Федеральный исследовательский центр «Информатика и управление»
Российской академии наук

Нистратов Андрей Андреевич

ПРОГРАММНЫЕ, ТЕХНОЛОГИЧЕСКИЕ И МЕТОДИЧЕСКИЕ РЕШЕНИЯ ДЛЯ УПРЕЖДАЮЩЕГО УПРАВЛЕНИЯ РИСКАМИ В ПРИЛОЖЕНИЯХ СИСТЕМНОЙ ИНЖЕНЕРИИ

Диссертация
на соискание ученой степени доктора технических наук
по специальности 2.3.5 «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»

Научный консультант:
заслуженный деятель науки РФ,
доктор технических наук,
профессор Зацаринный А.А.

Москва 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Анализ происходящих в мире научно-технических изменений в условиях разнородных природных, техногенных и социальных угроз побуждает к широкомасштабному исследованию и применению концептуальных воззрений и методов системной инженерии. Системная инженерия объединяет разнородные научно-технические усилия главным образом на том, как рациональным образом построить и эффективно эксплуатировать различные искусственно создаваемые системы. Возникновение системной инженерии в России произошло, в первую очередь, благодаря достижениям в области атомной энергетики, ракетостроения, освоения космоса и обеспечения безопасности сложных систем [1-5].

Сегодня наиболее узким местом отечественной системной инженерии является отсутствие доступных и широко применимых программных и технологических решений, ориентированных на прогнозирование и упреждающее управление рисками в достижении системных целей с использованием вычислительных систем (ВС) и компьютерных сетей (КС). При этом важно именно упреждающее управление рисками, позволяющее за счет своевременного распознавания признаков развития разнородных угроз избежать появление критичных событий или смягчить возможные последствия от реализации угроз.

Степень разработанности темы. За рубежом проблематика системной инженерии была поднята в работах Н. Винера, поддержана в 60-70-е годы Г.Х. Гудом, Л. Клейнроком, Р.З. Маколом, Дж. Мартином (работы издавались в СССР на русском языке), позже в части управления рисками проблематику развивали B. Boehm, H.Kumamoto, E. Henley, D. Vose, E.H. Conrow, J. Mun и другие ученые США [6-14]. В Европе риск-ориентированный подход в системной инженерии получил развитие в работах научно-технических школ таких современных ученых, как M. Eid, V. Rosato (Франция), En. Zio (Италия), K. Kolowrocki (Польша) [15-17]. Вопросы многосторонней методической оценки качества и безопасности функционирования различных систем с использованием вероятностного моделирования были заложены в школах отечественных ученых Б.В. Гнеденко, П.С. Краснощекова, Н.А. Махутова, Н.Н. Моисеева. В последние десятилетия исследования были продолжены и расширены В.А. Балыбердиным, И.В. Бычковым, В.И. Васильевым, Я.Д. Вишняковым, С.А. Головиным, Л.И. Григорьевым, Г.В. Дружининым, С.Г. Емельяновым, А.О. Жуковым, А.А. Зацаринным, С.П. Киселевой, С.М. Климовым, К.К. Колиным, В.Ю. Королевым, А.И. Костогрызовым, И.В. Котенко, В.В. Кульбой, В.В. Липаевым, А.С. Марковым, В.В. Москвичевым, Д.А. Новиковым, С.А. Петренко, Б.А. Позиным, Г.Я. Резниковым, И.Н. Синициным, И.А. Соколовым, П.В. Степановым, А.А. Стрельцовым, В.А. Сухомлиным, А.А. Сычуговым, И.А. Шереметом, Ю.И. Шокиным, Ю.К. Язовым, другими российскими

и зарубежными учеными и получили практическое развитие и приложение в поисковых и прикладных работах различных НИИ, научно-производственных предприятий и объединений при решении практических задач системной инженерии [18-100]. Анализ упомянутых и многих других исследований показывает, что в условиях разнородных неопределенностей для критичных систем тематика управления рисками сохраняет свою практическую важность. Глобальный контекст для системной инженерии в настоящее время определяют растущие человеческие и социальные потребности, необходимость развития научно-методических основ системной инженерии и расширение областей ее применения в условиях разнородных вызовов и угроз, совершенствование инструментариев, моделей и методов решения практических задач, востребованность улучшения обучения и подготовки кадров. Перспективная системная инженерия должна поддерживаться междисциплинарной теоретической основой, методами и инструментариями исследований на уровне ВС и КС, основанными на моделях, позволяющих лучше понимать все более сложные системы и решения, принимаемые в условиях разнородных неопределенностей [5].

Вместе с тем, несмотря на наличие множества моделей, связанных с оценкой качества и безопасности функционирования систем, подавляющее большинство из них ориентировано на удовлетворение конкретных задаваемых специфических потребностей, и, зачастую, как реакция на факты негативных событий. А, учитывая структурную сложность анализируемых систем, многие из существующих моделей оказываются трудно адаптируемыми к применению по мере изменения условий и возникновения новых потребностей в моделировании процессов в жизненном цикле (ЖЦ) систем. За редким исключением возможности существующих информационных технологий не используются для вероятностного прогнозирования и упреждающего управления рисками. Тем самым в системной инженерии отсутствует широко доступный программно-технологический сервис для моделирования систем различного функционального назначения и вероятностного прогнозирования рисков по единой вероятностной шкале. В результате упускаются практические эффекты от адекватного применения накапливаемой оперативной информации для выявления скрытых закономерностей и возможностей в функционировании систем, в т.ч. извлекаемых из прецедентов и аналогий в смежных областях. На сегодня возникло критичное методологическое и программно-технологическое противоречие между объективными потребностями в упреждающем управлении рисками в приложениях системной инженерии и реальными программными и технологическими возможностями в применении в реальном времени получаемых результатов прогнозирования [5].

Таким образом, в условиях современных и ожидаемых вызовов и угроз, возрастающих неопределенностей в противодействии западным санкциям при построении нового мироустройства все вышеизложенное подтверждает острую **актуальность тематики** диссертационных исследований.

Осуществляя научный поиск практических путей, способствующих устранению выявленного противоречия, настоящая диссертационная работа посвящена решению важной **научной проблемы** разработки программных, технологических и методических решений для ВС и КС, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии.

Объектом исследования являются математическое и программное обеспечение ВС и КС, предназначенное для аналитического решения задач системной инженерии. Предметом исследования являются научно обоснованные программные, технологические и методические решения для ВС и КС, ориентированные на прогнозирование и упреждающее управление рисками в ЖЦ систем при реализации стандартизованных процессов и решении прямых и обратных задач системной инженерии.

Целью диссертационного исследования является обоснование рациональных способов снижения и удержания рисков в допустимых пределах на стадиях жизненного цикла систем различного функционального назначения в условиях реальных и гипотетических вызовов и угроз на основе применения предлагаемых новых научно обоснованных программных, технологических и методических решений для вычислительных систем и компьютерных сетей.

Результаты диссертационных исследований представлены в пяти разделах, это:

1. Анализ существующих подходов к управлению рисками в приложениях системной инженерии. Постановка научной проблемы;

2. Разработка программных решений, обеспечивающих прогнозирование рисков и обоснование упреждающих мер противодействия угрозам с использованием ВС и КС;

3. Разработка технологических решений для автономного и удаленного режимов поддержки принятия решений по упреждающему управлению рисками в приложениях системной инженерии;

4. Разработка типовых методик применения технологии поддержки риск-ориентированной системной инженерии;

5. Разработка рекомендаций по снижению и удержанию рисков в допустимых пределах в ЖЦ систем различного функционального назначения на основе применения технологии поддержки риск-ориентированной системной инженерии.

Соответствие паспорту специальности. Тема исследования и полученные ре-

зультаты соответствуют направлениям исследований, изложенным в пунктах 4, 7, 9, 10 паспорта специальности 2.3.5. «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» -(п.4 – «Интеллектуальные системы машинного обучения, управления базами данных и знаний, **инструментальные средства разработки цифровых продуктов**», п.7 – «**Модели, методы,** архитектуры, алгоритмы, форматы, протоколы и **программные средства человеко-машинных интерфейсов**, компьютерной графики, визуализации, обработки изображений и видеоданных, систем виртуальной реальности, **многомодального взаимодействия в социокиберфизических системах**», п.9 – «**Модели, методы, алгоритмы, облачные технологии и программная инфраструктура организации глобально распределенной обработки данных**», п.10 – «**Оценка качества, стандартизация и сопровождение программных систем**»).

Основные положения, выносимые на защиту:

1) комплекс новых программных и технологических решений для ВС и КС, включая:

- решения по программной инфраструктуре глобально распределенного прогнозирования рисков и моделированию процессов;

- комплексы программ моделирования систем для прогнозирования рисков (частных и интегрального), выявления угроз, анализа альтернатив и обоснования системных требований к характеристикам процессов;

- прототип базы знаний для подготовки исходных данных для моделирования и поддержки принятия аналитических решений на стадиях жизненного цикла систем;

- технологические решения по интеграции моделей и созданных комплексов программ, обеспечивающие реализацию новых аналитических возможностей по вероятностному прогнозированию и упреждающему управлению рисками;

2) созданный прототип технологии поддержки риск-ориентированной системной инженерии, основанный на новых программных и технологических решениях для ВС и КС, обеспечивающий упреждающее выявление «узких мест» и определение рациональных способов снижения и удержания рисков в допустимых пределах на стадиях жизненного цикла систем различного функционального назначения в условиях реальных и гипотетических вызовов и угроз;

3) методические решения для пользователей ВС и КС, включающие комплекс типовых методик и обеспечивающих применение созданного прототипа технологии поддержки риск-ориентированной системной инженерии для конкретных приложений;

4) основные положения по моделированию систем, прогнозированию и упреждающему управлению рисками, реализованные в качестве основы методических

рекомендаций национальных стандартов по информационным технологиям, системной и программной инженерии.

Научная новизна полученных результатов определяется:

новыми научно обоснованными программными и технологическими решениями для ВС и КС, обеспечивающими интеграцию существующих и усовершенствованных базовых моделей, создание и ведение прототипа базы знаний для моделирования в ЖЦ систем различного функционального назначения, за счет чего достигается расширение аналитических возможностей по прогнозированию и упреждающему управлению рисками;

новыми методическими решениями задач системной инженерии, позволяющими в отличие от существующих подходов стандартизованным способом широко применять с использованием ВС и КС усовершенствованные вероятностные модели и разработанные программные и технологические решения, интерпретировать результаты прогнозирования рисков, извлекать в условиях разнородных неопределенностей знания о достижимых прагматических эффектах и обосновывать рекомендации по упреждающему управлению рисками, снижению и удержанию рисков в допустимых пределах

Теоретическую значимость работы определяют:

1) сформулированные и доказанные четыре теоремы, ориентированные на прогнозирование и упреждающее управление рисками в сложных системах, расширяющие границы применимости существующих базовых моделей за счет учета различий в длительностях диагностики и восстановления нарушаемой целостности элементов системы, создающие дополнительные знания по остаточному времени на реагирование для мониторируемых объектов, обеспечивающие повышение адекватности вероятностного моделирования с использованием математического и программного обеспечения ВС и КС и включающие:

- Теорему 1 о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности системы;
- Теорему 2 об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта; выявленные закономерности в соотношениях исходных данных для непревышения задаваемого допустимого уровня риска и сохранения целостности моделируемой системы; следствие из Теоремы 2 - об ограничениях при выборе периода между диагностиками, ориентированного на непревышение допустимого риска нарушения целостности системы;

- Теорему 3 о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- Теорему 4 о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам;

2) как следствие из применения Теорем 1-4: усовершенствованные вероятностные модели прогнозирования рисков и методы повышения их точности, реализованные в национальных стандартах и позволяющие в отличие от существующих учесть особенности функционирования составных элементов сложной системы, в т.ч. различного рода угрозы и вызовы, распределенные по элементам системы, возможные меры периодического контроля и восстановления нарушаемой целостности. Усовершенствованные модели и методы для анализа системных элементов, сложных систем и процессов формируют математическое обеспечение и специальное программное обеспечение созданного прототипа технологии поддержки риск-ориентированной системной инженерии с использованием ВС и КС .

Практическая значимость работы заключается в следующем:

- программные и методические решения применены при разработке отчетов о НИР для прогноза рисков нарушения качества и безопасности функционирования информационно-телекоммуникационных систем, при разработке отчетных и методических материалов по госзаданию FFNG 2024-0010, выполненному ФИЦ ИУ РАН;

- программные, технологические и методические решения реализованы при выполнении работ по созданию и эксплуатации программного прототипа подсистемы поддержки принятия решений по управлению рисками в рамках системы дистанционного контроля промышленной безопасности (СДК ПБ) на угольных шахтах в интересах генерального заказчика АО «СУЭК-Кузбасс» в 2016г. (в части прогнозирования рисков), в 2017г. (в части создания прототипа подсистемы поддержки принятия решений по управлению рисками прототипа СДК ПБ), в 2018г. (в части развития прототипа), в 2019г. (в части тиражирования прототипа), а также в ГОСТ Р 58494-2019 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов», что подтверждено актом о реализации ООО НИИ прикладной математики и сертификации;

- предложенные вероятностные модели и методы реализованы в 2021 году в 18 национальных стандартах системной инженерии: ГОСТ Р 59329, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59347, ГОСТ Р 59349, ГОСТ Р 59353,

ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357 в части моделирования стандартных процессов приобретения и поставки продукции и услуг, управления инфраструктурой системы, управления человеческими ресурсами, управления качеством системы, управления знаниями о системе, планирования проекта, оценки и контроля проекта, управления решениями, управления рисками для системы, управления информацией, измерений, определения архитектуры системы, системного анализа, передачи, аттестации, функционирования и сопровождения системы, изъятия и списания системы, что подтверждено актом о реализации от ФБУ НТЦ «Энергобезопасность»;

- стандартизованные усовершенствованные модели, методы и методические решения, включенные в ГОСТ Р 59329-2021 – ГОСТ Р 59357-2021, внедрены в практику работы национального и межнационального технического комитета «Информационные технологии» (ТК-МТК-022) в части ссылок и рекомендаций по использованию созданных методов, моделей и демонстрационных примеров системной инженерии в новых национальных стандартах 2024-2025гг.: ГОСТ Р 56920-2024 «Системная и программная инженерия. Тестирование программного обеспечения. Общие положения (ISO/IEC/IEEE 29119-1:2022, NEQ)»; ГОСТ Р 57193-2025 «Системная и программная инженерия. Процессы жизненного цикла систем (ISO/IEC/IEEE 15288:2021, NEQ)»; ГОСТ Р 71303-2024 «Системная и программная инженерия. Возможности программных инструментариев для организационного управления инцидентами. Общие положения (ISO/IEC 23531:2020, NEQ)»; ГОСТ Р 71304-2024 «Системная и программная инженерия. Гарантии обеспечения качества систем и программных средств. Основные понятия и термины (ISO/IEC/IEEE 15026-1:2019, NEQ)»; ГОСТ 71438-2024 «Информационные технологии. Оценка процессов. Система измерения процессов для оценки их возможностей (ISO/IEC 33020:2019, NEQ)», ГОСТ Р 71439-2024 «Системная и программная инженерия. Методы и инструментарии продуктовой линейки программных средств и систем. Общие положения (ISO/IEC 26580:2021, NEQ)»; ГОСТ Р 71440-2024 «Информационные технологии. Оценка процессов. Руководство по определению рисков в процессах (ISO/IEC TR 33015:2019, NEQ)»; ГОСТ Р 71998-2025 «Информационные технологии. Требования и оценка качества систем и программного обеспечения. Определение качества ИТ-услуг (ISO/IEC TS 25025:2021, NEQ)». Это подтверждено актом ТК-МТК-022 о внедрении результатов диссертационной работы;

- усовершенствованные базовые модели и методы, программные и методические решения использованы в практике работы Комиссии РАН по техногенной безопасности при анализе техногенных рисков, что подтверждено актом о применении результатов исследований от Председателя упомянутой Комиссии РАН члена-корреспондента РАН

Махутова Н.А. при написании разделов изданного в 2025г. тома монографии «Безопасность России. Правовые, социально-экономические и научно-технологические аспекты. Тематический блок «Национальная безопасность». Системная инженерия в проблемах национальной безопасности» (научный руководитель – Махутов Н.А.), соавторство отражено в монографии [5];

- на основе применения разработанного прототипа технологии поддержки риск-ориентированной системной инженерии были получены научно обоснованные рекомендации по решению следующих практических задач: 1) задач анализа и организации на предприятии процессов системного анализа, управления человеческими ресурсами, управления качеством и рисками; 2) задач прогнозирования на срок до 2037 года и удержания в допустимых пределах различных рисков разрушения бизнеса (потери инвестиций) применительно к фармацевтическому предприятию, созданному в рамках частно-государственного партнерства, что подтверждено актом о реализации ООО «ПРАНАФАРМ» (г. Самара);

- усовершенствованные базовые модели и методы, программные, технологические и методические решения внедрены в учебный процесс кафедры АСУ факультета автоматики и вычислительной техники РГУ нефти и газа им. И.М.Губкина, используются в читаемом авторском курсе по системной инженерии и лабораторных занятиях.

Личный вклад автора в науку. Диссертационная работа выполнена автором самостоятельно. В работе использованы материалы, полученные лично автором, а также опубликованные в соавторстве [4, 5, 49, 52, 53, 58, 64, 69, 70, 77, 83, 84, 97, 101 - 167] (вклад по каждой из работ отмечен в автореферате). Авторский вклад в науку включает вклады в усовершенствованные базовые модели и методы, программные, технологические и методические решения, ориентированные на прогнозирование и упреждающее управление рисками в приложениях системной инженерии – см. рис. 1.

Теоретический вклад (в математическое обеспечение) для решения задач системной инженерии позволил усовершенствовать существующую концепцию управления рисками и состоит: в формулировке и доказательстве теорем 1-4; в усовершенствовании на основе теорем моделей и методов повышения адекватности вероятностного моделирования для анализа функционирования системных элементов, сложных систем и выполняемых процессов на уровне прогнозируемых рисков; в доведении усовершенствованных моделей и методов до реализации в 19 национальных стандартах; и, как следствие теорем, в разработке методов повышения адекватности вероятностного моделирования с использованием ВС и КС (пп. 9, 10 паспорта специальности 2.3.5).

Рис. 1 Авторский вклад в науку

Вклад в программные и технологические решения для упреждающего управления рисками в приложениях системной инженерии состоит в создании прототипа технологии поддержки риск-ориентированной системной инженерии, включая: комплексы программ для моделирования стандартизованных процессов системной инженерии; встроенные технологические возможностей по предоставлению обобщенных и детальных вероятностных прогнозов; прототип базы знаний для моделирования [168 - 180] (пп. 4, 7, 9 паспорта специальности 2.3.5).

Вклад в методические решения состоит в разработке комплекса типовых методик применения созданного прототипа технологии поддержки риск-ориентированной системной инженерии, а также в разработке практических рекомендации по снижению и удержанию рисков в допустимых пределах в жизненном цикле систем на основе применения созданного прототипа (пп. 9, 10 паспорта специальности 2.3.5).

Методология и методы исследований. В основу диссертационных исследований положены общая теория систем, теория открытых систем, теория управления, теория вероятностей, теория информационно-телекоммуникационных систем и сетей, методы удаленного мониторинга состояний объектов, сбора, обработки и хранения информации, методы системной инженерии, математического и системного анализа, методы

оптимального управления, методы разработки архитектур и программной инфраструктуры, методы построения систем управления базами данных и знаний, методы создания человеко-машинных интерфейсов, методы разработки безопасного программного обеспечения.

Достоверность и обоснованность полученных результатов, выводов и рекомендаций обусловлена тем, что:

в разработанных программных, технологических и методических решениях корректно применены рекомендации стандартов системной и программной инженерии, методы теории открытых систем, теории информационно-телекоммуникационных систем и сетей, методы удаленного мониторинга состояний объектов, сбора, обработки и хранения информации, методы разработки архитектур и программной инфраструктуры, методы построения систем управления базами данных и знаний, методы создания человеко-машинных интерфейсов. Эффективность решений подтверждена в ходе выполнения ряда НИОКР, проиллюстрирована на практических примерах;

при моделировании использованы проверяемые данные, факты и статистическая информация о системных процессах контроля, мониторинга и восстановления нарушаемой целостности с обоснованием подбора объектов анализа;

получаемые результаты расчетов согласуются с опытными и статистическими данными в различных областях приложений (в т.ч. для информационных систем, систем дистанционного контроля промышленной безопасности, систем хранения зерновой продукции), включая результаты сравнения с проведенными ранее исследованиями других авторов;

во всех многочисленных рассмотренных случаях установлена близость полученных результатов с результатами применения методов оценки надежности и безопасности функционирования различного рода систем, полученных из независимых источников.

Апробация работы осуществлялась на образцах сложных систем различного функционального назначения. Результаты работы докладывались на 2-й и 4-й Международной конференции по транспортной информации и безопасности (ICTIS, Китай-2013, Канада-2017), VIII и XIII Международной конференции «Современные информационные технологии и ИТ-образование» (SITITO, МГУ, Москва, 2013, 2018), Всероссийской конференции «Конкурентоспособность и импортозамещение в нефтегазовом комплексе» (РГУ нефти и газа, 2015), 1-й и 2-й Международной конференции по прикладной математике и моделированию (AMSM, Китай-2016, Таиланд-2017), 52-м Международном семинаре Европейской Ассоциации безопасности, надежности и данных (ESReDA, Вильнюс, 2017), 2-й Международной конференции по системной надежности и безопасности (ICSRS, Италия, 2017), 2-й Международной конференции по социальным наукам и исследованиям в

образовании (ACSS-SSTR, Москва, 2017), 11-м Международном семинаре по надежности и безопасности (SSARS, Польша, 2017), Международной конференции по математике, моделированию и алгоритмам (MMSA, Китай, 2018), Международной конференции по физике, вычислениям и математическому моделированию (PCMM, Китай, 2018), Международной конференции по коммуникациям, сетям и искусственному интеллекту (CNAI, Китай, 2018), Глобальной конференции по умной промышленности (Челябинск, 2018), 6-й и 7-й Международной конференции по актуальным проблемам системной и программной инженерии (ВШЭ, Москва, 2019, 2021), IX и XII Международной научной конференции "Стандартизация, сертификация, обеспечение эффективности, качества и безопасности информационных технологий" ("ИТ-Стандарт", Москва, 2019, 2023), 12-й Международной конференции «Компьютерный анализ и моделирование данных» (CDAM, Минск, 2019), III Межведомственной научно-практической технической конференции «Телекоммуникации и кибербезопасность: специальные системы и технологии» (Серпухов, 2021), Всероссийской научно-технической конференции «Кибернетика и информационная безопасность» («КИБ», МИФИ, 2023), XI и XIII Международной научно-технической конференции по безопасным информационным технологиям (BIT, МГТУ им. Н.Э. Баумана, 2021, 2023).

Публикации. Основные положения диссертационных исследований отражены в 80 научных публикациях (из них 11 без соавторов), в т.ч. в 4 монографиях, изданных в России и за рубежом. 20 публикаций представлены в журналах из Перечня ВАК, 28 - в зарубежных изданиях, цитируемых в международных базах данных, 20 – в материалах отечественных и международных конференций [4, 5, 49, 52, 53, 58, 64, 69, 70, 77, 83, 84, 97, 101 - 167]. Имеется 9 свидетельств Роспатента на программы для ЭВМ, в ноябре 2025г. поданы заявки на регистрацию в Роспатенте еще четырех программ для ЭВМ (без соавторов) [168 – 181].

Объем и структура диссертации. Материалы диссертации изложены на 350 страницах машинописного текста; включают введение, 5 глав, заключение, приложения. Список литературы насчитывает 192 наименования.

1 АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К УПРАВЛЕНИЮ РИСКАМИ В ПРИЛОЖЕНИЯХ СИСТЕМНОЙ ИНЖЕНЕРИИ. ПОСТАНОВКА НАУЧНОЙ ПРОБЛЕМЫ

1.1 Выявление тенденций в приложениях системной инженерии, характеризующих важность управления рисками

Согласно ГОСТ Р 57193-2025 «Системная и программная инженерия. Процессы жизненного цикла систем» (разработанного с учетом положений одноименного международного стандарта ISO/IEC/IEEE 15288, NEQ) системная инженерия – это междисциплинарный подход, управляющий полным техническим и организаторским усилием, требуемым для преобразования ряда потребностей заинтересованных сторон, ожиданий и ограничений в решение и для поддержки этого решения в течение его жизни. Т.е. системная инженерия по сути заключается в сосредоточении научно-технических усилий на том, как рациональным образом построить и эффективно эксплуатировать различные искусственно создаваемые системы, а также выводить их из эксплуатации. При этом под системой понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей [2, 5, 37, 77].

Согласно прогнозам Международного совета по системной инженерии (INCOSE) глобальный контекст для системной инженерии ближайшего десятилетия определяют [1, 5, 67 – 167]:

расширение применения системной инженерии в различных областях промышленности, а также для содействия в формировании стратегий, связанных с социальными и природными системами;

охват и изучение разнообразия подходов к разработке систем, необходимость развития теоретических основ системной инженерии, совершенствование инструментариев, моделей и методов решения сложных задач;

появляющиеся социо-экономические вызовы, связанные с обеспечением доступности к информации, коммуникациям и образованию, с растущими человеческими и социальными потребностями, с сохранением здоровья, обеспечением чистой водой и пропитанием и пр.;

вызовы природной среды, такие как изменения климата, воспроизводимость ресурсов.

Все эти аспекты характеризуются высокой степенью разнородных неопределенностей (природных, техногенных, информационных, социальных и пр.), влияющих на создание и применение систем различного функционального назначения.

Возможности системной инженерии должны обеспечивать всестороннюю интеграцию многочисленных технических, рыночных, социальных и экологических требований заинтересованных сторон с учетом всего жизненного цикла систем и долгосрочных рисков. На системную инженерию возлагается интегрирующая роль в поддержке взаимодействия и сотрудничества, охватывающего широкий спектр научных дисциплин. Для этого перспективная системная инженерия должна поддерживаться междисциплинарной теоретической основой, методами и инструментариями прогнозирования и исследований, основанными на моделях, позволяющих в условиях реальных и гипотетичных вызовов и угроз осуществлять упреждающее выявление «узких мест» и определение рациональных способов снижения и удержания рисков в допустимых пределах в жизненном цикле различных систем. Системы будут создаваться обученными специалистами с использованием эффективных инструментариев, реализующих прагматичные инновации для поддержания необходимой конкурентоспособности на отечественном и мировом научно-технологическом рынке.

Проведенный анализ показал [5, 167 – 167], что сегодня глобальные потребности в рациональном построении и эффективном применении различных систем существенно опережают прогресс в области системной инженерии. Практическое применение во многом основано на эвристике и варьируется в зависимости от отраслей, организаций и типов систем. Перекрестное внедрение в различных отраслях промышленности существующих методов системной инженерии идет медленно. Теоретические основы системной инженерии еще продолжают находиться в стадии становления. Ключевой нерешенной проблемой остается слабая междисциплинарная интеграция научно-технических усилий, применимая на разных этапах жизненного цикла различных систем.

В диссертации рассматриваются сложные системы, целенаправленно создаваемые человеком для различных приложений – автоматизированные системы управления, информационно-телекоммуникационные системы, энергетические и промышленные структуры (в т.ч. отдельные предприятия, нефтегазовые и транспортные комплексы, предприятия опасного производства, фармацевтические заводы), цифровые двойники, различные системы с использованием искусственного интеллекта и др. Изучаемые в работе взгляды и методы системной инженерии – это сначала обоснование системных требований, способных привести к успеху. Далее, исходя из этих требований у системных аналитиков, в т.ч. лиц, принимающих решения, появляются возможности для целенаправленного поиска обоснованных идей и эффективных решений на основе применимых методов и моделей, физически понятных и обеспечивающих оперативную оценку, прогнозирование и оптимизацию частных и интегральных показателей в жизненном цикле систем.

В России системная инженерия традиционно нацелена не только на обеспечение обоснованной безопасности и достижимого качества, но и на обеспечение сбалансированных эффектов, устойчивого функционирования и развития систем. Ожидаемые эффекты опираются на применение различных методов системного анализа, под которым понимается научный метод системного познания, предназначенный для решения практических задач системной инженерии путем представления рассматриваемых системных процессов, системы и/или соответствующего проекта в виде приемлемой моделируемой системы (более подробно см. например, ГОСТ Р 59989 – ГОСТ Р 59994). Под моделируемой системой понимается система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей в условиях их применения. В качестве модели системы могут выступать формализованные сущности, объединенные целевым назначением (по ГОСТ Р 59341). Например, при проведении системного анализа в принимаемых допущениях, ограничениях и предположениях модель может формально описывать процесс, функциональные действия, множество активов или множество этих или иных сущностей в их целенаправленном применении в задаваемых условиях [5, 167 – 167].

Методы системного анализа применяются при создании, модернизации, развитии и эксплуатации системы для обеспечения ее качества, безопасности и/или эффективности, а также при выведении системы из эксплуатации (для обеспечения требований безопасности). Так, для условий неопределенности методы системного анализа включают:

- измерение и оценку специальных показателей, связанных с критичными сущностями рассматриваемой системы, прогнозирование рисков, интерпретацию и анализ приемлемости получаемых результатов для рассматриваемых системных процессов, системы (и/или ее элементов) и/или проекта;

- определение с использованием вероятностного прогнозирования рисков существенных угроз и условий, способных при том или ином развитии событий негативно повлиять на свойства рассматриваемых системных процессов, системы (и/или ее элементов) и/или проекта;

- обоснование с использованием вероятностного прогнозирования рисков и оптимизации упреждающих мер обеспечения и повышению качества, безопасности и/или эффективности рассматриваемой системы (и/или ее элементов) и достижения целей системной инженерии при задаваемых ограничениях в задаваемый период времени.

Ожидается, что в ближайшие 10 лет системная инженерия добьется значительных успехов в решении приоритетных задач обеспечения национальной безопасности России.

Анализируемые системы будут продолжать рассматриваться как сложные системы, структурно состоящие из подсистем и системных элементов. Последние, в свою очередь, сами будут представлять собой специфические киберфизические системы во взаимодействии с человеком или искусственным интеллектом [5, 167 – 167].

Роль и место системной инженерии в решении актуальных практических задач проиллюстрированы на абстрактном рисунке 1.1. Актуальность и влияние системной инженерии будут продолжать расти, выходя за рамки крупномасштабной разработки отдельных систем и продуктов, расширяя тем самым спектр приложений для инженерных и социально-технических систем [5, 167].

Рис. 1.1 Роль и место системной инженерии в решении актуальных практических задач

Системная инженерия неизбежно привнесет в цифровую трансформацию междисциплинарный подход, который уже сейчас имеет решающее значение для внедрения инноваций, улучшения качества, безопасности и эффективности систем, повышения доверия конечных пользователей. Практика системного проектирования в определяющей степени будет ориентирована на модели, используя обширную библиотеку повторно используемых элементов, позволяя быстро реагировать на изменения в потребностях заинтересованных сторон и технологиях. При этом будут остро востребованы необходимые

методы системной инженерии для управления постоянно растущей сложностью и рисками на протяжении всего жизненного цикла систем. Системные аналитики, руководствуясь задаваемыми требованиями заинтересованных сторон, допустимыми условиями и ограничениями, используя специальные методы, модели и инструментарии, накапливаемые знания и мониторируемые данные, будут оперативно вырабатывать и обосновывать варианты системных решений. Лучшие из предлагаемых решений подлежат воплощению в конкретных приложениях, которые, в свою очередь, согласно изначальному замыслу будут оказывать изначально задуманное влияние на реальную жизнь и общество. Заинтересованные стороны, учитывая это влияние, будут формулировать новые (или уточненные) требования, что повлечет за собой необходимость нового (или уточняющего) прогнозирования различных рисков и решения задач системной инженерии относительно рассматриваемой системы. И в той или иной степени вариации это повторяется при реализации различных процессов в жизненном цикле систем (анализ процессов см. в 1.2).

Таким образом в условиях разнородных неопределенностей роль системной инженерии в решении практических задач характеризуется научной фундаментальностью в достижении целей системы за счет оперативного прогнозирования рисков, упреждающего выявления «узких мест» и определения рациональных способов снижения и удержания рисков в допустимых пределах. Место системной инженерии – везде, где возникает потребность в решении задач системного анализа и оптимизации, а также поиска и исследования новых практических идей и возможностей [5, 167].

С годами методы управления рисками в системной инженерии становятся все более востребованным из-за глобальных социально-экономических изменений в сочетании с технологическим прогрессом, из-за растущей сложности и расширения практических возможностей различных систем, из-за происходящих в мире изменений. Чтобы понять, в какой точке эволюционного развития может оказаться Россия в ближайшие 10 лет и как рациональным образом управлять этим развитием, необходимо своевременно выявить тенденции в приложениях системной инженерии, провести анализ множества складывающихся тенденций в изменениях различного рода систем с точки зрения упреждающего управления рисками.

Анализ проводится в неразрывной связи системной инженерии с решением задач функционирования, развития и комплексной безопасности сложных систем, подлежащих исследованиям для обеспечения национальной безопасности России согласно «Стратегии национальной безопасности Российской Федерации» (далее по тексту - «Стратегия…») [4, 5, 167]. Здесь и далее в работе используется структуризация, принятая в «Стратегии…» от уровня национальных интересов и стратегических национальных приоритетов (см. рис.

1.2) до уровня задач, подлежащих решению с использованием методов системной инженерии.

Рис. 1.2 Структурирование стратегии национальной безопасности РФ до уровня национальных интересов и стратегических национальных приоритетов

В общем случае для самых различных систем актуальные задачи системной инженерии связаны с:

- реализацией государственной стратегии в экономике;

- обеспечением безопасности и устойчивого развития регионов;

- обеспечением качества функционирования и развитием народнохозяйственных, инженерно-технических, энергетических, транспортных систем, систем связи и коммуникаций;

- обеспечением безопасности систем жизнеобеспечения и жизнедеятельности человека;

- обеспечением эффективности оборонно-промышленного комплекса;

- развитием критических технологий (например, компьютерного моделирования; информационных и когнитивных технологий; технологий информационных, управляющих, навигационных систем; технологий поиска, разведки, разработки месторождений полезных ископаемых и их добычи; технологий атомной энергетики;

технологий предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера);

- обеспечением безопасности критической информационной инфраструктуры, информационной и информационно-психологической безопасности;

- обеспечением промышленной безопасности, технической диагностики, управления ресурсом эксплуатации критически важных объектов и систем;

- обеспечением энергетической безопасности (в том числе функционирования и развития топливно-энергетического комплекса, нефтяной, газовой и нефтехимической промышленности, электроэнергетики, трубопроводного транспорта);

- обеспечением ядерной и радиационной безопасности;

- обеспечением безопасности горнодобывающей промышленности;

- обеспечением продовольственной безопасности;

- обеспечением экологической безопасности, экодиагностики и охраны природы;

- обеспечением безопасности освоения континентальных шельфов;

- решением иных задач обеспечения национальной безопасности, часть из которых рассматривается в настоящей работе.

При этом применение методов системной инженерии основано на формальных постановках задач анализа и оптимизации. В этой связи рассмотрим основные тенденции в приложениях системной инженерии, в изменениях различного рода систем, подлежащих анализу и оптимизации в интересах обеспечения национальной безопасности Российской Федерации согласно «Стратегии…» (см. рис. 1.3) [4, 5, 167 - 167]. Адекватная реакция на выявленные тенденции позволит лицам, принимающим решения, ученым и специалистам сориентироваться в нынешних условиях в направлениях результативного применения, дальнейшего совершенствования и развития методов системной инженерии.

1-я тенденция заключается в повороте к кардинальному совершенствованию мобилизационных возможностей государства для укрепления оборонно-промышленного комплекса и обороны страны.

2-я тенденция в изменениях различного рода систем заключается в расширенном практическом внедрении результатов технического прогресса для совершенствования и развития функциональных возможностей систем.

Рис. 1.3 Основные тенденции в изменениях различного рода систем

Технический прогресс позволяет создавать новые системные решения, в свою очередь потребности в различных системах стимулируют развитие технологий. Получается взаимообратное стимулирующее влияние, поскольку технологические достижения и системные решения в значительной степени взаимозависимы. Проектирование систем базируется в основном на доступных технологиях, но по мере развития технологий становятся возможными новые проектные решения. Перед разработчиками технологий стоит задача сосредоточить научно-технические усилия, чтобы «поспеть в срок» с учетом меняющихся потребностей и ожиданий заинтересованных сторон. В свою очередь, применение и демонстрация новых технологий в конкретных системах могут подтвердить полезность технологических достижений, в т.ч. от создания новых материалов, развития информационных технологий, преобразования и накопления энергии, от удивительных возможностей биотехнологий и др. до их прагматического применения для развития страны и противодействия разнородным угрозам.

Уже сегодня многие системные решения начинают активно базироваться на киберфизических системах, включающих в свой состав датчики, средства обработки

данных, сети и хранилища данных для управления системными процессами. Со своей стороны системы сами могут выступать как части более крупной системы, формируемой из составных систем. Они взаимосвязаны с другими системами для совместного использования ресурсов и информации. Например, на слуху такие системы как "умные " здания, "умный" транспорт, "умные" коммунальные службы. Они являются частью "умных" городов. Подобные сложные системы все чаще используют средства и системы искусственного интеллекта (ИИ) - см. подробнее 4-ю тенденцию.

По мере того как общество извлекает выгоду из расширения возможностей систем, потребители начинают ожидать большего от этих систем. Ожидания связываются, как правило, с обеспечением и повышением качества, безопасности, эффективности систем, предсказуемости и устойчивости их функционирования, доступности по цене.

3-я тенденция заключается в существенном усложнении систем, обострении проблематики информационной безопасности, широком внедрении методов количественного прогнозирования рисков и обоснования упреждающих мер противодействия разнородным угрозам.

Сложность возникает при проектировании систем, при этом расширяется множество разнородных угроз и взаимосвязей. В условиях неопределенностей возникают дополнительные зависимости и уязвимости, обостряются вопросы отказоустойчивости и информационной безопасности. Разнородные угрозы порождают риски, которые необходимо понимать и раскрывать лицам, принимающим решения. Конкретные научно-технические усилия должны быть сосредоточены на устойчивом удержании рисков в допустимых пределах с учетом возможных ущербов и последствий с соблюдением баланс интересов различных заинтересованных сторон.

Ожидается, что в комплект инструментариев системного аналитика прочно войдут различные модели, позволяющие осуществлять количественное прогнозирование рисков для недетерминированных систем, а также улучшать способность постоянно отслеживать поведение систем с течением времени. Практика системной инженерии потребует интеллектуальных механизмов сбора данных и будет включать как формальные, так и полуформальные методы выявления возникающих начальных признаков возникновения и проявления угроз, обнаружения, количественной оценки и управления рисками в условиях неопределенностей. Аналитические методы системной инженерии позволят использовать большие массивы данных мониторинга в режиме реального времени. Инструменты визуализации позволят проводить интерактивный анализ с различных точек зрения заинтересованных сторон, позволяя лицам, принимающим решения, получать новые идеи, проводить анализ "что, если…" и сообщать о влиянии своих решений. Ожидается широкое

внедрении методов количественного прогнозирования рисков и обоснования упреждающих мер противодействия разнородным угрозам.

На системном уровне границы между отраслями, рынками, областями применения, требованиями и показателями эффективности систем должны быть охарактеризованы количественно в их взаимовлиянии. При этом также должны учитываться вопросы сложности, качества, адаптируемости и масштабируемости программного обеспечения. Масштабируемые системы должны быть приспосабливаемыми к целому ряду характеристик и возможностей системы без переделки фундаментальных архитектурных решений. Масштабируемость и адаптируемость должны учитываться с момента создания конкретных систем.

4-я тенденция заключается в целенаправленной интеллектуализации систем и технологий. Применение элементов и систем, реализующих технологии и возможности искусственного интеллекта, функции автоматизации и автономии, использующих усовершенствованные датчики для определения функционального поведения, самодиагностики и ремонта системы, начинают становиться обычным явлением. Однако многие условия неопределенности сохраняются, а вместе с ними сохраняется актуальность вопросов проверяемости, безопасности и доверия к интеллектуальным системам, объяснения и понимания логики их действий.

Формализованное представление информации на основе онтологии становится нормой, на основе которой обеспечивается не только осведомленность множественных элементов системы о состоянии друг друга, но и прослеживаемость различных действий. Инструментарии системной инженерии будут дополнены методами и управляемыми параметрами, учитывающими контекст. Это позволит системному аналитику уделять больше времени творческим задачам и меньше рутинным операциям ввода данных, проверки согласованности, формирования отчетов и многим другим. Вместо рутинных действий системные аналитики будут сообщать интеллектуализированным инструментариям системной инженерии о своих намерениях по проектированию. В ответ такие инструментарии должны помогать в разработке качественных спецификаций, подборе необходимых данных, проведении расчетов, анализе и интерпретации получаемых результатов, формировании и обосновании рекомендаций, а также в оформлении аналитических отчетов и иной конструкторской и эксплуатационной документации. Кроме того, системные аналитики сами будут чаще участвовать в разработке систем с компонентами искусственного интеллекта, что потребует новых навыков системной инженерии. Системные аналитики будут играть решающую роль в разработке наборов

данных для машинного обучения и проверки поведения систем, оценки различных показателей качества, безопасности и эффективности.

Интеллектуальные системы станут обычным явлением в различных областях, таких как государственная и общественная безопасность, городские комплексы, жилые дома, бытовая техника, здравоохранение, финансовые услуги, энергетика, телекоммуникации, частный и общественный транспорт, сельское хозяйство. Интеллект будет приближаться к автономным устройствам и системам и удаляться от централизованного управления.

Проектирование на основе риск-ориентированного подхода с определенным акцентом на обоснованный пользовательский опыт станет ключевым фактором успеха интеллектуальных систем. Системы уже сегодня начинают проектироваться таким образом, чтобы содержать данные и информационные потоки, необходимые для их постоянного развития. Система, создающая другую систему, представляющую интерес, сама начинает представлять практический интерес, т.е. обе эти системы начинают сливаться в одну интегрированную систему систем. И таких сложных систем, комплексируемых из различных систем, будет становиться все больше.

Применение искусственного интеллекта, основанное на больших массивах данных и экспертных знаниях предметной области, приведет к серьезным изменениям в методах и инструментариях системной инженерии, помогая системному аналитику быть более эффективным при выработке, обосновании и предоставлении решений. Для сложных систем, которые продолжают обучаться и модифицировать себя в процессе эксплуатации, обычные методы системной инженерии, свойственные концу прошлого века, будут терять свою актуальность. Более привлекательными станут модели и методы, адаптирующиеся под сложные структуры, подлежащие созданию и системным исследованиям.

Вместе с тем системы искусственного интеллекта могут иметь значительные социальные и этические последствия, которые необходимо учитывать при проектировании. Примерами могут служить критические решения, принимаемые автономными транспортными средствами (с нарушениями существующих норм безопасности), а также то, как эти системы потенциально могут создавать информацию, нарушающую требования по обеспечению конфиденциальности. Методы обработки данных в интеллектуальных системах будут требовать постоянного совершенства. Кроме того, верификация и валидация этих систем в настоящее время основаны на традиционных подходах системной инженерии. Неизбежно потребуются новые методы, позволяющие учесть непрозрачность того, как системы искусственного интеллекта принимают решения. В свою очередь необходимость постоянной проверки машинно дообучаемых и эволюционирующих систем и сравнение их развития с предыдущими версиями по показателям качества, безопасности

и эффективности также потребует совершенствования методов системной инженерии (новые версии не должны допускать деградации интеллекта по сравнению с предшественниками).

5-я тенденция заключается в неизбежном заметном влиянии цифровой трансформации на создаваемые системы, выпускаемую продукцию, стиль и методы работы людей. Коммерческие и государственные предприятия активно предпринимают усилия по модернизации процессов и продукции, переходя к надежному цифровому представлению корпоративной информации и семантической интеграции информации по всему предприятию и цепочкам поставок для проектирования, разработки, производства, сопровождения, обеспечения логистики и бизнес-анализа. Разработка знаний, представление информации, управление моделями и аналитика данных уже начинают и будут лежать в основе способов принятия решений и выполнения совместных работ. Потребительская ценность будет достигаться не только за счет конечной продукции, но и во все большей степени за счет предоставления услуг. Цифровая трансформация обеспечит преимущества более гибким и конкурентоспособным предприятиям. При создании еще более совершенных продуктов и услуг, а также в интересах снижения себестоимости продукции программируемые роботы будут дополнять и по возможности - заменять физических работников, что повлечет за собой исчезновение профессий, базирующихся главным образом на физическом труде работников.

При цифровой трансформации предприятия неизбежно повысится его зависимость от принятия научно обоснованных количественных решений, оптимизируемых процессов разработки и рациональной автоматизации систем. Как следствие, математическое моделирование и системный анализ, визуализация системных решений, процессов и проектов, обеспечиваемых высокоточными цифровыми представлениями, будут доминировать в практике всех инженерных дисциплин. Доступность и низкая стоимость использования вычислительных ресурсов позволят системным аналитикам оценивать широкий и разнообразный набор альтернатив и сценариев для все более сложных систем. При этом дополнительные возможности искусственного интеллекта будут способствовать все большей их интеграции с возможностями аналитических инструментариев на протяжении всего жизненного цикла конкретных систем.

Цифровые представления систем позволят изучать детали проекта, его преимущества и недостатки, в т.ч. на уровне физических, технических, эксплуатационных характеристик, аспектов безопасности. Ожидается, что использование виртуальной реальности и/или дополненной реальности, включая среды с высокой степенью погружения, цифровое представление продуктов, производственной и эксплуатационной среды будут

всеобъемлющими. Цифровое представление станет обычным явлением при анализе систем на протяжении всего их жизненного цикла. Это позволит инженерам исследовать конструкции и методы производства как концептуально, так и физически с различных точек зрения, помещая себя в виртуальную среду интересующей системы. Специализированные визуализации помогут системным аналитикам понять поведение систем и ее элементов в зависимости от времени. Анализ неопределенностей и альтернатив будет проводиться намного быстрее и гораздо более детально, в т.ч. с использованием вероятностных методов прогнозирования рисков. Методы системной инженерии будут адаптироваться к используемым цифровым технологиям и трансформироваться с их помощью.

Растущая зависимость стиля и методов работы от цифровых представлений потребует тщательного анализа кибербезопасности в целях защиты информации и соблюдения прав на интеллектуальную собственность. Актуальность системного анализа этих вопросов в том, что киберпространство постоянно развивается, ежедневно появляются новые угрозы, в том числе более широкий спектр субъектов национальных государств, осуществляющих атаки с целью получения политической, стратегической и экономической выгоды. Должен быть обеспечен анализ рисков в киберпространстве на протяжении всего жизненного цикла анализируемых систем, включая анализ цепочек поставок комплектующих для устранения любых «узких» мест. Все большее распространение будут получать инструментарии моделирования, помогающие тестировать и оценивать кибернетические аспекты системы, обеспечивая целостную картину ее безопасности в жизненном цикле (сегодня слишком часто эти аспекты рассматривается только на поздних этапах разработки системы).

6-я тенденция заключается в переходе промышленности на принципы и технологии индустрии 4.0. Промышленность всего мира еще несколько лет будет находиться в процессе переосмысления самой себя, приспосабливаясь к новым социальным и технологическим вызовам. За последние триста лет промышленность эволюционировала от примитивной механизации к массовому производству, затем к автоматизации на основе электроники, а теперь и к киберфизическим системам, объединяющим вычисления, сетевые взаимодействия и физические процессы. Встроенные компьютеры и сети отслеживают физические процессы и управляют ими с помощью контуров обратной связи, в которых физические процессы влияют на вычисления и наоборот. Глобальное взаимодействие и взаимозависимость машин, складов, логистических систем и инжиниринга в рамках киберфизических систем создают неограниченную гибкость автономных автоматизированных процессов (немецкая академия технологий Acatech назвала этот подход “Индустрией 4.0”).

В соответствии с "Индустрией 4.0" логика и управление производством существенно меняются и формируют основу для «умных» фабрик. Продукты отслеживаются, на любой момент времени известно состояние их производства и отгрузки, а конфигурации их состояния заносятся в индивидуальную каталогизацию на каждом этапе их жизненного цикла. Информация о каждом компоненте более крупной системы становится прозрачной для клиентов, производителей и цепочек поставок. Цифровые двойники находятся в центре общего жизненного цикла разработки системы. Цифровые цепочки взаимодействующих инструментов и процессов являются бесшовными на протяжении всего жизненного цикла, устанавливаются на каждом звене участвующих игроков, доступны для всех участников и пользуются доверием.

7-я тенденция заключается в построении нового социального общества и решении социальных проблем методами, базирующимися на интеграции реального физического мира с виртуальным киберпространством.

Новое социальное общество (называемое иногда в англоязычной литературе как «Общество 5.0») формирует стремление современного человека и подрастающего поколения к широкому применению социально-ориентированных киберфизических систем. Экономический прогресс увязывается с решением социальных проблем с использованием различных систем, интегрирующих киберпространство и физическое пространство. В этом социальном обществе данные с датчиков в физическом пространстве накапливаются в киберпространстве, анализируются с привлечением искусственного интеллекта, а результаты передаются обратно людям в физическом пространстве в различных формах для прагматичного применения в жизни.

Методы системной инженерии включают интегрированные концепции взаимодействия киберфизических систем с пользователем с учетом человеческого фактора во всех аспектах проектирования систем. По мере становления нового общества социально-ориентированные киберфизические системы будут становиться все более автономными, при этом они должны быть безопасными и заслуживающими доверия в условиях разнородных угроз (информационных, политических, экономических, природных, социальных и др.). Анализ и прогнозирование поведения таких систем будут более сложными, но ожидается, что системные аналитики будут проектировать и анализировать эти системы с учетом естественных принципов. Практика системной инженерии будет включать методы оценки человеческого фактора и удобства использования, выявления возникающих признаков проявления угроз со стороны киберфизических систем, а также обнаружения и управления их непредвиденным поведением.

Человеко-машинные интерфейсы продолжат развиваться в соответствии с современными тенденциями, предоставляя пользователям широкий спектр способов взаимодействия с системами, включая голос, прикосновения, жесты, мысли. При этом по-прежнему будут рассматриваться различные аспекты, которые полежат адекватной интеграции. Это - человеческие и организационные факторы, планирование и управление проектами, трудовые ресурсы и эволюция рабочих мест, персонал, обучение, жизненно важные аспекты, включая гигиену труда, безопасность, окружающую среду, пригодность для проживания и выживаемость человека. Должны учитываться точки зрения всего персонала, начиная от владельцев систем и конечных пользователей и заканчивая операторами, персоналом технической поддержки и сопровождения.

8-я тенденция заключается в накоплении и использовании знаний для повышения качества, безопасности и эффективности систем и оптимизации управления предприятиями, проектами и системами.

Стремясь оправдать ожидания заинтересованных сторон, предприятия, которые разрабатывают, производят, эксплуатируют и поддерживают системы, сталкиваются с растущей конкуренцией на мировом рынке. Это требует, чтобы они предоставляли инновационные продукты и услуги, одновременно сокращая затраты и время производственного цикла, повышая устойчивость и реагируя на изменения в законодательстве, киберугрозы и сбои в цепочках поставок. Знания становятся важнейшим активом предприятий. Чтобы предприятие оставалось конкурентоспособным, создаваемые инновации, используемые технологии и навыки рабочей силы должны постоянно развиваться на основе этих знаний. Цифровые технологии позволят трансформировать способы сбора, повторного использования, эксплуатации и защиты знаний предприятиями посредством цифрового представления и семантической интеграции всей информации. Развивающиеся на этой основе когнитивные технологии, включая более широкое применение искусственного интеллекта, позволят использовать автоматизацию и автономию для выполнения все более сложных задач, предоставляя людям дополнительные возможности для повышения качества, безопасности и эффективности систем за счет внедрения инноваций.

Для того, чтобы предприятие продолжало эффективно развиваться, им необходимо надлежащим образом управлять. Успешные предприятия будущего должны предвидеть новые технологии и быстро осваивать их. Недостаточно будет просто ждать, пока технология зарекомендует себя на рынке. Системный подход будет иметь решающее значение для понимания технологий, которые будут наиболее важны для предприятия и оптимизации управления предприятиями, проектами и системами.

Настоящее и будущее системной инженерии основано на моделях (математических, физических, комбинированных), использующих среды моделирования, имитации и визуализации для определения, анализа, проектирования, верификации и валидации систем. В условиях неопределенностей особое значение приобретает вероятностное моделирование, прогнозирование и оптимизация. Иллюстрация роли вероятностного моделирования, прогнозирования и оптимизации для системного решения задач и обоснования упреждающих действий в условиях неопределенности приведена на рис. 1.4. Прогнозирование в полной мере базируется на мониторинге состояний, накоплении и рациональном использовании знаний, в т.ч. формируемых в режиме реального времени функционирования различных систем [2, 4, 5, 167].

Рис. 1.4 Иллюстрация роли вероятностного моделирования, прогнозирования и оптимизации для системного решения задач и обоснования упреждающих действий в условиях неопределенности

Различные методы извлечения знаний и анализа необходимых данных, обработки и интерпретации результатов моделирования будут более широко внедряться в практику системной инженерии. Моделируемые, наблюдаемые и экспериментальные данные будут собираться, индексироваться и интегрироваться с проектными моделями для улучшения понимания сложных систем. Все это поможет более эффективно разбираться с крупномасштабными наборами данных и разносторонне исследовать сложные системы, в

т.ч. поведение систем во времени в различных проектных и, при необходимости, в запроектных условиях эксплуатации.

9-я тенденция заключается в развороте к системному решению проблем экологической безопасности и рационального природопользования. Потребление невозобновляемых ресурсов в результате экономической деятельности будет все больше требовать улучшения глобального управления, стратегий утилизации отходов, устойчивой политики, местных действий и вспомогательных систем для решения проблем экологической безопасности и рационального природопользования.

Изменение окружающей среды неизбежно приводит к изменениям в условиях жизни и влияет на биологическое разнообразие, климат, глобальный перенос тепла, доступность пресной воды и других природных ресурсов, необходимых для поддержания жизнедеятельности и благополучия человека. Общее качество окружающей среды станет приоритетом, требующим глобального сотрудничества в заботе об экологической устойчивости.

Чтобы сохранить естественную природу России для многих поколений, обязанностью системных аналитиков на долгие годы будет анализ различных форм взаимодействия между природными и антропогенными системами, разработка подходов к смягчению экологических последствий и обоснование эффективных мер рационального природопользования при реализации государственной экономической политики.

Наконец 10-я важная тенденция, рассматриваемая в настоящей работе, заключается в реформировании профессиональной подготовки специалистов для эффективного решения проблем системной инженерии.

Сегодня все больше отраслей народного хозяйства признают системную инженерию важнейшим междисциплинарным научно-техническим направлением, позволяющим на практике справляться с растущей сложностью современных систем. Однако увеличивающийся во всем мире спрос на высококвалифицированных специалистов, способных эффективно решать проблемы системной инженерии во многих прикладных областях, превышает имеющиеся предложения. Отчасти это связано со стремлением “высокотехнологичных” организаций к более глубокой, но и более конкретно зауженной (из-за ограниченного срока обучения) инженерной специализации для своих «сиюминутных» специально фрагментированных проектных работ. Т.е. временные потребности “высокотехнологичных” организаций, заточенные на эгоистичное извлечение выгод в конкретный период времени в условиях капитализма, сами представляют собой искусственные ограничения для высокопрофессиональной подготовки специалистов системной инженерии широкого профиля. Развитие автоматизации и автономности систем,

быстро меняющиеся технологии и потребность в кибербезопасных и надежных системах увеличили потребность в широких компетенциях в области системной инженерии. Растет понимание того, что необходимо дополнение сложившихся предметных компетенций с упором на расширение технического кругозора, развитие системного мышления и овладение соответствующими междисциплинарными методами. Несмотря на растущее в России число университетских программ для выпускников и программ профессиональной подготовки, большинство специалистов, призванных волею судьбы профессионально решать на практике проблемы системной инженерии, не имеют формального образования в области системной инженерии, а учатся “без отрыва от производства”. Это, в свою очередь, ограничивает способность таких специалистов быть в курсе последних достижений в области науки, практики и технологий с уровнем компетентности, требуемым для адекватного анализа и оптимизации сложных систем различного функционального назначения.

Система высшего образования и профессиональной подготовки специалистов (включая переподготовку, наставничество и обучение) должны обеспечивать овладение мультидисциплинарными компетенциями на протяжении всей их творческой жизни. К фундаментальным специализациям, поддерживающим методы системной инженерии, относятся основы теории вероятностей, теории управления, теории систем и сетей, теории принятия решений, исследования операций, анализа рисков, теории информации, программно-технические основы киберфизических систем с прикладным ИТ-наполнением. Системщик также должен понимать, как строить вероятностное пространство событий, как интерпретировать и использовать вероятность и статистику для понимания рисков и неопределенности, а также понимать принципы взаимосвязи для управления сложностью систем. В дополнение к этим научным и аналитическим основам системной инженерии в обязательном порядке добавляются методы системного анализа и эвристики, отраженные в стандартах, справочниках и руководствах, накопленных за десятилетия работы с крупномасштабными критически важными и потенциально опасными объектами и системами.

Непрерывное образование, профессиональная подготовка специалистов с развитием системного мышления позволят сформировать широкий круг инженерных и управленческих кадров, обладающих необходимыми техническими и лидерскими компетенциями для эффективного решения проблем системной инженерии в интересах обеспечения национальной безопасности России.

Таким образом, в результате проведенных исследований выявлены и сформулированы 10 основных тенденций в приложениях системной инженерии,

характеризующих важность управления рисками на ближайшую многолетнюю перспективу, это [5, 167, 167]:

1) поворот к кардинальному совершенствованию мобилизационных возможностей государства для укрепления оборонно-промышленного комплекса и обороны страны;

2) расширенное практическое внедрение результатов технического прогресса для совершенствования и развития функциональных возможностей систем (с ожиданием повышения качества, безопасности, эффективности систем, предсказуемости и устойчивости их функционирования, доступности по цене);

3) существенное усложнение систем, обострение проблематики информационной безопасности, широкое внедрение методов количественного прогнозирования рисков и обоснования упреждающих мер противодействия разнородным угрозам;

4) целенаправленная интеллектуализация систем и технологий (с необходимым обеспечением проверяемости, безопасности и доверия к интеллектуальным системам, объяснением и пониманием логики их действий);

5) заметное влияние цифровой трансформации на создаваемые системы, выпускаемую продукцию, стиль и методы работы людей;

6) переход промышленности на принципы и технологии индустрии 4.0 (с «умными» фабриками, киберфизическими системами, цифровыми двойниками и цепочками взаимодействующих инструментов и процессов);

7) построение нового социального общества и решение социальных проблем методами, базирующимися на интеграции реального физического мира с виртуальным киберпространством;

8) накопление и использование знаний для повышения качества, безопасности и эффективности систем и оптимизации управления предприятиями, проектами и системами;

9) разворот к системному решению проблем экологической безопасности и рационального природопользования;

10) реформирование профессиональной подготовки специалистов для эффективного решения проблем системной инженерии.

В России особое место в методах системной инженерии занимают методы анализа различных процессов жизненного цикла систем. Во многом это обосновано не только важностью этих процессов для получения конечных системных результатов, но и традиционным лидерством российской научной школы в области теории вероятностей и теории случайных процессов, на базе которых строятся вероятностные модели для прогнозирования рисков применительно к сложным системам.

Далее, прежде, чем сформулировать решаемую научную проблему, приводится более детальная вербальная характеристика самих процессов жизненного цикла систем и анализ существующих подходов к управлению рисками. Это важно для последующего понимания формализованной сути предлагаемых программных и технологических решений для ВС и КС и извлекаемых при вероятностном моделировании прагматических эффектов.

1.2 Анализ существующих подходов к управлению рисками в жизненном цикле систем

В общем случае в жизненном цикле систем различного функционального назначения используются следующие стандартизованные процессы (по ГОСТ Р 57193):

- процессы соглашения – процессы приобретения и поставки продукции и услуг;

- процессы организационного обеспечения проекта – процессов управления моделью жизненного цикла, инфраструктурой, портфелем проектов, человеческими ресурсами, качеством, знаниями;

- процессы технического управления – процессы планирования проекта, оценки и контроля проекта, управления решениями, рисками, конфигурацией, информацией, измерений, гарантии качества;

- технические процессы – процессы анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы.

Для более глубокого понимания идей и возможностей системной инженерии в таблице 1.1 стандартизованные процессы жизненного цикла систем детализированы до уровня возможных целей в их общем виде и типовые действий в процессах [2, 4, 5, 83-85, 101, 136, 149, 151, 167].

Таблица 1.1. Анализ процессов жизненного цикла систем, целей и типовых действий

Процессы	Цели	Основные типовые действия в процессе
Процесс приобретения продукции и/или услуг для системы	Надежная реализация приобретения продукции и/или услуг заданного качества в заданные сроки согласно соглашению	1) выбор поставщика; 2) заключение соглашения, предусматривающего удовлетворение конкретных требований, контрольные сроки, условия верификации, приемки, аттестации приобретаемых продукции и/или услуг, обработки исключительных ситуаций, процедуры контроля и оценки изменений, графики оплаты; 3) выполнение соглашения и его контроль
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс поставки продукции и услуг для системы	Надежная поставка продукции и/или услуг заданного качества в заданные сроки согласно соглашению	1) заключение соглашения между приобретающей стороной и поставщиком; 2) выполнение соглашения и его контроль
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс управления моделью жизненного цикла системы	Определение, сопровождение и обеспечение гарантий наличия в организации необходимых политик, процессов, моделей, инструментариев и процедур для их использования в жизненном цикле системы	1) определение политик и процедур для управления процессом, реализация процесса; 2) определение системных процессов, которые реализуют требования согласно принятым стратегиям организации; 3) определение ролей, ответственности, подотчетности и полномочий должностных лиц; 4) определение бизнес-критериев, обеспечивающих управление развитием системы; 5) определение моделей жизненного цикла, описывающих необходимые стадии и этапы жизненного цикла систем, согласованные с целями и; 6) сбор и системный анализ статистики, технических данных, результатов оценок и прогнозов для понимания сильных и слабых сторон применяемых процессов. Использование результатов системного анализа в качестве обратной связи для совершенствования системных процессов и технологий и внесения корректирующих изменений; 7) контроль выполнения процесса в организации, включая обратную связь; 8) проведение периодического анализа моделей жизненного цикла системы, используемых в различных проектах, включая анализ их реальной пригодности, адекватности и эффективности в каждом из проектов и оценку соответствующих улучшений; 9) определение возможностей улучшений по результатам системного анализа; 10) реализация совершенствующих улучшений, изучение и обобщение положительного опыта, информирование заинтересованных сторон об эффектах
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс управления инфраструктурой системы	Поддержка таких проектных и эксплуатационных решений и действий, выполнение которых формирует функциональные возможности для создания (модернизации, развития) и/или эксплуатации системы и/или выведения ее из эксплуатации	1) определение проектных требований к инфраструктуре; 2) выработка стратегии по создание (модернизацию) и развитие инфраструктуры; 3) разработка ТЗ на создание (модернизацию) или развитие инфраструктуры; 4) разработка рабочей документации; 5) определение элементов инфраструктуры, включая инструментарии, программные средства, программно-аппаратные и технические средства, услуги и стандарты; 6) отбор элементов инфраструктуры, удовлетворяющих требованиям проекта; 7) анализ соответствия отобранных элементов инфраструктуры требованиям проекта; 8) приобретение необходимых элементов инфраструктуры, проведение их сертификационных и аттестационных испытаний (при необходимости); 9) техническое обслуживание (сопровождение) и необходимая поддержку инфраструктуры; 10) оценка рисков нарушения надежности реализации процесса, оценка эффективности функционирования системы с использованием процесса
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс управления портфелем проектов	Инициация и поддержание необходимых проектов, направленных на достижение стратегических целей организации	1) формирование портфеля проектов и обеспечение управления портфелем; 2) системный анализ портфеля проектов, включая: а) анализ степени продвижения проектов, соответствия действующим правовым и нормативным документам, принятым решениям, приказам и распоряжениям, выполнения планов и процедур в жизненном цикле систем для обеспечения их жизнеспособности; б) принятие решений по продолжению или переопределению проектов; в) уточнение приоритетов проектов по интегральному показателю и/или в результате обоснованной необходимости для организации; г) оптимизацию и обеспечение сбалансированности портфеля проектов (в т.ч. уточнение состава портфеля проектов, распределения ресурсов между проектами); 3) контроль портфеля проектов, включая оперативное выявление отклонений текущих показателей от плановых и обеспечение корректирующих действий для их устранения; 4) завершение проектов, включая отмену или приостановку проектов, в которых риски перевешивают выгоду от длительных инвестиций
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс управления человеческими ресурсами системы	Обеспечение конкретной системы человеческими ресурсами, необходимыми и достаточными для достижения ее целей на протяжении жизненного цикла	1) формирование человеческих ресурсов: а) определение требований к набираемому персоналу и потребностей в навыках для текущих и ожидаемых проектов; б) составление плана подбора персонала; в) оценка и планирование развития навыков персонала: г) поддержка, оценка и контроль функциональных действий персонала; д) определение стратегии развития навыков персонала; 2) развитие человеческих ресурсов: а) мотивирование и стимулирование труда; б) профессиональное обучение и повышение квалификации; в) наставничество и консультирование; г) делегирование полномочий; д) планирование карьеры; е) привлечение квалифицированных специалистов; 3) оценка эффективности реализации процесса; 4) оценка безопасности, качества и эффективности функционирования системыа
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс управления качеством системы	Удовлетворение организационным и проектным целям в области качества с достижением требуемой удовлетворенности заказчика и пользователей системы	1) планирование управления качеством, включая: а) определение целей, политики и процедур; б) определение обязанностей и полномочий для реализации управления качеством; в) определение критериев и методов оценки качества; г) обеспечение ресурсами и информацией для управления качеством; 2) оценку управления качеством, включая: а) сбор и анализ результатов оценки процесса в соответствии с определенными критериями; б) оценку удовлетворенности заказчика; в) периодический анализ действий по обеспечению качества, контроль улучшений качества для процессов, продукции и услуг; 3) выполнение корректирующих и упреждающих действий по управлению качеством, включая: а) планирование корректирующих действий; б) планирование упреждающих мер при выявлении недопустимых рисков; в) осуществление корректирующих действий
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс управления знаниями о системе	Повышение качества и/или безопасности и/или эффективности системы или связанных с ней систем за счет приобретения, создания, распространения, своевременного применения и сохранения полезных знаний в их жизненном цикле	1) определение потребностей в знаниях; 2) определение стратегии управления знаниями (включая составление планов по получению и поддержанию активов знаний, определение механизмов и процедур для генерации новых знаний, защиты, контроля и доступа к информации и знаниям, хранения и поиска знаний, в том числе распространенных вне организации); 3) определение знаний, которые подлежат управлению; 4) определение проектов, для которых может быть извлечена польза из применения знаний; 5) создание или приобретение активов знаний, сохранение знаний, включая защиту активов; 6) распространение активов знаний по организации; 7) сопровождение активов знаний, контроль и регистрация использования активов знаний, переоценка технологической и рыночной стоимости активов знаний; 8) оценку эффективности процесса управления знаниями; 9) оценку эффективности функционирования организации с использованием процесса
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс планирования проекта	Определение требований и состава работ проекта, составление и доведение до заинтересованных сторон эффективного и выполнимого плана, скоординированного с планами других проектов организации	1) определение требований проекта; 2) определение состава работ и разработку планов проекта, включая определение дат начала и окончания работ, ключевых событий и этапов, взаимосвязи между работами, определение графика привлечения необходимых ресурсов, утверждение календарного плана проекта; 3) планирование бюджета, персонала, закупок, мер по обеспечению качества и безопасности; 4) планирование мероприятий по определению и оценке основных рисков проекта и порядка реагирования на выявляемые риски; 5) планирование мероприятий по определению порядка и обмену информацией между участниками проекта, определению порядка работы с изменениями в проекте; 6) определение модели жизненного цикла проекта с учетом конкретных моделей жизненного цикла систем, используемых в различных проектах организации
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс оценки и контроля проекта	Определение, сопровождение и обеспечение гарантий наличия в организации необходимых политик, процессов, моделей, методик, инструментариев и процедур и их результативное использование в проекте	1) определение стратегии процесса, включая методы оценки, графики работ, необходимые управленческие решения; 2) системный анализ достижения целей и реализации планов проекта, анализ производственных планов для определения их результативности и выполнимости; 3) сравнение плановой и фактической стоимости проекта, анализ сроков выполнения; 4) оценка распределения ролей, ответственности, подотчетности и полномочий персонала; 5) оценка адекватности ресурсов, в т.ч.инфраструктуру, персонал, финансирование, время; 6) оценка выполнения проекта, включая сбор данных и оценку фактических и плановых затрат, наличие материалов, получение услуг, анализ других технических данных; 7) организацию необходимого управления, анализа, аудита и инспекций, регулярные проверки критичных процессов и новых технологий, своевременная корректировка планов; 8) анализ результатов проверок и подготовка рекомендаций по совершенствованию системы; 9) санкционирование продвижения проекта к следующей контрольной точке или событию
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс управления решениями	Обеспечение аналитической основы для определения, характеристики и оценки множества альтернативных решений, выбора наиболее предпочтительных решений и направлений действий на любом этапе жизненного цикла системы	1) планирование управления решениями, включая: а) разработку стратегии, в т.ч. определение ролей, обязанностей, подотчетности и полномочий, установление приоритетов, формирование принципов формализации, математического моделирования и отношения к результатам решений; б) определение потребностей в решении, включая формулирование проблем, неблагоприятных тенденций и открывающихся возможностей; в) вовлечение соответствующих сторон в процесс принятия решений, использование их опыта и знаний; 2) сбор, обработка и анализ информации для принятия решений, включая: а) сбор и обработку данных, анализ их качества; б) обоснование и выбор оцениваемых показателей и критериев принятия решений, выбор и/или разработка методик системного анализа; в) определение области компромиссов и ограничений, обоснование допустимых значений показателей, характеризующих приемлемые решения, формирование альтернативных вариантов решений для системного анализа; г) проведение системного анализа альтернативных вариантов решений и возможных направлений действий; 3) принятие решений и управление решениями, включая: а) решение формализованных оптимизационных задач для альтернативных вариантов; б) определение предпочтительных альтернатив, обоснование и принятие в режиме реального времени приемлемого решения и рациональных направлений действий; в) документирование, отслеживание принятых ранее решений, в т.ч. оценку эффективности, исправление неблагоприятных тенденций
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс управления рисками для системы	Своевременная идентификация рисков, обоснование и реализация эффективных упреждающих мер по снижению рисков или их удержанию в допустимых пределах	1) планирование и управление профилем рисков, включая: а) определение стратегии управления рисками для всех иерархических уровней системы; б) определение и документирование контекста процесса управления рисками, формирование предположений и ограничений, определение множества возможных событий, способных привести к рисковым ситуациям, улучшению, предотвращению, ухудшению, ускорению или задержкам в достижении целей системы; в) определение, обоснование и документирование допустимых рисков и условий, при которых риски могут быть приняты на допустимом уровне; г) определение и сопровождение профиля рисков, ведение отчетности о состоянии каждого из рисков (в т.ч. определение частоты возникновения угроз, времени их развития, периодичности и длительности контроля целостности отслеживаемых параметров, времени восстановления целостности после нарушений, определение возможных последствий и допустимых уровней рисков), весомость каждого риска, возможные действия, планируемые в качестве реакции на недопустимые риски, включая определение необходимых ресурсов; 2) оценка и анализ рисков, включая: а) идентификацияю рисков, в т.ч. через различные исследования надежности, безопасности, производительности, качества и эффективности системы, оценку технологий и архитектуры, анализ альтернативных решений; б) оценку вероятности реализации угроз и возможных ущербов по каждому из идентифицированных рисков, оценивание рисков в сравнении с допустимым уровнем; в) для каждого риска, превышающего допустимый уровень – определение, обоснование и документирование рекомендуемых упреждающих мер противодействия угрозам (направленных на уменьшение риска или смягчение возможных негативных последствий); 3) реагирование на риски, включая: а) выбор альтернативных решений для реакции на риски (в т.ч. упреждающих мер противодействия); б) реализацию мер реакции для снижения рисков до допустимого уровня; в) мониторинг критичных параметров, количественный анализ рисков; г) целенаправленное применение мер реакции на риски; 4) непрерывный контроль рисков, включая: а) контроль идентифицированных рисков и контекста управления рисками во времени; б) количественный анализ показателей рисков, включая сравнение с прогнозируемыми ранее рисками (для оценки эффективности принятых ранее и дополнительных упреждающих мер и реакции на риски); в) выявление новых рисков и источников угроз в различных процессах, реализуемых в жизненном цикле системы
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс управления конфигурацией системы	Определение и формирование требуемых конфигураций, управление изменениями, контроль целостности и обеспечение для заинтересованных сторон санкционированного доступа к конфигурациям в течение жизненного цикла системы	1) подготовительные мероприятия: а) разработку плана управления конфигурацией; б) определение стратегии управления конфигурацией, включая механизм разрешения или запрета доступа, выпуска и управления изменениями элементов конфигурации, указание мест и условий хранения системы и элементов конфигурации, требования к окружающей среде, указание носителей информации, определение порядка управления изменениями и координации по множеству организаций, определение порядка архивирования и поиска объектов конфигурации, артефактов и данных управления конфигурацией; 2) определение конфигурации, включая определение структуры системы, выбор элементов конфигурации и определение базовой конфигурации; 3) управление изменениями, включая: а) сбор, регистрацию, оценку и категорирование заявок по изменениям, включая оценку воздействия предложенных изменений на проектные планы, затраты, выгоды, риски, качество и сроки; б) распределение обязанностей по представлению и внедрению изменений; в) представление заявки для анализа и согласования изменений; д) верификацию изменений; е) обеспечение прослеживаемости изменений; 4) поддержание отчетности о состоянии конфигурации системы и системных элементов; 5) аудит конфигурации для определения соответствия установленным требованиям; 6) контроль за выпуском, включая согласование выпусков и поставок системы, контроль и управление выпусками и поставками системы
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс управления информацией системы	создание, получение, подтверждение, преобразование, сохранение, восстановление, распространение необходимой информации в системе и избавление от ненужной информации. В результате обеспечивается надежное и своевременное предоставление заинтересованным сторонам полной, достоверной и, если необходимо, конфиденциальной информации для ее использования по назначению	1) определение стратегии управления информацией системы; 2) определение информационных объектов, которые подлежат управлению; 3) определение полномочий и ответственности при управлении информацией системы; 4) определение содержания, форматов и структур информационных объектов; 5) определение действий по сопровождению информации (включая анализ статуса хранящейся информации для обеспечения ее полноты, достоверности, безопасности и пригодности); 6) сбор, контроль, обработка, хранение и предоставление информации, подлежащей использованию; 7) сопровождение информационных объектов и записей об их хранении с регистрацией статуса используемой информации и сохранением возможностей к ее восстановлению; 8) обеспечение требуемого уровня безопасности информации для определенных пользователей; 9) архивирование информации (при необходимости); 10) уничтожение ненужной, недостоверной или недействительной информации
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс измерений системы	Сбор объективной информации о разработанных продуктах и/или услугах, оценка путем прямых расчетов или моделирования, анализ процессов, прогнозирование рисков, эффективности и возможностей системы, а в случае выведения системы из эксплуатации – оценка выполнения требований и ограничений	1) планирование измерений, включая: а) определение стратегии измерений; б) описание характеристик организации, проводящей измерения; в) идентификацию и упорядочение по приоритетам информационных потребностей, основанных на бизнес-целях организации, целях проекта, рисках и других факторах, связанных с системными решениями; г) выбор и документирование показателей и единиц измерения, удовлетворяющих информационным потребностям; д) определение процедур сбора данных, анализа, доступа и отчетности; е) определение критериев для оценки результатов измерений; ж) определение ресурсов для решения задач измерений; з) определение и планирование обеспечивающих систем, услуг или технологий; 2) выполнение измерений, включая: а) интеграцию процедур для генерации, сбора, анализа необходимых данных и представления отчетов; б) непосредственно проведение измерений, получение результатов; в) сбор, сохранение, проверку и анализ полученных результатов; г) документирование результатов; 3) оценка измерений, включая оценку самого процесса, полученных результатов измерений, обоснование предложений по усовершенствованию и соответствующее информирование заинтересованных сторон
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс гарантии качества для системы	Обеспечение уверенности в том, что задаваемые требования к качеству системы будут выполнены	1) подготовка к выполнению процесса, включая: а) определение стратегии в обеспечении гарантии качества, в т.ч. распределение ролей, ответственности, подотчетности и полномочий, обеспечение действий применительно к каждому из процессов, к привлекаемым поставщикам, к процессам оценки и контроля, измерений, верификации, аттестации, к проведению инспекций и испытаний, определение количественных критериев оценки и принятия качества; б) обеспечение независимости в оценках качества; 2) выполнение количественных оценок качества; 3) документирование для обеспечения гарантии качества; 4) реагирование на инциденты и проблемы, включая: а) регистрацию, анализ и классификацию инцидентов и проблем, принятие соответствующих мер реагирования; б) выявление и анализ тенденций в инцидентах и проблемах; в) информирование заинтересованных сторон о состоянии, прогнозах и реагировании на инциденты и проблемы; г) отслеживание инцидентов и проблем до их полного разрешения
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс анализа бизнеса или назначения системы	Определение проблем бизнеса или назначения и выявление имеющихся возможностей, характеристика области потенциальных решений и определение потенциальных решений, которые помогут разрешить проблемы и/или обеспечить реализацию выявленных возможностей системы	1) подготовительные мероприятия, включая: а) анализ проблем, вызовов и возможностей в стратегии организации; б) определение стратегии анализа бизнеса или назначения системы, в т.ч. определение проблем, выявление потенциальных возможностей, характеристика области возможных решений и выбор классов решений; в) определение требований к обеспечивающим системам или услугам, получение или приобретение доступа к ним; 2) определение проблем, вызовов и возможностей, связанных с улучшением безопасности, снижением затрат, повышением эффективности, изменениями в регулированиях, изучением фактов неудовлетворенности заинтересованных сторон, а также политических, экономических, социальных, технологических, экологических и юридических факторов; 3) характеристика области возможных решений, включая определение базовых концепций функционирования (эксплуатации) и других концепций для всех стадий жизненного цикла системы, определение альтернативных классов возможных решений; 4) оценка альтернативных классов, включая оценку каждого альтернативного класса возможных решений и выбор предпочтительных альтернативных классов; 5) управление процессом, включая: а) поддержку двунаправленной прослеживаемости от возникающих проблем, вызовов и возможностей бизнеса или назначения системы, классов решений к организационной стратегии, потребностям и требованиям заинтересованных сторон, результатам системного анализа и достижимым эффектам; б) обеспечение документирования, сохранения и своевременной модификации процесса
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс определения потребностей и требований заинтересованной стороны	Определение требований к системе, выполнение которых должно обеспечить удовлетворение потребностей заинтересованных сторон в заданной среде применения системы	1) подготовительные действия, включая: а) определение заинтересованных сторон, имеющих законный интерес к системе в течение ее жизненного цикла; б) определение стратегии выполнения процесса; в) анализ необходимости применения обеспечивающих систем или услуг для процесса, планирование их приобретения и применения; г) получение или приобретение доступа к обеспечивающим системам или услугам (при необходимости); 2) определение потребностей заинтересованных сторон: а) определение контекста использования системы; б) выявление явных и подразумеваемых потребностей; в) распределение выявленных потребностей по приоритетам; г) определение потребностей заинтересованных сторон и их обоснование, ориентированное на достижение целей системы; 3) разработка концепции функционирования (эксплуатации) и других концепций жизненного цикла системы; 4) преобразование потребностей заинтересованных сторон в конкретные формализованные требования, включая: а) требования к критичным характеристикам, в т.ч. по гарантиям безопасности; б) требования, связанные со сценариями, требующими выполнения функций, обеспечения необходимого взаимодействия, ориентации на ограничительные условия и критичные характеристики качества, безопасности и эффективности системы; в) ограничения для системных решений; 5) анализ потребностей и формализованных требований заинтересованных сторон, включая: а) определение критичных показателей функционирования; б) доведение результатов анализа до заинтересованных сторон; в) разрешение проблем в тех случаях, когда обнаружены нарушения в формулировании требований; 6) управление процессом определения потребностей и требований заинтересованных сторон, включая: а) документирование соглашения в части учета потребностей и требований заинтересованных сторон; б) обеспечение прослеживаемости потребностей и требований заинтересованных сторон, подлежащих учету в системных требованиях; в) поддержание основных информационных активов, связанных с реализацией рассматриваемого процесса
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс определения системных требований	Преобразование ориентированного на пользователей представления заинтересованных сторон о возможностях системы в требования для такого технического предоставления решения, которое удовлетворит эксплуатационным потребностям пользователей и возможностям разработчика по реализации этих решений	1) определение заинтересованных сторон, имеющих законный интерес к системе в течение ее жизненного цикла, определение потребностей и требований заинтересованных сторон, представляющих начальные неформальные посылки для технических решений (замысел новой системы, модернизация или развитие существующей системы); 2) определение контекста использования системы, требований и порядка взаимодействия с другими системами, необходимыми для обеспечения установленных потребностей и требований заинтересованных сторон; 3) разработку концепции функционирования (эксплуатации) системы и других концепций жизненного цикла системы; 4) преобразование потребностей и требований заинтересованных сторон в конкретные системные требования, включая: требования к критичным характеристикам; требования, связанные с понятиями жизненного цикла системы, сценариями, взаимодействиями, ограничениями и критичными характеристиками качества и эффективности функционирования системы; требования по ограничению принимаемых системных решений; 5) анализ потребностей и требований заинтересованных сторон, включая обеспечение обратной связи для получения гарантии того, что их потребности, требования и ожидания правильно интерпретированы и выражены в системных требованиях; 6) поддержание основных информационных активов, создаваемых в рамках процесса; 7) формирование ТЗ на выполнение определенных работ

Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс определения архитектуры системы	Подготовка возможных вариантов архитектуры системы, выбор из этих вариантов приемлемого варианта (одного или нескольких, если это необходимо), который структурирует интересы заинтересованных сторон, отвечает системным требованиям и выражает во множестве согласованных представлений различные точки зрения на систему	1) подготовительные действия, включая: анализ необходимой информации (исследования рынка, промышленных проектов, планов и намерений конкурентов, научных результатов, организационной политики и директив, нормативных и юридических ограничений, функциональной концепции и эксплуатационной среды системы); уточнение требований заинтересованных сторон, связанных с архитектурой, таких как требования к функционированию (например, надежности, безопасности, эффективности), сопровождению, развитию системы и окружающей среды, производству; выработку подходов к разработке и стратегии модернизации и развития архитектуры системы; определение критериев оценки вариантов архитектуры, основанных на учете интересов заинтересованных сторон и основных системных требований; определение требований и взаимодействий для обеспечивающих систем или услуг, получение доступа к обеспечивающим системам; 2) разработка описаний для вариантов архитектуры и/или разработку действующих моделей (и/или прототипов) архитектуры системы включая: выбор, приспосабливание или разработку точек зрения на архитектуру и необходимых моделей; определение потенциальной структуры архитектуры, которая будет использоваться в разрабатываемых моделях и архитектурных представлениях; выбор или разработку методик и инструментариев для поддержания моделирования; выбор, приспосабливание или разработку моделей и представлений для архитектурных вариантов; согласование моделей архитектуры; 3) оценку вариантов архитектуры, включая оценку каждого варианта применительно к ограничениям и требованиям; выбор и обоснование предпочтительного варианта; 4) управление выбранной архитектурой, включая официальное согласование архитектуры с заинтересованными сторонами, поддержание соответствия и полноты характеристик; 5) поддержание стратегии определения и оценки архитектуры
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс определения проекта	Определение характеристик системы, ее элементов и их взаимодействия между собой и с внешним окружением на детальном уровне, достаточном для выполнения процессов реализации и комплексирования системы и обеспечивающим соблюдение предъявляемых требований и согласованность с принятой архитектурой	1) подготовительные мероприятия, включая: а) определение технологий, использование которых потребуется для каждого системного элемента; б) определение необходимых показателей проекта; в) определение принципов и основных положений по развитию проекта; г) определение требований и взаимодействий для обеспечивающих систем или услуг, получение или приобретение доступа к ним; 2) определение характеристик проекта и средств реализации для каждого системного элемента, включая: распределение системных требований по системным элементам, а) определение необходимых инструментов проектирования; преобразование системных требований и архитектурных характеристик в характеристики проекта; оценку достижимости характеристик проекта; уточнение или определение взаимодействия системных элементов между собой и с внешним окружением; разработку составных компонентов проекта; 3) оценка альтернатив для получения готовых системных элементов; 4) управление проектом, включая: установление и поддержку двунаправленной прослеживаемости между детальными характеристиками проекта, системными требованиями и объектами архитектуры системы; целенаправленное системное обоснование реализуемости и эффективности основных положений проекта
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс системного анализа	Удовлетворение аналитических потребностей заинтересованных сторон в поддержке принятия актуальных решений в течении жизненного цикла создаваемой (модернизируемой) системы	1) подготовку к проведению системного анализа, включая: а) определение вопросов, требующих системного анализа, и сторон, заинтересованных в проведении системного анализа относительно понимания функциональных возможностей системы, результативности и контроля состояния эксплуатационной среды, прогнозирования рисков, выявления явных и скрытых угроз, оценки и обоснования стратегий, технического облика и сбалансированных системных решений и планов, сравнения альтернатив, выработки критериев и осуществления прогноза безопасности, качества и эффективности системы для задаваемых условий, выработки требований к характеристикам системы, оценки свойств и критичности влияния различных параметров на поведение системы, определения допустимых рисков, разрешения противоречий, рациональной настройки параметров и поддержания устойчивости функционирования системы; б) формулирование целей системного анализа, установление их связи с удовлетворением аналитических потребностей заинтересованных сторон в поддержке принятия решений в жизненном цикле создаваемой (модернизируемой) системы или системы, выводимой из эксплуатации; в) определение области исследований, обоснование условий, предположений и допущений для обеспечения адекватности проводимого системного анализа; г) определение и согласование стратегии системного анализа, в т.ч. установление критериев и логических правил интерпретации получаемых результатов; д) выбор из существующих или разработку специальных методов, моделей и методик, применимых для системного анализа; е) определение и планирование действий, в т.ч. относительно необходимых обеспечивающих систем или услуг; ж) сбор исходных данных, их систематизацию и подготовку в виде, пригодном для применения; 2) непосредственно проведение системного анализа, включая: а) применение выбранных или специально разработанных методов, моделей и методик для разрешения выявленных проблем; б) анализ получаемых результатов системного анализа на предмет их непротиворечивости и согласованности; в) логическая интерпретация получаемых результатов и их рассмотрение с точки зрения решения задач системной инженерии и поддержки принятия решений; г) формулирование выводов, заключений и рекомендаций по результатам системного анализа; д) документирование результатов системного анализа, доведение их до заинтересованных сторон для принятия решений; 3) управление системным анализом, включая: а) поддержку двунаправленной прослеживаемости между результатами и анализируемыми сущностями системы, что должно позволять прослеживание логики в обоснованиях и/или принимаемых решениях; б) сопровождение результатов системного анализа в жизненном цикле системы для рационального решения актуальных задач системной инженерии
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс реализации системы	Создание системных элементов, заданных по результатам выполнения процессов определения потребностей и требований заинтересованных сторон, системных требований, определения архитектуры и проекта системы	1) подготовительные мероприятия, включая: а) определение стратегии реализации системы; б) определение текущих или предполагаемых ограничений выбранной технологии реализации системы, материалов, а также ограничений обеспечивающих систем; в) получение или приобретение доступа к обеспечивающим системам, услугам и материалам, которые предполагается использовать в процессе реализации системы; 2) реализацию системы (системных элементов), включая: а) создание, закупку или адаптацию системных элементов согласно технологическим процедурам; б) комплектование и хранение системных элементов; в) регистрацию данных, подтверждающих соответствие результатов реализации системным требованиям; 3) управление результатами реализации системы (системных элементов), включая: а) документирование результатов реализации и любых обнаруженных отклонений; б) установление и поддержку двунаправленной прослеживаемости между реализованными системными элементами и архитектурой, проектом и системными требованиями; в) обеспечение сохранности и своевременной модификации основных информационных объектов процесса
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс комплексирования системы	Создание единой системы из множества системных элементов, обеспечение взаимодействий между системными элементами и интеграция рассматриваемой системы с взаимодействующими системами	1) подготовительные мероприятия, включая: а) определение стратегии комплексирования системы; б) определение точек, в которых будет производиться контроль целостности комплексируемых конфигураций системы, взаимодействий системных элементов и корректности выполнения конкретных функций; в) определение требований к обеспечивающим системам или услугам, которые предполагается использовать в процессе комплексирования системы, получение или приобретение доступа к ним; 2) осуществление комплексирования системы, включая: а) получение в согласованные сроки реализованных системных элементов; б) сборку реализованных системных элементов до уровня комплексируемой системы; в) проверку взаимодействий, выполнения требований к функциям и критичным характеристикам качества и безопасности; 3) управление результатами комплексирования системы, включая: а) документирование результатов комплексирования системы и любых обнаруженных отклонений; б) поддержку прослеживаемости между комплексируемыми системными элементами, а также между ними и стратегией, архитектурой системы, проектом и системными требованиями; в) обеспечение сохранности и своевременной модификации основных информационных объектов процесса
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс верификации системы	Предоставление объективных доказательств того, что системный элемент или система удовлетворяет заданным требованиям и обладает заданными характеристиками	1) подготовительные действия: а) определение области верификации и соответствующих действий; б) определение ограничений; в) выбор или разработка методов и методик верификации, определение условий и критериев для каждого действия с учетом специфики системы, целей проекта и допустимых рисков; г) определение стратегии верификации, включая определение соотношения между областью верификации, ограничениями и методами выполнения действий верификации с привлечением обеспечивающих систем, моделей, испытательных стендов, тренажеров, компетентного персонала, вспомогательных услуг для подтверждения того, что системный элемент или система были «построены правильно» (минимизируя стоимость, сроки и/или риски при верификации); д) определение ограничений, вытекающих из стратегии верификации системы (в т.ч. ограничения, связанные с методами и точностью измерений, неопределенностью, воспроизводимостью, пригодностью, доступностью и взаимодействиями); е) получение или приобретение доступа к обеспечивающим системам или вспомогательным услугам; 2) непосредственно проведение верификации, включая: а) выполнение верификации в среде, близкой к эксплуатационной или ее виртуальному представлению; б) документирование результатов верификации и выявленных отклонений; в) регистрацию эксплуатационных инцидентов, выявленных проблем и предложений по их разрешению; г) обеспечение прослеживаемости в архитектуре системы, проекте и системных требованиях
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс передачи системы	Предоставление поставщиком приобретающей стороне полностью скомплексированной и верифицированной системы, готовой к функционированию в заданной эксплуатационной среде согласно требованиям заинтересованных сторон	1) подготовительные мероприятия, включая: а) определение стратегии передачи; б) определение потребности в изменении основных средств или участка местоположения системы; в) определение методики и плана предварительных и приемочных испытаний системы; г) организацию обучения операторов, пользователей и заинтересованных сторон; д) определение требований к обеспечивающим системам или услугам, получение доступа к ним; е) подготовку к отгрузке и получению системных элементов и обеспечивающих систем; 2) непосредственно передачу системы, включая: подготовку участка местоположения для эксплуатации системы; отгрузку и получение системных элементов и обеспечивающих систем; установку системы в ее эксплуатационном местоположении, демонстрацию соответствия установки системы предъявляемым требованиям; обучение операторов, пользователей и других заинтересованных сторон; приведение системы в эксплуатационное состояние и оценку готовности системы; демонстрацию функционирования системы и устойчивости выполнения функций, анализ результатов; принятие системы в эксплуатацию; 3) управление результатами передачи, включая: регистрацию результатов передачи и любых обнаруженных отклонений; регистрацию инцидентов и проблем, возникающих при эксплуатации; поддержку прослеживаемости между системными элементами, стратегией передачи, архитектурой системы, проектом и системными требованиями; обеспечение сохранности и своевременной модификации основных информационных объектов процесса
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс аттестации (валидации) системы	Предоставление объективных доказательств того, что при применении в заданной эксплуатационной среде система обеспечит выполнение заданных требований заинтересованных сторон	1) подготовительные действия: определение области аттестации; определение ограничений; выбор или разработку соответствующих методов и методик, определение условий и критериев для каждого действия процесса аттестации с учетом специфики системы, целей проекта и допустимых рисков; определение стратегии аттестации; определение ограничений системы, вытекающих из стратегии аттестации; определение и планирование действий относительно обеспечивающих систем или вспомогательных услуг; 2) проведение непосредственно аттестации, включая: выполнение процедуры аттестации согласно принятой стратегии в среде, близкой к эксплуатационной среде или ее виртуальному представлению с определенными обеспечивающими системами и ресурсами; рассмотрение результатов аттестации с целью подтверждения функциональной готовности системы; документирование результатов аттестации и выявленных отклонений; регистрацию эксплуатационных инцидентов, выявленных проблем и гарантий того, что они практически разрешаемы; обеспечение прослеживаемости системных элементов, прошедших аттестацию, и стратегии аттестации, архитектуры системы, проекта и системных требований
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс функционирования системы	Применение системы по назначению	1) подготовительные действия: определение стратегии эксплуатации системы, включая определение критериев и методов обеспечения качества производимой продукции и/или услуг, способов организации приемлемого функционирования и реагирования на отклонения, методов защиты окружающей среды, технологий обеспечения устойчивости и безопасности функционирования системы; определение ограничений в применении системы; определение и планирование действий относительно необходимых обеспечивающих систем, услуг и материалов, необходимых для поддержки функционирования рассматриваемой системы, и обеспечение доступа к ним; определение требований к квалификации и обучению персонала, прием на работу и возложение обязанностей на обученных и компетентных операторов рассматриваемой и обеспечивающих систем; 2) действия по обеспечению функционирования и управлению процессом, включая: применение системы по ее целевому назначению в заданных условиях эксплуатации согласно требованиям заинтересованных сторон; применение материалов и иных ресурсов, необходимых для производства продукции и/или оказания услуг системой, для управления системой и поддержки процесса; контроль функционирования системы, включая поддержку стратегии эксплуатации системы, сравнительное сопоставление затрат и ущербов с целями и ограничениями; регистрацию эксплуатационных инцидентов, случаев отклонений от приемлемого функционирования системы, выявление проблем в обеспечении приемлемого функционирования, реагирование на инциденты и отклонения и восстановление приемлемого функционирования системы; анализ данных по инцидентам, выявленным проблемам и отклонениям от приемлемого функционирования системы для определения их первопричин, прогнозирования рисков и принятия упреждающих мер по обеспечению безопасности и улучшению процесса функционирования системы; поддерживание двунаправленной прослеживаемости возможностей системных элементов, участвующих в процессе функционирования системы, относительно системных требований и требований заинтересованных сторон; 3) действия по поддержке конкретных заинтересованных сторон, включая обеспечение им помощи и консультаций и определение степени их удовлетворенности
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		
Процесс сопровождения системы	Поддержание функционирования системы в соответствии с ее назначением и предъявляемыми системными требованиями	1) подготовительные мероприятия: определение стратегии сопровождения системы; подготовка планов сопровождения, материально-технического обеспечения и поддержания жизненного цикла; определение ограничений системы, следующих из потребностей ее сопровождения; получение или приобретение доступа к обеспечивающим системам и системным элементам, необходимым по жизненному цикл, к запасным частям, услугам и материалам, предполагаемым к использованию в процессе сопровождения системы; 2) выполнение необходимых действий по сопровождению, включая: регистрацию и анализ возникающих инцидентов, сбоев и отказов с целью устранения негативных последствий, а также их анализ и планирование необходимых упреждающих действий по их предотвращению; выполнение регламентных процедур по устранению сбоев и/или замене системных элементов и восстановлению системы до уровня ее эксплуатационного состояния или запасного (резервного) режима эксплуатации; выполнение процедур упреждающего сопровождения, обеспечивая замену или обслуживание системных элементов согласно плановым срокам (т.е. до наступления отказа); идентификацию отказов при выявлении несоответствий в функционировании системы; отслеживание моментов, когда требуется модификация (адаптация) или усовершенствование системы; приобретение, обучение и аттестацию персонала для обеспечения и поддержания достаточного числа операторов системы (по мере необходимости); 3) обеспечение интегрированной логистической поддержки процесса сопровождения системы, включая: анализ эффективности по затратам (результаты которого могут повлиять на начальный проект системы или планирование запасных частей и регламентное обслуживание в период эксплуатации, а также потребовать управления цепочками поставок); необходимые действия для того, чтобы требуемые ресурсы были доступны в нужном месте и в нужное время; комплектование, обработку, хранение и транспортировку системных элементов и запасных частей, необходимых по жизненному циклу системы; постоянный контроль за тем, чтобы планируемые действия логистики отвечали требованиям процесса сопровождения системы, были реализуемы и поддержаны ресурсами, в т.ч. обученным персоналом; 4) управление результатами сопровождения, включая: регистрацию и анализ результатов сопровождения и логистики, отклонений от штатного исполнения, сбоев, отказов, инцидентов и проблем, возникающих во время эксплуатации, выработку мер реакции на отклонения; определение тенденций в возникновении сбоев, отказов, инцидентов, проблем и отклонений в действиях логистики и сопровождения; поддержку прослеживаемости между действиями по сопровождению, системными элементами и артефактами системы; обеспечение сохранности и своевременной модификации основных информационных объектов процесса; контроль удовлетворенности заинтересованных сторон функционированием и обеспечением сопровождения системы; подготовку отчетов о результатах сопровождения
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Процесс изъятия и списания системы	Цель - должным образом завершить существование системы (подсистемы или системного элемента)	1) определение стратегии процесса изъятия и списания системы, в которой учитывают вопросы остановки эксплуатации, обеспечения безопасности системы и защищенности информации, возможность дальнейшего их использования; 2) определение и планирование действий относительно необходимых обеспечивающих систем или услуг, получение доступа к обеспечивающим системам или услугам; 3) определение основных средства, мест хранения, критериев для проведения инспекции и сроков хранения, если система подлежит хранению; 4) определение упреждающих методов для предотвращения повторного применения в цепочках поставок тех элементов и материалов, которые не следует предлагать вновь, повторно востребовать или использовать после завершения процесса; 5) завершение функционирования системы для подготовки к выведению из эксплуатации, непосредственно выведение системы из эксплуатации; 6) перераспределение, переустройство или увольнение операторов системы и регистрацию соответствующих знаний по эксплуатации системы, обеспечение охраны и защиты знаний и навыков операторов; 7) разборку системы до уровня управляемых частей с тем, чтобы облегчить их изъятие для повторного использования, переработки, ремонта, перестройки, разрушения или архивирования; 8) разборку системных элементов и их частей, которые не предназначены для повторного использования, способом, который подтвердит, что они не возвращаются в цепочки поставок; 9) проведение (по мере необходимости) разрушения системных элементов таким образом, чтобы уменьшить затраты на выполнение работ или облегчить процесс изъятия и списания системы; 10) подтверждение того, что в результате процесса изъятия и списания системы отсутствуют факторы, наносящие вред здоровью, безопасности, защищенности информации и экологии; 11) архивирование информации, собранной в течение жизненного цикла системы для разрешения возможных конфликтов в случаях опасности здоровью, безопасности, защищенности информации и окружающей среды; 12) сохранения знаний, базирующихся на накопленном опыте
Результат анализа: по возможности необходимо упреждающее управление соответствующими рисками при выполнении процесса с учетом задаваемых требований		

Таким образом, в результате проведенного анализа установлено: по возможности необходимо упреждающее управление соответствующими рисками с учетом задаваемых требований при выполнении всех стандартизованных процессов:

процессов соглашения – приобретения и поставки продукции и услуг;

процессов организационного обеспечения проекта – управления моделью жизненного цикла, инфраструктурой, портфелем проектов, человеческими ресурсами, качеством, знаниями;

процессов технического управления – планирования проекта, оценки и контроля проекта, управления решениями, рисками, конфигурацией, информацией, измерений, гарантии качества;

технических процессов – анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы.

