapter 5

Decision-Making Model for Offshore Offloading Operations Based on Probabilistic Risk Assessment

by C. E. Patiño Rodriguez

## Chapter 6

Natural Hazards: Systematic Assessment of Their Contribution to Risk and Their Consequences

by Berg Heinz-Peter and Roewekamp Marina

## Chapter 7

Models for Testing Modifiable Systems

by Alexey Markov, Alexander Barabanov and Valentin Tsirlov

## Chapter 8

Probabilistic Model of Delay Propagation along the Train Flow

by Vladimir Chebotarev, Boris Davydov and Kseniya Kablukova

## Chapter 9

The Approach of Probabilistic Risk Analysis and Rationale of Preventive Measures for Space Systems and Technologies

by Nikolay Paramonov

## Chapter 10

Periodic Monitoring and Recovery of Resources in Information Systems

by Alexey Markov, Alexander Barabanov and Valentin Tsirlov

## Chapter 11

Probabilistic Analysis of the Influence of Staff Qualification and Information-Psychological Conditions on the Level of Systems Information Security

by Igor Goncharov, Nikita Goncharov, Pavel Parinov, Sergey Kochedykov and Alexander Dushkin

## Chapter 12

Analysis of Terrorist Attack Scenarios and Measures for Countering Terrorist Threats

by Dmitry O. Reznikov, Nikolay A. Makhutov and Rasim S. Akhmetkhanov

ISBN: 978-1-78923-775-7

Print ISBN: 978-1-78923-774-0

DOI: 10.5772/intechopen.71396

2020





# **Наименования, область применения и структура - отвечают требованиям стандартов, ГОСТ Р 1.2 и ГОСТ Р 1.5, регламентирующим создание национальных стандартов**

## ***Пример типовой структуры***

- 1 Область применения*
- 2 Нормативные ссылки*
- 3 Термины, определения и сокращения*
- 4 Основные положения системной инженерии по защите информации в процессе управления инфраструктурой*
- 5 Общие требования системной инженерии к защите информации в процессе управления инфраструктурой*
- 6 Специальные требования к количественным показателям*
- 7 Требования к системному анализу*
- Приложение А (справочное) Пример перечня защищаемых активов*
- Приложение Б (справочное) Пример перечня угроз*
- Приложение В (справочное) Типовые методы и модели для прогнозирования рисков*
- Приложение Г (справочное) Методические указания по прогнозированию рисков для процесса управления инфраструктурой*
- Приложение Д (справочное) Типовые допустимые значения показателей рисков для процесса управления инфраструктурой*
- Приложение Е (справочное) Примерный перечень методик системного анализа для процесса управления инфраструктурой ..... ..*
- Библиография*



# Суть – в формировании и использовании знаний



# ПОСЛЕ ПРИНЯТИЯ ПРЕДЛАГАЕМЫХ СТАНДАРТОВ СИСТЕМНОЙ ИНЖЕНЕРИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

## СТИМУЛЫ ДЛЯ ПРЕДПРИЯТИЙ

1. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 31.12.2015 № 683
2. Стратегия научно-технологического развития Российской Федерации, утверждена Указом Президента РФ от 01.12.2016 №642
3. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ 05.12.2016 № 646
4. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утверждена Указом Президента РФ от 09.05.2017 № 203
5. Стратегия экономической безопасности Российской Федерации на период до 2030 года, утвержденная Указом Президента РФ от 13.05.2017 № 208
6. ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017г. № 187-ФЗ
7. Программа «Цифровая экономика РФ», утверждена распоряжением Правительства РФ от 28.07.2017 № 1632-р
8. Доктрина энергетической безопасности Российской Федерации, утвержденная Указом Президента РФ от 13.05.2019 № 216
9. Концепции создания государственной единой облачной платформы, утвержденной распоряжением Правительства РФ от 28.08.2019 г. №1911-р

**Ответственность за  
ИБ – на предприятиях**

**Регуляторы – по Положениям  
(в т.ч. контроль, надзор вне сферы ИБ )**

В процессах  
риски–езде

Поддержка методами  
прогнозирования рисков

Добавлены стандарты по каждому из процессов в жизненном цикле систем. В процессы встроены требования отечественных НД. Ориентация - на риск-ориентированный подход с рекомендациями «как оценивать риски количественно». Это означает принципиальную возможность корректного решения обратных задач эффективного управления безопасностью, исходя из задаваемого уровня допустимого риска

**Итог – все процессы охвачены, риски по ИБ оцениваются как качественно, так и количественно строго на научной основе. Обучение, сертификация – проводятся по методическим рекомендациям стандартов, гарантии формируются самими предприятиями на основе прогнозирования рисков и корректного решения обратных задач эффективного управления безопасностью, исходя из задаваемого уровня допустимого риска**



# Предложения в Решение

- Признать целесообразным для обеспечения промышленной безопасности разработку 29 стандартов системной инженерии, выставленных на публичное обсуждение и устанавливающих основные требования системной инженерии к защите информации для различного рода систем. Члены Круглого стола констатируют, что наименования, область применения и структура представленных 29 проектов стандартов в целом отвечают требованиям стандартов ГОСТ Р 1.2 и ГОСТ Р 1.5, регламентирующим создание национальных стандартов

- Поручить члену Комитета Нистратову А.А. обобщить представленные замечания по содержанию рассмотренных 29 проектов стандартов и представить на утверждение председателю Комитета ТПП РФ по промышленной безопасности отзывы Комитета по первым редакциям стандартов для их высылки установленным порядком в национальный ТК 22 «Информационные технологии» в срок до 26.10.2020