Вместе с тем в существующей концепции управления рисками выявлены следующие недостатки, сдерживающие эффективное решение задач системной инженерии (см. рис. 1.5), а именно [5, 167]:

- не осуществляется целенаправленной обработки информации для системного обоснования рациональных мер противодействия угрозам;

- используемые методы расчета рисков специфичны, результаты несравнимы;

- для разнородных угроз задачи количественного обоснования требований к стандартным процессам при ограничениях на ресурсы и допустимые риски – не решаются.

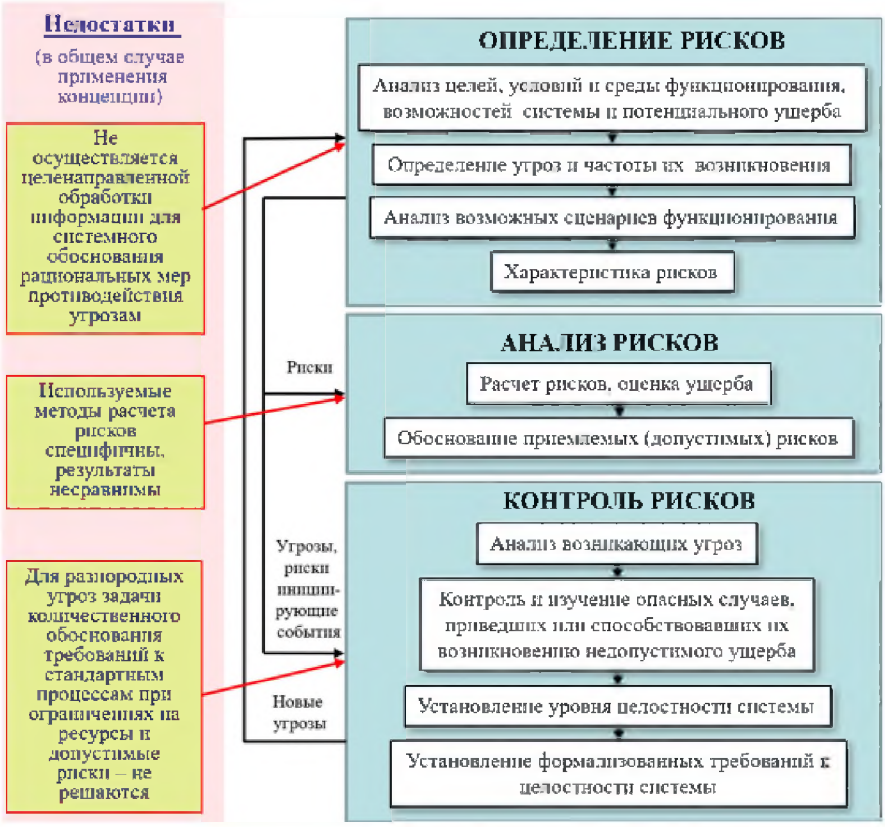


Рис. 1.5 Выявленные недостатки в существующей концепции управления рисками, сдерживающие эффективное решение задач системной инженерии

Для устранения этих недостатков требуется принципиальное развитие программно-технологической поддержки риск-ориентированной системной инженерии для решения практических задач, позволяющее усовершенствование существующих вероятностных моделей и генерацию новых моделей, адаптируемых к сложным системам различной логической структуры в различных областях функционального приложения систем. Для этого необходимо создание и внедрение широко применимых программных, технологических и методических решений для упреждающего управления рисками.

1.3 Разработка принципов создания и внедрения программных, технологических и методических решений, широко применимых для упреждающего управления рисками с использованием вычислительных систем и компьютерных сетей

Упреждающее управление рисками при решении практических задач в приложениях системной инженерии базируется на:

- формулировании непротиворечивых целей в жизненном цикле системы;

- математически корректных постановках задач, ориентированных на научно обоснованное достижение сформулированных целей применительно к рассматриваемым процессам, системе, проекту;

- выборе и/или разработке основных и вспомогательных показателей для всесторонних оценок и прогнозов;

- определении способов формализации, выборе и/или разработке формализованных моделей, методов и критериев;

- использовании результатов системного анализа для принятия решений.

В условиях неопределенностей для количественного прогнозирования рисков и обоснования эффективных упреждающих мер по снижению этих рисков или их удержанию в допустимых пределах широко применяются вероятностные методы и модели. В этом – их научно – практическая значимость [2, 5, 167].

Основными решаемыми аналитическими задачами при этом являются [2, 4, 5, 136, 149, 167, 167]:

- прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы, интерпретация и анализ приемлемости получаемых результатов, включая сравнение с допустимыми рисками;

- определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество и/или безопасность и/или эффективность рассматриваемой системы;

- определение и обоснование в жизненном цикле системы упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства качества и/или безопасности и/или эффективности рассматриваемой системы при задаваемых ограничениях в задаваемый период прогноза.

Применение вероятностных методов и моделей с использованием ВС и КС позволяет построить функцию распределения (ФР) времени до нарушения целостности системы и целостности ее критичных элементов или иную аналогичную по аналитической сути функциональную зависимость (ФР – основное понятие теории вероятностей и ее

приложений). Под целостностью моделируемой системы понимается такое ее состояние, которое отвечает целевому назначению модели системы в течение задаваемого периода прогноза. При этом понятие «нарушения целостности» применительно к конкретной анализируемой системе должно быть определено в терминах учитываемых показателей с учетом необходимой специфики системы [2, 4, 5, 20, 27, 29-33, 37, 167, 167] и др.

На рис. 1.6 проиллюстрированы ограничения к допустимым рискам, экспоненциальная и некая более адекватная ФР времени между соседними нарушениями системной целостности с одинаковой частотой нарушений λ (вместо ФР может быть использована функция, аппроксимирующая ФР – например, функция, построенная по методам ГОСТ Р 59341) [2, 5, 37, 167, 167].

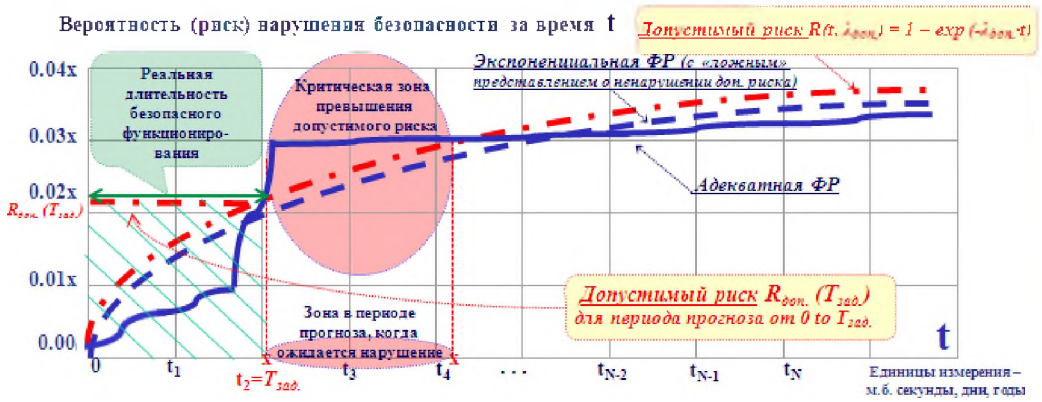


Рис. 1.6 Фрагменты ФР, демонстрирующие экспоненциальную и более адекватную аппроксимацию

Какие скрытые знания могут быть выявлены при таком вероятностном прогнозировании рисков? Ориентируясь на простейшую, весьма грубую, аппроксимацию экспоненциальной ФР (с одним параметром – частотой нарушений), можно сравнительно легко констатировать выполнение или невыполнение задаваемых требований к уровню допустимых рисков. Ниже «пограничной полосы» (пунктирной с точками) - требование выполнено, выше – не выполнено. Однако на этом извлекаемые знания исчерпываются… Из «плюсов» - лишь удобство сравнения. И все… Ориентируясь на построенную ФР, учитывающую характеристики угроз, функции контроля и восстановления приемлемого состояния после нарушений или обнаружения признаков возможных нарушений, например, с помощью предлагаемых моделей [2, 5, 37, 167, 167], возможно извлечение изначально скрытых знаний, позволяющих (см. рис. 1.6):

- рассчитать реальную зависимость вероятности нарушения критичных условий (например, нарушения допустимого качества, безопасности или эффективности) системы и

составных подсистем от характеристик разнородных угроз и предпринимаемых мер противодействия угрозам;

- оценить точность прогнозирования по сравнению с упрощенной экспоненциальной аппроксимацией ФР, учитывающей лишь частоту нарушений;

- определить период эффективного функционирования, в течение которого нарушений критичных условий не ожидается (по критерию непревышения допустимых рисков) – для определения упреждающих противодействий угрозам за время, не превосходящее данного периода;

- выделить зоны прогнозных периодов времени, когда возможны нарушения требований допустимого риска – для определения упреждающих противодействий угрозам или обоснованное уточнение риска для этих зон (в т.ч. избегание рисков или смягчение требований из-за неизбежного резкого возрастания рисков в пределах, признанных приемлемыми);

- сравнить периоды эффективного функционирования, в течение которого нарушений критичных условий для системы не ожидается (по критерию непревышения допустимых рисков) с соответствующими периодами при экспоненциальной аппроксимации ФР.

Кроме того, оказывается возможным извлечение дополнительных знаний – см., например [5, 167 - 167]:

- расчет средней наработки на нарушение целостности (качества, безопасности или эффективности), как обратную к ней величину - частоту нарушений целостности (качества, безопасности или эффективности) системы и составных элементов в условиях задаваемых разнородных угроз и предпринимаемых мер противодействия угрозам;

- сравнение средней наработки на нарушение целостности (качества, безопасности или эффективности) или частоты нарушений целостности системы со средней наработкой или частотой нарушений целостности при упрощенной экспоненциальной аппроксимации ФР.

Кроме этого, зафиксировав уровни «допустимых рисков» для системы и составных подсистем, а также считая неизменными все параметры, за исключением одного, возможно решение различных оптимизационных задач, связанных с обоснованием эффективных упреждающих мер обеспечения целостности моделируемой системы в условиях разнородных угроз. Тем самым с использованием ВС и КС применительно к моделируемой системе в принятых допущениях и ограничениях для условий неопределенности способы противодействия угрозам могут быть формализованы в масштабе времени, близком к реальному.

Построение и оперирование более адекватной ФР или аналогичной вероятностной зависимостью позволяет выявить и познать какие-либо закономерности в ожидаемом

поведении систем в условиях неопределенностей и выработать логичные решения. Именно поэтому использование вероятностных подходов является актуальным для прогнозирования рисков и обоснования эффективных упреждающих мер по снижению этих рисков или их удержанию в допустимых пределах (в дополнение к измерениям специальных показателей, связанных с различными критичными сущностями системы).

Изложенные выше аналитические возможности на уровне адекватной ФР могут быть эффективно использованы при корректном выборе показателей, методов и моделей, которые позволяют спрогнозировать представление о возможных причинах возникновения недопустимых рисков:

- на уровне целевых аналитических потребностей (применительно к процессам, элементам, подсистемам и системе в целом);

- на уровнях отдельного процесса и интеграции различных процессов (используемых применительно к элементам, подсистемам и системе в целом);

- на уровне расчетных показателей частного и интегрального рисков при создании и эксплуатации систем различного назначения.

Выявляемые скрытые знания при вероятностном прогнозировании рисков подлежат использованию для решения многогранных аналитических задач (в т.ч. анализа рисков, обоснования требований и оптимизации) и достижения на этой основе прагматических эффектов в жизненном цикле систем – см. рис. 1.7 [5, 167, 167].

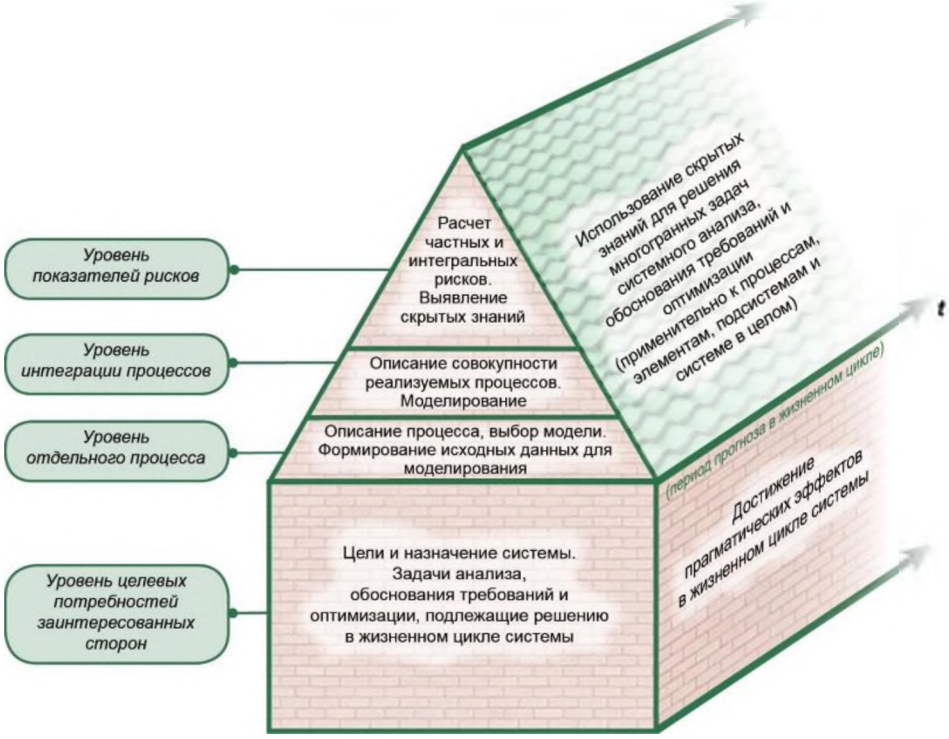


Рис. 1.7 Использование скрытых знаний при вероятностном прогнозировании рисков для достижения прагматических эффектов в жизненном цикле систем

Учитывая приведенные выше аргументы, при создании и внедрении программных, технологических и методических решений, широко применимых для упреждающего управления рисками с использованием ВС и КС предлагается руководствоваться следующими основными принципами:

- принципом системности, предполагающим наличие целеполагания и связанности в реализации системных процессов жизненного цикла в условиях создания, модернизации, развития, эксплуатации системы и выведения ее из эксплуатации;

- принципом сбалансированности эффектов в пределах допустимых рисков в условиях неопределенностей, возможных угроз и объективных ограничений для системы;

- принципом эффективного управления рисками, предполагающим оправданность деятельности по управлению рисками с учетом социально-экономических факторов (практическая деятельность по управлению рисками не может быть оправдана, если выгода от этой деятельности в целом не превышает вызываемого ею ущерба);

- прецедентным принципом для обоснования допустимых рисков в случае его предпочтительности в сравнении с ориентацией на систему-эталон или проект-эталон;

- принципом непревышения предельно допустимых экологических нагрузок на системы (чтобы обеспечение безопасности человека, живущего сегодня, достигалось путем реализации таких решений, которые сохранили бы способность природы обеспечить безопасность и потребности будущих поколений).

Все применяемые принципы при упреждающем управлении рисками в приложениях системной инженерии должны быть согласованы с принципом целенаправленности осуществляемых действий.

На сегодня разработка универсальных инструментариев, позволяющих оперативно спрогнозировать разнородные риски по единой вероятностной шкале для различных процессов и систем, аналитически обосновать эффективные меры противодействия угрозам, максимизировать выигрыш и минимизировать возможные ущербы находится на самой начальной стадии формирования отдаленных прототипов. Масштабное внедрение риск-ориентированного подхода в решения задач системной инженерии на основе сформулированных выше принципов немыслимо без целенаправленного решения научной проблемы разработки широко применимых программных, технологических и методических решений для ВС и КС, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии.

Для более детальной постановки научной проблемы необходимо предварительное определение требований к формализованным методам риск-ориентированного подхода с использованием ВС и КС.

1.4 Определение требований к формализованным методам риск-ориентированного подхода

Предлагаемые ниже требования к формализованным методам риск-ориентированного подхода применимы ко всем стандартизованным процессам, используемым в жизненном цикле систем (процессам соглашений, организационного обеспечения проекта, технического управления, техническим процессам) и ориентированы на формализованное использование ВС и КС с учетом рекомендаций ГОСТ Р 59991-2022 по системному анализу при управлении рисками [2, 5, 37, 136, 149, 167, 167].

Требования формализованным методам риск-ориентированного подхода включают:

- требования к моделям и методам оценки специальных показателей и обоснования их допустимых значений;
- требования к моделям и методам прогнозирования рисков и обоснования допустимых рисков;
- требования к методам определения существенных угроз и условий;
- требования к методам поддержки принятия решений в жизненном цикле систем.

Требования к моделям и методам оценки специальных показателей предполагают, что используемые модели и методы должны быть функционально связаны с целями рассматриваемой системы, ее масштабами, имеющими место вызовами и возможными угрозами. В качестве исходных используются данные, получаемые по факту (например, в процессе функционирования системы) и гипотетичные данные (например, в сравнении с системами-аналогами). В общем случае с использованием расчетных специальных показателей применение моделей и методов должно способствовать рациональному решению задач системной инженерии.

Выбираемые и/или разрабатываемые модели и методы прогнозирования рисков должны обеспечивать достижение сформулированных целей системного анализа для условий неопределенности и практичное решение задач, поставленных для достижения этих целей.

Прогнозирование рисков используется для формального решения задач системного анализа, связанных с ранним распознаванием и оценкой развития предпосылок к нарушению качества, безопасности и/или эффективности системы, обоснованием эффективных предупреждающих мер по снижению рисков или удержанию рисков в

допустимых пределах, определением существенных угроз, поддержкой принятия решений в приложениях системной инженерии. В зависимости от целей решаемых задач прогнозируемый риск связывают с заранее определенным периодом прогноза (например, на месяц, год, на несколько лет), с возможными сценариями возникновения и развития угроз, ожидаемых для этого периода.

Для прогнозирования рисков при решении поставленных задач системной инженерии должны быть:

- определены потенциально существенные угрозы или условия, для которых при том или ином развитии событий возможно негативное воздействие на свойства рассматриваемых системных процессов, системы (и/или ее элементов) и/или проекта;

- определены количественные показатели прогнозируемых рисков, выбраны, адаптированы или разработаны модели и методы прогнозирования рисков, способы снижения рисков и методики системного анализа;

- реализованы сбор и обработка исходных данных, обеспечивающих применение моделей, методов и методик системного анализа;

- предусмотрены способы использования результатов прогнозирования рисков в интересах эффективного решения задач системной инженерии.

При выполнении системных процессов, обеспечении качества, безопасности и эффективности рассматриваемой системы допустимые риски выступают в качестве количественных норм эффективности мер противодействия угрозам. Значения допустимых рисков определяют применительно к риску нарушения надежности реализации рассматриваемого процесса как такового, риску нарушения реализации процесса с учетом дополнительных специфических системных требований, а также интегральным рискам нарушения качества, безопасности и эффективности системы в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза.

Методы обоснования допустимых рисков должны быть определены до начала планирования и реализации рассматриваемого процесса. Допустимые риски по возможности должны быть установлены в количественной форме с учетом специфики системы по прецедентному принципу или с использованием ориентации на риски, свойственные системе-эталону, которая выбирается в качестве аналога для моделируемой системы.

Методы количественного обоснования допустимых рисков по прецедентному принципу должны предусматривать формирование статистики по состоявшимся фактам. В результате моделирования применительно к условиям различных произошедших событий формируется база знаний, устанавливающая соответствие расчетных значений

прогнозируемых рисков тем реальным событиям, которые состоялись и оказались свойственными этим ситуациям. Соответствие устанавливают по журналам регистрации нарушений (качества, безопасности и/или эффективности системы), регистрации случаев нарушения реализации рассматриваемого процесса. Учитывается собираемая статистика, из нее выбираются прецеденты нарушений. Для задаваемого периода прогноза расчетные значения рисков, свойственные состоявшимся нарушениям, определяются как недопустимые, а меньшие по сравнению с недопустимыми определяют как допустимые. Альтернативным прецедентному принципу считается выбор допустимого риска при ориентации на систему-эталон (см., например, ГОСТ Р 59341-2021).

Методы определения существенных угроз и условий, способных при том или ином развитии событий негативно повлиять на рассматриваемый процесс, систему (и/или ее элементы) и/или проект, должны быть целенаправлены на раннее распознавание и оценку развития предпосылок к нарушению качества, безопасности и/или эффективности системы. Определение существенных угроз и условий выполняется по оценкам специальных показателей, связанных с критичными сущностями рассматриваемой системы, а также с использованием прогнозирования рисков [2, 5, 37, 136, 149, 167, 167].

Для определения существенных угроз и условий при отсутствии или недостаточности фактических данных, а также при необходимости учета различных неопределенностей на задаваемый период прогноза рассматриваемый процесс, система или соответствующий проект представляются в виде формализуемой моделируемой системы. Для выбранных показателей риска нарушения надежности реализации рассматриваемого процесса как такового, риска нарушения реализации процесса с учетом дополнительных специфических системных требований, интегральных рисков нарушения качества, безопасности и/или эффективности моделируемой системы устанавливаются допустимые уровни рисков с точки зрения их существенности (они могут выражаться с использованием расчетной вероятности нанесения ущерба с учетом тяжести этого ущерба).

В зависимости от решаемой задачи системного анализа для определения существенных угроз и условий применительно к моделируемой системе в задаваемый период прогноза могут быть использованы следующие критерии [2, 5, 37, 136, 149, 167, 167]:

- при задаваемых условиях угроза признается существенной, если для нее расчетное значения риска превышает установленное значение соответствующего допустимого риска (возможно определение существенности угрозы отдельно для каждого из рисков: риска нарушения надежности реализации рассматриваемого процесса как такового, риска нарушения реализации процесса с учетом дополнительных специфических системных

требований, а также интегральных рисков нарушения качества, безопасности и/или эффективности моделируемой системы, в том числе в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза);

- при полном перечне существенных угроз рассматриваемые условия признаются существенными (применительно к конкретной угрозе или когда само условие как таковое представляет собой угрозу), если для них расчетные значения интегральных рисков нарушения качества, безопасности или эффективности моделируемой системы превышают установленные значения допустимых рисков.

Непревышение допустимого риска интерпретируется как соблюдение условий по удержанию риска в допустимых пределах в течение периода прогноза или как несущественность рассматриваемых угроз и условий.

Если в приложении к моделируемой системе все расчетные риски не превышают установленных допустимых рисков, это означает, что результаты моделирования подтверждают удержание рисков в допустимых пределах, несущественность или отсутствие существенных угроз в течение всего периода прогноза. Если все расчетные риски превышают максимально допустимые, это означает высокую уязвимость моделируемой системы с точки зрения нарушения качества, безопасности и/или эффективности системы для установленных допустимых рисков.

Методы поддержки принятия решений в приложениях системной инженерии должны учитывать результаты прогнозирования рисков, обоснования допустимых рисков, обоснования эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах, определения существенных угроз и условий. Применение методов должно быть ориентировано:

- на обеспечение надежности реализации рассматриваемого процесса и обоснование мер для достижения его целей и целей системного анализа процесса;

- противодействие угрозам и определение сбалансированных решений системной инженерии при средне- и долгосрочном планировании;

- обоснование предложений по повышению качества, безопасности и/или эффективности системы и совершенствование системного анализа и методов решения задач системного анализа процесса управления рисками для системы.

Устанавливаемые при этом значения допустимых рисков играют роль ограничений для формального решения основных и вспомогательных задач системного анализа. В зависимости от целей решаемых задач допустимый риск связывают с заранее определенным периодом прогноза, используемыми сценариями возникновения и развития угроз, возможным ущербом, ожидаемым для этого периода прогноза, а также с условиями

возможных комбинаций используемых системных процессов в задаваемом периоде прогноза.

Поддержка принятия решений по обеспечению реализации различных процессов основана на мониторинге состояний и прогнозировании рисков. Это позволяет определять в жизненном цикле системы приемлемые для периода прогноза нормы эффективности мер противодействия угрозам и решать задачи по определению существенных угроз и условий.

Поддержка принятия решений по обоснованию мер, направленных на достижение целей рассматриваемого процесса и противодействие угрозам основана на предварительных действиях (см. подраздел 1.3). Следует заранее определить меры, направленные на обеспечение качества, безопасности и эффективности системы, определение существенных угроз и на восстановление приемлемых условий реализации рассматриваемого процесса в случае определения предпосылок к нарушению или непосредственно следов произошедших нарушений из-за реализации угроз. Причины наступления событий, связанных с выявленными предпосылками к нарушениям качества, безопасности и/или эффективности системы, существенными угрозами и условиями, произошедшими нарушениями в системных процессах, подлежат учету для недопущения подобных повторений и/или уточнения предупреждающих мер, обеспечения приемлемых условий реализации системных процессов и наполнения базы знаний [5, 136, 149, 167, 167].

Поддержка принятия сбалансированных решений системной инженерии при среднесрочном планировании основана на системном анализе значений расчетных показателей рисков с учетом специфики системы. При недопустимых значениях прогнозируемых рисков и/или при наступлении реальных нарушений в рассматриваемом системном процессе должны быть выявлены их причины и определены меры для целенаправленного планового восстановления надежности выполнения этого процесса на уровне рисков, не превышающих допустимые. При средне- и долгосрочном планировании должен быть обеспечен баланс по критерию «эффективность — стоимость». Для обоснования сбалансированных решений системной инженерии при средне- и долгосрочном планировании используются модели, методы и методики системного анализа и рекомендации по снижению рисков и определению допустимых значений показателей рисков. Для обоснования предложений по повышению качества, безопасности и/или эффективности системы и совершенствованию непосредственно самого системного анализа процесса управления рисками следует также использовать выявленные закономерности и обоснованные рекомендации по снижению рисков и определению допустимых значений показателей рисков [5, 136, 149, 167, 167].

Таким образом, в результате проведенного анализа в интересах совершенствования вероятностных моделей и создания программных, технологических и методических решений для использования ВС и КС сформулированы основные требования к формализованным методам риск-ориентированного подхода, включающие:

- требования к моделям и методам оценки специальных показателей и обоснования их допустимых значений;

- требования к моделям и методам прогнозирования рисков и обоснования допустимых рисков;

- требования к методам определения существенных угроз и условий;

- требования к методам поддержки принятия решений в жизненном цикле систем.

Сформулированные требования позволяют перейти к постановке научной проблемы.

1.5 Постановка научной проблемы

Для обеспечения эффективного решения задач системной инженерии при реализации национальных стратегий развития РФ (согласно результатам анализа в 1.1) и повышения готовности к изменениям современных систем (согласно тенденциям, выявленным в 1.1) в рамках постановки научной проблемы предлагается идея целенаправленной обработки информации об угрозах, возможных и реализуемых мерах контроля, мониторинга и восстановления нарушаемой целостности для управления процессами (см. 1.2) на основе упреждающего выявления «узких мест» и определения рациональных способов снижения и удержания рисков в допустимых пределах в жизненном цикле систем различного функционального назначения согласно сформулированным принципам (см. 1.3) и требованиям к формализованным методам риск-ориентированного подхода (см. 1.4).

Научная проблема ставится таким образом, чтобы предлагаемые новые научно обоснованные программные, технологические и методические решения для ВС и КС позволяли обеспечить в жизненном цикле систем [5, 167]:

- вероятностное прогнозирование соответствующих рисков и обоснование допустимых значений рисков;

- определение существенных угроз и условий по критериям сравнения соответствующих рисков;

- выработку научно обоснованных организационно-технических решений по управлению системными процессами;

- поддержку принятия аналитических и оптимизационных решений задач системной инженерии.

Примечание. Примерами возможного применения программных, технологических и методических решений для оптимизации рассматриваемых систем являются: обоснование параметров системных процессов, на которых достижим минимум затрат (на этапах создания) при ограничениях на допустимые риски или минимум интегрального риска (при эксплуатации системы) при задаваемых ограничениях.

Созданные программные, технологические и методические решения для ВС и КС должны представлять собой прототип интеллектуального инструментария системного аналитика, опирающегося на стандартизованные модели и применимого в жизненном цикле систем различного функционального назначения для решения практических задач системной инженерии. С его помощью новый порядок решения задач системной инженерии должен занимать считанные часы (вместо нынешних недель или использования грубых или субъективных оценок из-за длительности или отказов от адекватного решения с надеждой на авось). А с внедрением интеллектуальных помощников в виде систем искусственного интеллекта для определения исходных данных моделирования и анализа результатов моделирования, потребуются минуты.

На выходе решения поставленной научной проблемы – программные, технологические и методические решения для ВС и КС, включая прототип технологии поддержки риск-ориентированной системной инженерии (который и является неким прототипом инструментария системного аналитика), позволяющие на практике реализовывать риск-ориентированный подход для упреждающего управления рисками в приложениях системной инженерии. При использовании такой технологии поддержки риск-ориентированной системной инженерии системный аналитик будет оперировать цифровым образом системы в терминах прогнозных рисков. Отличие от существующих инструментариев разработки сложных систем – взгляд на 3 шага вперед, это - прогноз, рекомендации, обоснование.

Понятность вероятностного прогнозирования должна быть обеспечена выбором таких показателей рисков, которые позволяют получить практическую интерпретацию результатов математического моделирования (на уровне «вероятности успеха» и/или «риска неудачи») при изменении исходных данных, характеризующих угрозы и меры противодействия угрозам, процессы контроля, мониторинга и восстановления целостности систем, а также иных исходных данных (см. раздел 2).

Доступность к программным и технологическим решениям должна быть обеспечена с помощью технологии удаленного доступа через ВС и КС к функциональным возможностям и результатам моделирования (см. раздел 3).

Систематизация результатов моделирования должна достигаться исследованиями полученных результатов, оформленными в автоматическом режиме в виде аналитического отчета и предоставляемыми удаленному пользователю. При этом основные объекты

исследований определяются методическими решениями, предлагаемыми системному аналитику при использовании ВС и КС (см. раздел 4).

Работоспособность предлагаемых программных, технологических и методических решений для ВС и КС должна демонстрироваться разъясняемыми примерами практического решения задач системной инженерии на базе созданного прототипа технологии поддержки риск-ориентированной системной инженерии. Кроме того, с применением созданного прототипа должны быть разработаны научно обоснованные рекомендации по снижению и удержанию рисков в допустимых пределах в жизненном цикле систем различного функционального назначения (см. разделы 2 - 5).

Таким образом, в диссертации поставлена важная научная проблема разработки программных, технологических и методических решений для ВС и КС, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии. Целью диссертационного исследования определено обоснование рациональных способов снижения и удержания рисков в допустимых пределах на стадиях жизненного цикла систем различного функционального назначения в условиях реальных и гипотетических вызовов и угроз на основе применения предлагаемых новых научно обоснованных программных, технологических и методических решений для вычислительных систем и компьютерных сетей.

Это соответствует направлениям исследований, изложенным в пунктах 4, 7, 9, 10 паспорта специальности 2.3.5. «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

1.6 Выводы по разделу 1

В результате проведенного анализа существующих подходов к управлению рисками в приложениях системной инженерии сделаны следующие выводы.

1. В условиях разнородных неопределенностей роль системной инженерии в решении практических задач характеризуется научной фундаментальностью в достижении целей системы за счет оперативного прогнозирования рисков, упреждающего выявления «узких мест» и определения рациональных способов снижения и удержания рисков в допустимых пределах. Место системной инженерии – везде, где возникает потребность в решении задач системного анализа и оптимизации, а также поиска и исследования новых практических идей и возможностей.

2. Выявлены и сформулированы 10 основных тенденций в приложениях системной инженерии, характеризующих важность управления рисками на ближайшую многолетнюю перспективу, это:

1) поворот к кардинальному совершенствованию мобилизационных возможностей государства для укрепления оборонно-промышленного комплекса и обороны страны;

2) расширенное практическое внедрение результатов технического прогресса для совершенствования и развития функциональных возможностей систем (с ожиданием повышения качества, безопасности, эффективности систем, предсказуемости и устойчивости их функционирования, доступности по цене);

3) существенное усложнение систем, обострение проблематики информационной безопасности, широкое внедрение методов количественного прогнозирования рисков и обоснования упреждающих мер противодействия разнородным угрозам;

4) целенаправленная интеллектуализация систем и технологий (с необходимым обеспечением проверяемости, безопасности и доверия к интеллектуальным системам, объяснением и пониманием логики их действий);

5) заметное влияние цифровой трансформации на создаваемые системы, выпускаемую продукцию, стиль и методы работы людей;

6) переход промышленности на принципы и технологии индустрии 4.0 (с «умными» фабриками, киберфизическими системами, цифровыми двойниками и цепочками взаимодействующих инструментов и процессов);

7) построение нового социального общества и решение социальных проблем методами, базирующимися на интеграции реального физического мира с виртуальным киберпространством;

8) накопление и использование знаний для повышения качества, безопасности и эффективности систем и оптимизации управления предприятиями, проектами и системами;

9) разворот к системному решению проблем экологической безопасности и рационального природопользования;

10) реформирование профессиональной подготовки специалистов для эффективного решения проблем системной инженерии.

3. Установлено: по возможности необходимо упреждающее управление соответствующими рисками с учетом задаваемых требований при выполнении всех стандартизованных процессов:

процессов соглашения – приобретения и поставки продукции и услуг;

процессов организационного обеспечения проекта – управления моделью жизненного цикла, инфраструктурой, портфелем проектов, человеческими ресурсами, качеством, знаниями;

процессов технического управления – планирования проекта, оценки и контроля проекта, управления решениями, рисками, конфигурацией, информацией, измерений, гарантии качества;

технических процессов – анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы.

4. При создании и внедрении программных, технологических и методических решений, широко применимых для упреждающего управления рисками с использованием ВС и КС предложено руководствоваться следующими основными принципами:

- принципом системности, предполагающим наличие целеполагания и связанности в реализации системных процессов жизненного цикла в условиях создания, модернизации, развития, эксплуатации системы и выведения ее из эксплуатации;

- принципом сбалансированности эффектов в пределах допустимых рисков в условиях неопределенностей, возможных угроз и объективных ограничений для системы;

- принципом эффективного управления рисками, предполагающим оправданность деятельности по управлению рисками с учетом социально-экономических факторов (практическая деятельность по управлению рисками не может быть оправдана, если выгода от этой деятельности в целом не превышает вызываемого ею ущерба);

- прецедентным принципом для обоснования допустимых рисков в случае его предпочтительности в сравнении с ориентацией на систему-эталон или проект-эталон;

- принципом непревышения предельно допустимых экологических нагрузок на системы (чтобы обеспечение безопасности человека, живущего сегодня, достигалось путем

реализации таких решений, которые сохранили бы способность природы обеспечить безопасность и потребности будущих поколений).

Все применяемые принципы при упреждающем управлении рисками в приложениях системной инженерии должны быть согласованы с принципом целенаправленности осуществляемых действий.

5. В интересах совершенствования вероятностных моделей и создания программных, технологических и методических решений для использования ВС и КС сформулированы основные требования к формализованным методам риск-ориентированного подхода, включающие:

- требования к моделям и методам оценки специальных показателей и обоснования их допустимых значений;

- требования к моделям и методам прогнозирования рисков и обоснования допустимых рисков;

- требования к методам определения существенных угроз и условий;

- требования к методам поддержки принятия решений в жизненном цикле систем.

6. Поставлена важная научная проблема разработки широко применимых программных, технологических и методических решений для ВС и КС, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии. Целью диссертационного исследования определено обоснование рациональных способов снижения и удержания рисков в допустимых пределах на стадиях жизненного цикла систем различного функционального назначения в условиях реальных и гипотетических вызовов и угроз на основе применения предлагаемых новых научно обоснованных программных, технологических и методических решений для вычислительных систем и компьютерных сетей.

2. РАЗРАБОТКА ПРОГРАММНЫХ РЕШЕНИЙ, ОБЕСПЕЧИВАЮЩИХ ПРОГНОЗИРОВАНИЕ РИСКОВ И ОБОСНОВАНИЕ УПРЕЖДАЮЩИХ МЕР ПРОТИВОДЕЙСТВИЯ УГРОЗАМ

2.1 Анализ существующих программных решений по прогнозированию рисков для решения задач системной инженерии

Программные решения в интересах системной инженерии поддерживают, как правило, принятую в организации методологию. Например, принятая методология может базироваться на методологии идентификации инцидентов, представляющих серьезные (существенные) угрозы (МИСУИ), и методологии идентификации эталонных сценариев инцидентов (МИЭСИ). Обзор распространенной методологии по ГОСТ Р 54145 «Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Общая методология» представлен на рис. 2.1.

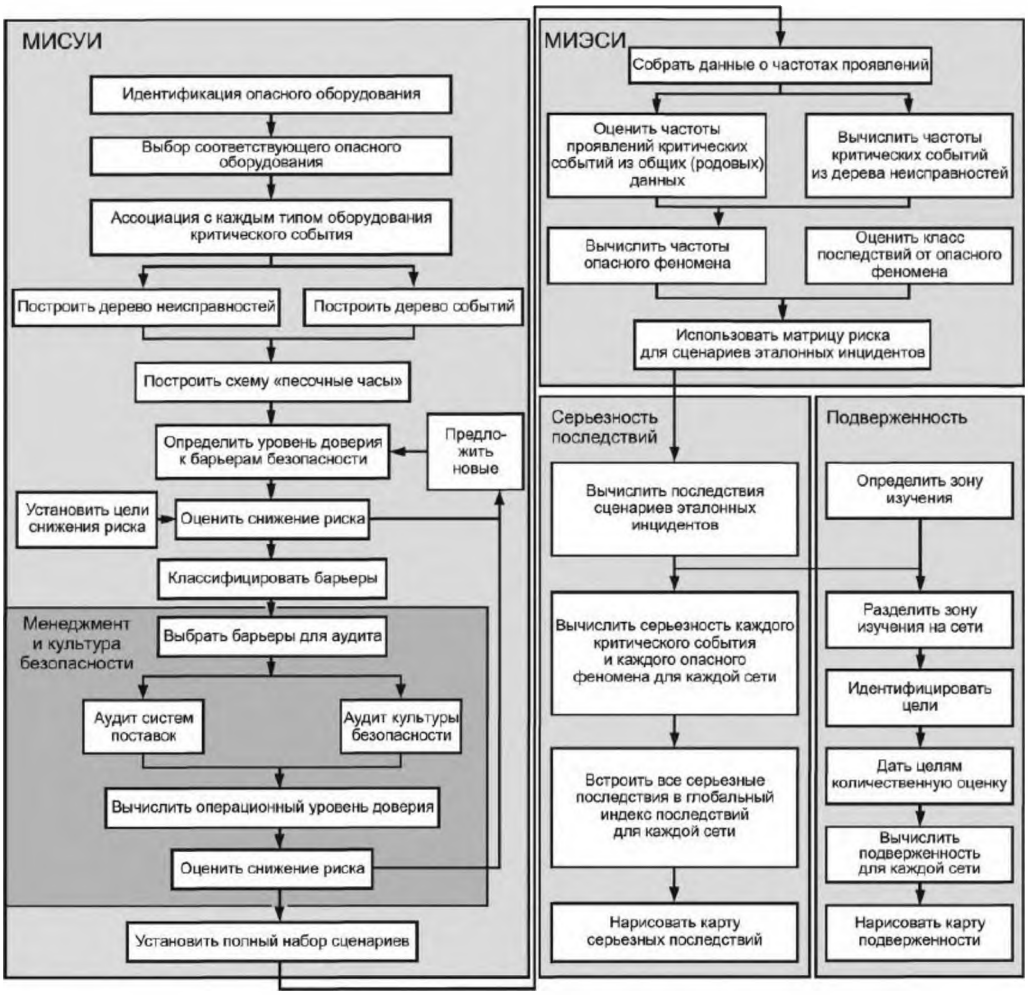


Рис. 2.1 Общий обзор методологии по ГОСТ Р 54145

Аналогичные подходы изложены и в других стандартах. Так, системный анализ процесса управления рисками осуществляют с учетом специфики системы и рекомендаций ГОСТ Р ИСО 9000, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 14258, ГОСТ

Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р МЭК 61069-2,…8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508, ГОСТ Р 72160 и др. При этом чаще всего применяемые методологии используют подход постфактум, основанный на показателе частоты состоявшихся проявлений критических событий (там, где это возможно) и на экспертных оценках критичности негативных последствий. Такого рода программные решения охватывают главным образом организационные аспекты управления рисками, базируясь при этом на качественном прогнозе, не связывая упреждающее управление для достижения системных целей с вероятностным прогнозированием рисков.

Одно из первых программных решений по вероятностному прогнозированию рисков было представлено в 2000 году в Комплексе для Оценки Качества функционирования информационных систем (КОК) - "ноу-хау" (Свидетельство о государственной регистрации программы для ЭВМ №2000610272) [182, 183]. В программе «Защищенность от опасных воздействий» этого комплекса КОК расчетная базовая модель учитывает следующие исходные данные (см. рис. 2.2): σ – частота возникновения источников угроз в моделируемой системе; β – среднее время активизации (развития) угроз с момента возникновения источников угроз до нарушения установленных требований по обеспечению целостности моделируемой системы или до инцидента; $T_{меж}$ – время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы (постоянная величина, задаваемая для системы); $T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы (подразумевается, что в нем учитывается среднее время восстановления нарушенной целостности системы); $T_{зад}$ – задаваемая длительность периода прогноза.

Рис. 2.2 Форма ввода исходных данных в программном комплексе КОК (2000г.)

Усовершенствование и развитие программных средств КОК при авторском участии (см. также подразделы 2.2-2.5) проведено в период 2004 – 2010гг. в комплексах «Моделирование

процессов в жизненном цикле систем», "Моделирование процессов" - "ноу-хау" (Свидетельство о государственной регистрации программы для ЭВМ №2004610858), «Программно-инструментальный комплекс оценки качества функционирования информационных систем через Интернет «КОК-Интернет» - "ноу-хау"» (Свидетельство о государственной регистрации программы для ЭВМ №2008612348), «Программно-вычислительный комплекс оценки качества производственных процессов (сертификат соответствия № РОСС RU.СП20.Н00015)» (Свидетельство о государственной регистрации программы для ЭВМ № 2010614145), «Комплекс для оценки качества информационных и административно-управленческих процессов при функционировании электронного правительства (КОК-ЭП)» (Свидетельство о государственной регистрации программы для ЭВМ № 2010617017) [169 – 174] – см. рис. 2.3.

Рис. 2.3 Копии свидетельств Роспатента на программные инструментарии 2004 – 2010гг.

В итоге к 2013г. был создан прототип Интернет-технологии удаленного прогноза рисков для решения ряда аналитических задач прогнозирования рисков для систем различного функционального назначения [175 - 177].

Рис. 2.4 Общее описание созданной в 2013г. Интернет-технологии прогнозирования рисков

Программное обеспечение Интернет-технологии, размещаемое на сервере, состояло из программных средств расчета рисков в загрузочных модулях (бинарный код) для аппаратных платформ, основанных на архитектуре типа INTEL/PENTIUM и использоваться под управлением операционной системы ОС Windows 2000/ NT/ XP. Программно-технические средства пользователя должны были включать в свой состав компьютер с выходом в Интернет и браузер с установленной поддержкой Adobe Flash Player. Программное обеспечение персонального компьютера пользователя должно воспринимать doc- или pdf –файлы для чтения предоставляемых аналитических результатов. Для получения аналитического отчета пользователю достаточно было зайти на конкретный сайт, и далее в удаленном режиме осуществлялось прогнозирование рисков по авторским моделям. Пользователь знакомился с общим описанием, заносил свои регистрационные данные (см. рис. 2.5). Для создания последовательной цепочки элементов использовались формы ввода данных для отдельного элемента – см. рис. 2.6.

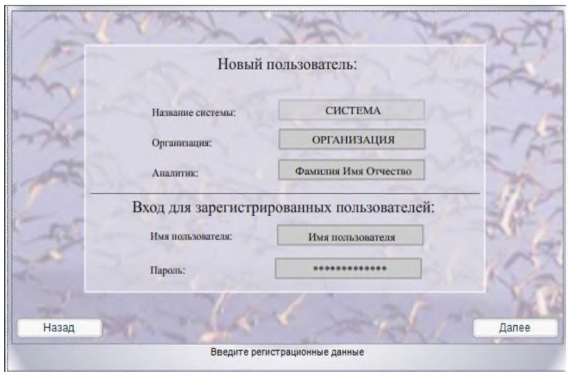


Рис. 2.5 Регистрационные данные

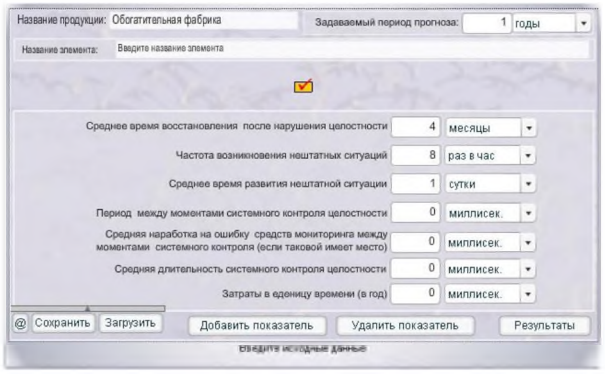


Рис. 2.6. Пример формы ввода данных для отдельного элемента сложной структуры

Сформированные исходные данные посылались на расчет путем нажатия клавиши «Результаты». В итоге применения разработанной Интернет-технологии осуществлялся прогноз показателей рисков, формирование за несколько минут и размещение на сайте в доступном для пользователя месте аналитического отчета, формируемого в виде файла формата .pdf или .doc согласно заданным для расчетов исходным данным.

В 2013г. программно-методические идеи были успешно защищены в рамках кандидатской диссертации «Методика прогнозирования техногенных рисков и ее реализация с использованием Интернет-технологии» по специальности 05.13.17 «Теоретические основы информатики» [186]. Акты о реализации результатов этих диссертационных исследований на ФГКУ комбината хранения нефтепродуктов «Монтаж» Росрезерва, на Тугнуйской обогатительной фабрике Сибирской угольной энергетической компании (СУЭК), в ФГНУ «Центр информационных технологий и систем» (ФГНУ ЦИТиС) и в РГУ нефти и газа им. И.М.Губкина отражены на рис. 2.7.

«Утверждаю»
ВрИО директора ФГКУ «Монтаж»
А.В.Бушмелев
« 29 » ноября 2012г.

АКТ
реализации положений диссертационной работы Нистратова Андрея Андреевича на соискание ученой степени кандидата технических наук по специальности 05.13.17

Настоящий акт свидетельствует, что методические положения по расчету вероятностных показателей качества и рисков, разработанные Нистратовым А.А. в рамках своей диссертационной работы, были реализованы при создании прототипа технологии прогноза качества и рисков, внедренного на ФГКУ «Монтаж» Росрезерва.

Заместитель директора ФГКУ «Монтаж» Е.Ю. Макулина

«Утверждаю»
Исполняющий обязанности Первого заместителя исполнительного директора по обогащению ООО «Тугнуйская обогатительная фабрика»
Шкодин И.В.
« » ноября 2012г.

АКТ
реализации положений диссертационной работы Нистратова Андрея Андреевича на соискание ученой степени кандидата технических наук по специальности 05.13.17

Настоящий акт свидетельствует, что модель противодействия нарушениям функциональной целостности на предприятии в условиях возникновения и активизации угроз, разработанная Нистратовым А.А. в рамках своей диссертационной работы, была реализована в программных моделях возникновения и активизации угроз, сбора и обработки информации о потенциальной опасности и противодействия угрозам, внедренных на Тугнуйской обогатительной фабрике.

Заместитель исполнительного директора по производственному контролю, промышленной безопасности, охране труда и охране окружающей среды ООО «Тугнуйская обогатительная фабрика»
Яровой Г.И.

ЦИТиС
"Центр информационных технологий и систем органов исполнительной власти"
(ФГКУ ЦИТиС)
№ 6-14-39

Акт реализации

Настоящий акт составлен о том, что методические материалы диссертационной работы на соискание ученой степени кандидата технических наук Нистратова Андрея Андреевича, посвященные исследованиям в области прогноза рисков нарушения безопасности функционирования информационных систем, реализованы при подготовке отчета о НИР шифр «З-Идея-КУРЗ».

Отчет о НИР принят заказчиком – войсковой частью 43753.

Заместитель директора
по научной работе
дфмн, профессор В.М. Симонов

Начальник управления
кти, доцент М.М. Безкоровайный

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Российский государственный университет
нефти и газа имени И. М. Губкина»
119991, г. Москва, Ленинский просп., д. 65, корп. 1
Телефон: (499) 233-92-25; факс: (499) 135-88-95
E-mail: com@gubkin.ru; http://www.gubkin.ru
4 марта 2013г. № 530/301
на № от

АКТ
реализации программных решений диссертационной работы Нистратова Андрея Андреевича «Методика прогнозирования техногенных рисков с помощью Интернет-технологии (на примерах систем различного функционального назначения)» на соискание ученой степени кандидата технических наук по специальности 05.13.17

Настоящий акт свидетельствует, что методические и программные решения, разработанные Нистратовым А.А. в рамках своей диссертационной работы, реализованы в учебном процессе РГУ нефти и газа имени И.М.Губкина и были использованы:

магистрами при выполнении лабораторных работ по направлению подготовки «Информатика и вычислительная техника» (230100), программа «Автоматизированные системы диспетчерского управления в нефтегазовом комплексе» (230100.01);

соискателем ученой степени кандидата технических наук при проведении расчетов по управлению рисками нарушения качества функционирования трубопроводного транспорта газа в условиях полуострова Ямал.

Первый проректор
по стратегическому развитию и ИТ М.А. Силин

Заведующий кафедрой АСУ
доктор технических наук, профессор Л.И.Григорьев

Руководитель дирекции
информационных интернет-ресурсов А.Е.Бурцева

Рис. 2.7 Акты о реализации диссертационных исследований по прогнозированию техногенных рисков с использованием Интернет-технологии в 2013г.

Накопленный положительный опыт [4, 5, 49, 52, 53, 58, 64, 69, 70, 77, 83, 84, 97, 101 - 167] позволил существенно усовершенствовать созданные ранее программные средства. К примеру, в версиях 2018г. появилась возможность дополнительного учета отдельно времени диагностики и времени восстановления целостности системы – см. рис. 2.8-2.10, подразделы 2.2-2.5, раздел 3.

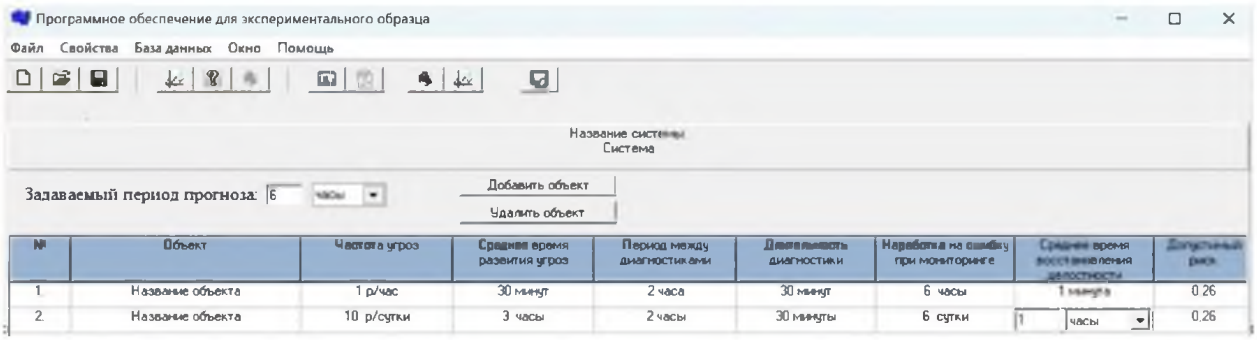


Рис. 2.8 Пример формы ввода данных (в примере - для двух последовательных элементов сложной структуры, 2018г.)

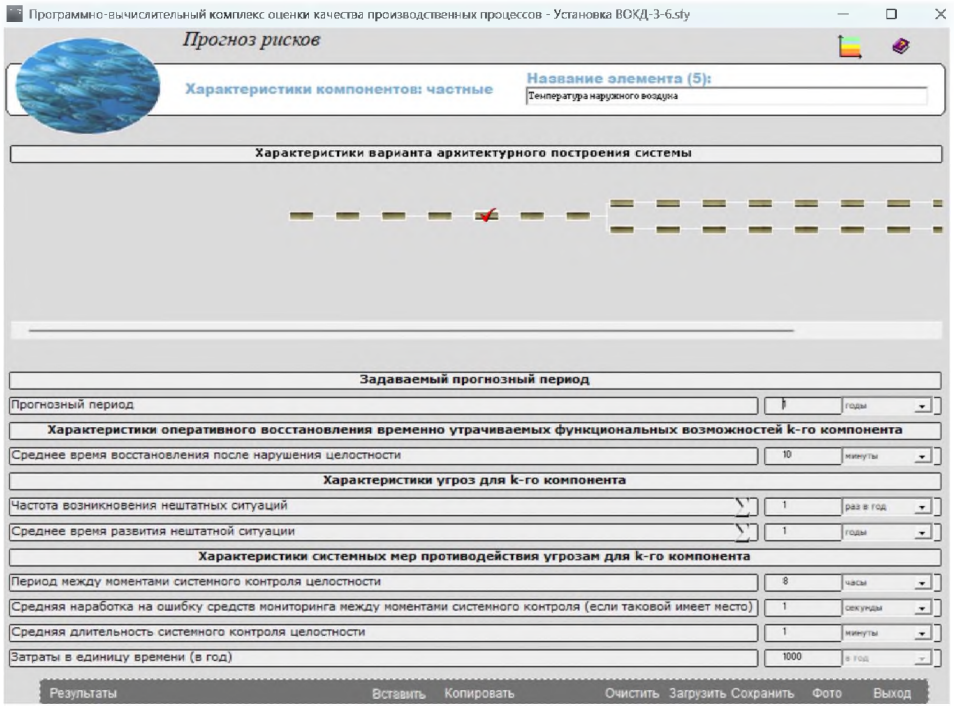


Рис. 2.9. Пример формы ввода данных для элементов сложной структуры (2018г.)

Рис. 2.10 Копии свидетельств Роспатента на программные инструментарии 2018г.

Ретроспективный анализ показал, что возрастание потребностей системной инженерии, научно-технический прогресс в сфере информационных технологий и телекоммуникаций, устаревание программного обеспечения на фоне санкций стран Запада, осознание важности и масштабности моделирования с учетом практических особенностей привели к необходимости дальнейшего научного развития вероятностных моделей, создания усовершенствованных программных, технологических и методических решений в интересах упреждающего управления рисками для систем различного функционального назначения. При этом особый акцент сделан на моделировании стандартизованных процессов в жизненном цикле различных систем, а также на внедрении зарекомендовавших себя методов в национальные стандарты.

2.2 Совершенствование вероятностных моделей для прогнозирования и упреждающего управления рисками в жизненном цикле систем

Применяемые вероятностные модели относятся к математическому обеспечению, реализуемому в предлагаемых программных решениях (в специальном программном обеспечении) для ВС и КС. Логика совершенствования вероятностных моделей, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии, включает в себя следующие шаги:

- 1-й шаг – построение пространства элементарных событий и определение формализованных показателей для вероятностного пространства, обеспечивающего аналитическое прогнозирование рисков с возможностями решения прямых и обратных задач;

- 2-й шаг – выбор вероятностных моделей, обладающих потенциалом совершенствования для моделирования систем различного функционального назначения в

интересах аналитического прогнозирования рисков и способных после совершенствования к использованию в качестве базовых (т.е. выбор источников базовых моделей);

- 3-й шаг – теоретическое обоснование для совершенствования выбранных моделей до уровня базовых путем:

учета различий во временах диагностики и восстановления целостности моделируемой системы, представимой в виде «черного ящика»;

определения универсальной вспомогательной модели показателей, используемой для извлечения знаний из процесса мониторинга данных для их включения в исходные данные базовых моделей;

придания возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков» (т.е. сложная система содержит при формализации более, чем один структурный элемент, представимый в виде «черного ящика»);

- 4-й шаг – прогнозная оценка остаточного времени до нарушения целостности моделируемой системы путем статистического использования базовых моделей;

- 5-й шаг – реализация основных положений по моделированию, аналитическому прогнозированию рисков и упреждающему управлению рисками в национальных стандартах;

- 6-й шаг – формирование концептуального облика создаваемого прототипа технологии поддержки риск-ориентированной системной инженерии, на основе реализации предлагаемых математического обеспечения, программных и технологических решений для ВС и КС.

2.2.1 Построение пространства элементарных событий. Определение формализованных показателей для прогнозирования рисков

Осуществляется 1-й шаг предлагаемой логики – построение пространства элементарных событий и определение формализованных показателей для вероятностного пространства, обеспечивающего аналитическое прогнозирование рисков с возможностями решения прямых и обратных задач.

Аналитическое прогнозирование рисков выполняется на основе вероятностного моделирования систем. Для практического применения предлагаются методы и модели [4, 5, 49, 52, 53, 58, 64, 69, 70, 77, 83, 84, 97, 101 - 167], доведенные до реализации в ГОСТ Р 59329 – ГОСТ Р 59357, ГОСТ Р 59989 – ГОСТ Р 59994 (далеко не исчерпывающие списка адекватных моделей). В этих методах и моделях субъективные весовые коэффициенты

исключены. Более высокая объективность исходных данных для расчетов исключает «подгонки» под любые пожелания, ожидания и нормативы, не привязанные к конкретным формальным методам. Предлагаемые методы базируются на классически построенном вероятностном пространстве (Ω, B, P) [20, 184], где Ω – конечное пространство элементарных событий; B – класс всех подмножеств множества Ω, удовлетворяющий свойствам сигма-алгебры; P – вероятностная мера на пространстве элементарных событий. При этом, поскольку $\Omega=\{\omega_k\}$ – конечное, в моделях установлено отображение $\omega_k \rightarrow p_k = P(\omega_k)$ такое, что $p_k \geq 0$ и $\sum_k p_k = 1$, подход стандартизован - дополнительно к указанным выше национальным стандартам такой подход принят в международном стандарте ГОСТ Р ИСО 3534-1 «Статистические методы. Словарь и условные обозначения. Часть 1. Общие статистические термины и термины, используемые в теории вероятностей».

При функционировании системы в условиях разнородных угроз степень приемлемости происходящих событий предлагается оценивать вероятностью «успеха» и/или риском «неудачи» с учетом возможных ущербов в течение заданного прогнозного периода времени. В каждом конкретном случае понятие «успеха» должно быть определено в терминах приемлемого состояния рассматриваемой системы для выполнения заданных или ожидаемых функций. Понятие «неудачи» означает отсутствие «успеха». Предполагается, что анализ рассматриваемых угроз может быть формализован с использованием понятия моделируемой системы (т.е. системы, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели и, при необходимости, формализованных моделей учитываемых сущностей в условиях их применения). При этом получаемые результаты системного анализа для какой-либо моделируемой системы используются в интерпретации к исходной системе, в интересах которой проводятся соответствующие расчеты [4, 5, 37, 49, 52, 53, 58, 64, 69, 70, 77, 83, 84, 97, 167].

В моделях простой структуры система рассматривается как «черный ящик», для него сделано предположение о множестве угроз и наличии (или отсутствии) технологии системного контроля целостности системы и восстановления системы после состоявшихся нарушений (или выявленных предпосылок к нарушениям). В моделях сложной структуры под моделируемой системой понимается определенная упорядоченная совокупность составных элементов, каждый из которых логически представляет собой «черный ящик». В общем случае в системах сложной структуры для различных элементов может быть свое множество угроз или специфичные технологии системного контроля и восстановления целостности системы. Под целостностью моделируемой системы понимается такое ее

состояние, которое отвечает целевому назначению модели системы в течение задаваемого периода прогноза.

Например, при моделировании, направленном на прогнозирование риска нарушения требований по защите информации, целевое назначение моделируемой системы проявляется в выполнении требований по защите информации. Такая интерпретация подразумевает выполнение требований по защите информации не только применительно к защищаемым активам и действиям, с использованием которых создают и получают выходные результаты, но и к самим выходным результатам, которые применяют (или планируют к созданию, получению и/или применению). В итоге для каждого из элементов моделируемой системы и системы в целом в приложении к прогнозированию риска нарушения требований по защите информации пространство элементарных событий на временной оси могут образовывать два основных состояния: - «Выполнение требований по защите информации в системе обеспечено», если в течение всего периода прогноза обеспечено выполнение требований по защите информации; - «Выполнение требований по защите информации в системе нарушено» – в противном случае. В результате математического моделирования рассчитывается вероятность приемлемого выполнения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе обеспечено») в течение всего периода прогноза и ее дополнение до единицы, представляющее собой вероятность нарушения требований по защите информации (т. е. пребывания в состоянии «Выполнение требований по защите информации в системе нарушено»). В свою очередь вероятность нарушения требований по защите информации в течение всего периода прогноза в сопоставлении с возможным ущербом определяет риск нарушения требований по защите информации.

Анализ показал, что на практике широко распространены качественные показатели для оценки рисков, выражаемые в относительных понятиях «больше - меньше», «выше - ниже». Они используются в условиях слабой неопределенности относительно угроз и эксплуатационных характеристик систем. Качественные показатели в основном отражают экспертный (субъективный) подход, они обусловлены необходимостью выполнения конкретных требований, задаваемых на вербальном уровне в техническом задании на систему и иных нормативно-правовых документах. Например, ряд качественных показателей в области обеспечения информационной безопасности определен в

ГОСТ Р ИСО/МЭК 27005 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

Требования к количественным показателям носят объективный характер. В системном процессе в условиях неопределенности эти требования, как правило, учитывают:

- критичные сущности рассматриваемых системных процессов, системы и/или проекта, характеризующие безопасность системы;
- требования заинтересованных сторон, выходные результаты и выполняемые действия процесса;
- потенциальные угрозы безопасности системы, а также возможные сценарии возникновения и развития этих угроз;
- практическую интерпретацию оцениваемых специальных показателей и вероятностных результатов прогнозирования рисков при планировании и реализации системных процессов, возможные предупреждающие меры по снижению рисков или их удержанию в допустимых пределах;
- способы дальнейшего использования результатов оценки специальных показателей и прогнозирования рисков;
- методы использования результатов для решения практических задач прогнозирования рисков и обоснования эффективных упреждающих мер по снижению этих рисков или их удержанию в допустимых пределах.

Проведенный анализ позволил сформировать предложения по рекомендуемым показателям рисков, ссылки на типовые методы и модели, ограничения на допустимые риски и перечни методик для решения задач системной инженерии – см. таблицу 2.1 [4, 5, 49, 52, 53, 58, 64, 69, 70, 77, 83, 84, 97, 136, 149, 167]. При этом даны ссылки на соответствующие стандарты, в т.ч. на 19 стандартов, созданных при непосредственном участии автора – см. подраздел 2.3.

Таблица 2.1 Ссылки на рекомендуемые показатели рисков, типовые методы и модели, ограничения на допустимые риски, перечни методик

Системные процессы	Вероятностные показатели риска	Ссылки на типовые модели, методы, допустимые риски и перечень методик на их основе
Процессы приобретения и поставки продукции и услуг для системы	- риск нарушения надежности реализации процесса как такового без учета дополнительных требований (ДТ); - риск нарушения ДССТ на примере требований по защите информации (ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59329–2021, методы, модели -прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс управления моделью жизненного цикла системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - обобщенный риск нарушения реализации процесса с учетом ДССТ (в том числе на примере требований по ЗИ)	ГОСТ Р 59330–2021, методы, модели -прил. В; допустимые риски – прил. Г; перечень методик – прил. Д; ГОСТ Р 59992–2022, методы, модели -прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс управления инфраструктурой системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - обобщенный риск нарушения реализации процесса с учетом ДССТ (в том числе на примере требований по ЗИ)	ГОСТ Р 59331–2021, методы, модели -прил. В; допустимые риски – прил. Д ; перечень методик – прил. Е; ГОСТ Р 59993–2022, методы, модели -прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс управления портфелем проектов	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59332–2021, методы, модели -прил. В; допустимые риски – прил. Г ; перечень методик – прил. Д
Процесс управления человеческими ресурсами системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59333–2021, методы, модели -прил. В; допустимые риски – прил. Д; перечень методик – прил. Е
Процесс управления качеством системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - обобщенный риск нарушения реализации процесса с учетом ДССТ (в том числе на примере требований по ЗИ)	ГОСТ Р 59334–2021, методы, модели -прил. В; допустимые риски – прил. Г; перечень методик – прил. Д; ГОСТ Р 59989–2022, методы, модели -прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс управления знаниями о системе	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59335–2021, методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е
Процесс планирования проекта	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59336–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс оценки и контроля проекта	- для системных процессов риски по ГОСТ Р 59337–2021, 6.3 (с учетом ДССТ на примере требований по ЗИ) и ГОСТ Р 59990–2022, 6.3	ГОСТ Р 59337–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д; ГОСТ Р 59990–2022, методы, модели -прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс управления решениями	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59338–2021, методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е
Процесс управления рисками для системы	- для системных процессов риски по ГОСТ Р 59339–2021, 6.3 (с учетом ДССТ на примере требований по ЗИ); - интегральные риски нарушения качества системы в сценарных условиях комбинации используемых системных процессов в течение задаваемого периода прогноза по ГОСТ Р 59991–2022, 6.3	ГОСТ Р 59339–2021, методы, модели -прил. В; допустимые риски – прил. Д; перечень методик – прил. Е; ГОСТ Р 59991–2022, методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е

Процесс управления конфигурацией системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59340–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс управления информацией системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примерах требований к надежности и своевременности предоставления, полноты и достоверности выходной информации, требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примерах требований к надежности и своевременности предоставления, полноты и достоверности выходной информации, требований по ЗИ); - вероятностные показатели надежности и своевременности предоставления, полноты, достоверности и конфиденциальности выходной информации	ГОСТ Р 59341–2021, методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е. ГОСТ Р 58494–2019, прил. Е.2.
Процесс измерений системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59342–2021, методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е
Процесс гарантии качества для системы	по ГОСТ Р 59994–2022, п. 6.3	ГОСТ Р 59343–2021 методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е; ГОСТ Р 59994–2022 методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс анализа бизнеса или назначения системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59344–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс определения потребностей и требований заинтересованной стороны для системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59345–2021, методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е
Процесс определения системных требований (на примере требований по ЗИ)	- частные показатели риска реализации угроз безопасности информации, направленных на нарушение функционирования системы, в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска); - частные показатели риска реализации угроз утечки конфиденциальной информации в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения требований по защите конфиденциальной информации); - интегральные показатели риска реализации угроз, направленных на нарушение функционирования системы в течение ее жизненного цикла, в условиях отсутствия и применения мер защиты, предлагаемых в ходе формирования системных требований	ГОСТ Р 59346–2021, методы, модели - приложения В, Д; допустимые риски – прил. Е; перечень методик – прил. Ж
Процесс определения архитектуры системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59347–2021, методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е
Процесс определения проекта	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59348–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс системного анализа	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59349–2021, методы, модели -прил. В; допустимые риски – прил. Д; перечень методик – прил. Е
Процесс реализации системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59350–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д

Процесс комплексирования системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59351–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс верификации системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения дополнительных специфических требований (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59352–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс передачи системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59353–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д
Процесс аттестации системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59354–2021, методы, модели - прил. В; допустимые риски – прил. Г ; перечень методик – прил. Д
Процесс функционирования системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59355–2021, методы, модели - прил. В; допустимые риски – прил. Д ; перечень методик – прил. Е
Процесс сопровождения системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59356–2021, методы, модели - прил. В; допустимые риски – прил. Д; перечень методик – прил. Е
Процесс изъятия и списания системы	- риск нарушения надежности реализации процесса как такового (без учета ДТ); - риск нарушения ДССТ (на примере требований по ЗИ); - риск нарушения реализации процесса с учетом ДССТ (на примере требований по ЗИ)	ГОСТ Р 59357–2021, методы, модели - прил. В; допустимые риски – прил. Г; перечень методик – прил. Д

В результате проведенного анализа на сформулированном пространстве элементарных событий в условиях различных неопределенностей (с учетом специфических физически измеримых показателей) предложено использовать следующие показатели рисков, одинаково свойственных для любого рода систем:

- риск нарушения рассматриваемого системного процесса как такового для реализации основных функциональных требований (для любого из рассматриваемых процессов соглашения, процессов организационного обеспечения проекта, процессов технического управления и технических процессов) в течение задаваемого периода прогноза;

- риск нарушения рассматриваемого системного процесса с учетом дополнительных специфических системных требований (ДССТ) в течение задаваемого периода прогноза;

и, как более обобщенные за счет расширительного толкования понятия целостности системы:

- риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза при реализации основных функциональных требований;

- риск нарушения дополнительных специфических требований к моделируемой системе в течение задаваемого периода прогноза;

- интегральный риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза при реализации основных функциональных требований и дополнительных специфических требований.

2.2.2 Выбор вероятностных моделей для использования в качестве источников базовых моделей

Осуществляется 2-й шаг предлагаемой логики совершенствования вероятностных моделей, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии, – это выбор вероятностных моделей, обладающих потенциалом совершенствования для моделирования систем различного функционального назначения в интересах аналитического прогнозирования рисков и способных после совершенствования к использованию в качестве базовых. Выбор источников базовых вероятностных моделей осуществляется не только для их совершенствования в интересах широкого применения при использовании системных процессов, но и для демонстрации применимости предлагаемых программных, технологических и методических решений, допускающих подключение новых вероятностных моделей, в т.ч. выходящих за рамки настоящей диссертации.

При выборе вероятностных моделей, которые могут быть приняты для использования в качестве базовых, необходимо учитывать, что расчет вероятностных показателей делается при условии или в предположении реальной или гипотетической повторяемости возможных событий и их независимости.

В типовой математической формализации приняты следующие предположения [4, 5, 37, 136, 149, 167]:

к началу периода прогноза целостность моделируемой системы полагается обеспеченной, в условиях неопределенностей возникновение и разрастание различных угроз целостности моделируемой системы описывается в терминах случайных событий;

для различных вариантов развития угроз существуют технологии и меры для выявления признаков возникновения источников угроз и воспрепятствования реализации угрозам, а также выявления следов реализации угроз.

Кроме того, делается предположение о наличии возможностей по определению предпосылок к реализации угроз, а также возможностей по приемлемому восстановлению нарушаемых условий функционирования моделируемой системы (с точки зрения противодействия угрозам). Обоснованное использование выбранных мер противодействия угрозам является предупреждающими контрмерами.

С учетом различных неопределенностей относительно возможных угроз при выборе базовых моделей принято допущение о пуассоновских потоках моментов возникновения событий на временной оси и об экспоненциальном распределении времени развития угроз. Предположение о пуассоновости обосновано тем, что в период прогноза общий поток моментов возникновения событий гипотетически представляет собой сумму большого числа составных разнородных потоков. Интенсивность каждого из слагаемых потоков мала по сравнению с интенсивностью суммарного потока – в такой ситуации действует предельная теорема Хинчина – Григолиониса, согласно которой суммарный поток будет близок к пуассоновскому. В свою очередь, экспоненциальное распределение обладает свойством отсутствия последействия. Это означает, что согласно предположению об экспоненциальности остаток времени до реализации угрозы всегда имеет то же распределение с тем же параметром, что и время с момента возникновения угрозы. Это предполагает более тяжелые условия функционирования моделируемой системы [4, 5, 37].

Среди множества проанализированных вероятностных моделей из таблицы 2.1 и [2, 4, 5, 37] выбраны две широко применимые модели «черного ящика» в их изначальном варианте [37], поскольку они с определенной степенью адекватности способны формально описать все 30 рассматриваемых в работе процессов в жизненном цикле различных систем. Это – «Модель «черного ящика» при отсутствии какого-либо контроля» и «Модель «черного ящика» при реализации технологии периодического системного контроля» [4, 5, 167].

2.2.2.1 Модель «черного ящика» при отсутствии какого-либо контроля [2, 5, 37, 49, 167]

Моделируемая система представляется в виде «черного ящика», функционирование которого не контролируется. При функционировании в результате возникновения угроз и их развитии может произойти нарушение целостности системы. Восстановление нарушаемой целостности системы осуществляется по мере ее нарушения. К примеру, при прогнозировании риска нарушения требований по защите информации нарушение целостности системы интерпретируется как нарушение возможностей по выполнению требований по защите информации. С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения целостности системы в течение заданного периода прогноза. С точки зрения системной инженерии этот результат может быть интерпретирован следующим образом: результатом применения модели является расчетная вероятность нарушения целостности системы (или какого-либо процесса, если в качестве анализируемой системы рассматривается конкретный процесс) в течение заданного периода прогноза при отсутствии какого-либо контроля.

Модель представляет собой частный случай модели 2.2.2.2, если период между диагностиками целостности системы больше периода прогноза. Учитывая это, используются формулы (1) – (5) из 2.2.2.2.

2.2.2.2 Модель «черного ящика» при реализации технологии периодического системного контроля [2, 5, 37, 49, 167]

Поскольку целостность моделируемой системы, представленной в виде «черного ящика», может быть нарушена по различным причинам, осуществляется периодический контроль (диагностика) состояния целостности. К примеру, из-за случайного характера ряда угроз, различных организационных, программно-технических и технологических причин, различного уровня квалификации специалистов, привлекаемых для контроля, неэффективных мер поддержания или восстановления приемлемых условий функционирования системы и в силу иных причин выполнение требований по защите информации в системе может быть нарушено. Такое нарушение способно повлечь за собой негативные последствия с недопустимым ущербом для системы.

Развитие событий в моделируемой системе считается не нарушающим целостности в течение заданного периода прогноза, если к началу этого периода целостность системы обеспечена и в течение всего периода либо источники угроз не активизируются, либо после активизации до реализации угроз происходит их своевременное выявление и принятие адекватных мер противодействия угрозам. В целях моделирования предполагают, что существуют не только средства контроля (диагностики) целостности (выполнения требований по защите информации), но и способы поддержания и/или восстановления возможностей по обеспечению целостности при выявлении источников или следов начала активизации угроз. Восстановление осуществляется лишь в период системного контроля (диагностики). Соответственно, чем чаще осуществляют системный контроль с должной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии ненарушения целостности из-за возможных угроз в период прогноза. Это достигается на основе того, что в принятой модели за счет предупреждающих действий по результатам диагностики устраняются появившиеся и/или активизируемые угрозы, тем самым отдаляется во времени момент нанесения ущерба от реализации какой-либо угрозы.

За основу анализа принят следующий последовательный алгоритм возникновения и развития потенциальной угрозы: сначала возникает источник угрозы, после чего он начинает активизироваться, представляя возможную угрозу для нарушения целостности системы. По прошествии периода активизации, свойственного этому источнику угрозы

(в общем случае этот период активизации представляет собой случайную величину), наступает виртуальный момент непосредственно реализации угрозы с возможными негативными последствиями. Если после виртуального начала активизации угрозы на временной оси наступает очередная диагностика целостности моделируемой системы, то дальнейшая активизация угрозы полагается предотвращенной до нанесения недопустимого ущерба, а источник угроз – нейтрализованным (до возможного нового появления какой-либо угрозы после прошедшей диагностики) – см. рис. 2.11 [2, 5, 37, 49]. Циклы регенерации на рис. 2.10 определяются соседними вертикальными черточками, при этом для упрощения на рисунке время диагностики и восстановления равны нулю. Случаи 1, 4 характеризуют реализацию возникшей угрозы в течение заданного периода прогноза $T_{зад.}$, т.е. переход состояния системы в элементарное состояние «неудачи». Случаи 2, 3, 5 – характеризуют пребывание состояния системы в элементарном состоянии «успех» в течение всего периода прогноза $T_{зад.}$

Если активизация мгновенная, это считают эквивалентным внезапному отказу применительно к надежности систем по ГОСТ Р 27.102.

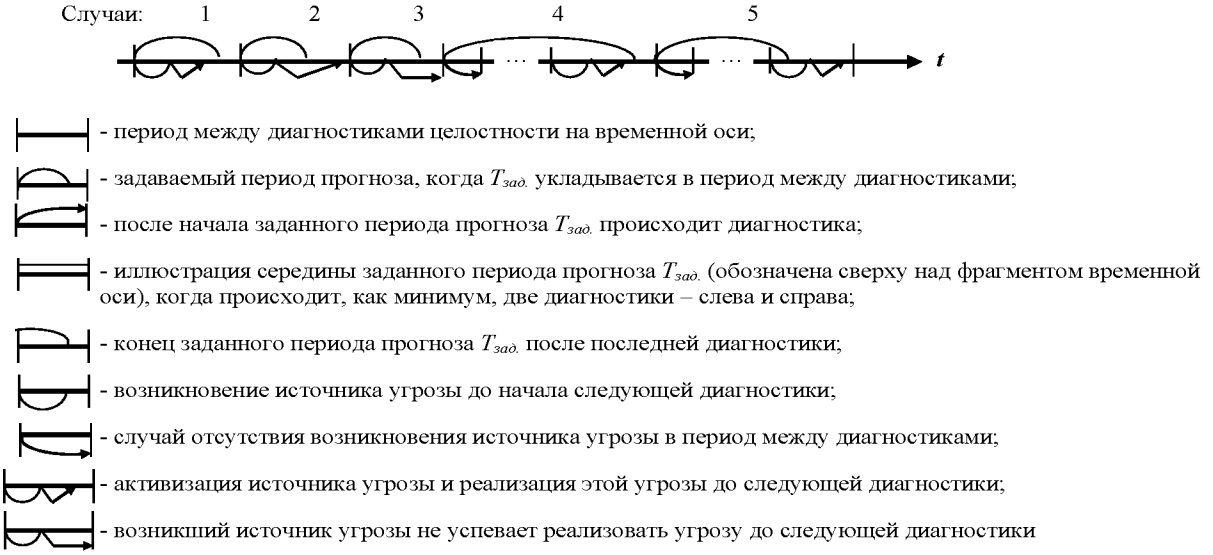


Рис. 2.11 Формальные случаи сохранения и нарушения целостности

С точки зрения системной инженерии формальным результатом применения модели является расчетная вероятность нарушения целостности моделируемой системы в течение заданного периода прогноза при реализации технологии периодического системного контроля (диагностики). При этом учитываются предпринимаемые меры периодической диагностики и восстановления целостности.

Формально должны быть определены следующие исходные данные:

σ – частота возникновения источников угроз в моделируемой системе;

β – среднее время активизации (развития) угроз с момента возникновения источников угроз до нарушения установленных требований по обеспечению целостности моделируемой системы или до инцидента;

$T_{меж}$ – время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы (постоянная величина, задаваемая для системы);

$T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы (подразумевается, что в нем учитывается среднее время восстановления нарушенной целостности системы);

$T_{зад}$ – задаваемая длительность периода прогноза.

В общем случае оценку вероятности нарушения целостности моделируемой системы $R_{наруш}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{зад}$) в течение периода прогноза $T_{зад}$ осуществляют по формуле [2, 5, 37, 49, 167]:

$$R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}) = 1 - P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}), \quad (2.1)$$

где $P_{возд}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{зад}$) – вероятность отсутствия нарушений целостности в течение периода $T_{зад}$. Возможны два варианта:- вариант 1 – заданный период прогноза $T_{зад}$ меньше периода между окончаниями соседних контролей ($T_{зад} < T_{меж} + T_{диаг}$);

- вариант 2 – заданный период прогноза $T_{зад}$ больше или равен периоду между окончаниями соседних контролей ($T_{зад} \geq T_{меж} + T_{диаг}$), т. е. за это время заведомо произойдет один или более контролей системы с восстановлением нарушенной целостности (если нарушения имели место к началу контроля).

Для варианта 1 при условии независимости исходных характеристик вероятность $P_{возд\,(1)}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{зад}$) отсутствия нарушений целостности моделируемой системы в течение периода прогноза $T_{зад}$ вычисляется по формуле [2, 5, 37, 49]:

$$P_{возд(1)} = \begin{cases} (\sigma - \beta^{-1})^{-1}\left\{\sigma e^{-T_{зад}/\beta} - \beta^{-1} e^{-\sigma T_{зад}}\right\}, \text{если } \sigma \neq \beta^{-1}, \\ e^{-\sigma T_{зад}}\left[1 + \sigma T_{зад}\right], \text{если } \sigma = \beta^{-1}. \end{cases} \quad (2.2)$$

Примечание – Формулу (2.2) используют для оценки риска отсутствия нарушений целостности при отсутствии какого-либо контроля в предположении, что к началу периода прогноза целостность моделируемой системы обеспечена.

Для варианта 2 при условии независимости исходных характеристик вероятность отсутствия нарушений целостности моделируемой системы в течение прогноза $T_{зад}$ вычисляется по формуле:

$$P_{возд\,(2)} = P_{серед} \cdot P_{кон}, \quad (2.3)$$

где $P_{\text{серед}}$ — вероятность отсутствия нарушений целостности системы в течение всех периодов между системными контролями, целиком вошедшими в границы времени $T_{\text{зад}}$, вычисляемая по формуле

$$P_{\text{серед}} = P^{N}_{\text{возд (1)}}\left(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{меж}} + T_{\text{диаг}}\right), \quad (2.4)$$

где N — число периодов между диагностиками, которые целиком вошли в границы времени $T_{\text{зад}}$, с округлением до целого числа, $N = [T_{\text{зад}}/(T_{\text{меж}} + T_{\text{диаг}})]$ – целая часть (именно из-за оперирования целой частью при построении зависимости расчетной вероятности от времени прогноза может появиться пилообразность);

$P_{\text{кон}}$ – вероятность отсутствия нарушений целостности системы после последнего системного контроля в конце периода прогноза до истечения времени $T_{\text{зад}}$, вычисляемая по формуле (2.2), т. е.

$$P_{\text{кон}} = P_{\text{возд (1)}}\left(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{ост}}\right),$$

где $T_{\text{ост}}$ — остаток времени в общем заданном периоде $T_{\text{зад}}$ по завершении N полных периодов, вычисляемый по формуле

$$T_{\text{ост}} = T_{\text{зад}} - N \cdot (T_{\text{меж}} + T_{\text{диаг}}). \quad (2.5)$$

Формула (2.3) логически интерпретируется так: для обеспечения целостности системы за весь период прогноза требуется обеспечение целостности на каждом из временных участков – будь то середина или конец задаваемого периода прогноза $T_{\text{зад}}$.

Примечание. Для расчетов $P_{\text{возд (2)}}$ возможны иные вероятностные меры – например, когда N – действительное число, учитывающее не только целую, но и дробную части (в этом случае пилообразность исчезнет, получится классическая функция распределения).

В итоге вероятность отсутствия нарушений целостности системы в течение периода прогноза $T_{\text{зад}}$ определяется аналитическими выражениями (2.2) – (2.5) в зависимости от варианта соотношений между исходными данными. Это позволяет вычислить по формуле (2.1) вероятность нарушения целостности системы $R_{\text{наруш}}\left(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}}\right)$ в течение заданного периода прогноза $T_{\text{зад}}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления нарушаемой целостности. С учетом возможного ущерба эта вероятность характеризует расчетный риск нарушения целостности системы в течение заданного периода прогноза при реализации технологии периодического системного контроля.

Впервые эти модели были предложены и исследованы А.И. Костогрызовым [2, 37, 185, 186]. В настоящей диссертации на основе этих предложены усовершенствованные модели (см. подраздел 2.3), дополнительно учитывающие различия в значениях времен диагностики и восстановления системы [5, 37, 49, 167], после чего именно эти

усовершенствованные модели далее по тексту будут именоваться как базовые для применения в ВС и КС.

Примечание – В частном случае, когда период между диагностиками больше периода прогноза $T_{зад} < T_{меж}$, модель 2.2.2.2 превращается в модель 2.2.2.1 для прогноза риска в моделируемой системе при отсутствии какого-либо контроля.

2.2.3 Теорема 1 (о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности системы)

Осуществляется начальный фрагмент 3-го шага предлагаемой логики совершенствования вероятностных моделей, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии. Это - теоретическое обоснование совершенствования выбранных моделей до уровня базовых путем учета различий во временах диагностики и восстановления целостности моделируемой системы, представимой в виде «черного ящика».

В 2.2.2 рассмотрены модели, предполагающие равенство средних времен диагностики и восстановления целостности моделируемой системы. На практике это, как правило, не так. Для устранения этого недостатка предлагается Теорема 1, применение которой позволяет учесть различия в средних временах диагностики и восстановления целостности моделируемой системы, изначальные исследования в этом направлении были проведены в кандидатской диссертации [186].

Теорема 1 (о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности системы).

Пусть процесс функционирования системы формализован с помощью модели 2.2.2.2 (для технологии периодического контроля) и характеризуется исходными данными: σ – частотой возникновения источников угроз в моделируемой системе; β – средним временем развития угроз с момента возникновения источников угроз до нарушения установленных требований по обеспечению целостности моделируемой системы или до инцидента; $T_{меж}$ – временем между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы (постоянная величина, задаваемая для системы); $T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы (подразумевается, что в нем учитывается среднее время восстановления нарушенной целостности системы); $T_{зад}$ – задаваемая длительность периода прогноза. Тогда, если в анализируемой системе длительность контроля (диагностики) может принимать одно из двух значений – либо длительность диагностики в течение среднего времени $T_{диаг.}$ с подтверждением целостности при отсутствии каких-либо нарушений, либо с учетом восстановления нарушенной

целостности – длительность в течение среднего времени $T_{восст.}$, то расчетный риск нарушения целостности, учитывающий оба этих значения длительности контроля (диагностики и восстановления), существует и с заданной точностью $\varepsilon>0$ при прочих равных условиях может быть определен путем применения модели 2.2.2.1 по формулам (2.1) – (2.5) с входным значением усредненной длительности контроля $T_{диагн.}^{(n)}$, вычисляемым итерационно:

1-я итерация: $T_{диагн.}^{(1)} = \min (T_{диагн.}, T_{восст.})$ и задаваемых на входе модели 2.2.2.2. Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление целостности;

2-я итерация осуществляется после расчета риска $R_{.}^{(1)}$ с использованием модели 2.2.2.2 по исходным данным 1-й итерации:

$$T_{диагн.}^{(2)} = T_{диагн.}^{(1)} (1 - R_{.}^{(1)}) + R_{.}^{(1)} \max (T_{диагн.}, T_{восст.}),$$

где $R_{.}^{(1)}$ – риск нарушения целостности с исходным значением $T_{диагн.}^{(1)}$;

…

n-я итерация осуществляется после расчета по модели 1 риска $R_{.}^{(n-1)}$ по исходным данным, получаемым после (n-1)-й итерации:

$$T_{диагн.}^{(n)} = T_{диагн.}^{(n-1)} (1 - R_{.}^{(n-1)}) + R_{.}^{(n-1)} \max (T_{диагн.}, T_{восст.}), \qquad (2.6)$$

где $R_{неконтр.}^{(n-1)}$ вычисляется по модели 2.2.2.2, но уже в качестве исходного выступает $T_{диагн.}^{(n-1)}$, рассчитанное на предыдущем шаге итерации.

Условием завершения расчета риска с заданной точностью $\varepsilon>0$ является применение модели 1 на n-й итерации, когда исходным выступает такая длительность контроля $T_{диагн.}^{(n)}$, что выполняется условие: $\left| R_{.}^{(n)} - R_{.}^{(n-1)} \right| \le \varepsilon$.

При этом применительно к ВС и КС для достижения практически приемлемой адекватности значение ε должно быть не более, чем 0.001 от задаваемого значения допустимого риска нарушения целостности системы. Доказательство Теоремы 1 приведено в приложении А.1. В дополнение к исследованиям [186] определены приемлемые для практических расчетов границы значения ε .

Тем самым обоснованность применения метода итераций доказана с помощью предложенной Теоремы 1 о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики ($T_{диаг.}$) и восстановления ($T_{восст.}$) целостности системы. Математическая суть теоремы 1 реализована в национальных стандартах (см. подраздел 2.3) и отражена в программных решениях (см. подразделы 2.4, 2.5). Корректность подтверждена многочисленными программными расчетами при решении практических задач – см. разделы 4, 5.

2.2.4. Совершенствование базовых моделей для анализа системных элементов, сложных систем и процессов [5, 37, 49, 64, 131, 139, 167]

В рамках 2.2.4 завершается осуществление 3-го шага предлагаемой логики совершенствования вероятностных моделей, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии. Это - теоретическое обоснование для совершенствования выбранных моделей до уровня базовых путем:

определения универсальной вспомогательной модели показателей (УВМП), используемой для извлечения знаний из процесса мониторинга данных для их включения в исходные данные базовых моделей (см. 2.2.4.1);

придания возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков» (2.2.4.2).

2.2.4.1 Определение универсальной вспомогательной модели показателей, используемой для извлечения знаний из процесса мониторинга данных [5, 64, 131, 139, 167]

Идея создания УВМП, используемой для извлечения знаний из процесса мониторинга данных для их включения в исходные данные базовых моделей, родилась из анализа функционирования системы дистанционного контроля (мониторинга) промышленной безопасности (СДК) на угольных шахтах, ГОСТ Р 58494-2019 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов» (разработан применением метода из теоремы 1 – см. приложение Е стандарта).

На практике могут возникать трудности с определение исходных данных для моделирования с использованием модели, получаемой по результатам применения теоремы 1 из 2.2.3. Так, если для исходных данных $T_{меж}$ и $T_{диаг}$ задаваемые значения для моделирования легко определяемы по конструкторским, эксплуатационным документам или организационным инструкциям, в т.ч. в сравнении с системами-аналогами, $T_{зад}$ – это задаваемое значение периода прогноза для исследований, то для таких исходных данных, как σ (частота возникновения источников угроз), β (среднее время развития угроз) и $T_{восст}$ (среднее время восстановления нарушенной целостности) возникает правомерный вопрос: «Где для них брать изначальные значения для моделирования?» Для ответа на этот вопрос предлагается нижеследующее определение универсальной вспомогательной модели показателей, используемой для извлечения знаний из процесса мониторинга данных.

Но прежде - несколько вводных слов о СДК [5, 64, 131, 139]. Построение и поддержка мер по обеспечению промышленной безопасности (ПБ) опасных производственных

объектов (ОПО) в нефтегазовой и химической промышленности, в угольной отрасли и др. областях требует системного подхода. В соответствии с этим подходом прежде всего необходимо осознать весь спектр возможных угроз для конкретного объекта и для каждой из этих угроз продумать тактику ее отражения. В этих целях нужно использовать самые разноплановые средства и приемы — законодательные, экономические, административные и психологические, а также функциональные возможности информационных технологий (ИТ). Поиск кардинальных направлений совершенствования ПБ, выгодных для бизнеса и государства, привел к осознанию острой необходимости и целесообразности создания и внедрения СДК, переводящих внутреннее информационное сопровождение процессов функционирования отдельного ОПО в режим полной прозрачности и широкой доступности в реальном времени для всех заинтересованных и ответственных сторон. Наряду с этим на основе рационального внедрения СДК ПБ реализуемый переход от сложившегося экспертного подхода к применению риск-ориентированного подхода получает необходимое информационное наполнение.

Предлагаемый к использованию вероятностный анализ функционирования СДК ПБ в его влиянии на интегральные риски нарушения ПБ позволяет оценить функционирование ОПО на заданный период прогноза. Подход применим для аналитического обоснования системных требований к СДК, системного определения сбалансированных мер, предупреждающих нарушения целостности подсистем, элементов и ОПО в целом при ограничениях на ресурсы и допустимые риски.

Дистанционный контроль промышленной безопасности ОПО предназначен для обеспечения возможности прогнозирования и предупреждения возможных аварийных ситуаций, минимизации роли человеческого фактора, в т.ч. в части контрольных и надзорных функций, на основе сбора и аналитической обработки в режиме реального времени информации о контролируемых параметрах отслеживаемых объектов. Например, объектами контроля и анализа результатов функционирования СДК для предприятий нефтегазового комплекса являются технологическое оборудование и технологические процессы добычи, транспортировки, переработки нефти и газа, эксплуатирующий персонал, системы и средства обеспечения ПБ.

Роль СДК определяется ее функциями, к основным из которых относятся (рис. 2.12) [5, 64, 131, 139]:

оперативный сбор данных об основных параметрах технологического процесса, авариях и инцидентах;

сбор и обработка данных производственного контроля, показателей, характеризующих состояние ПБ, информации контроля технического состояния и

диагностики оборудования, информация о наличии нарушений и результатов их устранения;

дистанционный непрерывный мониторинг состояния ОПО в реальном времени;

аналитическая обработка данных дистанционного контроля, прогноз состояния контролируемого объекта, оперативная оценка и прогнозирование рисков нарушения ПБ;

отображение информации о состоянии производственных систем и технологических процессов с необходимым уровнем обобщения и детализации.

Рис. 2.12 Взгляд на роль СДК ПБ [131]

В отличии от обычного контроля, осуществляемого на ОПО (когда государственный надзорный орган в области ПБ, а часто и органы контроля самого предприятия, получают информацию только по факту инцидента или аварии, не обладая достоверной информацией об отклонении состояния системных элементов от нормативного состояния на начальной стадии развития предаварийной ситуации, когда можно предотвратить инцидент или аварию), СДК переводит сам контроль, прозрачность состояния безопасности ОПО, оперативность получения важной информации (о фактах и прогнозах), а также необходимость адекватной реакции на критичные отклонения в совершенно новый временной масштаб, характеризуемый как масштаб реального времени (измеряемый секундами-минутами).

Для вероятностного прогнозирования рисков в СДК осуществляется формальное определение пространства элементарных событий. Это пространство элементарных событий формируют текущие события различных классов. При этом события по степени опасности могут интерпретироваться аналогично сфетофорной сигнализации – «зеленый», «желтый», «красный».

Обобщая изложенную идею, предлагается аналогичным образом определить модель УВМП, используемую для извлечения знаний из процесса мониторинга данных с целью вычисления следующих изначальных исходных данных базовых моделей функционирования «черного ящика»: σ (частоты возникновения источников угроз), β (среднего времени развития угроз) и $T_{восст}$ (среднего времени восстановления нарушенной целостности). Это определение зафиксировано на уровне универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349 «Системная инженерия. Защита информации в процессе системного анализа» (разработанного с авторским участием) – см. рис. 2.13.

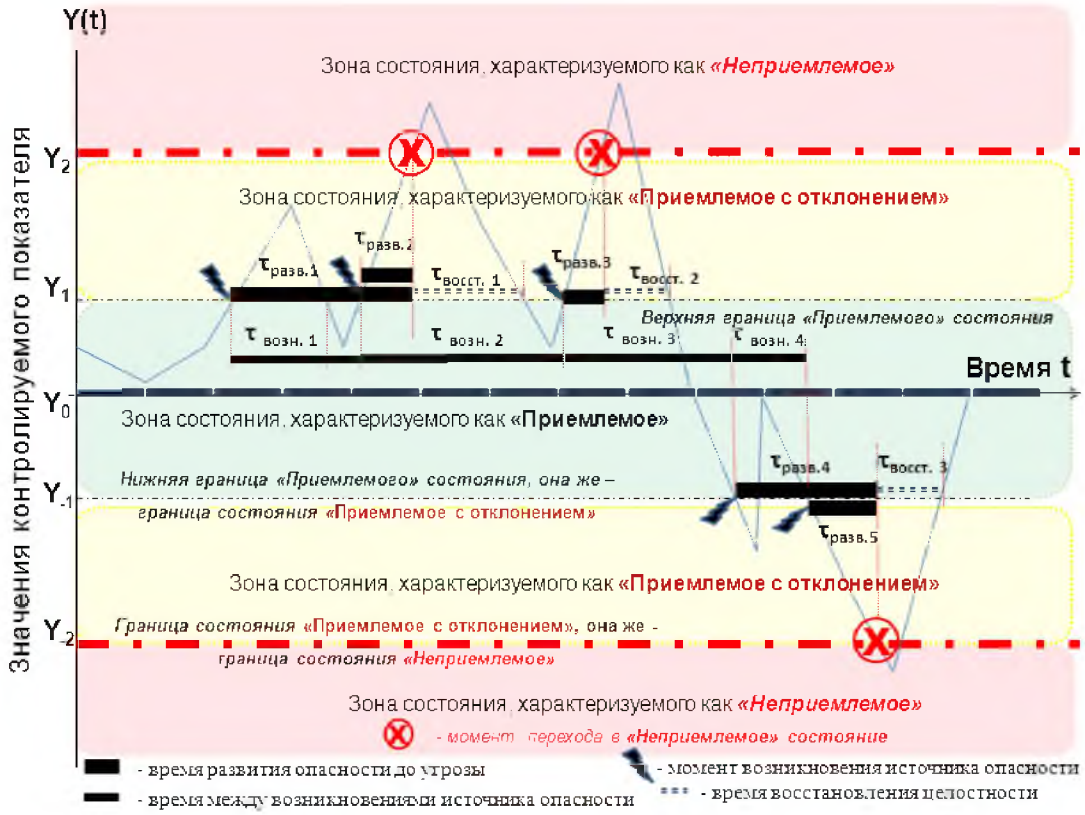


Рис. 2.13 Элементарные состояния контролируемого показателя УВМП во времени и временные характеристики для прогнозирования рисков

Суть предлагаемого к применению УВМП в следующем. В любой момент времени у ответственных лиц, принимающих решение, имеет место формальное представление о том, какое элементарное состояние эксплуатируемой системы «нормально» и «приемлемо», а какое «неприемлемо» и требует управляющей реакции для улучшения. Т. е. на любой момент времени по каждому из критичных показателей (или по их совокупности) можно с однозначной уверенностью определить, что его (их) значения находятся в состоянии, которое может быть охарактеризовано как «Приемлемое» или «Приемлемое с отклонением» (когда за счет определенных организационных или обычных технических усилий по улучшению значения критичного показателя можно удерживать систему от

перехода этого показателя в зону «Неприемлемого» состояния) или как «Неприемлемое» состояние (когда требуются кардинальные решения по восстановлению условий, которые в существующем виде уже не обеспечивают или в ближайшее время при бездействии не будут гарантировать требуемого уровня эффективности системы). Переход критичного показателя в состояние «Неприемлемое» характеризует начало развития угрозы. Граница «Приемлемое с отклонением» характеризует те некоторые уступки по сравнению с наилучшим достигнутым результатом для критичного показателя, которые могут быть допущены с учетом имеющих место неопределенностей.

При этом становятся определенными недостающие исходные данные σ, β, $T_{восст}$. Эти исходные данные формируются по следующему алгоритму, описанному ниже в привязке к регистрируемым значениям критичного показателя на рис. 2.13.

Частота возникновения источников угроз (σ), среднее время развития угроз (β) и среднее время восстановления нарушаемой целостности моделируемой системы ($T_{восст}$), как пример, могут быть определены выражениями:

$$\sigma = 1/[(\tau_{возн.1} + \tau_{возн.2} + \tau_{возн.3} + \tau_{возн.4})/4],$$

$$\beta = (\tau_{разв.1} + \tau_{разв.2} + \tau_{разв.3} + \tau_{разв.4} + \tau_{разв.5})/5,$$

$$T_{восст} = (\tau_{восст.1} + \tau_{восст.2} + \tau_{восст.3})/3.$$

Здесь $\tau_{возн.i}$ – i-й интервал времени между возникновениями источника угроз; $\tau_{разв.j}$ – j-й интервал времени развития угроз с момента возникновения источника угроз до нарушения нормальных условий; $\tau_{восст.m}$ – m-й интервал времени восстановления нарушаемой целостности.

Значения σ, β, $T_{восст}$, получаемые в результате применения предложенного выше алгоритма к статистическим данным контроля на уровне УВМП, являются исходными данными для формального описания моделируемой системы с учетом возможности прогнозирования динамики разнородных событий. Роль в УВМП каждого из учитываемых критичных событий сводится к определению временных значений характеристик σ, β, $T_{восст}$ для использования в последующем в базовых моделях.

2.2.4.2 Теоретическое обоснование возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков» [5, 37, 49, 64, 131, 139, 167]

Применение теоремы 1, получившихся моделей из 2.2.3 позволяет вычислять искомые вероятностные показатели для любого задаваемого периода прогноза, при этом недостающие исходные данные могут быть сформированы с использованием УВМП согласно описанию 2.2.4.1. Если период прогноза пробегает значения от 0 до

бесконечности, из расчетных значений вероятности возможно построить более адекватную ФР времени наработки системы на нарушение целостности (по сравнению с экспоненциальной аппроксимацией), позволяющую при прогнозировании выявлять скрытые знания. Все это – для «черного ящика», т.е. для простой структуры из одного элемента. На практике зачастую возникает необходимость осуществлять вероятностные прогнозы для сложных систем.

Для этого рекомендуется следующий теоретический подход. Для решения практических задач сложная система декомпозируется до составных элементов и подсистем в виде параллельно-последовательной структуры с последующим их сворачиванием при интеграции в систему в целом – см. рис. 2.14 [5, 37, 49, 64, 131, 139, 167].

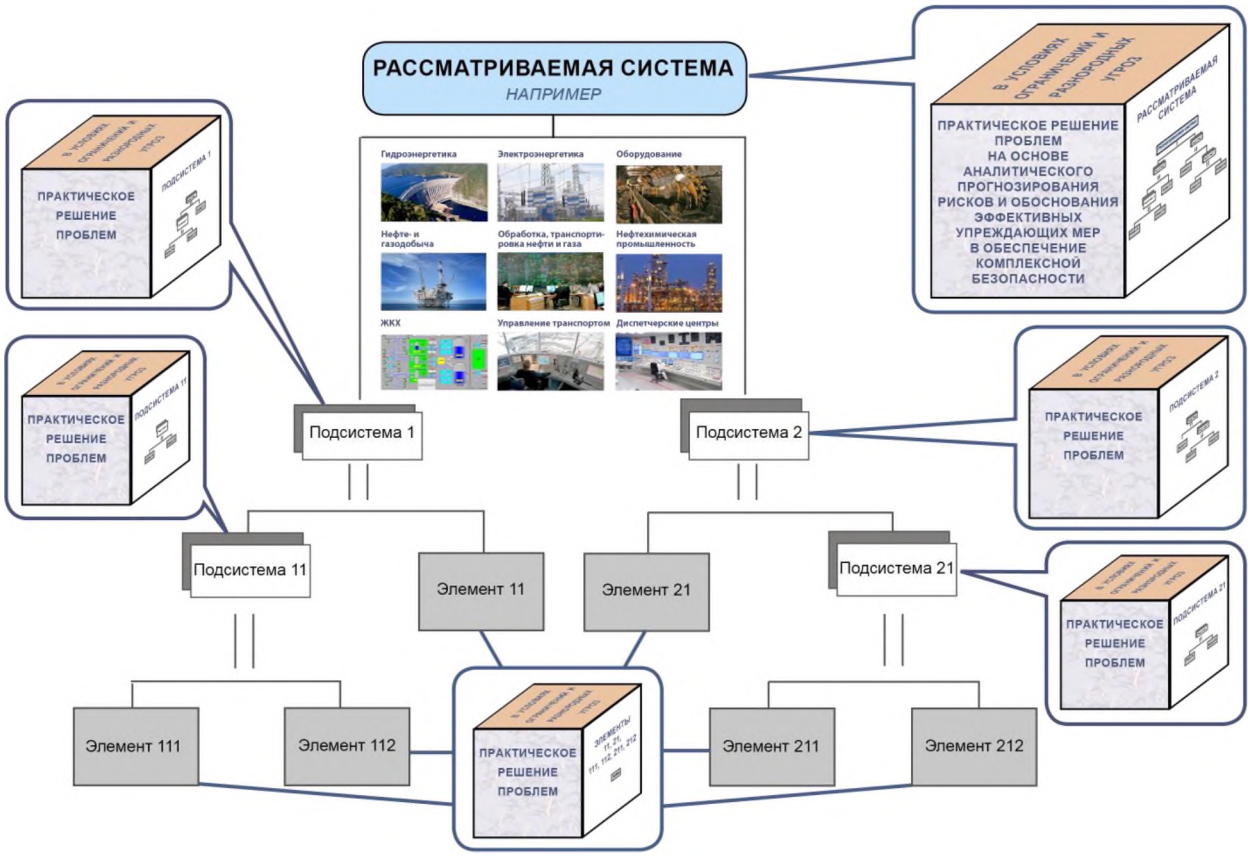


Рис. 2.14 Пример декомпозиции сложной системы до составных элементов для решения практических задач

Для комплексной оценки в приложении к моделируемым системам сколь угодно сложной параллельно-последовательной структуры предлагается использовать следующий алгоритм генерации новых моделей [2, 5, 37, 49, 64, 131, 139, 167].

Примечание. Алгоритм еще в 80-х годах прошлого века проф. Е.С. Вентцель излагала в лекциях по теории вероятностей и в практических упражнениях для студентов [187].

Рассмотрим простейшую структуру из двух независимых элементов, соединенных последовательно, что означает логическое соединение «И» (рис. 2.15), или параллельно, что означает логическое соединение «ИЛИ» (рис. 2.16). Предположение независимости имеет место быть.

Рис. 2.15 Система из последовательно соединенных элементов

Рис. 2.16 Система из параллельно соединенных элементов

Обозначив для i-го элемента функцию распределения (ФР) времени наработки на нарушение целостности через $B_i(t)=P(\tau_i \le t)$, получим:

1) для последовательно соединенных независимых элементов время до возможного нарушения целостности равно минимуму из двух времен τ_i: выхода из строя 1-го или 2-го элементов (т. е. система переходит в состояние нарушенной целостности, когда откажет либо 1-й, либо 2-й элемент). В этом случае для системы в целом ФР времени наработки B(t) на нарушение целостности определяется выражением

$$B(t) = P(\min(\tau 1, \tau 2) \le t)=1- P(\min(\tau 1, \tau 2) > t)=1-P(\tau 1 > t)P(\tau 2 > t)= 1–[1-B1(t)] [1- B2(t)], \quad (2.7)$$

2) для параллельно соединенных независимых элементов (когда оба элемента находятся в функциональном состоянии и при выходе из строя одного из них другой продолжает функционировать) время до возможного нарушения целостности равно максимуму из двух времен τ_i: выхода из строя 1-го и 2-го элементов, т.е. система переходит в состояние нарушенной целостности, когда выйдут из строя оба - и 1-й и 2-й элементы. В этом случае ФР времени наработки на нарушение целостности для системы в целом

$$B(t) = P(\max(\tau 1, \tau 2) \le t)= P(\tau 1 \le t)\, P(\tau 2 \le t)= B1(t)\, B2(t). \quad (2.8)$$

Применяя приведенные рекуррентные соотношения (2.7) – (2.8), можно получать соответствующие оценки для сколь угодно сложной логической структуры с параллельно-последовательным соединением элементов. На выходе моделирования системы – вероятность обеспечения целостности в течение заданного периода времени. Если для каждого элемента просчитать эту вероятность для всех точек $T_{зад.}$ от нуля до бесконечности, то получится траектория ФР времени обеспечения целостности по каждому из элементов (или траектория, не являющаяся ФР, но близко ее аппроксимирующая) в зависимости от расчетных параметров – этот подход реализован, например, в ГОСТ Р 59341-2021, приложение В (см. подробнее подраздел 2.3).

2.2.5 Теоремы о прогнозировании остаточного времени до нарушения целостности моделируемой системы [64, 123, 167]

Осуществляется 4-й шаг предлагаемой логики совершенствования вероятностных моделей, ориентированных на прогнозирование и упреждающее управление рисками в приложениях системной инженерии. Это - прогнозная оценка остаточного времени до нарушения целостности моделируемой системы путем статистического использования базовых моделей. При этом прогнозная оценка осуществляется с использованием дополнительных расчетных показателей, предложенных в 2.2.1:

- прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта;

- среднего остаточного времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- среднего остаточного времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

С учетом практической важности этих показателей для рационального управления рисками в приложениях системной инженерии ниже сформулированы и доказаны три теоремы:

- Теорема 2 об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта;

- Теорема 3 о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- Теорема 4 о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Примечание. Выражение «…нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта» в Теоремах 2 и 3 привязаны к контексту доказательств (см. приложение А). Без искажения общего смысла это выражение в Теоремах 2 и 3 может быть интерпретировано как «…нарушения целостности исследуемого объекта» - см. типовые методики раздела 4.

2.2.5.1 Теорема 2 (об условиях существования прогнозной оценки среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта) и Следствие из нее

Важность прогноза среднего остаточного времени на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона по данным мониторинга поясним на примере функционирования оборудования в опасном производстве. Прогноз осуществляется при выходе значений какого-либо параметра конкретного оборудования за границы рабочего диапазона, оставаясь в границах нормативного диапазона. Рассматривается оборудование, в процессе функционирования которого с использованием средств телеметрии выполняется мониторинг состояния отдельных контролируемых параметров (например, давления, температуры, уровень воды в водосборнике или других критичных параметров). Выделяются границы рабочего и нормативного диапазонов для каждого из параметров – пример фиксации значений параметров во времени отражен на рис. 2.17 (чтобы понять полное родство, можно сравнить с УВМП на рис. 2.13).

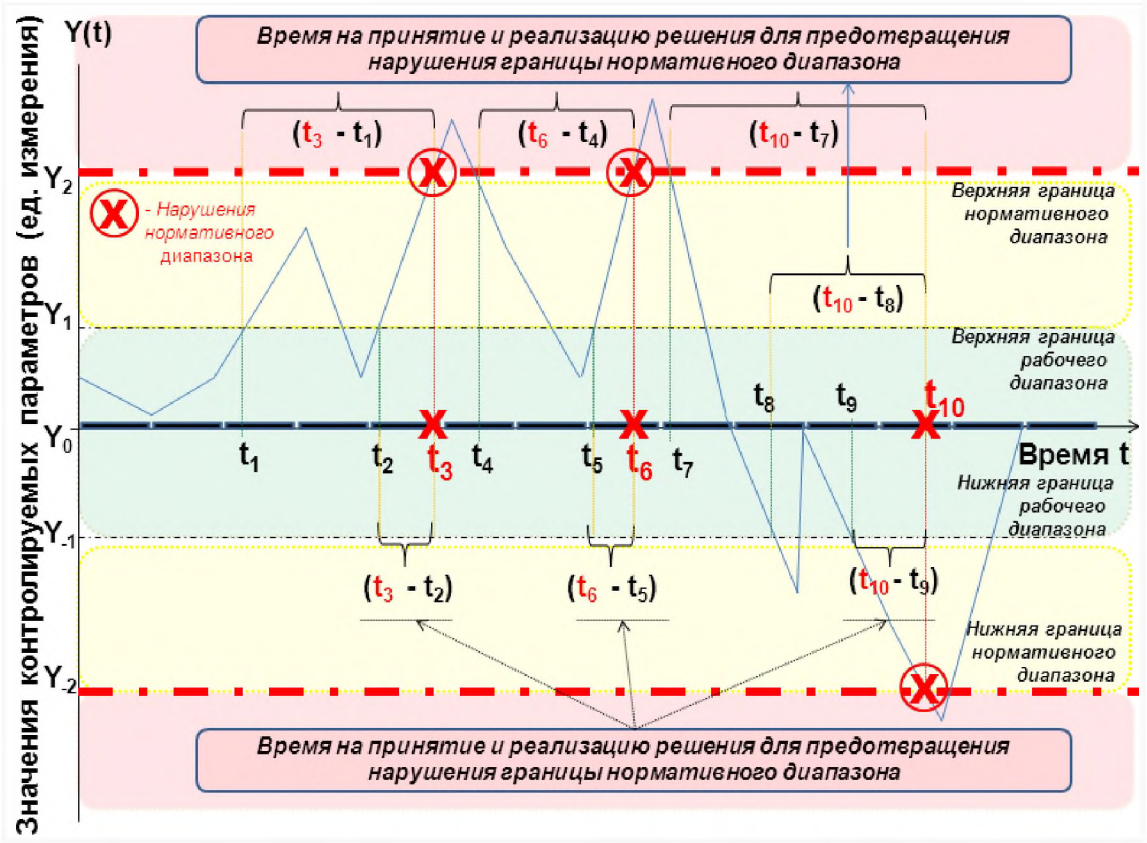


Рис. 2.17 Фиксация значений параметра относительно границ рабочего и нормативного диапазонов (это частный случай УВМП – см. рис. 2.13)

На рисунке 2.17 отражено реальное время, затрачиваемое на принятие и реализацию решения для предотвращения нарушения границы нормативного диапазона (т.е. то время, которое на момент события является на самом деле неизвестным и подлежит определению). Это – по факту из отображаемой статистики, т.е. на практике это данные постфактум, которые иногда могут быть использованы для субъективной ориентации на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона. Вместе с тем, когда отслеживаемых параметров много, в условиях неопределенности и дефицита времени эти и другие отслеживаемые данные позволяют сформировать исходные данные для применения базовых моделей из 2.2.2.2 – 2.2.2.4 для получения более объективных оценок.

В терминах элементарных событий (рассмотренных в 2.2.1) могут быть определены следующие состояния значений отслеживаемого параметра оборудования: в границах рабочего диапазона, за границами рабочего диапазона, оставаясь в границах нормативного диапазона, за границами нормативного диапазона и их привязку к конкретным значениям из каталогов контролируемых параметров оборудования и/или состояния технологических процессов в опасном производстве. По фактическим данным мониторинга осуществляется анализ статистики с определением моментов начала и конца пребывания значений параметра в границах рабочего диапазона, за границами рабочего диапазона, оставаясь в границах нормативного диапазона, и за границами нормативного диапазона (см. рис. 2.7). В результате анализа собираемых данных диспетчер предприятия опасного производства при возникновении признаков возможных нарушений выдает указания мастерам для соответствующих действий по восстановлению функционирования оборудования до приемлемых условий, свойственных рабочему диапазону значений отслеживаемых параметров.

Возможны два варианта содержания используемой статистики в зависимости от ее качества: при наличии и при отсутствии прецедентов выхода значений параметра за границы нормативного диапазона.

Если по используемой статистике было $K \geq 1$ прецедентов перехода параметра за границы нормативного диапазона в моменты t_1, t_2, …,t_K, то ожидаемое среднее время, имеющееся для принятия и реализации предупреждающих мер $T_{\text{упрежд.ож}}$ (т.е. до перехода за границы нормативного диапазона), может быть положено равным

$$T_{\text{упрежд. ож}} = \{[(t_1 - t_{11\ \text{за раб}}) + \ldots + (t_1 - t_{S(1)1\ \text{за раб}})] + \ldots + [(t_K - t_{1K\ \text{за раб}}) + \ldots$$
$$\ldots + (t_K - t_{S(K)K\ \text{за раб}})]\}/[S(1) + \ldots + S(K)],$$

где $t_{s(k)k\ \text{за раб}}$ – момент $s(k)$-го перехода за границы рабочего диапазона, оставаясь в границах нормативного диапазона, для k-го прецедента перехода за границы нормативного диапазона, $s(k)=1,\ldots,S(k)$, $k=1,\ldots,K$;

$S(k)$ – количество переходов за границы рабочего диапазона, оставаясь в границах нормативного диапазона, для k-го прецедента, $k=1,\ldots,K$.

Примечание. В примере на рис. 2.17 моменты t_3, t_6, t_{10} – определяют прецеденты перехода за границы нормативного диапазона (т.е. K=3). Моменты t_1, t_2, t_4, t_5, t_7, t_8, t_9 – определяют моменты перехода в элементарное состояние за границами рабочего диапазона, оставаясь в границах нормативного диапазона, причем моменты t_1, t_2 относятся к 1-му прецеденту перехода параметра в элементарное состояние за границами нормативного диапазона (k=1, $S(1)$=2), t_4, t_5 относятся ко 2-му прецеденту перехода параметра в элементарное состояние за границами нормативного диапазона (k=2, $S(2)$=2), t_7, t_8, t_9 относятся к 3-му прецеденту перехода параметра в элементарное состояние за границами нормативного диапазона (k=3, $S(3)$=3). $S(1)+S(2)+S(3)=7$.

Если какая-либо специфика в поведении параметра отсутствует, то учитывается вся предыдущая статистика:

$$T_{\text{упрежд. ож}} = \{[(t_3-t_1)+(t_3-t_2)]+[(t_6-t_4)+(t_6-t_5)]+[(t_{10}-t_7)+(t_{10}-t_8)+(t_{10}-t_9)]\}/7.$$

В этом случае учитываются как выходы за пределы рабочего диапазона, так и возвращения в пределы нормативного диапазона, т.е. статистика на рис. 2.17 учитывает время с моментов t_1, t_2 до 1-го прецедента в момент t_3, с моментов t_4, t_5 до 2-го прецедента в момент t_6, с моментов t_7, t_8, t_9 до 3-го прецедента в момент t_{10}.

Для учета специфики поведения параметра возможен учет предыдущего состояния, из которого значения параметра вышли за границы рабочего диапазона, оставаясь в границах нормативного диапазона. Например, на угольной шахте это касается критичного параметра «Уровень воды в водосборнике», когда при наполнении водосборника, т.е. при выходе значений уровня воды за границы рабочего диапазона, время до выхода значений параметра за границы нормативного диапазона может измеряться десятками минут. Тогда как при освобождении водосборника, т.е. после возвращения значений уровня воды из-за границ нормативного диапазона, время до следующего выхода значений параметра опять за границы нормативного диапазона может измеряться часами и десятками часов. При учете подобной специфики возможны случаи:

- если предыдущее состояние было в границах рабочего диапазона, то ожидаемое среднее время, имеющееся для принятия и реализации предупреждающих мер, полагается равным $T_{\text{упрежд.ож}} = [(t_3-t_1)+(t_3-t_2)+(t_6-t_5)+(t_{10}-t_8)+(t_{10}-t_9)]/5$.

Примечание. В этом случае статистика на рис.2.17 учитывает лишь выходы за пределы рабочего диапазона в моменты t_1, t_2, t_5, t_8, t_9;

- если предыдущее состояние было за границами нормативного диапазона, то ожидаемое среднее время, имеющееся для принятия и реализации предупреждающих мер, полагают равным $T_{упрежд.ож} = [(t_6 - t_4) + (t_{10} - t_7)]/2$.

Примечание. В этом случае статистика на рис. 2.17 учитывает лишь возвращения в пределы нормативного диапазона в моменты t_4, t_7.

Если же по используемой статистике не было ни одного прецедента перехода параметра в элементарное состояние за границами нормативного диапазона (т.е. K=0), но были $U \geq 1$ прецедентов перехода значений параметра за границы рабочего диапазона, оставаясь в границах нормативного диапазона, то выполняются следующие действия:

- устанавливается допустимый риск выхода значений этого параметра за границы нормативного диапазона в течение заданного периода прогноза $T_{зад}$, т.е. задается допустимый уровень вероятности $R_{доп}$ ($T_{зад}$). В терминах риска это означает установление формальной границы перехода параметра за границы нормативного диапазона из состояния за границами рабочего диапазона, оставаясь в границах нормативного диапазона;

- прогнозируемое среднее время $T_{упрежд. прогноз}$ на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона оценивается как среднее время до перехода из состояния за границами рабочего диапазона (оставаясь в границах нормативного диапазона) в состояние за границами нормативного диапазона. Отсутствие статистики выхода за границы нормативного диапазона требует использования вероятностного моделирования.

В этом случае применима «Модель «черного ящика» при отсутствии какого-либо контроля» (из 2.2.2.1). При ее использовании оказывается справедливой предлагаемая Теорема 2. Нарушение целостности моделируемой системы при использовании УВМП состоит в переходе в «Неприемлемое» состояние. При использовании модели из 2.2.2.1 лицо, принимающее решение о принятии упреждающих мер, придерживается предположения о худшем развитии событий, оценивая снизу – какое можно ожидать время до возможного нарушения нормативного диапазона с момента установления (или восстановления) изначально приемлемого состояния критичного параметра. В качестве моделируемой системы, представимой в виде «черного ящика», выступает такая сущность, как критичный параметр мониторируемого объекта, управление которым осуществляется путем принятия упреждающих мер на основе анализа текущих значений отслеживаемого параметра и нижней оценки ожидаемого остаточного времени до нарушения установленного для этого параметра нормативного диапазона допустимых значений.

Теорема 2 (об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение возможного

нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта).

Пусть для моделируемой системы соблюдается условие или принимается предположение о реальной или гипотетической повторяемости возможных событий и их независимости, а элементарные состояния отслеживаемого критичного параметра характеризуются тремя зонами с использованием УВМП (из 2.2.4.1): «Приемлемое», «Приемлемое с отклонением», «Неприемлемое». Причем для системы установлен допустимый уровень риска нарушения ее целостности $R_{доп}$ ($0 < R_{доп} < 1$). Тогда при использовании «Модели «черного ящика» при отсутствии какого-либо контроля» (из 2.2.2.1) с задаваемой расчетной точностью ε ($0.01R_{доп} \leq \varepsilon \leq 0.1R_{доп}$) прогнозная нижняя оценка x_{0min} среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта существует лишь в определенной рассчитываемой области доверительной вероятности. В этой рассчитываемой области доверительной вероятности прогнозная нижняя оценка среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона x_{0min}, является единственной ненулевой и может быть вычислена как результат решения следующей обратной задачи: найти такое минимальное среднее время развития угроз x_{0min}, при котором риск нарушения целостности моделируемой системы будет достигать значение установленного допустимого уровня риска $R_{доп}$ с заданной точностью ε. При этом дополнение до 1 соответствующего точке x_{0min} значения риска характеризует достижимую доверительную вероятность для этой вычисленной прогнозной нижней оценки среднего остаточного времени. Доказательство Теоремы 2 приведено в приложении А.2.

Теорема 2 действует при использовании модели из 2.2.2.1. В этом случае лицо, принимающее решение о принятии упреждающих мер, придерживается предположения о худшем развитии событий, оценивая снизу – какое можно ожидать время до возможного нарушения нормативного диапазона с момента установления (или восстановления) изначально приемлемого состояния критичного параметра. Такие параметры модели, как $T_{меж}$ (время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы) и $T_{диаг}$ (среднее время системной диагностики целостности моделируемой системы) никакой роли не играют, т.к. искомая оценка для остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона достигается до наступления какой-либо очередной диагностики, т.е. ФР времени до нарушения целостности моделируемой системы $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}) = R_{наруш}(\sigma, \beta, T_{зад})$. Иными словами – это оценка остаточного

времени, если не предпринимать никаких упреждающих мер противодействия угрозам (в предположении, что все идет без какой-либо реакции на переходы в состояние «Приемлемое с отклонением»). Следует отметить, что прогноз остаточного времени осуществляется для определения не только и не столько минимального времени до события, связанного с переходом значений критичного параметра в состояние «Неприемлемое» - оно может не наступить вовсе из-за оперативной реакции при переходах в состояние «Приемлемое с отклонением» для недопущения перехода в состояние «Неприемлемое». И тут приемлема «Модель «черного ящика» при реализации технологии периодического системного контроля» (из 2.2.2.2). Как следствие, возникает потребность в решении двух практических вопросов: «Какой по длительности выбирать период между диагностиками целостности системы?» и «Каково среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам?».

Второй вопрос по сути состоит в том, чтобы понять, как изменится остаточное время до перехода в состояние «Неприемлемое», если реагировать на отклонения оперативно? Ответ на этот второй вопрос дает предлагаемая в 2.2.5.2 Теорема 3 (о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам).

Первый вопрос – практический, слишком частая диагностика отнимает вычислительные ресурсы системы, поэтому желательно выбирать максимально возможную длительность периода между диагностиками, но так, чтобы риск нарушения целостности системы был не ниже допустимого. Ответ на этот вопрос вытекает из нижеследующего Следствия из Теоремы 2.

Следствие из Теоремы 2. Следствие из Теоремы 2 (об ограничениях при выборе периода между диагностиками целостности системы, ориентированного на непревышение допустимого риска нарушения целостности системы)**.**

Пусть для моделируемой системы выполняются условия Теоремы 2 и дополнительно для моделирования приемлема «Модель «черного ящика» при реализации технологии периодического системного контроля» (из 2.2.2.2). Тогда при выборе периода между диагностиками целостности моделируемой системы $T_{между}$, ориентированного на непревышение задаваемого допустимого риска $R_{доп}=0.1$, необходимо руководствоваться следующими ограничениями:

когда средний период между моментами возникновения угроз σ^{-1} на порядок меньше нижней оценки среднего остаточного времени на принятие упреждающих мер x_{0min} ,

вычисленной по результатам применения Теоремы 2 (т.е. для $\sigma^{-1}=0.1x_{0min}$), выбираемый период между диагностиками целостности моделируемой системы $T_{между}$ по длительности не должен превышать 0.2 от вычисленного значения x_{0min};

когда средний период между моментами возникновения угроз σ^{-1} вдвое меньше нижней оценки среднего остаточного времени на принятие упреждающих мер x_{0min} , вычисленной по результатам применения Теоремы 2 (т.е. для $\sigma^{-1}=0.5x_{0min}$), выбираемый период между диагностиками целостности моделируемой системы $T_{между}$ по длительности не должен превышать 0.39 от вычисленного значения x_{0min};

когда средний период между моментами возникновения угроз σ^{-1} равен нижней оценке среднего остаточного времени на принятие упреждающих мер x_{0min} , вычисленной по результатам применения Теоремы 2 (т.е. для $\sigma^{-1}=x_{0min}$), выбираемый период между диагностиками целостности моделируемой системы $T_{между}$ по длительности не должен превышать 0.53 от вычисленного значения x_{0min};

когда средний период между моментами возникновения угроз σ^{-1} в 5 раз больше нижней оценки среднего остаточного времени на принятие упреждающих мер x_{0min} , вычисленной по результатам применения Теоремы 2 (т.е. для $\sigma^{-1}=5x_{0min}$), выбираемый период между диагностиками целостности моделируемой системы $T_{между}$ по длительности не должен превышать вычисленного значения x_{0min} в 1.3 раза;

когда средний период между моментами возникновения угроз σ^{-1} в 10 раз больше нижней оценки среднего остаточного времени на принятие упреждающих мер x_{0min} , вычисленной по результатам применения Теоремы 2 (т.е. для $\sigma^{-1}=10x_{0min}$), выбираемый период между диагностиками целостности моделируемой системы $T_{между}$ по длительности не должен превышать вычисленного значения x_{0min} в 1.9 раза.

Примечание. Значение задаваемого допустимого уровня $R_{доп}=0.1$ непринципиально, оно выбрано лишь для иллюстрации предлагаемого подхода к определению ограничений на основе выявляемых закономерностей (кроме того, такой уровень рекомендуется ГОСТ Р 59991-2022). Выявленные ниже закономерности позволяют установить ограничения, аналогичные по логике их определения, для любого задаваемого значения $R_{доп}$.

Доказательство Следствия из Теоремы 2 опирается на выявленные закономерности и приведено в приложении А.3.

2.2.5.2 Теорема 3 (о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам)

Теорема 3. Пусть для моделируемой системы соблюдается условие или принимается предположение о реальной или гипотетической повторяемости возможных событий и их

независимости, а элементарные состояния отслеживаемого критичного параметра характеризуются тремя зонами с использованием УВМП (из 2.2.4.1): «Приемлемое», «Приемлемое с отклонением», «Неприемлемое». Тогда среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам может быть определено как математическое ожидание ФР времени до нарушения целостности моделируемой системы, вычисляемое с использованием «Модели «черного ящика» при реализации технологии периодического системного контроля» (из 2.2.2.2).

Доказательство Теоремы 3 приведено в приложении А.4.

Положения Теоремы 3 в полной мере применимы, если использовать результаты применения Теоремы 1 о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности моделируемой системы (2.3). В этом случае расчет $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, t)$ заменяется на расчет $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст.}}, t)$, учитывающий различия во временах диагностики и восстановления целостности моделируемой системы.

2.2.5.3 Теорема 4 (о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам)

Теоремы 2 и 3 действуют при использовании моделей «черного ящика» из 2.2.2.1 и 2.2.2.2, т.е. не для сложной системы, логически состоящей из составных элементов.

Для сложной системы возникает тот же самый актуальный вопрос: «Каково среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам?» При этом по-прежнему элементарные состояния отслеживаемых критичных параметров в каждом из составных элементов сложной системы характеризуются тремя зонами с использованием УВМП: «Приемлемое», «Приемлемое с отклонением», «Неприемлемое» (со своими границами нормативных диапазонов).

Для этого случая применимо теоретическое обоснование возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков», осуществленное в 2.2.4.2.

Соответствующий ответ на сформулированный выше вопрос дает предлагаемая Теорема 4 (о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам).

Теорема 4. Пусть для решения практических задач моделируемая сложная система допускает декомпозицию до составных элементов и подсистем в виде параллельно-последовательной структуры с последующим их сворачиванием при интеграции с использованием логических соединений «И», «ИЛИ» (согласно 2.2.4.2). Для каждого из элементов соблюдается условие или принимается предположение о реальной или гипотетической повторяемости возможных событий и их независимости, а элементарные состояния отслеживаемых критичных параметров характеризуются тремя зонами с использованием УВМП (из 2.2.4.1): «Приемлемое», «Приемлемое с отклонением», «Неприемлемое». Тогда с использованием результатов Теоремы 3 среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам может быть определено как математическое ожидание ФР времени до нарушения целостности интегрированной моделируемой сложной системы, вычисляемой с использованием «Модели «черного ящика» при реализации технологии периодического системного контроля» (из 2.2.2.2).

Доказательство Теоремы 4 приведено в приложении А.5.

Таким образом, применения предложенных Теоремы 1 (о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности), универсальной вспомогательной модели показателей, используемой для извлечения знаний из процесса мониторинга данных, Теоремы 2 (об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта) и Следствия из нее, Теоремы 3 (о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам), теоретического обоснования возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков», и Теоремы 4 (о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам) позволили осуществить теоретические усовершенствования существующих моделей и тем самым сформировать в этом разделе базовые модели математического обеспечения для анализа системных элементов, сложных систем и процессов с использованием ВС и КС. При разработке далее программных решений используются именно эти усовершенствованные базовые модели: «Модель «черного ящика» при отсутствии какого-либо контроля»,

«Модель «черного ящика» при реализации технологии периодического системного контроля», модель сложной системы, интегрируемой из «черных ящиков».

С учетом основных положений Теорем 1 – 4 с использованием ВС и КС наряду с рисками, определенными в 2.2.1, при разработке программных решений предлагается дополнительно вычислять следующие расчетные показатели:

- прогнозную оценку среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта;

- среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

2.3 Основные положения по моделированию, прогнозированию и упреждающему управлению рисками в национальных стандартах и их реализация [5, 136, 149, 167]

В рамках реализации 5-го шага в логике построения математического обеспечения создаваемого прототипа технологии поддержки риск-ориентированной системной инженерии для ВС и КС, основные положения по моделированию, прогнозированию и упреждающему управлению рисками, разработанные и описанные в подразделах 2.2 – 2.3, реализованы в 19 национальных стандартах:

ГОСТ Р 58494-2019 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов»;

ГОСТ Р 59329-2021 «Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы»;

ГОСТ Р 59331-2021 «Системная инженерия. Защита информации в процессе управления инфраструктурой системы»;

ГОСТ Р 59333-2021 «Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы»;

ГОСТ Р 59334-2021 «Системная инженерия. Защита информации в процессе управления качеством системы»;

ГОСТ Р 59335-2021 «Системная инженерия. Защита информации в процессе управления знаниями о системе»;

ГОСТ Р 59336-2021 «Системная инженерия. Защита информации в процессе планирования проекта»;

ГОСТ Р 59337-2021 «Системная инженерия. Защита информации в процессе оценки и контроля проекта»;

ГОСТ Р 59338-2021 «Системная инженерия. Защита информации в процессе управления решениями»;

ГОСТ Р 59339-2021 «Системная инженерия. Защита информации в процессе управления рисками для системы»;

ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы»;

ГОСТ Р 59342-2021 «Системная инженерия. Защита информации в процессе измерений системы»;

ГОСТ Р 59347-2021 «Системная инженерия. Защита информации в процессе определения архитектуры системы»;

ГОСТ Р 59356-2021 «Системная и программная инженерия. Защита информации в процессе сопровождения системы»;

ГОСТ Р 59349-2021 «Системная инженерия. Защита информации в процессе системного анализа»;

ГОСТ Р 59355-2021 «Системная и программная инженерия. Защита информации в процессе функционирования системы»;

ГОСТ Р 59353-2021 «Системная инженерия. Защита информации в процессе передачи системы»;

ГОСТ Р 59354-2021 «Системная инженерия. Защита информации в процессе аттестации системы»;

ГОСТ Р 59357-2021 «Системная инженерия. Защита информации в процессе изъятия и списания системы».

Разработанные в 2.2 и 2.3 методы и модели, усовершенствованные на основе доказанных теорем 1-4, реализованные в перечисленных стандартах, ориентированы на широкомасштабное практическое использование. Так, относительно ГОСТ Р 58494-2019 имеет смысл привести следующие комментарии к практическим примерам использования УВМП в системе дистанционного контроля (СДК) в угольной шахте (детальные примеры приведены далее в разделе 4 диссертации). Рассмотрим вариант применения УВМП для описания СДК, отслеживающей наряду с другими параметрами оборудования расход воды, подаваемой в вакуум-насос. В начальный период опытной эксплуатации СДК устанавливаемые значения рабочих и нормативных диапазонов подлежат адекватной настройке и интерпретации, а наблюдаемые критичные отклонения в значениях параметров оборудования могут по инерции игнорироваться (т.е. не влекут за собой надлежащей оперативной реакции). Разработка Теорем 2, 3 помогает на шахтах ответить на важный

практический вопрос: «Сколько времени есть у мастера для устранения критичных отклонений?».

Ответ на этот вопрос состоит в следующем. Набранная в СДК статистика видеоданных позволяет в ряде случаев определять время, которое есть у мастера для устранения критичных отклонений, усредняя реальное время перехода в нарушение нормативов – см. фрагмент для анализа видеоданных на рис. 2.18 для отдельного оборудования. Для мастера нахождение в «желтой» зоне (потребление воды от 330 до 400 л/мин.) - это ожидаемое время для оперативного восстановления целостности контролируемого оборудования.

Вместе с тем, помесячное изменение значений параметра на рис. 2.19 свидетельствует о том, что диапазон «желтой» зоны – узок (от 60 до 62 м^3/мин. для шахты). В результате критичное нарушение наступает практически внезапно (в теории надежности это определяется как «внезапный отказ»).

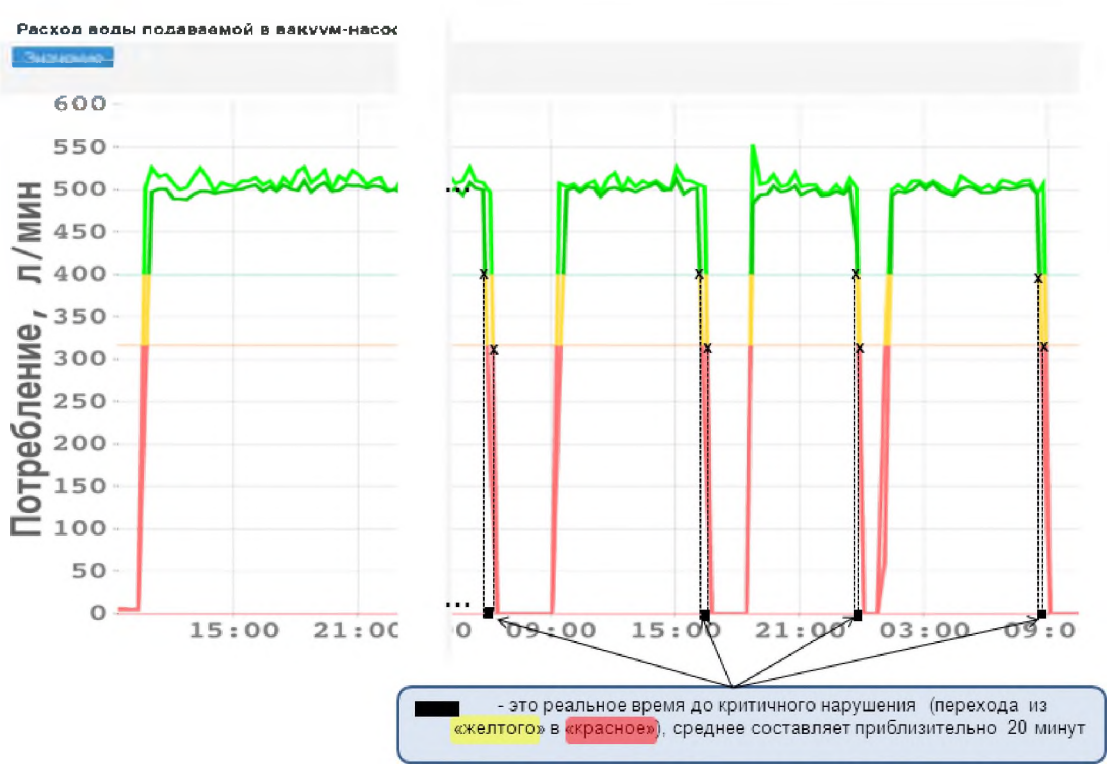


Рис. 2.18 Оценки ожидаемого времени для оперативного восстановления целостности контролируемого оборудования по видеоданным

Рис. 2.19 «Желтый» диапазон узок, в результате критичное нарушение наступает практически внезапно

Если принятые нормативы обоснованы, то внезапный переход в «красную» зону 2-3 раза в неделю может интерпретироваться как «аварийная ситуация» или же лишь как временно неработоспособен (*«желто-оранжевая»* зона), т.к. на практике аварийной ситуации не было. Т.е., если параметры находятся «за пределами нормы», но обеспечивается временная работоспособность элемента, могут иметь место отдельные временные нарушения требований эксплуатации или предпосылки к ним или инциденты, не переходящие в предаварийное состояние или аварии, при этом штатными методами оперативного восстановления целостности производства (например, методами текущего ремонта) обеспечивается временное состояние работоспособности, но требуется принятие упреждающих или регламентных мер технического обслуживания и обеспечения надежности до состояния «в рабочих пределах» *(«зеленая»* зона). Это означает, что внедрение СДК обостряет проблему адекватного обоснования нормативных диапазонов для оборудования, интерпретации получаемых результатов, их сравнения с реальностью, учета и анализа причин возникновения критичных отклонений.

Съемы данных СДК позволяют совместно с временными характеристиками текущего ремонта формировать исходные данные для вероятностного моделирования. Так, рис. 2.20 свидетельствует о длительной (вначале) и оперативной (в конце) реакции на температуру подшипника, вышедшей за пределы рабочего диапазона. Тем не менее, с учетом анализа причин такой разницы усреднение этих характеристик дает представление об ожидаемом времени восстановления целостности (что позволяет автоматически формировать соответствующие исходные данные для моделирования). Само моделирование за счет комплексного учета различных параметров и прогнозирования рисков позволит более точно определять время, которое есть у мастера для устранения критичных отклонений.

Рис. 2.20 Примеры времени восстановления рабочего диапазона по видеоданным

Резюме из приведенных комментариев: определение нормативных диапазонов подлежит дополнительному обоснованию с применением доказанных теорем с учетом ожидаемого времени до критичного нарушения (перехода из «желтого» в «красное») и имеющихся практических возможностей по восстановлению целостности системы – см. методические предложения в подразделе 4.5 диссертации.

Те же самые усовершенствованные базовые модели широко применимы и для иных областей приложения (см. прикладные примеры в разделах 3-5). Тем самым на приведенном выше примере проиллюстрирована практичность теоретических проработок подразделов 2.2 и 2.3 до уровня математического обеспечения создаваемого прототипа технологии поддержки риск-ориентированной системной инженерии.

Авторское участие в разработке вышеперечисленных стандартов в части основных положений по моделированию, прогнозированию и упреждающему управлению рисками подтверждено актами о реализации от соразработчиков стандартов - ООО НИИПМС и ФБУ «НТЦ Энергобезопасность» - см. Приложение В.

Стандартизованные методы и модели, реализованные в этих стандартах, внедрены в практику работы национального и межнационального технического комитета «Информационные технологии» (ТК-МТК-022) в части рекомендаций по использованию созданных методов, моделей и демонстрационных примеров системной инженерии (в т.ч. путем ссылок на вышеперечисленные стандарты ГОСТ Р 58494, ГОСТ Р 59329 - ГОСТ Р 59357) в новых национальных стандартах последних лет, адаптированных с учетом международных стандартов:

ГОСТ Р 56920-2024 «Системная и программная инженерия. Тестирование программного обеспечения. Общие положения (ISO/IEC/IEEE 29119-1:2022, NEQ)»;

ГОСТ Р 71303-2024 «Системная и программная инженерия. Возможности программных инструментариев для организационного управления инцидентами. Общие положения (ISO/IEC 23531:2020, NEQ)»;

ГОСТ Р 71439-2024 «Системная и программная инженерия. Методы и инструментарии продуктовой линейки программных средств и систем. Общие положения (ISO/IEC 26580:2021, NEQ)»;

ГОСТ Р 71304-2024 «Системная и программная инженерия. Гарантии обеспечения качества систем и программных средств. Основные понятия и термины (ISO/IEC/IEEE 15026-1:2019, NEQ)»;

ГОСТ Р 71440-2024 «Информационные технологии. Оценка процессов. Руководство по определению рисков в процессах (ISO/IEC TR 33015:2019, NEQ)»;

ГОСТ 71438-2024 «Информационные технологии. Оценка процессов. Система измерения процессов для оценки их возможностей (ISO/IEC 33020:2019, NEQ)»;

ГОСТ Р 57100-2025 «Системная и программная инженерия. Описание архитектуры (ISO/IEC/IEEE 42010:2022, NEQ)»;

ГОСТ Р 57193-2025 «Системная и программная инженерия. Процессы жизненного цикла систем (ISO/IEC/IEEE 15288:2021, NEQ)»;

ГОСТ Р 71998-2025 «Информационные технологии. Требования и оценка качества систем и программного обеспечения. Определение качества ИТ-услуг (ISO/IEC TS 25025:2021, NEQ)».

Это подтверждено актом ТК-МТК-022 о применении результатов исследований - см. Приложение В. В целом авторский вклад в математическое обеспечение создаваемого прототипа технологии поддержки риск-ориентированной системной инженерии с использованием ВС и КС представлен на рис. 2.21 [167].

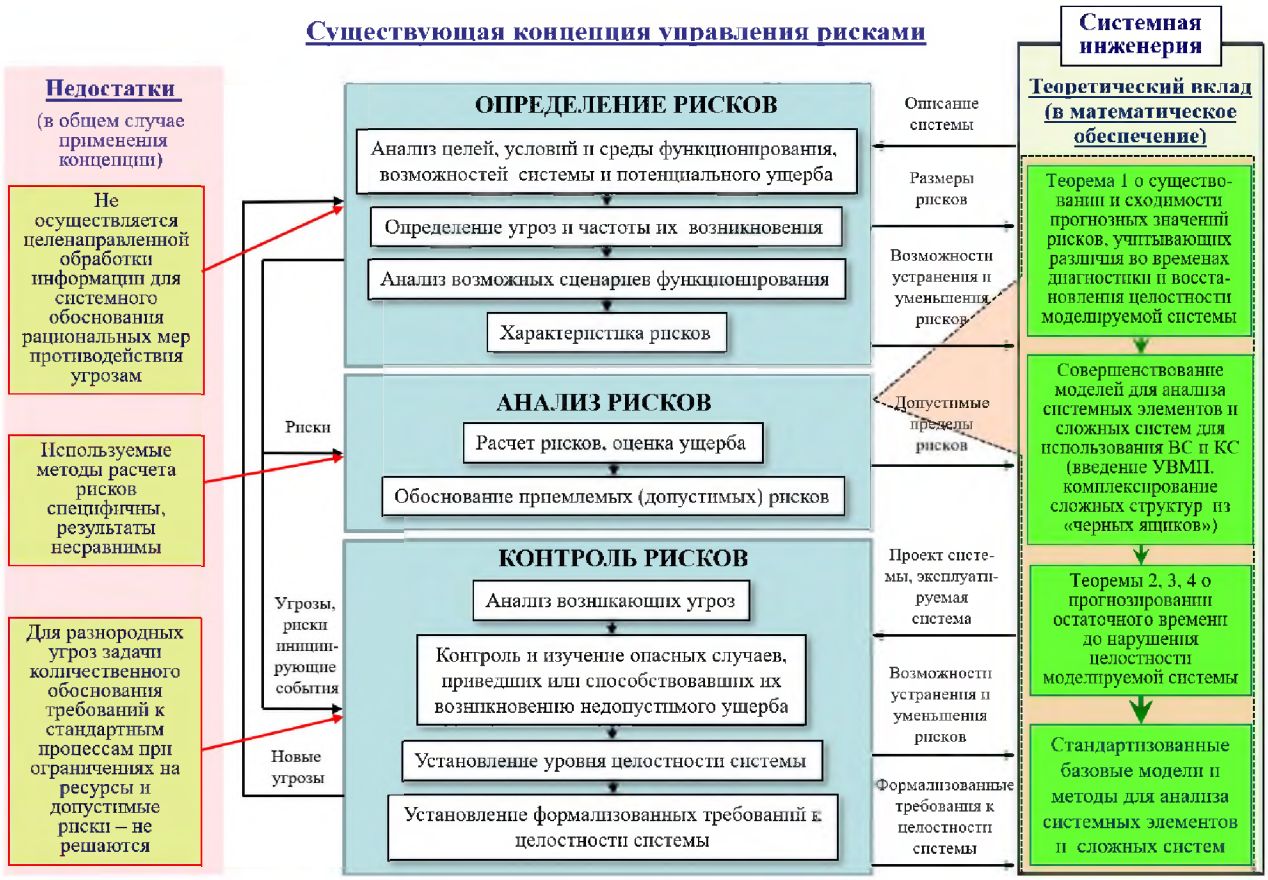


Рис. 2.21 Теоретический вклад в математическое обеспечение создаваемого прототипа технологии поддержки риск-ориентированной системной инженерии

Таким образом, предложенные основные положения по моделированию, прогнозированию и упреждающему управлению рисками реализованы в национальном стандарте ГОСТ Р 58494 для систем дистанционного контроля опасных производственных объектов, утвержденном Росстандартом в 2019г. и введенном в действие с 2020г., и 18 национальных стандартах системной инженерии ГОСТ Р 59329, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59347, ГОСТ Р 59349, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357 в части моделирования стандартных процессов приобретения и поставки продукции и услуг, управления инфраструктурой системы, управления человеческими ресурсами, управления качеством системы, управления знаниями о системе, планирования проекта, оценки и контроля проекта, управления решениями, управления рисками для системы, управления информацией, измерений, определения архитектуры системы, системного анализа, передачи, аттестации, функционирования и сопровождения системы, изъятия и списания системы. Стандарты по системной инженерии утверждены Росстандартом и введены в действие с 2021 года.

2.4 Программные решения для моделирования стандартизованных процессов системной инженерии

Программные решения для моделирования стандартизованных процессов системной инженерии базируются на программах для ЭВМ, созданных в период 2004-2018гг. (см. подраздел 2.1) и на усовершенствованном математическом обеспечении с применением Теорем 1 – 4 (см. подразделы 2.2, 2.3).

Разработки 2004-2018 гг. включают 9 комплексов программ [168 - 176]:

«Моделирование процессов в жизненном цикле систем "Моделирование процессов" - "ноу-хау"» (Свидетельство о государственной регистрации программы для ЭВМ №2004610858);

«Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2006610219);

«Программно-инструментальный комплекс оценки качества функционирования информационных систем через Интернет «КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008612348);

«Программно-инструментальный комплекс сопровождения систем менеджмента качества «OPISys-КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008614525);

«Программно-вычислительный комплекс оценки качества производственных процессов» (Свидетельство о государственной регистрации программы для ЭВМ № 2010614145);

«Комплекс для оценки качества информационных и административно-управленческих процессов при функционировании электронного правительства (КОК-ЭП)» (Свидетельство о государственной регистрации программы для ЭВМ № 2010617017);

«Удаленная аналитическая поддержка информирования о вероятностно-временных показателях функционирования системы и ее элементов при реализации риск-ориентированного подхода» (Свидетельство о государственной регистрации программы для ЭВМ №2018617949);

«Удаленное обоснование требований к средствам и условиям обеспечения качества функционирования «умных» систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618572);

«Удаленное вероятностное прогнозирование качества функционирования информатизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618686).

Дополнительно в период 2019 – 2025гг. созданы 4 программы для ЭВМ [177 – 180]:

«Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021»;

«Модуль формирования отчетности по результатам вероятностного прогнозирования рисков для сложной системы с последовательным соединением элементов»;

«Модуль проверки достаточности данных для прогнозирования рисков по статистике»;

«Модель технологической поддержки риск-ориентированной системной инженерии».

Для подключения базовых моделей и проведения расчетов сначала формируются исходные данные, каковыми в общем случае являются:

– частота возникновения источников угроз в моделируемой системе;

– среднее время активизации (развития) угроз с момента возникновения источников угроз до нарушения установленных требований по обеспечению целостности моделируемой системы или до инцидента;

– время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

– среднее время системной диагностики целостности моделируемой системы;

– среднее время восстановления нарушенной целостности системы;

– задаваемая длительность периода прогноза.

В свою очередь расчеты проводятся в интересах получения расчетных показателей и их зависимостей от изменения исходных данных. Основными расчетными показателями являются:

- риск нарушения целостности моделируемой системы за период прогноза при реализации основных функциональных требований;

- риск нарушения дополнительных специфических требований к моделируемой системе за период прогноза;

- интегральный риск нарушения целостности моделируемой системы за период прогноза при реализации основных функциональных требований и дополнительных специфических требований;

- прогнозная оценка среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра;

- среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра при своевременном принятии упреждающих мер противодействия угрозам;

- среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Системным аналитиком определяется тип модели:

- «Модель «черного ящика» при отсутствии какого-либо контроля» (см. 2.2.2.1);

- «Модель «черного ящика» при реализации технологии периодического системного контроля» (см. 2.2.2.2);

- модель сложной системы, интегрируемой из «черных ящиков» (см. 2.2.4.2).

Для модели сложной системы, интегрируемой из «черных ящиков», строится или выбирается из заготовок архитектура формализованной сложной системы в терминах «И», «ИЛИ» логического построения последовательно-параллельной структуры. После этого для каждого из составных элементов формируются исходные данные, перечисленные выше. Формирование исходных данных осуществляется из данных мониторинга в реальном времени (для этого дополнительно разрабатываются средства трансформации данных из формата мониторинга в формат моделей) или вручную.

После этого с использованием созданных программных решений осуществляется непосредственно моделирование, автоматическое формирование результатов расчетов. Получаемые результаты позволяют решать задач системной инженерии, такие, как задачи:

- анализа альтернатив в заданных процессах системной инженерии;

- оценки критичности влияния различных параметров заданных процессов системной инженерии на поведение системы;

- прогнозирования интегрального риска;

- обоснования требований к допустимым значениям исходных данных для упреждающего управления рисками.

Программный «Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021» реализует алгоритм, описанный в 2.2.4.1 с применением Теоремы 3 и стандартизованный в ГОСТ Р 59349-2021 «Системная инженерия. Защита информации в процессе системного анализа». С учетом элементарных состояний контролируемого показателя УВМП во времени и временных характеристик, отслеживаемых при мониторинге, в данной программе определяются следующие исходные данные для моделирования: частота возникновения источников угроз (σ), среднее время развития угроз (β) и среднее время восстановления нарушаемой целостности моделируемой системы

($T_{восст}$). Эти данные наряду с другими, определяемыми организационными регламентами предприятия, подаются на вход в программную «Модель технологической поддержки риск-ориентированной системной инженерии» (см. подробнее в 3.5). При этом достаточность данных для прогнозирования рисков по статистике, аккумулируемой от средств мониторинга, определяется с использованием программного «Модуля проверки достаточности данных для прогнозирования рисков по статистике» (см. подробнее в 3.4). Укрупненная блок-схема реализации программных решений «Модуля определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021» отражена на рис. 2.22. В результате применения программы формируются данные для расчетов: частота возникновения угроз, средние времена развития угроз и восстановления целостности, используемые для моделируемой системы данного мониторируемого объекта.

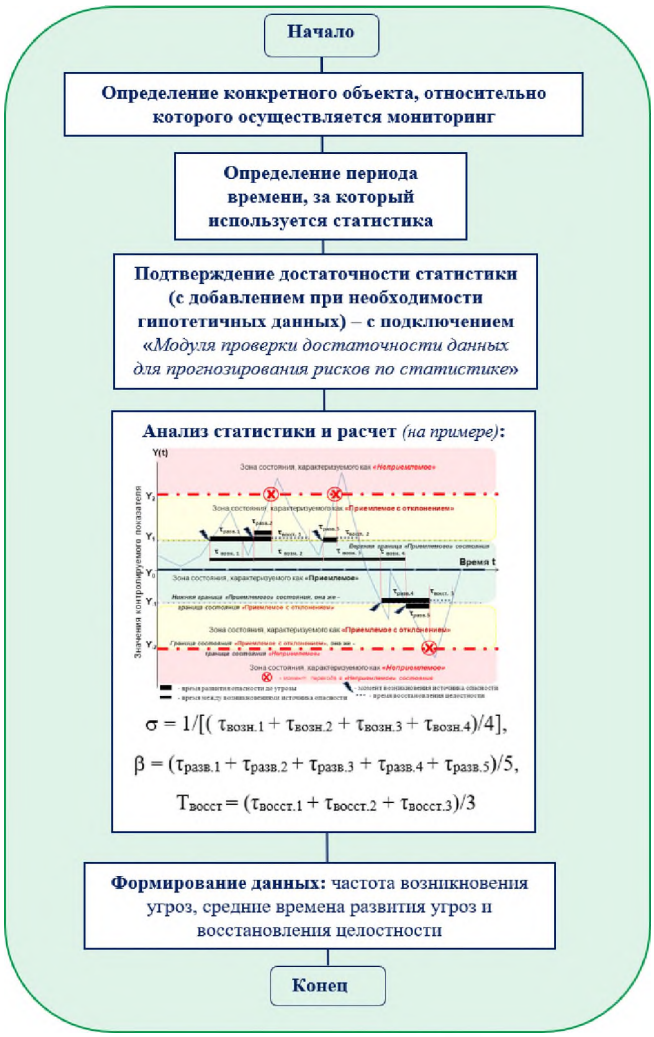


Рис. 2.22 Укрупненная блок-схема реализации программных решений «Модуля определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021»

В результате применения «Модуля формирования отчетности по результатам вероятностного прогнозирования рисков …» формируются соответствующие аналитические отчеты. Пример шаблона такого отчета применительно к объекту промышленной безопасности приведен ниже.

«АНАЛИТИЧЕСКИЙ ОТЧЕТ ПО ПРОГНОЗИРОВАНИЮ РИСКОВ НАРУШЕНИЯ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ.

Оценка рисков и среднего времени до нарушения

Отчет сформирован подсистемой "**ПРОГНОЗИРОВАНИЕ РИСКОВ НАРУШЕНИЯ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ. Оценка рисков и среднего времени до нарушения**" по запросу "Name"

Анализируемая структура: " Название структуры " *(из вводимых данных или путем выбора из заготовок!)*
Логическая структура:
Идентификация элементов. Интерпретация безопасности (из требований ФЗ, нормативных документов или из требований пользователя).
Описание структуры, последовательных подсистем и элементов:
…, в т.ч. перечень угроз и признаков наличия или возникновения источников угроз (с указанием в последующем причин – Причина 1, причина 2 – из вводимых данных пользователя).
Время поступления запроса:
Указывается время инициации запроса на моделирование

Расчетные показатели:
Интегральный риск критичного нарушения структуры за период прогноза (*если не реагировать*);
Риски критичного нарушения для каждой i-й последовательной подсистемы (*если не реагировать*);
Интегральный риск критичного нарушения структуры за период прогноза (*если всегда реагировать оперативно*);
Риски критичного нарушения для каждой i-й последовательной подсистемы (*если всегда реагировать оперативно*);
Среднее время до возможного нарушения для системы (*если не реагировать*)
Среднее время до возможного нарушения для системы (*если всегда реагировать оперативно*)
Среднее время до возможного нарушения для каждой i-й последовательной подсистемы (*если не реагировать*)
Среднее время до возможного нарушения для каждой i-й последовательной подсистемы (*если всегда реагировать оперативно*)
Нормативные границы для риска критичного нарушения: *из нормативов (подлежат обоснованию по результатам опытной эксплуатации).*

Исходные данные:
Задаваемый период прогноза.

По каждому элементу:
Частота возникновения угроз:
Среднее время развития угроз:
Период между контролями целостности:
Средняя длительность контроля целостности:
Среднее время восстановления (после нарушений):

Результаты расчетов:
Если не реагировать, то интегральный риск критичного нарушения функционирования системы за период Тзад = R – *за пределами нормы.*
Если всегда реагировать оперативно, то интегральный риск критичного нарушения функционирования системы за период Тзад = R – *в пределах нормы.*
Если не реагировать, то риск критичного нарушения i-й подсистемы за период Тзад = R – *за пределами нормы.*
Если всегда реагировать оперативно, то риск критичного нарушения i-й подсистемы за период Тзад = R – *в пределах нормы.*
Если не реагировать, то среднее время до возможного нарушения для системы = Т *xxx,xx часов*
Если всегда реагировать оперативно, то среднее время до возможного нарушения для системы = Т *xxx,xx часов*
Если не реагировать, то среднее время до возможного нарушения для каждой i-й последовательной подсистемы= Т *xxx,xx часов*
Если всегда реагировать оперативно, то среднее время до возможного нарушения для каждой i-й последовательной подсистемы = Т *xxx,xx часов*

Дата формирования отчета:……..»

Другие примеры отчетности по обобщенным и детальным вероятностным прогнозам для встроенных программных систем отражены в подразделе 3.3.

Разработанные программы для ЭВМ «Модуль проверки достаточности данных для прогнозирования рисков по статистике» и «Модель технологической поддержки риск-ориентированной системной инженерии» представлены в соответствующем контексте в разделе 3.

2.5 Выводы по разделу 2

1. Проведенный анализ показал, что возрастание потребностей системной инженерии, научно-технический прогресс в сфере информационных технологий и телекоммуникаций, устаревание программного обеспечения на фоне санкций стран Запада, осознание важности, перспективности и масштабности моделирования с учетом практических особенностей привели к необходимости дальнейшего научного развития вероятностных моделей, создания усовершенствованных программных, технологических и методических решений в интересах упреждающего управления рисками для систем различного функционального назначения. При этом особый акцент сделан на моделировании стандартизованных процессов в жизненном цикле различных систем, а также на внедрении зарекомендовавших себя методов в национальные стандарты.

2. Для совершенствования математического обеспечения в интересах широкого применения моделирования в области системной инженерии:

- сформулирована и доказана Теорема 1 о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности;

- предложена универсальная вспомогательная модель показателей (УВМП), используемая для извлечения знаний из процесса мониторинга данных и применимая для формирования исходных данных при моделировании систем различного функционального назначения;

- сформулирована и доказана Теорема 2 об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта и Следствие из нее;

- сформулирована и доказана Теорема 3 о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- с помощью Теорем 1-3 сделано теоретическое обоснование возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков»;

- сформулирована и доказана Теорема 4 о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Применение Теорем 1-4 и УВМП позволило осуществить теоретические усовершенствования существующих моделей и тем самым сформировать базовые модели математического обеспечения для анализа системных элементов, сложных систем и процессов в интересах широкого применения моделирования в области системной инженерии с использованием ВС и КС.

3. На сформулированном пространстве элементарных событий в условиях различных неопределенностей предложено использовать следующие показатели, одинаково свойственные для любого рода систем:

- риск нарушения рассматриваемого системного процесса как такового для реализации основных функциональных требований в течение задаваемого периода прогноза;

- риск нарушения рассматриваемого системного процесса с учетом дополнительных специфических системных требований в течение задаваемого периода прогноза;

- риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза при реализации основных функциональных требований;

- риск нарушения дополнительных специфических требований к моделируемой системе в течение задаваемого периода прогноза;

- интегральный риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза при реализации основных функциональных требований и дополнительных специфических требований;

- прогнозная нижняя оценка среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта;

- среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

4. Для расчета показателей предложено использовать комплексы программ для ЭВМ, созданные с участием автора в 2004-2018гг. [168 - 176]:

«Моделирование процессов в жизненном цикле систем "Моделирование процессов" - "ноу-хау"» (Свидетельство о государственной регистрации программы для ЭВМ №2004610858);

«Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2006610219);

«Программно-инструментальный комплекс оценки качества функционирования информационных систем через Интернет «КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008612348);

«Программно-инструментальный комплекс сопровождения систем менеджмента качества «OPISys-КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008614525);

«Программно-вычислительный комплекс оценки качества производственных процессов» (Свидетельство о государственной регистрации программы для ЭВМ №2010614145);

«Комплекс для оценки качества информационных и административно-управленческих процессов при функционировании электронного правительства (КОК-ЭП)» (Свидетельство о государственной регистрации программы для ЭВМ № 2010617017);

«Удаленная аналитическая поддержка информирования о вероятностно-временных показателях функционирования системы и ее элементов при реализации риск-ориентированного подхода» (Свидетельство о государственной регистрации программы для ЭВМ №2018617949);

«Удаленное обоснование требований к средствам и условиям обеспечения качества функционирования «умных» систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618572);

«Удаленное вероятностное прогнозирование качества функционирования информатизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618686).

Дополнительно в период 2019–2025гг. разработаны программы для ЭВМ (без соавторов) [177 - 178]:

«Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021». В результате применения модуля формируются данные для расчетов: частота возникновения угроз, средние времена развития угроз и восстановления целостности, используемые для моделируемой системы данного мониторируемого объекта;

«Модуль формирования отчетности по результатам вероятностного прогнозирования рисков для сложной системы с последовательным соединением элементов», позволяющего формировать соответствующие аналитические отчеты для последующего решения задач системной инженерии.

Примечание. Дополнительно разработанные в период 2019 – 2025гг. программы для ЭВМ «Модуль проверки достаточности данных для прогнозирования рисков по статистике» и «Модель технологической поддержки риск-ориентированной системной инженерии» [179 – 180] представлены в разделе 3.

3. РАЗРАБОТКА ТЕХНОЛОГИЧЕСКИХ РЕШЕНИЙ ДЛЯ ПОДДЕРЖКИ УПРЕЖДАЮЩЕГО УПРАВЛЕНИЯ РИСКАМИ В ПРИЛОЖЕНИЯХ СИСТЕМНОЙ ИНЖЕНЕРИИ

3.1 Определение концептуального облика технологических решений для вычислительных систем и компьютерных сетей

Для современного системного аналитика, ориентированного на эффективное решение задач согласно «Стратегии национальной безопасности РФ», «Стратегия научно-технологического развития РФ», стратегиям цифровой трансформации, указам Президента РФ «О национальных целях развития РФ на период до 2030 года и на перспективу до 2036 года», «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоемких технологий», доктринам безопасности (энергетической, информационной), ФЗ «О стратегическом планировании в РФ», «О промышленной безопасности опасных производственных объектов», ФЗ «О безопасности объектов ТЭК», ФЗ «О безопасности критической информационной инфраструктуры РФ», «Основам государственной политики РФ в Арктике на период до 2035 года» и др. важно владеть интеллектуальными инструментариями, применяемыми для поддержки упреждающего управления рисками в приложениях системной инженерии. Однако таких широко применимых инструментариев, позволяющих оперативно количественно спрогнозировать разнородные риски по единой вероятностной шкале для различных процессов и систем, аналитически обосновать эффективные меры противодействия угрозам, максимизировать выигрыш и минимизировать возможные ущербы, сегодня практически нет. Большинство из немногих созданных инструментариев ориентируются на качественный анализ рисков или носят узкоспециализированный характер.

Идет стадия создания таких достаточно универсальных инструментариев. С их помощью новый порядок решения задач системной инженерии займет считанные часы, а с внедрением интеллектуальных помощников в виде систем искусственного интеллекта для определения исходных данных моделирования и анализа результатов моделирования, потребуются минуты. На выходе – научно обоснованные рекомендации по практическому решению задач системной инженерии. Образно концептуальный облик предлагаемых технологических решений, нацеленных на создание прототипа технологии поддержки риск-ориентированной системной инженерии для решения практических задач системной инженерии с использованием ВС и КС представлен на рис. 3.1 [5, 167].

Рис. 3.1 Концептуальный облик разрабатываемых технологических решений

В основе предлагаемого подхода – усовершенствованная концепция управления рисками, позволяющая устранить следующие существующие недостатки (отмеченные в 1-м разделе):

- не осуществляется целенаправленной обработки информации для системного обоснования рациональных мер противодействия угрозам;

- используемые методы расчета рисков специфичны, результаты несравнимы;

- для разнородных угроз задачи количественного обоснования требований к стандартным процессам при ограничениях на ресурсы и допустимые риски – не решаются.

Реализация предлагаемых концептуальных положений по упреждающему управлению рисками опирается на вероятностное моделирование, прогнозирование и оптимизацию для системного решения задач и обоснования возможных упреждающих действий в условиях неопределенности. В свою очередь, прогнозирование базируется на мониторинге состояний, накоплении и рациональном использовании знаний, в т.ч. формируемых в режиме реального времени функционирования различных систем.

Применение концепции позволяет спрогнозировать представление о возможных причинах возникновения недопустимых рисков:

- на уровне целевых аналитических потребностей (применительно к процессам, элементам, подсистемам и системе в целом);

- на уровнях отдельного процесса и интеграции различных процессов (используемых применительно к элементам, подсистемам и системе в целом);

- на уровне расчетных показателей частного и интегрального рисков при создании и эксплуатации систем различного назначения.

Ожидается, что при реализации предлагаемого подхода системный аналитик будет оперировать цифровым образом рассматриваемых систем в терминах прогнозных рисков. Отличие от существующих инструментариев – взгляд условно на 3 шага вперед, это - прогноз, рекомендации и обоснование решений для задач системной инженерии.

Разработанные во 2-м разделе программные решения, а также предложенный концептуальный облик предлагаемых решений для ВС и КС позволяют перейти к разработке непосредственно технологических решений для упреждающего управления рисками в приложениях системной инженерии.

3.2 Аналитическое комплексирование разработанных программных решений

Согласно описанному выше концептуальному облику технологических решений для ВС и КС создание прототипа технологии поддержки риск-ориентированной системной инженерии предлагается осуществлять путем аналитического комплексирования разработанных программных решений. Реализованная в диссертации идея такого аналитического комплексирования представлена на рис. 3.2.

Многомодальное взаимодействие с источниками данных предлагается осуществлять с использованием:

- телеметрических данных от оборудования;

- данных, выбираемых из базы данных, учитывающей специфику приложений системы, в т.ч. в различных форматах;

- данных, вводимых в формате программных решений базовых моделей.

Для подключения базовых моделей осуществляются необходимые действия по управлению данными в интересах прогнозирования рисков и использования предоставляемых прогнозов (это могут быть организационные, регламентные, правовые действия, действия по трансформации к нужному формату, обеспечению информационной безопасности или иные технические манипуляции).

Рис. 3.2 Иллюстрация реализуемой идеи аналитического комплексирования разработанных программных решений

В интересах решения задач системной инженерии реализуется мониторинг (при наличии) и прогноз риска нарушения приемлемого выполнения заданных процессов системной инженерии.

При этом осуществляются [5, 167]:

- в ЖЦ системы: информирование о системных требованиях к характеристикам системы, предоставление необходимых данных, учет условий и принятых ограничений;

- на этапах разработки, модернизации и развития системы: прогнозирование рисков, анализ альтернатив по результатам расчетов;

- на этапах эксплуатации и сопровождения системы: прогнозирование рисков, оценка критичности влияния различных параметров на поведение системы;

- при проектировании, выполнении, контроле и управлении процессами: реализации аналитических возможностей по выявлению существенных угроз и приемлемых условий для анализируемых процессов;

- при интеграции исследований на различных мета-уровнях: прогнозирование интегрального риска, в т.ч. для совокупности стандартных процессов в ЖЦ системы, обоснование условий удержания рисков в допустимых пределах.

Используются различные человеко-машинные интерфейсы, приспособленные для применения предложенных базовых моделей.

Аналитическое комплексирование разработанных программных решений может быть проиллюстрировано примерами решения задач системной инженерии на различных слоях мета-уровней – см. рис. 3.3 – 3.9.

На рис. 3.3 продемонстрирован 1-й слой – на примере анализа возможностей использования созданного прототипа технологии при реализации доктрины энергетической безопасности – в интересах выбора критерия для решения задач анализа, см. пример в 5.1, в деталях - рис. 5.2.

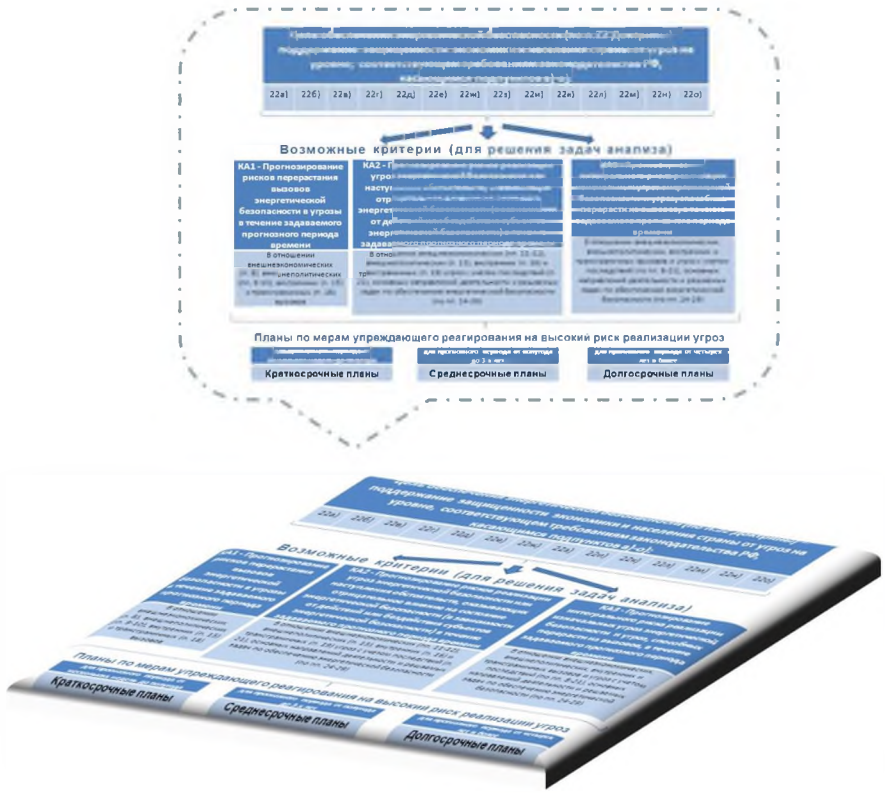


Рис. 3.3 Иллюстрация 1-го слоя на примере выбора критерия для решения задач анализа

На рис. 3.4 продемонстрирован 2-й слой – на примере анализа возможностей использования созданного прототипа технологии при реализации доктрины энергетической безопасности – в интересах формализованного описания связи «цели – направления деятельности – решаемые задачи – риски – угрозы – характеристики угроз», см. пример в 5.1, в деталях - рис. 5.4.

Рис. 3.4 Иллюстрация 2-го слоя на примере формализованного описания связи «цели – направления деятельности – решаемые задачи – риски – угрозы – характеристики угроз»

На рис. 3.5 продемонстрирован 3-й слой – на примере прогнозирования рисков для ручного и автоматизированного режимов работы отдельного оборудования (например, системы водоотлива) на конкретной угольной шахте, см. пример в 4.2, в деталях - рис. 4.2.

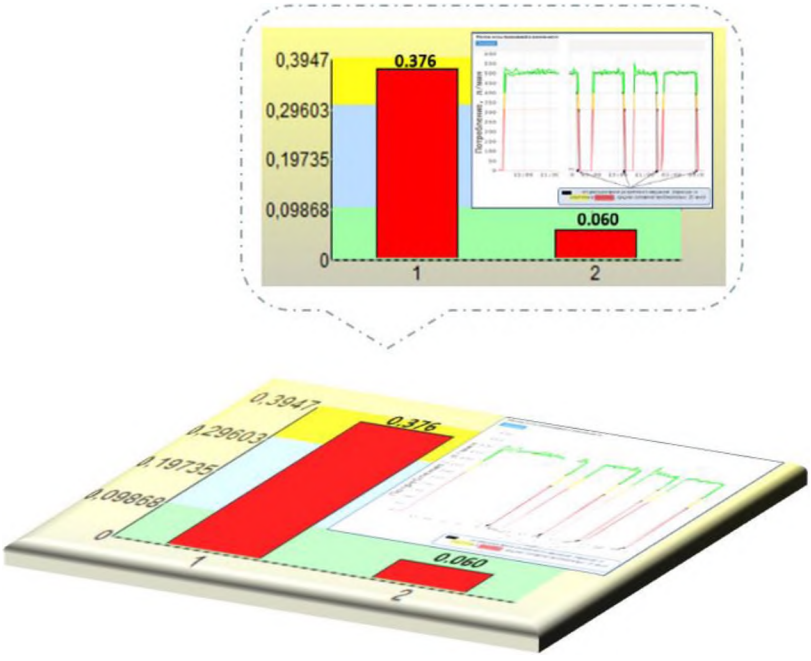


Рис. 3.5 Иллюстрация 3-го слоя на примере прогнозирования рисков для ручного и автоматизированного режимов работы отдельного оборудования

На рис. 3.6 продемонстрирован 4-й слой – на примере формализации функционирования объектов системы дистанционного контроля (СДК) промышленной безопасности - для прогнозирования рисков в угольной отрасли, см. пример в 4.4, в деталях - рис. 4.31.

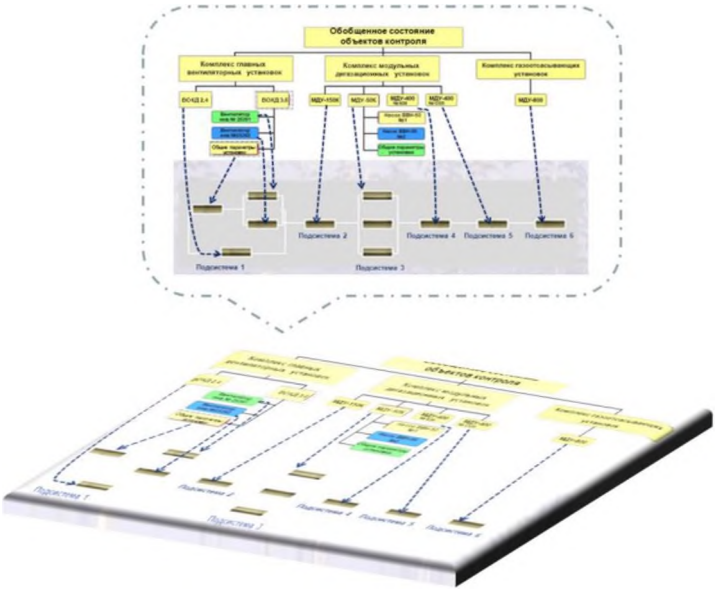


Рис. 3.6 Иллюстрация 4-го слоя на примере формализации функционирования объектов СДК промышленной безопасности

На рис. 3.7 продемонстрирован 5-й слой – на примере изучения изменения интегрального риска нарушения промышленной безопасности с использованием СДК во времени, см. пример в 4.4, в деталях - рис. 4.34.

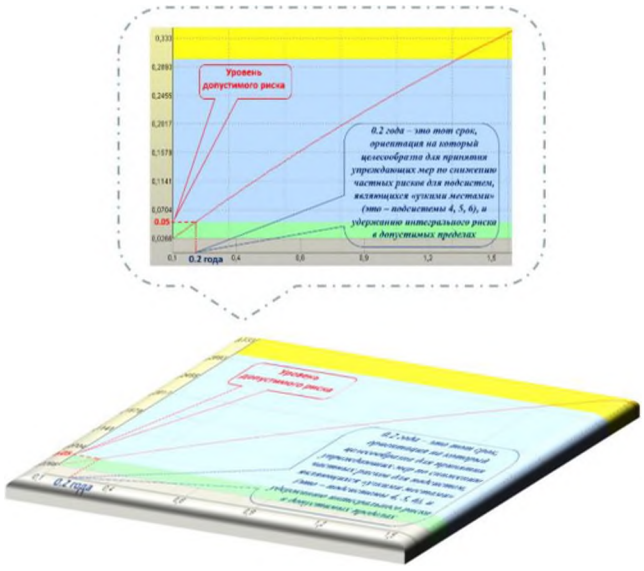


Рис. 3.7 Иллюстрация 5-го слоя на примере изучения изменения интегрального риска нарушения промышленной безопасности с использованием СДК во времени

На рис. 3.8 продемонстрирован 6-й слой – на примере моделирования многомодального взаимодействия социокиберфизических систем в жизненном цикле обогатительной фабрики в угольной отрасли, см. пример в 5.3, в деталях – на рис. 5.20, 5.21, 5.22.

Рис. 3.8 Иллюстрация 6-го слоя на примере моделирования многомодального взаимодействия социокиберфизических систем в жизненном цикле обогатительной фабрики в угольной отрасли

На рис. 3.9 на абстрактном уровне проиллюстрированы возможности упреждающего управления рисками на различных мета-уровнях в жизненном цикле систем (различные мета-уровни проиллюстрированы с помощью слоев, изображенных на рис. 3.3 – 3.8).

Количество слоев и их содержание могут быть различным в зависимости от целей и мета-уровней решаемых задач системной инженерии. Различные примеры отражены в разделах 4 и 5 диссертации.

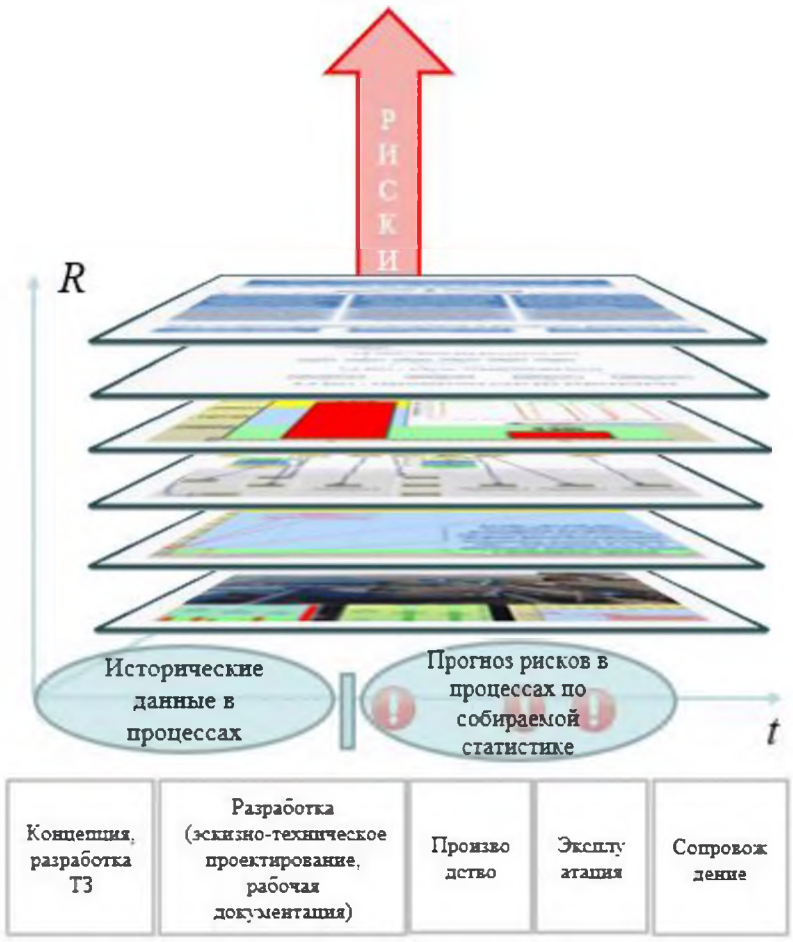


Рис. 3.9 Абстрактная иллюстрация возможностей упреждающего управления рисками на различных мета-уровнях в жизненном цикле систем

3.3 Разработка встроенных технологических возможностей по предоставлению обобщенных и детальных вероятностных прогнозов

В подразделе с учетом современных требований на базе программных решений (см. подраздел 1.5 и раздел 2) предлагается вариант создания встроенных технологических возможностей по предоставлению в дополнение к фактическим данным о состоянии системы еще и обобщенных и детальных вероятностных прогнозов. Это особенно актуально для АСУ ТП, применимых на опасных производственных объектах в различных областях народного хозяйства. Предлагаемые технологические возможности разработаны на основе принятых в подразделе 1.4 принципов создания и внедрения широко применимых программных, технологических и методических решений для упреждающего управления рисками.

Изложение решений приводится с привязкой к системам дистанционного контроля (СДК) промышленной безопасности (ПБ) опасных производственных объектов (ОПО) в

рамках функций многофункциональных систем безопасности угольных шахт (МФСБ) согласно ГОСТ Р 58494-2019 «Оборудование горно-шахтное. МФСБ. Система дистанционного контроля опасных производственных объектов» (авторское участие подтверждено актом реализации - см. Приложение Г) [64, 126, 131, 139].

Примечание. МФСБ объединяет в горных выработках шахты, надшахтных зданиях и сооружениях системы и средства, обеспечивающие организацию и осуществление безопасности ведения горных работ, контроль и управление технологическими и производственными процессами в нормальных, предаварийных и аварийных условиях, предотвращение условий возникновения различных видов опасности динамического, аэрологического и техногенного характера, контроль соответствия технологических процессов заданным параметрам, применение систем противоаварийной защиты людей, оборудования и сооружений (см. ГОСТ Р 54977 и ГОСТ Р 55154).

Согласно ГОСТ Р 58494-2019 применение СДК ПБ нацелено на оперативное выявление и оповещение ответственных лиц о предпосылках возникновения либо о возникновении опасных ситуаций на ОПО, удаленную информационно-аналитическую поддержку ответственных лиц в интересах обеспечения нормальных условий функционирования ОПО и реализации на предприятиях риск-ориентированного подхода путем расчета и представления в режиме реального времени показателей состояния ПБ на ОПО. Применение СДК 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 и др.

СДК ПБ ОПО применяют, как правило, на уровне следующих систем МФСБ:

- для обеспечения аэрологической безопасности (системы контроля и управления стационарными вентиляторными установками, вентиляторами местного проветривания и газоотсасывающими установками; системы контроля и управления дегазационными установками и контроля подземной дегазационной сети; системы аэрогазового контроля; системы контроля запыленности воздуха и пылевых отложений);

- для обеспечения контроля и прогноза динамических явлений (системы геофизических наблюдений; системы регионального, локального и текущего прогноза динамических явлений);

- для обеспечения пожарной безопасности (системы обнаружения ранних признаков эндогенных и экзогенных пожаров и локализации экзогенных пожаров; системы контроля и управления пожарным водоснабжением);

- для обеспечения связи, оповещения и определения местоположения персонала (системы определения местоположения персонала в горных выработках шахты; системы поиска и обнаружения людей, застигнутых аварией; системы оперативной, громкоговорящей и аварийной подземной связи и аварийного оповещения; системы из независимых каналов связи с подразделением профессиональной аварийно-спасательной службы или профессионального аварийно-спасательного формирования, обслуживающего шахту);

- для обеспечения взрывозащиты (системы контроля и управления средствами взрывозащиты горных выработок; системы контроля и управления средствами взрывозащиты в газоотсасывающих и дегазационных трубопроводах и установках).

Примечание. Перечисленные выше системы МФСБ упомянуты согласно Федеральным нормам и правилам в области промышленной безопасности «Правила безопасности в угольных шахтах» (в редакции приказов Ростехнадзора от 19 ноября 2013 г. № 550, от 2 апреля 2015 г. № 129, от 22 июня 2016 г. №236, от 8 августа 2017 г. № 303).

Информацию МФСБ, а также иную информацию, которой оперируют на ОПО, используют в СДК ПБ для повышения безопасности и эффективности функционирования опасных производственных объектов в целом.

В рамках предлагаемых технологических возможностей в зависимости от целей моделирования анализируемые объекты логически представляются (см. подраздел 2.2):

для отдельных системных элементов или при огрубленном моделировании сложной системы – в виде «черного ящика» (т.е. с представлением о входах и выходах без выделения внутренних структурных элементов);

для сложных систем - в виде логической структуры с декомпозицией до уровня составных подсистем и системных элементов, характеризуемых их параметрами и условиями эксплуатации и объединяемых логическими условиями «И» и «ИЛИ».

В рамках использования предлагаемых технологических возможностей целями прогнозирования рисков являются:

установление степени вероятного нарушения ПБ анализируемого объекта для текущих сценариев возникновения и развития угроз, применяемых мер системного контроля и мониторинга состояний и восстановления целостности объектов (например, подсистемы МФСБ, оборудования, отдельного параметра);

обоснование уровня допустимого риска по «прецедентному принципу»;

обоснование предотвращения условий возникновения различных видов опасностей за период прогноза;

сравнительный анализ возможностей противодействия угрозам;

обоснование упреждающих мер по снижению или удержанию в допустимых пределах рисков и/или снижение затрат и/или возможных ущербов в практике создания, эксплуатации, технического обслуживания, модернизации и развития системы обеспечения ПБ ОПО при задаваемых ограничениях;

создание базы знаний и вариантов решения задач сбалансированного управления рисками.

Технологические возможности действуют в виртуальной среде на оборудовании, выделенном для их реализации на пилотном участке Заказчика (см. акт реализации в Приложении В). Состав и конфигурация требуемых программно-технических средств в составе ВС и КС на объекте Заказчика включают:

- сервер - 1 шт. со спецификациями: ЦПУ – 2 x Intel Xeon 4 ядра 2ГГц; накопитель на жестком магнитном диске- не менее1 ТБ; ОЗУ - 16 ГБ; RAID; LAN - 100 Мбит/с; монитор, клавиатура (рус./лат.), «мышь»;

- рабочая станция – 1 шт. со спецификациями: ЦПУ - intel core i5 или выше; оперативная память не менее 2GB; свободное место на жестком диске – не менее 200GB; 4 порта USB 2.0; LAN; ЖК-монитор 19" или больше, клавиатура (рус./лат.), «мышь»;

- средства телекоммуникаций, действующие у заказчика.

Должен быть обеспечен доступ к базам данным Заказчика, содержащих данные, собираемые от мониторируемого оборудования в СДК ПБ.

Для использования технологических возможностей должен указываться пользователь, владеющий соответствующими полномочиями. Добавление/изменение причин и мер целенаправленного воздействия осуществляется пользователем, ответственным за конкретный параметр мониторируемого оборудования. В итоге применения предлагаемых технологических возможностей ответственному лицу СДК ПБ предоставляются аналитические отчеты, содержащие следующие показатели, рекомендованные ГОСТ Р 58494-2019:

прогнозируемое остаточное время на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона при каждом выходе значений параметра за границы рабочего диапазона;

условные средние времена до выхода значений параметра за границы нормативного диапазона для условий, если оперативно реагировать на выходы значений параметров за границы рабочего диапазона и если не реагировать на эти отклонения;

риски нарушения границ нормативного диапазона хотя бы по одному из контролируемых параметров за смену, сутки, неделю, месяц, год с учетом последствий (в вероятностном представлении).

Прогнозируемое остаточное время на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона формируется принудительно при каждом выходе значений параметра за границы рабочего диапазона – пример предупреждения представлен на рис. 3.10.

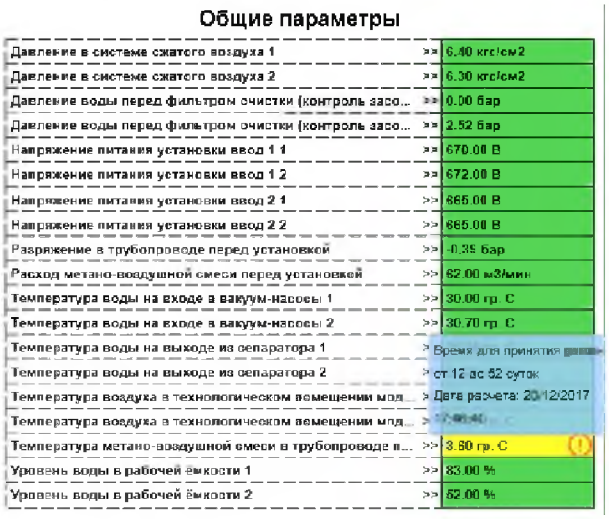


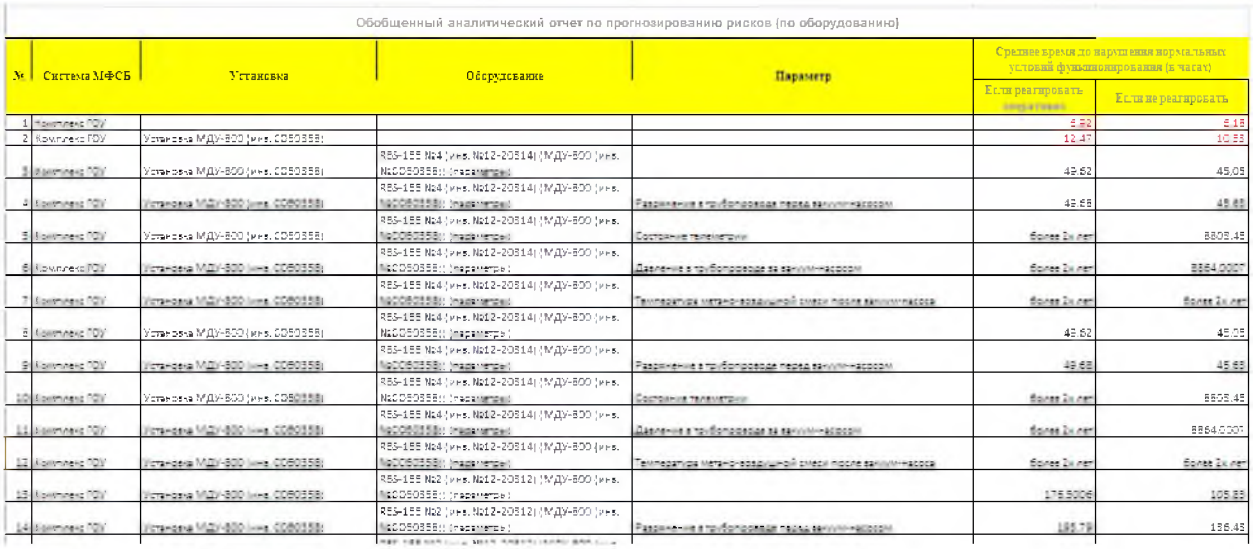
Рис. 3.10 Пример предупреждения по параметру «Температура метано-воздушной смеси в трубопроводе…»

Наименования и содержание обобщенных и детальных отчетов в формате Excel на примере газоотсасывающей установки (ГОУ) представлены обобщенные отчеты - по установке на рис. 3.11, по оборудованию – фрагмент на рис. 3.12. Фрагмент детального отчета в табличной форме представлен на рис. 3.13.

Обобщенный аналитический отчет по прогнозированию рисков (по установке)

№	Система МФСБ	Установка	Оборудование	Среднее время до нарушения нормальных условий функционирования (в часах)	
				Если реагировать оперативно	Если не реагировать
1	Комплекс ГОУ			5,52	5,16
2	Комплекс ГОУ	Установка МДУ-800 (инв. СО50355)		12,47	10,53
3	Комплекс ГОУ	Установка МДУ-800 (инв. СО50355)	ББЗ-155 №4 (инв. №12-20314) (МДУ-800 (инв. №СО50355) (параметры)	45,62	45,05
4	Комплекс ГОУ	Установка МДУ-800 (инв. СО50355)	ББЗ-155 №4 (инв. №12-20314) (МДУ-800 (инв. №СО50355) (параметры)	45,62	45,05
5	Комплекс ГОУ	Установка МДУ-800 (инв. СО50355)	ББЗ-155 №2 (инв. №12-20312) (МДУ-800 (инв. №СО50355) (параметры)	175,5005	105,83
6	Комплекс ГОУ	Установка МДУ-800 (инв. СО50355)	ББЗ-155 №4 (инв. №12-20314) (МДУ-800 (инв. №СО50355) (параметры)	45,62	45,05
7	Комплекс ГОУ	Установка МДУ-800 (инв. СО50355)	ББЗ-155 №2 (инв. №12-20312) (МДУ-800 (инв. №СО50355) (параметры)	176,5006	105,83
8	Комплекс ГОУ	Установка МДУ-800 (инв. СО50355)	Общие параметры МДУ-800 (инв. №СО50355) (параметры)	15,82	15,72
9	Комплекс ГОУ	Установка МДУ-400 (инв. 63943)		15,53	14,55
10	Комплекс ГОУ	Установка МДУ-400 (инв. 63943)	Общие параметры МДУ-400 (инв. №63943) (параметры)	17,25	16,37
11	Комплекс ГОУ	Установка МДУ-400 (инв. 63943)	Общие параметры МДУ-400 (инв. №63943) (параметры)	17,25	16,37
12	Комплекс ГОУ	Установка МДУ-400 (инв. 63943)	ББЗ-155 №1 (инв. №12-1711Р) (МДУ-400 (инв. №63943) (параметры)	154,57	131,3041
				Сформировано:	28.12.2018 17:05:26

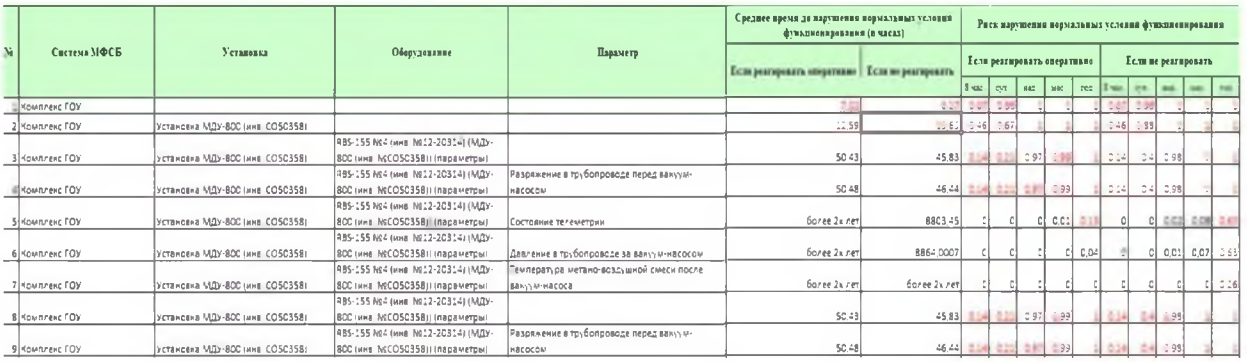
Рис. 3.11 Пример обобщенного отчета (по установке)



Обобщенный аналитический отчет по прогнозированию рисков (по оборудованию)

№	Система МФСБ	Установка	Оборудование	Параметр	Среднее время до нарушения нормальных условий функционирования (в часах)	
					Если реагировать оперативно	Если не реагировать
1	Комплекс ГОУ					8,82
2	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)				12,47
3	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)			45,83
4	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Разряжение в трубопроводе перед вакуум-насосом		46,48
5	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Состояние телеметрии	более 2х лет	8803,45
6	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Давление в трубопроводе за вакуум-насосом	более 2х лет	8864,0007
7	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Температура метано-воздушной смеси после вакуум-насоса	более 2х лет	более 2х лет
8	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)			45,83
9	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Разряжение в трубопроводе перед вакуум-насосом		46,48
10	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Состояние телеметрии	более 2х лет	8803,45
11	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Давление в трубопроводе за вакуум-насосом	более 2х лет	8864,0007
12	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Температура метано-воздушной смеси после вакуум-насоса	более 2х лет	более 2х лет
13	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №2 (инв. №12-20812) (МДУ-800 (инв. №COSO358)) (параметры)		176,5006	105,83
14	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №2 (инв. №12-20812) (МДУ-800 (инв. №COSO358)) (параметры)	Разряжение в трубопроводе перед вакуум-насосом	185,78	136,48

Рис. 3.12 Пример фрагмента обобщенного отчета (по оборудованию)



№	Система МФСБ	Установка	Оборудование	Параметр	Среднее время до нарушения нормальных условий функционирования (в часах)		Риск нарушения нормальных условий функционирования									
					Если реагировать оперативно	Если не реагировать	Если реагировать оперативно					Если не реагировать				
							8 час	сут	нед	мес	год	8 час	сут	нед	мес	год
1	Комплекс ГОУ				8,82	8,82	0,91	0,99	1	1	1	0,91	0,99	1	1	1
2	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)			12,59	12,59	0,86	0,97	1	1	1	0,86	0,99	1	1	1
3	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)		50,43	45,83	0,34	0,93	0,97	0,99	1	0,34	0,94	0,98	1	1
4	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Разряжение в трубопроводе перед вакуум-насосом	50,48	46,48	0,34	0,93	0,97	0,99	1	0,34	0,94	0,98	1	1
5	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Состояние телеметрии	более 2х лет	8803,45	0	0	0	0,01	0,13	0	0	0,01	0,08	0,87
6	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Давление в трубопроводе за вакуум-насосом	более 2х лет	8864,0007	0	0	0	0	0,04	0	0	0,01	0,07	0,93
7	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Температура метано-воздушной смеси после вакуум-насоса	более 2х лет	более 2х лет	0	0	0	0	0	0	0	0	0	0
8	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)		50,43	45,83	0,34	0,93	0,97	0,99	1	0,34	0,94	0,98	1	1
9	Комплекс ГОУ	Установка МДУ-800 (инв. COSO358)	RBS-155 №4 (инв. №12-20814) (МДУ-800 (инв. №COSO358)) (параметры)	Разряжение в трубопроводе перед вакуум-насосом	50,48	46,48	0,34	0,93	0,97	0,99	1	0,34	0,94	0,98	1	1

Рис. 3.13 Пример фрагмента детального отчета в табличной форме

Исходными данными для прогнозирования рисков являются текущие данные мониторинга по параметрам, оборудованию, установкам, регистрируемые в СДК ПБ.

Ответственному лицу остается задать вид отчета, ожидаемого к получению – обобщенный или детальный – см. рис. 3.14.

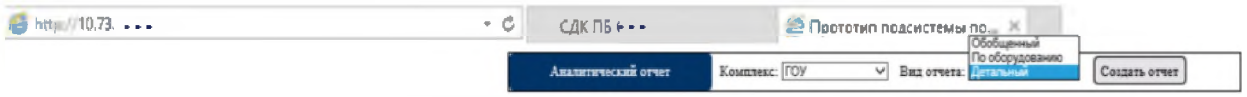


Рис. 3.14 Предлагаемый список отчетов

Отчет предоставляется при нажатии на клавишу «Создать отчет».

Установление степени вероятного нарушения ПБ анализируемого объекта для текущих сценариев возникновения и развития угроз, применяемых мер системного контроля и мониторинга состояний и восстановления целостности объектов осуществляется на уровне:

прогнозируемого остаточного времени на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона при каждом выходе значений параметра за границы рабочего диапазона (см. рис. 2.13, 2.17 – 2.20);

условных средних времен до выхода значений параметра за границы нормативного диапазона для условий, если оперативно реагировать на выходы значений параметров за границы рабочего диапазона и если не реагировать на эти отклонения – с использованием аналитических отчетов (см. подразделы 2.2 – 2.4).

Обоснования уровня допустимого риска по «прецедентному принципу» заключается в использовании научных методов прогнозирования рисков […], реализованных в вероятностных моделях, и выборе такого уровня риска, который достижим (по прецедентам из практики) и устраивает все заинтересованные стороны на ОПО в условиях существующих ограничений с использованием детальных аналитических отчетов (см. раздел 2 и рис. 3.10 – 3.13).

Обоснование предотвращения условий возникновения различных видов опасностей за период прогноза заключается в ориентации на установленные уровни допустимого риска по «прецедентному принципу» и выделении тех параметров, оборудования, установок, для которых допустимые риски нарушаются – с использованием детальных аналитических отчетов. Предпринимаются меры, направленные на недопущение превышения допустимых рисков по выделенным параметрам.

Сравнительный анализ возможностей противодействия угрозам осуществляется путем сравнения достигаемых показателей времени и рисков с использованием более детальных аналитических отчетов (см., например, рис. 3.13).

Обоснование упреждающих мер по снижению или удержанию в допустимых пределах рисков и/или снижение затрат и/или возможных ущербов в практике создания, эксплуатации, технического обслуживания, модернизации и развития системы обеспечения ПБ ОПО при задаваемых ограничениях осуществляется путем решения оптимизационных задач с использованием детальных аналитических отчетов.

Создание базы знаний и вариантов решения задач сбалансированного управления рисками осуществляется с использованием детальных аналитических отчетов и выявлении причин и анализа неудовлетворительных результатов. Результаты могут оказаться неудовлетворительными из-за того, что в исходных данных для моделирования учтены те события, которые по решению ответственного лица не должны были учитываться (например, при ремонте и контрольных проверках параметр несколько раз выходил за границы нормативного диапазона, что сказалось на автоматически сформированных исходных данных. Как следствие – необоснованно завышенные риски).

База знаний формируется путем добавления/изменения причин выхода значений параметров за границы нормативного диапазона, а также мер целенаправленного воздействия по недопущению выхода значений параметров за границы нормативного диапазона (см. рис. 2.17).

Пользователь (ответственный за контролируемый параметр) может просмотреть все события выхода значений параметра за границы нормативного диапазона (либо в «желтую зону»), которые формируются из базы данных. На практике для того чтобы повысить адекватность прогноза остаточного времени, необходимого для оперативного принятия упреждающих мер, вводятся причины возникновения данных событий, а также предпринятые меры по недопущению выхода значений параметра за границы нормативного диапазона. Вводимые данные классифицируются и уточняются при дальнейших расчетах. Используются различные человеко-машинные интерфейсы, приспособленные для применения предложенных базовых моделей.

Для решения задач по расчету времени, необходимом для оперативного принятия упреждающих мер, частота возникновения источников угроз (σ), среднее время развития угроз (β) и среднее время восстановления нарушаемой целостности моделируемой системы ($T_{восст}$) формируются автоматически из БД с использованием разработанного «Модуля определения частоты возникновения угроз, времен развития угроз и восстановления в УВМП по ГОСТ Р 59349» учетом достаточности статистики (см. подраздел 3.4). Алгоритмы формирования входных данных изложены в 2.2.4.1.

Путем последовательного выбора «Подсистемы», «Установки», «Блока» и «Оборудования» возможен выбор параметра для отображения событий, предшествующих выходу за границы нормативного диапазона (см. рис. 3.15) и для отображения событий, при которых выход за границы нормативного диапазона не произошел (см. 3.16).

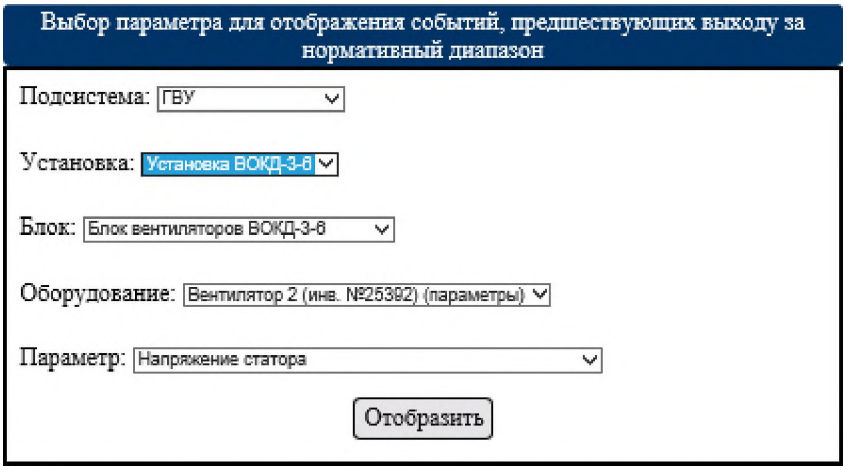


Рис. 3.15 Выбор параметра для отображения событий, предшествующих выходу за границы нормативного диапазона

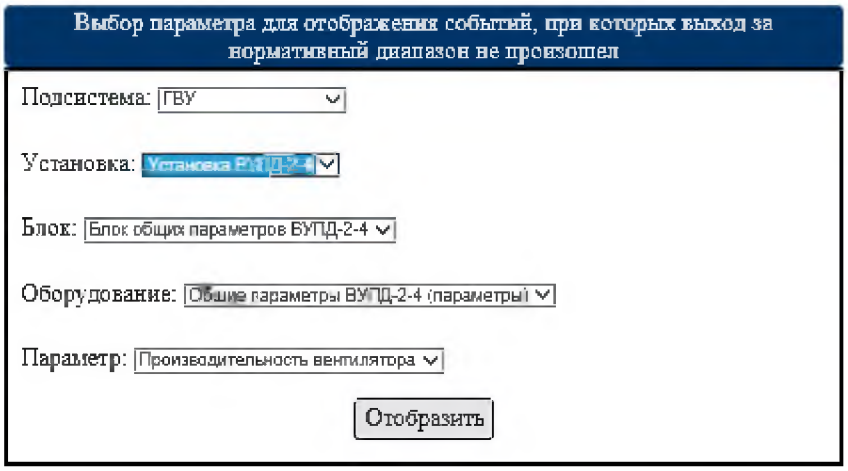


Рис. 3.16 Выбор параметра для отображения событий, при которых выход за границы нормативного диапазона не произошел

После выбора соответствующего параметра предусматривается предоставление таблицы с событиями, в том числе с учетом базы знаний – см. рис. 3.17, 3.18.

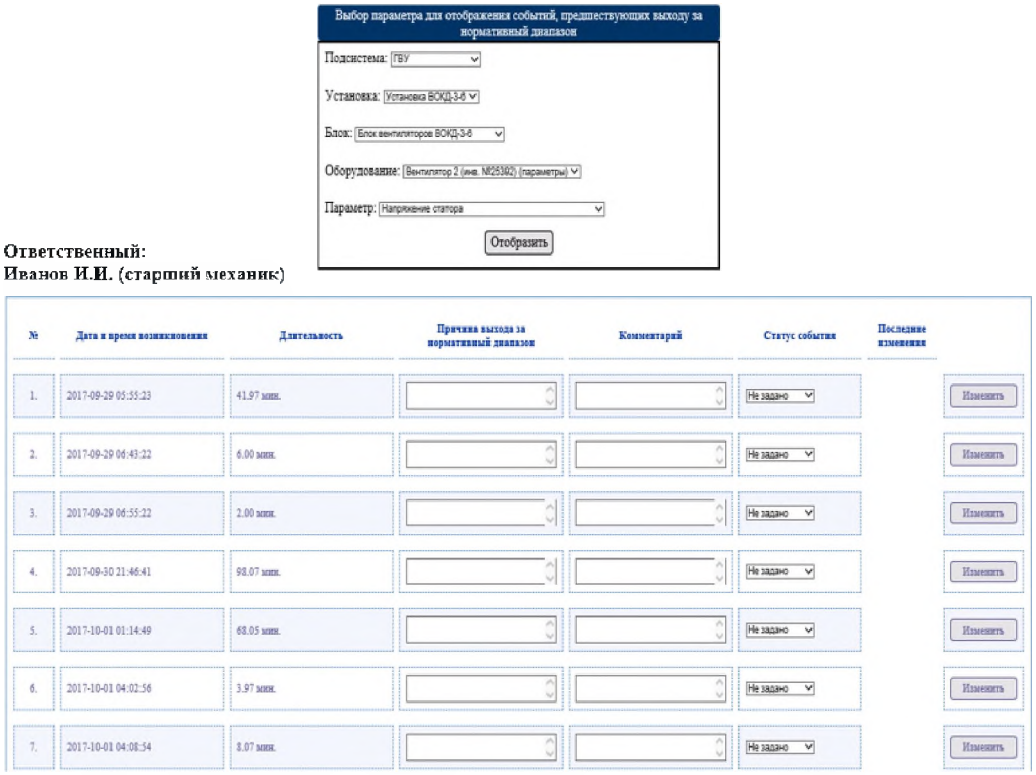


Рисунок 3.17 Отображение событий, с возможностью изменения/замены причины их возникновения

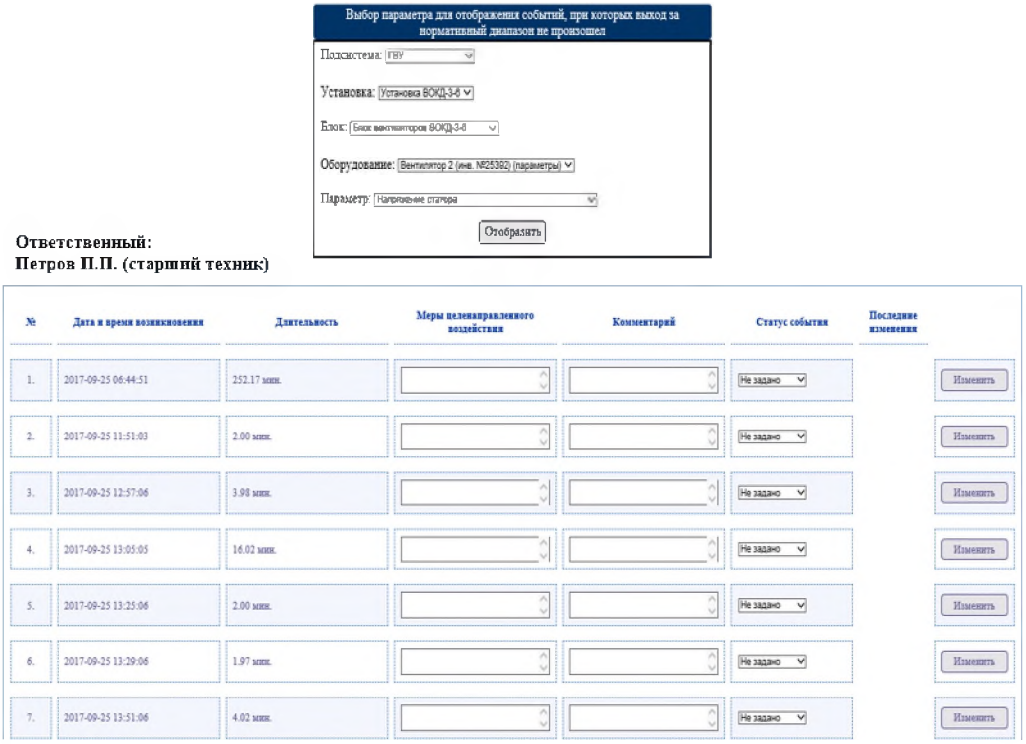


Рис. 3.18 Отображение событий, с возможностью изменения/замены мер целенаправленного воздействия для предотвращения выхода значений за границы нормативного диапазона с использованием УВМП

Возможна корректировка расчетных данных о наличии остаточного времени для принятия мер по предотвращению выхода значения параметра за границы нормативного диапазона. Для этого в таблице на рис. 3.19 отображается дата возникшего события, длительность данного события и ответственный за данный параметр сотрудник.

Рис. 3.19 Наименование столбцов таблицы корректировки

После отображения результатов базы данных и базы знаний – те поля, которые были заполнены, отображаются в виде текста причины или меры целенаправленного воздействия, комментария по событию, статусу события и лица, вносившего последние изменения для данного события, см. рис.3.20.

Рис.3.20 Пример отображения заполненного события

Статусом события могут быть четыре возможных варианта, см. рис.3.21:

- «Не задано» - такие варианты не содержат причин или мер целенаправленных воздействий;
- «Ожидаемое» - данные события являются необратимыми и их необходимо учитывать всегда;
- «Неожиданное» - событие, которое произошло случайно, без каких-либо предпосылок;
- «Исключаемое» - событие, которое было ошибочно включено в БД.

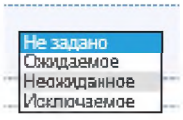


Рис.3.21 Варианты статусов событий

Заполненные причины и меры целенаправленных воздействий как реакция на события, повлекшие изменения значений параметра (как положительные, так и отрицательные) учитываются при отображении времени остаточного ресурса.

Меню с выбором подсистем для формирования аналитического отчета представлено на рис. 3.22.

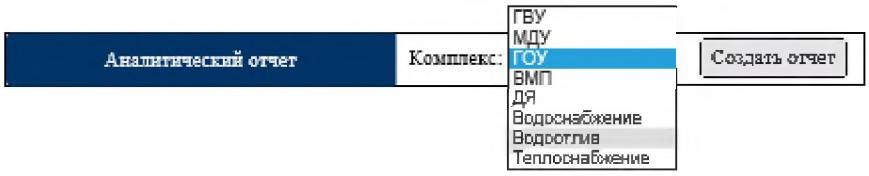


Рис. 3.22 Выбор подсистем для формирования аналитических отчетов

Пример обобщенного аналитического отчета представлен ниже (сформирован на данных отладочной БД). При этом в "Комплексе главных вентиляторных установок (ГВУ)" отсутствуют отклонения от нормы в период прогноза для заданного множества угроз по каждому из мониторируемых параметров, если «И» в «Установке ВУПД-2-4», «И» в «Установке ВОКД-3-6» отсутствуют отклонения от нормы в этот период.

Примечание. ВОКД-3-6 – это тип осевого двухступенчатого вентилятора, используемого для главного проветривания крупных шахт горнодобывающих отраслей промышленности. ВУПД-2-4 – это иной тип главной вентиляторной установки, используемой для проветривания шахт.

Обобщенно для всего "Комплекса ГВУ" и составных установок прогнозный период при моделировании задан 1 год. Для «Установки ВУПД-2-4» частота возникновения источников угроз (σ) составляет 1 раз в год, среднее время развития угроз (β) составляет 1 сутки, среднее время восстановления нарушаемой целостности ($T_{восст}$) равно 1 часу, время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы ($T_{меж}$) составляет 1 час. Для «Установки ВОКД-3-6» исходные данные отличаются лишь тем, что частота возникновения источников угроз (σ) составляет 2 раза в год, остальные исходные данные – те же, что и для «Установки ВУПД-2-4».

«ОБОБЩЕННЫЙ АНАЛИТИЧЕСКИЙ ОТЧЕТ (пример)

Анализируемая структура: "Комплекс ГВУ".
В состав оцениваемой структуры входят:
- Установка ВУПД-2-4;
- Установка ВОКД-3-6.

Логическую структуру (Установка ВУПД-2-4) определяют:
- ВУПД-2,4 (общие параметры для установки) (параметры);
- Вентилятор (параметры);
- Вентилятор (параметры).

Логическую структуру (Установка ВОКД-3-6) определяют:
- ВОКД-3,6 (общие параметры для установки) (параметры);
- Вентилятор (параметры);
- Вентилятор (параметры).

Контролируемые параметры (Установка ВУПД-2-4):
для «ВУПД-2,4 (общие параметры для установки) (параметры)»:
- Производительность вентилятора;
- Депрессия вентилятора.

для «ВУПД-2,4 (общие параметры для установки) (параметры)»:
- Производительность вентилятора;
- Депрессия вентилятора.

для «Вентилятор (параметры)»:
- Радиальные колебания подшипников вентилятора (3);
- Радиальные колебания подшипников вентилятора (2);
- Радиальные колебания подшипников вентилятора (1);
- Температура подшипника ротора вентилятора (3);
- Температура подшипника ротора вентилятора (2);
- Температура подшипника ротора вентилятора (1).

для «Вентилятор (параметры)»:
- Радиальные колебания подшипников вентилятора (3);
- Радиальные колебания подшипников вентилятора (2);
- Радиальные колебания подшипников вентилятора (1);
- Температура подшипника ротора вентилятора (3);
- Температура подшипника ротора вентилятора (2);
- Температура подшипника ротора вентилятора (1).

Контролируемые параметры (Установка ВОКД-3-6):
для «ВОКД-3,6 (общие параметры для установки) (параметры)»:
- Температура воздуха в машинном зале вентиляторной установки;
- Напряжение 230 В 2;

- Напряжение 230 В 1;
- Температура воздуха в канале вентилятора;
- Температура наружного воздуха;
- Компрессия ВГП (ВУ);
- Производительность ВГП (ВУ).

для «ВОКД-3,6 (общие параметры для установки) (параметры)»:

- Температура воздуха в машинном зале вентиляторной установки;
- Напряжение 230 В 2;
- Напряжение 230 В 1;
- Температура воздуха в канале вентилятора;
- Температура наружного воздуха;
- Компрессия ВГП (ВУ);
- Производительность ВГП (ВУ).

для «Вентилятор (параметры)»:

- Напряжение статора;
- Ток статора по фазам 2;
- Ток статора по фазам 1;
- Температура подшипника двигателя вентилятора;
- Температура подшипника ротора вентилятора.

для «Вентилятор (параметры)»:

- Ток статора по фазам 2;
- Ток статора по фазам 1;
- Температура подшипника двигателя вентилятора;
- Температура подшипника ротора вентилятора;
- Напряжение статора.

Примечание: названия составных элементов оцениваемой структуры считываются из базы данных СДК ПБ без дополнительных изменений.

Обобщенные результаты прогнозирования по запасу временного ресурса

Если оперативно реагировать на выходы значений параметров за границы рабочего диапазона, то

- риск нарушения промышленной безопасности (наступления инцидента ПБ) за год составит:

за моделируемую систему («Комплекс ГВУ») в целом – 0.083;

за элемент «Установка ВУПД-2-4» - 0.021;

за элемент «Установка ВОКД-3-6» - 0.063;

- условные средние времена до следующего инцидента составляют:

за моделируемую систему («Комплекс ГВУ») в целом – 81286 часов (9,28 лет);

за элемент «Установка ВУПД-2-4» - 411654 часа (46,99 лет);

за элемент «Установка ВОКД-3-6» - 134070 часов (15,3 года) - см. рис. 3.23.

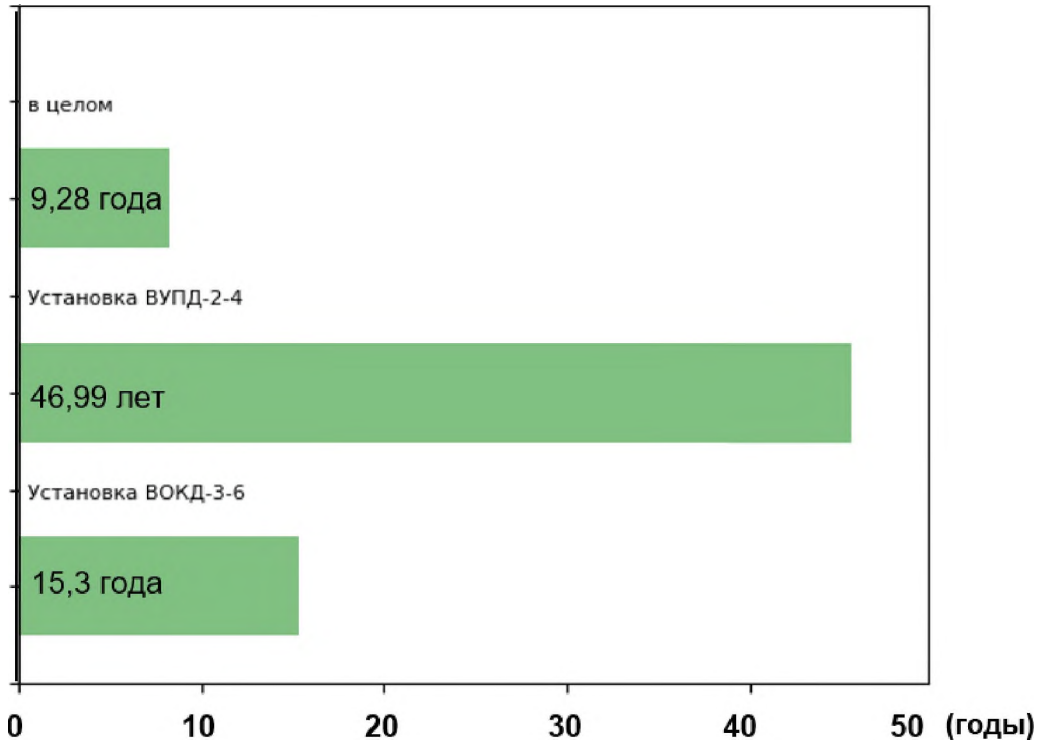


Рис. 3.23 Прогнозируемое условное среднее время до следующего инцидента (если оперативно реагировать на выходы значений параметров за границы рабочего диапазона)

Если не реагировать на выходы значений параметров за границы рабочего диапазона, то:

- риск нарушения промышленной безопасности (наступления инцидента ПБ) за год составит:

за моделируемую систему («Комплекс ГВУ») в целом – 0.950;

за элемент «Установка ВУПД-2-4» - 0.631;

за элемент «Установка ВОКД-3-6» - 0.864;

- условные средние времена до следующего инцидента составляют:

за моделируемую систему («Комплекс ГВУ») в целом – 2213 часов (0,2526 года);

за элемент «Установка ВУПД-2-4» - 8792 часа (1,004 года);

за элемент «Установка ВОКД-3-6» - 4410 часов (0,5034 года) - см. рис. 3.24.

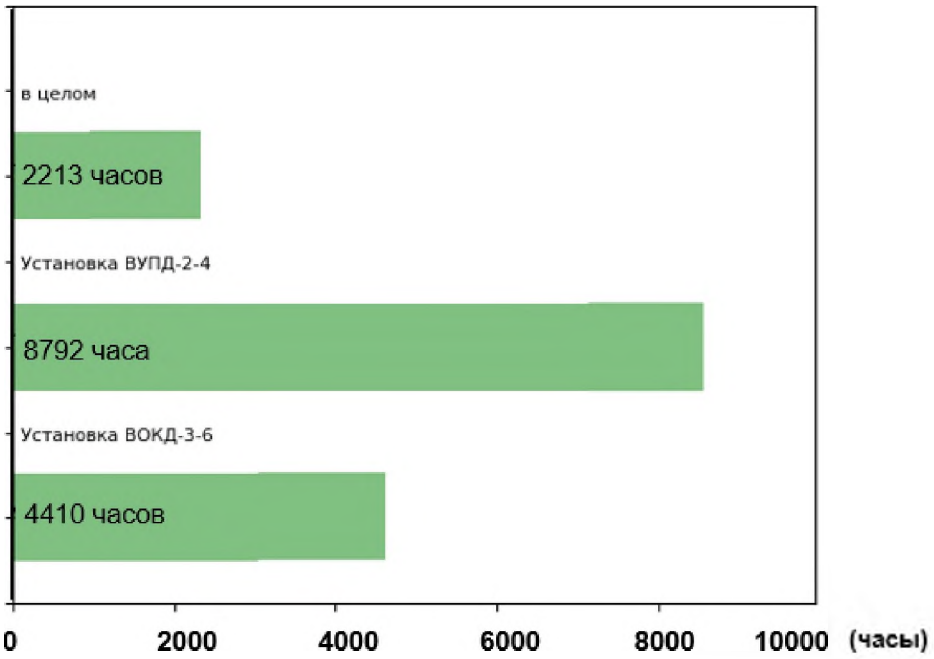


Рис. 3.24 Прогнозируемое условное среднее время до следующего инцидента (если не реагировать на выходы значений параметров за границы рабочего диапазона)

Отчет сформирован в автоматическом режиме «Указывается дата» по запросу "Пользователь"».

Полученные результаты расчетов свидетельствуют о практичности применения СДК ПБ. Должностными лицами используются различные человеко-машинные интерфейсы, приспособленные для применения предложенных базовых моделей. Вместе с тем, необходимо отметить недостаточность используемой статистики, т.к. возникновение источников угроз составляет около 2 раз в год на фоне прогноза длительностью 1 год.

Для определения «достаточности» статистики в 3.4 предложен подход, реализованный в разработанном «Модуле проверки достаточности данных для прогнозирования рисков по статистике» [179] (см. 3.4). Проверка «достаточности» статистики позволит говорить о формировании прототипа базы знаний для моделирования с использованием предлагаемых программных и технологических решений.

3.4 Формирование прототипа базы знаний для моделирования

3.4.1 Определение «достаточности» статистики

Исследования в 3.3 показали практичность использования УВМП, введенного выше в 2.2.4.1. При переходе параметра из «зеленой» в «желтую» зону подключаются технологические возможности по расчету запаса временного ресурса у обслуживающего персонала. При этом, если в БД статистика является достаточной для вероятностного

моделирования, с использованием предлагаемых программных и технологических решений производится оценка среднего остаточного ресурса времени по параметру, отмеченному «желтым» цветом – см. рис. 3.25.

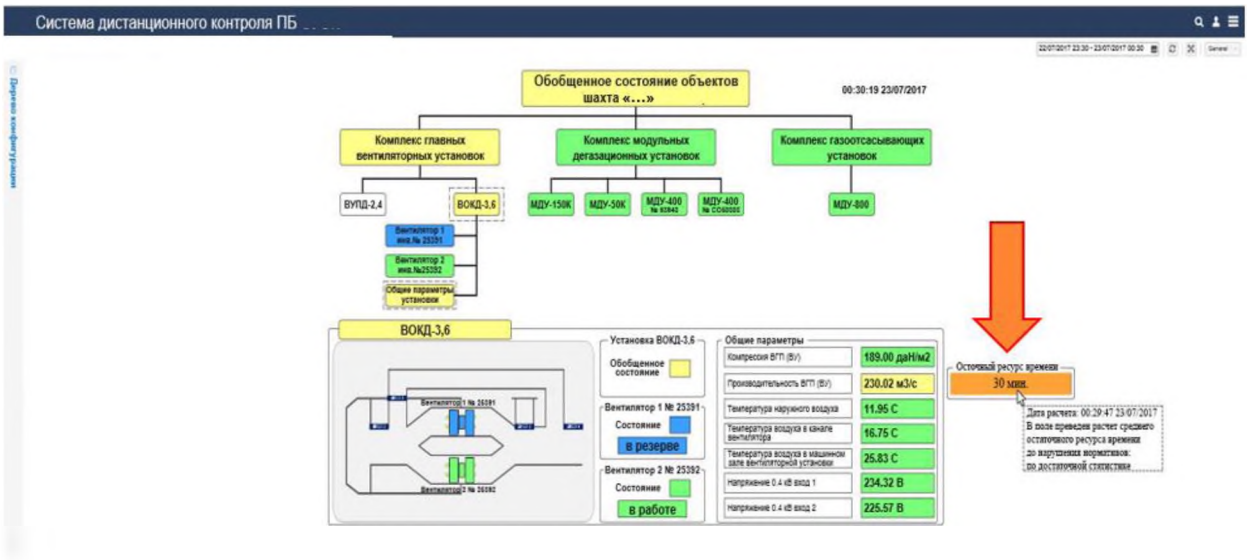


Рис. 3.25 Пример ожидаемого результата при достаточной статистике

Указывается остаточное время до перехода значений параметра в «красную» зону по статистике, а при наведении – даются комментарии по дате и содержательной интерпретации. Давать универсальное определение «достаточности» статистики при использовании УВМП для всевозможных задач системной инженерии представляется нецелесообразным из-за разнообразия критериев прикладного использования этой статистики. Вместе с тем, понятие «достаточности» статистики имеет смысл разъяснить на примерах применения СДК ПБ. Тем самым предлагается эмпирический алгоритм, направленный на повышение адекватности вероятностного моделирования.

Определение (на примерах для угольных шахт). Статистика по конкретному параметру считается достаточной для оценки запаса временного ресурса у обслуживающего персонала СДК ПБ относительно данного критичного параметра, если этой статистикой зафиксировано более 4-х прецедентов перехода из элементарного состояния «в рабочих пределах» (из «зеленой» зоны) в состояние «за пределами нормы» (в «красную» зону) за 6 последних месяцев, и для этой статистики выполняются условия: отношение максимального значения промежутков к минимальному не превышает 4-х единиц (условие 1), более 80% промежутков не более, чем в 2 раза отличаются от среднего (условие 2) и менее 30% промежутков подряд отклоняются от максимального или минимального значения не более, чем вдвое, т.е. не группируются (условие 3).

Примечание. Перечисленные % и отношения представляют собой эмпирические параметры системы МФСБ, настраиваемые при необходимости.

Три введенных практических условия для определения достаточности статистики - это попытка в период опытной эксплуатации СДК ПБ (когда временно может отсутствовать привязка к истинным причинам возникновения отклонений) отсечь уникальные случаи (содержащие частые групповые нарушения, обусловленные каскадными нарушениями из-за одной причины, отладочными работами и пр.), а также случаи отсутствия должной реакции на сигналы СДК.

Примечание. По результатам опытной эксплуатации СДК ПБ возможно введение дополнительных условий «достаточности» статистики.

Введенное определение «достаточности» статистики иллюстрируется следующими примерами.

Пример 3.4.1. Пусть было 11 прецедентов перехода из элементарного состояния «в рабочих пределах» («зеленое») в состояние «за рабочими пределами - предаварийное состояние» («желтое»), и лишь 7 – в состояние «за пределами нормы» («красное»). Т.е. – есть 6 промежутков (между восемью переходами в «красное») за 6 месяцев, в среднем величина 1-го промежутка равна 1 месяцу.

Если на практике 2 промежутка произошли за 1-й месяц (с промежутком 15 суток), 2 – за последний (с промежутком 15 суток), а 2 – за 4 месяца (с промежутком 2 месяца). Тогда из 6 промежутков 1, 2, 5, 6-й промежутки в 2 раза меньше среднего, а 3-й и 4-й – в 2 раза больше среднего. Условие 1 – выполнено, т.к. отношение максимума к минимуму = 4 (2мес/15суток=4). Все 100% в 2 раза отличаются от среднего, т.е. условие 2 – тоже выполнено. Но 3-е условие – не выполнено, т.к. 2 промежутка подряд (33.3%) отклоняются от минимума в 4 раза – см. рисунок 2.10! Такая статистика не может быть использована как «достаточная».

$T_{конца}$

X-----X----X----------X----------X-----X-----X-----

Рис. 3.26 Условие 3 – не выполнено, статистика полагается «недостаточной»

Т.е. в примере 3.4.1 есть группировки прецедентов, которые при оценке предопределяют такое среднее время, которое в разы отличается и от короткого, и от длинного остаточного временного ресурса у обслуживающего персонала (и которое в статистике не наблюдалось)! В случае примера 3.4.1 потребуется прогнозировать с применением вероятностных моделей и гипотетических сценариев появления и развития угроз.

Пример 3.4.2. Пусть было 13 прецедентов перехода из элементарного состояния «в рабочих пределах» («зеленое») в состояние «за рабочими пределами - предаварийное состояние» («желтое»), и все – в состояние «за пределами нормы» («красное»). Т.е. – есть 12 промежутков (между 13 залетами в «красное») за 6 месяцев, в среднем величина 1-го промежутка равна 15 суток. Если на практике в среднем 2 промежутка происходят за месяц (с промежутком 15 суток) – см. рис. 3.27, то условие 1 выполнено, т.к. отношение max к min меньше 4. Все 100% не более, чем в 2 раза отличаются от среднего, т.е. условие 2 – тоже выполнено. И менее 30% промежутков подряд отклоняются от максимума или минимума не более, чем вдвое (т.е. нет диссонирующих группировок). Статистика может рассматриваться для использования в дальнейшем моделировании как «достаточная».

$T_{конца}$

x-----x-----x----x---x------x----------x-----x--------x----x----------x---------x-------x----

Рис. 3.27 Условия «достаточности» выполнены

Вывод: статистика – достаточная для формирования исходных данных вероятностного моделирования с использованием УВМП.

3.4.2 Формирование начальных значений исходных данных

Из базы данных СДК ПБ извлекаются данные, характеризующие переходы из «зеленой» зоны в «желтую» и из «желтой» - в «красную» – см. пример на рис. 3.28 (эта же статистика в других целях приведена на рис. 2.18). Эти данные нужны либо для прямой оценки остаточного времени (если статистики достаточно), либо для формирования начальных исходных данных для моделирования с использованием гипотетичных данных (если статистики недостаточно).

Рис. 3.28 Оценки ожидаемого времени до критичного нарушения

При формировании начальных значений для моделирования рассматриваются два случая: случай 1 – оценка по достаточной статистике и случай 2 – прогнозирование с применением вероятностных моделей, если нет достаточной статистики.

Для случая 1 – по достаточной статистике - берутся последние 6 месяцев. Если по используемой статистике были N прецедентов перехода параметра в элементарное состояние «за пределами нормы» (т.е. в «желтый» диапазон) в моменты $t_1, t_2, \ldots, t_N$, то для момента оценки при нахождении значений параметра за пределами рабочего диапазона (т.е. в «желтой» зоне) ожидаемый временной ресурс, имеющийся для принятия упреждающих мер до перехода в состояние «за пределами нормы» (в «красную» зону), полагается равным в среднем $T_{упрежд.ож.}$:

$$T_{упрежд.ож.} = [(t_1 - t_{1\ за\ раб.}) + (t_2 - t_{2\ за\ раб.}) + \ldots + (t_S - t_{S\ за\ раб.})]/S,$$

где $t_{s\ за\ раб.}$ – это первый до s-го прецедента момент выхода значений параметра из элементарного состояния «в рабочих пределах» (из «зеленой» зоны) за установленные пределы после восстановления целостности оборудования после (s-1)-го пребывания в состоянии «за пределами нормы» (в «красную» зону), $s=1,\ldots,S$, $t_0=0$.

Наряду с оценкой среднего времени $T_{упрежд.ож.}$ определяется среднее время восстановления $T_{восст.}$ (см. рис. 3.28).

$T_{восст.} = [(t_{1ж.} - t_{1кр.}) + (t_{2ж.} - t_{2кр.}) + \ldots + (t_{Sж.} - t_{Sкр.})]/S,$

где $t_{Sкр.}$ – это момент первого s-го прецедента выхода «за пределы нормы» (в «красную» зону из «желтой»), s=1,…,S;

$t_{Sж.}$ – это момент первого возврата в пределы нормы (в «желтую» зону) после s-го перехода «за пределы нормы» (в «красную» зону), s=1,…,S.

Примечание. Статистика исчисляется с момента последнего прецедента, т.е. $T_{конца}$. Это сделано для уменьшения ненужной детализации статистики, чтобы избежать избыточных сложностей с усреднением весовых значений на «концах».

3.4.3 Формирование последующих значений при обновлении данных

Формирование последующих значений при обновлении данных в СДК ПБ осуществляется для того, чтобы каждый раз не анализировать всю статистику, а использовать итерационный пересчет. Тем самым сокращается время модельных расчетов.

Рассматриваются те же два случая: случай 1 – оценка по достаточной статистике и случай 2 – прогнозирование с применением вероятностных моделей, если нет достаточной статистики.

Случай 1 – по достаточной предыдущей статистике.

В базе данных содержится текущее среднее время $T_{упрежд.ож. (n)}$, построенное для $S_{(n)}$ отклонений или по предыдущим итерациям.

$T_{упрежд.ож. (n)} = [(t_1 - t_{1 за раб.}) + (t_2 - t_{2 за раб.}) + \ldots + (t_S - t_{S за раб.})]/S_{(n)},$

а также среднее время восстановления $T_{восст.}$:

$T_{восст. (n)} = [(t_{1ж.} - t_{1кр.}) + (t_{2ж.} - t_{2кр.}) + \ldots + (t_{Sж.} - t_{Sкр.})]/ S_{(n)}.$

Для нового среза произошли дополнительно $S_{(+1)}$ отклонений (например, 1, 2 или больше). Начиная с окончания предыдущего среза используется накопленная статистика за время $T_{среза(+1)}$, куда добавляется время до предыдущего прецедента. Для этого периода $T_{среза(+1)}$ определяется свое $T_{упрежд.ож.(+1)}$ методами, изложенными выше.

Тогда с учетом взвешивания пропорционально длительностям периодов $T_{статистики}$ и $T_{среза(+1)}$ имеем:

$T_{упрежд.ож.(n+1)} = [T_{статистики} \times T_{упрежд.ож.(n)} + T_{среза(+1)} \times T_{упрежд.ож.(+1)}] / [T_{статистики (без} T_{конца)} + T_{среза(+1)}].$

При формировании начальных исходных данных для вероятностного моделирования используются те же рассуждения.

Тогда с учетом взвешивания пропорционально длительностям периодов $T_{статистики}$ и $T_{среза(+1)}$ имеем:

текущая частота возникновения угроз $\sigma_{(n+1)}$ равна

$\sigma_{(n+1)} = [T_{статистики} \times \sigma_{(n)} + T_{среза(+1)} \times \sigma_{(+1)}] / [T_{статистики} + T_{среза(+1)}].$

Примечание. Статистика исчисляется с момента последнего прецедента, т.е. $T_{конца}$. Это сделано для уменьшения ненужной детализации статистики, чтобы избежать избыточных сложностей с усреднением «концов» при формировании (n+1)-го значения $\sigma_{(n+1)}$ по $\sigma_{n.}$.

Для случая 2 – без достаточной статистики – для вероятностного моделирования используются те же рассуждения и те же формулы при формировании начальных исходных данных. Отличие в том, что за счет использования гипотетических сценариев результаты прогнозных расчетов могут иметь несколько иную интерпретацию.

В случае 2, если статистических данных недостаточно (в т.ч., если вообще нет), производится прогноз времени для условий:

– если на изменение цвета с «зеленого» на «желтый» нет реакции должностных лиц (т.е., если на практике наблюдается игнорирование данных СДК ПБ);

– если всегда следует оперативная реакция на сигнал (т.е., если на практике наблюдается восприятие сигналов СДК ПБ как руководство к возвращению значений параметра в рабочий диапазон) - см. рис.3.29.

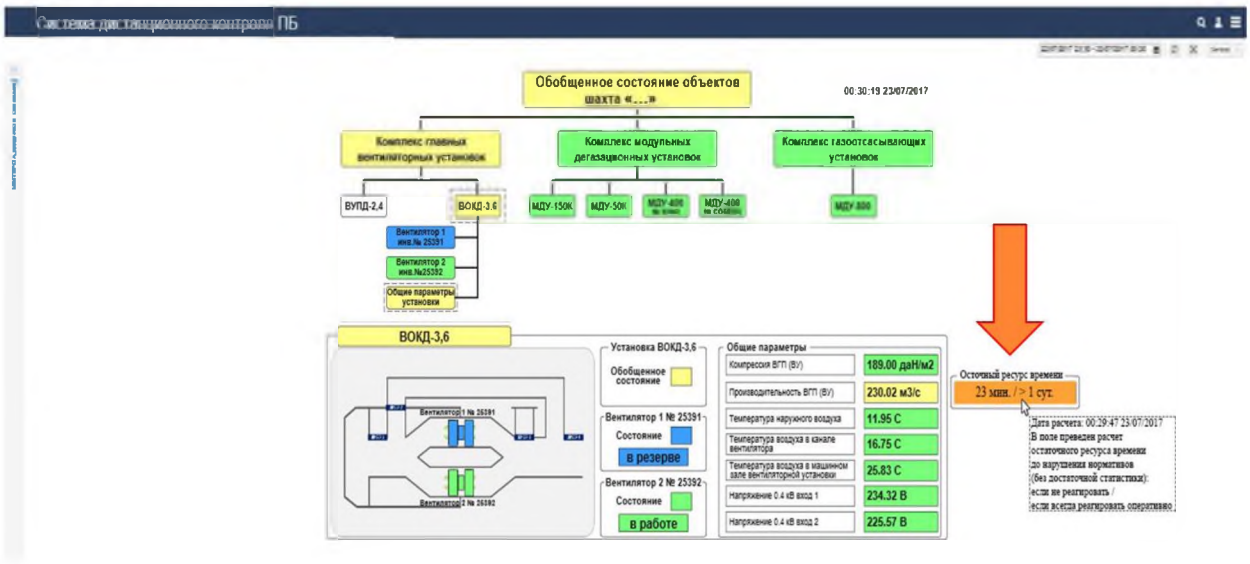


Рис. 3.29 Пример ожидаемого результата при недостаточной статистике

В случае большого остаточного ресурса времени (например, более суток, месяцы, годы) на экране имеет смысл отображать оценку « >1 сут., если реагировать оперативно». В СДК ПБ это необходимо для избегания ненужных расслаблений в среде обслуживающего персонала объектов опасного производства. В аналитическом отчете могут быть даны разъяснения, связанные с прикладной интерпретацией прогноза остаточного временного ресурса.

3.4.4 Прикладная интерпретация прогноза остаточного временного ресурса для формирования базы знаний

На практике прогнозируемое значение времени у обслуживающего персонала на принятие и реализацию решения для предотвращения нарушения границы нормативного диапазона по данным от СДК ПБ может (и, как правило, будет) отличаться от реальных событий. Действительно, в ряде случаев указанное время проходит, а прогнозируемый переход за границы нормативного диапазона не происходит, хотя пребывание значений отслеживаемого параметра за пределами рабочего диапазона сохранялось.

Теоретическое объяснение этого в том, что прогнозируемое среднее время на принятие и реализацию решения для предотвращения нарушения границы нормативного диапазона будет не менее $T_{упрежд.прогноз.min}$ и не более $T_{упрежд.прогноз.max}$ с доверительной вероятностью от 0.95 до 0.99, например, на рис. 3.30 – от 12 до 52 суток. Это интерпретируется так: при многократном повторении ситуаций ориентация на минимальное время прогнозного диапазона (12 суток для принятия упреждающих мер), в 99 случаях из 100 за эти 12 суток перехода за границы нормативного диапазона не произойдет, т.е. лишь в одном случае из 100 возможно нарушение нормативного диапазона. Если же ориентироваться на максимальное время прогнозного диапазона (52 суток для принятия упреждающих мер), то в 95 случаях из 100 за эти 52 суток перехода за границы нормативного диапазона не произойдет, т.е. лишь в 5 случаях из 100 возможно нарушение нормативного диапазона за эти 52 суток.

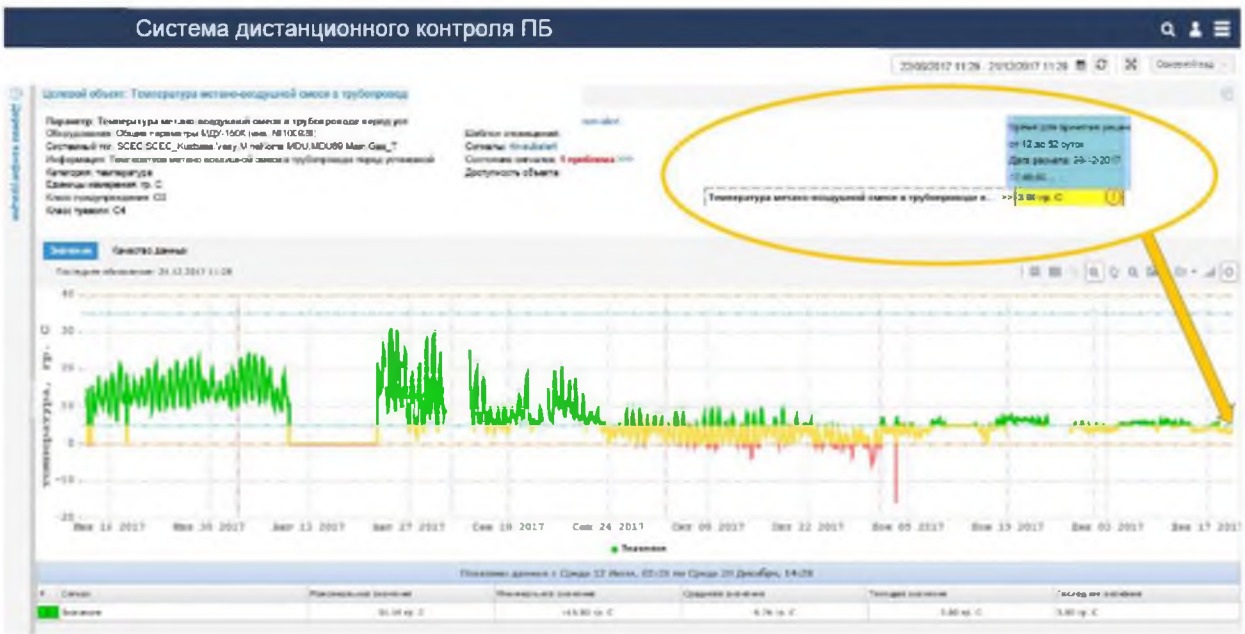


Рис. 3.30 Статистика за полгода для прогноза остаточного временного ресурса по параметру «температура метано-воздушной смеси»

В рамках прототипа базы знаний осуществляется наглядное доказательство практичности вероятностного моделирования с использованием собираемой статистики. Причем не требуется проведения специальных экспериментов (с умышленным ожиданием нарушения нормативного диапазона, т.к. такие эксперименты без дополнительных мер могут рассматриваться как халатность, а при наступлении ущерба – как умышленное вредительство).

Для доказательства используется статистическое определение исходных данных σ - частоты выхода значений параметра за пределы рабочего диапазона (определяется автоматически по статистике данных, собираемых в СДК ПБ), β - среднего времени до перехода значений параметра за границы нормативного диапазона после выхода за пределы рабочего диапазона. Здесь используются теоретические результаты, полученные во 2-м разделе (Теоремы 2-4 и следствие из Теоремы 2). Также по статистике определяется количество нарушений ПБ (имевших место инцидентов) при общем количестве оцениваемых событий. Для чистоты доказательств в базе знаний важно, чтобы количество нарушений границ нормативного диапазона измерялось как минимум, несколькими единицами, а общее количество – сотнями при обычных условиях эксплуатации. Отношение количества нарушений границ нормативного диапазона к общему количеству оцениваемых событий выхода за пределы рабочего диапазона дает оценку вероятности нарушений границ нормативного диапазона. Далее для этих же исходных данных осуществляются расчеты по предложенным моделям. Результаты сравнения должны быть устойчиво близки. Это служит дополнительным доказательством практической полезности прогнозирования остаточного временного ресурса в режиме реального времени функционирования СДК ПБ.

3.5 Создание прототипа технологии поддержки риск-ориентированной системной инженерии

Разработанные базовые модели и программные решения (раздел 2), концептуальный облик технологических решений для ВС и КС (подраздел 3.1), способ аналитического комплексирования программных решений (подраздел 3.2), встроенные технологические возможности по предоставлению обобщенных и детальных вероятностных прогнозов (подраздел 3.3), сформированный прототип базы знаний для моделирования (подраздел 3.4), объединенные общим замыслом диссертации, позволили создать прототип технологии поддержки риск-ориентированной системной инженерии – см. рис. 3.31 [167].

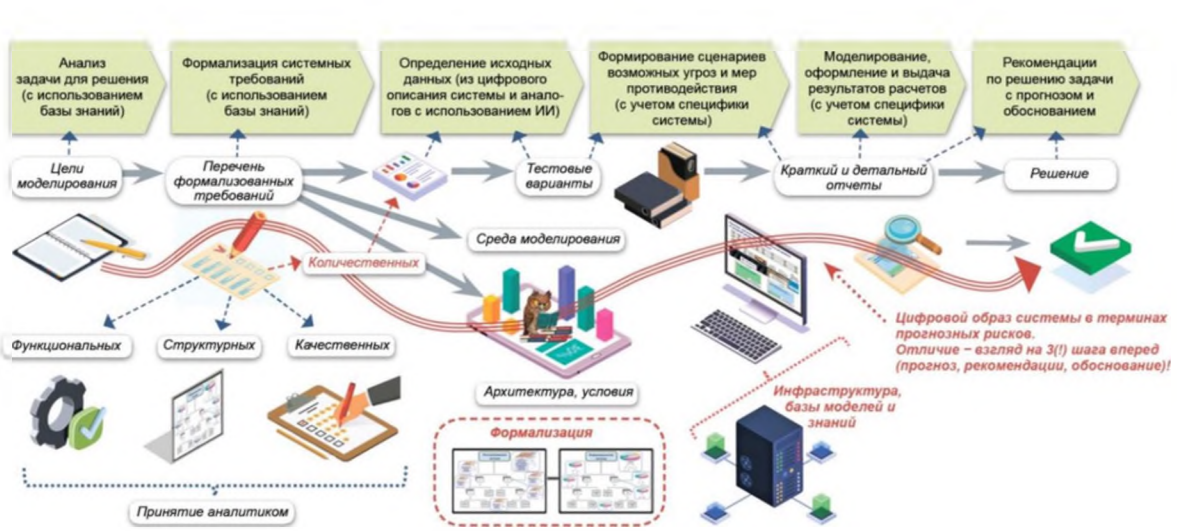


Рис. 3.31 Иллюстрация созданного прототипа технологии поддержки риск-ориентированной системной инженерии

В общем случае применение предлагаемого прототипа нацелено на аналитическую поддержку следующих задач риск-ориентированной системной инженерии (не ограничиваясь перечисленными ниже):

задач оценки специальных показателей рисков, связанных с критичными сущностями рассматриваемой системы;

задач прогнозирования рисков, свойственных реализуемым системным процессам;

задач обоснования допустимых значений специальных показателей, связанных с критичными сущностями рассматриваемой системы, и допустимых рисков;

задач определения существенных угроз и условий для рассматриваемых системных процессов, системы и/или проекта с использованием прогнозируемых рисков,

комплексом задач поддержки принятия решений по обеспечению качества, безопасности и/или эффективности рассматриваемой системы в ее жизненном цикле.

Инфраструктура прототипа представляет собой совокупность клиент-серверных программных модулей, разделенных на подготовку данных для анализа, расчет и прогноз, мониторинг данных и аналитическое обоснование рекомендаций.

Исходя из целей моделирования с помощью прототипа осуществляется анализ самой задачи системной инженерии для решения и последующая формализация системных требований с использованием созданного прототипа базы знаний.

Далее с учетом среды моделирования (off-line, on-line или встроенное моделирование в АСУ ТП), исходя из цифрового описания моделируемой системы или аналога определяются необходимые исходные данные. С учетом специфики системы формируются сценарии возможных угроз и мер противодействия угрозам.

После этого осуществляется моделирование, оформление и выдача результатов расчетов с предоставлением соответствующих рекомендаций по решению задачи системной инженерии с необходимыми прогнозом и обоснованием.

Разработанный укрупненный алгоритм практического применения прототипа технологии поддержки риск-ориентированной системной инженерии представлен на рис. 3.32.

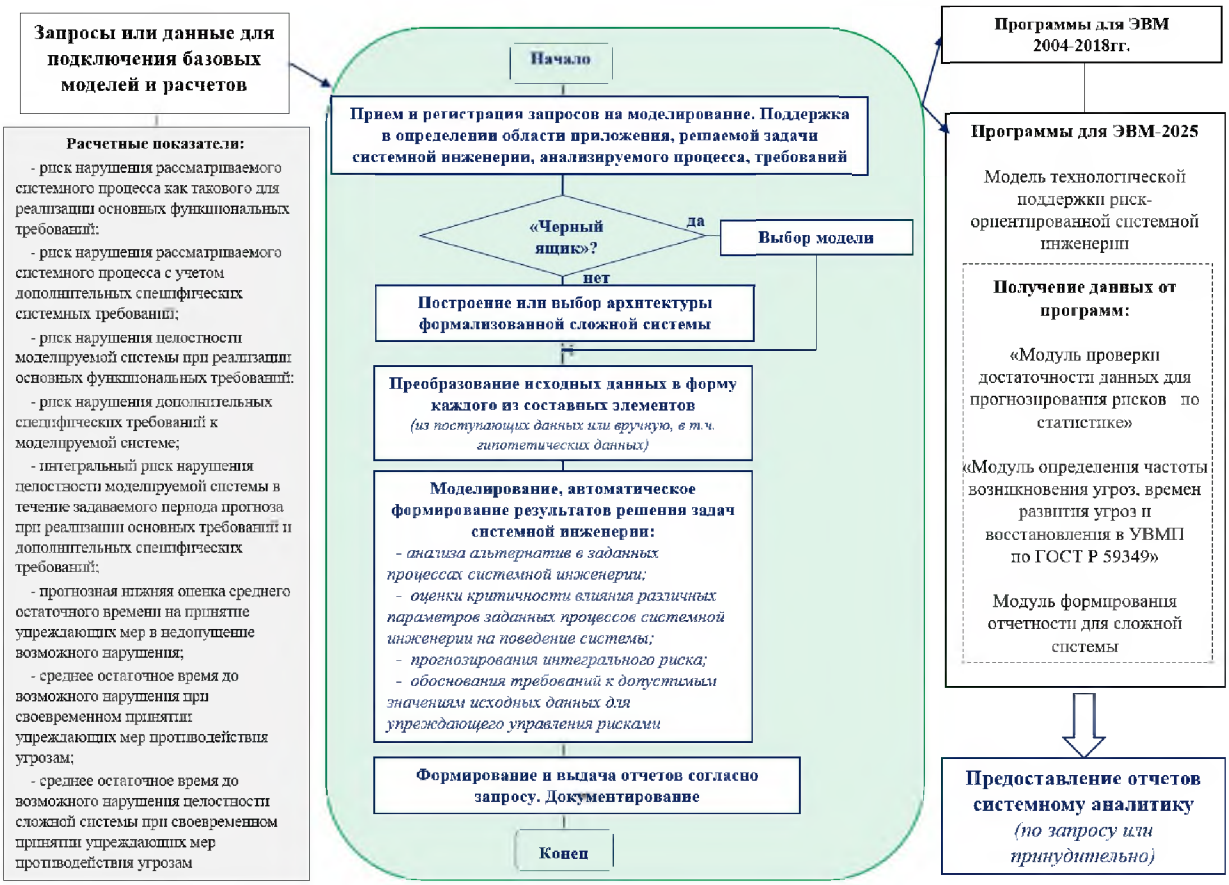


Рис. 3.32 Укрупненный алгоритм практического применения созданного прототипа для общего случая

Запросы или данные для подключения базовых моделей и расчетов инициируют функциональное подключение прототипа.

В общем случае расчетными показателями являются:

- риск нарушения целостности моделируемой системы за период прогноза при реализации основных функциональных требований;

- риск нарушения дополнительных специфических требований к моделируемой системе за период прогноза;

- интегральный риск нарушения целостности моделируемой системы за период прогноза при реализации основных функциональных требований и дополнительных специфических требований;

- прогнозная оценка среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра;

- среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра при своевременном принятии упреждающих мер противодействия угрозам;

- среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Прототип реализует прием и регистрацию запросов на моделирование. Осуществляется поддержка в определении области приложения, непосредственно самой решаемой задачи системной инженерии, а также анализируемого процесса и требований, подлежащих учету при решении задачи (законодательных, правовых, нормативных, специфических).

После этого имеет место определение способа моделирования: с использованием «черного ящика» или с использованием сложной системы, логически представляемой последовательно-параллельной структурой из «черных ящиков». В последнем случае для рассматриваемой системы осуществляется построение или выбор архитектуры формализованной сложной системы – см. п. 2.2.4.2 «Теоретическое обоснование возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков».

После формализации осуществляется преобразование исходных данных в форму каждого из составных элементов (из поступающих данных или вручную, в т.ч. гипотетических данных), для «черного ящика» система состоит из одного элемента.

Далее реализуется непосредственно моделирование, автоматическое формирование результатов решения задач системной инженерии, в т.ч. таких, как задач:

- анализа альтернатив в заданных процессах системной инженерии;

- оценки критичности влияния различных параметров заданных процессов системной инженерии на поведение системы;

- прогнозирования интегрального риска;

- обоснования требований к допустимым значениям исходных данных для упреждающего управления рисками.

В заключение сеанса с помощью прототипа осуществляется формирование и выдача отчетов согласно содержания изначального запроса, а также необходимое документирование по этому запросу.

С учетом специфики рассматриваемой системы возможна адаптация в применении предложенного прототипа технологии поддержки риск-ориентированной системной инженерии. Так, адаптированный алгоритм применения прототипа для встроенных технологических возможностей для систем дистанционного контроля (мониторинга) промышленной безопасности (СДК) в опасном производстве представлен на рис. 3.33.

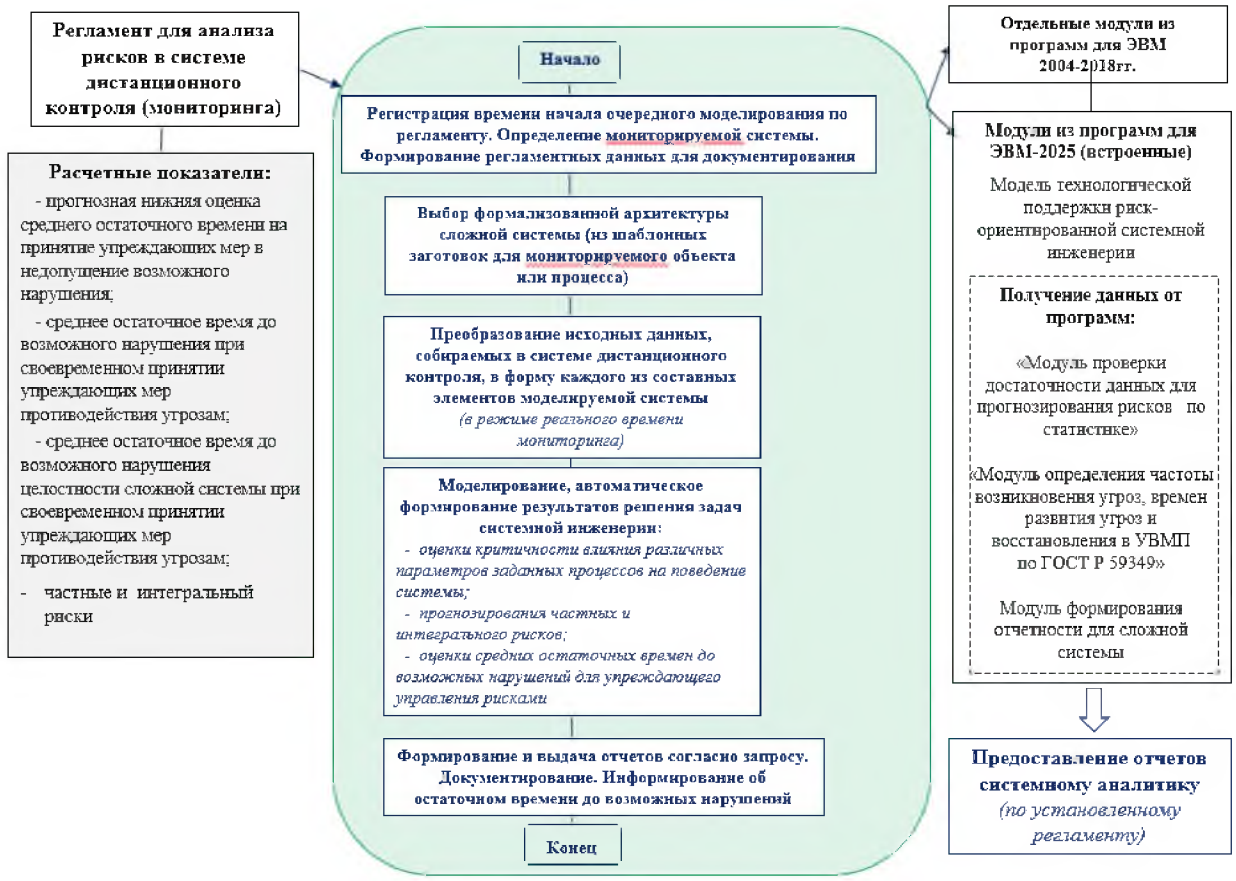


Рис. 3.33 Алгоритм применения прототипа для встроенных технологических возможностей

В данном случае порядок инициации запросов для формального подключения базовых моделей и расчетов определяется регламентом для анализа рисков в СДК.

Основными расчетными показателями являются:

- среднее остаточное время на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта;

- среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Прототип реализует регистрацию времени начала очередного моделирования по регламенту. Осуществляется определение мониторируемой системы, формируются регламентные данные для документирования.

После этого из шаблонных заготовок для мониторируемого объекта или процесса, исходя из специфики определенной на предыдущем шаге мониторируемой системы (например, исходя из специфики конкретного оборудования), осуществляется выбор формализованной архитектуры сложной системы.

Далее осуществляется преобразование исходных данных, собираемых в СДК, в форму каждого из составных элементов моделируемой системы (в режиме реального времени процесса мониторинга).

И после этого реализуется непосредственно моделирование и автоматическое формирование результатов решения задач системной инженерии, в частности:

- оценки критичности влияния различных параметров заданных процессов на поведение системы;

- прогнозирования частных и интегрального рисков;

- оценки средних остаточных времен до возможных нарушений для упреждающего управления рисками.

В завершении регламентного подключения прототипа осуществляется формирование и выдача отчетов согласно запросу, а также необходимое документирование по этому запросу и информирование об остаточном времени до возможных нарушений.

Примеры см. выше в подразделах 3.3, 3.4, а также в разделах 4, 5.

Таким образом, создан прототип технологии поддержки риск-ориентированной системной инженерии, основанный на идеях информационно-логической, программной и технологической интеграции разработанных базовых моделей и программных решений (раздел 2), концептуального облика технологических решений для ВС и КС (подраздел 3.1), предложенного способа аналитического комплексирования программных решений (подраздел 3.2), встроенных технологических возможностей по предоставлению обобщенных и детальных вероятностных прогнозов (подраздел 3.3), сформированного прототипа базы знаний для моделирования (подраздел 3.4). Практическое использование прототипа поддерживается разработанной программой для ЭВМ - «Моделью

технологической поддержки риск-ориентированной системной инженерии», организационно (и в ряде случаев – програмно) скомплексированном с другими разработанными программами для ЭВМ [168 – 180]:

«Моделирование процессов в жизненном цикле систем "Моделирование процессов" - "ноу-хау"» (Свидетельство о государственной регистрации программы для ЭВМ №2004610858);

«Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2006610219);

«Программно-инструментальный комплекс оценки качества функционирования информационных систем через Интернет «КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008612348);

«Программно-инструментальный комплекс сопровождения систем менеджмента качества «OPISys-КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008614525);

«Программно-вычислительный комплекс оценки качества производственных процессов» (Свидетельство о государственной регистрации программы для ЭВМ № 2010614145);

«Комплекс для оценки качества информационных и административно-управленческих процессов при функционировании электронного правительства (КОК-ЭП)» (Свидетельство о государственной регистрации программы для ЭВМ № 2010617017);

«Удаленная аналитическая поддержка информирования о вероятностно-временных показателях функционирования системы и ее элементов при реализации риск-ориентированного подхода» (Свидетельство о государственной регистрации программы для ЭВМ №2018617949);

«Удаленное обоснование требований к средствам и условиям обеспечения качества функционирования «умных» систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618572);

«Удаленное вероятностное прогнозирование качества функционирования информатизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618686);

«Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021»;

«Модуль формирования отчетности по результатам вероятностного прогнозирования

рисков для сложной системы с последовательным соединением элементов»;

«Модуль проверки достаточности данных для прогнозирования рисков по статистике»;

«Модель технологической поддержки риск-ориентированной системной инженерии».

В общем случае при использовании технологических возможностей расчетными показателями являются:

- риск нарушения целостности моделируемой системы за период прогноза при реализации основных функциональных требований;

- риск нарушения дополнительных специфических требований к моделируемой системе за период прогноза;

- интегральный риск нарушения целостности моделируемой системы за период прогноза при реализации основных функциональных требований и дополнительных специфических требований;

- прогнозная оценка среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра;

- среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра при своевременном принятии упреждающих мер противодействия угрозам;

- среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Ряд созданных технологических возможностей продемонстрирован на практических примерах.

3.6 Выводы по разделу 3

В итоге проведенных выше исследований создан комплекс новых программных и технологических решений для ВС и КС, охватывающий: решения по программной инфраструктуре глобально распределенного прогнозирования рисков и моделированию процессов; комплексы программ моделирования систем для прогнозирования рисков, выявления угроз, анализа альтернатив и обоснования системных требований к характеристикам процессов; прототип базы знаний для подготовки исходных данных для моделирования и поддержки принятия аналитических решений на стадиях жизненного цикла систем; технологические решения по интеграции моделей и созданных комплексов программ, обеспечивающие реализацию новых аналитических возможностей по вероятностному прогнозированию и упреждающему управлению рисками.

Основные результаты исследований характеризуются следующими научно-техническими аспектами.

1. Разработан концептуальный облик технологических решений для ВС и КС. Реализация предложенных концептуальных положений по упреждающему управлению рисками опирается на вероятностное моделирование, прогнозирование и оптимизацию для системного решения задач и обоснования возможных упреждающих действий в условиях неопределенности. В свою очередь, прогнозирование базируется на мониторинге состояний, накоплении и рациональном использовании знаний, в т.ч. формируемых в режиме реального времени функционирования различных систем.

Показано, что при реализации предлагаемого подхода системный аналитик будет оперировать цифровым образом рассматриваемых систем в терминах прогнозных рисков. Отличие от существующих инструментариев – взгляд условно на 3 шага вперед, это - прогноз, рекомендации и обоснование решений для задач системной инженерии.

2. Предложен вариант послойного аналитического комплексирования разработанных программных решений на различных мета-уровнях. При этом многомодальное взаимодействие с источниками данных осуществляется с использованием: телеметрических данных от оборудования; данных, выбираемых из базы данных, учитывающей специфику приложений системы, в т.ч. в различных форматах; данных, вводимых в формате программных решений базовых моделей.

В интересах решения задач системной инженерии реализован мониторинг и прогноз риска нарушения приемлемого выполнения заданных процессов системной инженерии. В рамках созданных программно-технологических решений используются различные человеко-машинные интерфейсы, приспособленные для применения предложенных базовых моделей.

Показано, что при этом осуществляются:

- в ЖЦ системы: информирование о системных требованиях к характеристикам системы, предоставление необходимых данных, учет условий и принятых ограничений;

- на этапах разработки, модернизации и развития системы: прогнозирование рисков, анализ альтернатив по результатам расчетов;

- на этапах эксплуатации и сопровождения системы: прогнозирование рисков, оценка критичности влияния различных параметров на поведение системы;

- при проектировании, выполнении, контроле и управлении процессами: реализации аналитических возможностей по выявлению существенных угроз и приемлемых условий для анализируемых процессов;

- при интеграции исследований на различных мета-уровнях: прогнозирование интегрального риска, в т.ч. для совокупности стандартных процессов в ЖЦ системы, обоснование условий удержания рисков в допустимых пределах.

3. Разработаны и описаны встроенные технологические возможности по предоставлению обобщенных и детальных вероятностных прогнозов, доведенные до реализации в СДК ПБ на объектах опасного производства. Разработан программно-технологический «Модуль формирования отчетности по результатам вероятностного прогнозирования рисков для сложной системы с последовательным соединением элементов». В итоге применения предлагаемых технологических возможностей ответственному лицу СДК ПБ предоставляются аналитические отчеты, содержащие следующие показатели, рекомендованные ГОСТ Р 58494-2019 «Оборудование горно-шахтное. МФСБ. Система дистанционного контроля опасных производственных объектов»:

прогнозируемое остаточное время на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона при каждом выходе значений параметра за границы рабочего диапазона;

условные средние времена до выхода значений параметра за границы нормативного диапазона для условий, если оперативно реагировать на выходы значений параметров за границы рабочего диапазона и если не реагировать на эти отклонения;

риски нарушения границ нормативного диапазона хотя бы по одному из контролируемых параметров за смену, сутки, неделю, месяц, год с учетом последствий (в вероятностном представлении).

4. Разработан «Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в УВМП по ГОСТ Р 59349», позволяющий определять необходимые исходные данные для моделирования: частоту возникновения источников

угроз, среднее время развития угроз и среднее время восстановления нарушаемой целостности моделируемой системы. Показано, как эти исходные данные формируются автоматически из базы данных созданных СДК ПБ.

5. Сформирован прототип базы знаний для моделирования, позволяющий определять «достаточность» используемой статистики при формировании следующих исходных данных: частоты возникновения источников угроз, среднего времени развития угроз и среднего времени восстановления нарушаемой целостности моделируемой системы формируются автоматически из БД с использованием разработанного «Модуля определения частоты возникновения угроз, времен развития угроз и восстановления в УВМП по ГОСТ Р 59349». Указаны способы повышения практической полезности прогнозирования остаточного временного ресурса в режиме реального времени функционирования СДК ПБ.

6. Создан прототип технологии поддержки риск-ориентированной системной инженерии, основанный на новых программных и технологических решениях для ВС и КС, поддерживающий информационно-логическую, программную и технологическую интеграцию разработанных базовых моделей и программных решений для ВС и КС и обеспечивающий путем моделирования упреждающее выявление «узких мест» и определение рациональных способов снижения и удержания рисков в допустимых пределах на стадиях жизненного цикла систем различного функционального назначения в условиях реальных и гипотетических вызовов и угроз, а также оформление и выдачу результатов расчетов с предоставлением соответствующих рекомендаций по решению задач системной инженерии. Инфраструктура прототипа представляет собой совокупность клиент-серверных программных модулей, разделенных на подготовку данных для анализа, расчет и прогноз, мониторинг данных и аналитическое обоснование рекомендаций. Исходя из целей моделирования с помощью прототипа осуществляется анализ самой задачи системной инженерии для решения и последующая формализация системных требований с использованием созданного прототипа базы знаний. Далее с учетом среды моделирования (off-line, on-line или встроенное моделирование в АСУ ТП), исходя из цифрового описания моделируемой системы или аналога определяются необходимые исходные данные. С учетом специфики системы формируются сценарии возможных угроз и мер противодействия угрозам. После этого осуществляется моделирование, оформление и выдача результатов расчетов с предоставлением соответствующих рекомендаций по решению задачи системной инженерии.

Для упреждающего управления рисками в приложениях системной инженерии практическое использование прототипа поддерживается описанной «Моделью

технологической поддержки риск-ориентированной системной инженерии», организационно (и в ряде случаев – программно) скомплексированном с другими разработанными программами для ЭВМ:

«Моделирование процессов в жизненном цикле систем "Моделирование процессов" - "ноу-хау"» (Свидетельство о государственной регистрации программы для ЭВМ №2004610858);

«Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2006610219);

«Программно-инструментальный комплекс оценки качества функционирования информационных систем через Интернет «КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008612348);

«Программно-инструментальный комплекс сопровождения систем менеджмента качества «OPISys-КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008614525);

«Программно-вычислительный комплекс оценки качества производственных процессов» (Свидетельство о государственной регистрации программы для ЭВМ № 2010614145);

«Комплекс для оценки качества информационных и административно-управленческих процессов при функционировании электронного правительства (КОК-ЭП)» (Свидетельство о государственной регистрации программы для ЭВМ № 2010617017);

«Удаленная аналитическая поддержка информирования о вероятностно-временных показателях функционирования системы и ее элементов при реализации риск-ориентированного подхода» (Свидетельство о государственной регистрации программы для ЭВМ №2018617949);

«Удаленное обоснование требований к средствам и условиям обеспечения качества функционирования «умных» систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618572);

«Удаленное вероятностное прогнозирование качества функционирования информатизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618686);

«Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021»;

«Модуль формирования отчетности по результатам вероятностного прогнозирования

рисков для сложной системы с последовательным соединением элементов»;

«Модуль проверки достаточности данных для прогнозирования рисков по статистике»;

«Модель технологической поддержки риск-ориентированной системной инженерии».

В общем случае при использовании технологических возможностей расчетными показателями являются:

- риск нарушения целостности моделируемой системы за период прогноза при реализации основных функциональных требований;

- риск нарушения дополнительных специфических требований к моделируемой системе за период прогноза;

- интегральный риск нарушения целостности моделируемой системы за период прогноза при реализации основных функциональных требований и дополнительных специфических требований;

- прогнозная оценка среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра;

- среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра при своевременном принятии упреждающих мер противодействия угрозам;

- среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Ряд созданных технологических возможностей продемонстрирован на практических примерах.

4. РАЗРАБОТКА ТИПОВЫХ МЕТОДИК ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ПОДДЕРЖКИ РИСК-ОРИЕНТИРОВАННОЙ СИСТЕМНОЙ ИНЖЕНЕРИИ

С учетом разработанных в разделах 2 и 3 программных и технологических решений для ВС и КС в настоящем разделе предлагаются методические решения, включающие:

- общие положения по разработке типовых методик;

- типовую методику прогнозирования рисков нарушения целостности моделируемой системы, представимой в виде «черного ящика», на различных мета-уровнях;

- пример определения границ рабочего диапазона критичных параметров мониторируемого объекта по видеоданным;

- типовую методику прогнозирования рисков нарушения целостности сложной моделируемой системы;

- пример упреждающего управления рисками для системы дистанционного контроля промышленной безопасности.

Применение предложенных методических решений демонстрируется на приложениях к исследованию функционирования гипотетичной угольной шахты, включая:

- сравнение ручного контроля расхода воды в системе водоотлива с автоматическим контролем и восстановлением водного баланса с использованием системы дистанционного контроля (СДК);

- определение границ рабочего диапазона критичных параметров контролируемого оборудования;

- прогнозирование рисков нарушения промышленной безопасности (ПБ) главной вентиляторной установки (ГВУ) шахты и утраты работоспособности ГВУ для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках системы контроля без использования возможностей СДК и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

- прогнозирование рисков нарушения ПБ на опасном производственном объекте (ОПО), рассматриваемом как сложная система, когда в качестве мониторируемых подсистем выступают комплексы главных вентиляторных установок (ГВУ), модульных дегазационных установок (МДУ), газоотсасывающих установок;

- обоснование путей усовершенствования (перевооружения) системы вентиляции, аспирации и пылеподавления на обогатительной фабрике.

С использованием разработанных методических решений осуществлен самоанализ надежности функционального применения созданного прототипа технологии поддержки риск-ориентированной системной инженерии.

4.1 Общие прикладные подходы к разработке типовых методик [167]

Основной особенностью предлагаемых типовых методик является их ориентация на применение созданного прототипа технологии поддержки риск-ориентированной системной инженерии, включая применение предложенных в разделах 2 и 3 теоретических усовершенствований и сформированных базовых моделей и методов для анализа системных элементов и сложных систем, созданных авторских программных и технологических решения для ВС и КС – см. рис. 4.1.

Рис. 4.1 Связь предлагаемых методических решений с результатами исследований 2-го и 3-го разделов

Предлагаемые методические решения включают в себя комплекс типовых методик по применению разработанных вероятностных моделей, программных и технологических решений для пользователей ВС и КС. Приводятся примеры, призванные продемонстрировать работоспособность методик. В совокупности с примерами из раздела 5 приводятся рекомендации по повышению качества, безопасности и извлечению прагматических эффектов для систем различного функционального назначения.

В качестве исследуемой для прогнозирования рисков может выступать система, целенаправленно создаваемая человеком для различных приложений с учетом

усовершенствований, программных и технологических решений, описанных в разделах 2 и 3 диссертации, это:

отдельная система, рассматриваемая как единое целое и представимая в виде «черного ящика» (см. базовые модели);

сложная система, формализуемая согласно положениям 2.4.2;

система систем, которая также может быть формализуема согласно положениям 2.4.2.

Примечание. Система систем (СС) — это совокупность систем, которые взаимодействуют между собой для обеспечения уникальных возможностей, которые ни одна из входящих в нее систем не может реализовать самостоятельно. Составляющая система представляет собой автономную систему, каждая из которых создавалась разными заказчиками со своими целями, задачами, кругом пользователей, жизненным циклом, в разные, заранее не согласованные, сроки (по ГОСТ Р 57193).

Примерами исследуемых систем могут служить энергетические и промышленные структуры (в т.ч. отдельные предприятия, нефтегазовые и транспортные комплексы, предприятия опасного производства, фармацевтические заводы), автоматизированные системы управления, информационно-телекоммуникационные системы, цифровые двойники, различные системы с использованием искусственного интеллекта и др., состоящие из подсистем и/или системных элементов, также подлежащих рассмотрению – подробнее см. примеры в разделах 4, 5.

Поскольку предлагаемые методики ориентируются не только на авторские решения (т.е. при использовании методик применимы не только решения из разделов 2 и 3), то предполагается, что в состав материально-технического и метрологического обеспечения для каждой методики входят (по возможности):

- конструкторская и эксплуатационная документация на исследуемую систему;
- перечень отслеживаемых угроз, вербальные модели угроз;
- системный журнал учета предпосылок к нарушениям и самих нарушений целостности исследуемой системы (например, инцидентов, аварий);
- планы ликвидации аварийных ситуаций и восстановления целостности исследуемой системы после нарушений целостности;
- обязанности должностных лиц и инструкции по эксплуатации исследуемой системы и ее составных элементов;
- инструментально-моделирующие комплексы подсистемы поддержки принятия решений (например, из раздела 3), реализующие математические методы расчетов выбранных показателей (например, с использованием базовых моделей из раздела 2).

По результатам применения методик составляется соответствующий протокол или отчет.

В завершении 4-го раздела приведены результаты некоторого анализа надежности функционального применения созданного прототипа технологии поддержки риск-ориентированной системной инженерии (т.е. прототип применен для системного анализа самого себя).

4.2 Типовая методика прогнозирования рисков нарушения целостности моделируемой системы, представимой в виде «черного ящика»

4.2.1 Исследуемая система

В качестве исследуемой выступает отдельная моделируемая система, рассматриваемая как единое целое и представимая для моделирования в виде «черного ящика» на различных мета-уровнях (см. рис. 1.7 в разделе 1 и базовые модели в разделе 2). Примерами такой исследуемой системы могут служить системный процесс, оборудование предприятия, рассматриваемое как самостоятельный производственный объект, отдельный критичный параметр мониторируемого объекта, конкретная критичная сущность в задаваемых условиях, рассматриваемая как единое целое (например, система водоотлива на угольной шахте, контролирующая расход воды, подаваемой в вакуум-насос (см. 4.2.7). Другой пример критичной сущности - зерно в складских условиях хранения (см. подраздел 5.4), отдельный оператор или группа операторов, рассматриваемая как единое целое.

4.2.2 Цель прогнозирования рисков

Основной целью прогнозирования рисков является установление степени вероятного нарушения целостности исследуемой системы за период прогноза в интересах решения следующих аналитических задач:

оценки риска в течение заданного периода прогноза безотносительно уровня допустимого риска и в сравнении с установленным допустимым риском для различных сценариев возникновения и развития угроз, применяемых мер системного контроля состояний и восстановления целостности системы;

научного обоснования уровня допустимого риска для исследуемой системы по «прецедентному принципу»;

научного обоснования критичных условий возникновения различных угроз;

сравнительного анализа различных вариантов поведения системы для возможных сценариев развития угроз и мер противодействия угрозам;

научного обоснования упреждающих мер по снижению или удержанию в допустимых пределах рисков и/или снижению затрат и/или возможных ущербов в практике создания, эксплуатации, технического обслуживания, модернизации и развития системы при задаваемых ограничениях;

создания базы знаний и вариантов решения типовых практических задач упреждающего управления рисками.

4.2.3 Общие положения

В качестве общих используются положения из подразделов 1.2, 1.3 (рис. 1.7), положения из 2.1, 2.2.1, 2.2.2 с усовершенствованиями и возможностями согласно Теореме 1 (о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности), Теореме 2 (об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта), выявленным закономерностям в соотношениях исходных данных для непревышения задаваемого допустимого уровня риска и сохранения целостности моделируемой системы, Следствию из Теоремы 2 (об ограничениях при выборе периода между диагностиками целостности системы, ориентированного на непревышение допустимого риска нарушения целостности системы), Теореме 3 (о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам) из раздела 2 (см. также приложение А).

4.2.4 Оцениваемые показатели и расчетные соотношения

К оцениваемым показателям для исследуемой системы, представленной в виде «черного ящика» для исследований на различных мета-уровнях, относятся:

- риск нарушения целостности системы в течение задаваемого периода прогноза;

- нижняя оценка среднего остаточного времени на принятие упреждающих мер в недопущение нарушения целостности системы;

- среднее остаточное время до нарушения целостности системы при своевременном принятии упреждающих мер противодействия угрозам.

При использовании понятия допустимого риска по вычисляемым зависимостям могут быть определены те значения исходных данных, при которых в задаваемый период прогноза будут отсутствовать случаи нарушение установленных ограничений с допустимой вероятностью (что будет характеризовать состояние удержания рисков для системы в допустимых пределах).

Для расчета показателей используются базовые модели раздела 2, усовершенствованные возможностями согласно Теоремам 1, 2, 3.

4.2.5 Исходные данные и порядок прогнозирования рисков

Исходными данными для прогнозирования рисков в общем случае выступают:

σ – частота возникновения источников угроз в моделируемой системе;

β – среднее время развития угроз с момента возникновения источников угроз до нарушения установленных требований по обеспечению целостности моделируемой системы или до инцидента;

$T_{меж}$ – время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы (постоянная величина, задаваемая для системы);

$T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы (подразумевается, что в нем учитывается среднее время восстановления нарушенной целостности системы);

$T_{восст}$ – среднее время восстановления нарушенной целостности системы;

$T_{зад}$ – задаваемая длительность периода прогноза.

Для прогнозирования рисков необходимо наличие возможностей по применению (в т.ч. удаленному) созданного прототипа технологии поддержки риск-ориентированной системной инженерии или его отдельных компонентов, позволяющих проведение расчетов для достижения поставленных целей.

Порядок прогнозирования рисков с использованием ВС и КС в полной мере предопределен возможностями программно-технологических решений (см. разделы 2, 3).

Примечание. Согласно усовершенствованной концепции (см. рис. 3.1 и 4.1) для анализа могут быть использованы другие приемлемые вероятностные модели и соответствующие им исходные данные – см., например, модели из ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы».

4.2.6 Обработка, анализ и использование результатов прогнозирования. Отчетность

В общем случае расчеты, обработка и анализ получаемых результатов прогнозирования проводятся с применением разработанных программных инструментариев (см. разделы 2, 3) на основе значений исходных данных, которые могут вводиться аналитиком вручную или автоматически в рамках систем контроля состояния элементов системы (например – с помощью систем дистанционного контроля – см. ГОСТ Р 58494-2019 «Оборудование горно-шахтное. Многофункциональные системы

безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов», созданного с авторским участием). Результаты расчетов представляются в виде гистограмм, графиков и/или таблиц (последнее – при необходимости). Результаты расчетов предназначены к использованию для обеспечения упреждающего управления рисками. Приводимые ниже примеры могут рассматриваться как варианты решения практических задач, а также как интеллектуальный вклад в формируемую базу знаний.

По результатам проведения оценки составляется протокол или отчет, осуществляется пополнение сформированного прототипа базы знаний для последующего моделирования (см. подраздел 3.4).

4.2.7 Пример [64, 131, 139]

Рассмотрим моделируемую систему водоотлива на угольной шахте, контролирующую расход воды, подаваемой в вакуум-насос (см. видеоданные на рис. 2.18 – 2.19 из раздела 2), в варианте применения УВМП. С использованием модели из 2.2.2 проведем сравнение ручного контроля расхода воды, подаваемой в вакуум-насос (вариант 1), с автоматическим контролем и восстановлением водного баланса с использованием СДК (вариант 2).

Ручной контроль расхода воды (вариант 1) характеризуется следующими исходными данными:

– частота возникновения источников угроз в моделируемой системе $\sigma = 6$ раз в месяц;

– среднее время развития угроз $\beta = 4$ часа;

– время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы $T_{меж} = 30$ минут;

– среднее время системной диагностики целостности моделируемой системы (подразумевается, что в нем учитывается среднее время восстановления нарушенной целостности системы) $T_{диаг} = 10$ минут;

– задаваемая длительность периода прогноза $T_{зад} = 1$ месяц.

Для сравнения автоматический контроль и восстановление водного баланса с использованием СДК (вариант 2) характеризуется следующими исходными данными:

– частота возникновения источников угроз в моделируемой системе $\sigma = 6$ раз в месяц (т.е. без изменений в сравнении с ручным контролем расхода воды);

– среднее время развития угроз $\beta = 4$ часа (т.е. без изменений);

– время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы $T_{меж}$ = 3 минуты (полагается, что с использованием СДК съем данных осуществляется каждые 3 минуты);

– среднее время системной диагностики целостности моделируемой системы (подразумевается, что в нем учитывается среднее время восстановления нарушенной целостности системы) $T_{диаг}$ = 2 минуты, подразумевая, что не только ускоряется само время диагностики, но и уменьшается среднее время восстановления нарушенной целостности системы за счет внедрения автоматического способа восстановления водного баланса, возвращая моделируемую систему из «желтого» состояния в «зеленое» в режиме реального времени функционирования СДК, т.е. не дожидаясь «недоливов-переливов»;

– задаваемая длительность периода прогноза $T_{зад}$=1 месяц (т.е. то же, что в варианте 1).

На рис. 4.2 представлены сравниваемые уровни рисков, а на рис. 4.3 – 4.10 - зависимости рисков от изменения исходных данных – слева результаты для ручного контроля расхода воды (без СДК) – вариант 1, справа с использованием СДК - вариант 2.

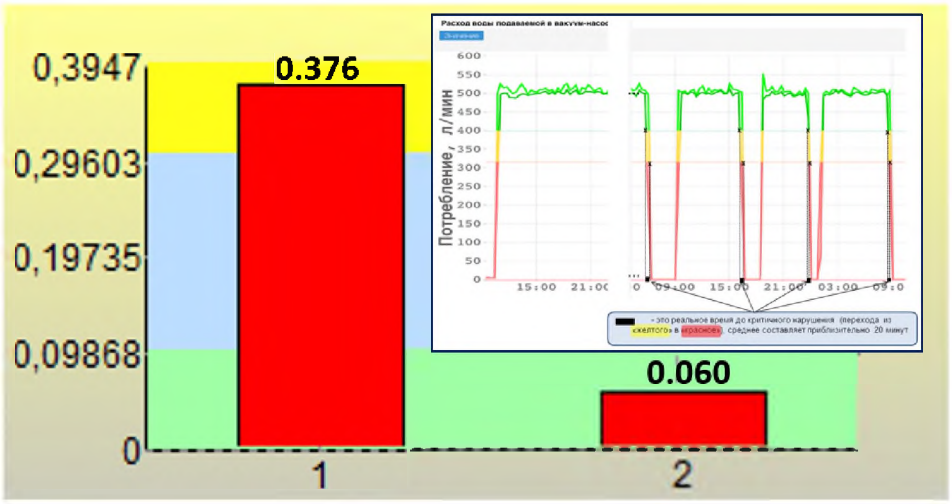


Рис. 4.2 Риски нарушения целостности для ручного контроля (слева) и с использованием СДК (справа)

Анализ результатов расчетов на рис. 4.2 показал снижение в 6.27 раз риска нарушения целостности для 2-го варианта использования СДК в сравнении с 1-м вариантом ручного контроля расхода воды (без СДК). Зависимость риска от частоты возникновения источников угроз σ для варианта 1 возрастает с уровня 0.21 до 0.61, для варианта 2 – с уровня 0.03 до 0.12 – см. рис. 4.3, 4.4. Т.е. при частоте возникновения источников угроз 3 раза в месяц риск с использованием СДК (для 2-го варианта) ниже в 7 раз, а при частоте возникновения источников угроз 12 раз в месяц риск с использованием СДК (для 2-го варианта) ниже в 5.26 раза. Иными словами, частота возникновения источников угроз σ - это критичный параметр для риска нарушения целостности системы водоотлива. За счет

использования СДК при изменении частоты возникновения источников угроз σ в диапазоне -50%+100% риск устойчиво ниже в среднем в 6.13 раз (6.13 раз = (7 раз + 5.26раз)/2).

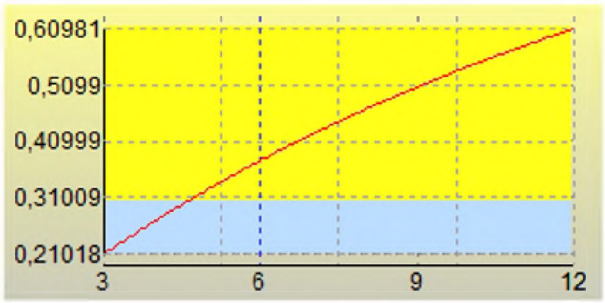


Рис. 4.3 Зависимость риска от частоты возникновения источников угроз σ (раз в месяц) для варианта 1

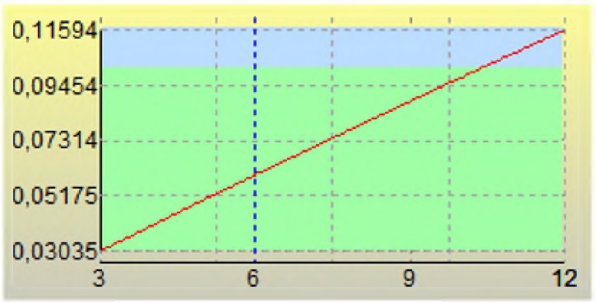


Рис. 4.4 Зависимость риска от частоты возникновения источников угроз σ (раз в месяц) для варианта 2

Зависимость риска от среднего времени развития угроз β для варианта 1 снижается с уровня 0.59 до 0.22, для варианта 2 – с уровня 0.12 до 0.03 – см. рис. 4.5, 4.6, т.е. при среднем времени развития угроз, равном двум часам, риск с использованием СДК (для 2-го варианта) ниже в 5.13 раз, а при среднем времени развития угроз, равном 8 часам, риск с использованием СДК (для 2-го варианта) ниже в 7.06 раз. Иными словами, среднее время развития угроз β - это критичный параметр для риска нарушения целостности системы водоотлива, причем при изменении в диапазоне -50%+100% риск устойчиво ниже по сравнению с вариантом 1 приблизительно в той же степени критичности, как и для частоты возникновения источников угроз σ.

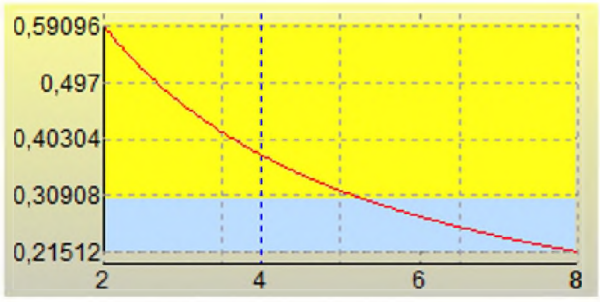


Рис. 4.5 Зависимость риска от времени развития угроз β (в часах) для варианта 1

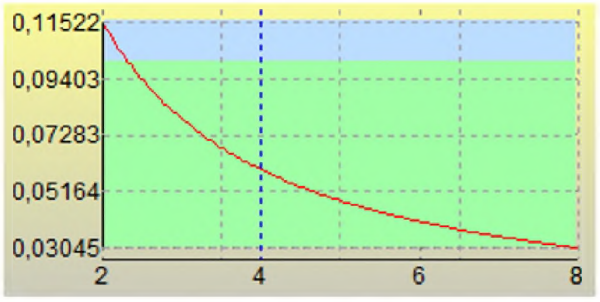


Рис. 4.6 Зависимость риска от времени развития угроз β (в часах) для варианта 2

Зависимость риска от времени между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы $T_{меж}$ для варианта 1 повышается с уровня 0.26 до 0.55, для варианта 2 – с уровня 0.04 до 0.09 – см. рис. 4.7, 4.8, т.е. при времени между диагностиками полторы минуты риск с использованием СДК (для 2-го варианта) ниже в 6.17 раз в сравнении с ручным вариантом 1 ($T_{меж}$ = 15 минут), а при времени между диагностиками, равном 6 минутам, риск с использованием СДК (для 2-го варианта) ниже в 7.06 раз в сравнении с ручным вариантом 1 ($T_{меж}$ = 60 минут). Иными словами, время между окончанием предыдущей и началом очередной диагностики целостности моделируемой

системы $T_{меж}$ - это существенно более критичный параметр для риска нарушения целостности системы водоотлива в сравнении с частотой возникновения источников угроз σ и средним временем развития угроз β. Причем при изменении $T_{меж}$ в диапазоне -50%+100% риск для варианта 2 устойчиво ниже по сравнению с вариантом 1 приблизительно в среднем в 6.62 раза (6.62 раза ~ (6.17 раз+ 7.06 раз)/2).

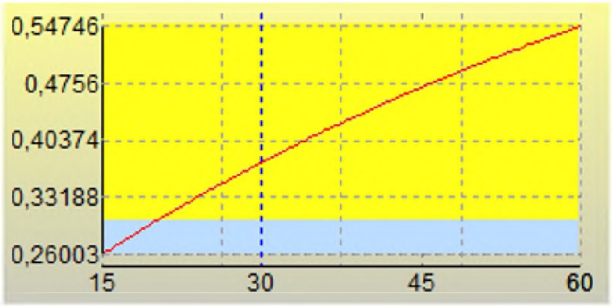


Рис. 4.7 Зависимость риска от времени между диагностиками $T_{меж}$ (в минутах) для варианта 1

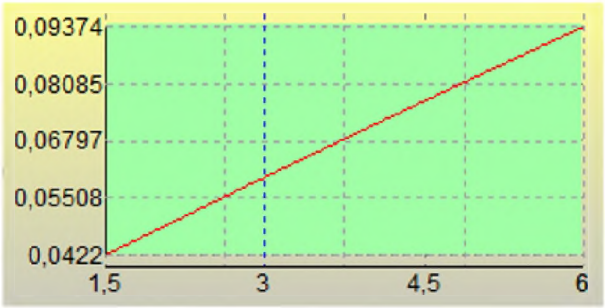


Рис. 4.8 Зависимость риска от времени между диагностиками $T_{меж}$ (в минутах) для варианта 2

Зависимость риска от средней длительности диагностики $T_{диаг}$ для варианта 1 возрастает с уровня 0.34 до 0.44, для варианта 2 – с уровня 0.05 до 0.08 – см. рис. 4.9, 4.10, т.е. при средней длительности диагностики, равной 1 минуте, риск с использованием СДК (для 2-го варианта) ниже в 7.07 раз в сравнении с ручным вариантом 1 ($T_{диаг}$ = 5 минут), а при средней длительности диагностики 4 минуты риск с использованием СДК (для 2-го варианта) ниже в 5.34 раза в сравнении с ручным вариантом 1 ($T_{диаг}$ = 20 минут). Иными словами, средняя длительность диагностики $T_{диаг}$ - это менее критичный параметр для риска нарушения целостности системы водоотлива. За счет использования СДК при изменении средней длительности диагностики $T_{диаг}$ в диапазоне -50%+100% риск для варианта 2 устойчиво ниже по сравнению с вариантом 1 приблизительно в среднем в 6.21 раза (6.21 раза ~ (7.07 раз + 5.34 раза)/2). Т.е. риск для варианта 2 устойчиво ниже по сравнению с вариантом 1 приблизительно в той же степени критичности, как и для частоты возникновения источников угроз σ и среднего времени развития угроз β.

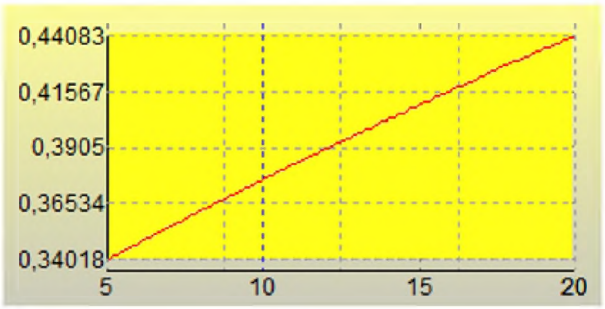


Рис. 4.9 Зависимость риска от длительности диагностики $T_{диаг}$ (в минутах) для варианта 1

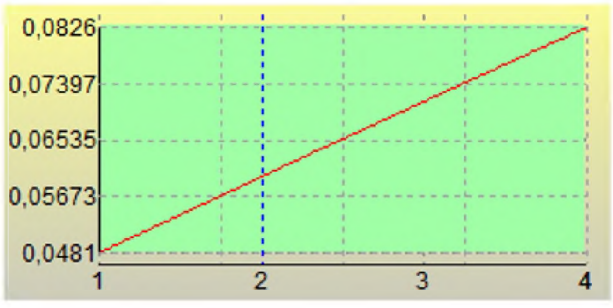


Рис. 4.10 Зависимость риска от длительности диагностики $T_{диаг}$ (в минутах) для варианта 2

Зависимость риска от длительности периода прогноза $T_{зад}$ для варианта 1 возрастает с уровня 0.21 до 0.61, для варианта 2 – с уровня 0.03 до 0.16 – см. рис. 4.11, 4.12, т.е. при длительности периода прогноза, равном 0.5 месяца, риск с использованием СДК (для 2-го варианта) ниже в 6.91 раза, а при длительности периода прогноза 2 месяца риск с использованием СДК (для 2-го варианта) ниже в 5.27 раз. За счет использования СДК при изменении длительности периода прогноза $T_{диаг}$ в диапазоне -50%+100% риск для варианта 2 устойчиво ниже по сравнению с вариантом 1 приблизительно в среднем в 6.09 раза (6.09 раза = (6.91 раза + 5.27 раза)/2). Вместе с тем необходимо помнить, что на практике период прогноза для расчетных показателей подбирают таким образом, чтобы вероятностные значения рисков не превышали допустимые. В этом случае для задаваемых при моделировании условий имеет место гарантия того, что за этот период возможно принятие упреждающих мер для удержания рисков в допустимых пределах.

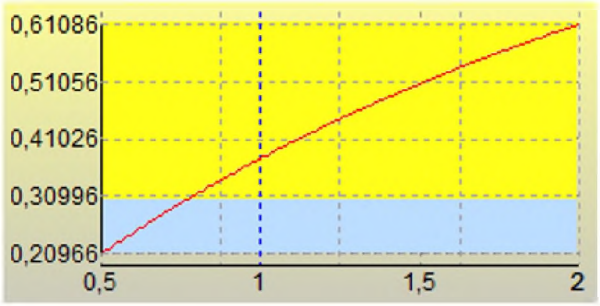


Рис. 4.11 Зависимость риска от длительности периода прогноза $T_{зад}$ (в месяцах) для варианта 1

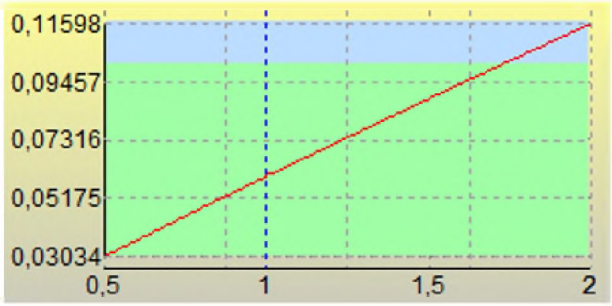


Рис. 4.12 Зависимость риска от длительности периода прогноза $T_{зад}$ (в месяцах) для варианта 2

Таким образом, работоспособность предложенной методики прогнозирования рисков нарушения целостности моделируемой системы, представимой в виде «черного ящика», продемонстрирована на примере сравнения двух вариантов функционирования моделируемой системы водоотлива на угольной шахте – для ручного контроля расхода воды, подаваемой в вакуум-насос (вариант 1), в сравнении с автоматическим контролем и восстановлением водного баланса с использованием СДК (вариант 2).

Важно отметить, что критичными при проведении расчетов являются устанавливаемые границы рабочего диапазона (см. УВМП – рис. 2.13, 2.17), влияющие на выходы и возвращения моделируемой системы из «желтого» состояния в «зеленое». Т.е. решение задачи определения границ рабочего диапазона критичных параметров, в первую очередь параметров контролируемого оборудования, является практически важным для получения более адекватных результатов моделирования.

4.3 Адаптация методики для определения границ рабочего диапазона критичных параметров контролируемого оборудования

Проводя адаптацию предложенной методики, решение задачи определения границ рабочего диапазона критичных параметров продемонстрируем на практическом примере поиска границы рабочего диапазона для параметра «Расход воздуха» в канале шахты на вентиляторной установке типа ВУПД-2, 4 путем ориентации на приемлемое время реакции на отклонения в расходе воздуха за заданное время [64, 131, 139].

Условие задачи – следующее. Для каждого параметра есть границы нормативного диапазона, вне этих границ «красная» зона состояний характеризуется в терминах элементарных состояний УВМП как «Неприемлемое». Вся зона внутри границ нормативного диапазона – это формально рабочий диапазон – «зеленая» зона, характеризующая состояния в ней как «Приемлемое» – см. видеоданные на рис. 2.18, 2.19 и рис. 4.13, где верхняя граница нормативного диапазона составляет 7620 условных единиц, а нижняя – 2580 у.е. Эти границы – не меняются, если они задаются производителем оборудования в функциональных требованиях к условиям эксплуатации или в гарантийных ограничениях. Но на практике они также могут быть установлены по результатам эмпирических исследований. Чтобы избежать внезапных отказов при переходе из «зеленой» зоны в «красную», внутри рабочего диапазона требуется выделить условную границу «желтой» зоны, которая будет характеризовать предпосылку нарушения нормативного диапазона (в терминах элементарных событий УВМП это будет зона состояния «Приемлемое с отклонением»).

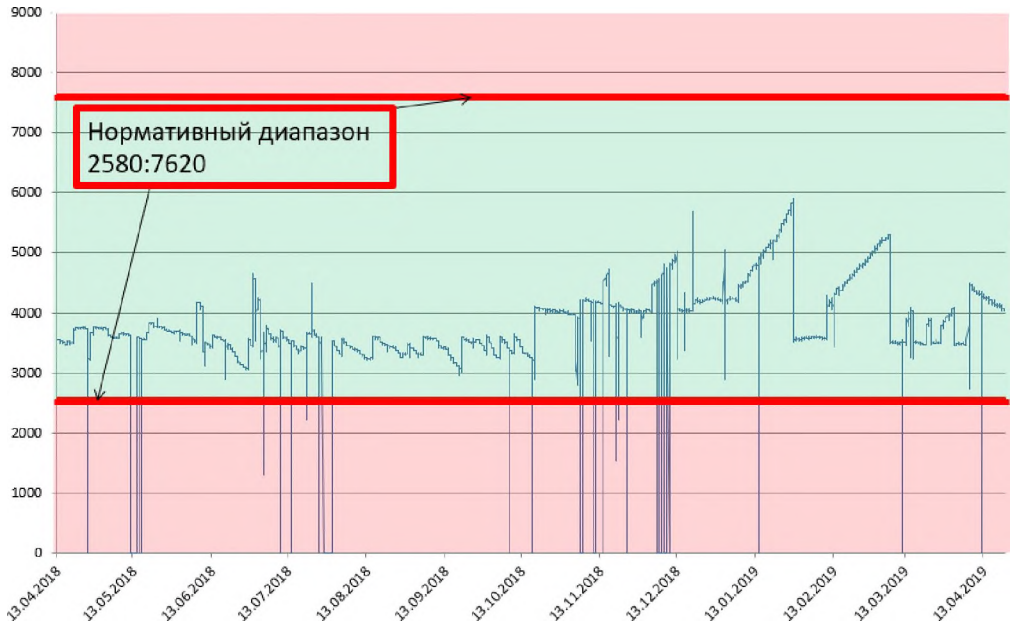


Рис. 4.13 «Расход воздуха» - общая картина по вентиляторной установке ВУПД-2,4 за год с указанием только состояний «Приемлемое» («зеленая» зона) и «Неприемлемое» («красная»)

Решение задачи базируется на реализации идеи ориентации на приемлемое время реакции мастера на отклонение за заданное время $T_{зад}$. Для приближения к реалиям угольной шахты период прогноза $T_{зад}$ рассматривается в подразделе равным 30 минутам. Для инженерного решения задачи предлагается выполнять 4 методических шага.

Шаг 1. Сначала формируются исходные данные для моделирования по значениям параметра «Расход воздуха» в течение заданного периода времени (например, за год).

Фиксируются нарушения нормативного диапазона за выбранный период времени (прошедший год) – см. рис. 4.13. Здесь для простоты понимания возможны 2 варианта:

- Вариант 1.1 Если были нарушения нормативного диапазона, определяется среднее значение параметра внутри рабочего диапазона в течение заданного периода времени, после чего определяется минимальное время, за которое значение параметра отклонилось от среднего значения до границы нормативного диапазона. Для упрощения назовем быстрым переход до границы нормативного диапазона, если он длился менее или около 1 часа, а если более 1 часа (например, 2 и более часов) – медленным;

- Вариант 1.2 Пересечений нормативного диапазона за заданный период времени не было. В этом случае переход границы нормативного диапазона по умолчанию определим как медленный.

Шаг 2. Устанавливается следующий критерий определения искомых границ рабочего диапазона внутри нормативного диапазона. Для общего случая двух границ нормативного диапазона – верхней и нижней – согласно критерию выбирается такая искомая условная граница предпосылки к инциденту, при которой частота пересечения этой условной границы за год в направлении границ нормативного диапазона будет таковой, что вероятность нарушения границ нормативного диапазона будет не ниже доверительного уровня 0.99.

Примечание. С инженерной точки зрения критерий может быть проинтерпретирован так: если мастер реагирует корректно на отклонения за 30 минут, то условно в 99 случаях из 100 возможно предотвращение нарушения границ нормативного диапазона.

Шаг 3. Для расчетов применяется предложенная базовая модель из подраздела 2.2. Определяется такая максимально допустимая частота нарушений границ рабочего диапазона (за год), для которой расчетная вероятность нарушения границ нормативного диапазона будет не ниже доверительного уровня 0.99.

Для общего случая исходные данные для такого расчета искомой частоты нарушений границ рабочего диапазона отражены на рис. 4.13. Вариант 1 характеризует быстрое развитие угрозы β, т.е. быстрый переход за границу нормативного диапазона от среднего

значения - за 1 час, а вариант 2 характеризует медленное развитие угрозы, т.е. переход за границу нормативного диапазона за 2 часа. Период между диагностиками $T_{меж}$ =2 минуты, время на реакцию в связи с отклонением от нормы $T_{диаг}$ = 30 минут. Период прогноза, для которого оценивается вероятность нарушения границ нормативного диапазона – 1 сутки. Подлежит определению частота возникновения угроз σ при заданном ограничении на доверительный уровень 0.99 для вероятности нарушения границ нормативного диапазона.

Результаты расчетов по модели показали (см. рис. 4.14): максимальное количество выходов в год за искомую границу внутри рабочего диапазона должен быть в среднем не более 16 раз в год для быстроизменяемых отклонений (1-й вариант) и не более 30 раз в год для медленноизменяемых отклонений. В этом случае как минимум в 99 случаях из 100 при правильной реакции ответственного лица (мастера) на отклонения в течение 30 минут возможно предотвращение нарушения границ нормативного диапазона.

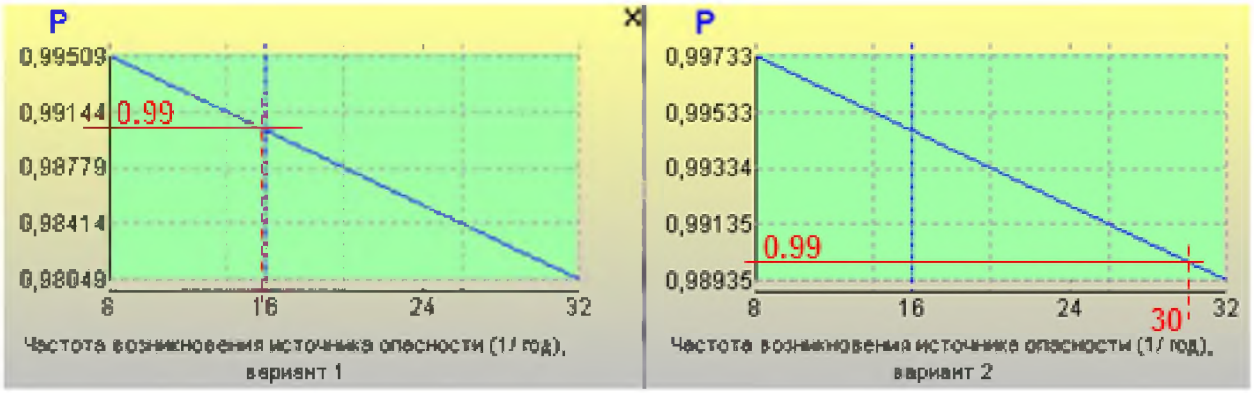


Рис. 4.14 – Определение допустимой частоты нарушений границ рабочего диапазона, для которой возможно предотвращение нарушения границ нормативного диапазона с доверительной вероятностью 0.99

Шаг 4 (инженерный поиск). Имея реальный график значений параметра за год с установленным нормативным диапазоном 2580:7620 у.е. для значений исследуемого параметра (см. рис. 4.13), от условной средней горизонтальной линии ее (эту линию) начинают передвигать вверх (для определения верхней границы) и вниз (для определения нижней границы), т.е. передвигаются две горизонтальные прямые – вверх и вниз. Эти горизонтальные прямые играют роль условных границ рабочего диапазона – верхней и нижней. Каждая условная граница в своем поиске рационального уровня перемещается вертикально до тех пор, пока количество отклонений (начиная с пересечения условной границы) в сторону границы нормативного диапазона не достигнет минимального уровня 16 раз в год и не превысит 30 раз в год.

Если при этом для конкретной границы (нижней или верхней) все отклонения быстроизменяемые (около 1 часа и менее), то ориентируются на количество отклонений, выходящих за пределы рабочего диапазона 16 отклонений в год. Если все отклонения

медленноизменяемые (2 часа и более), то ориентируются на количество отклонений, выходящих за пределы рабочего диапазона 30 отклонений в год. Если отклонения смешанные (как быстроизменяемые, так и медленноизменяемые), то ориентируются на количество отклонений, выходящих за пределы рабочего диапазона от 16 до 30 отклонений с учетом пропорции. Если количество отклонений меньше 16, то условная граница проводится как можно дальше от соответствующей границы нормативного диапазона, фиксируя за пределами рабочего диапазона количество отклонений, максимально близкое к 16. Если количество отклонений за нормативные границы равно 0, то делается предположение о хотя бы одном гипотетичном медленноизменяемом отклонении с повторением шагов 1-4.

Имея график значений параметра за год (см. рис. 4.13), с помощью способа, описанного выше в шаге 4, ищутся условные границы количества отклонений вне рабочей зоны (сверху – над передвигаемой вверх горизонтальной линии), пока количество отклонений за пределами этой границы не достигнет уровня около 16 раз в год – см. рис. 4.15 (отклонения сверху с возвратами в рабочую зону пронумерованы на рисунке красным цветом с соответствующими стрелочками и нумерацией от 1 до 20). Для верхней границы при поиске выясняется, что характер отклонений может быть определен как смесь отклонений быстроизменяемых с медленноизменяемыми.

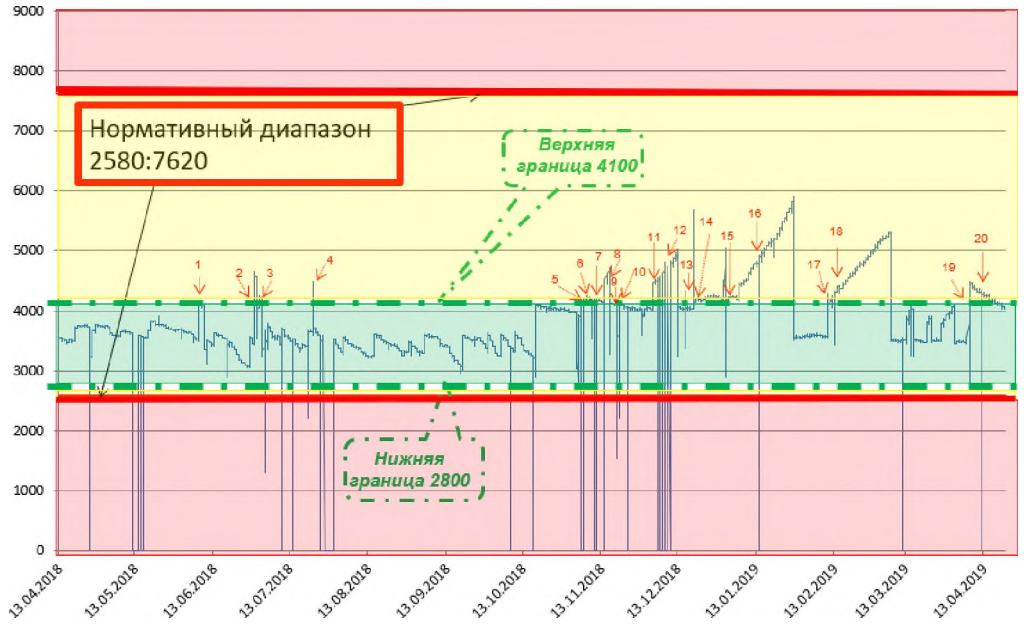


Рис. 4.15 Расчетные границы зоны «Приемлемое с отклонением» («желтая»), когда нарушения границ нормативного диапазона предотвращаются с доверительной вероятностью 0.99

Результаты поиска границ зоны «Приемлемое с отклонением» («желтая»), когда нарушения границ нормативного диапазона предотвращаются с доверительной вероятностью 0.99 согласно описанным выше шагам 1 – 4 отражены на рис. 4.15.

В итоге при нормативном диапазоне 2580:7620 у.е. для допустимых значений параметра «Расход воздуха» установлены нижняя и верхняя граница рабочей зоны (состояние «Приемлемое», «зеленая» зона) – это 2800:4100 у.е.. Диапазоны 2580:2800 у.е. и 4100:7620 у.е. превращаются в зону состояний «Приемлемое с отклонением», что (с учетом возможностей мастера корректно реагировать за 30 минут) при сложившихся условиях обеспечит ненарушение нормативного диапазона с вероятностью не ниже 0.99.

Выбор более удаленной границы рабочего диапазона от границы нормативного диапазона с максимальным приближением к границам от 16 до 30 отклонений, удовлетворяющий сформулированным критериям в шагах 1-4, обусловлен стремлением с одной стороны успеть отреагировать за приемлемое время принятия решения (30 минут), а с другой – сократить необоснованно частые отвлечения ответственных лиц. Если количество отклонений за конкретную нормативную границу превышают 30, то на практике снижается уровень доверительной вероятности до 0.95 (при этом границы рабочего диапазона по результатам моделирования составят 80 для быстроизменяемых отклонений и 170 для медленноизменяемых отклонений) с повторением шагов 1-4.

Предложенный инженерный подход для определения границ рабочего диапазона критичных параметров контролируемого оборудования по данным мониторинга в полной мере отвечает применению Теоремы 3 о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам (см. раздел 2). Так, в точках расчета по 1-му варианту (σ=16 раз в год) вероятность нарушения границ нормативного диапазона составит 0.9902. а по 2-му варианту 0.9900 (при σ=30 раз в год), т.е. расхождение в четвертом знаке, что соизмеримо с инженерной точностью самих расчетов. Это дополнительно подтверждает адекватность как предложенной во 2-м разделе Теоремы 3, так и предложенного в этом подразделе инженерного подхода.

При дальнейшем изложении различных примеров исходим из обоснованности границ зоны «Приемлемое с отклонением» изложенным выше способом или иным объективно приемлемым способом.

4.4 Типовая методика прогнозирования рисков нарушения целостности сложной моделируемой системы

4.4.1 Исследуемая система и ее логическая структура

В качестве исследуемой может выступать одна из следующих моделируемых систем:

сложная система, включающая в свой состав подсистемы и/или системные элементы и формализуемая согласно положениям 2.4.2;

система систем, которая может быть формализуема согласно положениям 2.4.2.

Так, на опасном производственном объекте (ОПО) в угольной отрасли, рассматриваемом как сложная система, в качестве подсистем могут выступать, например, комплексы главных вентиляторных установок (ГВУ), модульных дегазационных установок (МДУ), газоотсасывающих установок (ГОУ). А в качестве системных элементов в комплексе главных вентиляторных установок могут рассматриваться основной и резервный вентиляторы, общие параметры установки.

В зависимости от целей прогнозирования рисков исследуемая сложная система логически может быть представлена в виде логической структуры с декомпозицией до уровня составных подсистем и системных элементов, характеризуемых их характеристиками и условиями эксплуатации и объединяемых логическими условиями «И» и «ИЛИ». В системах сложной структуры возможны различные комбинации логических условий «И», «ИЛИ».

Примечания. 1. Логическое условие «И» для двух связанных этим условием элементов интерпретируется так: система из двух последовательно соединяемых элементов находится в состоянии целостности, когда «И» первая подсистема, «И» вторая подсистема находятся в состоянии целостности.

2. Логические условие «ИЛИ» для двух связанных этим условием элементов интерпретируется так: система из двух параллельно соединяемых элементов находится в состоянии целостности, когда «ИЛИ» первая подсистема, «ИЛИ» вторая подсистема находятся в состоянии целостности.

В качестве системы систем могут быть рассмотрены, например, совокупность предприятий в нефтяной, газовой, угольной и торфяной отрасли (это – объединяемые системы) в их объединении в топливно-энергетическом комплексе (ТЭК) государства, интегрирующем нефтяную, газовую, угольную и торфяную отрасли, электроэнергетику и теплоснабжение (т.е. некоторые исследуемые фрагменты ТЭК при моделировании могут рассматриваться как интегрированные системы систем – см. пример в 5.1).

4.4.2 Цели прогнозирования рисков

Основной целью прогнозирования рисков является установление степени вероятного нарушения целостности исследуемых системы, составных систем, подсистем и системных элементов за период прогноза в интересах решения аналитических задач:

оценки рисков в течение заданного периода прогноза безотносительно уровней допустимых рисков и в сравнении с установленными допустимыми рисками для различных сценариев возникновения и развития угроз, применяемых мер системного контроля состояний и восстановления целостности для исследуемых системы, составных систем, подсистем и системных элементов;

научного обоснования уровня допустимых рисков по «прецедентному принципу» для исследуемых системы, составных систем, подсистем и системных элементов;

научного обоснования критичных условий возникновения различных угроз для исследуемых системы, составных систем, подсистем и системных элементов;

сравнительного анализа различных вариантов поведения применительно к исследуемым системе, составным системам, подсистемам и системным элементам для возможных сценариев развития угроз и мер противодействия угрозам;

научного обоснования упреждающих мер по снижению или удержанию в допустимых пределах рисков и/или снижению затрат и/или возможных ущербов в практике создания, эксплуатации, технического обслуживания, модернизации и развития при задаваемых ограничениях для исследуемых системы, составных систем, подсистем и системных элементов;

создания базы знаний и вариантов решения типовых практических задач упреждающего управления рисками для исследуемых системы, составных систем, подсистем и системных элементов.

4.4.3 Общие положения

В качестве общих положений могут быть использованы положения из 2.1, 2.2.1, 2.2.2 с усовершенствованиями и возможностями согласно Теореме 1 (о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности), Теореме 2 (об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта), выявленным закономерностям в соотношениях исходных данных для непревышения задаваемого допустимого уровня риска и сохранения целостности моделируемой системы, Следствию из Теоремы 2 (об ограничениях при

выборе периода между диагностиками целостности системы, ориентированного на непревышение допустимого риска нарушения целостности системы), Теореме 3 (о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам), теоретическому обоснованию возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков», Теореме 4 (о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам) из раздела 2, а также реализации их программных и технологических решений из разделов 2, 3.

4.4.4 Оцениваемые показатели и расчетные соотношения

К оцениваемым показателям для исследуемой сложной системы относятся:

1) для сложной системы, объединяющей на верхнем уровне иерархии составные подсистемы с помощью логического соединения «И» (составные подсистемы могут представлять собой самостоятельные параллельно-последовательные структуры, в которых элементы объединяются с использованием логических соединений «И», «ИЛИ»), и для системы систем, в которой составные системы объединяются логическим соединением «И» (составные системы могут представлять собой самостоятельные параллельно-последовательные структуры, в которых элементы объединяются с использованием логических соединений «И», «ИЛИ»):

- риск нарушения целостности сложной системы в течение задаваемого периода прогноза;
- риск нарушения целостности составляющих составных подсистем и систем верхнего уровня в течение задаваемого периода прогноза;
- нижняя оценка среднего остаточного времени на принятие упреждающих мер в недопущение нарушения целостности сложной системы;
- нижние оценки среднего остаточного времени на принятие упреждающих мер в недопущение нарушения целостности составляющих составных подсистем и систем верхнего уровня;
- среднее остаточное время до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам;
- среднее остаточное время до нарушения целостности составляющих составных подсистем и систем верхнего уровня при своевременном принятии в них упреждающих мер противодействия угрозам.

2) для сложной системы объединяющей на верхнем уровне иерархии подсистемы с помощью логического соединения «ИЛИ» (составные подсистемы могут представлять собой самостоятельные параллельно-последовательные структуры, в которых элементы объединяются с использованием логических соединений «И», «ИЛИ»):

- риск нарушения целостности сложной системы в течение задаваемого периода прогноза;

- нижняя оценка среднего остаточного времени на принятие упреждающих мер в недопущение нарушения целостности сложной системы;

- среднее остаточное время до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Примечание. В случае 1) показатели характеризуют систему в целом и на верхнем уровне объединения. В случае 2) показатели характеризуют систему в целом. Для анализа подсистем с учетом их уникальной структуры требуется анализ этих подсистем как самостоятельных исследуемых систем сложной или простой структуры. Тем самым возможен анализ любых параллельно-последовательных структур с логическим объединением «И», «ИЛИ».

При использовании понятия допустимого риска по вычисляемым зависимостям могут быть определены те значения входных данных, при которых в задаваемый период прогноза будет наблюдаться ненарушение установленных ограничений. Это будет характеризовать состояние удержания рисков для сложной системы в допустимых пределах.

4.4.5 Исходные данные для прогнозирования рисков

Задается исходная параллельно-последовательная структура сложной системы, использующая логические соединения «И», «ИЛИ» согласно положениям 2.4.2.

Для сложной системы задается единый период прогноза:

$T_{зад}$ – задаваемая длительность периода прогноза.

Исходными данными для прогнозирования рисков применительно к каждому составному элементу выступают:

σ – частота возникновения источников угроз в моделируемом элементе;

β – среднее время развития угроз с момента возникновения источников угроз до нарушения установленных требований по обеспечению целостности моделируемого элемента или до инцидента;

$T_{меж}$ – время между окончанием предыдущей и началом очередной диагностики целостности моделируемого элемента (постоянная величина, задаваемая для элемента);

$T_{диаг}$ – среднее время системной диагностики целостности моделируемого элемента;

$T_{восст}$ – среднее время восстановления нарушенной целостности элемента.

Примечание. Согласно усовершенствованной концепции (см. рис. 3.1 и 4.1) для анализа могут быть использованы другие приемлемые вероятностные модели и соответствующие им исходные данные – см., например, модели из ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы».

4.4.6 Порядок прогнозирования рисков

Порядок прогнозирования рисков в полной мере предопределен возможностями предложенных программных и технологических решений (см. разделы 2, 3 диссертации) и в общем случае осуществляется по следующим шагам.

Шаг 1 (выполняется аналитиком). Сначала должно быть изучено описание исследуемого объекта с пониманием того, является ли объект с точки зрения построения его модели системным элементом, недекомпозируемой системой или сложной системой. Должны быть изучены схемы и режимы функционирования объекта с выявлением резервирования в целях обеспечения его целостности. Анализируются возможный вид моделируемой системы (простая система, представимая в виде «черного ящика», или сложная система), а также источники и возможности получения исходных данных для моделирования.

Шаг 2 (выполняется аналитиком). Выполняются пункты 4.4.1, 4.4.2 методики. Должно быть сформировано полное логическое «дерево отказов» (нарушений целостности) с характеристикой опасностей, развития угроз и ожидаемых последствий (без указания вероятностей переходов) или логическая параллельно-последовательная структура моделируемой системы (для сложных систем) с декомпозицией до уровня составных подсистем и элементов и характеристикой условий нарушения целостности в логике «И», «ИЛИ». Построение структуры с помощью ПВК эквивалентно формированию полного требуемого логического «дерева отказов» (нарушений целостности). Таким образом на шаге 2 для проведения исследований делается окончательный выбор: подлежит исследованию простая система («черный ящик») или сложная система с пониманием способов формирования исходных данных для моделирования.

Шаг 3 (выполняется аналитиком или автоматически по заранее подготовленным шаблонам, например, для мониторируемого оборудования, состав и структура которого заведомо известны). Определяется приемлемость общих положений для прогнозирования рисков по п. 4.4.3 методики. Для сложной системы формируется само множество элементов верхнего уровня (всего – N, $N \geq 1$ элементов, обеспечивающих функционирование анализируемого объекта. Если $N=1$, это – простая система, если $N>1$, это – сложная система), по которым выполняется прогноз интегрального показателя. Множество

выбранных элементов при N>1 логически объединяется условием «И» и тем самым анализируемый объект как сложная система представляется в виде последовательной цепочки  или при наличии резервирования – условие «ИЛИ» с представлением в виде  . Каждый из элементов верхнего уровня сложной системы сам может быть сложной системой.

Шаг 4. (выполняется аналитиком или автоматизированной системой исследуемой системы согласно установленному регламенту в динамике ее функционирования, например, с использованием УВМП и встроенных технологические возможностей СДК по предоставлению обобщенных и детальных вероятностных прогнозов). Выбираются расчетные показатели по п. 4.4.4 методики.

Шаг 5 (выполняется аналитиком или автоматизированной системой исследуемой системы согласно установленному регламенту в динамике ее функционирования, например, с использованием УВМП и встроенных технологические возможностей СДК, в т.ч. с использованием отдельных программ прототипа технологии поддержки риск-ориентированной системной инженерии). Выполняются пункты 4.4.5 методики. По каждому элементу системы для последующих расчетов определяются значения следующих исходных данных:

перечень опасностей, являющихся источниками угроз целостности, развивающихся во времени до момента реализации какой-либо угрозы, описательные модели угроз и возможные ущербы при нарушении целостности (эти данные используются в качестве комментариев в отчетных материалах);

оперативные исходные данные, в т.ч., возможно, формируемые из данных датчиков с помощью УВМП (позволяющей определить характеристики: σ – частоту возникновения источников угроз в моделируемом элементе; β – среднее время развития угроз с момента возникновения источников угроз до нарушения установленных требований по обеспечению целостности моделируемого элемента или до инцидента; $T_{восст}$ – среднее время восстановления нарушенной целостности элемента);

период между моментами системной диагностики или контроля целостности ($T_{меж}$ – время между окончанием предыдущей и началом очередной диагностики целостности моделируемого элемента, это - постоянная величина, задаваемая для элемента);

средняя длительность системной диагностики или контроля целостности ($T_{диаг}$ – среднее время системной диагностики целостности моделируемого элемента, определяемая с помощью УВМП или путем измерений).

Иллюстрация угроз, мер контроля, мониторинга и восстановления целостности составных подсистем анализируемого объекта– см., например, рис. 4.15.

Шаг 6 (выполняется с использованием прототипа технологии поддержки риск-ориентированной системной инженерии). Выполняется расчет выбранных показателей для задаваемой точки прогноза с использованием разработанных программных и технологических решений, представленных в разделах 2 и 3.

Шаг 7 (выполняется с использованием прототипа технологии поддержки риск-ориентированной системной инженерии). По результатам расчетов формируется аналитический отчет.

4.4.7 Обработка, анализ и использование результатов прогнозирования. Отчетность

В общем случае расчеты, обработка и анализ получаемых результатов прогнозирования проводятся с применением разработанных программных и технологических решений (см. разделы 2, 3) на основе значений исходных данных, которые вводятся аналитиком вручную или автоматизированной системой исследуемой системы согласно установленному регламенту в динамике ее функционирования, например, с использованием УВМП и встроенных технологические возможностей СДК, в т.ч. с использованием отдельных программ прототипа технологии поддержки риск-ориентированной системной инженерии. Результаты расчетов представляются в виде гистограмм, графиков и/или таблиц (последнее – при необходимости). Результаты расчетов предназначены к использованию для обеспечения упреждающего управления рисками. Приводимые ниже примеры могут рассматриваться как варианты решения практических задач.

По результатам прогнозирования рисков составляется протокол или отчет (формируемый окончательно системным аналитиком с учетом автоматически формируемых аналитических отчетов или автоматизированной системой исследуемой системы согласно установленному регламенту в динамике ее функционирования, например, с использованием встроенных технологические возможностей СДК, в т.ч. с использованием отдельных программ прототипа технологии поддержки риск-ориентированной системной инженерии). Осуществляется пополнение сформированного прототипа базы знаний для последующего моделирования (см. подраздел 3.4).

4.4.8 Примеры [5, 64, 131, 139, 167]

В качестве примеров, призванных продемонстрировать работоспособность методики, приводятся варианты применения методики применительно к типовой системе дистанционного контроля (СДК) промышленной безопасности (ПБ).

В общем случае прогнозирования рисков нарушения ПБ требуется ввести элементарные состояния каждого из элементов, подсистем и системы в целом (с учетом логических взаимосвязей элементов и подсистем – например, по «дереву отказов»):

«штатное обеспечение ПБ» *(«зеленый»)*, когда утвержденные на ОПО требования обеспечения ПБ выполняются, отсутствуют факты нарушения требований ПБ и инциденты с нарушением ПБ;

«условное обеспечение ПБ» *(«желтый»)*, когда могут иметь место отдельные временные отступления от требований ПБ или предпосылки к нарушению ПБ или инциденты, не переходящие в предаварийное состояние или аварии на опасном производственном объекте (ОПО), при этом штатными методами восстановления целостности производства обеспечивается временное состояние отсутствия критичных нарушений ПБ, но требуется принятие упреждающих или регламентных мер улучшения ПБ до состояния «штатное обеспечение ПБ» *(«зеленый»)*;

«критичное нарушение ПБ» *(«красный»),* когда наступает аварийная ситуация, при этом штатными методами оперативного восстановления целостности производства (методами текущего ремонта) невозможно обеспечить временное состояние работоспособности, требуется принятие неотложных, упреждающих или регламентных мер технического обслуживания и обеспечения ПБ до состояния «штатное обеспечение ПБ» *(«зеленый»)* или «условное обеспечение ПБ» *(«желтый»)*.

В частных случаях критичным для ПБ рассматриваемого объекта могут оказаться утрата работоспособности какой-либо системы, подсистемы, системного элемента или хотя бы однократный выход за пределы нормированных значений для одного или нескольких параметров оборудования. Возможен расчет различных по своей интерпретации рисков. Например, если в общем случае это может быть «риск критичного нарушения ПБ», то в частных случаях исследований надежности - «риск утраты работоспособности», при исследованиях чувствительности параметров функционирования оборудования - «риск отклонения от нормы» в течение заданного периода прогноза.

Тогда для частного случая, когда критичным для ПБ является утрата работоспособности какой-либо системы, подсистемы, системного элемента, для прогнозирования рисков нарушения работоспособности, вводятся элементарные состояния каждого из элементов:

«штатно работоспособен» *(«зеленый»)*, когда обеспечивается работоспособность элемента согласно требуемым условиям эксплуатации;

«условно работоспособен» *(«желтый»)*, когда обеспечивается временная работоспособность элемента, могут иметь место отдельные временные нарушения требований эксплуатации или предпосылки к ним или инциденты, не переходящие в предаварийное состояние или аварии на ОПО, при этом штатными методами оперативного восстановления целостности производства (методами текущего ремонта) обеспечивается временное состояние работоспособности, но требуется принятие упреждающих или регламентных мер технического обслуживания и обеспечения надежности до состояния «штатно работоспособен» *(«зеленый»)*;

«неработоспособен» *(«красный»),* когда наступает отказ (т.е. элемент не работает), способный привести к аварийной ситуации или аварии на ОПО, при этом штатными методами оперативного восстановления целостности производства (методами текущего ремонта) невозможно обеспечить временное состояние работоспособности, требуется принятие неотложных, упреждающих или регламентных мер технического обслуживания и обеспечения надежности до состояния «штатно работоспособен» *(«зеленый»)* или «условно работоспособен» *(«желтый»)*.

А для частного случая, когда критичным для ПБ является хотя бы однократный выход за пределы нормированных значений для одного или нескольких параметров оборудования, может потребоваться введение элементарных состояний каждого из элементов (см. УВМП в разделе 2): «в рабочих пределах» *(«зеленый»)*; «за рабочими пределами, но в пределах нормы» *(«желтый»)*; «за пределами нормы» *(«красный»),* что в общем случае на практике вовсе может не означать «неработоспособен».

В общем случае возможно расширение или переименование самих элементарных событий, главное, чтобы они формировали полное множество.

Использование аппарата прогнозирования рисков по настоящей методике позволяет обосновывать допустимые риски. По существу для каждого объекта или системы или элемента существует свой норматив допустимости (приемлемости). Приоритетным является выбор критерия допустимости риска, основанного на «прецедентном» принципе. А именно: принимаемые упреждающие меры снижения риска или удержания его в допустимых пределах считаются достаточными только тогда, когда за период эксплуатации объекта не произойдет критичных нарушений ПБ, которые могли бы быть предотвращены за счет использования упреждающих мер, определяемых в режиме реального времени или в планово-упреждающем порядке. Определение достигаемых при этом количественных значений частных и интегральных показателей рисков по настоящей методике, носящей

универсальной характер по объектам приложения, даст представление об уровне допустимого риска не только для этих объектов (систем, элементов), выбранных в качестве сравнительного эталона, но и для других объектов (систем, элементов) с аналогичными условиями эксплуатации и подобной значимостью по возможным ущербам.

В качестве мер противодействия угрозам, способным при их применении снизить расчетные риски, могут выступать более частая (по сравнению со временем развития угроз) системная диагностика или контроль с восстановлением нарушаемой целостности, использование действенного непрерывного мониторинга состояний между диагностиками с оперативным исправлением появляющихся отклонений по признакам угроз, сокращение времени диагностики, сокращение времени восстановления целостности после критичных нарушений.

После многократных прогнозов с использованием настоящей методики для реальных случаев инцидентов и аварий «до» и «после» их наступления, задаваясь уровнем допустимого риска, становится возможным научное обоснование упреждающих мер по снижению или удержанию в допустимых пределах рисков и/или снижению затрат и/или возможных ущербов в практике создания, эксплуатации, технического обслуживания, модернизации и развития системы обеспечения ПБ при задаваемых ограничениях. Кроме того, с применением настоящей методики возможно научно обоснованное определение сбалансированных системных мер, предупреждающих аварийные ситуации при ограничениях на ресурсы и допустимые риски, а также оценка и обоснование эффективных кратко-, средне- и долгосрочных планов на предприятиях по обеспечению ПБ. Это оказывается возможным путем решения самостоятельных оптимизационных производственных задач, использующих расчетные показатели прогнозируемых рисков.

Основными оцениваемыми показателями являются:

1) в общем случае:

риск критичного нарушения ПБ рассматриваемого объекта («черного ящика») в течение заданного периода прогноза для трех случаев управления: без принятия каких-либо мер противодействия угрозам, с принятием мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

ожидаемое среднее время безопасного функционирования рассматриваемого объекта («черного ящика») для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

для системы сложной структуры дополнительно по составным компонентам (для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК):

риски нарушения ПБ в течение заданного периода прогноза составных подсистем (логически объединяемых условием «И»);

ожидаемое среднее время безопасного функционирования составных подсистем (логически объединяемых условием «И»);

Примечание. С привязкой к пространству элементарных событий риск критичного нарушения ПБ означает вероятность хотя бы одного перехода за период прогноза из состояний «штатное обеспечение ПБ» (подкрашивается в СДК *«зеленым»*) или «условное обеспечение ПБ» *(*подкрашивается в СДК *«желтым»*), в которых объект находился изначально, в состояние «критичное нарушение ПБ» *(*подкрашивается в СДК *«красным»);*

2) в частном случае, когда критичным для ПБ является утрата работоспособности какой-либо системы, подсистемы, системного элемента:

риск утраты работоспособности в течение заданного периода прогноза для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

ожидаемое среднее время надежного функционирования для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

для системы сложной структуры дополнительно по составным компонентам(для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК:

риски утраты работоспособности в течение заданного периода прогноза составных подсистем (логически объединяемых условием «И»);

ожидаемое среднее время надежного функционирования составных подсистем (логически объединяемых условием «И»);

Примечание. 1. С привязкой к пространству элементарных событий риск утраты работоспособности означает вероятность хотя бы одного перехода за период прогноза из состояний «штатно работоспособен» («зеленый») или «условно работоспособен» («желтый») в состояние «неработоспособен» («красный»).

2. Если условно вырезать пребывание в состоянии «штатно работоспособен» («зеленый»), то ожидаемое среднее время надежного функционирования составных подсистем (находясь в состоянии

«условно работоспособен» («желтый») до перехода в состояние «неработоспособен» («красный»)) есть ничто иное, как ожидаемое время у мастеров до критичного нарушения с момента выхода значений параметров оборудования из рабочего диапазона. Т.е. для мастера это – ожидаемое время на восстановление целостности.

3) в частном случае, когда критичным для ПБ является хотя бы однократный выход за пределы нормированных значений для одного или нескольких параметров оборудования:

риск критичного отклонения от нормы в течение заданного периода прогноза для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

ожидаемое среднее время функционирования в пределах нормы для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

для системы сложной структуры дополнительно по составным компонентам для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК:

– риски критичного отклонения от нормы в течение заданного периода прогноза для составных рассматриваемых параметров (логически объединяемых условием «И»);

- ожидаемое среднее время функционирования оборудования в пределах нормы по составным рассматриваемым параметрам (логически объединяемых условием «И»);

Примечание. С привязкой к пространству элементарных событий риск критичного отклонения от нормы означает вероятность хотя бы одного перехода за период прогноза из состояний «в рабочих пределах» *(«зеленый»)* или «за рабочими пределами, но в пределах нормы» *(«желтый»)* в состояние «за пределами нормы» *(«красный»);*

4) в частном случае, когда критичным для ПБ является хотя бы однократный выход за пределы рабочего диапазона для одного или нескольких параметров оборудования:

риск выхода за рабочие пределы, но в пределах нормы, в течение заданного периода прогноза для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК);

ожидаемое среднее время функционирования в пределах рабочего диапазона (для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия

мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

для системы сложной структуры дополнительно по составным компонентам:

– риски выхода за рабочие пределы, но в пределах нормы, в течение заданного периода прогноза для составных рассматриваемых параметров (логически объединяемых условием «И»);

- ожидаемое среднее время функционирования оборудования в пределах рабочего диапазона по составным рассматриваемым параметрам (логически объединяемых условием «И»).

Примечание. С привязкой к пространству элементарных событий риск выхода за рабочие пределы, но в пределах нормы, означает вероятность хотя бы одного перехода за период прогноза из состояний «в рабочих пределах» *(«зеленый»)* в состояние «за рабочими пределами, но в пределах нормы» *(«желтый»)*.

После идентификации опасностей для каждого элемента, подсистемы и системы в целом определяются логические условия реализации угроз. На рис. 4.16 приведен пример типичного фрагмента дерева отказов, способных привести к аварии на ОПО из-за отказа главной вентиляторной установки (ГВУ) и повышенной концентрации метана.

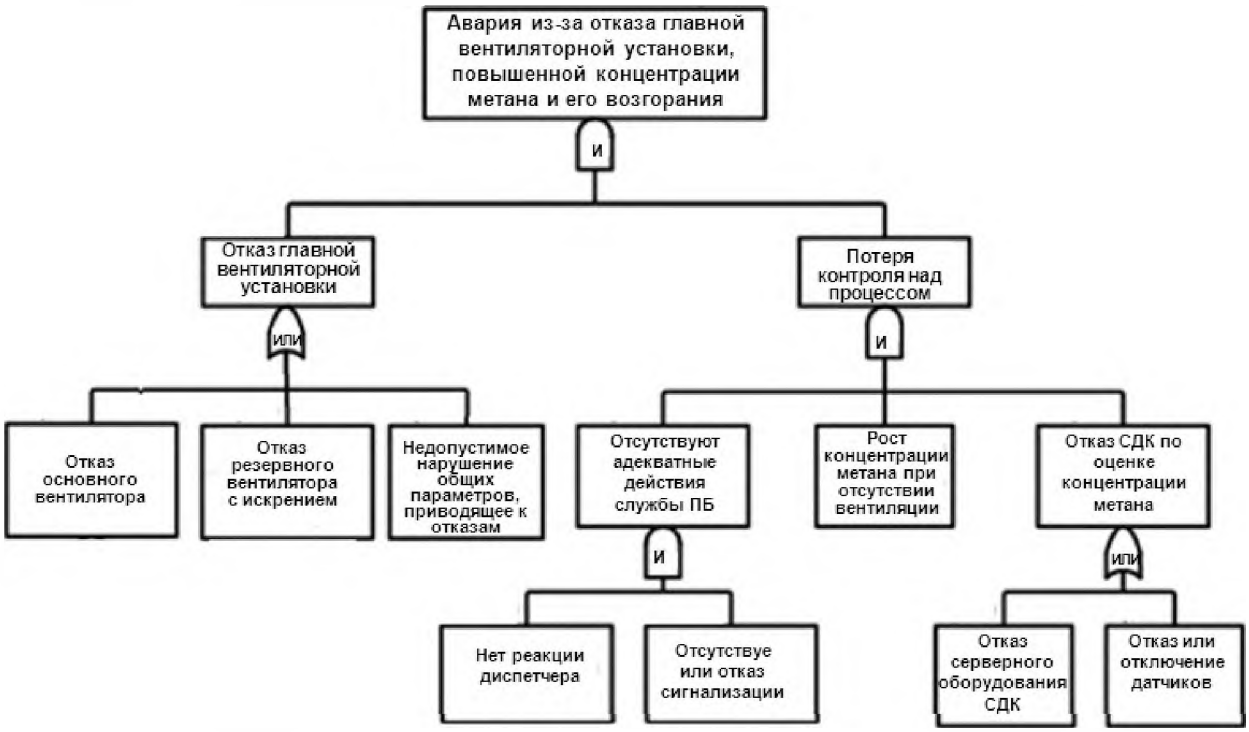


Рис. 4.16 Пример типичного фрагмента дерева отказов для анализа ПБ

Этот фрагмент отражает следующее. Авария возможна, когда наблюдается отказ ГВУ, приводящий к возгоранию метана, при потере контроля над процессом. В этом случае строится структурно-логическая схема для прогнозирования риска «нарушения ПБ» рассматриваемого объекта в логике условий «И», «ИЛИ». Логические рассуждения

следующие: объект перейдет в состояние «нарушения ПБ», когда «И» наступит отказ ГВУ, «И» будет потерян контроль над процессом его функционирования. При этом предполагается, что сохранение контроля над процессом способно предотвратить наступление аварийной ситуации или аварии на ОПО, а методами текущего ремонта, осуществляемого по результатам контроля, возможно временное обеспечение ПБ до устранения выявленных отклонений. В свою очередь, отказ ГВУ (левая подсистема на рис. 4.16) наступает, когда при отказе основного вентилятора «ИЛИ» откажет резервный вентилятор, который в результате отказа окажется способным заискрить, «ИЛИ» произойдет недопустимое нарушение общих параметров - например, недопустимый бросок высокого напряжения, способный вызвать искру.

С другой стороны (правая подсистема), контроль над процессом теряется, когда при росте концентрации метана при отсутствии вентиляции, т.е. используются логические условия:

«И» отсутствуют адекватные действия служб ОПО (главного инженера, главного механика, службы безопасности), что возможно «ИЛИ» из-за отсутствия реакции диспетчера по какой-либо причине (например, из-за сердечного приступа, низкой квалификации и др.), «ИЛИ» из-за отказа сигнализации или ее отсутствия;

«И» наблюдается отказ СДК по оценке концентрации метана, что возможно «ИЛИ» из-за отказа серверного оборудования, «ИЛИ» из-за отказа или отключения датчиков.

Пример 4.4.8.1 Исследуемая система - главная вентиляторная установка.

Задача 1-4.4.8.1. Рассматривается фрагмент «дерева отказов», способных привести к аварии на ОПО из-за отказа главной вентиляторной установки и повышенной концентрации метана. В качестве анализируемого объекта для прогнозирования рисков нарушения ПБ с использованием СКД выступает главная вентиляторная установка (ГВУ) с осевым двухступенчатым вентилятором (ГВУ ВОКД 3,6) – см. рис. 4.17.

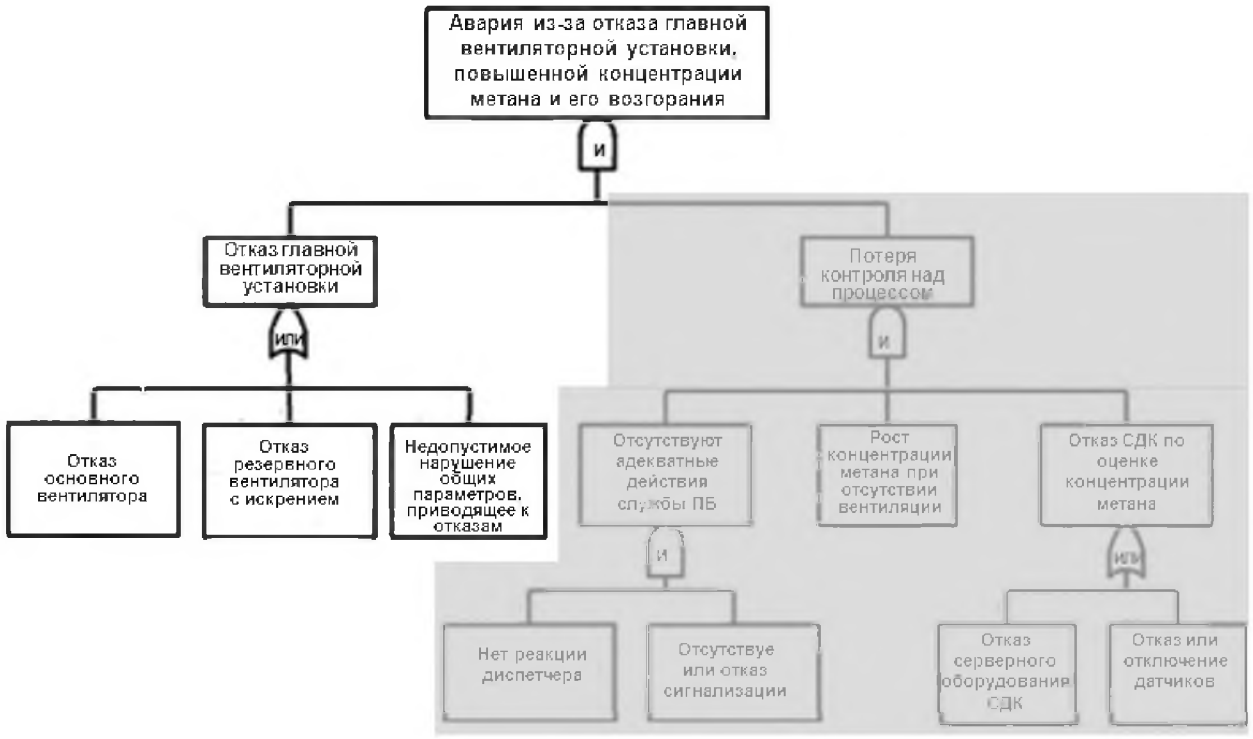


Рис. 4.17 Фрагмент дерева отказов, способных привести к аварии на ОПО из-за отказа главной вентиляторной установки (ГВУ)

При анализе статистики функционирования СДК учитываются различные элементарные состояния системы вплоть до реального или предположительного «нарушения ПБ» *(«красный»)*. Пример подобного состояния ГВУ ВОКД 3,6, учитываемого для определения частоты возникновения угроз по исследуемому объекту, отражен на рис. 4.18.

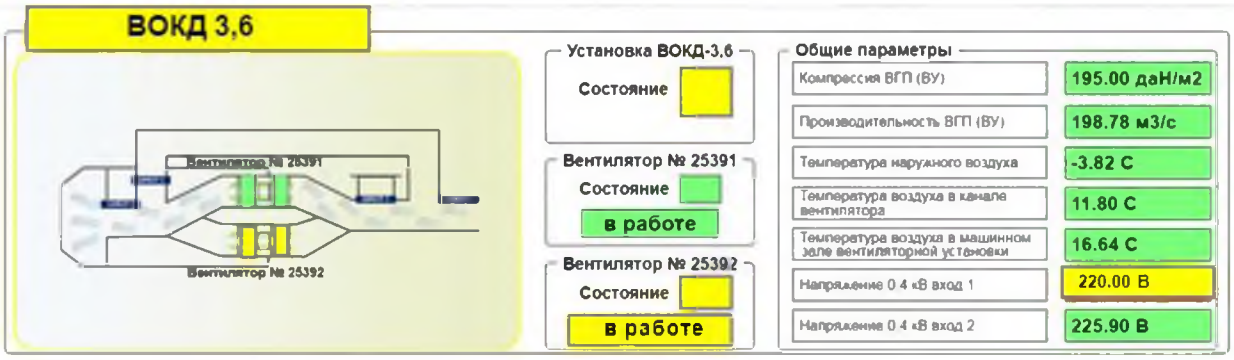


Рис. 4.18 Пример состояния ВОКД 3,6

Требуется осуществить прогноз рисков нарушения ПБ на 1 сутки и на 1 год для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК.

Решение задачи 1-4.4.8.1. Формализация для прогнозирования рисков отражена на рис. 4.19. Представленная формализация интерпретируется так: анализируемый объект (ВОКД 3,6) перейдет из состояния «условное обеспечение ПБ» *(«желтый»)* в состояние «критичное нарушение ПБ» *(«красный»)*, если «ИЛИ» 1-я подсистема, «ИЛИ» 2-я подсистема перейдет в состояние «критичное нарушение ПБ» *(«красный»)*. В свою очередь, с учетом резервирования вентиляторов 2-я подсистема перейдет в состояние «критичное нарушение ПБ» *(«красный»)*, когда «И» элемент 2.1, «И» элемент 2.2 окажутся в состоянии «критичное нарушение ПБ» *(«красный»)*.

Рис. 4.19 Формализация ВОКД 3,6 в виде сложной структуры для решения задачи 1-4.4.8.1

Для каждого из элементов формализации определяются необходимые исходные данные для прогнозирования рисков (см. п. 4.4.5 методики).

Перечень опасностей, перерастающих в угрозы, описательные модели угроз и возможные ущербы при нарушении ПБ связаны с опасностью аварии из-за возгорания метана согласно дереву отказов на рис. 4.16, 4.17. Ущерб эквивалентен крупному пожару на шахте.

Частота возникновения угроз и среднее время развития угроз определяются на базе статистики функционирования СДК, журналов инцидентов и критичных нарушений ПБ. Для прогнозирования определялась суммарная средняя длительность пребывания в состояниях «штатное обеспечение ПБ» *(«зеленый»)* и «условное обеспечение ПБ» *(«желтый»)* вплоть до перехода в состояние «критичное нарушение ПБ» *(«красный»)*. В эту суммарную длительность не включался тот последний отрезок из времени пребывания в состоянии «условное обеспечение ПБ» *(«желтый»)*, который, прошел с последнего инцидента. Среднее по этим отрезкам характеризует среднее время развития угроз с момента их возникновения до достижения критического уровня. Обратное значение полученной суммарной длительности пребывания в состояниях «штатное обеспечение ПБ» *(«зеленый»)* и «условное обеспечение ПБ» *(«желтый»)* (за исключением последнего упомянутого отрезка) представляет собой частоту возникновения угроз.

Положим, вычисленная по статистике функционирования СДК частота возникновения угроз для каждого из элементов составила 1 раз в месяц, среднее время развития угроз – 30 минут, что соизмеримо со временем эвакуации работников из шахты при возникновении пожарной угрозы. Период между моментами системной диагностики или контроля целостности (с восстановлением целостности при выявлении критичных нарушений) положен равным 1 суткам – это период между рабочими сменами. С использованием СДК средняя длительность системной диагностики составляет около 10 секунд (сюда включено время анализа результатов обработки каждого съема данных, поступающих от датчиков). Средняя наработка на ошибку средств мониторинга положен равным 1 году – наработка на отказ используемых датчиков. Среднее время восстановления целостности при нарушениях – 2 часа, что эквивалентно среднему времени текущего ремонта.

Результаты прогнозирования рисков на 1 год показали следующее.

Если не использовать механизмы управления, не предпринимать каких-либо мер противодействия угрозам (т.е. ничего не делать), то аварии неизбежны, риск близок к 1 (рис. 4.20), среднее время до нарушения ПБ при этом составит 488 часов, т.е. всего 20 суток (рис. 4.21).

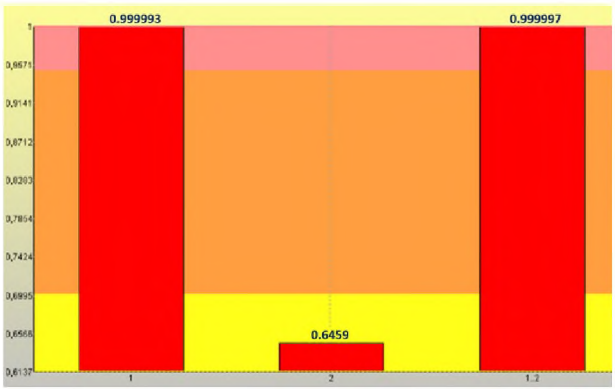


Рис. 4.20 Риск критичного нарушения ПБ за год при полном бездействии (1- за 1-ю подсистему, 2- за 2-ю подсистему, 1…2 – за систему в целом)

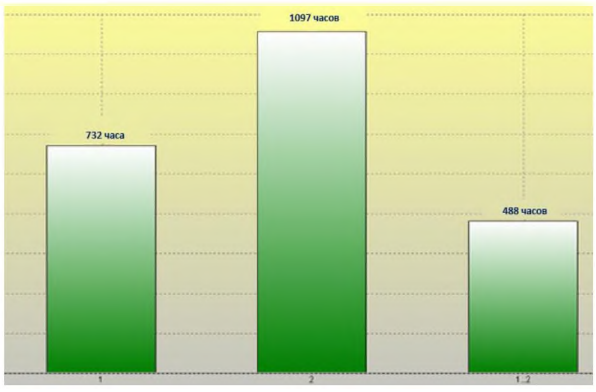


Рис. 4.21 Среднее время до нарушения ПБ при полном бездействии

Если принимать меры в рамках обычной системы контроля (без использования возможностей СДК) с периодическим системным контролем 1 раз в смену (1 раз в сутки) без осуществления непрерывного мониторинга, то аварии по-прежнему неизбежны, риск за год близок к 1, среднее время до нарушения ПБ при этом составит 498 часов, т.е. лишь на 10 часов больше, чем при полном бездействии.

Если идеально использовать механизмы управления, т.е. мгновенно предпринимать оперативные меры сразу же по выявлении определенных предпосылок, не допускать

ошибок в течение года, устранять все выявленные нарушения при каждой смене, то риск критичного нарушения ПБ снижается до уровня 0.015 (см. рис. 4.22), среднее время до нарушения ПБ при этом составит около 40 лет – это в идеале (см. рис. 4.23).

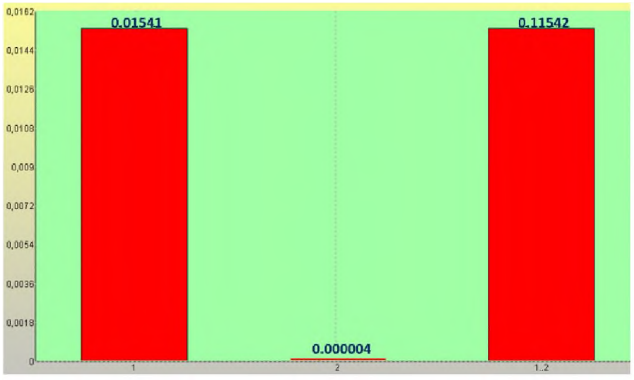


Рис. 4.22 Риск критичного нарушения ПБ за год при идеальном управлении (1- за 1-ю подсистему, 2- за 2-ю подсистему, 1…2 – за систему в целом)

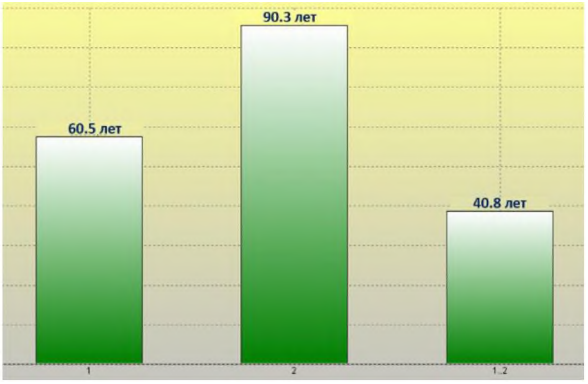


Рис. 4.23 Среднее время до нарушения ПБ при идеальном управлении (в годах)

При прогнозе на сутки получены следующие результаты.

Если не использовать механизмы управления, не предпринимать каких-либо мер противодействия угрозам (т.е. ничего не делать), риск критичного нарушения ПБ составит 0.032, среднее время до нарушения ПБ сохраняется - около 20 суток. Интерпретация такова: вероятность критичных нарушений ПБ окажется в 30 раз меньше, чем вероятность его отсутствия. Если принимать меры в рамках СК (без использования возможностей СДК) с периодическим системным контролем 1 раз в смену (1 раз в сутки) без осуществления непрерывного мониторинга, то риск критичного нарушения ПБ за сутки составит те же 0.032, как и при полном бездействии. Дело в том, что за сутки периодический эффект за смену (1 раз в сутки) – неощутим.

Если в течение суток идеально использовать механизмы управления, т.е. мгновенно предпринимать оперативные меры сразу же по выявлении предпосылок, не допускать ошибок, устранять все выявленные нарушения при каждой очередной смене, то риск критичного нарушения ПБ снижается до уровня 0.00004. Это – в 375 раз меньше, чем при полном бездействии и в рамках обычной системы контроля (без использования возможностей СДК). Интерпретация риска 0.00004 такова: вероятность хотя бы одного нарушения ПБ в 25000 раз ниже, нежели вероятность его отсутствия. Это – в 800 раз эффективнее, чем для обычной системы контроля без использования возможностей СДК.

Вывод по задаче 1-4.4.8.1. Для главной вентиляторной установки использование возможностей СДК позволяет в десятки-сотни раз снизить существующие риски критичных нарушений ПБ за сутки. Без использования возможностей СДК по мониторингу

нарушения ПБ за год неизбежны (для рассмотренного сценария угроз). При идеальном управлении с использованием СДК риск критичного нарушения ПБ за год может снизиться до уровня 0.015, что в 65.7 раз ниже, чем вероятность безопасного функционирования главной вентиляторной установки, равной 0.985 (0.985 = 1 - 0.015).

Задача 2-4.4.8.1. Прогнозирование риска утраты работоспособности.

На практике более часто наступает утрата работоспособности ГВУ, опосредованно влияющая на ПБ, но приводящая к вынужденным простоям ОПО, т.е. к ущербам в виде недополученной прибыли. Эта задача представляет собой взгляд на функционирование ГВУ с точки зрения надежности. Расчетный показатель – риск утраты работоспособности.

Рассмотрим фрагмент «дерева отказов», способных привести к простоям в работе ОПО из-за отказа главной вентиляторной установки – см. рис. 4.16 и рис. 4.24.

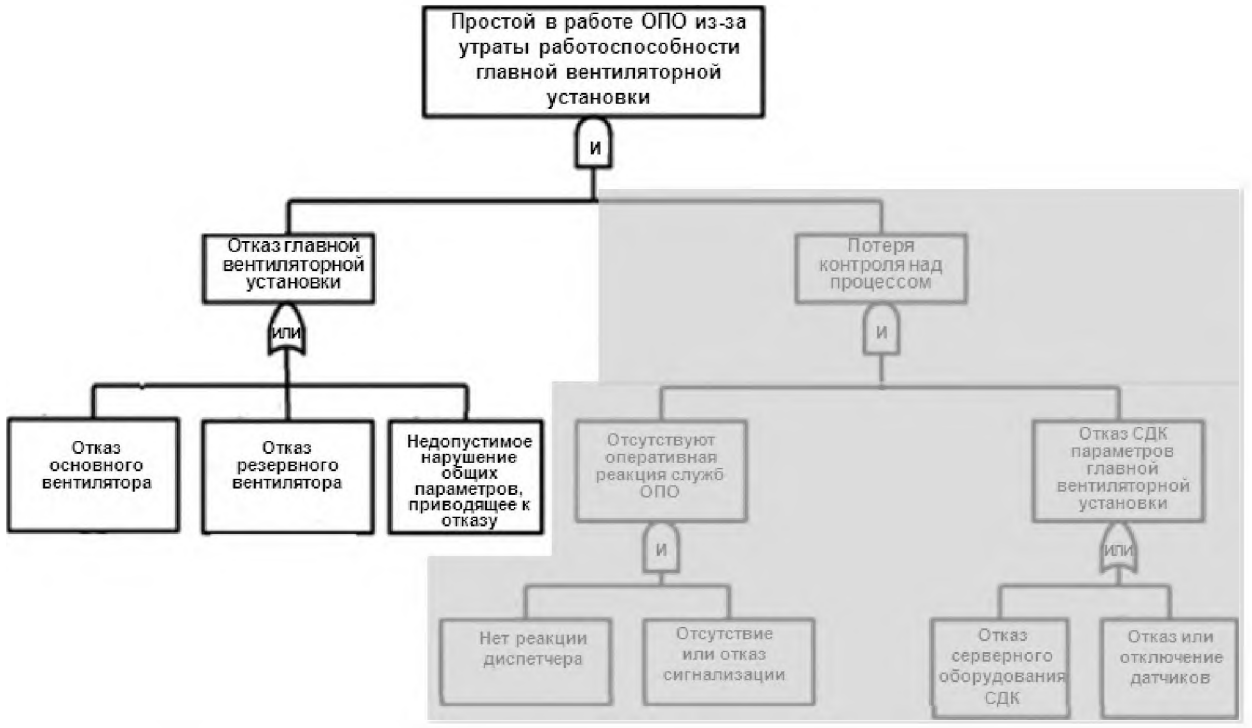


Рис. 4.24 Фрагмент дерева отказов, способных привести к простоям в работе ОПО из-за отказа главной вентиляторной установки (ГВУ)

В качестве анализируемого объекта для прогнозирования рисков нарушения ПБ выступает тот же ГВУ ВОКД 3,6, что и в задаче 1-4.4.8.1.

При анализе статистики функционирования СДК учитываются различные элементарные состояния системы вплоть до реального состояния «неработоспособен» *(«красный»).* Пример подобного состояния ГВУ ВОКД 3,6, учитываемого для определения частоты возникновения угроз по исследуемому объекту, отражен на рис. 4.25.

Рис. 4.25 Пример состояния ВОКД 3,6

Требуется осуществить прогноз рисков утраты работоспособности ГВУ на 1 сутки и на 1 год для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках обычной системы контроля (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК.

Решение задачи 2-4.4.8.1 с использованием предложенных решений из разделов 2 и 3.

Структура для прогнозирования рисков аналогична структуре, отраженной на рис. 4.17-4.19. Представленная формализация интерпретируется так: анализируемый объект (ВОКД 3,6) перейдет из состояния «условно работоспособен» *(«желтый»)* в состояние «неработоспособен» *(«красный»)*, если «ИЛИ» 1-я подсистема, «ИЛИ» 2-я подсистема перейдет в состояние «неработоспособен» *(«красный»)*. В свою очередь, с учетом резервирования вентиляторов 2-я подсистема перейдет в состояние «неработоспособен» *(«красный»)*, когда «И» элемент 2.1, «И» элемент 2.2 окажутся в состоянии «неработоспособен» *(«красный»)*.

Для каждого из элементов определяются необходимые исходные данные для прогнозирования рисков (см. подраздел 4.4.5 методики).

Перечень опасностей, перерастающих в угрозы, описательные модели угроз и возможные ущербы при нарушении ПБ связаны с простоями ОПО из-за ненадежности ГВУ согласно «дереву отказов». Ущерб эквивалентен недополученного на шахте дохода из-за вынужденных простоев.

Частота возникновения угроз и среднее время развития угроз определяются на базе статистики функционирования СДК, журналов инцидентов и отказов – все в полной аналогии с подходом, изложенным для задачи 1-4.4.8.1.

В отличие от условий задачи 1-4.4.8.1 частота возникновения угроз, приводящих к простоям ОПО, для 1-й подсистемы (общие параметры обработки) полагается равной 1 раз в неделю, для элемента 2.1 (основной вентилятор) - 2 раза в неделю, для элемента 2.2

(резервный вентилятор) – 1 раз в месяц (в задаче 1.1 для всех элементов - 1 раз в месяц). Остальные исходные данные – те же, что и для задачи 1-4.4.8.1.

Результаты прогнозирования рисков на сутки показали следующее.

Если не использовать механизмы управления, не предпринимать каких-либо мер противодействия угрозам (т.е. ничего не делать) либо не использовать возможности СДК по мониторингу оборудования, то риск утраты работоспособности за сутки равен 0.13 (см. рис. 4.26), что в 4 раза выше, чем риск для нарушения ПБ по условиям задачи 1-4.4.8.1. Среднее время до нарушения ПБ при этом составит 142 часа, т.е. в 3,4 раза меньше, чем для задачи 1-4.4.8.1 (см. рис. 4.27).

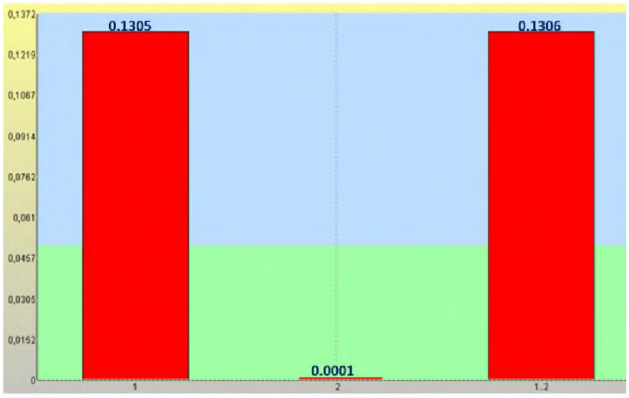


Рис. 4.26 Риск критичного нарушения ПБ за сутки при полном бездействии в задаче 2-4.4.7.1 (1- за 1-ю подсистему, 2- за 2-ю подсистему, 1…2 – за систему в целом)

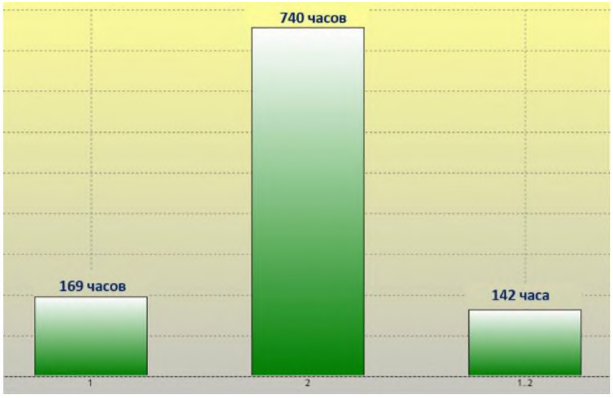


Рис. 4.27 Среднее время до нарушения ПБ при полном бездействии

Если идеально использовать механизмы управления, т.е. мгновенно предпринимать оперативные меры противодействия угрозам сразу же по выявлении предпосылок, не допускать ошибок в среднем в течение года, устранять все выявленные нарушения при каждой смене, то риск утраты работоспособности снижается до уровня 0.0002, что в 720 раз ниже, чем для существующей СК (без использования возможностей СДК), и в 4.5 раза выше, чем для задачи 1-4.4.8.1, среднее время наработки на отказ при этом составит 12 лет, т.е. в 3 раза меньше, чем для задачи 1-4.4.8.1.

Вывод по задаче 2-4.4.8.1. Для главной вентиляторной установки использование возможностей СДК позволяет в сотни раз снизить существующие риски утраты работоспособности за сутки. При возрастании частоты угроз на элементы ГВУ в 4-8 раз риск утраты работоспособности по сравнению с риском нарушения ПБ повышается в 4-5 раз, а среднее время наработки на отказ – снижается в 3-4 раза.

В задачах 1-4.4.8.1 и 2-4.4.8.1 различные риски прогнозировались для главной вентиляторной установки, т.е. фактически для отдельного конкретного оборудования. По мере структурного усложнения исследуемой системы показатели рисков должны логично

ухудшаться (т.к. количество последовательно объединяемых моделируемых подсистем возрастает). При этом важно понять, насколько существенным окажется ухудшение? Для ответа на этот вопрос ниже разбирается пример 4.4.8.2.

Пример 4.4.8.2. Исследуемая система – совокупность всех мониторируемых объектов.

В результате функционирования СДК со временем фиксируются конкретные состояния объектов контроля – например, на рис. 4.28 отражается элементарное состояние «условное обеспечение ПБ» *(«желтый»)*, а на рис. 4.29 - «критичное нарушение ПБ» *(«красный»)*.

Рис. 4.28 Все объекты контроля в состоянии «условное обеспечение ПБ» *(«желтый»)* и «штатное обеспечение ПБ» *(«зеленый»)*, плюс резерв

Рис. 4.29 Состояние «критичное нарушение ПБ» *(«красный»)*

Требуется спрогнозировать, каковы риски нарушения ПБ за 1 год и за сутки для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках СК (без использования возможностей СДК) и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК.

Решение. Рассмотрим фрагмент верхнего уровня «дерева отказов», способных привести к нарушению ПБ на ОПО. Причины определяются отказами со стороны комплекса главных вентиляторных установок (ГВУ), комплекса модульных дегазационных

установок (МДУ), комплекса газоотсасывающих установок – см. рис. 4.30.

Рис. 4.30 Фрагмент «дерева отказов» верхнего уровня

Логическая структура анализируемого объекта для прогнозирования рисков отражена на рис. 4.31.

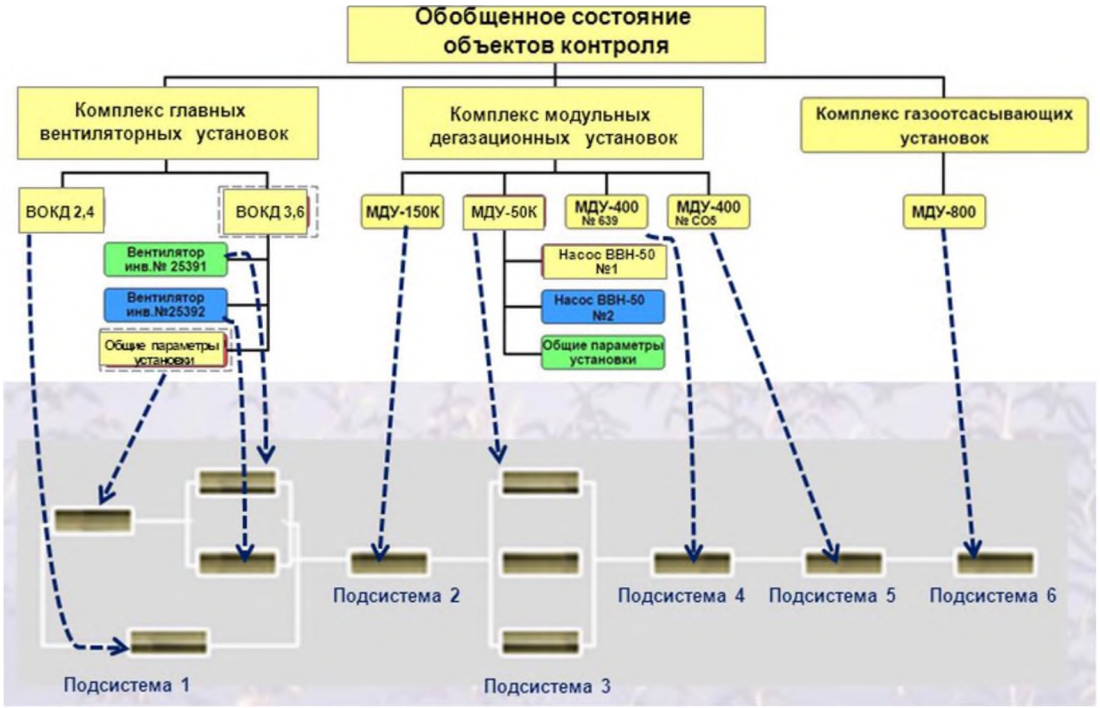


Рис. 4.31 Логическая структура для прогнозирования рисков

Для каждого из элементов формализации из статистики функционирования СДК, журналов инцидентов, функционирования различных комплексов и составных элементов определяются необходимые исходные данные для прогнозирования рисков согласно положениям 4.4.5 методики. Для ВОКД 3,6 применяются исходные данные, использованные для задачи 1-4.4.8.1, для ВОКД 2,4 и элементов МДУ 50К, – исходные данные, использованные для вентиляторов ВОКД 3,6. Для МДУ-400 частота угроз

положена равной 1 раз в неделю, для МДУ-800 - 2 раза в неделю, остальные данные – те, что использованы для задачи 1-4.4.8.1.

Результаты прогнозирования рисков на 1 год показали следующее.

Если не использовать механизмы управления, не предпринимать каких-либо мер противодействия угрозам (т.е. ничего не делать), то аварии неизбежны, риск практически равен 1, среднее время до нарушения ПБ при этом составит 41 час.

Если принимать меры в рамках СК (без использования возможностей СДК) с периодическим системным контролем 1 раз в смену (1 раз в сутки) без осуществления непрерывного мониторинга, то аварии по-прежнему неизбежны, среднее время до нарушения ПБ при этом составит по-прежнему 41 час, т.е. практически то же, что при полном бездействии. Узкими местами являются подсистемы 2, 4, 5, 6.

Если идеально использовать механизмы управления, т.е. мгновенно предпринимать оперативные меры сразу же по выявлении предпосылок, не допускать ошибок в среднем в течение года, устранять все выявленные нарушения при каждой смене, то риск критичного нарушения ПБ снижается до уровня 0.24 (см. рис. 4.32), что всего в 3 раза меньше, чем вероятность безопасного функционирования. Среднее время до нарушения ПБ при этом составит около 3.6 года - это в идеале (см. рис. 4.33).

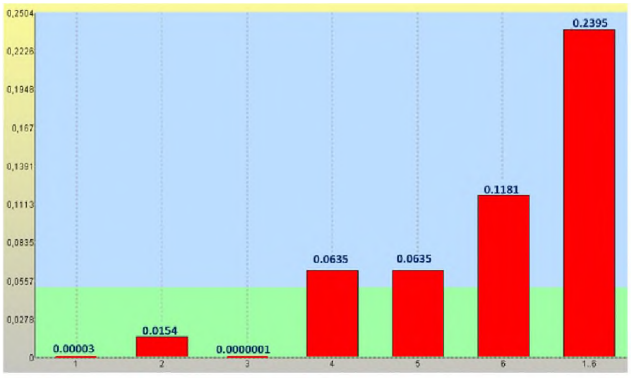


Рис. 4.32 Риск критичного нарушения ПБ за год при идеальном управлении в задаче 4.4.7.2 (1- за 1-ю подсистему, 2- за 2-ю подсистему, …, 1…6 – за систему в целом)

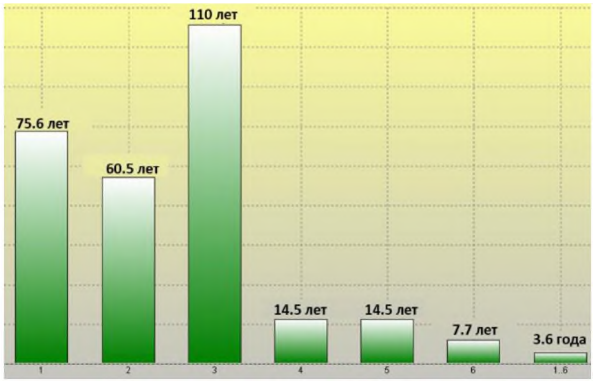


Рис. 4.33 Среднее время до нарушения ПБ при идеальном управлении

Зависимость риска нарушения ПБ от времени прогноза от 0.1 года до полутора лет отражена на рис. 4.34, риск со временем возрастает с уровня 0.027 (для периода прогноза 0.1 года) до уровня выше 0.3 (за 1.5 года). При этом, выбирая в качестве допустимого риска уровень 0.05 (который согласно ГОСТ Р 59991-2022 «Системная инженерия. Системный анализ процесса управления рисками для системы» рекомендуется при ориентации на обоснование для системы-эталона, в нашем случае - при управлении, ориентированном на идеальное), период прогноза выбирать до 0.2 года, т.е. не более 72 дней, чтобы

вероятностное значение интегрального риска не превышало допустимого уровня 0.05. В этом случае ориентация на 0.2 года – это тот срок, в течение которого целесообразно предпринимать упреждающие меры по снижению частных рисков для подсистем, являющихся «узкими местами» (это – подсистемы 4, 5, 6), и удержанию интегрального риска в допустимых пределах, т.е. не выше 0.05.

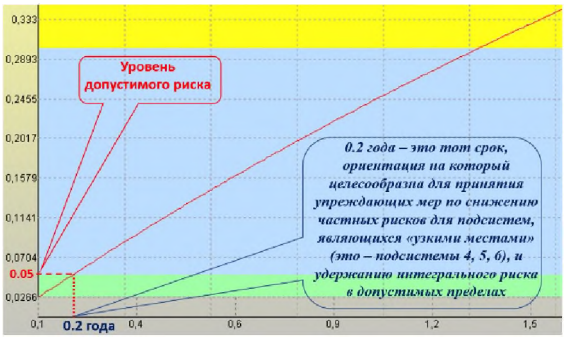


Рис. 4.34 Зависимость риска от периода прогноза (фрагмент ФР)

При прогнозе на сутки получены следующие результаты.

Если не использовать механизмы управления, не предпринимать каких-либо мер противодействия угрозам (т.е. ничего не делать), риск критичного нарушения ПБ за сутки составит 0.47, т.е. вероятность критичных нарушений ПБ окажется сравнимой с вероятностью его отсутствия. Если принимать меры в рамках обычной системы контроля (без использования возможностей СДК) с периодическим системным контролем 1 раз в смену (1 раз в сутки) без осуществления непрерывного мониторинга, то риск критичного нарушения ПБ за сутки составит 0.45 (см. рис. 4.35), т.е. практически как и при полном бездействии.

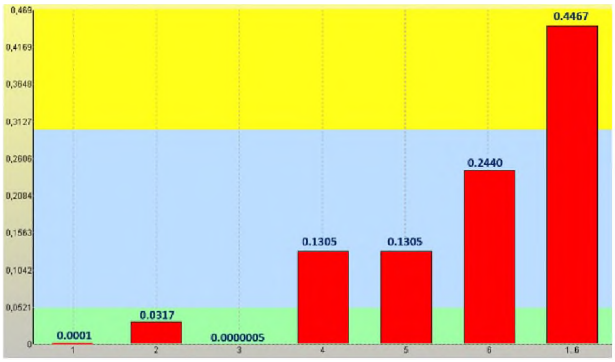


Рис. 4.35 Риск критичного нарушения ПБ за сутки при полном бездействии в задаче 4.4.7.2 (1- за 1-ю подсистему, 2- за 2-ю подсистему, …, 1…6 – за систему в целом)

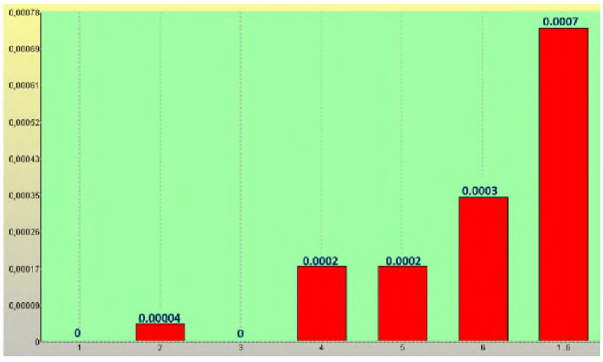


Рис. 4.36 Риск критичного нарушения ПБ за сутки при идеальном управлении в задаче 4.4.8.2 (1- за 1-ю подсистему, 2- за 2-ю подсистему, …, 1…6 – за систему в целом)

Если в течение суток идеально использовать механизмы управления, т.е. мгновенно предпринимать оперативные меры сразу же по выявлении предпосылок, не допускать

ошибок, устранять все выявленные нарушения при каждой очередной смене, то риск критичного нарушения ПБ снижается до уровня 0.0007 (см. рис. 4.36). Это – в 600 раз меньше, чем при полном бездействии и в рамках СК (без использования возможностей СДК). Интерпретация риска 0.0007 такова: вероятность хотя бы одного нарушения ПБ в 14000 раз ниже, нежели вероятность его отсутствия. Это – очень высокая гарантия отсутствия нарушений ПБ.

Вывод по решению задачи 4.4.8.2. Для всех объектов контроля использование возможностей СДК по мониторингу позволяет в сотни раз снизить существующие риски критичных нарушений ПБ за сутки. Без использования возможностей СДК по мониторингу нарушения ПБ для рассмотренного сценария угроз неизбежны. При идеальном управлении с использованием СДК риск критичного нарушения ПБ за год может снизиться до уровня 0.24, что в 3 раза ниже, чем вероятность безопасного функционирования исследуемого оборудования.

4.5 Адаптация для надежности функционального применения созданного прототипа технологии поддержки риск-ориентированной системной инженерии

Проводя адаптацию типовой методики подраздела 4.4 для оценки надежности выполнения функциональных действий созданным прототипом технологии поддержки риск-ориентированной системной инженерии в качестве моделируемой системы выбран непосредственно сам прототип.

Прототип технологии поддержки риск-ориентированной системной инженерии представлен в виде моделируемой системы из пяти подсистем - см. рис. 4.37 (сформировано из рис. 3.31, 4.1).

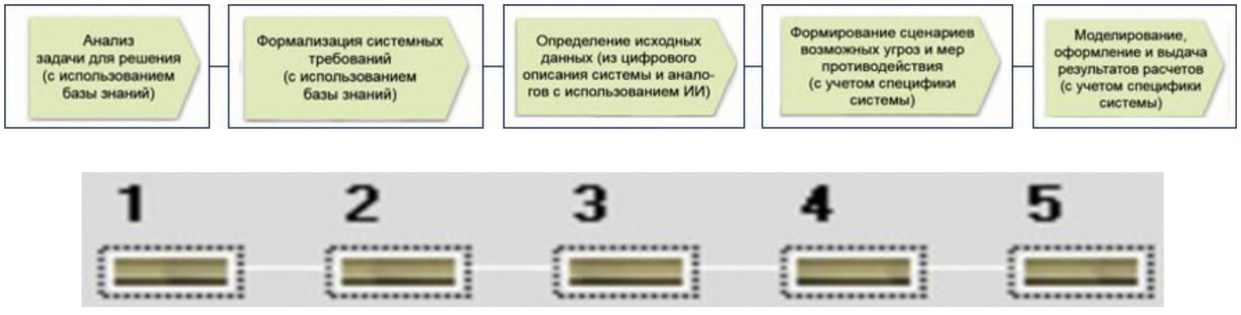


Рис. 4.37 Формализация моделируемой системы (созданного прототипа технологии поддержки риск-ориентированной системной инженерии) в виде 5 подсистем

1-я подсистема осуществляет анализ задачи, востребованной для ее решения.

2-я подсистема осуществляет формализацию системных требований для решения задачи.

3-я подсистема осуществляет определение исходных данных (например, из цифрового описания различных систем, рассматриваемых для решения задачи, в т.ч с использованием технологий искусственного интеллекта).

4-я подсистема осуществляет формирование сценариев возможных угроз и мер противодействия угрозам с учетом специфики систем, рассматриваемых для решения задачи.

5-я подсистема осуществляет непосредственно моделирование, оформление и выдачу результатов моделирования для их последующего использования.

Для расчета риска нарушения надежности выполнения функциональных действий в моделируемой системе применительно к каждому из элементов системы используются следующие исходные данные:

σ – частота возникновения источников угроз с точки зрения нарушения надежности выполнения функциональных действий;

β – среднее время развития угроз с момента их возникновения до нарушения целостности моделируемой системы с точки зрения нарушения надежности выполнения функциональных действий;

$T_{меж}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{восст}$ – среднее время восстановления нарушаемой целостности моделируемой системы.

Для всей моделируемой системы задается длительность периода прогноза $T_{зад}$.

Исходные данные для моделируемой системы сформированы из набранной статистики за период эксплуатации прототипа и его отдельных программных средств в различных системах в период с 2019 по 2025гг. – см. таблицу 4.1.

Таблица 4.1 – Исходные данные для моделирования

Исходные параметры	Подсистема 1	Подсистема 2	Подсистема 3	Подсистема 4	Подсистема 5
σ	12 раз в год (недопонимание моделей из-за необученности пользователей)	7 раз в год (некорректная формализация системных требований из-за ошибок пользователей)	361 раз в год (недоиспользование возможных способов извлечения исходных данных из цифровых	361 раз в год (затруднения в характеристиках возможных угроз и мер противодействия угрозам)	1 раз в год (технический сбой при моделировании)

			описаний систем)		
β	20 суток (развитие угрозы до ее реализации сопоставимо со сроком на представление отчетных материалов заказчику)	20 суток (развитие угрозы до ее реализации сопоставимо со сроком на представление отчетных материалов заказчику)	20 суток (развитие угрозы до ее реализации сопоставимо со сроком на представление отчетных материалов заказчику)	20 суток (развитие угрозы до ее реализации сопоставимо со сроком на представление отчетных материалов заказчику)	20 суток (развитие угрозы до ее реализации сопоставимо со сроком на представление отчетных материалов заказчику)
$T_{меж}$	10 минут (при постоянном контроле соизмеримо с временем на восприятие решаемой задачи)	10 минут (при постоянном контроле соизмеримо с временем на восприятие решаемой задачи)	10 минут (при постоянном контроле соизмеримо с временем на восприятие решаемой задачи)	10 минут (при постоянном контроле соизмеримо с временем на восприятие решаемой задачи)	10 минут (при постоянном контроле соизмеримо с временем на восприятие решаемой задачи)
$T_{диаг}$	1 минута (подтверждение надежности при нормальной работе)	1 минута (подтверждение надежности при нормальной работе)	1 минута (подтверждение надежности при нормальной работе)	1 минута (подтверждение надежности при нормальной работе)	1 минута (подтверждение надежности при нормальной работе)
$T_{восст}$	4 часа (среднее время восстановления по статистике)	20 часов (среднее время восстановления по статистике)	15 минут (среднее время восстановления по статистике)	15 минут (среднее время восстановления по статистике)	20 часов (среднее время восстановления по статистике)

Результаты прогноза риска нарушения надежности выполнения функциональных действий в моделируемой системе в течение года (в вероятностном выражении) отражены на рис. 4.38, 4.39. Анализ этих результатов показал следующее: риск нарушения надежности выполнения функциональных действий в моделируемой системе в течение года составляет 0.2611. Узким местом были 3-я и 4-я подсистемы, в которых наблюдался 361 случай возникновений угроз надежности выполнения требуемых функциональных действий (риск = 0.1386). В решающей степени это объяснялось недостаточной образовательной базой пользователей прототипа (начинающие системные аналитики, аспиранты, студенты) для подготовки исходных данных и формального описания содержательных сценариев возникновения и развития угроз при проведении системного анализа.

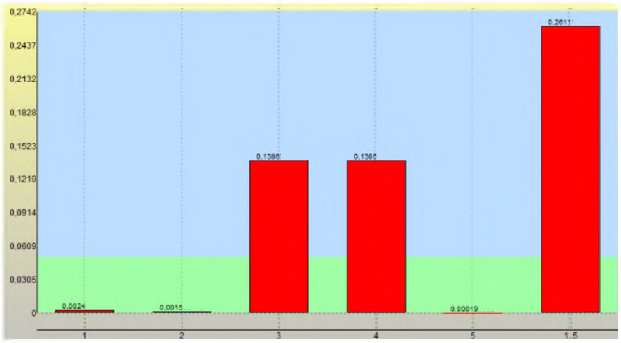


Рис. 4.38 Риск нарушения надежности выполнения функциональных действий в моделируемой системе в течение года

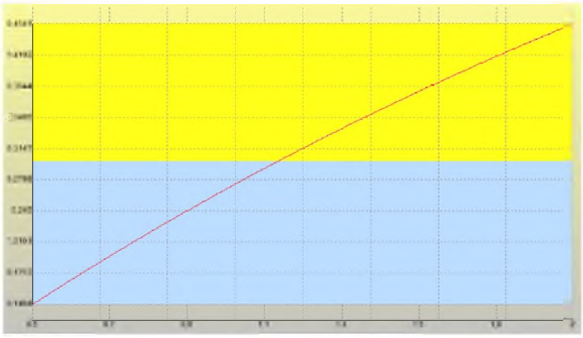


Рис. 4.39 Зависимость расчетного риска надежности выполнения функциональных действий в моделируемой системе от периода прогноза (от полугода до двух лет)

Несмотря на несущественность материального ущерба от реализации угроз, расчетный уровень риска существенно превышал условно допустимый. Так, соответствующая вероятность надежного выполнения функциональных действий в моделируемой системе составит 0.7389 (1-0.2611=0.7389), в то время, как рекомендуемый уровень составляет не ниже 0.99 при ориентации на систему-эталон (по ГОСТ Р 59341, приложению Д). Оставалось искать организационно-технический способ снижения риска нарушения надежности выполнения функциональных действий для этих подсистем.

Такой способ заключался в резервировании функций определения исходных данных, формирования сценариев возможных угроз и мер противодействия угрозам. Логическое резервирование обеспечивается, если выход из строя (отказ) одного элемента подстраховывается работой другого элемента. На самом деле можно сказать, что такая подстраховка уже частично осуществлялась, т.к. одновременно работали 3 системных аналитика (один – непосредственно пользователь прототипа, один обученный специалист, помогающий использованию прототипа в автономном режиме и один из разработчиков, осуществляющий сопровождение прототипа в удаленном режиме). Двое последних участников имели возможности использовать другие вычислительные средства для применения прототипа, кроме того они в совершенстве владели возможностями сформированной базы знаний быстрого осуществления функций определения исходных данных, формирования сценариев возможных угроз и мер противодействия угрозам с учетом специфики рассматриваемых систем. Тем самым логический или технический отказ у одного из участников применения прототипа не приводил к отказу выполнения соответствующих функциональных действий 3-й и 4-й подсистем, т.к. оставались действующими другие участники применения прототипа. В итоге вместо моделируемой

системы на рис. 4.37 получается другая моделируемая система с резервированием, подлежащая анализу – см. рис. 4.37.

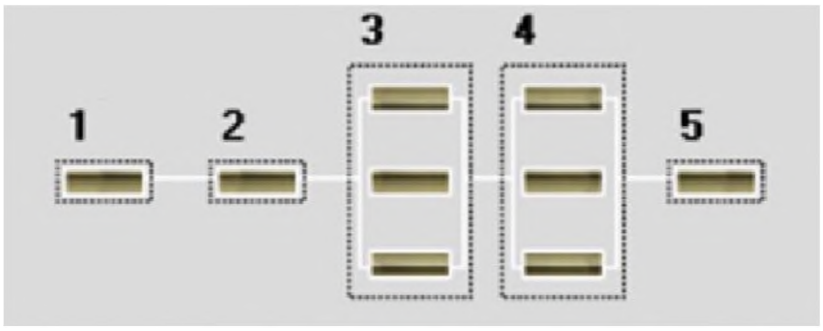


Рис. 4.40 Моделируемая система из пяти подсистем, критичных с точки зрения надежности применения прототипа технологии поддержки риск-ориентированной системной инженерии (с резервированием 3-й и 4-й подсистем)

Здесь подразумевается взаимное резервирование функциональных действий 3-й и 4-й подсистем со стороны трех участников моделирования.

Результаты прогноза риска нарушения надежности выполнения функциональных действий в моделируемой системе в течение года (в вероятностном выражении) отражены на рис. 4.41, 4.42.

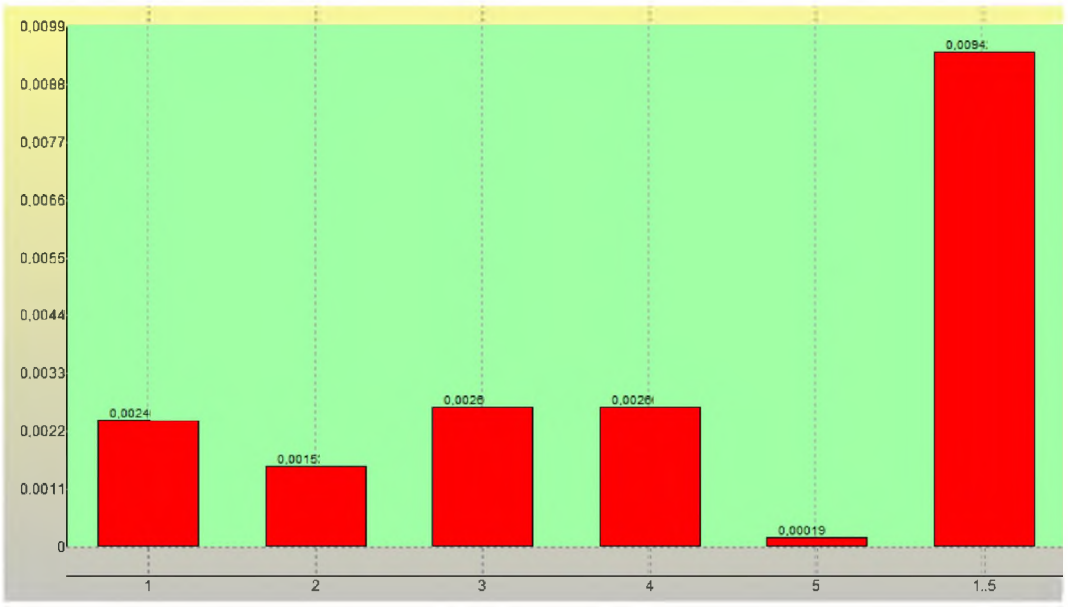


Рис. 4.41 Риск нарушения надежности выполнения функциональных действий в моделируемой системе с резервированием в течение года

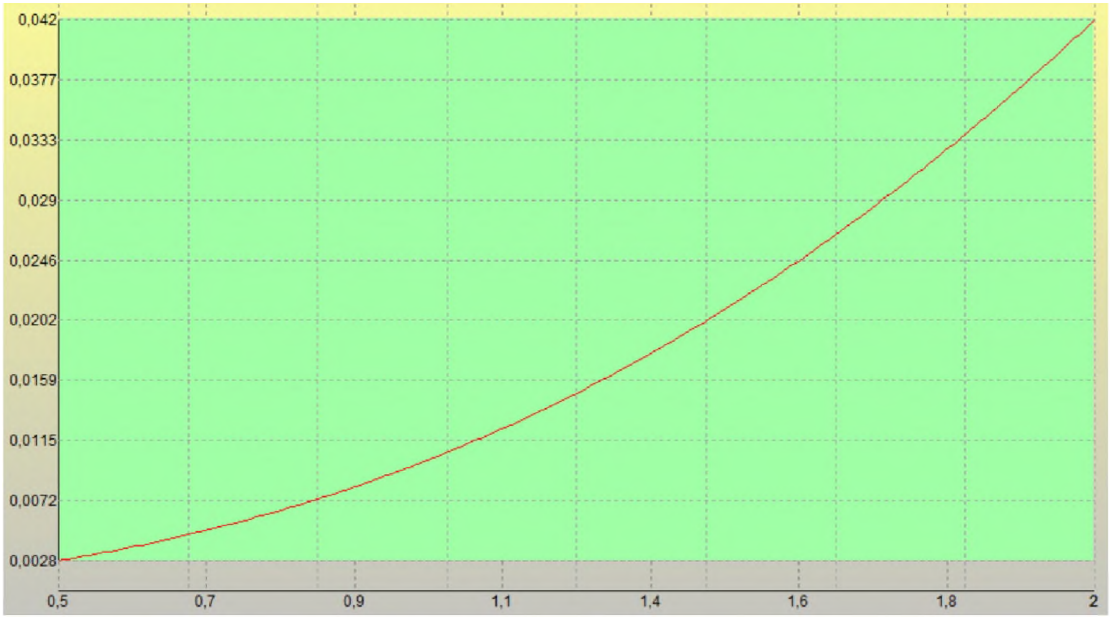


Рис. 4.42 Зависимость расчетного риска в моделируемой системе с резервированием от периода прогноза (от полугода до двух лет)

Анализ результатов моделирования показал следующее: риск нарушения надежности выполнения функциональных действий в моделируемой системе в течение года составила 0.0094. Т.е. соответствующая вероятность надежного выполнения функциональных действий в моделируемой системе в течение года составила 0.9906, что можно считать приемлемым результатом для обеспечения надежности применения созданного прототипа технологии поддержки риск-ориентированной системной инженерии.

4.6 Выводы по разделу 4

В результате научной проработки вопросов методического использования созданных программных и технологических решений для прогнозирования и упреждающего управления рисками в жизненном цикле систем сделаны следующие выводы.

1. Разработаны типовая методика прогнозирования рисков нарушения целостности моделируемой системы, представимой в виде «черного ящика», и типовая методика прогнозирования рисков нарушения целостности сложной моделируемой системы, применимые в жизненном цикле систем различного назначения.

2. Разработан инженерный подход к определению границ рабочего диапазона критичных параметров мониторируемого объекта. С инженерной точки зрения применение этого подхода дополнительно подтвердило и проиллюстрировало корректность аргументации доказанной в разделе 2 Теоремы 3 (о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам).

3. Применение разработанных типовых методик и инженерного подхода продемонстрировано на примерах исследований функционирования гипотетичной угольной шахты, включая:

- сравнение ручного контроля расхода воды в системе водоотлива с автоматическим контролем и восстановлением водного баланса с использованием системы дистанционного контроля (СДК);

- определение границ рабочего диапазона критичных параметров контролируемого оборудования;

- прогнозирование рисков нарушения промышленной безопасности главной вентиляторной установки (ГВУ) шахты и утраты работоспособности ГВУ для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках системы контроля без использования возможностей СДК и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК. Так, количественно обосновано, что для ГВУ использование возможностей СДК позволяет в сотни раз снизить существующие риски критичных нарушений ПБ и риски утраты работоспособности за сутки;

- прогнозирование рисков нарушения ПБ на опасном производственном объекте, рассматриваемом как сложная система, когда в качестве мониторируемых подсистем выступают комплексы главных вентиляторных установок, модульных дегазационных установок, газоотсасывающих установок. Так, количественно обосновано, что использование возможностей СДК по мониторингу всех объектов контроля позволяет в

сотни раз снизить существующие риски критичных нарушений ПБ за сутки. За год при идеальном управлении с использованием СДК риск критичного нарушения ПБ может снизиться до уровня 0.24, что в 3 раза ниже, чем вероятность безопасного функционирования исследуемого оборудования.

4. С применением разработанных методик проведен самоанализ надежности функционального применения созданного прототипа технологии поддержки риск-ориентированной системной инженерии (т.е. прототип применен для системного анализа самого себя). Результаты проведенного самоанализа по исходным данным, полученным в ходе опытной эксплуатации прототипа и его отдельных программных средств, подтвердили надежность применения созданного прототипа, при этом соответствующая вероятность надежного выполнения функциональных действий с использованием прототипа в течение года составила выше 0.99.

5. Разработанные методические решения в совокупности с разработанными в разделах 2 и 3 программными и технологическими решениями для ВС и КС позволили констатировать создание в итоге практически востребованных научно-техническим сообществом прототипа технологии поддержки риск-ориентированной системной инженерии.

5. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО СНИЖЕНИЮ И УДЕРЖАНИЮ РИСКОВ В ДОПУСТИМЫХ ПРЕДЕЛАХ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ РАЗЛИЧНОГО ФУНКЦИОНАЛЬНОГО НАЗНАЧЕНИЯ НА ОСНОВЕ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ПОДДЕРЖКИ РИСК-ОРИЕНТИРОВАННОЙ СИСТЕМНОЙ ИНЖЕНЕРИИ

На основе разработанных в разделах 2, 3, 4 программных, технологических и методических решений для ВС и КС в диссертации создан широко применимый прототип технологии поддержки риск-ориентированной системной инженерии. С учетом разработанных принципов для риск-ориентированного решения практических задач в настоящем разделе предлагаются расчетные примеры для различных областей приложения системной инженерии, вошедшие в сформированную базу знаний для моделирования и включающие рекомендации по:

- интерпретации возможностей использования созданного прототипа при реализации доктрины энергетической безопасности путем демонстрации способа логического преобразования изначального вербального описания сложной системы к формализованному виду, позволяющему использовать предложенные в диссертации программные, технологические и методические решения для формальных постановок и решений задач системной инженерии – см. подраздел 5.1;

- прогнозированию рисков по данным цифрового двойника промышленного объекта, сопровождаемого в процессе эксплуатации (на примере цифрового двойника фрагмента трубопроводной сети) – см. подразделе 5.2;

- моделированию многомодального взаимодействия социокиберфизических систем в жизненном цикле обогатительной фабрики в угольной отрасли – см. подраздел 5.3;

- оценке адекватности разработанных математических и программных решений на примерах управления рисками для обеспечения качества хранимого зерна – см. подраздел 5.4;

- извлечению знаний из анализа угроз злоумышленной модификации модели машинного обучения для сопровождаемых систем с искусственным интеллектом, а также демонстрацию расширяемости аналитических возможностей созданной инфраструктуры прототипа технологии поддержки риск-ориентированной системной инженерии – см. подраздел 5.5;

- использованию возможностей созданного прототипа в стандартизованных процессах системного анализа, управления человеческими ресурсами, качеством и рисками при проектировании и эксплуатации фармацевтического предприятия – см. подраздел 5.6.

Предлагаются перспективные направления дальнейших исследований в приложениях системной инженерии на основе использования результатов диссертации – см. подраздел 5.7.

Необходимо отметить, что разработанные программные, технологические и методические решения внедрены в учебный процесс РГУ нефти и газа им. И.М.Губкина по специализации «Системная инженерия» и были использованы магистрами при выполнении лабораторных работ по направлению подготовки дипломированных специалистов «Информатика и вычислительная техника» (654600), специальность «Автоматизированные системы обработки информации и управления» (220200). Это подтверждено актом о реализации – см. приложение В.

Ниже более подробно излагаются отдельные вопросы, связанные с применением созданного прототипа технологии поддержки риск-ориентированной системной инженерии, описанного в разделах 2-4 диссертации. Эти вопросы раскрываются в контексте формализации решения актуальных практических задач, вытекающих из ряда стратегических задач обеспечения национальной безопасности.

5.1 Рекомендации по интерпретации возможностей использования созданного прототипа технологии при реализации доктрины энергетической безопасности [145]

В подразделе предлагаются рекомендации по интерпретации возможностей использования созданного прототипа технологии поддержки риск-ориентированной системной инженерии в части анализа задачи для решения и формализации системных требований при реализации доктрины энергетической безопасности – см. рис. 5.1 (за исключением закрашенного серым цветом).

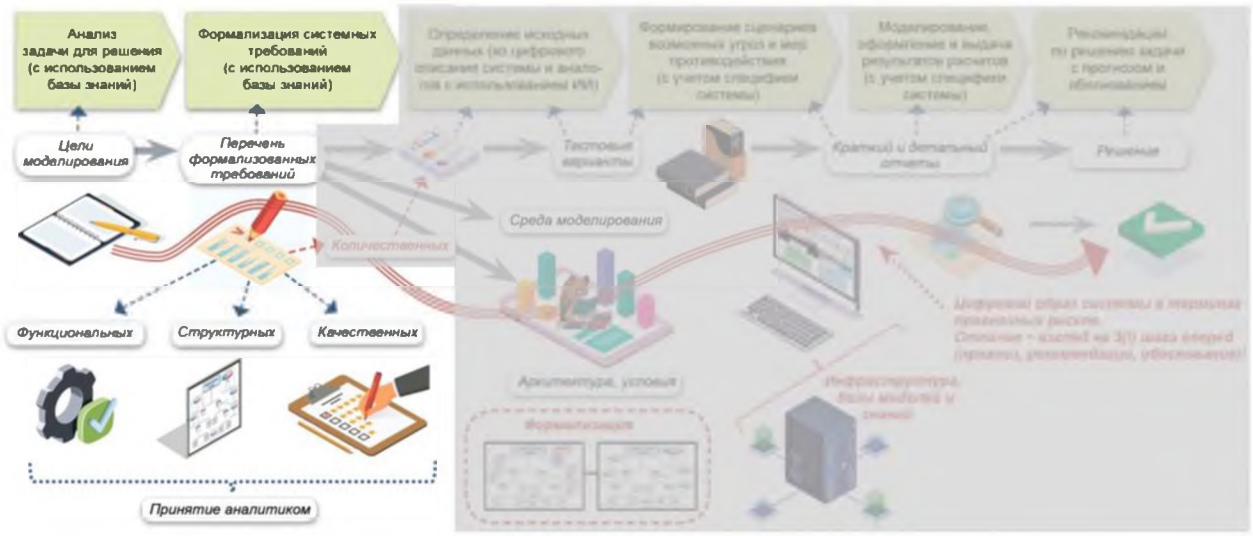


Рис. 5.1 Демонстрация возможностей применения разработанного прототипа в части анализа задачи для решения и формализации системных требований

Демонстрируется способ логического преобразования изначального вербального описания сложной системы к формализованному виду, позволяющему использовать предложенные в диссертации программные, технологические и методические решения для ВС и КС. Сведение вербального описания сложной системы к формализованному виду позволяет применять возможности созданного прототипа для формальной постановки и решения практических задач.

В качестве исследуемой системы в примере выступает технический облик гипотетичной многоуровневой системы управления рисками (СУР), подлежащей созданию в интересах обеспечения энергетической безопасности согласно "Доктрине энергетической безопасности Российской Федерации" (далее по тексту примера – Доктрина) и «Энергетической стратегии Российской Федерации на период до 2035 года».

С учетом множества факторов неопределенности состоянию энергетической безопасности государства, как моделируемой системе, присущи долговременные разнородные вызовы и угрозы. Основу энергетики государства составляет топливно-энергетический комплекс (ТЭК), включающий в себя нефтяную, газовую, угольную и торфяную отрасли, электроэнергетику и теплоснабжение. Предприятия ТЭК образуют критическую информационную инфраструктуру и подлежат всесторонней защите от разнородных угроз. При реализации энергетической стратегии неизбежны неопределенности в специфике решения практических задач, требующих математического моделирования, количественного прогнозирования рисков и системного анализа на различных мета-уровнях исследуемой системы СУР (см. идеи в 1-м разделе, рис. 1.7).

Для оценки состояния энергетической безопасности государства используются различные критерии, связанные с преследуемыми целями. Эти цели могут быть различными для федерального уровня, уровня федеральных округов, макрорегионов или отдельно взятого субъекта энергетической безопасности. Таким образом, заинтересованными сторонами, равно как и самостоятельными моделируемыми системами при решении задач системного анализа для СУР, могут выступать Российская Федерация в целом, федеральный округ, макрорегион или отдельно взятый субъект энергетической безопасности.

Набор применяемых критериев системного анализа должен опираться на доступную информацию для расчетов в СУР и позволять оценивать существующие и потенциально существенные угрозы и риски, обозначенные в Доктрине. Содержание каждого из критериев должно в полной мере отвечать преследуемой цели или совокупности целей и учитывать возможности прогнозирования динамики изменения состояния энергетической

безопасности государства во времени. Для реализации этих положений применимы различные методы и модели, использование которых ведет к достижению целей.

Основная цель обеспечения энергетической безопасности государства, как моделируемой системы, определена в пункте 22 Доктрины (далее используется обозначение цели от 22а) до 22о) в зависимости от конкретизации этих дефисов по тексту пункта 22 в Доктрине). Так, согласно Доктрине целью обеспечения энергетической безопасности является «поддержание защищенности экономики и населения страны от угроз энергетической безопасности на уровне, соответствующем требованиям законодательства Российской Федерации, касающимся:

- 22а) воспроизводства минерально-сырьевой базы ТЭК;

- 22б) надежного и устойчивого обеспечения российских потребителей энергоресурсами стандартного качества и услугами в сфере энергетики;

- 22в) формирования запаса продукции организаций ТЭК в государственном материальном резерве и поддержания его на необходимом уровне;

- 22г) обеспечения технической доступности инфраструктуры ТЭК для различных групп потребителей и возможности оказания им услуг в сфере энергетики;

- 22д) регулирования цен (тарифов) на продукцию организаций ТЭК и услуги в сфере энергетики;

- 22е) осуществления инвестиционной деятельности в сфере энергетики, обеспечения защиты прав инвесторов, контроля за иностранными инвестициями в российские организации ТЭК, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства;

- 22ж) осуществления антимонопольного регулирования и развития конкуренции, включая развитие организованной (биржевой) торговли продукцией организаций ТЭК;

- 22з) обеспечения энергосбережения и повышения энергетической эффективности;

- 22и) обеспечения антитеррористической защищенности и безопасности инфраструктуры и объектов ТЭК, в том числе в условиях чрезвычайных ситуаций;

- 22к) обеспечения защищенности критической информационной инфраструктуры объектов ТЭК;

- 22л) осуществления экспорта продукции, технологий и услуг организаций ТЭК;

- 22м) ограничения отрицательного воздействия на окружающую среду и обеспечения экологической безопасности хозяйственной деятельности организаций ТЭК;

- 22н) защиты населения и территорий от чрезвычайных ситуаций, возникающих на объектах ТЭК;

- 22о) применения российских технологий, оборудования, материалов, программного обеспечения при реализации инвестиционных проектов в отраслях ТЭК на территории РФ».

Тем самым по результатам рассмотрения вербального описания рассматриваемой проблематики определены заинтересованные стороны и цели системного анализа для СУР.

В рамках системного анализа СУР различают два типа критериев оценки:

1-й тип (анализ): критерии для решения задач анализа, в т. ч. связанных с прогнозированием рисков;

2-й тип (синтез): критерии для поддержки принятия решений по выработке рациональных упреждающих мер противодействия угрозам.

Далее по результатам изучения вербального описания для решения задач анализа определены следующие критерии 1-го типа КА1, КА2, КА3 (см. рисунок 5.2).

Рис. 5.2 Применимые критерии для решения задач анализа

Критерий КА1 – это критерий прогнозирования рисков перерастания вызовов энергетической безопасности в угрозы в течение задаваемого прогнозного периода времени в сравнении с допустимыми, что используется в отношении внешнеэкономических (см. п.

8 Доктрины), внешнеполитических (см. пп. 9–10 Доктрины), внутренних (см. п. 15 Доктрины) и трансграничных вызовов (см. п. 18 Доктрины).

Критерий КА2 – это критерий прогнозирования рисков реализации угроз энергетической безопасности или наступления обстоятельств, оказывающих отрицательное влияние на состояние энергетической безопасности (в зависимости от действий или бездействия субъектов энергетической безопасности) в течение задаваемого прогнозного периода времени в сравнении с допустимыми, что используется в отношении внешнеэкономических (см. пп. 11–12 Доктрины), внешнеполитических (см. п. 13 Доктрины), внутренних (см. п. 16 Доктрины) и трансграничных угроз (см. п. 19 Доктрины) с учетом последствий (см. п. 21 Доктрины), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24–29 Доктрины);

Критерий КА3 – это критерий прогнозирования интегрального риска реализации изначальных угроз энергетической безопасности и угроз, способных перерасти из вызовов, в течение задаваемого прогнозного периода времени в сравнении с допустимым уровнем. Это используется в отношении внешнеэкономических, внешнеполитических, внутренних и трансграничных вызовов и угроз с учетом последствий (по пп. 8–21 Доктрины), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24–29 Доктрины).

Введенные критерии связаны с прогнозированием соответствующих рисков. Согласно п.4 Доктрины под риском в области энергетической безопасности понимается возможность перерастания вызова энергетической безопасности в угрозу, реализации угрозы энергетической безопасности или наступления иных обстоятельств, оказывающих отрицательное влияние на состояние энергетической безопасности, в зависимости от действий или бездействия субъектов энергетической безопасности. В количественном выражении эти риски в полной мере могут быть оценены сочетанием вероятности нанесения ущерба и тяжести этого ущерба. Характеристика угроз, способных возникнуть из вызовов, отражена в Таблице 5.1. В свою очередь характеристика рисков в области энергетической безопасности, связанных с разнородными угрозами, и последствий от возможной реализации угроз отражена в Таблице 5.2. В этих таблицах введены соответствующие обозначения для последующей формализации постановок задач.

Таблица 5.1. Характеристика угроз, способных возникнуть из вызовов

Вызовы энергетической безопасности	**Угрозы, способные возникнуть из вызовов**
Внешнеэкономические вызовы (согласно п. 8 Доктрины):	Угрозы, способные возникнуть из внешнеэкономических вызовов:

Вызовы энергетической безопасности	**Угрозы, способные возникнуть из вызовов**
- ВнешЭВ8а) — перемещение центра мирового экономического роста в Азиатско-Тихоокеанский регион; - ВнешЭВ8б) — замедление роста мирового спроса на энергоресурсы и изменение его структуры, в том числе вследствие замещения нефтепродуктов другими видами энергоресурсов, развития энергосбережения и повышения энергетической эффективности; - ВнешЭВ8в) — увеличение мировой ресурсной базы углеводородного сырья, усиление конкуренции экспортеров энергоресурсов, в том числе в связи с появлением новых экспортеров; - ВнешЭВ8г) — изменение международного нормативно-правового регулирования в сфере энергетики и условий функционирования мировых энергетических рынков, усиление позиций потребителей; - ВнешЭВ8д) — рост производства сжиженного природного газа и его доли на мировых энергетических рынках, формирование глобального рынка природного газа; - ВнешЭВ8е) — увеличение доли возобновляемых источников энергии в мировом топливно-энергетическом балансе	- ВнешЭВ-У8а) — угрозы, связанные с перемещением центра мирового экономического роста в Азиатско-Тихоокеанский регион; - ВнешЭВ-У8б) — угрозы, связанные с замедлением роста мирового спроса на энергоресурсы и изменением его структуры, в том числе вследствие замещения нефтепродуктов другими видами энергоресурсов, развития энергосбережения и повышения энергетической эффективности; - ВнешЭВ-У8в) — угрозы, связанные с увеличением мировой ресурсной базы углеводородного сырья, усилением конкуренции экспортеров энергоресурсов, в том числе в связи с появлением новых экспортеров; - ВнешЭВ-У8г) — угрозы, связанные с изменением международного нормативно-правового регулирования в сфере энергетики и условий функционирования мировых энергетических рынков, усиление позиций потребителей; - ВнешЭВ-У8д) — угрозы, связанные с ростом производства сжиженного природного газа и его доли на мировых энергетических рынках, формированием глобального рынка природного газа; - ВнешЭВ-У8е) — угрозы, связанные с увеличением доли возобновляемых источников энергии в мировом топливно-энергетическом балансе
Внешнеполитические вызовы (согласно п. 9 Доктрины): - ВнешПВ9 — наращивание международных усилий по реализации климатической политики и ускоренному переходу к "зеленой экономике"	Угрозы, способные возникнуть из внешнеполитических вызовов: - ВнешПВ-У9 — угрозы, связанные с наращиванием международных усилий по реализации климатической политики и ускоренному переходу к "зеленой экономике"
Внутренние вызовы (согласно п. 15 Доктрины): - ВнВ15а) — переход РФ к новой модели социально- экономического развития, предполагающей структурную трансформацию экономики, сбалансированное пространственное и региональное развитие, модернизацию основных производственных фондов организаций, существенное повышение производительности труда и эффективности экономической деятельности; - ВнВ15б) — демографическая ситуация в РФ (медленный рост численности населения, увеличение в нем доли граждан старшего поколения, сокращение численности трудоспособного населения, внутренняя и внешняя миграция), влияющая как на перспективы внутреннего спроса на продукцию и услуги организаций ТЭК, так и на обеспеченность этих организаций трудовыми ресурсами	Угрозы, способные возникнуть из внутренних вызовов: - ВнВ-У15а) — угрозы, связанные с переходом РФ к новой модели социально- экономического развития, предполагающей структурную трансформацию экономики, сбалансированное пространственное и региональное развитие, модернизацией основных производственных фондов организаций, существенным повышением производительности труда и эффективности экономической деятельности; - ВнВ-У15б) — угрозы, связанные с демографической ситуацией в РФ (медленным ростом численности населения, увеличением в нем доли граждан старшего поколения, сокращением численности трудоспособного населения, внутренней и внешней миграцией), влияющие как на перспективы внутреннего спроса на продукцию и услуги организаций ТЭК, так и на обеспеченность этих организаций трудовыми ресурсами
Трансграничные вызовы (согласно п. 18 Доктрины): - ТрансВ18 — развитие и распространение прорывных технологий в сфере энергетики, в том числе технологий использования возобновляемых источников энергии, распределенной генерации электрической	Угрозы, способные возникнуть из трансграничных вызовов: - ТрансВ-У18 — угрозы, связанные с развитием и распространением прорывных технологий в сфере энергетики, в том числе технологий использования возобновляемых источников энергии, распределенной генерации электрической энергии,

Вызовы энергетической безопасности	Угрозы, способные возникнуть из вызовов
энергии, накопителей энергии, добычи углеводородного сырья из трудноизвлекаемых запасов, цифровых и интеллектуальных технологий, энергосберегающих и энергоэффективных технологий на транспорте, в строительстве, жилищно-коммунальном хозяйстве и промышленности	накопителей энергии, добычи углеводородного сырья из трудноизвлекаемых запасов, цифровых и интеллектуальных технологий, энергосберегающих и энергоэффективных технологий на транспорте, в строительстве, жилищно-коммунальном хозяйстве и промышленности

Таблица 5.2. Характеристика рисков, связанных с разнородными угрозами, и последствий от возможной реализации угроз

Угрозы энергетической безопасности	Риски в области энергетической безопасности
Внешнеэкономические, внешнеполитические и военно-политические угрозы (согласно пп. 8, 9, 11, 13 Доктрины): - угрозы от ВнешЭВ-У8а) до ВнешЭВ-У8е), способные возникнуть из внешнеэкономических вызовов; - угрозы ВнешПВ-У9, способные возникнуть из внешнеполитических вызовов; - ВнешЭУ11а) — сокращение традиционных для РФ внешних энергетических рынков и трудности, связанные с выходом на новые энергетические рынки; - ВнешЭУ11б) — использование иностранными государствами договорноправовых, международно-правовых и финансовых механизмов в целях нанесения ущерба топливно-энергетическому комплексу РФ и ее экономике в целом; - ВнешЭУ11в) — дискриминация российских организаций ТЭК на мировых энергетических рынках путем изменения международного нормативно-правового регулирования в сфере энергетики, в том числе под предлогом реализации климатической и экологической политики или диверсификации источников импорта энергоресурсов; - ВнешЭУ11г) — незаконный отбор экспортируемых Россией энергоресурсов при их транспортировке по территориям иностранных государств; - ВоенПУ13а) — резкое обострение военно-политической обстановки (межгосударственных отношений) и создание условий для применения военной силы; - ВоенПУ13б) — возникновение и эскалация на территориях государств, сопредельных с Российской Федерацией и ее союзниками, или в других регионах мира вооруженных конфликтов, угрожающих добыче, транспортировке или потреблению российских энергоресурсов, а также ограничивающих возможность использования российских технологий и оказания российскими организациями услуг в сфере энергетики	Риски, связанные с внешними вызовами и угрозами (согласно п. 14 Доктрины): - Р14а) – риск недостаточных темпов реагирования российских организаций ТЭК на тенденции в мировой энергетике, в том числе в части, касающейся освоения новых технологий и коммерческого использования запасов углеводородного сырья; - Р14б) – риск недостаточной эффективности механизмов предупреждения дискриминации российских организаций ТЭК со стороны иностранных государств и их объединений, а также механизмов противодействия такой дискриминации; - Р14в) – недостаточная готовность организаций ТЭК к функционированию в случае реализации военно-политических угроз; - Р14г) – принятие неверных долгосрочных инвестиционных решений в условиях высокой неопределенности мировых энергетических рынков
Внутренние угрозы (согласно пп. 15,16 Доктрины): - угрозы ВнВ-У15а) и ВнВ-У15б), способные возникнуть из внутренних вызовов; - ВнУ16а) — несоответствие возможностей ТЭК потребностям социально-экономического	Риски, связанные с внутренними вызовами и угрозами (согласно п. 17 Доктрины): - Р17а) – риск несогласованного развития отраслей ТЭК и видов деятельности в сфере энергетики, включая экспорт продукции и услуг организаций

Угрозы энергетической безопасности	Риски в области энергетической безопасности
развития РФ (энергетический дефицит или избыток энергетических мощностей и инфраструктуры ТЭК); - ВнУ16б) — снижение качества минерально-сырьевой базы ТЭК (истощение действующих месторождений, уменьшение размеров и снижение качества открываемых месторождений); - ВнУ16в) — недостаточная обеспеченность организаций ТЭК трудовыми ресурсами, в особенности высококвалифицированными кадрами; - ВнУ16г) — рост количества преступлений и правонарушений в сфере энергетики (хищения, коррупция, производство и продажа контрафактной продукции, неплатежи); - ВнУ16д) — рост количества нарушений в сфере трудовых отношений в организациях ТЭК, жилищно- коммунального хозяйства и транспорта, в том числе нарушений требований охраны труда, а также случаев проведения незаконных забастовок.	ТЭК, в условиях ограниченного государственного контроля и регулирования; - Р17б) – риск отсутствия в долгосрочной перспективе определенности относительно спроса на продукцию и услуги организаций ТЭК в субъектах РФ; - Р17в) – риск низкой эффективности осуществляемых субъектами энергетической безопасности мер по поддержанию финансовой устойчивости организаций ТЭК при наступлении неблагоприятных условий, таких как рост неплатежей за поставленные организациями ТЭК энергоресурсы и оказанные ими услуги, увеличение транспортных расходов и капитальных затрат таких организаций при освоении нефтегазовых месторождений, находящихся в удаленных местностях, усложнение компонентного состава нефтегазовых месторождений; - Р17г) – риск чрезмерной финансовой нагрузки на организации ТЭК в результате увеличения размеров налоговых, таможенных и иных платежей; - Р17д) – риск избыточности требований, касающихся обеспечения экологической безопасности при осуществлении деятельности в отраслях ТЭК, рост затрат организаций ТЭК на обеспечение выполнения таких требований; - Р17е) – риск необоснованной монополизации в отраслях ТЭК и неравных условий конкуренции в конкурентных видах деятельности в сфере энергетики; - Р17ж) – риск высокого уровня износа основных производственных фондов организаций ТЭК, низкой эффективности использования и недостаточных темпов обновления этих фондов; - Р17з) – риск нерационального потребления энергоресурсов; - Р17и) — риск недостаточных темпов реагирования системы профессионального образования на изменение потребности организаций ТЭК в квалифицированных кадрах
Трансграничные угрозы (согласно пп. 18, 19 Доктрины): - угрозы ТрансВ-У18, способные возникнуть из трансграничных вызовов; - ТрансУ19а) — террористическая и диверсионная деятельность, наносящая ущерб инфраструктуре и объектам ТЭК; - ТрансУ19б) — противоправное использование информационно-телекоммуникационных технологий, в том числе осуществление компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способное привести к нарушениям функционирования инфраструктуры и объектов ТЭК; - ТрансУ19в) — неблагоприятные и опасные природные явления, изменения окружающей среды, приводящие к нарушению нормального функционирования и разрушению инфраструктуры и объектов ТЭК	Риски, связанные с трансграничными вызовами и угрозами (согласно п. 20 Доктрины): - Р20а) — несоответствие технологического уровня российских организаций ТЭК современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков; - Р20б) — недостаточное развитие нормативно-правовой базы, сдерживающее внедрение инновационных технологий, в том числе технологий использования возобновляемых источников энергии, распределенной генерации электрической энергии и цифровых технологий в сфере энергетики; - Р20в) — недостаточная инновационная активность организаций ТЭК и организаций, осуществляющих деятельность в смежных отраслях экономики, ориентация таких организаций на

Угрозы энергетической безопасности	Риски в области энергетической безопасности
	импорт технологий вместо развития отечественного научно-технологического потенциала; - Р20г) — недостаточные темпы разработки и внедрения новых средств антитеррористической защиты инфраструктуры и объектов ТЭК; - Р20д) — недостаточный уровень защищенности инфраструктуры и объектов ТЭК от актов незаконного вмешательства и опасных природных явлений
Последствиями реализации угроз энергетической безопасности (согласно п. 21 Доктрины): - Посл21а) — причинение вреда жизни и здоровью граждан; - Посл21б) — нарушение нормального функционирования организаций, в том числе организаций ТЭК, и отраслей экономики РФ; - Посл21в) — увеличение расходов потребителей на организацию альтернативных способов топливо- и энергоснабжения и на создание запасов (резервов) энергоресурсов; - Посл21г) — рост цен (тарифов) на продукцию организаций ТЭК и услуги в сфере энергетики; - Посл21д) — снижение финансово устойчивости и прекращение деятельности организаций ТЭК; - Посл21е) — уменьшение объема инвестиций в отрасли ТЭК; - Посл21ж) — уменьшение налоговых, таможенных и иных платежей в бюджеты бюджетной системы РФ со стороны организаций ТЭК; - Посл21з) — необходимость выделения дополнительных бюджетных ассигнований на ликвидацию последствий реализации угроз энергетической безопасности	

Для поддержки принятия решений в СУР применимы критерии КВ1, КВ2, КВ3 для выработки рациональных упреждающих мер противодействия угрозам (критерии 2-го типа), действующие в условиях внешнеэкономических, внешнеполитических, внутренних и трансграничных вызовов и угроз с учетом последствий (по пп. 8–21 Доктрины), основных направлений деятельности и решаемых задач по обеспечению энергетической безопасности (по пп. 24–29 Доктрины) – см. рисунок 5.3.

Критерий КВ1 – это критерий удержания интегрального и/или частных рисков в допустимых пределах в течение задаваемого прогнозного периода времени при ограничениях на эксплуатационные условия и ресурсы.

Критерий КВ2 – это критерий минимизации затрат при ограничениях на допустимый уровень интегрального и/или частных рисков в течение задаваемого прогнозного периода времени, эксплуатационные условия и ресурсы.

Критерий КВ3 – это критерий минимизации интегрального риска при ограничениях на допустимый уровень частных рисков в течение задаваемого прогнозного периода времени, эксплуатационные условия и ресурсы.

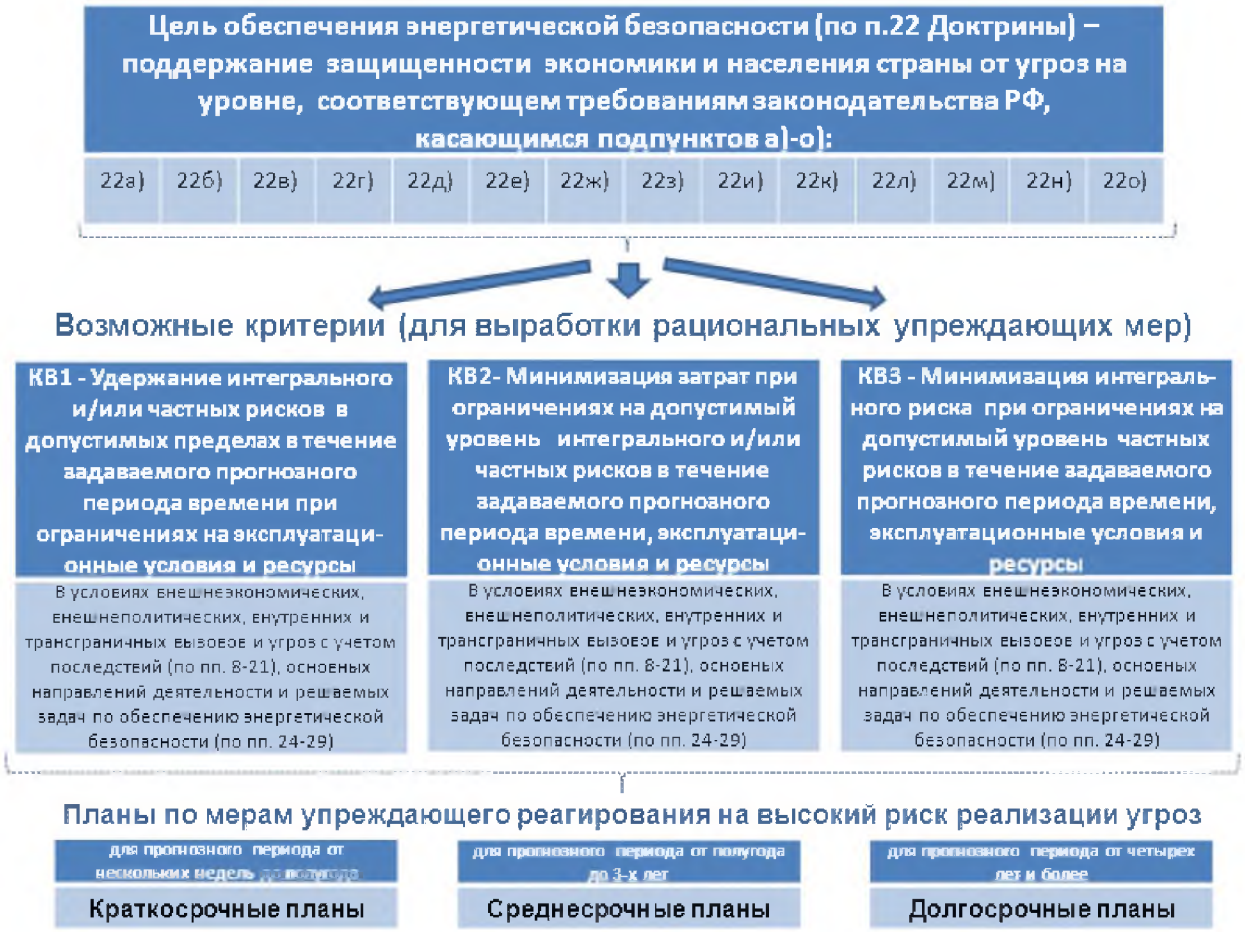


Рис. 5.3 Применимые критерии для решения задач выработки рациональных упреждающих мер

При этом под частными рисками в области энергетической безопасности понимаются (см. таблицы 5.1 и 5.2):

- риски, связанные с внешними вызовами и угрозами энергетической безопасности согласно п. 14 Доктрины, обозначаемые от Р14а) до Р14г);

- риски, связанные с внутренними вызовами и угрозами энергетической безопасности согласно п. 17 Доктрины, обозначаемые от Р17а) до Р17и);

- риски, связанные с трансграничным вызовами и угрозами энергетической безопасности согласно п. 20 Доктрины, обозначаемые от Р20а) до Р20д).

Под интегральным риском понимается сочетание вероятности нанесения ущерба и тяжести этого ущерба, характеризующее степень отрицательного влияния на состояние энергетической безопасности государства от реализации всего множества внешнеэкономических, внешнеполитических, военно-политических, внутренних и трансграничных угроз в области энергетической безопасности с учетом возможных последствий. Как пример - выполнение требований по защите информации реализуется путем достижения цели Доктрины с условным номером 22к), связанной с обеспечением защищенности критической информационной инфраструктуры объектов ТЭК.

По результатам решения задач анализа и выработки рациональных упреждающих мер формируют кратко- средне- и/или долгосрочные планы по реализации комплекса мер реагирования на невыполнение критичных ограничений на эксплуатационные условия и ресурсы и на недопустимые риски (см. рис. 5.1).

Планы формируют с привязкой к скоротечности реализации угроз и размеру соответствующего риска, рассчитываемого в динамике изменения состояния уровня энергетической безопасности. Например:

к 1-й группе могут быть отнесены краткосрочные планы по реализации комплекса мер, которые надлежит принять в качестве упреждающей реакции на высокий риск реализации угроз в течение заданного прогнозного периода от нескольких недель до полугода;

ко 2-й группе могут быть отнесены среднесрочные планы по реализации комплекса мер, которые надлежит принять в качестве упреждающей реакции на высокий риск реализации угроз в течение заданного прогнозного периода от полугода до 3-х лет, что соизмеримо с планированием бюджета РФ на 3 года;

к 3-й группе могут быть отнесены долгосрочные планы по реализации комплекса мер в качестве упреждающей реакции на высокий риск реализации угроз в течение заданного прогнозного периода более 3-х лет.

При этом основные направления деятельности по обеспечению энергетической безопасности определены п.24 Доктрины (далее по тексту обозначены от Д24а) до Д24д) согласно тексту п.24 Доктрины). Решаемые по этим направлениям задачи, которые могут находить свое отражение в кратко-, средне- и долгосрочных планах, определены в пп. 25—29 Доктрины (см. таблицу 5.3).

Таблица 5.3. Задачи для отражения в кратко-, средне- и долгосрочных планах

Основные направления деятельности по обеспечению энергетической безопасности	Решаемые задачи
- НД24а) — совершенствование государственного управления в области обеспечения энергетической безопасности	- НД24а)-З25а) — совершенствование нормативно-правовой базы по вопросам обеспечения безопасного, надежного и устойчивого функционирования инфраструктуры и объектов энергетики; - НД24а)-З25б) — создание системы управления рисками в области энергетической безопасности, обеспечение ее взаимодействия с государственными информационными системами, системами мониторинга и прогнозирования чрезвычайных ситуаций на объектах ТЭК, иными системами управления рисками, используемыми субъектами энергетической безопасности; - НД24а)-З25в) — обеспечение стабильности налоговой политики и нормативно-правового регулирования в сфере энергетики, способствующей оптимизации финансовой нагрузки на организации ТЭК и привлечению в них инвестиций; - НД24а)-З25г) — долгосрочное и сбалансированное регулирование цен (тарифов) на товары и услуги субъектов естественных монополий и субъектов, осуществляющих

Основные направления деятельности по обеспечению энергетической безопасности	Решаемые задачи
	регулируемые виды деятельности, совершенствование ценовой политики в сфере энергетики на внутреннем рынке и планомерный переход к рыночным механизмам ценообразования в этой сфере с учетом социальной ответственности организаций ТЭК; - НД24а)-325д) — развитие конкуренции в отраслях ТЭК на внутреннем рынке и исключение не отвечающей экономическим интересам Российской Федерации конкуренции между различными видами российских энергоресурсов на мировых энергетических рынках; - НД24а)-325е) — профилактика и пресечение преступных и противоправных действий в сфере энергетики, в том числе нецелевого использования и хищения бюджетных средств, неплатежей, борьба с коррупцией, теневой экономикой, производством и продажей контрафактной продукции; - НД24а)-325ж) — пресечение деятельности, осуществляемой специальными службами и организациями иностранных государств, террористическими и экстремистскими организациями, направленной на нанесение ущерба инфраструктуре и объектам ТЭК; - НД24а)-325з) — осуществление федерального государственного контроля (надзора) за обеспечением безопасности объектов ТЭК, защита объектов ТЭК (в том числе объектов критической информационной инфраструктуры) от совершения актов незаконного вмешательства; - НД24а)-325и) — внедрение новой модели государственного регулирования в области промышленной безопасности с учетом степени риска возникновения аварий и масштаба их возможных последствий; - НД24а)-325к) — повышение эффективности федерального государственного надзора в области промышленной безопасности в части, касающейся инфраструктуры и объектов ТЭК, сокращение количества бесхозяйных объектов и совершенствование правовых механизмов привлечения к ответственности за нарушение требований промышленной безопасности; - НД24а)-325л) — обеспечение безопасных условий труда работников организаций ТЭК, развитие системы управления охраной труда и предупреждения производственного травматизма, совершенствование механизмов государственного контроля (надзора) за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права; - НД24а)-325м) — обеспечение социальной защиты высвобождаемых работников градообразующих организаций угольной промышленности и ликвидация последствий ведения горных работ;
- НД24б) — поддержание минерально-сырьевой базы ТЭК и основных производственных фондов организаций ТЭК на уровне, необходимом для обеспечения энергетической безопасности	- НД24а)-325н) — стимулирование энергосбережения и повышения энергетической эффективности экономики - НД24б)-326а) — обеспечение воспроизводства минерально-сырьевой базы ТЭК, повышение эффективности недропользования; - НД24б)-326б) — обеспечение безопасности при использовании атомной энергии; - НД24б)-326в) — снижение уязвимости, обеспечение управляемости и живучести инфраструктуры и объектов ТЭК, включая резервирование их мощностей и создание запасов топлива, в том числе для обеспечения его поставок в периоды пикового потребления, в условиях чрезвычайных ситуаций, в период мобилизации и в военное время; - НД24б)-326г) — поддержание на необходимом уровне запасов продукции организаций ТЭК в государственном материальном резерве; - НД24б)-326д) — проведение комплексной модернизации и оптимизации основных производственных фондов организаций ТЭК с использованием преимущественно отечественных инновационных, энергоэффективных и экологически безопасных технологий и оборудования, изготовленного на территории Российской Федерации, подготовка необходимых для этого кадров; - НД24б)-326е) — сбалансированное развитие локальных и интегрируемых в Единую энергетическую систему России распределенных источников энергоснабжения, формирование с их участием локальных интеллектуальных энергетических систем;

Основные направления деятельности по обеспечению энергетической безопасности	Решаемые задачи
	- НД24б)-326ж) — уменьшение отрицательного воздействия хозяйственной деятельности организаций ТЭК на окружающую среду
- НД24в) – совершенствование территориально-производственной структуры ТЭК с учетом необходимости укрепления единства экономического пространства Российской Федерации	- НД24в)-327а) — развитие инфраструктуры и объектов ТЭК Восточной Сибири, Арктической зоны Российской Федерации, Дальнего Востока, Северного Кавказа, Крыма и Калининградской области; - НД24в)-327б) — поддержание технологического единства, надежности, управляемости, непрерывности и безопасности работы Единой системы газоснабжения, Единой энергетической системы России и системы магистральных трубопроводов для транспортировки нефти и нефтепродуктов; - НД24в)-327в) — развитие внутреннего рынка сжиженного природного газа в целях обеспечения энергетической безопасности территорий, удаленных от Единой системы газоснабжения; - НД24в)-327г) – обеспечение экономически эффективного сочетания использования систем централизованного электро- и теплоснабжения с развитием распределенной генерации электрической энергии и интеллектуализацией энергетических систем, а также с использованием местных ресурсов, в том числе возобновляемых источников энергии
- НД24г) - обеспечение международно-правовой защиты интересов российских организаций ТЭК и энергомашиностроения, поддержка экспорта их продукции, технологий и услуг	- НД24г)-328а) – развитие интеграционных связей в рамках Евразийского экономического союза и Содружества Независимых Государств, углубление партнерства в сфере энергетики по линии объединения БРИКС, Шанхайской организации сотрудничества, развитие сотрудничества с иностранными государствами в рамках Форума стран - экспортеров газа, с Организацией стран – экспортеров нефти и другими международными организациями; - НД24г)-328б) – противодействие дискриминации на мировых энергетических рынках российских организаций ТЭК, осуществляющих экспорт продукции, технологий и услуг и участвующих в реализации международных проектов; - НД24г)-328в) – совершенствование внешнеполитических инструментов и механизмов взаимодействия с основными профильными международными организациями и участниками мировых энергетических рынков в целях обеспечения устойчивого функционирования этих рынков; - НД24г)-328г) – содействие осуществляемой на равноправной основе международной научно-технологической кооперации, освоению передовых
- НД24д) – обеспечение технологической независимости ТЭК и повышение его конкурентоспособности	иностранных технологий, стандартов и практик в сфере энергетики - НД24д)-329а) – планомерное осуществление импортозамещения в критически важных для устойчивого функционирования ТЭК видах деятельности, в том числе локализация производства иностранного оборудования или создание его отечественных аналогов, разработка технологий (в том числе информационно-телекоммуникационных) и программного обеспечения; - НД24д)-329б) – развитие отечественного научно-технологического потенциала, создание и освоение передовых технологий в сфере энергетики, в том числе технологий использования возобновляемых источников энергии, наращивание производства на территории Российской Федерации конкурентоспособного основного и вспомогательного оборудования, создание центров компетенций; - НД24д)-329в) – предотвращение критического отставания Российской Федерации в развитии цифровых и интеллектуальных технологий в сфере энергетики, снижение уязвимости объектов критической информационной инфраструктуры ТЭК; - НД24д)-329г) – развитие компетенций во всех видах деятельности, критически важных для устойчивого функционирования ТЭК; - НД24д)-329д) – содействие развитию российского энергомашиностроения и приборостроения, российской электротехнической промышленности; - НД24д)-329е) – расширение участия организаций ТЭК в развитии системы профессионального образования и дополнительного профессионального образования в сфере энергетики

Перечисленные в таблицах 5.1, 5.2, 5.3 угрозы, риски и задачи представляют собой составные элементы СУР и элементы различных моделируемых систем, изучаемых при решении задач системного анализа в интересах обеспечения энергетической безопасности. Ниже приведены возможные способы по декомпозиции и интеграции моделируемых систем при решении задач системного анализа для различных мета-уровней (например, на уровне государства в целом, федерального округа, макрорегиона государства или отдельно взятого субъекта энергетической безопасности).

Способ 1. Мониторинг состояния энергетической безопасности ориентирован по своей сути на систематический сбор и анализ информации от различных источников, связанных с энергетикой (например, от энергетического оборудования). Дополнительно из других источников может быть использована общедоступная информация по политическим, экономическим, научно-технологическим, социальным аспектам, а также по принятому регламенту функционирования объектов ТЭК. Тем самым для каждого мета-уровня обеспечен сбор информации, способствующей объективной характеристике приемлемости или неприемлемости состояния энергетической безопасности по тому или иному показателю (см. также пример универсальной вспомогательной модели показателя – УВМП в разделе 2).

Способ 2. В качестве логической основы системного понимания структурно сложных моделируемых систем применимы «логические деревья», имеющие корень дерева (0-й ярус) и связанные с корнем вершины последующих ярусов (1-го, 2-го и т.д.), характеризующие различные сущности. Последний ярус представляет собой характеристики угроз для моделирования, определяемые по используемым исходным данным. Тем самым обеспечена двунаправленная прослеживаемость цепочки логических умозаключений от корня к конкретной вершине и обратно. А при установлении взаимосвязей разнородных вершин одного яруса и логической интерпретации этих взаимосвязей возможна логическая интерпретация результатов решения задач системного анализа и выработки упреждающих мер применительно ко всему «логическому дереву» в целом. Например, для макрорегиона, рассматриваемого в качестве моделируемой системы, корнем дерева может выступать сам макрорегион (0-й ярус), а в качестве вершин 1-го яруса – субъекты энергетической безопасности этого региона.

Для этих двух уровней логическая интерпретация может быть такова: энергетическая безопасность макрорегиона обеспечена, если обеспечена энергетическая безопасность каждого из субъектов энергетической безопасности этого региона. В основу такого логического описания архитектуры «логического дерева» положены базовые

принципы ГОСТ Р 57100-2025 «Системная и программная инженерия. Описание архитектуры».

Способ 3. Используя способы 1 и 2, с учетом основных направлений деятельности по обеспечению энергетической безопасности «логическое дерево» применительно к конкретному федеральному округу может быть сформировано следующим образом. В качестве корня дерева (0-й ярус) выступает сам федеральный округ, а характеристики угроз, используемые в качестве исходных данных при моделировании и расчетах критериев, образуют вершины последнего яруса дерева - см. рисунок 5.4. Эти последние вершины могут быть представлены с помощью УВМП.

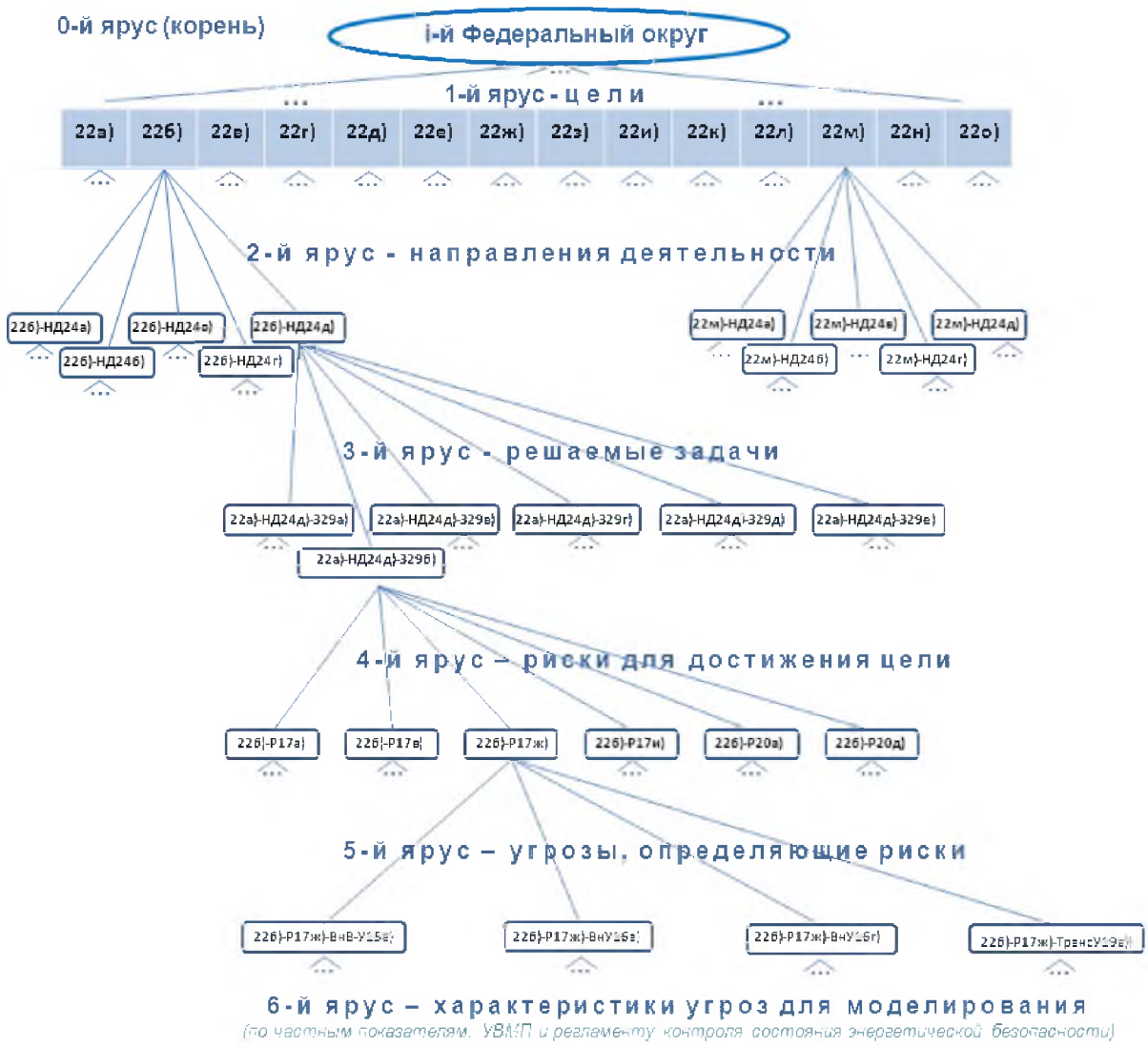


Рис. 5.4 «Логическое дерево» для описания связи «цели – направления деятельности – решаемые задачи – риски – угрозы – характеристики угроз»

Применительно к 0-му ярусу – корню (т. е. применительно к рассматриваемому федеральному округу) выбирают соответствующие цели 22а)–22о) Доктрины. Они образуют 1-й ярус дерева, т.е. каждая цель 22а)–22о) Доктрины – это вершина 1-го яруса. Всего для условно *i*-го федерального округа государства максимально может быть 14 вершин 1-го яруса: *i*.1-я вершина обозначена 22а), *i*.14-я вершина – обозначена 22о). Для описания связи «цели – направления деятельности – решаемые задачи – риски – угрозы – характеристики угроз» в качестве вершин 2-го яруса могут рассматриваться направления деятельности для достижения цели, 3-го яруса – решаемые задачи в рамках направления деятельности, на 4-м ярусе – риски для достижения целей путем решения конкретных задач, на 5-м ярусе – угрозы, определяющие эти риски, на 6-м ярусе – характеристики угроз для моделирования.

Например, каждое направление по п.24а)–24д) Доктрины образует вершину 2-го яруса, всего – 5 вершин 2-го яруса. Так, на рисунке 5.3 от *i*.2-й вершины 1-го яруса идут ветви к вершинам 2-го яруса, тогда соответствующие вершины 2-го яруса обозначаются от 22б)-НД24а) до 22б)-НД24д), а для *i*.12-й вершины 1-го яруса – соответственно от 22м)-НД24а) до 22м)-НД24д).

Решаемые задачи для каждого из направлений деятельности образуют 3-й ярус дерева, т.е. каждая задача по пп. 25–29 Доктрины – это вершины 3-го яруса. Таким образом, для направления деятельности 24а) Доктрины может быть до 13 вершин 3-го яруса. На ветвях от первой вершины 2-го яруса 22а)-НД24а) (такое обозначение для вершины 2-го яруса означает цель, связанную с воспроизводством минерально-сырьевой базы ТЭК согласно п. 22а) Доктрины и направление деятельности «совершенствование государственного управления в области обеспечения энергетической безопасности» согласно п. 24а) Доктрины) образуются вершины 3-го яруса. В частности, первая вершина будет означать первую решаемую задачу – «а) совершенствование нормативно-правовой базы по вопросам обеспечения безопасного, надежного и устойчивого функционирования инфраструктуры и объектов энергетики» согласно п. 25а) Доктрины, эта вершина будет обозначаться 22а)-НД24а)-З25а), а 13-я вершина 3-го яруса, относящаяся к задаче «н) стимулирование энергосбережения и повышения энергетической эффективности экономики» по п.25н) Доктрины будет обозначаться 22а)-НД24а)-З25н). Для 5-го направления деятельности 24д) Доктрины всего будет до 6 вершин 3-го яруса. Тогда для этого направления деятельности 1-я вершина яруса обозначается 22а)-НД24д)-З29а), а 6-я вершина, относящаяся к задаче по п.29е) Доктрины, будет обозначаться 22а)-НД24д)-З29е).

Таким образом, способ 3 описывает «логические деревья», образуемые из вербального описания области приложения СУР для формализации постановок задач

системной инженерии и последующего понимания результатов применения структурно сложных моделируемых систем при их решении.

УВМП позволяет сформировать унифицированное пространство элементарных состояний - «Приемлемое» (с выделением для упреждения состояния «Приемлемое с отклонением») и «Неприемлемое» для «логического дерева», а также универсальный механизм использования данных мониторинга для формирования исходных данных при прогнозировании рисков в СУР. Используя доступные временные данные регламента и системной диагностики $T_{меж}$ и $T_{диаг}$, в итоге получаются сформированными исходные данные для применения базовых моделей .

Результаты моделирования также подлежат интерпретации. Например, в цепочке «цели – направления деятельности – решаемые задачи – риски – угрозы – характеристики угроз» для поддержки принятия решений по выработке рациональных упреждающих мер противодействия угрозам с использованием фрагмента «логического дерева» в части рисков, относящихся к цели 22б), направлению деятельности 22б)-НД24д), решаемой задаче 22а)-НД24д)-329б) интегральный риск недостижения цели может быть интерпретирован следующим образом (см. рисунок 5.5).

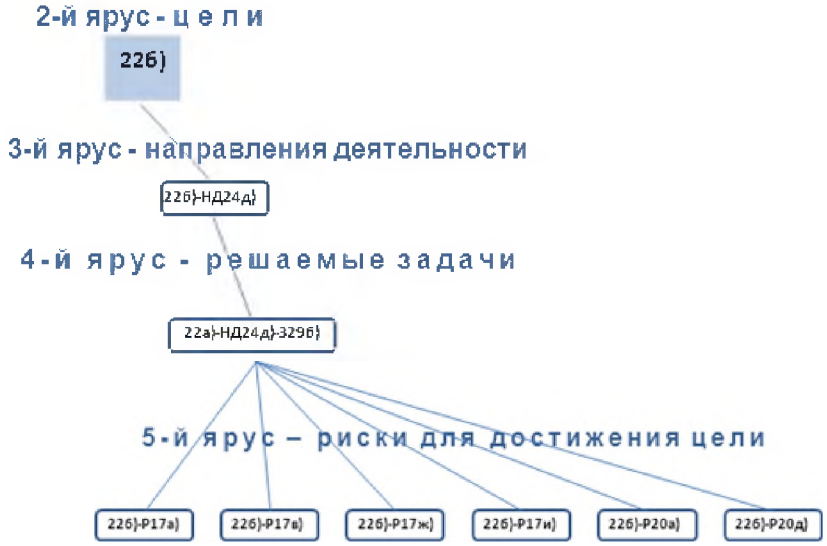


Рис. 5.5 Фрагмент, когда интегральный риск на уровне цели определяется составными рисками в рамках направления деятельности и решаемой задачи

Интерпретация: надежное и устойчивое обеспечение российских потребителей энергоресурсами стандартного качества и услугами в сфере энергетики в течение задаваемого периода прогноза при решении задачи развития отечественного научно-технологического потенциала, создания и освоения передовых технологий в сфере энергетики, в том числе технологий использования возобновляемых источников энергии, наращивание производства на территории государства конкурентоспособного основного и

вспомогательного оборудования, создание центров компетенций (см. 22а)-НД24д)-З29б)) в рамках направления деятельности по обеспечению технологической независимости ТЭК и повышения его конкурентоспособности (см. 22б)-НД24д)) окажется в состоянии «Неприемлемое», если в течение этого срока превысят допустимый уровень:

ИЛИ риск несогласованного развития отраслей ТЭК и видов деятельности в сфере энергетики, включая экспорт продукции и услуг организаций ТЭК, в условиях ограниченного государственного контроля и регулирования (см. 22б)-Р17а)),

ИЛИ риск низкой эффективности осуществляемых субъектами энергетической безопасности мер по поддержанию финансовой устойчивости организаций ТЭК при наступлении неблагоприятных условий, таких как рост неплатежей за поставленные организациями ТЭК энергоресурсы и оказанные ими услуги, увеличение транспортных расходов и капитальных затрат таких организаций при освоении нефтегазовых месторождений, находящихся в удаленных местностях, усложнение компонентного состава нефтегазовых месторождений (см. 22б)-Р17в)),

ИЛИ риск высокого уровня износа основных производственных фондов организаций ТЭК, низкая эффективность использования и недостаточные темпы обновления этих фондов (см. 22б)-Р17ж)),

ИЛИ риск недостаточных темпов реагирования системы профессионального образования на изменение потребности организаций ТЭК в квалифицированных кадрах (см. 22б)-Р17и));

ИЛИ риск несоответствия технологического уровня российских организаций ТЭК современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков (см. 22б)-Р20а));

ИЛИ риск недостаточного уровня защищенности инфраструктуры и объектов ТЭК от актов незаконного вмешательства и опасных природных явлений (см. 22б)-Р20д)).

В ином случае по указанной цели, направлению деятельности и решаемой задаче энергетическая безопасность в течение задаваемого периода прогноза будет находиться в состоянии «Приемлемое» или «Приемлемое с отклонением» с непревышением допустимых рисков.

Далее с использованием разработанных математических, программных, технологических и методических решений для ВС и КС становится возможным осуществление расчетов рисков для сложных структур и учет различных требований и условий (например, требований по защите информации). Сбалансированное упреждающее управление процессами возникновения, развития, контроля и нейтрализации возможных

угроз осуществляется как результат решения формально постановленных задач системного анализа путем целенаправленного использования моделей и выбранных критериев при соответствующих ограничениях.

Итогом завершения логического преобразования изначального вербального описания системы является вид формализации, представленный на рисунках 5.2 — 5.5 в обозначениях, приведенных в таблицах 5.1 — 5.3. Этот вид позволяет осуществить формальные постановки практических задач системного анализа энергетической безопасности, используя предложенных в диссертации математических, программных, технологических и методических решений для ВС и КС. Так, с использованием информации, собираемой и обрабатываемой в СУР могут быть формально поставлены и решены практические задачи:

- минимизации риска нарушения надежности обеспечения энергетической безопасности макрорегиона государства или отдельно взятого субъекта энергетической безопасности в ТЭК при ограничениях на отдельные допустимые риски реализации критичных угроз (для конкретных объектов и процессов), ресурсы и общие затраты на реализацию планов и при иных ограничениях;

- минимизации общих затрат на реализацию кратко-, средне- и/или долгосрочных планов при ограничениях на допустимый риск надежности обеспечения энергетической безопасности макрорегиона государства или отдельно взятого субъекта энергетической безопасности в ТЭК, на отдельные допустимые риски реализации критичных угроз (для конкретных объектов и процессов), ресурсы и при иных ограничениях;

- комбинации перечисленных выше или иных оптимизационных задач применительно к макрорегиону или отдельно взятому субъекту энергетической безопасности в ТЭК.

Результаты решения этих задач рекомендуются к использованию для обеспечения баланса по критерию «эффективность – стоимость» при кратко-, средне- и/или долгосрочном планировании на уровне макрорегиона государства или отдельно взятого субъекта энергетической безопасности. Далее в подразделах 5.2 – 5.6 разрабатываются рекомендации по использованию возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии в части определения исходных данных, формирования сценариев, моделирования и обоснования рекомендаций при решении задач системной инженерии – см. рис. 5.6 (за исключением закрашенного серым цветом).

Рис. 5.6 Демонстрация возможностей применения созданного прототипа в части определения исходных данных, формирования сценариев, моделирования и обоснования рекомендаций по решению задач – см. подразделы 5.2-5.6

5.2 Рекомендации по прогнозированию рисков по данным цифрового двойника промышленного объекта, сопровождаемого в процессе эксплуатации [156, 159]

В качестве другой области приложения разработанных программных, технологических и методических решений для ВС и КС в настоящем подразделе выступает цифровой двойник промышленного объекта, сопровождаемый в процессе эксплуатации трубопроводной сети. Под цифровым двойником промышленного объекта понимается виртуальная компьютерная модель этого объекта, воспроизводящая в цифровом виде состояние изменяемых критичных сущностей объекта, измеряемых во время эксплуатации. Сопровождение цифрового двойника заключается в актуализации данных реального состояния эксплуатируемого объекта с целью прогнозирования рисков и упреждающего противодействия угрозам безопасности.

Предложенные в разделах 2, 3, 4 программные, технологические и методические решения для ВС и КС позволяют в упреждающем режиме по единой вероятностной шкале количественно спрогнозировать и сравнить эффективность противодействия различным угрозам с соответствующей интерпретацией. Рассмотрим появившиеся аналитические возможности на конкретном примере сопровождаемого цифрового двойника промышленного объекта. Без принципиального ограничения общности в качестве промышленного объекта, сопровождаемого в процессе эксплуатации, рассматривается определенное множество критичных фрагментов магистральной трубопроводной сети. Пример цифрового двойника фрагмента магистральной трубы представлен на рис. 5.7, в

каждой точке – данные, в т.ч. привязанные ко времени измерения и сравнения с нормативными границами (например, по УВМП).

Рис. 5.7 Пример цифрового двойника фрагмента магистральной трубы

В приложении к фрагменту магистральной трубопроводной сети цифровой двойник описывает: характеристики фрагмента трубы (диаметр, толщину, проектное давление, покрытие, внутритрубное устройство и др.), проектную и рабочую документацию на строительство трубопроводной сети с привязкой ко времени, характеристики среды эксплуатации (месторасположение, характеристики местности, например – болото, переходы через водные преграды, автомобильные и железнодорожные пути и др.). Т.е. цифровые двойники фрагментов магистральных трубопроводных сетей, накапливающие исходные данные для прогнозирования рисков, по сути представляют собой моделируемые системы, позволяющие судить о состоянии реальных систем и подлежащие прагматичному использованию в интересах бизнеса.

Требуется разработать рекомендации по системному обоснованию технических мер, востребуемых по итогам регулярного диагностирования объекта для обеспечения и повышения безопасности его эксплуатации в условиях природных, технических, экономических и иных ограничений.

Для демонстрации работоспособности типовой методики прогнозирования рисков нарушения целостности сложной моделируемой системы (см подраздел 4.4) предлагается использовать усовершенствованные базовые вероятностные модели методы из раздела 2, они отражены в авторских работах [5, 167 и др.], а также см. ГОСТ Р 59991–2022 «Системная инженерия. Системный анализ процесса управления рисками для системы», в котором эти модели и методы рекомендованы.

Необходимыми исходными данными для прогнозирования рисков с использованием предложенных базовых моделей являются:

логическая структура моделируемой системы для анализа (выделяются критичные фрагменты);

по каждому составному фрагменту: частота возникновения угроз; среднее время развития угроз; период между диагностиками; длительность диагностики; среднее время восстановления целостности (т.е. те исходные данные, которые необходимы для применения усовершенствованных базовых моделей раздела 2).

Положим, по результатам внутритрубного диагностирования выделены критичные фрагменты:

на 1-м и 4-м фрагментах обнаружена зона продольных трещин, определен ремонт путем замены трубы;

на 2-м и 3-м фрагментах обнаружена язвенная коррозия, определен ремонт заменой катушки;

на 5-м и 6-м фрагментах, располагаемых в болотистой местности, выявлены продольные канавки и обширная коррозия с эквивалентом потери металла до 30%;

на 7-м фрагменте выявлен корррозионный износ глубиной более 10%.

Эти данные учтены при определении частота возникновения и среднего времени развития угроз.

Тем самым для прогнозирования рисков сформирована логическая структура сопровождаемого цифрового двойника в виде последовательно объединяемых 7 элементов исследуемой системы, т.е. семи фрагментов магистральной трубопроводной сети. Интерпретация такова – все множество фрагментов трубопроводной сети из 7 перечисленных фрагментов считается находящимся в состоянии целостности в течение заданного периода прогноза, если каждый из составных фрагментов в течение этого периода прогноза находится в состоянии целостности.

Исходя из производственных возможностей для всех фрагментов период между диагностиками равен 4 годам, длительность диагностики – 1 неделя, среднее время восстановления целостности – 1 месяц. Различающиеся для прогнозирования исходные данные по каждому из 7 элементов, определенные с учетом природных особенностей месторасположения фрагментов, сведены в Таблицу 5.4. Этих исходных данных достаточно для прогнозирования рисков.

Главный прогноз делается на 5 лет, полагая, что после каждой диагностики должны приниматься принципиальные решения по восстановлению требуемого уровня безопасности трубопроводной сети в условиях природных угроз. При этом оценивается интегральный риск нарушения целостности в зависимости от изменения исходных данных

диапазоне -50%+100% от задаваемых при моделировании. Вспомогательный прогноз для сравнения делается на 2 года.

Таблица 5.4 Исходные данные для прогнозирования рисков

Параметр	По фрагментам 1, 7	По фрагментам 2,3	По фрагментам 4,6	По фрагменту 5
Частота возникновения угроз	1 раз в 15 лет	1 раз в 8 лет	1 раз в 5 лет	1 раз в 5 лет
Среднее время развития угроз	5 лет	4 года	4 года	3 года

Допустимый уровень риска согласно требованиям ГОСТ Р 55999-2014, ГОСТ Р 59991-2022 полагается не выше 0.1, что соответствует вероятности успешного функционирования трубопроводной сети не ниже 0.9. Результаты прогнозирования рисков на уровне зависимости функции распределения времени нарушения целостности сопровождаемого цифрового двойника множества фрагментов магистральной трубопроводной сети показали следующее.

Риск нарушения целостности для всей моделируемой системы из 7 критичных фрагментов в течение 5 лет составит 0.77. Это означает, что вероятность успешного функционирования системы в течение 5 лет (0.23) более, чем в 3.3 раза ниже, чем риск реального нарушения на каком-либо из фрагментов.

Зависимость интегрального риска от периода прогноза приведен на рис. 5.8, 5.9. Анализ зависимости показывает, что лишь для прогнозного периода 1 год интегральный риск составит около 0.1 (на рис. 5.9).

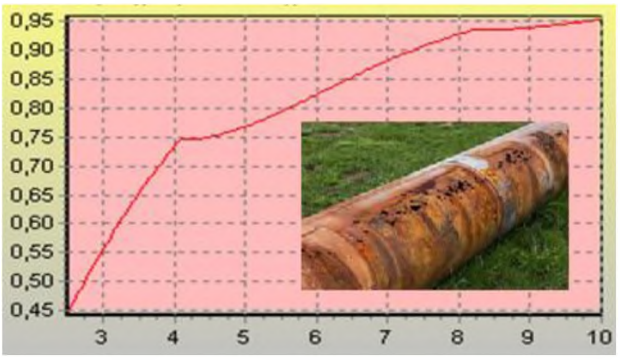


Рис. 5.8 Зависимость интегрального риска от периода прогноза, изменяемого в диапазоне от 2.5 до 10 лет

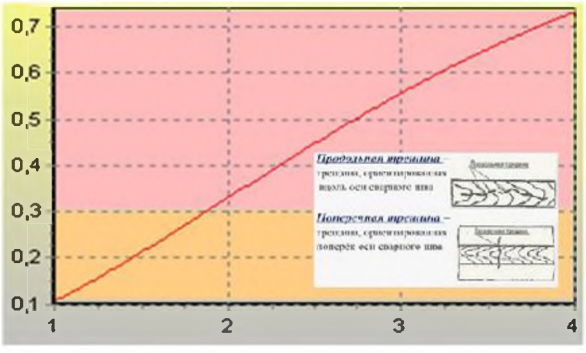


Рис. 5.9 Зависимость интегрального риска от периода прогноза, изменяемого в диапазоне от 1 года до 4-х лет

Анализ обобщенных результатов прогнозирования рисков при прогнозе на 5 лет позволил сделать следующие выводы: к зоне допустимого риска относятся фрагменты 1, 7; к зоне недопустимого риска относятся вся система в целом и фрагменты 2-6; наивысший риск, равный 0.3, относится к фрагменту 5, этот риск на 20% выше риска для фрагментов 4,

6. Это объясняется меньшим временем активизации угроз из-за корррозионного износа и корррозионно-агрессивных условий ее расположения (3 года вместо 4-х лет для соседних труб). Анализ обобщенных результатов прогнозирования рисков при прогнозе на 2 года позволил установить: к зоне допустимого риска (не выше 0.1) относятся все фрагменты; к зоне недопустимого риска относится вся система в целом (риск=0.33); наивысший риск, равный 0.09, по-прежнему относится к фрагменту 5. При этом приблизительное среднее время наработки на нарушение целостности для фрагмента 5 составит 13.08 года.

Детальный анализ чувствительности интегрального риска к изменению исходных характеристик фрагмента 5, использованных при моделировании, можно проследить по зависимостям, отраженным на рис. 5.10 – 5.11. На рис. 5.10, 5.11 при прогнозе соответственно на 5 лет и 2 года в зависимости от «частоты возникновения угроз» от 0.1 до 0.4 раз в год (от 1 до 4-х раз в 10 лет) при заданном 1 раз в 5 лет в таблице 5.4.

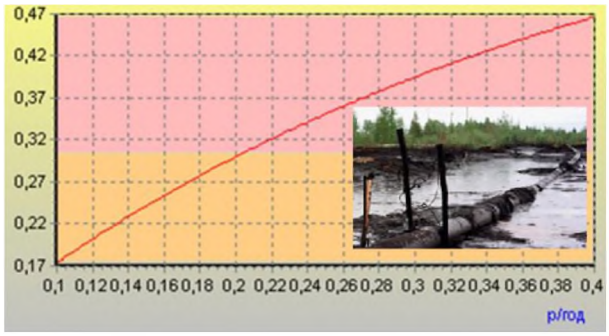


Рис. 5.10 Зависимость риска нарушения целостности от «частоты возникновения угроз» для фрагмента 5 при прогнозе на 5 лет

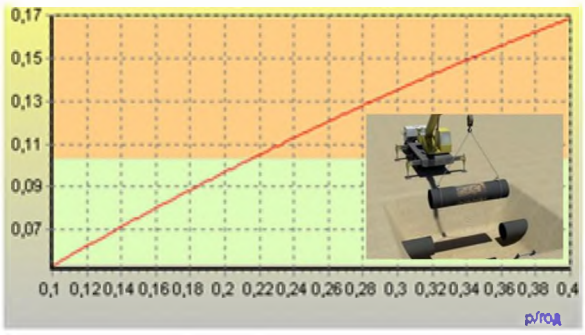


Рис. 5.11 Зависимость риска нарушения целостности от «частоты возникновения угроз» для фрагмента 5 при прогнозе на 2 года

На рис. 5.12, 5.13 при прогнозе соответственно на 5 лет и 2 года в зависимости от «среднего времени развития угроз» от полутора до 6 лет при заданных «3 года» в таблице 5.4.

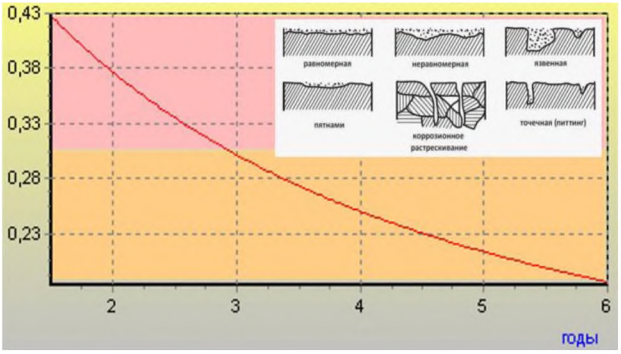


Рис. 5.12 Зависимость риска нарушения целостности от «среднего времени развития угроз» для фрагмента 5 при прогнозе на 5 лет

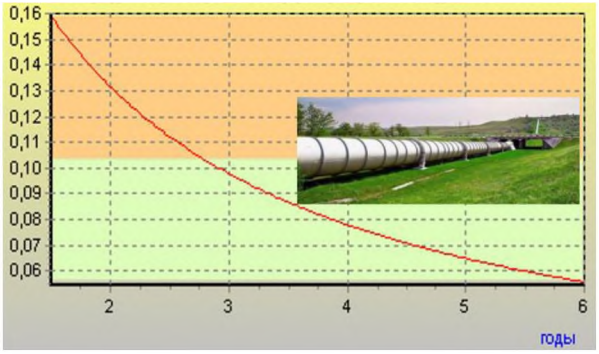


Рис. 5.13 Зависимость риска нарушения целостности от «среднего времени развития угроз» для фрагмента 5 при прогнозе на 2 года

Анализ детальных результатов прогнозных расчетов показывает обоснованность следующих рекомендаций в области противодействия угрозам, в т.ч. в условиях коррозионной агрессивности грунтов.

Чтобы не превышать риск 0.1 (т.е. обеспечивать успешность эксплуатации фрагмента трубопровода с вероятностью выше 0.9), необходимо:

- после 20 лет эксплуатации, при выявлении аномалий и эксплуатации в каррозионно-агрессивных условиях осуществлять внутритрубное диагностирование необходимо не через 4 года, а каждые 2 года;

- для ликвидации аномалий необходимо применять такие меры, которые гарантированно обеспечивают противодействие негативным природным воздействиям на срок не менее 3-х лет;

- для поддержки принятия управленческих решений вероятностные прогнозы осуществлять на срок, соизмеримый не только с долгосрочными планами (5-10 лет), но и со среднесрочными планами (2-4 года), а для этих прогнозных сроков при выявлении рисков, количественно превышающих допустимый уровень, осуществлять вероятностное прогнозирование рисков на период до 1 года для текущего планирования и упреждающего противодействия угрозам.

Эти рекомендации, полученные в результате вероятностного прогнозирования рисков сопровождаемого цифрового двойника фрагментов магистральной трубопроводной сети, служат аналитическим дополнением к техническим мерам, востребуемым по итогам регулярного внутритрубного диагностирования реальных сетей. Важно подчеркнуть, что за счет использования возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии проведение расчетов можно осуществлять не только за автоматизированным рабочим местом ВС в стационарных условиях, но и в полевых условиях, где возможно подключение к компьютерной сети.

Таким образом в подразделе разработаны рекомендации по применению предложенных в работе программных, технологических и методических решений для ВС и КС в приложении к сопровождаемым цифровым двойникам (на примере фрагментов магистральной трубопроводной сети). Предлагаемые рекомендации позволяют обеспечить удовлетворение важной аналитической потребности. А именно: применение созданного прототипа обеспечивает прослеживаемость и аналитическую зависимость прогнозных рисков от влияющих факторов. Это открывает важные прагматические возможности для системного обоснования и дополнения технических мер по итогам регулярного диагностирования объекта и способствует повышению безопасности его эксплуатации в условиях природных, технических, экономических и иных ограничений.

5.3 Рекомендации по моделированию многомодального взаимодействия социокиберфизических систем в жизненном цикле обогатительной фабрики в угольной отрасли [5, 167]

Согласно ГОСТ Р 71531-2024 под киберфизической системой понимается интеллектуальная система, включающая в себя спроектированные взаимодействующие сети физических и вычислительных компонентов. Соответственно добавление «социо» подразумевает дополнительное вовлечение в киберфизическую систему человека и общества, что для современных угольных предприятий уже стало вполне естественным.

Предложенная в 4.4 типовая методика прогнозирования рисков нарушения целостности сложной моделируемой системы в полной мере применима для сравнения различных вариантов, поиска улучшений и упреждающего управления рисками в жизненном цикле системы. Рассмотрим эти возможности на примере обогатительной фабрики (ОФ) в угольной отрасли, которая будет выступать в качестве исследуемой моделируемой системы. При этом многомодальность взаимодействия социокиберфизических систем в жизненном цикле ОФ проявляется при моделировании в значениях исходных данных. Так, в сравнении с взаимодействием «человек - человек» взаимодействия «машина - человек» и «машина – машина» способствуют увеличению времени развития угроз (за счет сокращения времени ввода и доведения информации), дисциплинирует периодическую диагностику и способствуют снижению длительности диагностики в результате использования средств автоматизации, мобильных средств связи, робототехники. Это учитывается при формировании исходных данных для моделирования. Многомодальность применительно к созданному прототипу технологии поддержки риск-ориентированной системной инженерии предполагает возможность использования исходных данных для моделирования через различные каналы (от телеметрических датчиков, из базы данных или отчетных Excel-форм организации, путем ввода данных с клавиатуры), а также в различной аналитической форме для дальнейшего использования (см. раздел 3).

Положим, на обогатительной фабрике возникла потребность в существенном усовершенствовании системы вентиляции, аспирации и пылеподавления (иными словами – потребность в перевооружении ОФ). Суть усовершенствования системы состоит в следующем. В зданиях и сооружениях обогатительной фабрики предусматриваются к установке системы приточно-вытяжной вентиляции с механическим и естественных побуждением. Для уменьшения пылевыделения предусматриваются пылезащитные укрытия мест перегрузки с устройством местных отсосов, отвода и очистки удаляемого

воздуха (аспирационные системы). В качестве пылеуловителей предусматриваются к установке мокрые пылеуловители, пылеулавливающие рециркуляционные аппараты. В надбункерных помещениях предусматриваются к установке системы метановытяжки, действующие во всё время пребывания угля в бункерах. Помимо вытяжной вентиляции предусматривается аварийная вентиляция, сблокированная с датчиками газоанализаторов и обеспечивающая восьмикратный воздухообмен (в соответствии с требованиями промышленной безопасности). В подземных и плохо проветриваемых помещениях, кроме того, предусматриваются к установке вытяжные вентиляционные системы. Компенсация вытяжного воздуха обеспечивается приточными установками, подающими наружный воздух, очищенный от пыли и подогретый в зимнее время. Размещение приточных установок предусмотрено в изолированных помещениях. Предусмотрено совершенствование системы автоматизации, внедрение системы дистанционного контроля (СДК) и блокировки вентиляционных систем. Угрозы нарушения промышленной безопасности могут возникать во всех перечисленных местах.

Для эффективного проведения работ по усовершенствованию системы вентиляции, аспирации и пылеподавления требуется решение следующих аналитических задач системной инженерии:

- задача 1-5.3 - провести сравнительный анализ эффективности системы вентиляции, аспирации и пылеподавления до и после усовершенствования ОФ;

- задача 2-5.3 – обосновать рекомендации по всесторонним улучшениям и осуществить упреждающее управление различными рисками и интегральным системным риском.

С применением «Типовой методики прогнозирования рисков нарушения целостности сложной моделируемой системы» (см. 4.4) рекомендуется следующий вариант аналитического решения задач.

Для формирования типовых исходных данных, необходимых для сравнительного анализа с использованием методики, в качестве составных исследуемых подсистем обогатительной фабрики выделены:

1) множество подсистем, характеризуемых совокупно (с дифференциацией по моделируемым сущностям): подсистема в погрузочных бункерах; подсистема в аккумулирующих бункерах; подсистема в головном столбе; подсистема в промежуточном столбе; подсистема в породных погрузочных бункерах; подсистема в промежуточном бункере;

2) обогащающая подсистема;

3) подсистема в галерее.

В качестве моделируемых рассматриваются сущности в каждой из исследуемых подсистем: человеческие факторы (с учетом возможностей многомодального взаимодействия различных социокиберфизических систем, используемых должностными лицами); факторы, определяемые состоянием основных фондов; организационно-производственные факторы и факторы, не зависящие от производственной деятельности (с учетом иных социокиберфизических систем, используемых внепроизводственной деятельности, например, в семьях должностных лиц, но способных стать источником возможных угроз и временных характеристик угроз).

Исследуемые подсистемы и моделируемые сущности до (в существующей системе) и после совершенствования (в системе после ее перевооружения) характеризуются исходными данными, описываемыми частотно-временными и иными характеристиками, отраженными в таблице 5.5.

Таблица 5.5 Общие характеристики угроз для существующей и ожидаемой усовершенствованной системы вентиляции, аспирации и пылеподавления (при различиях – через дробь: существующий вариант/после усовершенствования)

Исследуемые подсистемы	Угрозы, дестабилизирующие факторы, моделируемые сущности	Частота возник-новения угроз	Среднее время развития угроз	Период между контро-лями	Длитель-ность контроля (диагно-стики)	Длитель-ность восста-новления
1) Множество подсистем: - Подсистема в погрузочных бункерах - Подсистема в аккумулирующих бункерах - Подсистема в головном столбе - Подсистема в промежуточном столбе - Подсистема в породных погрузочных бункерах - Подсистема в промежуточном бункере	1. Человеческие факторы	6 р/год	1 нед	8 часов	1 час	1 час
	2. Факторы, определяемые состоянием основных фондов	6 р/мес / 6 р/год (за счет усоверш.)	1 мес	1 час / 10 мин. (за счет усоверш.)	1 час / 10 мин. (за счет усоверш.)	2 часа / 30 мин. (за счет усоверш.)
	3. Организационно-производственные факторы и факторы, не зависящие от производственной деятельности	6 р/год	2 мес	1 сут	1 час	1 час
2) Обогащающая подсистема	4. Человеческие факторы	1 р/год	1 нед	8 часов	1 час	1 час
	5. Факторы, определяемые состоянием основных фондов	1р/мес / 1р/год (за счет усоверш.)	1 мес	1 час / 10 мин. (за счет усоверш.)	1 час / 10 мин. (за счет усоверш.)	1 час / 30 мин. (за счет усоверш.)
	6. Организационно-производственные факторы и факторы, не зависящие от производственной деятельности	1 р/год	2 мес	1сут	1 час	1 час

3) Подсистема в галерее	7. Человеческие факторы	1 р/мес	1 нед	8 часов	1 час	1 час
	8. Факторы, определяемые состоянием основных фондов	1р/мес / 1р/год (за счет усоверш.)	1 мес	1 час / 10 мин. (за счет усоверш.)	1 час / 10 мин. (за счет усоверш.)	1 час / 30 мин. (за счет усоверш.)
	9. Организационно-производственные факторы и факторы, не зависящие от производственной деятельности	1 р/год	2 мес	1 сут	1 час	1 час

Структура исследуемой сложной системы – последовательное соединение элементов 1, 2, …, 9 из 2-й графы таблицы 5.5, логически объединяемых союзом «И» - 

.

Основные отличия в значениях по элементам заключаются:

- в частоте возникновения угроз, при этом за счет усовершенствований (перевооружения) частота возникновения угроз для факторов, определяемых состоянием основных фондов, снижается на порядок;

- в периоде между контролями и средней длительности контроля, где за счет внедрения СДК эти времена сокращаются в 6 раз - с одного часа до 10 минут;

- в средней длительности восстановления нарушаемой целостности в 2-4 раза - до 30 минут.

В качестве критичных показателей рассматриваются риск критичного нарушения целостности состояния системы вентиляции, аспирации и пылеподавления и среднего времени до нарушения целостности анализируемых сущностей (т.е. такого среднего времени нахождения всей совокупности и каждой из сущностей в состоянии, при котором обеспечивается достижение целей их функционирования). Затраты используются в качестве ограничений.

Для задачи 1-5.3 (сравнительный анализ эффективности системы до и после усовершенствования) результаты прогнозирования существующего риска критичного нарушения целостности состояния системы вентиляции, аспирации и пылеподавления и анализируемых сущностей за год, среднее ожидаемое время до нарушения целостности сущностей, а также зависимость интегрального риска от длительности прогнозного периода от полугода до 2-х лет отражены на рис. 5.14 – 5.16 (до перевооружения).

Рис. 5.14 Риск критичного нарушения целостности за год для каждой из сущностей (от 1-й по 9-ю) и всей совокупности сущностей (1..9) до перевооружения

Рис. 5.15 Среднее время до нарушения целостности каждой из сущностей (от 1-й по 9-ю) и всей совокупности сущностей (1..9) до перевооружения

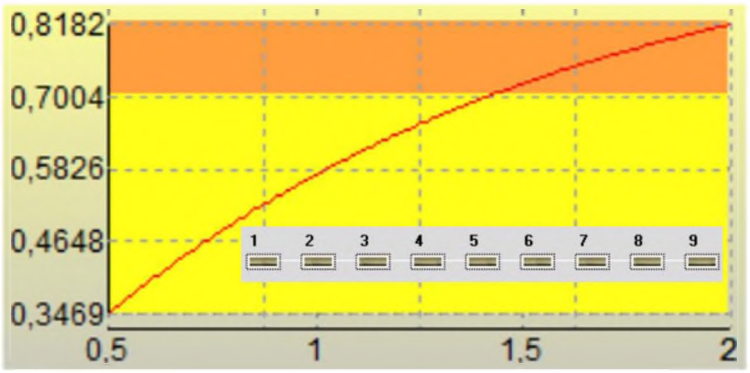


Рис. 5.16 Зависимость интегрального риска от длительности прогнозного периода от 0.5 года до 2-х лет для системы до перевооружения

Анализ расчетных результатов показал следующее.

Риск критичного нарушения целостности подсистем в погрузочных бункерах, аккумулирующих бункерах, головном и промежуточном столбах, в породных погрузочных бункерах и промежуточном бункере в течение года составит для моделирующих сущностей: 0.146 для человеческих факторов (1), 0.130 для факторов, определяемых состоянием основных фондов (2), 0.049 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности (3). Риск критичного нарушения целостности обогащающей подсистемы составит 0.026 для человеческих факторов (4), 0.071 для факторов, определяемых состоянием основных фондов (5), 0.008 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности (6). Наконец, риск критичного нарушения целостности подсистемы в галерее составит 0.270 для человеческих факторов (7), 0.071 для факторов, определяемые состоянием основных фондов (8), 0.008 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности (9) – см. рис. 4.39. Выделяется значение риска в 3) - галерее (0.270), это объясняется

сравнительно высокой частотой возникновения угроз со стороны человеческого фактора, частота = 1 раз в месяц, относительно частоты 1 раза в 2 месяца для 1) множества подсистем, где риск составляет 0.146 (т.е. риск ниже в 1.85 раза), а также относительно частоты 2 раз в год для 2) - обогащающей подсистемы, где риск составляет 0.026 (т.е. в 10.38 раз ниже риска, свойственного для галереи).

Примечание. Отметим, что значения расчетных рисков совпадают для показателей 5 и 8 (0.071) и показателей 6 и 9 (0.008), т.к. совпадают исходные данные для расчетов.

При этом, несмотря на то, что среднее время до нарушения целостности всей совокупности сущностей (1..9) составляет около 11.1 года (см. рис. 5.15), интегральный риск нарушения целостности всей системы вентиляции, аспирации и пылеподавления за год составит 0.574. Это говорит о том, что в течение года скорее нужно ожидать негативное воздействие исследованных дестабилизирующих факторов, нежели отсутствие их опасного проявления. В свою очередь за 2 года интегральный риск превысит 0.81, что свидетельствует о практической неизбежности аварий в системе вентиляции, аспирации и пылеподавления. Наиболее «узкое место» - человеческий фактор в галерее ОФ.

Подчеркнем – вышеизложенные результаты исследований характеризуют нынешнее состояние дел для существующей системы вентиляции, аспирации и пылеподавления ОФ.

Далее рассмотрим возможные риски после запланированных улучшений (перевооружения) системы вентиляции, аспирации и пылеподавления ОФ, исходные данные для прогнозирования рисков отражены в табл. 5.5 (под дробью).

Результаты прогнозирования существующего риска критичного нарушения целостности состояния системы вентиляции, аспирации и пылеподавления и анализируемых сущностей за год, среднее ожидаемое время до нарушения целостности сущностей, а также зависимость интегрального риска от длительности прогнозного периода от полугода до 2-х лет отражены на рис. 5.17 – 5.19 (после перевооружения).

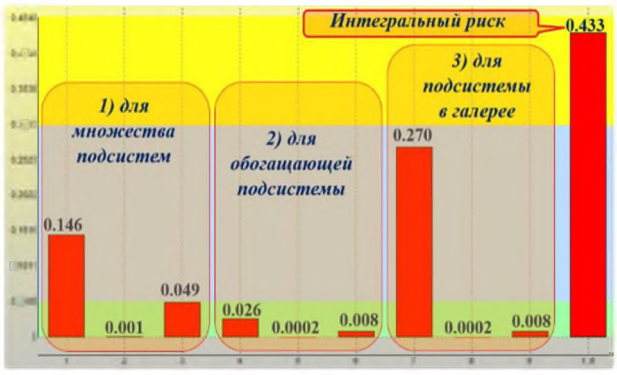


Рис. 5.17 Риск критичного нарушения целостности за год для каждой из сущностей (от 1-й по 9-ю) и всей совокупности сущностей (1..9) после перевооружения

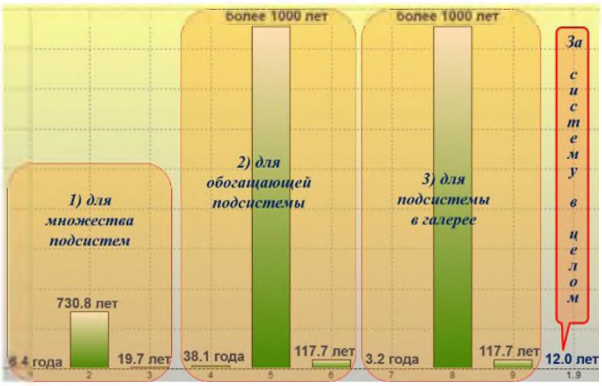


Рис. 5.18 Среднее время до нарушения целостности каждой из сущностей (от 1-й по 9-ю) и всей совокупности сущностей (1..9) после перевооружения

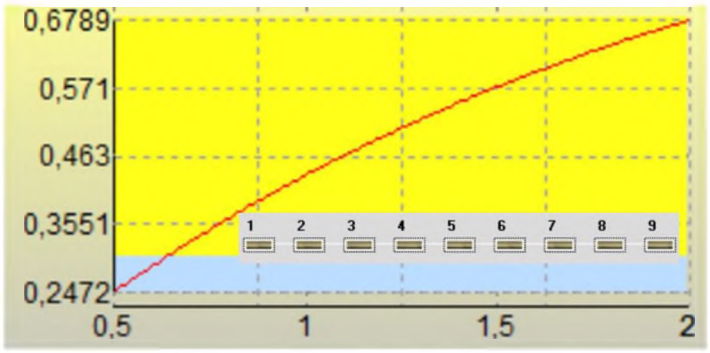


Рис. 5.19 Зависимость интегрального риска от длительности прогнозного периода от 0.5 года до 2-х лет для системы после перевооружения

Анализ расчетных результатов для системы вентиляции, аспирации и пылеподавления после ее усовершенствования (перевооружения) показал следующее.

Риск критичного нарушения целостности подсистем в погрузочных бункерах, аккумулирующих бункерах, головном и промежуточном столбах, в породных погрузочных бункерах и промежуточном бункере в течение года показывает для моделирующих сущностей: те же 0.146 для человеческих факторов (1), снижение за счет перевооружения до 0.001 с существующего уровня 0.130 для факторов, определяемых состоянием основных фондов (2), те же 0.049 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности (3). Риск критичного нарушения целостности обогащающей подсистемы показывает те же 0.026 для человеческих факторов (4), снижение за счет перевооружения до 0.0002 с существующего уровня 0.071 для факторов, определяемых состоянием основных фондов (5), те же 0.008 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности (6). Наконец, риск критичного нарушения целостности подсистемы в галерее показывает те же 0.270 для человеческих факторов (7), снижение за счет перевооружения до 0.0002 с существующего уровня 0.071 для факторов, определяемых состоянием основных фондов (8), те же 0.008 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности (9) – см. рис. 5.17. По сравнению с другими выделяется значение риска для человеческого фактора в 1) - множестве подсистем (0.146) и в 3) - галерее (0.270), это объясняется сравнительно высокой частотой возникновения угроз со стороны человеческого фактора, частота = 1 раз в 1-2 месяца.

При этом, несмотря на то, что среднее время до нарушения целостности всей совокупности сущностей (1..9) составляет около 12 лет (см. рис. 5.18), интегральный риск нарушения целостности всей системы вентиляции, аспирации и пылеподавления за год составит 0.433. Это говорит о том, что в течение года негативное воздействие

исследованных дестабилизирующих факторов может оказаться столь же вероятным, как и отсутствие их опасного проявления. В свою очередь за 2 года интегральный риск приблизится к 0.68, что вдвое превышает вероятность успешного развития событий в системе вентиляции, аспирации и пылеподавления – см. рис. 5.19. Наиболее «узкое место» - человеческий фактор в галерее ОФ, а также во множестве подсистем в погрузочных бункерах, аккумулирующих бункерах, головном и промежуточном столбах, в породных погрузочных бункерах и промежуточном бункере.

Резюме по решению аналитической задачи 1-5.3 (провести сравнительный анализ эффективности системы вентиляции, аспирации и пылеподавления до и после усовершенствования (перевооружения) ОФ) – следующее. Вышеизложенные интегральные результаты исследований характеризуют убедительное улучшение состояния дел для существующей системы вентиляции, аспирации и пылеподавления ОФ за счет перевооружения. Налицо – явные ожидаемые успехи от управления рисками на основе перевооружения (интегральный риск за год эксплуатации снизится на 33% - с существующего уровня 0.574 до 0.433, среднее время до нарушения целостности системы возрастет почти на год - с нынешних 11.1 до 12 лет). Вместе с тем, результаты прогноза на рис. 5.17 и 5.18 демонстрируют не только убедительные технические эффекты от улучшения характеристик основных фондов (см. колонки 2, 5, 8), но и откровенные недостатки (скорее - «узкие места») в противодействии угрозам со стороны человеческого фактора, оказывается, среднее время нарушения целостности подсистемы в галерее составит все те же 3.2 года, т.е. улучшений нет, достигнутый «эффект» - мнимый (см. колонки 1, 7). Этот явный дисбаланс остро нуждается в усовершенствованиях на основе управления рисками, т.к. на самом деле 12 лет до нарушения набирается за счет сверхнадежной работы новых основных фондов (см. колонки 3, 6) – получается как «средняя температура по больнице». И эффект – только технический, но далеко не системный!

Но чем можно еще управлять, за счет чего можно достичь реального системного эффекта, к чему нужно стремиться?

Для ответа на этот вопрос с использованием созданного прототипа технологии поддержки риск-ориентированной системной инженерии решается аналитическая задача 2-5.3 – обосновать рекомендации по всесторонним улучшениям и осуществить упреждающее управление различными рисками и интегральным системным риском.

Ниже для решения задачи 2-5.3 приводятся рекомендации по результатам дополнительных исследований, связанных со снижением рисков со стороны человеческого фактора.

Результаты решения задачи 1-5.3 показали надежность основных фондов после перевооружения. Более того, в отличие от других подсистем в обогащающей подсистеме риск нарушения целостности, связанный с человеческим фактором, составил приемлемые 0.026 за год (см. рис. 5.17). И это при прочих равных условиях было достигнуто за счет снижения частоты возникновения источников угроз со стороны человеческого фактора до одного раза в год.

По аналогии с обогащающей подсистемой 2) для решения задачи 2-5.3 полагаем для расчетов, что в таблице 5.5 в строке 1 частота возникновения угроз несколько снизится - до двух раз в год (вместо 6 раз в год, т.е. снизится в 3 раза), а в строке 7 – также 2 раза в год (вместо 1 раз в месяц, т.е. снизится в 6 раз). Но не до 1 раза в год, как для обогащающей подсистемы (4-я строка). На практике это вполне достижимо не только благодаря привлечению высококвалифицированных мастеров, работающих в режиме взаимного контроля и взаимовыручки, но и на основе привлечения дополнительных систем искусственного интеллекта и робототехники, способных работать без устали и помогающих не допускать текущих ошибок в работе человека – см. [5, 146, 160, 167].

Сама задача 2-5.3 представляет собой классическую обратную задачу поиска приемлемых рациональных решений при ограничениях (если бы искалось лучшее решение, это была бы классическая задача оптимизации).

Зададимся допустимым уровнем рисков для каждой из моделируемых подсистем 1,…, 9: за год значение прогнозируемого риска не должно превышать 0.05. Допустимый интегральный риск за год – не выше 0.20 при ограничениях на затраты, что соответствует рекомендациям ГОСТ Р 59991-2022 «Системная инженерия. Системный анализ процесса управления рисками для системы» (дополнительные затраты на снижение угроз от «человеческого фактора» полагаются для ОФ приемлемыми). Требуется определить такие условия эксплуатации ОФ в части проявления «человеческого фактора», при которых для моделируемой системы вентиляции, аспирации и пылеподавления при ее техническом перевооружении удастся удержать частные риски на уровне не выше 0.5, а интегральный риск – не выше 0.2 за год.

Результаты прогнозирования ожидаемого риска критичного нарушения целостности состояния исследуемой системы вентиляции, аспирации и пылеподавления и анализируемых сущностей за год, среднее ожидаемое время до нарушения целостности сущностей, а также зависимость интегрального риска от длительности прогнозного периода от полугода до 2-х лет отражены на рис. 5.20 – 5.22 (после формирования приемлемых условий противодействия угрозам со стороны «человеческого фактора»).

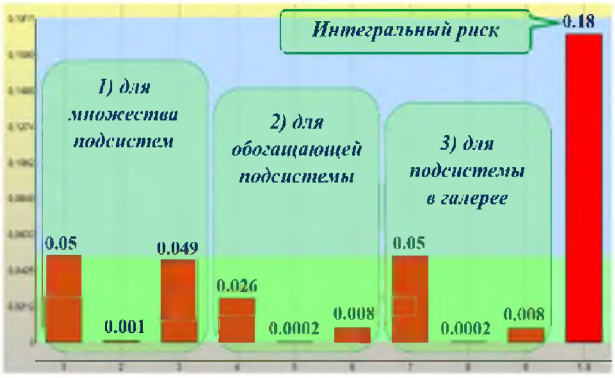


Рис. 5.20 Риск критичного нарушения целостности за год для каждой из сущностей (от 1-й по 9-ю) и всей совокупности сущностей (1..9) при условиях

Рис. 5.21 Среднее время до нарушения целостности каждой из сущностей (от 1-й по 9-ю) и всей совокупности сущностей (1..9) при условиях

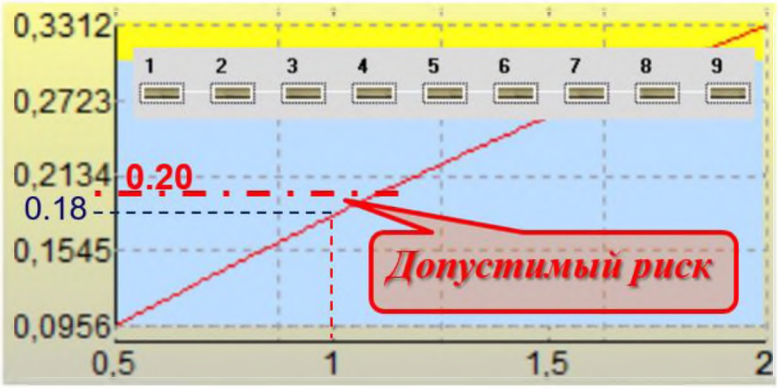


Рис. 5.22 Зависимость интегрального риска от длительности прогнозного периода от 0.5 года до 2-х лет для системы при условиях

Анализ расчетных результатов для системы вентиляции, аспирации и пылеподавления после уточнения достижимых условий по человеческому фактору показал следующее.

Риск критичного нарушения целостности подсистем в погрузочных бункерах, аккумулирующих бункерах, головном и промежуточном столбах, в породных погрузочных бункерах и промежуточном бункере в течение года показывает для моделирующих сущностей: допустимые 0.05 в сравнении с прежними 0.146 для человеческих факторов (1), снижение за счет перевооружения до 0.001 для факторов, определяемых состоянием основных фондов, это уже наблюдалось на рис. 5.17 (2), те же 0.049 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности (3). Риск критичного нарушения целостности обогащающей подсистемы показывает те же 0.026 для человеческих факторов (4), снижение за счет перевооружения до 0.0002 для факторов, определяемых состоянием основных фондов (5), те же 0.008 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности

(6) – это все уже наблюдалось на рис. 5.17 (т.к. изменений в исходных данных для моделирования не было). Наконец, риск критичного нарушения целостности подсистемы в галерее показывает допустимые 0.05 в сравнении с предыдущими 0.27 для человеческих факторов (7), снижение за счет перевооружения до 0.0002 для факторов, определяемых состоянием основных фондов (8), те же 0.008 для организационно-производственных факторов и факторов, не зависящие от производственной деятельности (9), это уже наблюдалось ранее – см. рис. 5.20.

При этом, несмотря на то, что среднее время до нарушения целостности всей совокупности сущностей (1..9) составляет по-прежнему около 12 лет (см. рис. 5.21), интегральный риск нарушения целостности всей системы вентиляции, аспирации и пылеподавления за год составит 0.18, что в 3.2 раза ниже в сравнении с существующем уровнем и в 2.4 раза ниже в сравнении с техническим перевооружением 0.433 (без оптимизации). Это говорит о том, что в течение года вероятность успешного функционирования системы вентиляции, аспирации и пылеподавления в 4.6 раза выше, нежели вероятность реализации сохраняемых угроз. В свою очередь при прогнозе на 2 года вероятность успешного функционирования системы по-прежнему будет вдвое выше интегрального риска нарушения целостности системы, и это – хороший результат, свидетельствующий об устойчивости безопасного функционирования системы – см. рис. 5.22.

Таким образом, за счет упреждающего управления рисками в задаче 2-4.5 удалось выявить условия к системе вентиляции, аспирации и пылеподавления, соблюдение которых позволит удерживать частные и интегральный риски в допустимых пределах. Т.е. с использованием созданной технологии поддержки риск-ориентированной системной инженерии разработаны рекомендации: условия эффективного взаимодействия социокиберфизических систем в жизненном цикле обогатительной фабрики в угольной отрасли должны быть не хуже приведенных в табл. 5.5 с характеристиками после перевооружения со следующей корректировкой частоты возникновения угроз со стороны «человеческого фактора» по строкам 1 и 7 – не чаще двух раз в год. В определении этих допустимых условий – суть рекомендаций по обеспечению эффективности системных мер по упреждающему управлению рисками дополнительно к результатам технического перевооружения в рассмотренном примере.

5.4 Рекомендации по оценке адекватности разработанных программных решений на примерах управления рисками для обеспечения качества хранимого зерна [104, 167, 186]

В качестве еще одной области приложения разработанных программных, технологических и методических решений для ВС и КС в настоящем подразделе выступает конкретная критичная сущность, рассматриваемая как единое целое – это сельскохозяйственное зерно в условиях хранения в региональном зернохранилище. С использованием созданного прототипа технологии поддержки риск-ориентированной системной инженерии предлагаются рекомендации по решению задачи обоснования допустимых рисков критичного нарушения качества и сроков хранения зерна.

Для понимания практической важности вопроса – несколько вводных пояснений. При хранении зерна его качество снижается из-за воздействий опасных биологических, химических и физических факторов. Так, Россельхознадзор контролирует состояние зерна только при его закупке и не имеет полномочий на контроль за состоянием хранилищ перед закладкой и в процессе хранения. Значения исходных данных для моделирования могут быть подчерпнуты из различных опубликованных данных. Так, было установлено, что из 450 тыс. т проверенного зерна более половины хранилось в ненадлежащих условиях. Около 60 тыс. т (13.33%) оказались зараженными вредителями (см., например, АиФ №48(1569), 1-7 декабря 2010г., с. 15). Много случаев самосогревания, что приводит к поражению зерна плесневыми грибами и делает его непригодным даже для технической переработки. Приведенные факты – это накопленная информация, которая может и должна быть преобразована путем моделирования в знания в интересах качественного хранения зерна, собираемого в России.

Демонстрируя работоспособность предложенной в 4.2 методики, целью прогнозирования рисков поставим установление степени вероятного нарушения целостности исследуемой системы за период прогноза в интересах сравнительного анализа различных вариантов поведения системы для возможных сценариев развития угроз и мер противодействия угрозам, а также обоснования допустимых рисков и сроков хранения зерна. Так, несмотря на меры контроля и действий по поддержанию и восстановлению качества, наступает момент времени, когда зерно из-за потери надлежащего качества окажется неприемлемым к использованию. Требуется сравнить различные варианты хранения зерна, а также определить максимально возможный период до нарушения целостности исследуемой системы, т.е. до наступления такого момента, когда хранимое зерно потеряет надлежащее качество.

Для решения этой практической задачи с использованием ВС или КС воспользуемся предлагаемой методикой и накопленной доступной информацией.

Перечень опасных биологических, химических, физических факторов, контролируемых признаков и предупреждающих действий при хранении зерна в очищенном и охлажденном состоянии дан в [167, 186]. Очищенное, сухое, не зараженное вредителями зерно можно хранить без потерь несколько лет. Однако, вредители, присутствующие на зернохранилищах и вокруг них, заселяют зерно и размножаются. Например, рисовый долгоносик при температуре от 20˚С до 25˚Св течение 2-х месяцев увеличивает свою численность в 15-45 раз. Зерно, загрязненное вредителями и продуктами их жизнедеятельности, становится токсичным, его нельзя использовать на продовольственные цели.

Рассмотрим защищенность зерна от вредителей, полагая в рамках примера, что именно от них исходит главная опасность. Учитывая, что при 12-15˚С продолжительность развития насекомых (к примеру, амбарного долгоносика) составляет 141-376 дней, а цикл развития от яйца до имаго составляет 1.5-2 месяца, положим, что с учетом возможных проблем с кондиционированием в хранилищах зерна частота скрытного появления критичных ситуаций в течение летне - осенних месяцев составляет не реже 1 раза в сутки (т.е. каждый день при температуре воздуха выше 12˚С возможно заражение или дальнейшая порча зерна насекомыми). Т.е. в рамках применения предложенной методики полагаются следующие значения для σ (частота возникновения источников угроз) и β (среднее время развития угроз): частота появления критичных ситуаций (σ) – от 1 раза в сутки до 1 раза в неделю; среднее время развития критичной ситуации (β) – 1.5 месяца.

При определении характеристик мер противодействия опасностям учитывается, что в условиях охлаждения зерна ниже температурного порога развития насекомых (ниже 10.2˚С) прекращается их спаривание, откладывание яиц и развитие всех стадий. Насекомые становятся малоподвижными и почти не питаются. Длительное пребывание насекомых при такой температуре приводит к их медленному вымиранию. Кроме того, поддержание влажности в среднем на уровне 13%-15% также способствует вымиранию насекомых. Для расчетов полагается: время между моментами системного контроля температуры и влажности ($T_{меж}$) = 1 час; длительность контроля с восстановлением штатного режима после его нарушения ($T_{диаг}$) = 1 час. Этой информации достаточно для прогнозирования риска нарушения целостности хранимого зерна с использованием модели 2.2.2.

Результаты прогноза на период от 1 года до 6 лет показали следующее.

В интересах сравнительного анализа: если частота появления критичных ситуаций составляет 1-2 раза в сутки, то риск нарушения целостности в течение года составит от 0.28 до 0.47, а в течение 2-х с небольшим лет – может превысить 0.5 – см. рис. 5.23 - 5.25.

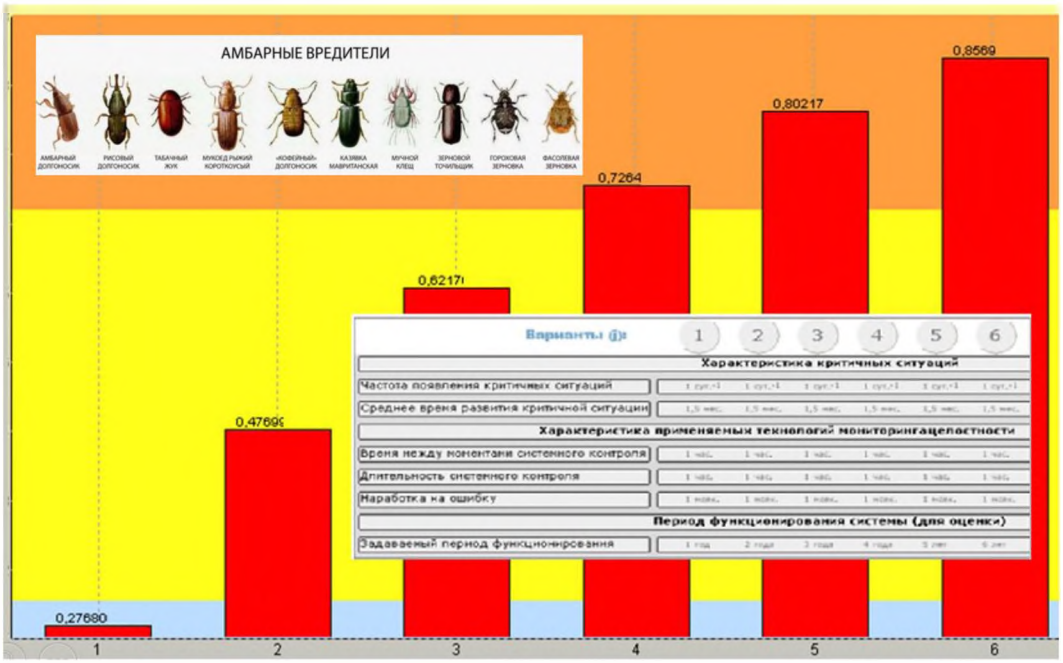


Рис. 5.23 Риск нарушения целостности моделируемой системы при частоте появления критичных ситуаций 1 р/сут. и периоде прогноза от 1 до 6 лет

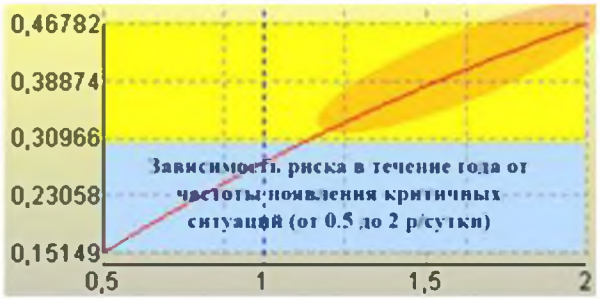


Рис. 5.24 Зависимость риска в течение года от частоты появления критичных ситуаций в сутки

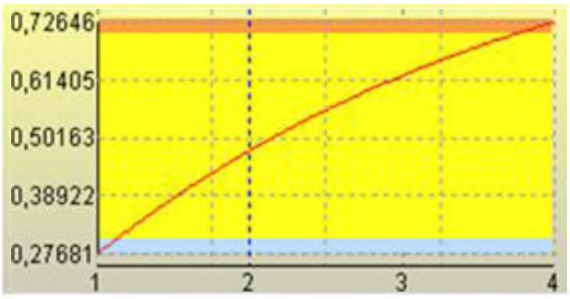


Рис. 5.25 Зависимость риска от задаваемого периода прогноза от 1 года до 4-х лет

Далее проведем расчеты для прогнозирования риска при более редких появлениях критичных ситуаций, а также для обоснования такого уровня частоты появления критичных ситуаций в зернохранилищах, который может считаться допустимым.

Результаты прогнозирования показывают - если частота появления критичных ситуаций составляет 1-2 раза в неделю, риск нарушения целостности моделируемой системы в течение года составит от 0.05 до 0.09, т.е. риск снижается в 5 раз с уровня 0.28 до 0.47. А при прогнозе на 6 лет риск составит 0.25-0.43 – см. рис. 5.26 (это лучше, чем риск в течение года при частоте появления критичных ситуаций 1- 2 раза в сутки!).

Наконец, риск в течение периода от 1.5 до 6 лет составит 0.07-0.25 – см. рис. 5.27.

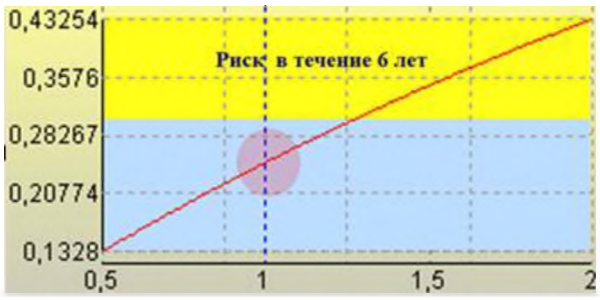


Рис. 5.26 Зависимость риска в течение 6 лет от частоты появления критичных ситуаций (от 0.5 до 2 раз в неделю)

Рис. 5.27 Зависимость риска в течение периода времени от 1.5 лет до 6 лет при появлении критичных ситуаций 1 раз в неделю

Полученные результаты стали источником следующих выявленных из накопленной информации закономерностей: вероятность сохранения качества хранимого зерна за 3-6 лет в 3-5 раз превышает вероятность потери качества, если условия хранения не допускают возникновения рассадников насекомых чаще, чем раз в неделю (это – фактическое обоснование допустимой частоты появления критичных ситуаций в зернохранилищах с использованием созданных базовых моделей). Тем самым результаты моделирования количественно в терминах риска не только охарактеризовали результаты натурных экспериментов, но и подтвердили их. Результаты многолетних исследований ВНИИ Зерна [188] подтвердили адекватность такого вывода.

Суть предлагаемых рекомендаций в следующем: полученные значения риска могут быть определены как допустимые для обеспечения качества хранимого зерна, а именно - риск нарушения качества хранимого зерна в зернохранилище не должен превышать 0.10 для срока хранения зерна 1 год и 0.25 для хранения зерна в течение 6 лет.

Таким образом, на примерах управления рисками для обеспечения качества хранимого зерна рекомендуется использование выявленной закономерности: если условия хранения не допускают возникновения рассадников насекомых чаще, чем раз в неделю, вероятность сохранения качества хранимого зерна за 3-6 лет в 3-5 раз превышает вероятность потери качества. Результаты многолетних исследований ВНИИ Зерна подтвердили адекватность такого вывода. Тем самым результаты проведенных исследований в сравнении с результатами иных специализированных исследований (ВНИИ Зерна) явились дополнительной аргументацией в подтверждение адекватности разработанных математических и программных решений в различных их приложениях.

5.5 Рекомендации по извлечению знаний из анализа угроз злоумышленной модификации модели машинного обучения для сопровождаемых систем с искусственным интеллектом [5, 152, 155, 167]

5.5.1 Характеристика проблематики злоумышленной модификации модели машинного обучения

Системы с искусственным интеллектом (СИИ) все глубже проникают в повседневную жизнь человека. И это далеко не только голосовые помощники в наших персональных телефонах, навигаторы, онлайн карты и иные удобные сервисы. СИИ все чаще используется в системах обеспечения безопасности на основе интеллектуальной обработки огромных потоков разнородной информации, поступающей от различных камер, сенсоров, устройств телеметрии. Программные средства (ПС) СИИ, обновляемые с помощью моделей машинного обучения, помогают соответствующим службам в распознавании лиц и документов, строений и сооружений и их местоположений, в идентификации предпосылок к нарушению информационной, промышленной, транспортной, экологической безопасности, в геологоразведке, медицине, фармацевтике и биологии, в мониторинге соблюдения правил дорожного движения, распознавая условия нарушения и государственные номера транспортных средств нарушителей и др. Эти примеры далеко не исчерпывают практических возможностей СИИ [189 - 192].

В основе эффектов от применения СИИ лежат обучаемые нейронные сети. Искусственные нейронные сети основаны на наборе персептронов, называемых нейронами. Каждый нейрон сопоставляет набор входных данных с выходными, используя функцию активации. Машинное обучение управляет весами и функцией активации таким образом, чтобы иметь возможность правильно определять выходные данные. В то время, как однослойная нейронная сеть (или персептрон) - это подход к разработке объектов, глубокая нейронная сеть позволяет изучать объекты, используя необработанные данные в качестве входных данных. За счет этого достигается существенное увеличение производительности СИИ по сравнению с обычным человеческим интеллектом при решении многих практических задач. При этом обеспечение безопасности информации СИИ должно предусматривать возможность противодействия злоумышленным угрозам подмены и модификации моделей машинного обучения и дообучения (ММО). Однако сегодня системная зависимость нарушения нормального функционирования СИИ от этих угроз является не только далеко не прозрачной, но и на количественном уровне не анализируется. Не представляя всего внутреннего содержания машинного обучения, заказчик и пользователи системы могут вполне воспринимать нарушения ее нормального

функционирования за обычное техническое несовершенство, не устанавливая прямой связи со злоумышленными действиями «умного» нарушителя по модификации ММО. Опасность в том, что нарушитель пытается целенаправленно подменить ММО или исказить обучающие данные, вводя тщательно разработанные ложные образцы так, чтобы в конечном итоге скомпрометировать весь процесс машинного обучения.

В рамках настоящего подраздела при разработке рекомендаций по извлечению знаний из анализа угроз злоумышленной модификации модели машинного обучения для сопровождаемых систем, использующих СИИ, из множества различных угроз выделены следующие актуальные угрозы[1]: угроза подмены ММО (УБИ.222) и угроза модификации ММО путем искажения («отравления») обучающих данных (УБИ.221). Это обусловлено следующими соображениями. В наше время нередко разработчики ПС, осуществляющие машинное обучение (дообучение), принадлежат сторонним организациям относительно разработчика систем, использующих СИИ. Они являются основными владельцами ММО, не хотят раскрывать и передавать заказчику и головному разработчику системы исходные тексты, находятся на субконтракте, сами разрабатывают ПС, в которых содержатся результаты машинного обучения, и контролируют его корректность. Обученные и дообученные ПС передаются заказчику и головному разработчику систем, использующих СИИ, для функционального тестирования, после чего оттестированные ПС принимаются в эксплуатацию в системе. Сертификация дообучаемых ПС по требованиям безопасности может оказаться нецелесообразной из-за длительности и дороговизны ее проведения для заказчика, а также из-за возможного нежелания владельцев ММО раскрывать все исходные тексты программ и методы обучения. В этом случае угрозы, связанные со злоумышленной модификацией ММО, становятся остро актуальными и требуют системного анализа.

Краткая характеристика угроз УБИ.222 и УБИ.221, а также возможных злоумышленных действий нарушителей, именуемых атаками (Attacks), приведена со ссылками на обобщенные взгляды в России и международном сообществе, анализирующем риски в СИИ[2] – см. также [155, 192] и сноски 3, 4.

Угроза УБИ.222 заключается в возможности подмены ММО внутренним нарушителем (с высоким потенциалом). Угроза обусловлена слабостями разграничения доступа в СИИ, реализация угрозы возможна при наличии у нарушителя непосредственного доступа к ММО.

---

[1] см. сайт ФСТЭК России https://bdu.fstec.ru/ - Банк данных угроз безопасности информации. ФАУ «ГНИИИ ПТЗИ ФСТЭК России». Дата обращения 25.01.2025

[2] Biggio B., Fumera G. and Roli F. Security evaluation of pattern classifiers under attack. *IEEE* transactions on knowledge and data engineering *26, 4.* 2014. *984-996.*

Угроза УБИ.221 заключается в возможности модификации ММО внешним нарушителем (с высоким потенциалом) или внутренним нарушителем (со средним или высоким потенциалом) путем искажения («отравления») обучающих данных. Угроза обусловлена недостатками алгоритмов машинного обучения и осуществления процесса машинного обучения. Реализация угрозы возможна при наличии у нарушителя возможности воздействовать на процесс машинного обучения. Атаки с искажением («отравлением») по сути представляют собой целенаправленное злоумышленное изменение обучающих данных во время машинного обучения для компрометации всего процесса машинного обучения («отравление» - это буквальный перевод на русский язык англоязычного термина *Poisoning Attack*).

Анализ возможностей нарушителя на этапе обучения состоят в следующем. Нарушитель пытается напрямую повлиять на ММО или повредить ее, изменяя набор данных, используемый для обучения. Самая распространенная атака - это простой доступ к частичным или полным данным обучения.

На сегодня выделяются три применимые стратегии атаки для модификации ММО, основанные на возможностях нарушителя – это стратегии ввода данных, модификации данных и искажения логики ММО.

Стратегия ввода данных используется, когда нарушитель не имеет никакого доступа к обучающим данным, а также к алгоритму обучения, но имеет возможность добавить новые данные в обучающий набор. Он может исказить целевую ММО, вставив ложные выборки в обучающий набор данных. Это влечет за собой некорректность машинного обучения при разработке соответствующих ПС.

Стратегия модификации данных используется, когда нарушитель не имеет доступа к алгоритму обучения, но имеет полный доступ к обучающим данным. Нарушитель напрямую искажает обучающие данные (например, путем прямого изменения меток обучающих данных), изменяя их до того, как они будут использованы целевой ММО. Это также влечет за собой некорректность машинного обучения при разработке соответствующих ПС.

Стратегия искажения логики ММО используется, когда нарушитель имеет возможность вмешиваться в алгоритм обучения (например, путем манипулирования входными характеристиками в зависимости от своих возможностей). Это наиболее опасные атаки, поскольку очень трудно разработать стратегию упреждающего противодействия злоумышленным действиям нарушителя, способного законным образом изменить логику обучения (подобного рода нарушения легко могут быть замаскированы под неумышленную «ошибку»). Искажение логики целенаправленно влечет за собой некорректность

машинного обучения при разработке соответствующих ПС, поскольку нарушителем контролируется и модифицируется сама целевая ММО.

Злоумышленные возможности нарушителя на этапе тестирования ПС состоят в следующем. Нарушитель пытается напрямую повлиять на ММО или повредить ее, изменяя набор данных. Атаки во время тестирования не влияют на целевую ММО, но приводят к неверным выходным результатам при использовании соответствующих ПС. Эффективность таких атак определяется главным образом объемом доступной нарушителю информации о целевой ММО.

Таким образом, реализация угроз злоумышленных действий по модификации ММО для СИИ рассчитана на «умного» нарушителя, понимающего свои возможности, представляющего и способного поставить достижимые задачи нарушения целостности системы. Вышеизложенные пояснения даны для понимания излагаемой далее формализации и системного анализа рассматриваемых угроз, мер противодействия этим угрозам и соответствующих рисков от реализации этих угроз.

Применение предлагаемого подхода к решению различных прямых и обратных задач для обеспечения эффективного целевого применения СИИ позволит прогнозировать риски и количественно обосновывать принимаемые решения о стратегии и мерах противодействия рассматриваемым угрозам. При проведении исследований основное внимание сосредоточено на анализе вероятностного выражения риска, полагается, что возможный ущерб (чаще - репутационный) противопоставляется расчетным значениям рисков и соответствующим условиям моделирования.

Примечание. Подход учитывает последние взгляды Национального института стандартизации США на таксономию внедрения в СИИ вредоносного машинного обучения, а также основы управления рисками для СИИ[3,4] и не противоречит им.

Одновременно при проведении исследований осуществляется использование ранее созданной вероятностной модели [2, 37, 49, 58], которая не рассматривалась в разделе 2. Тем самым в подразделе демонстрируется расширение аналитических возможностей созданной инфраструктуры путем добавления другой модели (авторское участие в создании модели при этом состояло в необходимом программировании формул и в соблюдении протоколов включения новых программ в созданную инфраструктуру).

---

[3] Adversarial Machine Learning. A Taxonomy and Terminology of Attaks and Mitigations (Вредоносное машинное обучение. Таксономия и терминология атак, и способов снижения их отрицательных последствий). NIST AI 100-2e2023 ipd, 2023. nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf

[4] Artificial Intelligence Risk Management Framework. NIST AI 100-1, 2023. nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

5.5.2 Расширение аналитических возможностей созданного прототипа путем добавления модели для оценки риска невыявления некорректностей в машинном обучении при разработке программных средств

Для оценки риска невыявления некорректностей в машинном обучении при разработке ПС предлагается использовать ранее созданной модели, адаптировав наименования исходных данных под решаемую задачу. Добавление этой модели одновременно демонстрирует реализацию функции расширения аналитических возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии (см. раздел 3).

Предлагаемая к использованию модель позволяет оценить возможность реализации рассматриваемых угроз при разработке ПС (в частности – при его тестировании) по показателям вероятности получения корректных результатов машинного обучения $P_{\text{корр}(1)}$ и риска невыявления некорректностей в машинном обучении. Модель адаптирует разработанные ранее вероятностные подходы [2, 37, 49, 58, 168, 181], которые доведены с участием автора до уровня реализации в ГОСТ Р 59341, приложении В.3.7.

Определение: считается, что при разработке ПС машинное обучение (дообучение) проведено корректно в моделируемой системе, если в процессе контроля обученных ПС до истечения заданного срока его контроля все некорректности выявлены и новые алгоритмические ошибки не допущены. Некорректности при разработке ПС (в параметрах, исходных текстах программ, алгоритмах, обучающих фотографиях, метках и опорных векторах, действиях и др., способных привести к нарушениям нормального функционирования ПС при эксплуатации СИИ) – это в общем случае то, что искажает ожидаемые результаты последующего применения ПС после их машинного обучения в условиях рассматриваемых угроз по сравнению со случаем отсутствия каких-либо угроз. Некорректности появляются в результате реализации угроз, описанных выше в разделе 2, и характеризуют отсутствие корректности машинного обучения в моделируемой системе. Требуемая корректность машинного обучения при разработке ПС в идеале заключается в недопущении злоумышленной модификации адекватной ММО и использования небезопасных версий ПС, а также в исключении искажения обучающих данных. В общем случае под корректностью машинного обучения при разработке ПС для СИИ понимается свойство ПС, получаемых в результате машинного обучения, обеспечивать получение правильных согласованных результатов или эффектов обработки информации в соответствии с целевым назначением этой обработки в моделируемой системе. Корректность обеспечивается на основе применения адекватных способов машинного обучения и контроля результатов обучения, позволяющих выявить все имеющие место некорректности

и не допустить алгоритмических ошибок при контроле обученных ПС. Корректность машинного обучения после контроля информации по обучаемым ПС является следствием приемлемого соотношения между объемом контролируемой информации, частью важной для принятия решения информации, подлежащей учету, скоростью контроля информации, частотой ошибок контролера, длительностью его непрерывной работы и ограничениями на допустимое время контроля. В качестве контролера могут выступать человек – разработчик ПС, учитель, тестировщик или аналитик (в т.ч. лицо, принимающее решение), программно-технические инструментальные средства, ориентированные на выявление некорректностей в машинном обучении при разработке ПС, или их комбинация.

Для моделирования процесса контроля информации в моделируемой системе при разработке ПС предлагаются адаптированные исходные данные [2, 5, 37, 49, 58, 161, 162]:

V – объем информации по обучаемым (при тестировании – по обученным) ПС, подлежащий контролю (объем измеряется в безразмерных условных единицах – у.е., это могут, например, быть количество параметров, строк текста, алгоритмов, обучающих фотографий, меток и опорных векторов, действий, количество нарушений нормального функционирования ПС при тестировании и др.);

μ – часть важной для принятия решения информации, которая должна быть объективно использована при контроле информации в заданном объеме V, измеряемая от 0 до 100% от анализируемого объема информации;

ν – скорость контроля (у.е. в единицу времени);

n – частота ошибок контроля 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной, влияющей на корректность машинного обучения);

$T_{\text{нар}}$ – среднее время наработки на алгоритмическую ошибку (когда объективно важная для принятия решения информация игнорируется, это – аналог ошибки контроля 2-го рода);

$T_{\text{непр}}$ – период непрерывной работы контролера;

$T_{\text{зад}}$ – задаваемое время на контроль информации.

Возможны 4 варианта соотношений между временем реального контроля $T_{\text{реальн}}$ всего контролируемого объема ($T_{\text{реальн}} = V/\nu$), задаваемым допустимым временем на контроль $T_{\text{зад}}$ и непрерывным временем работы контролера $T_{\text{непр}}$.

Вариант 1. Задаваемое время на контроль информации не меньше, чем время реального контроля (т. е. $T_{\text{реальн}} \leq T_{\text{зад}}$), а объем контролируемой информации относительно мал,

что позволяет проверить его за один период непрерывной работы контролера ($T_{\text{реальн}} \le T_{\text{непр}}$).

Для экспоненциальной аппроксимации распределений интервалов между ошибками в контролируемой информации, времени до свершения ошибки 1-го рода и времени наработки контролера на ошибку, а также при условии независимости исходных характеристик вероятность $P_{\text{после (1)}}(V, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад}})$ отсутствия некорректностей в машинном обучении после контроля для варианта 1 определяется выражением:

$$P_{\text{после (1)}} = \begin{cases} e^{-nV/\nu}\left[T_{\text{нар}}^{-1}\, e^{-\mu V} - \mu\nu e^{-V/(\nu\, T_{\text{нар}})}\right]/\left(T_{\text{нар}}^{-1} - \mu\nu\right), \text{если } T_{\text{нар}}^{-1} \neq \mu\nu, \\ e^{-(n+\mu\nu)V/\nu}, \text{если } T_{\text{нар}}^{-1} = \mu\nu. \end{cases} \quad (5.1)$$

Вариант 2. Задаваемое время на контроль информации не меньше, чем время реального контроля (т. е. $T_{\text{реальн}} \le T_{\text{зад}}$), но объем контролируемой информации относительно большой ($T_{\text{реальн}} > T_{\text{непр}}$). Это требует нескольких (N) периодов непрерывной работы контролера, в общем случае $N = V/(\nu T_{\text{непр}})$. Внутри каждого периода проверяют часть всего объема, равную в среднем $V_{\text{части (2)}} = V/N$, а допустимое время контроля информации для этой части принимается равным $T_{\text{зад части (2)}} = T_{\text{зад}}/N$. Тем самым для каждой контролируемой части выполняются условия варианта 1. Вероятность $P_{\text{после (2)}} = P_{\text{после (2)}}(V, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад}})$ отсутствия некорректностей в машинном обучении после контроля для варианта 2 определяется выражением:

$$P_{\text{после (2)}} = \left\{P_{\text{после (1)}}(V_{\text{части (2)}}, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад части (2)}})\right\}^N. \quad (5.2)$$

Вариант 3. Задаваемое время на контроль информации меньше, чем время реального контроля ($T_{\text{реальн}} > T_{\text{зад}}$) при задаваемой средней скорости контроля ν, т. е. объективно может быть проконтролирована лишь часть от всего объема информации при контроле, эта часть равна $V_{\text{части (3)}} = \nu T_{\text{зад}}$. В свою очередь, сам объем контролируемой информации относительно мал и может быть проверен за один период непрерывной работы контролера, т. е. $T_{\text{реальн}} \le T_{\text{непр}}$ и для проверяемого объема $V_{\text{части (3)}}$ выполняются условия варианта 1. Вероятность $P_{\text{после (3)}}$=$P_{\text{после (3)}}(V, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад}})$ отсутствия некорректностей в машинном обучении после его контроля для варианта 3 определяется выражением:

$$P_{\text{после (3)}} = [V_{\text{части (3)}}/V] \cdot P_{\text{после (1)}}\left(V_{\text{части (3)}}, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад}}\right) + \quad (5.3)$$
$$+[(V - V_{\text{части (3)}})/V] \cdot P_{\text{без контроля}},$$

где вероятность отсутствия некорректностей в непроверенной части информации, равной $V - V_{\text{части (3)}}$, составляет $P_{\text{без контроля}} = e^{-\mu(V - V_{\text{части (3)}})}$, а вероятность отсутствия некорректностей в объеме проверенной информации равна $P_{\text{после (1)}}(V_{\text{части (3)}}, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад}})$.

Вариант 4. Задаваемое время на контроль информации меньше, чем время реального контроля ($T_{\text{реальн}} > T_{\text{зад}}$), а объем контролируемой информации относительно большой ($T_{\text{реальн}} > T_{\text{непр}}$). Аналогично варианту 3 реально может быть проконтролирована лишь часть от всего объема, равная $V_{\text{части (4)}} = \nu T_{\text{зад}}$. Относительно этой части возможны два подварианта:

– подвариант 4.1: $T_{\text{зад}} \leq T_{\text{непр}}$, т. е. проверка будет завершена за один период непрерывной работы контролера;

– подвариант 4.2: $T_{\text{зад}} > T_{\text{непр}}$, т. е. потребуется несколько (N) периодов непрерывной работы контролера, $N = V_{\text{части (4)}}/(\nu T_{\text{непр}})$.

Для подварианта 4.1 вероятность отсутствия некорректностей в машинном обучении после контроля $P_{\text{после (4.1)}} = P_{\text{после (4.1)}}(V, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад}})$ определяется выражением:

$$P_{\text{после (4.1)}} = [V_{\text{части (4)}}/V] \cdot P_{\text{после (1)}}\left(V_{\text{части (4)}}, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад}}\right) + \\ + [V - V_{\text{части (4)}})/V] \cdot e^{-\mu\left(V - V_{\text{части (4)}}\right)}. \quad (5.4)$$

Для подварианта 4.2 внутри каждого периода проверяют новую часть, равную в среднем $V_{\text{части (4.2)}} = V_{\text{части (4)}}/N$, и допустимое время контроля для этой новой части принимают равным $T_{\text{зад части (4.2)}} = T_{\text{зад}}/N$.

Вероятность $P_{\text{после (4.2)}} = P_{\text{после (4.2)}}(V, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад}})$ отсутствия некорректностей в машинном обучении после его контроля определяется выражением:

$$P_{\text{после (4.2)}} = [V_{\text{части (4)}}/V] \cdot \left\{P_{\text{после (1)}}\left(V_{\text{части (4.2)}}, \mu, \nu, n, T_{\text{нар}}, T_{\text{непр}}, T_{\text{зад части (4.2)}}\right)\right\}^N + \\ + [V - V_{\text{части (4)}})/V] \cdot e^{-\mu\left(V - V_{\text{части (4)}}\right)}. \quad (5.5)$$

В итоге вероятность отсутствия некорректностей в машинном обучении после контроля $P_{\text{корр(1)}} = P_{\text{после}}$ определяется аналитическими выражениями для $P_{\text{после (1)}}$, $P_{\text{после (2)}}$, $P_{\text{после (3)}}$, $P_{\text{после (4.1)}}$, $P_{\text{после (4.2)}}$ в зависимости от варианта соотношений между исходными данными.

Для формирования исходных данных при моделировании могут использоваться статистические данные, включая данные для систем-аналогов, а также обоснованные гипотетические данные.

Для системного анализа результатов моделирования в оценках интегрального риска рекомендуется задание допустимого уровня $P_{\text{доп корр(1)}}$ и условия α. Условие α касается не только обеспечения корректности машинного обучения при разработке ПС, но и возможного ущерба при реализации угроз. Условие α формулируется в виде ограничений: $P_{\text{корр(1)}} \geq P_{\text{доп корр(1)}}$ и возможный ущерб от нарушения не превышает допустимого (это - формулировка условия α). Учет результатов моделирования в оценках интегрального риска

осуществляется с использованием индикаторного коэффициента $Z_{\text{корр}(1)}$ корректности машинного обучения при разработке ПС:

$$Z_{\text{корр}(1)} = \begin{cases} 1, & \text{если условие корректности машинного обучения при разработке ПС } \alpha \text{ выполнено,} \\ P_{\text{корр}(1)}, & \text{если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Сопоставление с возможным ущербом (или недополученным эффектом) позволяет рассматривать дополнение до единицы этого коэффициента $(1 - Z_{\text{корр}})$ в качестве вероятностного выражения риска невыявления некорректностей в машинном обучении при разработке ПС.

5.5.3 Описание модели для оценки риска невыявления некорректностей в машинном обучении при эксплуатации программных средств

Модель позволяет оценить возможность реализации рассматриваемых угроз УБИ.222 или УБИ.221 при эксплуатации ПС по показателю вероятности получения корректных результатов машинного обучения $P_{\text{корр}(2)}$ и риска невыявления некорректностей в машинном обучении при эксплуатации ПС.

Определение: считается, что машинное обучение (дообучение) характеризуется корректностью при эксплуатации ПС в течение заданного периода прогноза, если в течение этого периода не были реализованы угрозы, связанные с использованием потенциально небезопасных версий ПС, при разработке которых могли быть использованы искаженные («отравленные») нарушителем обучающие данные или осуществлена подмена или модификация ММО. Некорректности при эксплуатации ПС – это в общем случае возникновение на временной оси негативных событий, вызванных допущенными и пропущенными ошибками при разработке ПС, уязвимостями в ПС, способствующих нарушению нормального функционирования СИИ, согласно ее назначению. Некорректности появляются в результате реализации угроз, описанных выше в разделе 2, и характеризуют отсутствие корректности. Требуемая корректность машинного обучения при эксплуатации ПС достигается противодействием угрозам по факту выявления предпосылок или выявления непосредственного ущерба (недополученного эффекта) от реализации угроз при функционировании моделируемой системы. Корректность при эксплуатации ПС обеспечивается на основе анализа обращений пользователей на нарушения нормального функционирования СИИ с потенциально небезопасной версией ПС и/или на оперативное восстановление приемлемых условий ее функционирования. В качестве аналитика могут выступать оператор и пользователи системы, использующей СИИ, разработчик, осуществляющий сопровождение ПС, программно-аналитические

инструментальные средства, ориентированные на выявление некорректностей в машинном обучении при эксплуатации ПС, или их комбинация.

Примечание. Нарушение нормального функционирования моделируемой системы должно быть определено формально. Возможно использование экспертных границ с применением универсальной вспомогательной модели показателя (УВМП) – см. раздел 2.

В моделях для оценки риска невыявления некорректностей в машинном обучении (дообучении) при эксплуатации ПС под моделируемой системой понимается множество функциональных действий модели СИИ, выполняемых с использованием потенциально небезопасных версий ПС, получаемых от разработчиков по результатам машинного обучения или дообучения.

Для моделируемой системы возможно либо отсутствие какого-либо контроля, либо периодический системный контроль хода выполнения функциональных действий. Предлагаемые вероятностные модели и методы, предложенные в разделе 2 диссертации.

Моделируемая система представлена в виде «черного ящика». Специфика состоит в логическом переопределении исходных данных для моделирования. С формальной точки зрения результатом применения модели с учетом возможного ущерба (недополученного эффекта) является расчетный риск невыявления некорректностей в машинном обучении (дообучении) при эксплуатации ПС в моделируемой системе в течение заданного периода прогноза при реализации периодического системного контроля. Для расчета риска в моделируемой системе сложной структуры для каждого элемента используются исходные данные (см. раздел 2) [155]:

σ – частота возникновения источников угроз возникновения небезопасных версий ПС, при разработке которых были использованы искаженные («отравленные») нарушителем обучающие данные или была осуществлена подмена или модификация ММО;

β – среднее время развития угроз с момента их возникновения до нарушения нормального функционирования моделируемой системы;

$T_{меж}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{восст}$ – среднее время восстановления нарушаемой целостности моделируемой системы;

$T_{зад}$ – задаваемая длительность периода прогноза.

В итоге расчетная вероятность корректного машинного обучения ПС характеризуется вероятностью отсутствия нарушений целостности моделируемой системы в течение периода прогноза $T_{зад}$ и определяется теми же аналитическими выражениями (2.1) – (2.8), что и в моделях раздела 2.

Сопоставление с возможным ущербом (или недополученным эффектом) позволяет рассматривать расчетную вероятность по формуле (2.1) как риск невыявления некорректностей в машинном обучении при эксплуатации ПС в моделируемой системе при реализации предпринимаемых технологических мер периодического системного контроля и восстановления целостности моделируемой системы. Вероятностное значение этого риска представляет собой дополнение до единицы вероятности корректного машинного обучения ПС в течение заданного периода прогноза $P_{\text{корр(2)}}$.

В частном случае, когда период между диагностиками больше периода прогноза $\boldsymbol{T}_{\text{зад}} < \boldsymbol{T}_{\text{меж}}$, модель применима для прогноза риска при отсутствии какого-либо контроля.

Для системного анализа результатов моделирования в оценках интегрального риска (см., например, ГОСТ Р 59341-2021) рекомендуется задание допустимого уровня $P_{\text{доп корр(2)}}$ и условия α. Условие α касается не только обеспечения корректности машинного обучения при эксплуатации ПС, но и возможного ущерба при реализации угроз. Условие α формулируется в виде ограничений: $P_{\text{корр(2)}} \geq P_{\text{доп корр(2)}}$ и возможный ущерб от нарушения не превышает допустимого (это - формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляется с использованием индикаторного коэффициента $Z_{\text{корр(2)}}$ ($T_{\text{зад}}$) корректности машинного обучения при эксплуатации ПС:

$$Z_{\text{корр(2)}}(\text{Тзад}) =$$

$$\begin{cases} 1, & \text{если условие корректности машинного обучения при эксплуатации ПС } \alpha \text{ выполнено,} \\ P_{\text{корр(2)}}, & \text{если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Сопоставление с возможным ущербом (или недополученным эффектом) позволяет рассматривать дополнение до единицы этого коэффициента ($1 - Z_{\text{корр(2)}}$ ($T_{\text{зад}}$)) в качестве вероятностного выражения риска невыявления некорректностей в машинном обучении (дообучении) при эксплуатации ПС.

5.5.4 Оценка интегрального риска и примеры [83, 137, 143, 150-152, 155]

Показатель интегрального риска нарушения корректности машинного обучения в моделируемой СИИ позволяет оценить способность нормального функционирования системы в условиях потенциальных угроз злоумышленной подмены и/или модификации ММО. Интегральный риск используется для сравнения весомости прогнозируемых частных рисков, выявления существенных угроз и поддержки принятия решений для задач системного анализа при разработке и эксплуатации моделируемой системы.

В качестве интегрального предлагается виртуальный показатель $\boldsymbol{R}_{\text{интегр}}(\boldsymbol{T}_{\text{зад}})$ риска нарушения корректности машинного обучения в условиях рассматриваемых угроз

моделируемой СИИ, учитывающий в течение задаваемого периода прогноза $\boldsymbol{T}_{\text{зад}}$: риск невыявления некорректностей в машинном обучении (дообучении) при разработке ПС и риск невыявления некорректностей в машинном обучении (дообучении) при эксплуатации ПС. С учетом дополнительных условий α, а также в условиях независимости случайных событий этот показатель может быть рассчитан с использованием моделей из 5.5.2, 5.5.3:

$$R_{\text{нтегр}}(T_{\text{зад}}) = 1 - Z_{\text{корр}(1)} \cdot Z_{\text{корр}(2)}(T_{\text{зад}}). \quad (5.6)$$

Далее рассмотрим пример оценки риска при разработке ПС.

Уже сегодня количество систем, использующих СИИ в различных сферах человеческой деятельности, измеряется многими тысячами, а с широким внедрением Интернета вещей и развитием «умных» систем в ближайшем будущем это количество возрастет на порядки. Тем не менее проблематика количественных оценок исследуемых рисков в России только начинает разворачиваться, критичных случаев злоумышленных модификаций ММО в СИИ не наблюдалось (мошенничество в финансовой сфере – это в общем случае комплекс более специфичных угроз, требующих специального исследования). Соответственно статистика для формирования исходных данных в интересах анализа угроз злоумышленной модификации ММО для СИИ на сегодня практически отсутствует. Поэтому в примере используются правдоподобные гипотетические исходные данные для ориентировочной оценки возможностей наличия некорректностей в машинном обучении при разработке ПС для СИИ.

Положим, по одному исследуемому объекту (например, связанному с распознаванием лиц или документов, строений или сооружений и их местоположений) объем контролируемой информации измеряется различными артефактами общим количеством 1010 у.е. (например, это могут быть параметры объектов, количество строк текста, алгоритмов, обучающих фотографий, меток и опорных векторов, действий, количество нарушений нормального функционирования ПС при тестировании и др.). Т.е. объем информации, подлежащий контролю, для определенности может быть оценен числом V=1010 у.е.

Примечание. Должно быть дано формальное содержательное наполнение у.е. контролируемого объема артефактов при машинном обучении.

В качестве контролера выступает человек – один или несколько разработчиков ПС, учитель, тестировщик или аналитик (в т.ч. лицо, принимающее решение). При этом контроль, как правило, осуществляется не только и не столько по результату, сколько в ходе работ, связанных с машинным обучением (например, в режиме разделения времени «обучение-контроль»). С точки зрения математического моделирования контролеры совместно со средствами, ориентированные на выявление некорректностей в машинном обучении при разработке ПС, представляют собой единое целое.

Часть важной для принятия решения информации, которая должна быть объективно использована при контроле информации в заданном объеме V, рассматривается на уровне до 100% от анализируемого объема в у.е., для определенности положим μ=50%, полагая, что при исследованиях возможны изменения до 100%. Скорость контроля для человека положим вполне реальные 20 у.е. в час, т.е. ν =20 у.е. в час. Период непрерывной работы контролера полагаем равным 1 часу, после чего следует восстановительный отдых, т.е. $T_{\text{непр}}$ =1 час. Предположим, что наработка контролера на ошибку 2-го рода (пропуск некорректности) составляет 1 год, что свойственно для специалистов квалификации выше средней, т.е. $T_{\text{нар}}$=365 суток. На практике при разработке ПС частота ошибок контроля 1-го рода на порядок меньше, нежели частота ошибок 2-го рода, поэтому соответственно положим n =0.00027 раз в сутки. Время на контроль информации задается таким образом, чтобы успеть завершить контроль всего заданного объема артефактов при установленной скорости контроля.

Тем самым все необходимые исходные данные для моделирования сформированы. Результаты расчетов показывают, что вероятность получения корректных результатов машинного обучения $P_{\text{корр(1)}}$ = 0.994. Более того, достигается высокая степень устойчивости этих результатов (см. рис. 5.28 – 5.31), а именно: вероятность получения корректных результатов машинного обучения не опускается ниже 0.988 (при ориентации на обоснование для системы-эталона по ГОСТ Р 59341, приложению Д допустимый уровень составляет не менее 0.95).

С привязкой к единой вероятностной шкале измерений в сравнении с допустимым уровнем это служит научно обоснованным доказательством несущественности рассмотренных типов угроз в рамках рассмотренного сценария.

Необходимо отметить, что эти положительные результаты получены в предположении, что частота ошибок контроля 1-го рода на порядок меньше, нежели частота ошибок 2-го рода. Это – для случая отсутствия целенаправленных действий по искажению («отравлению») обучающих данных (УБИ.221) или подмене или модификации ММО (УБИ.222).

Несколько изменим сценарий развития угроз, представив себе внедрение в состав разработчиков ПС и контролеров потенциального нарушителя (осуществляющего машинное обучение и контроль), злоумышленно реализующего угрозы УБИ.221 или УБИ.222. Сохраняя неизменными все предыдущие исходные данные для моделирования, проведем дополнительные исследования, изменив лишь частоту ошибок контроля 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в

качестве важной), а именно: сделаем частоту ошибок контроля 1-го рода на порядок больше, нежели частота ошибок 2-го рода, т.е. положим n =0.027 раз в сутки.

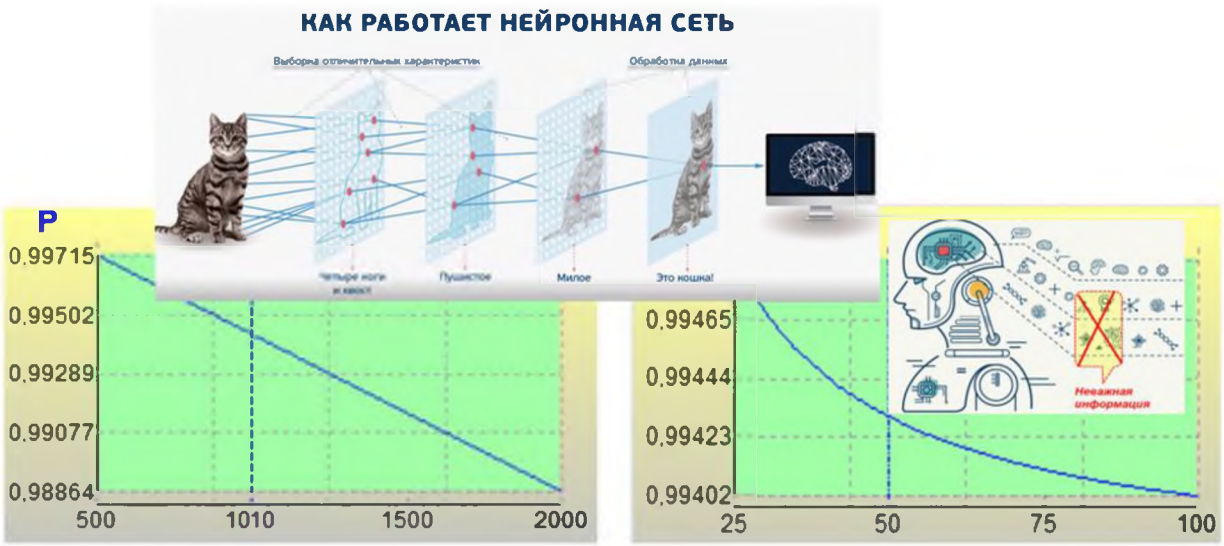


Рис. 5.28 Зависимость вероятности получения корректных результатов машинного обучения от контролируемого объема артефактов (в у.е.)

Рис. 5.29 Зависимость вероятности получения корректных результатов машинного обучения от части важной для принятия решения информации (в %)

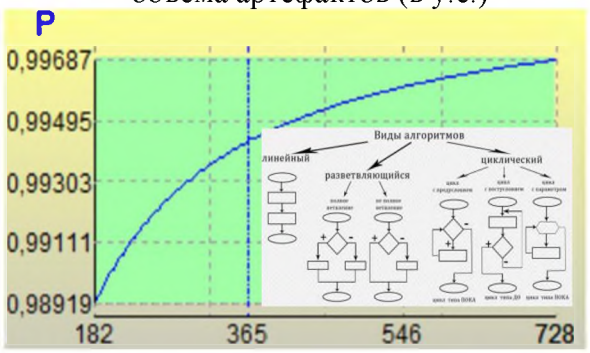


Рис. 5.30 Зависимость вероятности получения корректных результатов машинного обучения от наработки на алгоритмическую ошибку (в сутках)

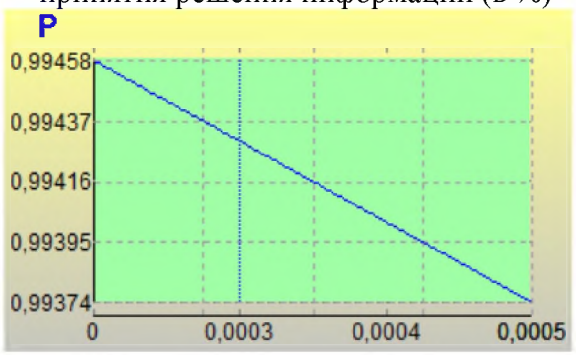


Рис. 5.31 Зависимость вероятности получения корректных результатов машинного обучения от частоты ошибок контроля 1-го рода (раз в сутки)

Результаты расчетов показывают, что в точке расчета вероятность получения корректных результатов машинного обучения при разработке ПС $P_{корр(1)}$ = 0.939. Это меньше, нежели допустимый уровень 0.95 при ориентации на обоснование для системы-эталона по ГОСТ Р 59341-2021, приложению Д (для вероятности получения корректных результатов обработки информации).

Примечание. При ориентации на прецедентный принцип допустимый уровень для $P_{корр(1)}$ по ГОСТ Р 59341-2021, приложению Д соответствует уровню 0.90.

Более детальные оценки показали следующее. При прочих неизменных условиях контролируемый объем артефактов оказывается очень критичным с точки зрения получения корректных результатов машинного обучения – см. рис. 5.32. Так, при

возрастании контролируемого объема до 2000 у.е. вероятность получения корректных результатов машинного обучения падает до 0.88. А допустимый уровень 0.95 будет преодолен, если контролируемый объем артефактов при прочих равных условиях не будет превышать 817 у.е. По этой причине актуальной для снижения риска невыявления некорректностей в машинном обучении при разработке ПС является следующая рекомендация: контролерам качества машинного обучения по возможности следует отбирать для проверки наиболее важные артефакты так, чтобы общее их количество в контролируемом объеме артефактов не превышало 817 у.е. Если этого достичь не удается, следует стараться применять рекомендации, излагаемые далее.

Часть важной для принятия решения информации, которая должна быть объективно использована при контроле информации в заданном объеме артефактов практически не критична – см. рис. 5.33. Это означает, что в условиях моделирования вся важная информация будет принята контролером во внимание. Скорость контроля и период непрерывной работы контролера практически не критичны. Вместе с тем сравнительно низкое абсолютное значение достигаемой вероятности получения корректных результатов машинного обучения (ниже 0.94) говорит о том, что снижения риска невыявления некорректностей в машинном обучении (дообучении) при разработке ПС следует искать в улучшении значений других параметров.

При прочих неизменных условиях в сравнении с ошибками 2-го рода частота ошибок контроля 1-го рода очень критична для получения корректных результатов машинного обучения – см. рис. 5.34, 5.35.

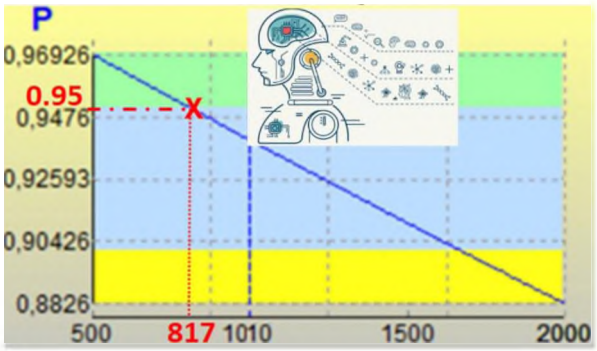


Рис. 5.32 Зависимость вероятности получения корректных результатов машинного обучения от контролируемого объема артефактов (в у.е.)

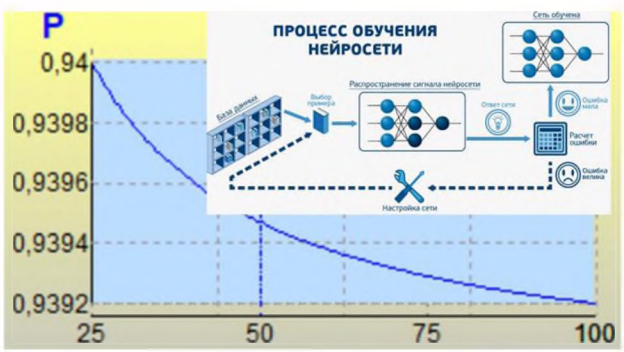


Рис. 5.33 Зависимость вероятности получения корректных результатов машинного обучения от части важной для принятия решения информации (в %)

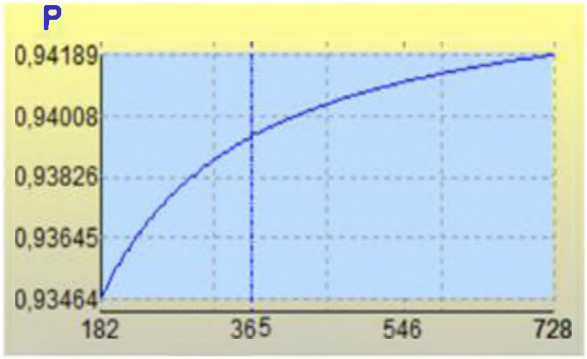


Рис. 5.34 Зависимость вероятности получения корректных результатов машинного обучения от наработки на алгоритмическую ошибку (в сутках)

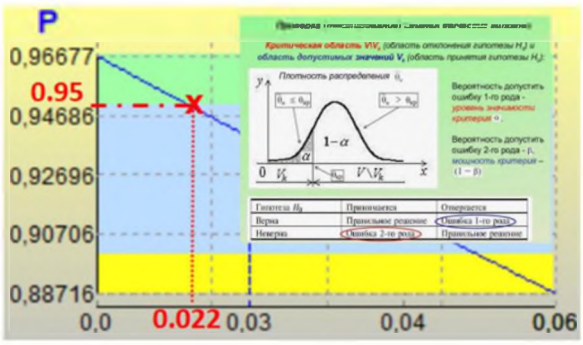


Рис. 5.35 Зависимость вероятности получения корректных результатов машинного обучения от частоты ошибок контроля 1-го рода (раз в сутки)

Анализ результатов моделирования показывает: при возрастании частоты ошибок контроля 1-го рода вдвое с 0.03 до 0.06 раз в сутки вероятность получения корректных результатов машинного обучения монотонно убывает с уровня 0.939 до 0.887. Это подчеркивает актуальность повышения квалификации контролеров машинного обучения. А допустимый уровень 0.95 будет преодолен, если частота ошибок контроля 1-го рода будет не выше 0.022 раз в сутки (что составляет приблизительно 8 раз в год).

Общая рекомендация: целесообразно отслеживать соотношение ошибок контроля 1-го и 2-го рода, не допуская превалирования ошибок 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной). Заметное превалирование ошибок 1-го рода является явным фактором возрастания риска невыявления некорректностей в машинном обучении при разработке ПС.

5.5.5 Рекомендации по формированию исходных данных для прогнозирования рисков

Выявление некорректностей в машинном обучении при эксплуатации ПС – это очень сложная практическая задача. В буквальном смысле как обучили ПС, такие прагматические эффекты и будут иметь место с точки зрения применения СИИ по назначению. Формально границы ожидаемых приемлемых эффектов применения СИИ рекомендуется определять в количественных показателях. Например:

- недопустимое время простоя оборудования (использующего СИИ) на объекте с непрерывным производством, влекущее за собой сокращение прибыли или ущербы, должно составлять в среднем не более 0.5 часа за один останов оборудования и не более 4-х раз в месяц (в техническом задании на систему это требование бизнеса преобразуется чисто в техническое требование, к примеру: должна быть обеспечена приемлемая надежность выполнения функций системой в течение года – с вероятностью не ниже 0.995 при среднем времени восстановления после отказа не более 0.5 часа);

- приемлемый эффект применения навигаторов транспортного средства – не менее 99.9% адекватности в навигации на заданной территории;

- приемлемая удовлетворенность клиентов от использования биометрической системы платежей в метрополитене по сравнению с другими средствами платежей - не менее 88%;

- прирост числа пациентов, для которых с применением СИИ установлен верный диагноз на ранней стадии опасного заболевания должен составлять не менее 20% по сравнению с обычным диагностированием;

- число адекватно распознанных номеров транспортных средств нарушителей на автомобильных дорогах должно быть не менее 95%;

- приемлемый уровень экономии энергии в «умном» доме – не менее 25% по сравнению обычными домами, не оснащенными СИИ, и т.п.

Это – системный взгляд с одной стороны (со стороны лиц, ожидающих успешных результатов применения систем, использующих СИИ). При этом даже с использованием СИИ неизбежны случайные ошибки человека.

С другой стороны на практике просматриваются два основных варианта создания и эксплуатации ПС, в которых реализуются результаты машинного обучения:

- вариант 1 (редкий) – разработчики ПС, осуществляющие машинное обучение и дообучение, принадлежат одной и той же головной организации, которая разрабатывает и сопровождает всю систему, использующую СИИ. В этом случае предотвращение внедрения злоумышленников в состав разработчиков ПС, осуществляющих машинное обучение (дообучение), и всесторонний контроль – это прерогатива заказчика и разработчика системы. Угрозы подмены и/или модификации ММО слабоактуальны, риски пренебрежимо малы;

- вариант 2 (распространенный) – разработчики ПС, осуществляющие машинное обучение (дообучение), принадлежат сторонним организациям относительно разработчика системы, использующей СИИ. Взаимоотношения заказчик – разработчик для этого варианта подробно описаны во введении при обосновании актуальности настоящей работы. В этом случае угрозы становятся актуальными, риски могут оказаться недопустимо большими.

В случае варианта 2 становится остро востребованной предложенная модель для оценки риска невыявления некорректностей в машинном обучении при эксплуатации ПС (см. 5.5.3). Однако здесь, если относительно определения средних времен между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы ($T_{меж}$) и непосредственно самой системной диагностики целостности ($T_{диаг}$)

трудностей не возникает, то с учетом отсутствия какой-либо статистики у аналитика встает правомерный вопрос – как приблизительно можно определить такие исходные данные, как частота возникновения источников угроз возникновения небезопасных версий ПС, при разработке которых были использованы искаженные («отравленные») нарушителем обучающие данные или была осуществлена подмена или модификация ММО (σ), среднее время развития угроз с момента их возникновения до нарушения нормального функционирования моделируемой системы (β), а также среднее время восстановления нарушаемой целостности моделируемой системы ($T_{восст}$). Для ответа на этот вопрос предлагается использование универсальной вспомогательной модели показателя (УВМП) – см. подраздел 2.4 диссертации.

Сегодняшний период развития СИИ в России примечателен тем, что потенциальные угрозы могут быть реализованы главным образом из-за случайных ошибок, нежели из злоумышленных намерений нарушителя. Поэтому есть достаточно высокая уверенность в том, что заказчики систем, использующих СИИ, и организации-разработчики соответствующих ПС не только тщательно подходят к отбору кадров, но и многие математические вопросы по машинному обучению в условиях дефицита высококвалифицированных специалистов решаются сообща (создавая тем самым условия взаимоконтроля). В связи с этим рекомендуется в качестве эталона, ориентированного на УВМП, и начальных границ зон «Приемлемое», «Приемлемое с отклонением», «Неприемлемое» брать те значения, которые характеризуют достижение прагматического эффекта сразу, как только он появляется (по сравнению со случаем функционирования системы без использования СИИ).

С учетом широкомасштабных перспективных работ в области искусственного интеллекта эта ситуация может поменяться буквально через несколько лет. И тогда изначальная версия эталона по УВМП послужит отправной пограничной полосой для обоснованных подозрений о наличии или отсутствии реализации угроз подмены и/или модификации ММО. По мере эксплуатации системы и сбора соответствующей статистики этот изначальный эталон может быть усовершенствован.

Таким образом, в подразделе 5.5 для систем, использующих СИИ, разработаны рекомендации по анализу актуальных угроз подмены ММО (УБИ.222) и модификации ММО путем искажения («отравления») обучающих данных (УБИ.221). В условиях принятых предположений и допущений предложено использовать вероятностные модели для оценки частных рисков невыявления некорректностей в машинном обучении (дообучении) при разработке и эксплуатации ПС, а также метод оценки интегрального риска нарушения корректности машинного обучения в течение задаваемого периода прогноза.

Риск невыявления некорректностей в машинном обучении (дообучении) при разработке ПС предложено оценивать в зависимости следующих исходных данных: объема информации по обучаемым ПС, подлежащего контролю; части важной для принятия решения информации, которая должна быть объективно использована при контроле информации в заданном объеме; скорости контроля; частоты ошибок контроля 1-го рода; среднего времени наработки на алгоритмическую ошибку; периода непрерывной работы контролера; задаваемого времени на контроль информации.

Риск невыявления некорректностей в машинном обучении (дообучении) при эксплуатации ПС предложено оценивать в зависимости следующих исходных данных: частоты возникновения источников угроз возникновения небезопасных версий ПС, при разработке которых были использованы искаженные («отравленные») нарушителем обучающие данные или была осуществлена подмена модели машинного обучения; среднего времени развития угроз с момента их возникновения до нарушения нормального функционирования моделируемой системы; среднего времени между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы; среднего времени системной диагностики целостности моделируемой системы; среднего времени восстановления нарушаемой целостности моделируемой системы; задаваемой длительности периода прогноза. В интересах формирования необходимых исходных данных для последующего моделирования предложено использовать универсальную вспомогательную модель показателя (УВМП), адаптированную для анализа рассматриваемых угроз.

Интегральный риск предложено оценивать через виртуальный показатель риска нарушения корректности машинного обучения в условиях рассматриваемых угроз в течение задаваемого периода прогноза в зависимости от рисков невыявления некорректностей в машинном обучении (дообучении) при разработке и эксплуатации ПС, а через них – в зависимости от исходных данных, обеспечивающих расчет соответствующих рисков.

Рекомендованный в 5.5 подход позволяет осуществлять вероятностную оценку корректности обучаемых ПС в системах, использующих СИИ, при их разработке и эксплуатации в условиях потенциальных угроз злоумышленной подмены и/или модификации ММО. Работоспособность предложенного подхода проиллюстрирована примерами. При этом в рамках изложения подхода продемонстрировано расширение аналитических возможностей созданной программной инфраструктуры путем добавления другой модели.

5.6 Рекомендации по упреждающему управлению рисками при проектировании и эксплуатации фармацевтического предприятия [5, 105, 167]

5.6.1 Замысел проведения исследований процессов при проектировании и эксплуатации фармацевтического предприятия

В подразделе разрабатываются рекомендации относительно использования возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии для решения некоторых аналитических задач в стандартизованных процессах в жизненном цикле исследуемой системы. В качестве исследуемой системы выступает гипотетическое фармацевтическое предприятие, поскольку его продукция всегда востребована для человека. Главной социальной целью функционирования фармацевтического предприятия в общем случае является укрепление здоровья граждан. При этом для владельцев предприятия главной экономической целью является извлечение устойчиво приемлемого эффекта от эксплуатации предприятия путем удержания различных рисков в допустимых пределах. К эффектам от эксплуатации предприятия могут быть отнесены непосредственно активная вовлеченность в решение экономических проблем региона и страны (т.е. полезность для общества), получение прибыли, развитие бизнеса и др. Это - основные аргументы в понимание «успешности» бизнеса. Разрушение бизнеса по какой-либо причине рассматривается владельцами и иными заинтересованными сторонами как «неуспех» предприятия.

Примечание. На практике разрушение бизнеса осуществляется, как правило, путем вынужденного банкротства предприятия.

Без ограничения общности применительно к проектированию и эксплуатации моделируемой системы рассматриваются процессы (см. раздел 1, ГОСТ Р 57193-2025):

- системного анализа (для достижения цели процесса - удовлетворения аналитических потребностей заинтересованных сторон в поддержке принятия актуальных решений в течении жизненного цикла создаваемой (модернизируемой) системы);

- управления человеческими ресурсами (для достижения цели процесса - обеспечения конкретной системы человеческими ресурсами, необходимыми и достаточными для достижения ее целей на протяжении жизненного цикла);

- управления качеством (для достижения цели процесса - удовлетворения организационным и проектным целями в области качества с достижением требуемой удовлетворенности заказчика и пользователей системы);

- управления рисками (для достижения цели процесса - своевременной идентификации рисков, обоснования и реализации эффективных упреждающих мер по снижению рисков или их удержанию в допустимых пределах).

В качестве основных рассматриваемых подсистем (элементов) моделируемой сложной системы фармацевтического предприятия рассматриваются:

- подсистема (элемент) 1 организации и обеспечения производства;

- подсистема (элемент) 2 службы главного инженера, обеспечения энергетической, экологической и пожарной безопасности;

- подсистема (элемент) 3 финансового обеспечения и обеспечения экономической безопасности;

- подсистема (элемент) 4 обеспечения качества, стандартизации, метрологии, кадрового обеспечения;

- подсистема (элемент) 5 обеспечения автоматизации производства, связи и компьютерного сопровождения, обеспечения информационной безопасности;

- подсистема (элемент) 6 юридического обеспечения, соблюдения и защита прав собственности;

- подсистема (элемент) 7 обеспечения ресурсами и материалами, складского хранения, логистического обеспечения;

- подсистема (элемент) 8 обеспечения маркетинга, сбыта продукции, рекламы, связи с обществом.

На основе сформированных правдоподобных исходных данных рассмотрены шесть актуальных примеров, сфокусированных на прогнозировании различных рисков, связанных с разрушением бизнеса фармацевтического предприятия в течение задаваемого периода прогноза. В условиях разнородных угроз в качестве основного пространства элементарных состояний (событий) в моделируемых системах используются два альтернативных состояния: «бизнес предприятия находится в приемлемом состоянии» и «бизнес предприятия находится в критичном состоянии разрушения», в т.ч. на уровне отдельных подсистем моделируемой системы. Эти элементарные состояния «приемлемого состояния» и «разрушения бизнеса» в полной мере аналогичны соответственно состояниям «успеха» и «неудачи» определенным выше.

Каждый отдельный элемент – это «черный ящик» без резервирования. В качестве исходных для моделирования отдельного элемента («черного ящика») для всех примеров 1-6 выступают следующие исходные данные: частота возникновения источников угроз (σ); среднее время развития угрозы до ее реализации в виде нарушения целостности элемента (β); время между окончанием предыдущей и началом очередной диагностики целостности элемента ($T_{меж}$); длительность диагностики элемента ($T_{диаг}$); среднее время восстановления нарушенной целостности элемента ($T_{восст}$); длительность периода прогноза. Условная нумерация составных сущностных подсистем (элементов) введена в интересах

формализованного моделирования и понимания последующих ссылок в примерах этого подрапздела.

Согласно замыслу проведения системных исследований в первом примере 1-5.6 этого подраздела (см. 5.6.2) структура моделируемой сложной системы рассматривается в виде, отраженном на рис. 5.36.

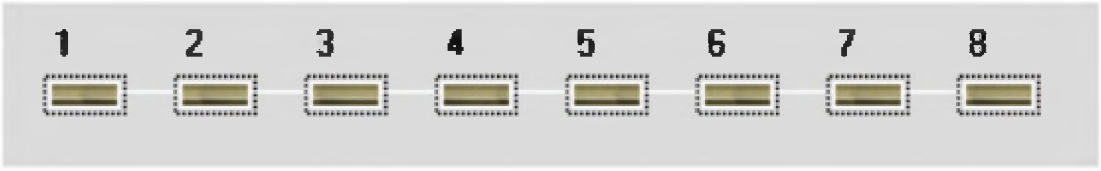


Рис. 5.36 Структура моделируемой системы примера 2

Моделируемая система состоит из 8 перечисленных выше подсистем, в терминах формализации каждая подсистема примера 1-5.6 – это элемент, представляющий собой «черный ящик» без резервирования. Подсистемы логически объединяются союзом «И», т.е. система работоспособна, если только работоспособна каждая подсистема (в примере 1 – если работоспособен каждый из восьми элементов). Т.е. успех предприятия зависит в первую очередь от успеха работы каждой подсистемы элемента подсистемы. И наоборот, основные риски – в подсистемах. Сначала выбрана именно эта упрощенная модель, когда сущность каждой подсистемы проявляется без учета какой-либо дополнительной взаимоувязанной целенаправленной поддержки со стороны руководства предприятием. В случае успешной работы поощряются те подсистемы, условный вес которых в достижении общего успеха максимален, а сопутствующие риски – минимальны. При этом интегрирующее управление со стороны руководства сводится к неким организационным формальностям, а по делу - к тому, чтобы не мешать работе подсистем, т.е. руководство - пассивно. Именно поэтому пример 1 с точки зрения формализации характеризуется так: «составные подсистемы – «черные ящики», пассивное управление предприятием». В примере осуществляется прогноз рисков разрушения бизнеса на интегральном уровне системы в целом. Также рассчитывается весовой вклад в этот интегральный риск со стороны сущностей каждого из составных элементов.

Неучет в первом примере механизма резервирования для элементов системы, когда таковой механизм в реальности присутствует, это весьма огрубленное представление действительности для моделирования. Действительно, в реальности с формальной точки зрения функционирование каждой составной подсистемы (элемента) 1 – 8 моделируемой системы поддерживается некоторым резервированием. Резервирование проявляется в том, что работоспособность каждой подсистемы (элемента) поддерживается несколькими работниками этой подсистемы.

В связи с этим согласно замыслу системных исследований далее для сравнения с первым примером (по структуре ) рассмотрены примеры 2-5.6 и 3-5.6 (см. соответственно 5.6.3 и 5.6.4).

Пример 2-5.6 – для каждого элемента системы характерно двукратное резервирование в моделируемой системе. Двукратность резервирования - это формальное положение о запасном приемлемом варианте выполнения каждой функции подсистемы (пример – замена заболевшего работника другим здоровым на время болезни). Структура и логические компоненты моделируемой системы примера 2-5.6 представлены на рис. 5.37. При этом роль руководства предприятия – пассивная. Поэтому пример 2-5.6 с точки зрения формализации характеризуется так: «составные подсистемы – «черные ящики» с двукратным резервированием, пассивное управление предприятием».

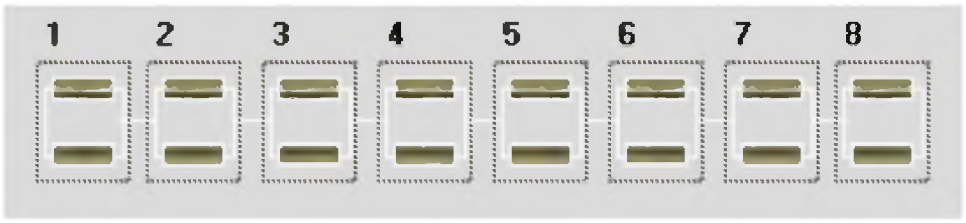


Рис. 5.37 Структура и логические компоненты моделируемой системы примера 2-5.6

Целостность моделируемой системы систем достигается, если обеспечена целостность каждой из восьми составных подсистем. В свою очередь, целостность i-й составной подсистемы (i=1,…,8) обеспечена, если обеспечена целостность ИЛИ одного, ИЛИ другого элемента этой составной системы. Элементы – те же, что в примере 1.

Пример 3-5.6 – для каждого подсистемы характерно трехкратное резервирование в моделируемой системе. Трехкратность резервирования элементов в подсистеме - это формальное положение о двух запасных приемлемых вариантах выполнения каждой функции подсистемы. Структура и логические компоненты моделируемой системы примера 2-5.6 представлены на рис. 5.38. При этом рассматриваемая роль руководства предприятия – по-прежнему пассивная. Поэтому пример 3-5.6 с точки зрения формализации характеризуется так: «составные подсистемы – «черные ящики» с трехкратным резервированием, пассивное управление предприятием».

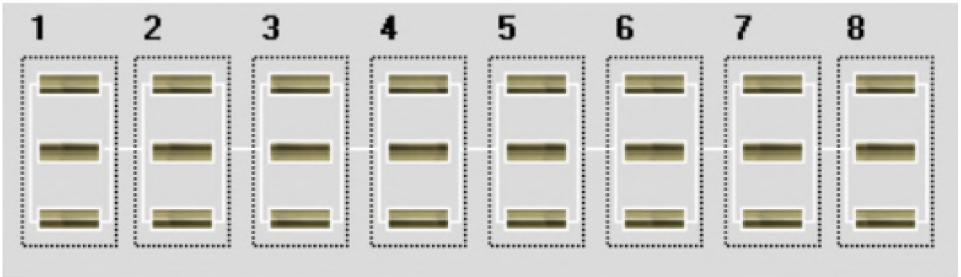


Рис. 5.38 Структура и логические компоненты моделируемой системы примера 3-5.6

Целостность моделируемой системы достигается, если обеспечена целостность каждой из восьми составных подсистем. В свою очередь, целостность i-й составной подсистемы (i = 1,…,8) обеспечена, если обеспечена целостность ИЛИ одного, ИЛИ второго, ИЛИ третьего элемента этой составной подсистемы. Элементы – те же, что в примерах 1-5.6, 2-5.6.

Примечание. Без ограничения общности разработанные программные, технологические и методические решения и созданная инфраструктура поддержки риск-ориентированной системной инженерии позволяет рассматривать более сложные структуры, нежели рассматриваемое двукратное и трехкратное резервирование с учетом .

Согласно замыслу в развитие примеров 1 – 3 в примерах 4 - 6 дополнительно учтено эффективное управление со стороны Руководства предприятия (см. 5.6.5 – 5.6.7). Под Руководством предприятия при формализации понимается генеральный директор предприятия и совет директоров предприятия (каждый директор отвечает за одну или несколько подсистем). Именно от рационального управления рисками, обоснованных и своевременных решений Руководства по возникающим проблемам, вызовам и угрозам и их воплощений зависит долговременная успешность предприятия. Т.е. формально, благодаря оперативным решениям, своими организационно-практическими действиям активное Руководство предприятия способно выступить как резервирующий элемент в режиме реального времени функционирования предприятия.

Оценки в примерах 4 - 6 призваны продемонстрировать по вероятностной шкале, насколько велико влияние Руководства предприятия в моделируемых системах в сравнении с расчетными рисками примеров 1 – 3 (в которых рассмотрен случай, когда при пассивном управлении со стороны Руководства предприятия основные решения в системе находятся в самоуправление руководителей подсистем).

Пример 4-5.6 – активное Руководство предприятия и восемь элементов из примера 1

(эти элементы располагаются внизу на рис. 5.39), формально резервирующие друг друга, рассматриваются как единая моделируемая система (структура – внутри системы). При проведении расчетов главный элемент сверху является формализованным аналогом Руководства предприятия. Структура и логические компоненты моделируемой системы систем примера 4, рассматриваемой в целом, представлены на рис. 5.39. Пример 4-5.6 с точки зрения формализации характеризуется так: «составные подсистемы – «черные ящики», активное управление предприятием». Смысл примера 4-5.6 состоит в том, чтобы оценить, насколько меняются расчетные риски в сравнении с примером 1-5.6, а также в сравнении с примерами 2-5.6 и 3-5.6.

Рис. 5.39. Структура и логические компоненты моделируемой системы примера 4-5.6

Пример 5-5.6 – активное Руководство предприятия и восемь составных подсистем с двукратным резервированием элементов (см. рис. 5.40), формально резервирующие друг друга, рассматриваются как единая моделируемая система (Руководство предприятия – это верхний элемент аналогично примеру 4-5.6). Структура и логические компоненты моделируемой системы примера 5-5.6, рассматриваемой в целом, представлены на рис. 5.40. Смысл примера 5-5.6 состоит в том, чтобы оценить, насколько меняются расчетные риски в сравнении с примером 2-5.6, а также в сравнении с примером 4-5.6. Пример 5-5.6 с точки зрения формализации характеризуется так: «составные подсистемы – «черные ящики» с двукратным резервированием, активное управление предприятием».

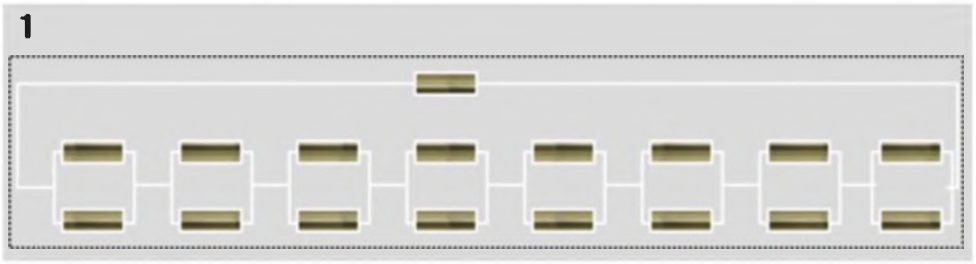


Рис. 5.40 Структура и логические компоненты моделируемой системы примера 5-5.6

Пример 6-5.6 – активное Руководство предприятия и восемь составных подсистем с трехкратным резервированием элементов (см. рис. 5.41), формально резервирующие друг друга, рассматриваются как единая моделируемая система (Руководство предприятия – это верхний элемент аналогично примерам 4-5.6, 5-5.6). Структура и логические компоненты моделируемой системы примера 6-5.6, рассматриваемой в целом, представлены на рис. 5.41.

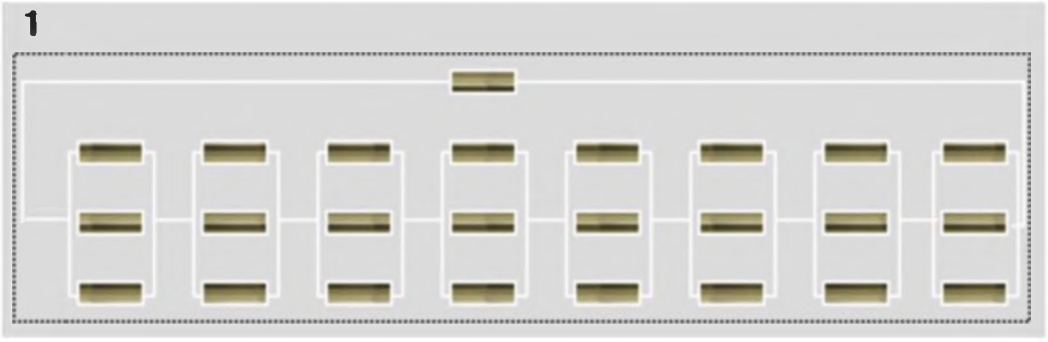


Рис. 5.41 Структура и логические компоненты моделируемой системы примера 6

Смысл примера 6-5.6 состоит в том, чтобы оценить, насколько меняются расчетные риски в сравнении с примерами 2-5.6 и 3-5.6, а также в сравнении с примерами 4-5.6, 5-5.6. Пример 6-5.6 с точки зрения формализации характеризуется так: «составные подсистемы – «черные ящики» с трехкратным резервированием, активное управление предприятием».

5.6.2 Пример 1-5.6, составные подсистемы – «черные ящики», пассивное управление предприятием

Пример 1-5.6 рассмотрен для системы из восьми элементов, каждый элемент – это «черный ящик» без резервирования – см. рис. 5.36. Условная нумерация составных сущностных элементов введена в интересах формализованного моделирования и последующих ссылок в примерах 1-6. Исходные данные для моделирования по каждому из рассматриваемых элементов с необходимыми пояснениями отражены в таблице 5.6.

Таблица 5.6 Усредненные исходные данные для моделирования

Подсистема (элемент) системы	Частота угроз σ	Среднее время развития угроз β	Период между диагностиками $T_{меж}$	Длительность диагностики $T_{диаг}$	Среднее время восстановления целостности $T_{восст}$
1 – организация и обеспечение производства	0.05 р/год (это - частота возникновения критичных событий для бизнеса в России, оценивается в среднем как один раз в 20 лет. К таковым относятся революционные события, возникновение региональных конфликтов)	10 лет (это - среднее время развития угроз бизнесу, т.е. при непринятии за этот срок действенных мер противодействия угрозам бизнес прекращает свое существование или уходит)	6 лет (этот период сравним с одним сроком правления Президента страны и Правительства. Президент предлагает новые способы противодействия угрозам бизнесу, вырабатывает стратегический план на период своего правления)	2 мес. (этот срок сравним с законодательным сроком введения в действие указов Президента страны и постановлений Правительства)	3 года (это – среднее время реализации важных решений в стране после начала разрешения критичных проблем для бизнеса)
2 – служба главного инженера, энергетическая, экологическая и пожарная безопасность	1 р/год (это – соизмеримо с ежегодными подведениями итогов и достижений в выполнении планов работы предприятия)	5 лет (этот срок на год меньше одного срока правления Президента страны и Правительства и учитывает возможные неблагоприятные события для службы главного инженера, угрозы для энергетической, экологической и пожарной безопасности)	1 нед. (это – средний срок между постановками проблем на предприятии в осмыслении новых вызовов и угроз, связанных с возможными неблагоприятными событиями для службы главного инженера, угрозами для энергетической, экологической и пожарной безопасности)	1 день (это – средний срок дискуссий при принятии решений по новым вызовам и угрозам, связанным с возможными неблагоприятными событиями для службы главного инженера, проблемами для энергетической, экологической и пожарной безопасности)	1 год (это – среднее время получения важных для предприятия положительных результатов после принятия решений по реакции на появляющиеся новые вызовы и угрозы для службы главного инженера, энергетической, экологической и пожарной безопасности)
3 – финансовое обеспечение, экономическая безопасность	0.1 р/год (с учетом начального капитала, сложившейся стабильности и объективной востребованности фармацевтической продукции	6 лет (это среднее время развития угроз до наступления негативных последствий для бизнеса, оно сравнимо с одним сроком правления	1 год (в среднем это – ежегодный срок подведения итогов и достижений в выполнении планов работы предприятия, а также сверки с курсом Президента	1 мес. (это – средний срок подготовки отчетов по выполнению планов предприятия)	3 года (это – среднее время получения важных результатов после реакции на выявленные или реализованные угрозы финансовому обеспечению и экономической

	положено, что угрозы финансо-вому обеспечению и экономической безопасности возникают в среднем 1 раз в 10 лет)	Президента страны и Правительства)	страны и Правительства)		безопасности предприятия)
4 – обеспечение качества, стандартизация, метрология, кадровое обеспечение	0.3 р/год (в среднем из-за разных причин частота возникновения критичных угроз нарушения качества продукции, в т.ч. из-за низкой квалификации или отсутствия кадров оценивается как 3 раза за 10 лет)	2 года (это - среднее время развития критичных угроз до наступления негативных последствий из-за нарушения качества продукции)	1 мес. (в среднем это - периодичность критичного анализа состояния на предприятии - 1 раз в месяц)	1 нед. (это – средний срок разбора проблем на предприятии при возникновении критичных угроз нарушения качества продукции)	1 год (это – среднее время восстановления нарушенного качества продукции при реализации критичных угроз)
5 – автоматизация производства, связь и компьютерное сопровождение, обеспечение информационной безопасности	0.2 р/год (в среднем каждые 5 лет возникают новые вызовы и угрозы для АСУ ТП, связи, угрозы информационной безопасности на предприятии, в т.ч. из-за не решенной в полной мере проблемы импортозамещения	3 года (если никак 3 года не реагировать на появляющиеся вызовы и угрозы, происходят негативные последствия – возникают технологические отказы и сбои, безвозвратно теряются технологии, возникают новые угрозы)	6 мес. (в среднем это - срок, через который осуществляется системный контроль состояния автоматизации производства, связи и компьютерного сопровождения, обеспечения информационной безопасности)	1 мес. (это – средний срок подготовки отчетности на предприятии по результатам системного контроля)	1 год (это – среднее время получения важных для предприятия положительных результатов после принятия решений по реакции на появляющиеся новые вызовы и угрозы для АСУ ТП, связи, угрозы информационной безопасности)
6 – юридическое обеспечение, соблюдение и защита прав собственности	1 р/год (это – соизмеримо с частотой возникновения различных юридических споров и судебных исков к предприятию)	5 лет (это - среднее время судебного разбирательства до окончательного разрешения юридических споров и судебных исков к предприятию)	1 мес. (в среднем это - периодичность критичного анализа возникающих споров и судебных исков к предприятию)	1 нед. (это – средний срок подготовки документов для разрешения каждого из юридических споров и судебных исков к предприятию)	1 год (это – среднее время восстановления после разрешения каждого из юридических споров и судебных исков к предприятию)
7 – обеспечение ресурсами и материалами, складское хранение, логистическое обеспечение	0.05 р/год (это - частота возникновения критичных событий для бизнеса в России, оценивается в среднем как один раз в 20 лет. К таковым относятся революционные события, возникновение региональных конфликтов)	6 лет (это среднее время развития угроз до наступления негативных последствий для бизнеса, оно сравнимо с одним сроком правления Президента страны и Правительства)	1 год (в среднем это – ежегодный срок подведения итогов и достижений в выполнении планов работы предприятия)	2 мес. (этот срок сравним с законодательным сроком введения в действие указов Президента страны и постановлений Правительства, затрагивающих обеспечение ресурсами и материалами, складское хранение, логистическое обеспечение)	3 года (это – среднее время получения важных для предприятия положительных результатов после принятия решений по реакции на появляющиеся новые вызовы и угрозы для обеспечения ресурсами и материалами, складского хранения, логистического обеспечения)
8 – маркетинг, сбыт продукции, реклама, связь с обществом	0.1 р/год (это – соизмеримо с ежегодными подведениями итогов и достижений в выполнении планов работы предприятия)	10 лет (это - среднее время развития угроз бизнесу, т.е. при непринятии за этот срок действенных мер противодействия угрозам бизнес прекращает свое существование или уходит)	1 год (в среднем это – ежегодный срок подведения итогов и достижений в выполнении планов работы предприятия)	3 мес. (этот срок сравним с законодательным сроком введения в действие указов Президента страны и постановлений Правительства, затрагивающих маркетинг, сбыт, реклама, связь с обществом)	10 лет (это – среднее время получения заметных результатов целенаправленной работы предприятия в области маркетинга, сбыта, рекламы, связи с обществом после реализации угроз бизнесу)

Требуется спрогнозировать риски разрушения бизнеса.

Результаты расчетов рисков разрушения бизнеса в примере 1-5.6 на уровне частных рисков по сущностям каждого из составных элементов (1, 2, …, 8) и на уровне интегрального риска (1..8) в условиях разнородных угроз за 6 лет прогноза отражены на рис. 5.42. Длительность прогнозного периода от 3-х до 12 лет для моделируемой системы систем сравнима с одним-двумя сроками правления Президента и Правительства РФ. Президент предлагает новые способы противодействия угрозам бизнесу, вырабатывает стратегический план на период своего правления.

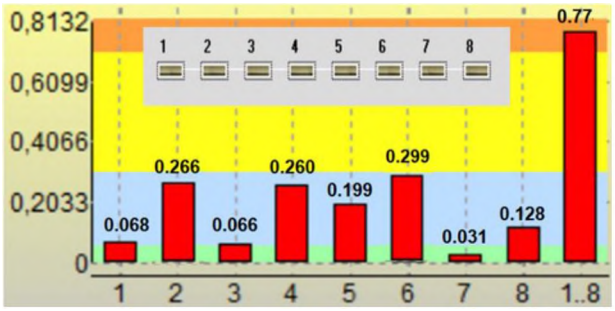


Рис. 5.42 Риски разрушения бизнеса за 6 лет прогноза для примера 1-5.6

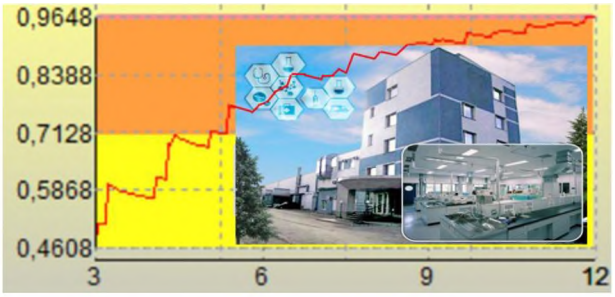


Рис. 5.43 Зависимость интегрального риска разрушения бизнеса при прогнозе на 3–12 лет

Анализ показал, что на множестве введенного пространства элементарных событий интегральный уровень риска разрушения бизнеса (0.77) за 6 лет прогноза более, чем в 3 раза превышает вероятность 0.23 сохранения приемлемого состояния бизнеса (0.23 = 1 – 0.77). При этом в условиях примера 1-5.6 (см. таблицу 5.6) наибольший вес в интегральный риск вносят риски для элементов 2, 4, 5, 6 (см. рис. 5.42):

- риск для «службы главного инженера, обеспечения энергетической, экологической и пожарной безопасности» (элемент 2), оцениваемый на уровне 0.266;

- риск для «обеспечения качества, стандартизации, метрологии, кадрового обеспечения» (элемент 4), оцениваемый на уровне 0.260;

- риск для «обеспечения автоматизации производства, связи и компьютерного сопровождения, обеспечения информационной безопасности» (элемент 5), оцениваемый на уровне 0.199;

- - риск для «юридического обеспечения, соблюдение и защита прав собственности» (элемент 6), оцениваемый на уровне 0.299.

Примечание. Чтобы не было заблуждений, подчеркнем - интегральный риск не равен сумме частных рисков, для понимания этого см. модели и методы в разделе 2 диссертации.

Дополнительное прогнозирование интегрального риска на 3-12 лет показало, что в течение трех лет прогноза разрушение бизнеса в моделируемой системе столь же вероятно, как

и его сохранение в приемлемом состоянии – см. рис. 5.43. Более того, при рассматриваемом сценарии развития событий и пассивном управлении в период с 7-го по 12-й годы прогноза разрушение духовно-нравственных ценностей в стране становится практически неизбежным с вероятностью 0.80 – 0.96. Что-то подобное на практике Россия ощущала в конце 90-х годов, негативные последствия того тяжелого времени для сохранения устойчивого бизнеса ощущаются до сих пор.

Примечание. Пилообразность траектории на рис. 5.43 связана с периодом между диагностиками, длительностью диагностики и временем восстановления нарушаемой целостности отдельных элементов моделируемой системы. Диагностика проведена, меры приняты – риск снижается, до следующей диагностики в условиях возможных угроз риски возрастают.

В целом сделанные расчеты при огрубленном моделировании в примере 1-5.6 свидетельствуют о практически недостаточной эффективности мер противодействия ожидаемым угрозам для сохранения бизнеса в приемлемом состоянии. Путем сопоставления с реальными событиями в России 90-х и в западном обществе в наше время получены количественные представления об уровне вероятности того, когда разрушение бизнеса становится практически неизбежным (это - вероятность на уровне 0.80 – 0.96 для сценарных условий примера, которая, согласно зависимости на рис. 5.43, достигается на 7-й год прогнозного периода).

Наряду с некоторой практичностью полученных результатов примера 1-5.6 не следует забывать о весьма огрубленном представлении действительности с помощью «черных ящиков» без резервирования. В реальности с формальной точки зрения функционирование каждого элемента моделируемой системы поддерживается многократным разносторонним резервированием для каждой из рассматриваемых подсистем предприятия. В связи с этим ниже рассмотрены примеры, учитывающие соответственно двух- и трехкратное резервирование в моделируемой системе. Поскольку кратность резервирования неясна для различных фармацевтических предприятий и регионов, где они работают (в реальности в различных регионах, где отсутствует кадровая проблема, кратность резервирования может превышать трехкратный уровень), последующие примеры дадут более точное представление об уровне достигаемых рисков.

5.6.3 Пример 2-5.6, составные подсистемы - «черные ящики» с двукратным резервированием, пассивное управление предприятием

В качестве моделируемой рассматривается система из восьми составных подсистем, каждая составная подсистема – это идентичные по функциональной сути те же элементы, что в примере 1-5.6, с добавлением взаимного резервирования (

).

Структура и логические компоненты моделируемой системы систем примера 2-5.6 представлены на рис. 5.37 с учетом пояснений в 5.6.1. Смысл резервирования – в том, что содержание целостности составной подсистемы обеспечивается, как минимум, двумя различными способами через возможности самой подсистемы. Каждый элемент в составных подсистемах 1,…, 8 – это «черный ящик» с соответствующими характеристиками по таблице 5.6 (как и в примере 1-5.6). Осуществляется прогноз рисков разрушения бизнеса в моделируемой системе как на интегральном уровне в целом, так и на уровне сущностей каждой из составных подсистем.

Результаты расчетов рисков разрушения бизнеса в примере 2-5.6 на уровне сущностей каждой из составных подсистем (1, 2, …, 8) и на интегральном уровне (1..8) в условиях разнородных угроз за 6 лет прогноза отражены на рис. 5.44.

Примечание. Составные подсистемы и элементы также могут представлять собой сложную систему, моделирование которой возможно с использованием созданной инфраструктуры поддержки риск-ориентированной системной инженерии. Так, на рис. 5.44 подсистема 5 (обеспечения автоматизации производства, связи и компьютерного сопровождения, обеспечения информационной безопасности) может функционально представлять собой АСУ ТП, основными ее подсистемами при более детальном моделировании могут быть рассмотрены: подсистемы варки, подработки, брожения, бардосушки, вентиляции, упаковки, управления разгонной колонной брагоректификационной установки (БРУ), рабочие места инженеров, подсистемы доступа в Интернет и др.

Требуется спрогнозировать риски разрушения бизнеса в сценарных условиях, отраженных в таблице 5.6 для каждого из элементов.

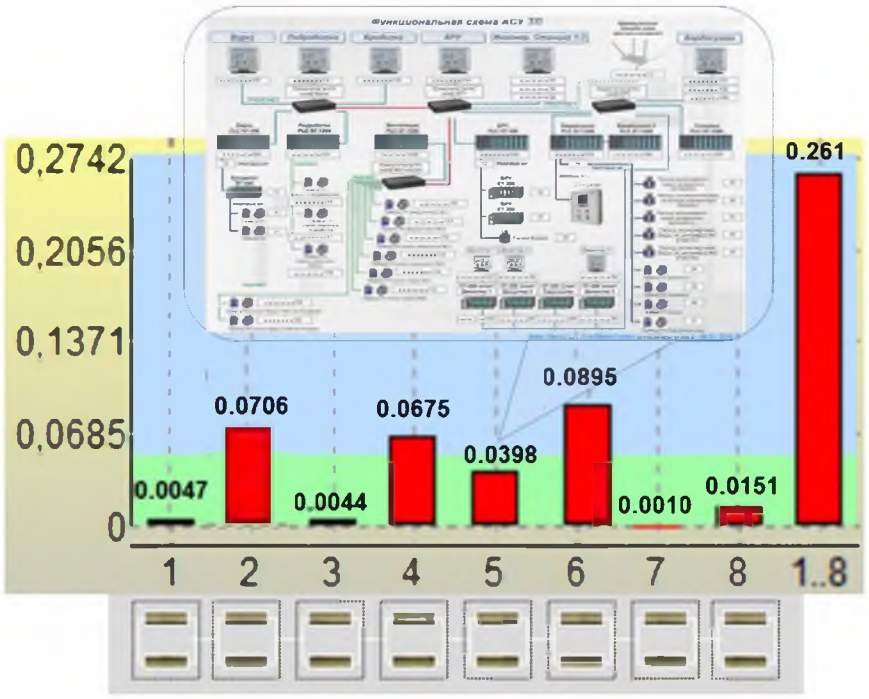


Рис. 5.44 Риски разрушения бизнеса за 6 лет прогноза для примера 2-5.6

Анализ показал, что интегральный уровень риска разрушения бизнеса 0.261 за 6 лет прогноза приблизительно в 3 раза ниже в сравнении с вероятностью 0.739 сохранения бизнеса на приемлемом уровне (0.739 = 1 – 0.261). Более того, интегральный риск (0.261) для примера 2 втрое ниже по сравнению с интегральным риском 0.77 для примера 1-5.6. Именно в этом проявляется более высокая точность моделирования на уровне двукратного резервирования по каждому из элементов. При этом в условиях примера 2-5.6 наибольший вес в интегральный риск вносят риски для составных систем 2, 4, 6 (см. рис. 5.44), которые в абсолютном выражении малы:

- риск для «службы главного инженера, обеспечения энергетической, экологической и пожарной безопасности» (составная подсистема 2), оцениваемый на уровне 0.0706;

- риск для «обеспечения качества, стандартизации, метрологии, кадрового обеспечения» (составная подсистема 4), оцениваемый на уровне 0.0675;

- риск для «юридического обеспечения, соблюдение и защита прав собственности» (составная подсистема 6), оцениваемый на уровне 0.0895.

Дополнительное прогнозирование интегрального риска на 3-12 лет показало, что, если в качестве приемлемого ориентироваться на уровень допустимого риска 0.2, то в течение пяти с половиной лет разрушения бизнеса в моделируемой системе систем не ожидается (т.е. риск на превысит допустимого уровня 0.2), а, начиная с 9-го года, интегральный риск разрушения бизнеса начнет превышать уровень 0.5 и в течение 12 лет прогноза достигнет уровня 0.72 – см. рис. 5.45. При рассматриваемом сценарии развития событий можно констатировать, что в течение пяти с половиной лет прогноза угрозы разрушения бизнеса для предприятия будут нейтрализованы с вероятностью не ниже 0.80 (за счет использования хотя бы двух различных способов противодействия угрозам в каждой из подсистем). Это внушает некоторый оптимизм в отношении мер ведения бизнеса при характеристиках воздействующих факторов по таблице 5.6.

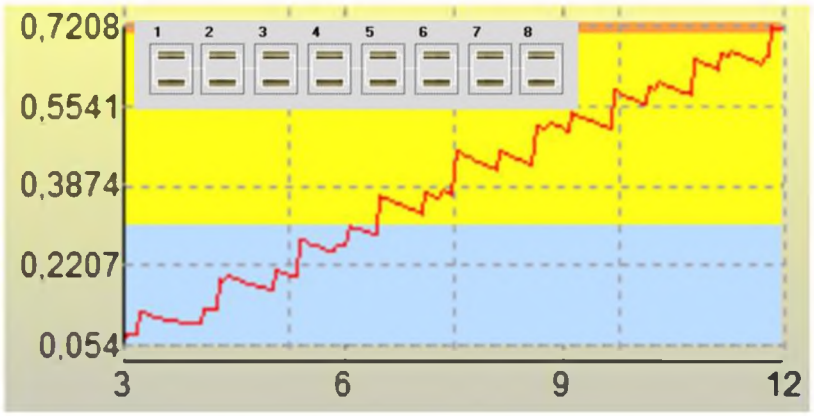


Рис. 5.45 Зависимость интегрального риска разрушения бизнеса при прогнозе на 3–12 лет (пример 2-5.6)

В целом сделанные расчеты свидетельствуют с одной стороны об уверенности в сохранении бизнеса в течение 5.5 лет, а с другой стороны - о возникновении повышенной неопределенности в противодействии ожидаемым угрозам для сохранения бизнеса в конце 12-летнего срока прогноза.

Таким образом, в примере 2-5.6 в сравнении с результатами примера 1 получены количественные представления о несколько более точных количественных оценках реального уровня риска разрушения бизнеса для рассматриваемого предприятия. Вместе с тем, поскольку кратность резервирования до конца неясна, далее в примере 3-5.6 оценим степень снижения реального уровня риска за счет трехкратного логического резервирования при моделировании.

5.6.4 Пример 3-5.6, составные подсистемы - «черные ящики» с трехкратным резервированием, пассивное управление предприятием

В качестве моделируемой рассматривается система из восьми составных подсистем, каждая составная подсистема – это идентичные по существу те же элементы, что в примерах 1 и 2, с взаимным трехкратным резервированием (). Структура и логические компоненты моделируемой системы примера 3 представлены на рис. 5.38 с учетом пояснений в 5.6.1. Каждый элемент в составных подсистемах 1,…, 8 – это «черный ящик» с соответствующими характеристиками по таблице 5.6 (как и в примерах 1-5.6, 2-5.6). Осуществляется прогноз рисков разрушения бизнеса в моделируемой системе как на интегральном уровне в целом, так и на уровне сущностей каждой из составных подсистем.

Результаты расчетов рисков разрушения бизнеса в примере 3-5.6 на уровне сущностей каждой из составных подсистем (1, 2, …, 8) и на интегральном уровне (1..8) в условиях разнородных угроз за 6 лет прогноза отражены на рис. 5.46.

Анализ показал, что интегральный уровень риска разрушения бизнеса 0.0715 за 6 лет прогноза более, чем в 3.6 раза ниже в сравнении с вероятностью 0.261 при двукратном резервировании в примере 2 и почти в 11 раз ниже в сравнении с вероятностью 0.77 при отсутствии резервирования в примере 1. Т.е. более детальное моделирование с учетом трехкратного резервирования по каждому из элементов проявляется в более точных оценках. В условиях примера 3 частные риски для каждой из составных систем 1, …, 8 не превышают 0.03. При этом достигаемая вероятность сохранения бизнеса на приемлемом уровне риска 0.9285 в 13 раз превышает вероятность разрушения бизнеса 0.0715=1–0.9285 (см. рис. 5.46).

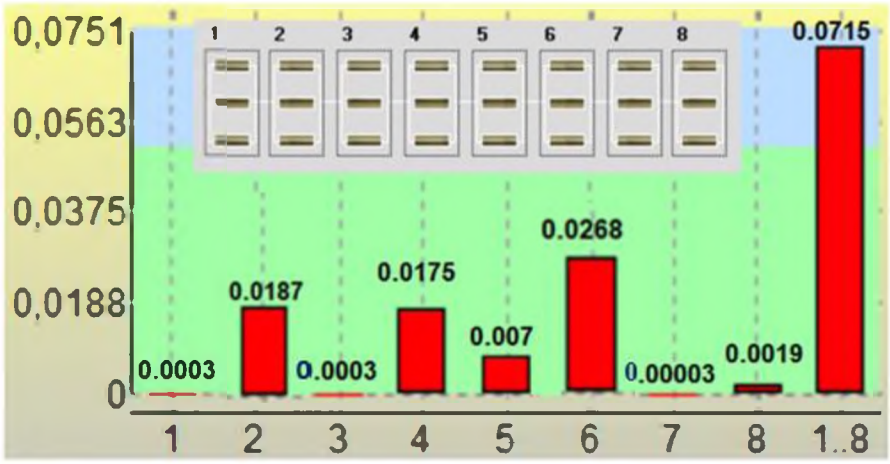


Рис. 5.46 Риски разрушения духовно-нравственных ценностей за 6 лет прогноза (пример 3-5.6)

Дополнительное прогнозирование интегрального риска на 3-12 лет показало, что в течение 8 лет разрушения бизнеса в моделируемой системе не ожидается (риск на превысит допустимого уровня 0.2), а к концу 12-го года прогноза риск не превысит 0.45 – см. рис. 5.47. Т.е. вероятность «успеха» устойчиво превосходит риск «неудачи».

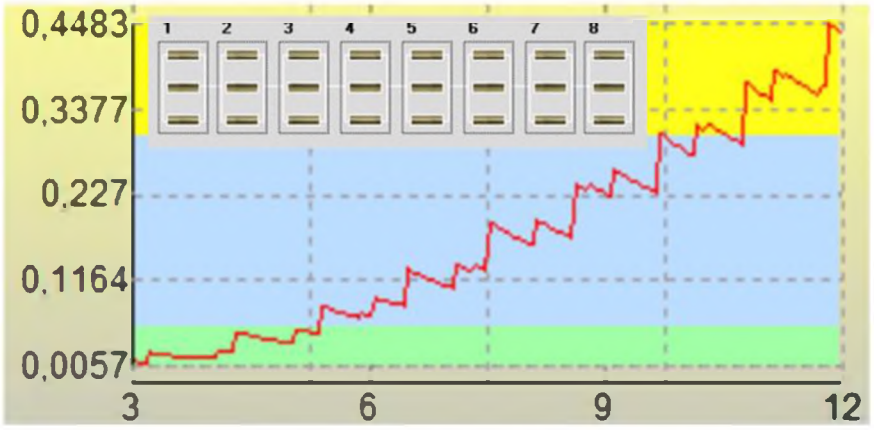


Рис. 5.47 Зависимость интегрального риска разрушения бизнеса при прогнозе на 3–12 лет (пример 3-5.6)

При рассматриваемом сценарии развития событий можно констатировать, что в течение восьми лет прогноза угрозы разрушения бизнеса будут нейтрализованы с вероятностью не ниже 0.80 (за счет использования, как минимум, трех различных способов противодействия угрозам в каждой из подсистем). Это внушает умеренный оптимизм в отношении мер сохранения бизнеса предприятия в моделируемой системе.

В целом сделанные расчеты свидетельствуют с одной стороны об уверенности в сохранении бизнеса в течение восьми лет, а с другой стороны - о наличии некоторой неопределенности в противодействии ожидаемым угрозам для сохранения бизнеса в конце

12-летнего срока прогноза при отсутствии какого-либо дополнительного целенаправленного управления рисками.

Таким образом, в примере 3-5.6 в сравнении с результатами примеров 1-5.6 и 2-5.6 получены количественные представления о существенно более точных оценках реального уровня риска разрушения бизнеса предприятия.

Напомним, в примерах 1 – 3 был рассмотрен случай пассивного управления со стороны Руководства предприятия. Далее в примерах 4 - 6 в моделируемых системах исследовано активное управление предприятием со стороны Руководства.

5.6.5 Пример 4-5.6, составные подсистемы – «черные ящики», активное управление предприятием

В моделируемой системе учтено активное управление со стороны «Руководства предприятия» в логической структуре, характеризующей резервирование действий. Структура и логические компоненты моделируемой системы примера 4 представлены на рис. 5.39 ( , главный элемент – сверху, нижние 8 элементов – те же, что в примере 1), каждый элемент – это «черный ящик». Исходные данные для элемента «Руководство предприятия» отражены в таблице 5.7, для остальных элементов - в таблице 5.6.

Таблица 5.7 Усредненные исходные данные для элемента «Руководство предприятия»

Главный элемент системы (сверху)	Частота угроз σ	Среднее время развития угроз β	Период между диагностиками $T^{*}_{меж}$	Длительность диагностики $T^{*}_{диаг}$	Среднее время восстановления целостности $T^{*}_{восст}$
Руководство предприятия	2 р/год (это - частота возникновения угроз глобального масштаба, требующих рассмотрения проблем Руководством предприятия)	1 год (это - среднее время развития угроз глобального масштаба до возникновения неприемлемого ущерба предприятию)	1 неделя (этот период между заседаниями совета директоров предприятия для решения накопившихся вопросов)	3 часа (это время сравнимо с длительность ю заседания совета директоров)	1 месяц (это – среднее время реализации важных решений после принятия решений Руководством предприятия)

Осуществляется прогноз риска разрушения бизнеса на интегральном уровне в целом, который может быть сравнимым с интегральными рисками всех примеров 1-6. Смысл примера 4-5.6 состоит в том, чтобы оценить, насколько меняются расчетные риски в сравнении с примером 1-5.6, а также в сравнении с примерами 2-5.6 и 3-5.6.

Результаты расчетов показали, что интегральный риск разрушения бизнеса в условиях разнородных угроз за 6 лет прогноза составит 0.323 – можно сравнить с 0.77 примера 1-5.6, 0.261 примера 2-5.6 и 0.0715 примера 3-5.6.

Прогнозирование интегрального риска на 3-12 лет показало, что разрушения бизнеса предприятия в моделируемой системе не ожидается в течение четырех лет (риск не превысит уровень 0.2, принятый выше в качестве допустимого), а, начиная с конца 8-го года, риск начнет превышать уровень 0.5 и к концу 12-го года прогноза достигнет уровня 0.64 – см. рис. 5.48.

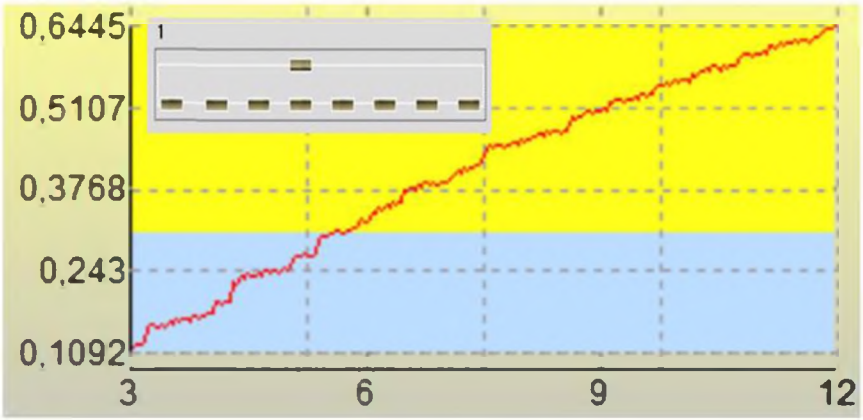


Рис. 5.48 Зависимость интегрального риска разрушения бизнеса при прогнозе на 3–12 лет (пример 4-5.6)

В целом сделанные расчеты свидетельствуют с одной стороны об уверенности в сохранении приемлемого состояния бизнеса в течение 4-х лет, а с другой стороны о возникновении повышенной неопределенности в противодействии ожидаемым угрозам для сохранения бизнеса в конце 12-летнего срока прогноза. Эти выводы сравнимы с выводами для примера 2-5.6, т.е. при самом грубом моделировании эффективность активного управления со стороны Руководства предприятия соизмерима с использованием мер двукратного резервирования по элементам 1,…,8 из примера -5.62.

5.6.6 Пример 5-5.6, составные подсистемы - «черные ящики» с двукратным резервированием, активное управление предприятием

В примере 5-5.6 структура и логические компоненты моделируемой системы представлены на рис. 5.40 ( , главный элемент – сверху, 8 составных подсистем в нижней строке – те же, что в примере 2, учитывающем двукратное резервирование).

В отличие от предыдущего примера в настоящем примере рассматривается более адекватная модель, учитывающая путем двукратного резервирования поддержку целостности восьми элементов нижней строки, характеризующих функциональную суть предприятия (аналогично структуре, рассмотренной в примере 2-5.6). Исходные данные для элемента «Руководство предприятия» отражены в табл. 5.7, для остальных элементов - в таблице5.6.

Результаты расчетов показали, что интегральный риск разрушения бизнеса в условиях разнородных угроз за 6 лет прогноза составит 0.109, т.е. в три раза лучше, нежели 0.323 примера 4-5.6, и в 2.5 раза лучше, нежели 0.261 примера 2, но хуже по сравнению с 0.0715 примера 3-5.6.

Прогнозирование интегрального риска на 3-12 лет показало, что в течение семи лет разрушения бизнеса предприятия в моделируемой системе не ожидается (риск на превысит уровень 0.2, принятый выше в качестве допустимого), а к концу 12-го года прогноза риск достигнет уровня почти 0.48, что соизмеримо с вероятностью сохранения бизнеса на приемлемом уровне – см. рис. 5.49.

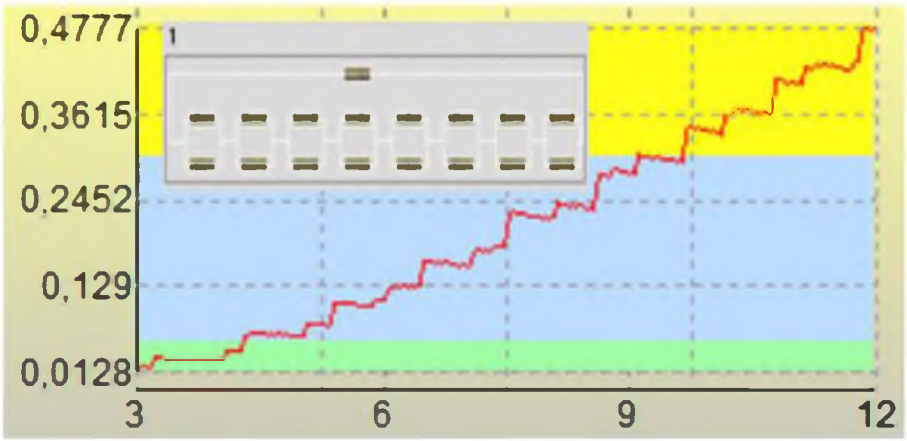


Рис. 5.49 Зависимость интегрального риска разрушения бизнеса при прогнозе на 3–12 лет (пример 5-5.6)

В целом сделанные расчеты свидетельствуют с одной стороны об уверенности в сохранении бизнеса в течение 7 лет, а с другой стороны - о возникновении повышенной неопределенности в противодействии ожидаемым угрозам для сохранения бизнеса в конце 12-летнего срока прогноза. Эти выводы очень близко сравнимы с выводами для примера 3-5.6, т.е. при более точном моделировании в примере 5 установлено, что эффективность активного управления со стороны Руководства предприятия соизмерима с использованием мер трехкратного резервирования по элементам 1,…,8 из примера 3-5.6.

5.6.7 Пример 6-5.6, составные подсистемы - «черные ящики» с трехкратным резервированием, активное управление предприятием

В примере 6-5.6 структура и логические компоненты моделируемой системы представлены на рис. 5.32 ( , главный элемент – сверху, 8 составных систем в нижней строке – те же, что в примере 3, учитывающем трехкратное резервирование).

В отличие от примеров 4-5.6 и 5-5.6 это – наиболее адекватная модель, учитывающая путем трехкратного резервирования поддержку целостности всех восьми элементов, характеризующих функциональную суть предприятия. Исходные данные для элемента «Руководство предприятия» отражены в табл. 5.7, для остальных элементов - в таблице 5.6. Смысл примера 6-5.6 состоит в том, чтобы оценить, насколько меняются расчетные риски по мере повышения адекватности моделирования.

Получаемый в результате расчетов прогноз риска разрушения бизнеса на интегральном уровне в целом в сравнении с интегральными рисками всех примеров 1-6 представлен в табл. 5.8.

Анализ показал, что использование наиболее адекватной модели примера 6 дает более реальное представление о достижимом уровне интегрального риска разрушения бизнеса – в вероятностном выражении это уровень около 0.030 в течение 6 прогнозных лет. Соответствующая вероятность сохранения бизнеса на приемлемом уровне в течение 6 лет составит достойные 0.970, что вполне сравнимо с вероятностью надежного функционирования современного оборудования в опасном производстве (см. примеры в разделе 4 диссертации).

Таблица 5.8 Сравнительные интегральные риски по всем примерам

Примеры	Характеристика примеров	**Интегральный риск разрушения** бизнеса / **вероятность сохранения** бизнеса на приемлемом уровне с прогнозом на 6 лет
Пример 1	Учтены 8 элементов, характеризующих функциональную суть предприятия без резервирования действий. Пассивное управление со стороны Руководства предприятия	**0.77/ 0.23**
Пример 2	Учтены 8 подсистем, характеризующих функциональную суть предприятия с двукратным резервированием действий. Пассивное управление со стороны Руководства предприятия	**0.261 / 0.739**
Пример 3	Учтены 8 подсистем, характеризующих функциональную суть предприятия с трехкратным резервированием действий. Пассивное управление со стороны Руководства предприятия	**0.0715 / 0.9285**
Пример 4	Учтена совместная работа элемента «Руководство предприятия» и 8 элементов, характеризующих функциональную суть предприятия без резервирования действий. Активное управление со стороны Руководства предприятия	**0.323 / 0.677**
Пример 5	Учтена совместная работа элемента «Руководство предприятия» и 8 подсистем, характеризующих функциональную суть предприятия с двукратным резервированием действий. Активное управление со стороны Руководства предприятия	**0.109 / 0.891**
Пример 6	Учтена совместная работа элемента «Руководство предприятия» и 8 подсистем, характеризующих функциональную суть предприятия с трехкратным резервированием действий. Активное управление со стороны Руководства предприятия	**0.030 / 0.970**

Прогнозирование интегрального риска на 3-12 лет показало, что разрушения бизнеса предприятия в моделируемой системе не ожидается в течение 10.5 лет (риск на превысит уровень 0.2, принятый выше в качестве допустимого), а к концу 12-го года риск приблизится к уровню 0.3 – см. рис. 5.50.

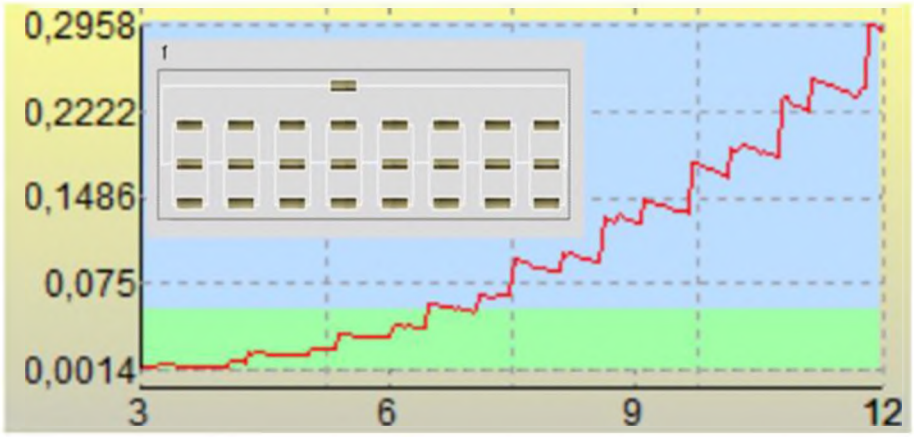


Рис. 5.50 Зависимость интегрального риска разрушения бизнеса при прогнозе на 3–12 лет (пример 6-5.6)

В целом сделанные расчеты свидетельствуют об уверенности в сохранении бизнеса на приемлемом уровне риска в течение 10.5 лет, а с другой стороны о необходимости соблюдения сценарных условий из таблиц 5.6, 5.7, обусловливающих удержание прогнозных рисков на допустимом уровне.

Расчеты при более адекватном моделировании в примерах 3-5.6 и 6-5.6 убедительно показали, что сохранение бизнеса определяется главным образом самими работниками предприятия (их ответственностью и широкой квалификацией для резервирования действий, формализуемыми временными характеристиками) при активном управлении и эффективной поддержке со стороны Руководства предприятия.

Примечание. Имеет смысл отметить, что работа предприятия, характеризуемая исходными данными примера 6-5.6, свойственна фармацевтическим предприятиям семейного бизнеса, где Руководство предприятия, зачастую являющееся его владельцем, заинтересовано не только в устойчивом бизнесе как таковом, но и обладает повышенным чувством ответственности перед обществом и государством.

Таким образом, в подразделе разностороннее применение возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии позволило разработать рекомендации по решению вопросов удержания в допустимых пределах рисков разрушения бизнеса применительно к фармацевтическому предприятию на этапах его проектирования и эксплуатации. Количественно доказано, что эффективность активного управления со стороны Руководства предприятия соизмерима с использованием мер дополнительного резервирования действий применительно ко всем службам организационного управления. Сформулированы условия, определяемые главным образом самими работниками предприятия (их ответственностью и широкой квалификацией для резервирования действий, формализуемыми временными характеристиками) при активном

управлении и эффективной поддержке со стороны Руководства предприятия, обеспечивающие сохранение бизнеса в долговременной перспективе.

5.7 Перспективные направлениях исследований

Проведенные в разделе 1 исследования показали, что в условиях разнородных неопределенностей роль системной инженерии в решении практических задач характеризуется научной фундаментальностью в достижении целей системы за счет оперативного прогнозирования рисков, упреждающего выявления «узких мест» и определения рациональных способов снижения и удержания рисков в допустимых пределах. Место системной инженерии – везде, где возникает потребность в решении задач системного анализа и оптимизации, а также поиска и исследования новых практических идей и возможностей. В последующих разделах 2 – 5 исследования проводились в неразрывной связи системной инженерии с решением задач функционирования, развития и комплексной безопасности сложных систем, подлежащих анализу для обеспечения национальной безопасности России согласно «Стратегии национальной безопасности Российской Федерации». Вместе с тем, в работе удалось лишь приоткрыть инженерный пласт проблем, для разрешения которых может быть использован потенциал научных решений настоящей диссертации. Ниже вкратце перечислены лишь некоторые из приоритетных задач, подлежащих решению с использованием методов системной инженерии и, соответственно, с применением разработанных в диссертации математических, программных, технологических и методических решений для ВС и КС (ссылочная нумерация на рисунках соответствует нумерации в «Стратегии…»), в частности [5]:

- на рис. 5.51 - для обеспечения государственной и общественной безопасности;
- на рис. 5.52 - для обеспечения информационной безопасности;
- на рис. 5.53 - для обеспечения экономической безопасности;
- на рис. 5.54 - для обеспечения научно-технологического развития;
- на рис. 5.55 - для обеспечения экологической безопасности и рационального природопользования;
- на рис. 5.56 - для защиты традиционных российских духовно-нравственных ценностей;
- на рис. 5.57 - для обеспечения стратегической стабильности и взаимовыгодного международного сотрудничества.

СТРАТЕГИЧЕСКИЙ НАЦИОНАЛЬНЫЙ ПРИОРИТЕТ

26.3) государственная и общественная безопасность

Цели: защита конституционного строя Российской Федерации, обеспечение ее суверенитета, независимости, государственной и территориальной целостности, защита основных прав и свобод человека и гражданина, укрепление гражданского мира и согласия, политической и социальной стабильности в обществе, совершенствование механизмов взаимодействия государства и гражданского общества, укрепление законности и правопорядка, искоренение коррупции, защита граждан и всех форм собственности, традиционных российских духовно-нравственных ценностей от противоправных посягательств, защита населения и территорий от чрезвычайных ситуаций природного и техногенного характера

47. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ

2) обеспечение безопасности проводимых на территории Российской Федерации общественно-политических и иных мероприятий;
3) обеспечение защиты и охраны государственной границы Российской Федерации, охраны территориального моря, исключительной экономической зоны и континентального шельфа Российской Федерации, а также модернизация пограничной инфраструктуры, совершенствование механизмов пограничного, таможенного, санитарно-эпидемиологического и иных видов контроля;
4) совершенствование системы общественного контроля, механизмов участия граждан и организаций в обеспечении государственной и общественной безопасности;

6) повышение уровня антитеррористической защищенности мест массового пребывания людей, объектов жизнеобеспечения населения, организаций оборонно-промышленного, атомного энергопромышленного, ядерного оружейного, химического, топливно-энергетического комплексов страны, объектов транспортной инфраструктуры, других критически важных и потенциально опасных объектов;
7) предупреждение и пресечение террористической и экстремистской деятельности организаций и физических лиц, попыток совершения актов ядерного, химического и биологического терроризма;
8) снижение уровня криминализации общественных отношений, развитие единой государственной системы профилактики правонарушений;

10) снижение уровня преступности в экономической сфере, в том числе в кредитно-финансовой, а также в сферах жилищно-коммунального хозяйства, использования земельных, лесных, водных и водных биологических ресурсов;
11) предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий;

18) повышение безопасности дорожного движения;
19) повышение эффективности мер по предупреждению и ликвидации чрезвычайных ситуаций природного и техногенного характера;
20) обеспечение защиты населения от опасных инфекционных заболеваний, способных вызвать чрезвычайную ситуацию в области санитарно-эпидемиологического благополучия населения;
21) прогнозирование влияния последствий изменения климата на состояние опасных производственных объектов, гидротехнических сооружений, транспортного комплекса, объектов жизнеобеспечения населения;
22) комплексное развитие правоохранительных органов, специальных служб, подразделений пожарной охраны и аварийно-спасательных формирований

Рис. 5.51 Задачи, подлежащие решению с использованием методов системной инженерии для обеспечения государственной и общественной безопасности

26.4) информационная безопасность

Цель: укрепление суверенитета Российской Федерации в информационном пространстве

57. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ

1) повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования;
2) развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз;
3) предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры Российской Федерации;
4) создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий;
5) повышение защищенности и устойчивости функционирования единой сети электросвязи Российской Федерации, российского сегмента сети "Интернет", иных значимых объектов информационно-коммуникационной инфраструктуры;
6) снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений установленных российским законодательством требований по защите такой информации и персональных данных;
7) предотвращение и (или) минимизация ущерба национальной безопасности, связанного с осуществлением иностранными государствами технической разведки;

10) развитие сил и средств информационного противоборства;

12) совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления

Рис. 5.52 Задачи, подлежащие решению с использованием методов системной инженерии для обеспечения информационной безопасности

26.5) экономическая безопасность

Цели: укрепление экономического суверенитета страны, повышение конкурентоспособности российской экономики и ее устойчивости к воздействию внешних и внутренних угроз, создание условий для экономического роста Российской Федерации, темпы которого будут выше мировых

67. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ

2) сохранение макроэкономической устойчивости, обеспечение сбалансированности бюджетной системы;

5) обеспечение устойчивого развития реального сектора экономики, создание высокотехнологичных производств, новых отраслей экономики, рынков товаров и услуг на основе перспективных высоких технологий;
6) повышение производительности труда путем модернизации промышленных предприятий и инфраструктуры, цифровизации, использования технологий искусственного интеллекта, создания высокотехнологичных рабочих мест;

8) укрепление достигнутых Российской Федерацией лидирующих позиций и конкурентных преимуществ в авиационной, судостроительной, ракетно-космической промышленности, двигателестроении, атомном энергопромышленном комплексе, а также в сфере информационно-коммуникационных технологий;

15) обеспечение энергетической безопасности Российской Федерации, в том числе обеспечение устойчивого тепло- и энергоснабжения населения и субъектов национальной экономики, повышение энергетической эффективности экономики и эффективности государственного управления в сфере топливно-энергетического комплекса;

19) развитие рыночной, энергетической, инженерной, инновационной и социальной инфраструктур;
20) обеспечение развития эффективной транспортной инфраструктуры и транспортной связанности страны;

23) повышение эффективности государственной макроэкономической политики путем развития системы стратегического планирования, внедрения риск-ориентированного подхода с учетом потенциальных внешних и внутренних вызовов и угроз экономической безопасности Российской Федерации;
24) совершенствование системы государственного контроля (надзора) в сфере экономической деятельности;

32) повышение эффективности использования бюджетных средств и управления принадлежащими государству активами

Рис. 5.53 Цели и задачи, подлежащие решению с использованием методов системной инженерии для обеспечения экономической безопасности

26.6) научно-технологическое развитие

Цель: обеспечение технологической независимости и конкурентоспособности страны, достижения национальных целей развития и реализации стратегических национальных приоритетов

76. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ

1) выработка и реализация на федеральном, региональном, отраслевом и корпоративном уровнях согласованной политики, обеспечивающей переход российской экономики на новую технологическую основу;

3) создание единой государственной системы управления научной, научно-технической и инновационной деятельностью;

5) ускоренное внедрение в промышленное производство результатов научных исследований для обеспечения полного научно-производственного цикла в соответствии с приоритетами социально-экономического, научного и научно-технологического развития Российской Федерации;
6) совершенствование системы фундаментальных научных исследований как важнейшей составляющей устойчивого развития Российской Федерации;
7) модернизация и развитие научной, научно-технической и инновационной инфраструктуры;

9) создание и развитие на территории Российской Федерации сети научных установок класса "мегасайенс", крупных исследовательских инфраструктур, центров коллективного пользования научно-технологическим оборудованием, экспериментального производства и инжиниринга;

12) создание национальной системы оценки результативности научной, научно-технической и инновационной деятельности;

14) развитие перспективных высоких технологий (нанотехнологии, робототехника, медицинские, биологические, генной инженерии, информационно-коммуникационные, квантовые, искусственного интеллекта, обработки больших данных, энергетические, лазерные, аддитивные, создания новых материалов, когнитивные, природоподобные технологии), суперкомпьютерных систем;
15) развитие междисциплинарных исследований;

17) проведение научных и научно-технических исследований в интересах обороны страны и безопасности государства;
18) активизация научных исследований в области обеспечения биологической, радиационной и химической безопасности Российской Федерации;
19) обеспечение передачи знаний и технологий между оборонным и гражданским секторами экономики;

23) подготовка научных и научно-педагогических кадров, высококвалифицированных специалистов по приоритетным направлениям научно-технологического развития Российской Федерации

Рис. 5.54 Цель и задачи, подлежащие решению с использованием методов системной инженерии для обеспечения научно-технологического развития

26.7) экологическая безопасность и рациональное природопользование

Цели: обеспечение качества окружающей среды, необходимого для благоприятной жизни человека, сохранение и восстановление природной среды, сбалансированное природопользование, смягчение негативных последствий изменения климата

83. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ

1) обеспечение экологически ориентированного роста экономики, стимулирование внедрения инновационных технологий, развитие экологически безопасных производств;
2) обеспечение рационального и эффективного использования природных ресурсов, развитие минерально-сырьевой базы;

4) формирование системы государственного регулирования выбросов парниковых газов, обеспечение реализации проектов по сокращению выбросов парниковых газов и увеличению их поглощения;

6) повышение эффективности обеспечения гидрометеорологической безопасности;

8) снижение объемов образования отходов производства и потребления, развитие индустрии их утилизации и вторичного использования;

12) решение экологических проблем и рациональное использование природных ресурсов Арктической зоны Российской Федерации;
13) повышение эффективности государственного экологического надзора, производственного и общественного контроля в сфере охраны окружающей среды;
14) развитие системы государственного экологического мониторинга и контроля за соблюдением экологических нормативов и природоохранных требований хозяйствующими субъектами, повышение эффективности прогнозирования опасных природных явлений и процессов, последствий влияния изменений климата на условия хозяйствования и жизнедеятельности человека;
15) развитие системы мониторинга биологических рисков для предупреждения биологических угроз и реагирования на них;
16) повышение технического потенциала и оснащенности сил, участвующих в мероприятиях по предотвращению и ликвидации негативных экологических последствий чрезвычайных ситуаций природного и техногенного характера

Рис. 5.55 Направления развития системной инженерии для обеспечения экологической безопасности и рационального природопользования

СТРАТЕГИЧЕСКИЙ НАЦИОНАЛЬНЫЙ ПРИОРИТЕТ

26.8) защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти

Цель: укрепление единства народов Российской Федерации на основе общероссийской гражданской идентичности, сохранения исконных общечеловеческих принципов и общественно значимых ориентиров социального развития

93. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ

4) реализация государственной информационной политики, направленной на усиление в массовом сознании роли традиционных российских духовно-нравственных и культурно-исторических ценностей, неприятие гражданами навязываемых извне деструктивных идей, стереотипов и моделей поведения;
5) развитие системы образования, обучения и воспитания как основы формирования развитой и социально ответственной личности, стремящейся к духовному, нравственному, интеллектуальному и физическому совершенству;

11) формирование государственного заказа на проведение научных исследований, публикацию научно-популярных материалов, создание произведений литературы и искусства, кинематографической, театральной, телевизионной, видео- и интернет-продукции, оказание услуг, направленных на сохранение традиционных российских духовно-нравственных ценностей и культуры, защиту исторической правды и сохранение исторической памяти, а также обеспечение контроля качества выполнения этого государственного заказа;

13) защита российского общества от внешней идейно-ценностной экспансии и внешнего деструктивного информационно-психологического воздействия, недопущение распространения продукции экстремистского содержания, пропаганды насилия, расовой и религиозной нетерпимости, межнациональной розни

Рис. 5.56 Задачи, подлежащие решению с использованием методов системной инженерии для защиты традиционных российских духовно-нравственных ценностей, культуры и исторической памяти

СТРАТЕГИЧЕСКИЙ НАЦИОНАЛЬНЫЙ ПРИОРИТЕТ

26.9) стратегическая стабильность и взаимовыгодное международное сотрудничество
Цели: создание благоприятных условий для устойчивого социально-экономического развития страны, укрепление национальной безопасности, упрочение позиций России как одного из влиятельных центров современного мира

101. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ

1) повышение устойчивости международно-правовой системы;
2) укрепление международного мира и безопасности, устранение предпосылок для развязывания глобальной войны и рисков применения ядерного оружия;
3) совершенствование механизмов обеспечения коллективной безопасности на глобальном и региональном уровнях, осуществление и при необходимости развитие мер доверия, предотвращение инцидентов в военной сфере;

11) содействие устранению и предотвращению возникновения очагов напряженности и конфликтов на территориях соседних с Российской Федерацией государств;

17) обеспечение интересов Российской Федерации, связанных с освоением космического пространства, Мирового океана, Арктики и Антарктики;

23) развитие сотрудничества в рамках международных организаций и институтов, расширение использования инструментов сетевой дипломатии;
24) развитие военно-политического и военно-технического сотрудничества с иностранными государствами;
25) развитие международного сотрудничества в области противодействия терроризму, экстремизму, коррупции, незаконному производству и обороту наркотических средств и психотропных веществ, нелегальной миграции, трансграничной преступности;
26) развитие международного сотрудничества в интересах формирования безопасного и равноправного глобального информационного пространства;
27) развитие взаимодействия с иностранными государствами в области охраны окружающей среды и предотвращения изменений климата;
28) содействие иностранным государствам в ликвидации последствий чрезвычайных ситуаций природного и техногенного характера, в борьбе с биологическими угрозами, распространением опасных инфекционных заболеваний;

32) расширение сотрудничества с государствами - участниками СНГ в области укрепления биологической безопасности

Рис. 5.57 Задачи, подлежащие решению с использованием методов системной инженерии для обеспечения стратегической стабильности и взаимовыгодного международного сотрудничества

При этом основными направлениями развития системной инженерии с использованием научных результатов диссертации для достижения целей государственной политики и эффективного решения задач в сфере обеспечения национальной безопасности определены:

– сосредоточение научно-технических усилий на достижении целей обеспечения требуемых безопасности, качества, сбалансированных эффектов и устойчивого функционирования и развития сложных систем;

– предоставление возможностей прогнозирования и рационального управления рисками в стандартных процессах жизненного цикла систем, совершенствование и накопление статистики и знаний, выявление общих аналитических закономерностей в интересах РФ;

– расширение на все решаемые задачи функциональных возможностей созданных моделей и методов системной инженерии, программных, технологических и методических решений по аналитическому прогнозированию и рациональному управлению рисками, межприкладное применение баз данных и баз знаний, выявленных общих аналитических закономерностей в интересах Российской Федерации;

– трансформация существующего подхода к созданию и использованию моделей и методов системной инженерии, ориентированных на конкретную систему, в технологию искусственного интеллекта поддержки принятия логичных решений, подтверждаемых прогнозными исследованиями по достижению требуемых безопасности, качества, сбалансированных эффектов и устойчивого функционирования и развития систем различного функционального назначения.

5.8 Выводы по разделу 5

В результате разработки рекомендаций по снижению и удержанию рисков в допустимых пределах в жизненном цикле различных систем на основе применения возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии сделаны следующие выводы.

1. Продемонстрирован способ логического преобразования изначального вербального описания сложной системы к формализованному виду, позволяющему использовать предложенные в диссертации вероятностные модели, программные, технологические и методические решения для ВС и КС. В качестве системы без ограничения общности рассмотрен технический облик гипотетичной многоуровневой системы управления рисками в интересах обеспечения энергетической безопасности согласно "Доктрине энергетической безопасности Российской Федерации". Сведение вербального описания сложной системы к формализованному виду позволило применить возможности созданного прототипа технологии поддержки риск-ориентированной системной инженерии для формальной постановки и дальнейшего решения практических задач:

- минимизации риска нарушения надежности обеспечения энергетической безопасности макрорегиона государства или отдельно взятого субъекта энергетической безопасности в ТЭК при ограничениях на отдельные допустимые риски реализации критичных угроз (для конкретных объектов и процессов), ресурсы и общие затраты на реализацию планов и при иных ограничениях;

- минимизации общих затрат на реализацию кратко-, средне- и/или долгосрочных планов при ограничениях на допустимый риск надежности обеспечения энергетической безопасности макрорегиона государства или отдельно взятого субъекта энергетической безопасности в ТЭК, на отдельные допустимые риски реализации критичных угроз (для конкретных объектов и процессов), ресурсы и при иных ограничениях;

- комбинации перечисленных выше или иных оптимизационных задач применительно к макрорегиону или отдельно взятому субъекту энергетической безопасности в ТЭК.

Результаты решения этих задач рекомендовано использовать для обеспечения баланса по критерию «эффективность – стоимость» при кратко-, средне- и/или долгосрочном планировании на уровне макрорегиона государства или отдельно взятого субъекта энергетической безопасности.

2. Применение разработанных программных, технологических и методических решений для ВС и КС и интерпретация получаемых результатов прогнозирования рисков в

приложении к сопровождаемым цифровым двойникам (на примере фрагментов магистральной трубопроводной сети) обеспечило прослеживаемость и аналитическую зависимость прогнозных рисков от влияющих факторов. Это открыло важные прагматические возможности для системного обоснования и дополнения технических мер, востребуемых по итогам регулярного диагностирования объекта, и обеспечило повышение безопасности его эксплуатации в условиях природных, технических, экономических и иных ограничений. За счет использования возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии проведение расчетов возможно не только за автоматизированным рабочим местом ВС в стационарных условиях, но и в полевых условиях, где возможно подключение к компьютерной сети.

3. Применение разработанных типовых методик и инженерного подхода продемонстрировано на примерах моделирования многомодального взаимодействия социокиберфизических систем в жизненном цикле обогатительной фабрики в угольной отрасли для изыскания путей усовершенствования (перевооружения) системы вентиляции, аспирации и пылеподавления, позволившее обосновать комплекс приемлемых условий к системе, соблюдение которых позволит удерживать частные и интегральный риски в допустимых пределах. Так, результаты расчетов позволили выявить «узкие места» и спрогнозировать снижение рисков на основе перевооружения (интегральный риск за год эксплуатации снизится на 33% с существующего уровня 0.574 до 0.433, среднее время до нарушения целостности системы возрастет почти на год - с нынешних 11.1 до 12 лет). Вместе с тем, выявлен явный дисбаланс в системе после перевооружения - на самом деле расчетные 12 лет до нарушения набираются за счет сверхнадежной работы новых основных фондов, оставляя опасность «человеческого фактора» на прежнем уровне, т.е. обнаруженный эффект – только технический, но далеко не системный. Дополнительные системные исследования позволили обосновать комплекс приемлемых условий к системе вентиляции, аспирации и пылеподавления, соблюдение которых позволит удерживать частные и интегральный риски в допустимых пределах.

4. С использованием предложенных базовых моделей на примерах управления рисками для обеспечения качества хранимого зерна была выявлена закономерность: если условия хранения не допускают возникновения рассадников насекомых чаще, чем раз в неделю, вероятность сохранения качества хранимого зерна за 3-6 лет в 3-5 раз превышает вероятность потери качества. Результаты многолетних исследований ВНИИ Зерна подтвердили адекватность такого вывода. Тем самым результаты проведенных исследований в сравнении с результатами иных специализированных исследований (ВНИИ

Зерна) явились дополнительной аргументацией в подтверждение адекватности разработанных математических и программных решений в различных их приложениях.

5. Продемонстрирована способность расширения аналитических возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии путем добавления другой модели. Так, разработаны вероятностные модели для оценки частных рисков невыявления некорректностей в машинном обучении (дообучении) при разработке и эксплуатации программных средств для систем искусственного интеллекта в условиях актуальных угроз подмены моделей машинного обучения (УБИ.222 по классификации ФСТЭК России) и их модификации путем искажения («отравления») обучающих данных (УБИ.221). Интегральный риск предложено оценивать через виртуальный показатель риска нарушения корректности машинного обучения в условиях рассматриваемых угроз в течение задаваемого периода прогноза в зависимости от рисков невыявления некорректностей в машинном обучении (дообучении) при разработке и эксплуатации программных средств, а через них – в зависимости от исходных данных, обеспечивающих расчет соответствующих рисков. Работоспособность предложенного подхода подтверждена количественными примерами.

6. Разностороннее использование возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии продемонстрировано на решении вопросов удержания в допустимых пределах рисков разрушения бизнеса применительно к фармацевтическому предприятию на этапах его проектирования и эксплуатации. Количественно доказано, что эффективность активного управления со стороны Руководства предприятия соизмерима с использованием мер дополнительного резервирования действий применительно ко всем службам организационного управления. Сформулированы условия, определяемые главным образом самими работниками предприятия (их ответственностью и широкой квалификацией для резервирования действий, формализуемыми временными характеристиками) при активном управлении и эффективной поддержке со стороны Руководства предприятия. Показано, что с высокой вероятностью именно соблюдение этих условий обеспечит сохранение бизнеса в долговременной перспективе.

7. Основными направлениями развития системной инженерии с использованием научных результатов диссертации для достижения целей государственной политики и эффективного решения задач в сфере обеспечения национальной безопасности определены:

– сосредоточение научно-технических усилий на достижении целей обеспечения требуемых безопасности, качества, сбалансированных эффектов и устойчивого функционирования и развития сложных систем;

– предоставление возможностей прогнозирования и рационального управления рисками в стандартных процессах жизненного цикла систем, совершенствование и накопление статистики и знаний, выявление общих аналитических закономерностей в интересах РФ;

– расширение на все решаемые задачи функциональных возможностей созданных моделей и методов системной инженерии, программных, технологических и методических решений по аналитическому прогнозированию и рациональному управлению рисками, межприкладное применение баз данных и баз знаний, выявленных общих аналитических закономерностей в интересах Российской Федерации;

– трансформация существующего подхода к созданию и использованию моделей и методов системной инженерии, ориентированных на конкретную систему, в технологию искусственного интеллекта поддержки принятия логичных решений, подтверждаемых прогнозными исследованиями по достижению требуемых безопасности, качества, сбалансированных эффектов и устойчивого функционирования и развития систем различного функционального назначения.

Заключение

Проведенный анализ показал, что в условиях неопределенностей роль системной инженерии в решении практических задач на ближайшие десятилетия характеризуется научной фундаментальностью в достижении целей систем различного функционального назначения за счет оперативного прогнозирования рисков, упреждающего выявления «узких мест» и определения рациональных способов снижения и удержания рисков в допустимых пределах. Место системной инженерии – везде, где возникает потребность в решении практических задач анализа и оптимизации, а также поиска и исследования новых идей и возможностей.

В приложении к применению в вычислительных системах и компьютерных сетях **изложены новые научно обоснованные программные, технологические и методические решения, реализованные в рамках созданного прототипа технологии риск-ориентированной системной инженерии**. **Внедрение полученных в диссертации результатов вносит значительный вклад в развитие процессов цифровой трансформации в различных отраслях народного хозяйства.** А именно:

изложенные новые научно обоснованные программные и технологические решения для ВС и КС обеспечивают интеграцию существующих и усовершенствованных базовых моделей, создание и ведение прототипа базы знаний для моделирования в ЖЦ систем различного функционального назначения, за счет чего достигается расширение аналитических возможностей по прогнозированию и упреждающему управлению рисками;

изложенные новые методические решения задач системной инженерии позволяют в отличие от существующих подходов стандартизованным способом широко применять с использованием ВС и КС усовершенствованные вероятностные модели и разработанные программные и технологические решения, интерпретировать результаты прогнозирования рисков, извлекать в условиях разнородных неопределенностей знания о достижимых прагматических эффектах и обосновывать рекомендации по упреждающему управлению рисками, снижению и удержанию рисков в допустимых пределах.

Актом Председателя Комиссии РАН по техногенной безопасности член-корреспондентом РАН Махутовым Н.А. подтверждено, что теоретические и методические результаты диссертационных исследований, а также созданные программные и технологические решения использованы в трех разделах изданной в 2025 году монографии «Безопасность России. Правовые, социально-экономические и научно-технологические аспекты. Тематический блок «Национальная безопасность». Системная инженерия в проблемах национальной безопасности», а именно: в разделе III «Основные положения системной инженерии для решения проблем обеспечения национальной безопасности»,

разделе VIII «Приложения системной инженерии к национальному приоритету по обеспечению экономической безопасности», разделе IX «Приложения системной инженерии к национальному приоритету по обеспечению научно-технологического развития».

В результате проведенных научных исследований в работе получены следующие основные результаты.

1. Выявлены и сформулированы 10 основных тенденций в приложениях системной инженерии, характеризующих важность управления рисками на ближайшую многолетнюю перспективу, это:

1) поворот к кардинальному совершенствованию мобилизационных возможностей государства для укрепления оборонно-промышленного комплекса и обороны страны;

2) расширенное практическое внедрение результатов технического прогресса для совершенствования и развития функциональных возможностей систем (с ожиданием повышения качества, безопасности, эффективности систем, предсказуемости и устойчивости их функционирования, доступности по цене);

3) существенное усложнение систем, обострение проблематики информационной безопасности, широкое внедрение методов количественного прогнозирования рисков и обоснования упреждающих мер противодействия разнородным угрозам;

4) целенаправленная интеллектуализация систем и технологий (с необходимым обеспечением проверяемости, безопасности и доверия к интеллектуальным системам, объяснением и пониманием логики их действий);

5) заметное влияние цифровой трансформации на создаваемые системы, выпускаемую продукцию, стиль и методы работы людей;

6) переход промышленности на принципы и технологии индустрии 4.0 (с «умными» фабриками, киберфизическими системами, цифровыми двойниками и цепочками взаимодействующих инструментов и процессов);

7) построение нового социального общества и решение социальных проблем методами, базирующимися на интеграции реального физического мира с виртуальным киберпространством;

8) накопление и использование знаний для повышения качества, безопасности и эффективности систем и оптимизации управления предприятиями, проектами и системами;

9) разворот к системному решению проблем экологической безопасности и рационального природопользования;

10) реформирование профессиональной подготовки специалистов для эффективного решения проблем системной инженерии.

2. Проведенный в контексте выявленных тенденций анализ показал, что возрастание потребностей системной инженерии, научно-технический прогресс в сфере информационных технологий и телекоммуникаций, устаревание программного обеспечения на фоне санкций стран Запада, осознание важности, перспективности и масштабности моделирования с учетом практических особенностей привели к необходимости дальнейшего научного развития вероятностных моделей, создания усовершенствованных программных, технологических и методических решений в интересах упреждающего управления рисками для систем различного функционального назначения. При этом особый акцент сделан на моделировании стандартизованных процессов в жизненном цикле различных систем, а также на внедрении зарекомендовавших себя методов в национальные стандарты. Установлено: по возможности необходимо упреждающее управление соответствующими рисками с учетом задаваемых требований при выполнении всех стандартизованных процессов:

процессов соглашения – приобретения и поставки продукции и услуг;

процессов организационного обеспечения проекта – управления моделью жизненного цикла, инфраструктурой, портфелем проектов, человеческими ресурсами, качеством, знаниями;

процессов технического управления – планирования проекта, оценки и контроля проекта, управления решениями, рисками, конфигурацией, информацией, измерений, гарантии качества;

технических процессов – анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа, реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы**.**

3. На сформулированном пространстве элементарных событий в условиях различных неопределенностей предложены следующие основные расчетные показатели, одинаково свойственные для любого рода системам:

- риск нарушения рассматриваемого системного процесса как такового для реализации основных функциональных требований в течение задаваемого периода прогноза;

- риск нарушения рассматриваемого системного процесса с учетом дополнительных специфических системных требований в течение задаваемого периода прогноза;

- риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза при реализации основных функциональных требований;

- риск нарушения дополнительных специфических требований к моделируемой системе в течение задаваемого периода прогноза;

- интегральный риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза при реализации основных функциональных требований и дополнительных специфических требований;

- прогнозная нижняя оценка среднего остаточного времени на принятие упреждающих мер в недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта;

- среднее остаточное время до возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- среднее остаточное время до возможного нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

4. Создан комплекс новых программных и технологических решений для ВС и КС, охватывающий: решения по программной инфраструктуре глобально распределенного прогнозирования рисков и моделированию процессов; комплексы программ моделирования систем для прогнозирования рисков, выявления угроз, анализа альтернатив и обоснования системных требований к характеристикам процессов; прототип базы знаний для подготовки исходных данных для моделирования и поддержки принятия аналитических решений на стадиях жизненного цикла систем; технологические решения по интеграции моделей и созданных комплексов программ, обеспечивающие реализацию новых аналитических возможностей по вероятностному прогнозированию и упреждающему управлению рисками. Эти решения характеризуются следующими научно-техническими аспектами, описываемыми в 4.1 – 4.8.

4.1. Для совершенствования математического обеспечения в интересах широкого применения моделирования в области системной инженерии:

- сформулирована и доказана Теорема 1 о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности;

- предложена универсальная вспомогательная модель показателей (УВМП), используемая для извлечения знаний из процесса мониторинга данных и применимая для формирования исходных данных при моделировании систем различного функционального назначения;

- сформулирована и доказана Теорема 2 об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в

недопущение возможного нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта и Следствие из нее;

- сформулирована и доказана Теорема 3 о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам;

- с помощью Теорем 1-3 сделано теоретическое обоснование возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых при моделировании из «черных ящиков»;

- сформулирована и доказана Теорема 4 о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам.

Применение Теорем 1-4 и УВМП позволило осуществить теоретические усовершенствования существующих моделей и тем самым сформировать базовые модели математического обеспечения для анализа системных элементов, сложных систем и процессов в интересах широкого применения моделирования в приложениях системной инженерии с использованием ВС и КС.

Эти усовершенствования математического обеспечения реализованы в предлагаемых программных решениях и ориентированы на использование предложенных базовых моделей для осуществления целенаправленного моделирования в ЖЦ систем.

4.2. Для упреждающего управления рисками в приложениях системной инженерии предложен комплекс программ для ЭВМ, созданных с участием автора в 2004-2025гг. (в т.ч. четыре – без соавторов):

«Моделирование процессов в жизненном цикле систем "Моделирование процессов" - "ноу-хау"» (Свидетельство о государственной регистрации программы для ЭВМ №2004610858);

«Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2006610219);

«Программно-инструментальный комплекс оценки качества функционирования информационных систем через Интернет «КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008612348);

«Программно-инструментальный комплекс сопровождения систем менеджмента качества «OPISys-КОК-Интернет» (Свидетельство о государственной регистрации программы для ЭВМ №2008614525);

«Программно-вычислительный комплекс оценки качества производственных

процессов» (Свидетельство о государственной регистрации программы для ЭВМ №2010614145);

«Комплекс для оценки качества информационных и административно-управленческих процессов при функционировании электронного правительства (КОК-ЭП)» (Свидетельство о государственной регистрации программы для ЭВМ № 2010617017);

«Удаленная аналитическая поддержка информирования о вероятностно-временных показателях функционирования системы и ее элементов при реализации риск-ориентированного подхода» (Свидетельство о государственной регистрации программы для ЭВМ №2018617949);

«Удаленное обоснование требований к средствам и условиям обеспечения качества функционирования «умных» систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618572);

«Удаленное вероятностное прогнозирование качества функционирования информатизированных систем» (Свидетельство о государственной регистрации программы для ЭВМ №2018618686);

«Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021» (2025);

«Модуль формирования отчетности по результатам вероятностного прогнозирования рисков для сложной системы с последовательным соединением элементов» (2025);

«Модуль проверки достаточности данных для прогнозирования рисков по статистике» (2025);

«Модель технологической поддержки риск-ориентированной системной инженерии» (2025).

4.3. Разработаны и реализованы концептуальные положения по упреждающему управлению рисками, опирающиеся на использование ВС и КС для вероятностного моделирования, прогнозирования рисков и оптимизации в аналитическом решении задач системной инженерии и обоснования возможных упреждающих действий в условиях неопределенности. Прогнозирование рисков базируется на мониторинге состояний, накоплении и рациональном использовании знаний, в т.ч. формируемых в режиме реального времени функционирования различных систем. Показано, что на основе применения предлагаемого подхода системный аналитик оперирует цифровым образом рассматриваемых систем в терминах прогнозных рисков. Отличие от существующих инструментариев – взгляд условно на 3 шага вперед, это - прогноз, рекомендации и обоснование решений для задач системной инженерии.

4.4. Предложен вариант послойного аналитического комплексирования разработанных программных решений на различных мета-уровнях. При этом многомодальное взаимодействие с источниками данных осуществляется с использованием: телеметрических данных от оборудования; данных, выбираемых из базы данных, учитывающей специфику приложений системы, в т.ч. в различных форматах; данных, вводимых в формате программных решений базовых моделей. В интересах решения задач системной инженерии реализован мониторинг и прогноз риска нарушения приемлемого выполнения заданных процессов системной инженерии. В рамках созданных программно-технологических решений использованы различные человеко-машинные интерфейсы, приспособленные для применения предложенных базовых моделей. Показано, что при этом осуществляются:

- в ЖЦ системы: информирование о системных требованиях к характеристикам системы, предоставление необходимых данных, учет условий и принятых ограничений;

- на этапах разработки, модернизации и развития системы: прогнозирование рисков, анализ альтернатив по результатам расчетов;

- на этапах эксплуатации и сопровождения системы: прогнозирование рисков, оценка критичности влияния различных параметров на поведение системы;

- при проектировании, выполнении, контроле и управлении процессами: реализации аналитических возможностей по выявлению существенных угроз и приемлемых условий для анализируемых процессов;

- при интеграции исследований на различных мета-уровнях: прогнозирование интегрального риска, в т.ч. для совокупности стандартных процессов в ЖЦ системы, обоснование условий удержания рисков в допустимых пределах.

4.5. Разработаны и описаны встроенные технологические возможности по предоставлению обобщенных и детальных вероятностных прогнозов, доведенные до реализации в системах дистанционного контроля промышленной безопасности (СДК ПБ) на объектах опасного производства. В итоге применения предлагаемых технологических возможностей ответственному лицу СДК ПБ предоставляются аналитические отчеты, содержащие следующие показатели, рекомендованные ГОСТ Р 58494-2019 «Оборудование горно-шахтное. МФСБ. Система дистанционного контроля опасных производственных объектов»:

прогнозируемое остаточное время на принятие и реализацию решения для предотвращения нарушения границ нормативного диапазона при каждом выходе значений параметра за границы рабочего диапазона;

условные средние времена до выхода значений параметра за границы нормативного

диапазона для условий, если оперативно реагировать на выходы значений параметров за границы рабочего диапазона и если не реагировать на эти отклонения;

риски нарушения границ нормативного диапазона хотя бы по одному из контролируемых параметров за смену, сутки, неделю, месяц, год с учетом последствий (в вероятностном представлении).

Практичность созданных математических, программных, технологических и методических решений подтверждена актом ООО «НИИ прикладной математики и сертификации» об их реализации при выполнении работ по созданию и эксплуатации программного прототипа подсистемы поддержки принятия решений по управлению рисками в рамках системы дистанционного контроля промышленной безопасности на угольных шахтах.

4.6 Разработан «Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в УВМП по ГОСТ Р 59349», позволяющий определять необходимые исходные данные для моделирования: частоту возникновения источников угроз, среднее время развития угроз и среднее время восстановления нарушаемой целостности моделируемой системы. Показано, как эти исходные данные формируются автоматически из базы данных созданных систем дистанционного контроля ПБ.

4.7. Сформирован прототип базы знаний для моделирования, позволяющий определять «достаточность» используемой статистики при формировании следующих исходных данных: частоты возникновения источников угроз, среднего времени развития угроз и среднего времени восстановления нарушаемой целостности моделируемой системы формируются автоматически из БД с использованием разработанного «Модуля определения частоты возникновения угроз, времен развития угроз и восстановления в УВМП по ГОСТ Р 59349». Указаны способы повышения практической полезности прогнозирования остаточного временного ресурса в режиме реального времени функционирования СДК ПБ.

4.8. Создан прототип технологии поддержки риск-ориентированной системной инженерии, основанный на новых программных и технологических решениях для ВС и КС, поддерживающий информационно-логическую, программную и технологическую интеграцию разработанных базовых моделей и программных решений для ВС и КС и обеспечивающий путем моделирования упреждающее выявление «узких мест» и определение рациональных способов снижения и удержания рисков в допустимых пределах на стадиях жизненного цикла систем различного функционального назначения в условиях реальных и гипотетических вызовов и угроз, а также оформление и выдачу результатов расчетов с предоставлением соответствующих рекомендаций по решению

задач системной инженерии. Инфраструктура прототипа представляет собой совокупность клиент-серверных программных модулей, разделенных на подготовку данных для анализа, расчет и прогноз, мониторинг данных и аналитическое обоснование рекомендаций. Исходя из целей моделирования с помощью прототипа осуществляется анализ самой задачи системной инженерии для решения и последующая формализация системных требований с использованием созданного прототипа базы знаний. Далее с учетом среды моделирования (off-line, on-line или встроенное моделирование в АСУ ТП), исходя из цифрового описания моделируемой системы или аналога определяются необходимые исходные данные. С учетом специфики системы формируются сценарии возможных угроз и мер противодействия угрозам. После этого осуществляется моделирование, оформление и выдача результатов расчетов с предоставлением соответствующих рекомендаций по решению задачи системной инженерии с необходимыми прогнозом и обоснованием.

5. Для ВС и КС разработаны методические решения:

- «Типовая методика прогнозирования рисков нарушения целостности моделируемой системы, представимой в виде «черного ящика», на различных мета-уровнях»;

- «Типовая методика прогнозирования рисков нарушения целостности сложной моделируемой системы»;

- инженерный подход к определению границ рабочего диапазона критичных параметров мониторируемого объекта, проиллюстрировавший корректность аргументации доказанной Теоремы 3 (о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам).

6. Работоспособность программных, технологических и методических решений продемонстрирована на примерах исследований функционирования гипотетичной угольной шахты, включая:

- сравнение ручного контроля расхода воды в системе водоотлива с автоматическим контролем и восстановлением водного баланса с использованием системы дистанционного контроля (СДК);

- определение границ рабочего диапазона критичных параметров контролируемого оборудования;

- прогнозирование рисков нарушения промышленной безопасности главной вентиляторной установки (ГВУ) шахты и утраты работоспособности ГВУ для трех случаев управления: без принятия каких-либо мер противодействия угрозам, принятия мер в рамках системы контроля без использования возможностей СДК и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК;

- прогнозирование рисков нарушения промышленной безопасности (ПБ) на опасном производственном объекте, рассматриваемом как сложная система, когда в качестве мониторируемых подсистем выступают комплексы главных вентиляторных установок, модульных дегазационных установок, газоотсасывающих установок.

7. Предложенные основные положения по моделированию, прогнозированию и упреждающему управлению рисками реализованы в национальном стандарте ГОСТ Р 58494-2019 «Оборудование горно-шахтное. МФСБ. Система дистанционного контроля опасных производственных объектов», утвержденном Росстандартом в 2019г. и введенном в действие с 2020г. Предложенные вероятностные модели и методы реализованы в 2021 году в 18 национальных стандартах системной инженерии: ГОСТ Р 59329, ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59334, ГОСТ Р 59335, ГОСТ Р 59336, ГОСТ Р 59337, ГОСТ Р 59338, ГОСТ Р 59339, ГОСТ Р 59341, ГОСТ Р 59342, ГОСТ Р 59347, ГОСТ Р 59349, ГОСТ Р 59353, ГОСТ Р 59354, ГОСТ Р 59355, ГОСТ Р 59356, ГОСТ Р 59357 в части моделирования стандартных процессов приобретения и поставки продукции и услуг, управления инфраструктурой системы, управления человеческими ресурсами, управления качеством системы, управления знаниями о системе, планирования проекта, оценки и контроля проекта, управления решениями, управления рисками для системы, управления информацией, измерений, определения архитектуры системы, системного анализа, передачи, аттестации, функционирования и сопровождения системы, изъятия и списания системы, что подтверждено актом о реализации от ФБУ НТЦ «Энергобезопасность». Стандартизованные усовершенствованные модели, методы и методические решения внедрены в практику работы национального и межнационального технического комитета «Информационные технологии» (ТК-МТК-022) в части ссылок и рекомендаций по использованию созданных методов, моделей и демонстрационных примеров системной инженерии в новых национальных стандартах 2024-2025гг.: ГОСТ Р 56920-2024 «Системная и программная инженерия. Тестирование программного обеспечения. Общие положения (ISO/IEC/IEEE 29119-1:2022, NEQ)»; ГОСТ Р 57193-2025 «Системная и программная инженерия. Процессы жизненного цикла систем (ISO/IEC/IEEE 15288:2021, NEQ)»; ГОСТ Р 71303-2024 «Системная и программная инженерия. Возможности программных инструментариев для организационного управления инцидентами. Общие положения (ISO/IEC 23531:2020, NEQ)»; ГОСТ Р 71304-2024 «Системная и программная инженерия. Гарантии обеспечения качества систем и программных средств. Основные понятия и термины (ISO/IEC/IEEE 15026-1:2019, NEQ)»; ГОСТ 71438-2024 «Информационные технологии. Оценка процессов. Система измерения процессов для оценки их возможностей (ISO/IEC 33020:2019, NEQ)», ГОСТ Р 71439-2024 «Системная и

программная инженерия. Методы и инструментарии продуктовой линейки программных средств и систем. Общие положения (ISO/IEC 26580:2021, NEQ)»; ГОСТ Р 71440-2024 «Информационные технологии. Оценка процессов. Руководство по определению рисков в процессах (ISO/IEC TR 33015:2019, NEQ)»; ГОСТ Р 71998-2025 «Информационные технологии. Требования и оценка качества систем и программного обеспечения. Определение качества ИТ-услуг (ISO/IEC TS 25025:2021, NEQ)». Это подтверждено актом ТК-МТК-022 о применении результатов исследований.

8. На основе применения предложенных программных, технологических и методических решений разработаны рекомендации по снижению и удержанию рисков в допустимых пределах в жизненном цикле различных систем. А именно (см. 8.1 – 8.6):

8.1. Продемонстрирован способ логического преобразования изначального вербального описания сложной системы к формализованному виду, позволяющему использовать предложенные в диссертации программные, технологические и методические решения для ВС и КС. В качестве системы без ограничения общности рассмотрен технический облик гипотетичной многоуровневой системы управления рисками в интересах обеспечения энергетической безопасности согласно "Доктрине энергетической безопасности Российской Федерации". Сведение вербального описания сложной системы к формализованному виду позволило применить возможности созданного прототипа технологии поддержки риск-ориентированной системной инженерии для формальной постановки и дальнейшего эффективного решения практических задач.

8.2. На основе прогнозирования рисков в приложении к сопровождаемым цифровым двойникам (на примере фрагментов магистральной трубопроводной сети) обеспечена прослеживаемость и аналитическая зависимость прогнозных рисков от влияющих факторов. Это открывает важные прагматические возможности для системного обоснования и дополнения технических мер, востребуемых по итогам регулярного диагностирования объекта, и способствует повышению безопасности его эксплуатации в условиях природных, технических, экономических и иных ограничений. За счет использования возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии проведение расчетов возможно не только за автоматизированным рабочим местом ВС в стационарных условиях, но и в полевых условиях, где возможно подключение к компьютерной сети.

8.3. На основе моделирования многомодального взаимодействия социокиберфизических систем в жизненном цикле обогатительной фабрики в угольной отрасли для изыскания путей усовершенствования (перевооружения) системы вентиляции,

аспирации и пылеподавления обоснован комплекс приемлемых условий к системе. Результаты расчетов позволили выявить «узкие места» и спрогнозировать снижение рисков на основе перевооружения. Вместе с тем, выявлен явный дисбаланс в системе после перевооружения - на самом деле длительный срок до нарушения набирается за счет сверхнадежной работы новых основных фондов, оставляя опасность «человеческого фактора» на прежнем уровне, т.е. обнаруженный эффект – только технический, но далеко не системный. Дополнительные системные исследования позволили обосновать комплекс приемлемых условий к системе вентиляции, аспирации и пылеподавления, соблюдение которых позволит удерживать частные и интегральный риски в допустимых пределах.

8.4. С использованием предложенных базовых моделей на примерах управления рисками для обеспечения качества хранимого зерна была выявлена закономерность: если условия хранения не допускают возникновения рассадников насекомых чаще, чем раз в неделю, вероятность сохранения качества хранимого зерна за 3-6 лет в 3-5 раз превышает вероятность потери качества. Результаты многолетних исследований ВНИИ Зерна подтвердили адекватность такого вывода. Тем самым результаты проведенных исследований в сравнении с результатами иных специализированных исследований (ВНИИ Зерна) явились дополнительной аргументацией в подтверждение адекватности разработанных вероятностных моделей и программных решений в различных их приложениях.

8.5. Продемонстрирована способность расширения аналитических возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии путем добавления другой модели. Так, разработаны вероятностные модели для оценки частных рисков невыявления некорректностей в машинном обучении (дообучении) при разработке и эксплуатации программных средств для систем искусственного интеллекта в условиях актуальных угроз подмены моделей машинного обучения (УБИ.222 по классификации ФСТЭК России) и их модификации путем искажения («отравления») обучающих данных (УБИ.221). Интегральный риск предложено оценивать через виртуальный показатель риска нарушения корректности машинного обучения в условиях рассматриваемых угроз в течение задаваемого периода прогноза в зависимости от рисков невыявления некорректностей в машинном обучении (дообучении) при разработке и эксплуатации программных средств, а через них – в зависимости от исходных данных, обеспечивающих расчет соответствующих рисков. Работоспособность предложенного подхода подтверждена количественными примерами.

8.6. Разностороннее использование возможностей созданного прототипа технологии поддержки риск-ориентированной системной инженерии продемонстрировано на решении

вопросов удержания в допустимых пределах рисков разрушения бизнеса применительно к фармацевтическому предприятию на этапах его проектирования и эксплуатации. Количественно доказано, что эффективность активного управления со стороны Руководства предприятия соизмерима с использованием мер дополнительного резервирования действий применительно ко всем службам организационного управления. Сформулированы условия, определяемые главным образом самими работниками предприятия (их ответственностью и широкой квалификацией для резервирования действий, формализуемыми временными характеристиками) при активном управлении и эффективной поддержке со стороны Руководства предприятия. Показано, что с высокой вероятностью именно соблюдение этих условий обеспечит сохранение бизнеса в долговременной перспективе. Прагматичность упреждающего прогнозирования рисков подтверждена актом реализации от производственного фармацевтического предприятия ООО «Пранафарм», приблизительный годовой экономический эффект оценен в 3 млн. руб. (за счет оптимизации организационного резервирования при ограничениях на допустимые риски и затраты).

9. Основными направлениями развития системной инженерии с использованием научных результатов диссертации для достижения целей государственной политики и эффективного решения задач в сфере обеспечения национальной безопасности определены:

– сосредоточение научно-технических усилий на достижении целей обеспечения требуемых безопасности, качества, сбалансированных эффектов и устойчивого функционирования и развития сложных систем;

– предоставление возможностей прогнозирования и упреждающего управления рисками в стандартных процессах жизненного цикла систем, совершенствование и накопление статистики и знаний, выявление общих аналитических закономерностей в интересах РФ;

– расширение на все решаемые задачи функциональных возможностей созданных моделей и методов системной инженерии, программных, технологических и методических решений по аналитическому прогнозированию и упреждающему управлению рисками, межприкладное применение баз данных и баз знаний, выявленных общих аналитических закономерностей в интересах Российской Федерации;

– трансформация существующего подхода к созданию и использованию моделей и методов системной инженерии, ориентированных на конкретную систему, в технологию искусственного интеллекта поддержки принятия логичных решений, подтверждаемых прогнозными исследованиями по достижению требуемых безопасности, качества, сбалансированных эффектов и устойчивого функционирования и развития систем различного функционального назначения.

Список литературы

1. Systems Engineering Handbook. A Guide for System Life Cycle Processes and Activities. Fifth Edition. 2023. INCOSE-TP-2003–002-05 URL: https://www.oreilly.com/library/view/incose-systems-engineering/9781119814290/f01.xhtml (дата обращения: 15.10.2025) - Текст: электронный.
2. Костогрызов, А. И. Инновационное управление качеством и рисками в жизненном цикле систем : монография / А.И. Костогрызов, П.В. Степанов. – М.: ВПК, 2008. – 404с. – ISBN 5-89370-012-0. - Текст: непосредственный.
3. Сухомлин, В.А. Введение в модельно-ориентированную системную и программную инженерию (MBSSE) : учебник / В.А. Сухомлин, В.Ю. Романов, Д.А. Гапанович. – Москва : Фонд «»Лига интернет-медиа». МАКС Пресс, 2024. - 672с. – ISBN 978-5-317-07289-6. - Текст: непосредственный.
4. **Нистратов, А.А.** Анализ тенденций в развитии системной инженерии / Костогрызов А.И., Нистратов А.А. // ИТ-стандарт : электронный журнал. - 2024, №3, - с. 4-20 https://itstd-journal.ru/?page_id=1080&article=315 (дата обращения: 15.10.2025) - Текст: электронный.
5. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Тематический блок "Национальная безопасность". Системная инженерия в проблемах национальной безопасности : монография / А. В. Анищенко, …А.А. Зацаринный, …, **А.А. Нистратов** [и др.]. Научный рук. – Махутов Н.А. - Москва: МГОФ «Знание», 2025. - 904 с. – ISBN 978-5-87633-211-0. - Текст: непосредственный.
6. Винер, Н. Кибернетика или Управление и связь в животном и машине : монография / Н. Винер. - Изд.2-е. М.: Сов.радио, 1968. -326с. - Текст: непосредственный.
7. Гуд, Г.Х. Системотехника: Введение в проектирование больших систем : монография / Г.Х. Гуд, Р.З. Макол – М.: Советское радио, 1962. – 383 с. - Текст: непосредственный.
8. Martin, J. System Analysis for Data Transmission. V. II / J. Martin, IBM System Research Institute. Prentice Hall, Inc., Englewood Cliffs. New Jersey. – 1972. - Текст: непосредственный.
9. Мартин, Дж. Системный анализ передачи данных : монография / Дж. Мартин - М.:Мир, 1975. т.2. - 432с. - Текст: непосредственный.
10. Kleinrock, L. Queueing systems, V.2: Computer applications / L. Kleinrock - John Wiley & Sons; New York. – 1976. - Текст: непосредственный.
11. Клейнрок, Л. Вычислительные системы с очередями : монография / Л. Клейнрок – М.: Мир, 1979. - Текст: непосредственный.
12. Boehm, B. Software Risk Management. / B. Boehm. Los Alamitos, CA; Tokyo, Japan: IEEE Computer Society Press, 1989. - pp. 115-125 - Текст: непосредственный.
13. Kumamoto, H. Probabilistic Risk Assessment and Management for Engineers and Scientists / H. Kumamoto and E. Henley. 2nd ed. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers (IEEE) Press. – 2011. - Текст: непосредственный.

14. Vose, D. Quantitative Risk Analysis / D. Vose 2nd ed. New York, NY, USA: John Wiley & Sons. 2000. - Текст: непосредственный.
15. Conrow, E.H. Effective Risk Management: Some Keys to Success / Conrow E.H. 2nd ed. Reston, VA, USA: American Institute of Aeronautics and Astronautics (AIAA). 2003. - Текст: непосредственный.
16. Mun, J. Modeling Risk, 2nd ed. Hoboken / J. Mun. USA: John Wiley & Sons 2010. - Текст: непосредственный.
17. Eid, M. Critical Infrastructure Disruption Scenarios Analyses via Simulation. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach / M. Eid, V. Rosato. SpringerOpen, - 2016. 43-62. - Текст: непосредственный.
18. Zio, En. An Introduction to the Basics of Reliability and Risk Analysis / En. Zio. World Scientific Publishing Co.Pte.Ltd; 2006. - Текст: непосредственный.
19. K. Kolowrocki K. Reliability and Safety of Complex Technical Systems and Processes / K. Kolowrocki, J. Soszynska-Budny Springer-Verlag London Limited. 2011 - Текст: непосредственный.
20. Гнеденко, Б.В. Приоритетные системы обслуживания : монография / Гнеденко Б.В., Даниелян Э.А., Димитров Б.Н., Климов Г.П., Матвеев В.Ф. - М.: МГУ, 1973.- 448 с. - Текст: непосредственный.
21. Месарович, М. Общая теория систем: математические основы : монография / М. Месарович, Я. Такахара – М: Мир, 1978, 312с. Текст: непосредственный.
22. Моисеев, Н.Н. Математические задачи системного анализа : монография / Н.Н. Моисеев – М.: Наука, 1981. – 488 с.– 239 с. - Текст: непосредственный.
23. Балыбердин, В.А. Методы анализа мультипрограммных систем : монография / В.А. Балыбердин – М. Радио и связь, 1982. – 152с. Текст: непосредственный.
24. Краснощеков, П.С. Принципы построения моделей : монография / П.С. Краснощеков, А.А. Петров. – М. Изд-во Московского университета. - 1983. – 264с. Текст: непосредственный.
25. Матвеев, В.Ф. Системы массового обслуживания : монография / В.Ф. Матвеев, В.Г. Ушаков - М.: МГУ, 1984. - Текст: непосредственный.
26. Дружинин, В. В. Системотехника : монография / В.В. Дружинин, Д.С. Конторов — М.: Радио и связь, 1985.- 200 с. - Текст: непосредственный.
27. Дружинин, Г.В. Надежность автоматизированных производственных систем : монография / Г.В. Дружинин — М.: Энергоатомиздат, 1986. - 480 с. Текст: непосредственный.
28. Мамиконов, А. Г. Достоверность, защита и резервирование информации в АСУ : монография / А.Г. Мамиконов, В.В. Кульба, А.Б. Шелков [и др.] - М.: Энергоатомиздат, 1986.-304 с. Текст: непосредственный.
29. Гнеденко, Б.В. Введение в теорию массового обслуживания : монография / Б.В. Гнеденко, И.Н. Коваленко - М.: Наука. 1987. Текст: непосредственный.
30. Балыбердин, В.А. Оценка и оптимизация характеристик систем обработки данных :

монография / В.А. Балыбердин – М.: Радио и связь, 1987. – 176с. - Текст: непосредственный.

31. Байхельт, Ф. Надежность и техническое обслуживание. Математический подход : монография / Ф. Байхельт, П. Франкен - М.: Радио и связь, 1988. -392с. Текст: непосредственный.
32. Костогрызов, А.И. Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа : монография / А.И. Костогрызов, А.В. Петухов, А.М. Щербина - М.: Изд. «Вооружение. Политика. Конверсия», 1994.- 278 с. - Текст: непосредственный.
33. Костогрызов, А.И. Сертификация функционирования автоматизированных информационных систем : монография / А.И. Костогрызов, В.В. Липаев - М.: Изд. «Вооружение. Политика. Конверсия», 1996.- 280 с. - Текст: непосредственный.
34. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности: монографии / Под ред. Махутова Н.А. – М.:МГОФ «Знание», 1998-2024, тома 1-70. - Текст: непосредственный.
35. Дружинин, Г.В. Учет свойств человека в моделях технологий : монография / Г.В. Дружинин - М.: МАИК "Наука/Интерпериодика", 2000. - 327 с. - Текст: непосредственный.
36. Прангишвили, И.В. Системный подход и общесистемные закономерности : монография / И.В. Прангишвили – М: СИНТЕГ, 2000, 528с. - Текст: непосредственный.
37. Костогрызов, А.И. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии : монография / А.И. Костогрызов, Г.А. Нистратов - М. Изд.”Вооружение, политика, конверсия”, 2004, 2-е изд.-2005.- 395с. – ISBN 5-902313-05-8. - Текст: непосредственный.
38. Липаев, В.В. Анализ и сокращение рисков проектов сложных программных систем : монография / В.В. Липаев – М.: СИНТЕГ, 2005. – 224с. - Текст: непосредственный.
39. Резников, Г.Я. Рациональный мониторинг процессов менеджмента качества на предприятиях (на примерах автомобильной и нефтегазовой промышленности и организаций повышения квалификации специалистов в Приволжском федеральном округе) : монография / Г.Я. Резников — М.: Изд-во «Мир», 2005 — 284 с. Текст: непосредственный.
40. Соложенцев Е.Д. Сценарное логико-вероятностное управление риском в бизнесе и технике : монография / Е.Д. Соложенцев – СПб.: Изд. Дом «Бизнес-пресса», 2006. – 530с. Текст: непосредственный.
41. Королев, В.Ю. Математические основы теории риска : монография / В.Ю. Королев, В.Е. Бенинг, С.Я. Шоргин – М.: Физ.-мат.лит., 2007 - Текст: непосредственный.
42. Синицын, И.Н. Фильтры Калмана и Пугачева : монография / И.Н. Синицын – М.: Логос, 2007. – 776с. - Текст: непосредственный.
43. Королев, В.Ю. Математические модели неоднородных потоков экстремальных событий : монография / В.Ю. Королев, И.А. Соколов -М.: ТОРУС ПРЕСС, 2008. – 192с. - Текст: непосредственный.

44. Григорьев, Л.И. Системные основы управления конкурентоспособностью в нефтегазовом комплексе / Л.И. Григорьев, В.Я. Кершенбаум, А.И. Костогрызов – М.:НИНГ, 2010, 374с. - Текст: непосредственный.
45. Шокин, Ю.И. Методика оценки антропогенных рисков территорий и построения картограмм рисков с использованием геоинформационных систем / Ю.И. Шокин, В.В. Москвичев, В.В. Ничепорчук // Вычислительные технологии. 2010. Т.15, №1. С. 120-131
46. Смелянский, Р.Л. Компьютерные сети: монография в 2 т. Т. 1. Системы передачи данных. / Р.Л. Смелянский - М.: Издательский центр «Академия». – 2011. – 304 с. - Текст: непосредственный.
47. Волчихин, В.И. Логико-алгебраические модели и методы в проектировании функциональной архитектуры распределенных систем хранения и обработки данных / В.И. Волчихин, С.А. Зинкин // Известия высших учебных заведений. Поволжский регион. Технические науки .— 2012 .— №2 .— С. 3-16 .— URL: https://rucont.ru/efd/269628 (дата обращения: 17.10.2025)
48. Емельянов, С.Г. Автоматизированные нечетко-логические системы управления : монография / С.Г. Емельянов - Инфра – М., 2012 ISBN 978-5-1600527-86 - Текст: непосредственный.
49. Kostogryzov, A. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, / Kostogryzov A., Nistratov G., **Nistratov A.** DOI: 10.5772/46106, Total Quality Management and Six Sigma, InTech, 2012, pp. 127-196, http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management (дата обращения: 15.10.2025) - Текст: электронный.
50. Зацаринный, А.А. Особенности проектирования и функционирования ситуационных центров / А.А. Зацаринный, А.П. Сучков., С.В. Козлов - Текст: непосредственный // Системы высокой доступности, 2012. Т.8, № 1. С. 12-22
51. Москвичев, В.В. Антропогенные и природные риски на территории Сибири / В.В. Москвичев, Ю.И. Шокин - Текст: непосредственный // Вестник РАН, 2012. Т. 82. № 2. С. 131-140
52. Kostogryzov, A. Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes / Kostogryzov A., Grigoriev L., Nistratov G., **Nistratov A**., Krylov V. // American Journal of Operations Research, 2013, 3, p.217-244. – DOI: 10.4236/ajor.2013.31A021, http://www.scirp.org/journal/ajor/ , https://www.scirp.org/journal/paperinformation?paperid=27562 (дата обращения: 15.10.2025) - Текст: электронный.
53. Kostogryzov, A. The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields / A. Kostogryzov, A. **Nistratov**, G. Nistratov // International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 3, September 2013, pp. 146-155. http://www.ijeit.com/archive.php
54. Костогрызов, А.И. Основы противоаварийной устойчивости угольных предприятий. / А.И. Костогрызов, В.Н. Костеренко, А.Н. Тимченко, В.Б. Артемьев - Библиотека горного инженера. Том 6 «Промышленная безопасность». Книга 11. - М.: Изд-во «Горное дело» ООО «Киммерийский центр», 2014. – 336с. - Текст: непосредственный.

55. Косяков, А. Системная инженерия. Принципы и практика: монография / А. Косяков, У. Свит [и др.] - М.: ДМК Пресс, 2014. 624 с. - Текст: непосредственный.
56. Киселева С.П. Теория эколого-ориентированного инновационного развития : диссертация на соискание ученой степени доктора экономических наук по специальности 08.00.05 / Киселева Светлана Петровна; Москва, ГОУВПО "Государственный университет управления", 2014. - 420с. - Текст: непосредственный.
57. Зацаринный, А.А. Об информационной поддержке деятельности в системах управления критическими технологиями на основе ситуационных центров / А.А. Зацаринный, С.В. Козлов, А.П. Шабанов - Текст: непосредственный // Системы управления, связи и безопасности, 2015, №4. - С.98-113.
58. Костогрызов, А.И. Прогнозирование рисков для обеспечения качества информации в сложных системах. / А.И. Костогрызов, П.В. Степанов, **А.А. Нистратов** [и др.] - Текст: непосредственный // Системы высокой доступности №3, т.2, 2016, с. 25-37
59. Синицын, И.Н. Методические вопросы развития российской интегрированной логистической поддержки для управления жизненным циклом наукоемкой продукции / И.Н. Синицын, А.С. Шаламов -Текст: непосредственный // Системы высокой доступности, 2016. Т.12. № 3. С.3–8.
60. Токарев, В.Л. Математическое обеспечение оценивания безопасности автоматизированных систем / В.Л. Токарев, А.А. Сычугов - Текст: непосредственный // Известия ТулГУ. Технические науки. Вып. 11. Часть 1 Тула: Изд-во ТулГУ, 2016. С. 158-166
61. Бычков И.В., Инфраструктура информационных ресурсов и технологии создания информационно-аналитических систем территориального управления : монография / И.В. Бычков, Г.М. Ружников, А.Е. Хмельнов. [и др.] - Новосибирск: Изд-во СО РАН, 2016. 238 с. - Текст: непосредственный
62. Шлюйкова, Д. П. Большие данные: современные подходы к хранению и обработке / Д.П. Шлюйкова – Текст: непосредственный // Наука, техника и образование. 2016. №1. С. 75-79.
63. Синицын, И.Н. Методическое и инструментальное программное обеспечение моделирования процессов в организационно-технико-экономических системах массового применения / И.Н. Синицын, А.С. Шаламов, Э.Р. Корепанов [и др.] - Текст : непосредственный // Системы высокой доступности, 2017. Т. 13. № 1. С. 65–90.
64. Artemyev V. Probabilistic methods of estimating the mean residual time before the next parameters abnor-malities for monitored critical systems. // Artemyev V., Kostogryzov A., **Nistratov A.** [etc.] - Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS- 2017), December 20-22, 2017, Milan, Italy, pp. 368-373 http://www.icsrs.org/
65. Васильев, В. И. Интеллектуальные системы защиты информации: учебное пособие / В. И. Васильев. 3-е изд., испр., и доп. – М.: «Издательство «Инновацонное машиностроение», 2017. – 200 с. - ISBN 978-5-9908302-6-4 - Текст: непосредственный.
66. Кудж, С.А. Информационное поле: Монография / Кудж С.А. — М.: МАКС Пресс, 2017. - 97 с. - Текст: непосредственный.

67. Москвичев, В.В. Информационная система территориального управления рисками развития и безопасностью / В.В. Москвичев, И.В. Бычков, В.П. Потапов [и др.] - Текст: непосредственный. // Вестник Российской академии наук. 2017. № 8. С. 696-705
68. Чернов, Д.В. Анализ современных требований и проблем обеспечения информационной безопасности автоматизированных систем управления технологическими процессами / Д.В. Чернов, А.А. Сычугов - Текст: непосредственный. // Журнал Нейрокомпьютеры: разработка, применение №8 - М.: "Изд.-во Радиотехника", 2018 с. 38-46
69. Kershenbaum, V. Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. / V. Kershenbaum, L. Grigoriev, P. Kanygin, **A. Nistratov** : IntechOpen, 2018: 55-79. http://dx.doi.org/10.5772/intechopen.74963
70. Kostogryzov, A. Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. / A. Kostogryzov, L. Grigoriev., **Nistratov A.** [etc.] Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI), Beijing, China. DEStech Publications, Inc., 2018, 298-303.
71. Зацаринный, А.А. Информационное пространство цифровой экономики. Концептуальные основы и проблемы формирования: монография / А.А. Зацаринный, Э.В. Киселев, В.А. Козлов, К.К. Колин. - Текст: непосредственный. - М.: ФИЦ ИУ РАН, 2018. 236 с.
72. Позин, Б.А. Принципы построения системы обеспечения жизненного цикла ответственных систем / Б.А Позин - Текст: непосредственный. // Труды института системного программирования РАН 2018, Том 30, №1, https://doi.org/10.15514/ISPRAS-2018-30(1)-7
73. Новиков, Д.А. Модели технологий / Д.А. Новиков, М.В. Белов - М.: Ленанд, 2019. - 160 с. - Текст: непосредственный
74. A. Kostogryzov, A. Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems / A. Kostogryzov and V. Korolev - Probability, Combinatorics and Control. - InTechOpen, 2020. DOI: http://dx.doi.org/10.5772/intechopen.89168
75. Колин К.К. Качество жизни в стратегии обеспечения национальной и глобальной безопасности / К.К. Колин - Текст: непосредственный // Проектирование будущего. Проблемы цифровой реальности, 2020, № 1. - С. 91-102
76. Язов, Ю.К. Сети Петри-Маркова и их применение при моделировании процессов реализации угроз безопасности информации в информационных системах : Монография / Ю.К. Язов, А.В. Анищенко - Воронеж: Кварта, 2020.–173 с. - Текст: непосредственный
77. Зацаринный, А.А. Приоритетные направления развития системной инженерии, предусматривающие применение риск-ориентированного подхода / А.А. Зацаринный, А.И. Костогрызов, **А.А. Нистратов** – Текст электронный // ИТ-Стандарт. – 2021. – № 4(29). – С. 23-37. – EDN FXJOMR https://itstd-journal.ru/?page_id=1080&article=243
78. Сычугов, А.А. Методы и алгоритмы оперативного обнаружения опасных состояний промышленных объектов : диссертация на соискание ученой степени доктора технических наук по специальности 05.13.01 / Сычугов Алексей Алексеевич; Тула, Тульский

государственный университет. - 2021г. – 256с. - Текст: непосредственный.

79. Борисов, В.В. Нечеткое ситуационное управление сложными системами на основе их композиционного гибридного моделирования / В.В. Борисов, Д.Ю. Авраменко - Текст: непосредственный // Системы управления, связи и безопасности. – 2021. – № 3. – С. 207-237. – doi: 10.24412/2410-9916-2021-3-207-237
80. Москвичёв, В.В. Цифровой паспорт безопасности территорий промышленных агломераций и регионов / В.В. Москвичёв, В.В. Ничепорчук, В.П. Потапов [и др.] - Текст: непосредственный // Вычислительные технологии. 2021. Т. 26. № 6. С. 110-132 - DOI:10.25743/ICT.2021.26.6.008
81. Четверушкин Б.Н., Якобовский М.В. О перспективах развития в России высокопроизводительных вычислений и предсказательного моделирования в современных технологиях / - Текст: непосредственный // Вестник Российской академии наук, 2021, Т.91, №12, с. 1108-1114. doi: 10.31857/S0869587321120057
82. Петренко С.А. Кибериммунология: научная монография / Петренко С.А. – СПб: «Издательский Дом «Афина». – 2021. – 240с. ISBN 978-5-9909868-7-9 - Текст: непосредственный
83. **Нистратов, А. А.** Аналитическое прогнозирование интегрального риска нарушения приемлемого выполнения совокупности стандартных процессов в жизненном цикле систем высокой доступности. Часть 1. Математические модели и методы / **А. А. Нистратов** - Текст: непосредственный // Системы высокой доступности. – 2021. – Т. 17, № 3. – С. 16-31. – DOI: 10.18127/j20729472-202103-02. – EDN ZTCLJK
84. **Нистратов, А.А.** Аналитическое прогнозирование интегрального риска нарушения приемлемого выполнения совокупности стандартных процессов в жизненном цикле систем высокой доступности. Часть 2. Программно-технологические решения. Примеры применения / **А. А. Нистратов** - Текст: непосредственный // Системы высокой доступности. – 2022. – Т. 18. – № 2. – С. 42-57. – DOI 10.18127/j20729472-202202-03. – EDN OVKLYJ
85. Костогрызов, А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии / А.И. Костогрызов - Текст: непосредственный // Вопросы кибербезопасности. 2022, №6(52), с.71-82. DOI:10.21681/2311-3456-2022-6-71-82
86. Шабанов Б.М. Методы и способы построения, выбора и применения высокопроизводительных вычислительных систем для выполнения научных и технических задач : Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.15 / Шабанов Борис Михайлович; Москва, Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук, 2019. – 264с. URL: https://www.frccsc.ru/sites/default/files/docs/ds/002-073-02/diss/08-shabanov/ds02-08-shabanov_main.pdf (дата обращения 21.04.2025).
87. Промыслов, В.Г. Оценка риска и обеспечение кибербезопасности атомных электростанций :

монография / В.Г. Промыслов, Н.Н. Акимов, …, Р.В. Мещеряков…[и др.] – М. ИПУ РАН, 2022. – 193с. ISBN/ISSN: 978-5-91450-262-8. - Текст: непосредственный

88. Москвичев В.В. Кластерный анализ в оценке территориальных рисков социально-природно-техногенных систем / В.В. Москвичев, У.С. Постникова, О.В. Тасейко - Текст: непосредственный // Вычислительные технологии. 2022. Т. 27. № 3
89. Гарбук, С.В. Задачи нормативно-технического регулирования интеллектуальных систем обработки данных дистанционного зондирования Земли /С.В. Гарбук. - Текст: непосредственный // «Современные проблемы дистанционного зондирования Земли из космоса». 2022. Т. 19, №1. С.107-122
90. Арустамян, С.С. Методические и реализационные аспекты внедрения процессов разработки безопасного программного обеспечения / С.С. Арустамян, В.В. Вареница, А.С. Марков - Текст: непосредственный // Безопасность информационных технологий. 2023. Т. 30. № 2. С. 23-37.
91. Колин, К.К. Структура показателей качества жизни для мониторинга ситуации в регионах России с использованием системы ситуационных центров. / К.К. Колин. В сборнике: Физико-техническая информатика (СРТ2023). Материалы Международной конференции. - Нижний Новгород, 2023. С. 12-21 - Текст: непосредственный
92. Котенко, И.В. Методология сбора данных для анализа безопасности промышленных киберфизических систем / И.В. Котенко, Е.В. Федорченко, Е.С. Новикова [и др.] - Текст: непосредственный // Вопросы кибербезопасности. 2023. № 5(57). С. 69-79.. doi: 10.21681/2311-3456-2023-5-69-79
93. Лысачев, М.Н. Искусственный интеллект. Анализ, тренды, мировой опыт / М. Н. Лысачев, А .Н. Прохоров. Под. ред. Д. А. Ларионов. — Корпоративное издание. — Москва; Белгород: КОНСТАНТА-принт, 2023. — 460с. ISBN 978-5-6048180-7-7. URL: data.digitalatom.ru/books/Artificial_Intelligence_book.pdf
94. Парамонов, Н.Б. Интеллектуальные методы управления наземными роботами / Н.Б. Парамонов, Н. А. Бочаров, К. А. Суминов. - Текст : непосредственный // Искусственный интеллект. Теория и практика : научно-практический междисциплинарный журнал. - 2023. - N 2. - С. 76-80. - ISSN 2949-3250
95. Язов, Ю.К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Санкт-Петербург: Наукоемкие технологии, 2023 г. – 258 с. - Текст: непосредственный
96. Котенко, И.В. Обнаружение атак на веб-приложения: анализ современных подходов. / И.В. Котенко, П.С. Соболев. Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024): XIII Международная научно-техническая и научно-методическая конференция (Санкт-Петербург, 27-28 февраля 2024г.): сборник научных статей. 2024. Т. 1. С. 497-501 Текст : непосредственный
97. Зацаринный, А. А. О перспективных программно-технологических решениях для

прогнозирования рисков в интеллектуальных системах управления и связи / А. А. Зацаринный, **А. А. Нистратов** – Текст : электронный // Радиолокация, навигация, связь : Сборник трудов XXXI Международной научно-технической конференции. В 6-ти томах, Воронеж, 15–17 апреля 2025 года. – Воронеж: Воронежский государственный университет, 2025. – С. 290-297. – EDN NEIRQK

98. Забежайло, М.И. К проблеме интеграции статистических и детерминистских методов интеллектуального анализа эмпирических данных / М.И. Забежайло Труды XXII Национальной конференции по искусственному интеллекту с международным участием (КИИ 2025). - 2025. - Том 1, с. 192 – 203, doi: 10.15622/rcai.2025.018
99. Борисов, В.В. Мягкие ситуационно-когнитивные модели для интеллектуальной поддержки принятия решений / В.В. Борисов, А.С. Федулов, С.А. Федулов Труды XXII Национальной конференции по искусственному интеллекту с международным участием (КИИ 2025). – 2025. - Том 2, с. 20-32 doi: 10.15622/rcai.2025.033
100. Шевалдов, С.С. Подход к поиску компонентов для программных систем на основе анализа мультимодальных данных. / С.С. Шевалдов, С.С. Филиппов Труды XXII Национальной конференции по искусственному интеллекту с международным участием (КИИ 2025). 2025. - Том 3, с. 424 – 434. doi: 10.15622/rcai.2025.103
101. **Нистратов, А.А.** Математическое моделирование стандартизованных процессов через Интернет для управления качеством и рисками / **А.А. Нистратов**, Г.А. Нистратов - Текст: непосредственный // Информатизация и связь. 2009, №3 , с. 29-39
102. Kostogryzov, A. Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems / A. Kostogryzov, V. Krylov, **A. Nistratov** [etc.]. Proceedings of the 1st Intern. Conf. on Transportation Information and Safety, ICTIS, June 30–July 2, 2011, Wuhan, China, pp. 845–854.
103. Попов, В.М. Вероятностный прогноз нарушения безопасности функционирования типовой системы инженерного обеспечения предприятия / В.М. Попов, А.И. Костогрызов, **А.А. Нистратов** [и др.] - Текст: непосредственный // Системы высокой доступности. 2011г. №3. с. 48-60
104. Костогрызов, А.И. Инновационный подход к управлению качеством и рисками в системе государственного материального резерва / А.И. Костогрызов, Г.А. Нистратов, **Нистратов А.А.** [и др.] - Текст: непосредственный // Сборник докладов международной научно-практической конференции “О проблемах обеспечения в современных условиях количественной и качественной сохранности материальных ценностей, поставляемых и закладываемых в государственный резерв”, часть 1, 05-06 сентября 2011 г., с. 356-370
105. Kostogryzov, A. Probabilistic predictive modeling for complex system risk assessments / A. Kostogryzov, N. Makhutov, **A. Nistratov**, G. Reznikov. - Time Series Analysis - New Insights. IntechOpen, 2023, pp. 73-105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments

106. Костогрызов, А.И. Методы и инструментарии прогнозирования качества и рисков и примеры их практических приложений для управления эффективностью систем в информационном обществе / А.И. Костогрызов, Г.А. Нистратов, **А.А. Нистратов А.А.** [и др.] - Текст: непосредственный // Сборник статей, тезисов докладов и материалов к конференции «Стандартизация, сертификация, обеспечение эффективности, качества и безопасности информационных технологий», 11-12 октября 2011, с. 7-19

107. Костогрызов, А.И. Управление рисками для обеспечения эффективности системы противоаварийной устойчивости опасных промышленных объектов. Часть 1. Общие положения / А.И. Костогрызов, А.Н. Тимченко, **Нистратов А.А.** [и др.] - Текст: непосредственный // Автоматизация, телемеханизация и связь в нефтяной промышленности 2012, №3, с. 21 – 35

108. Костогрызов, А.И. Управление рисками для обеспечения эффективности системы противоаварийной устойчивости опасных промышленных объектов. Часть 2. Стратегия и примеры / А.И. Костогрызов, А.Н. Тимченко, **Нистратов А.А.** [и др.] - Текст: непосредственный // Автоматизация, телемеханизация и связь в нефтяной промышленности 2012, №5, с. 18-28

109. Костогрызов, А.И. Моделирование процессов функционирования поста контроля почтовой корреспонденции / А.И. Костогрызов, **А.А. Нистратов**, Г.А. Нистратов [и др.] - Текст: непосредственный // Системы высокой доступности 2012, №1, т.8. - стр. 22-32

110. Костогрызов, А.И. Задачи обеспечения эффективности системы противоаварийной устойчивости предприятий и подходы к их решению / А.И. Костогрызов,…Бурцева А.Е., **А.А. Нистратов** [и др.] - Текст: непосредственный // Тезисы докладов IX Всероссийской научно-технической конференции «Актуальные проблемы развития нефтегазового комплекса России», Москва, 30.01 – 01.02.2012г., Часть 2, с 108.

111. Костогрызов, А.И. Прогноз качества и рисков для сложных систем: методы, технологии, возможности, эффекты / А.И. Костогрызов, …Григорьев Л.И., **Нистратов А.А.** - Текст: непосредственный // Тезисы докладов V Международной научно-технической конференции "Компьютерные технологии поддержки принятия решений в диспетчерском управлении газотранспортными и газодобывающими системами", Москва, 24-26 октября 2012г., с.45

112. Kostogryzov, A. Applicable Technologies to Forecast, Analyze and Optimize Reliability and Risks for Complex Systems / A. Kostogryzov A., **A. Nistratov,** G. Nistratov // Proceedings of the 6st International Summer Safety and Reliability Seminar, Poland, 2-8 September, Volume 3, Number 1, 2012, pp. 1-14

113. Kostogryzov, A. Knowledge mining based on Applications of the methods and technologies of risks prediction / A. Kostogryzov, V. Krylov, A. Nistratov [etc.] // Proceedings of the 2nd International Conference on Transportation Information and Safety (ICTIS2013, Wuhan, China）, June 28th ~July 1st 2013. p. 1214-1223

114. Kostogryzov, A.I. Innovative Management Based on Risks Prediction / A.I.

Kostogryzov,…G.A. Nistratov, **A.A. Nistratov** [etc.] // Information Engineering and Education Science – Zheng (Ed.). ©2015 Taylor & Francis Group, London, pp. 159-166

115. Костогрызов, А.И. Эффективные решения прикладных задач системной инженерии на основе адекватного прогнозирования рисков / А.И. Костогрызов, С.Г. Емельянов,…**А.А. Нистратов** [и др.] - Текст: непосредственный // Сборник научных трудов. Национальный исследовательский университет «Высшая школа экономики». – М.: Издательство НИУ ВШЭ, 2015 – 234с. (сс. 87-100) ISBN 978-5-94768-073-7

116. Kostogryzov, A. About accuracy of risks prediction and importance of increasing adequacy of used adequacy of used probabilistic models. / A. Kostogryzov A., **A. Nistratov**, I. Zubarev [etc.]. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars, Volume 6, Numbers 2, 2015: 71-80.

117. Kostogryzov, A. Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling / A. Kostogryzov, P. Stepanov, **A. Nistratov** [etc.] // Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016, Beijing, China, pp. 186-192. Copyright © 2016. The authors - Published by Atlantis Press www.dropbox.com/s/a4zw1yds8f4ecc5/AMSM2016%20Full%20Proceedings.pdf?dl=0

118. Бордюже, В.В. Импортозамещение программного обеспечения в нефтегазовом комплексе и пути решения возникающих проблем на принципах системной инженерии. / В.В. Бордюже, Л.И. Григорьев, А.И. Костогрызов, **А.А. Нистратов.** - Текст: непосредственный // Управление качеством в нефтегазовом комплексе, 2016, №1, с. 20-26

119. Костогрызов, А.И. Приложение принципов системной инженерии к аналитическому решению задач анализа и обоснования технического облика комплексов средств автоматизации организационных структур систем управления / А.И. Костогрызов, В.М. Лазарев, О.А. Литвинов, **А.Н. Нистратов** - Текст: непосредственный // Оборонный комплекс – научно-техническому прогрессу России, 2016, №2 (130), с.10-19

120. Kostogryzov A. Analytical modelling operation processes of composed and integrated information systems on the principles of system engineering. / A. Kostogryzov, P. Stepanov, **A. Nistratov** [etc.] // Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars, Volume 7, Number1, 2016, pp. 157-166 http://jpsra.am.gdynia.pl/archives/jpsra-2016-contents/

121. Костогрызов, А.И. Об обосновании путей повышения качества информационных технологий на принципах системной инженерии. / А.И. Костогрызов, П.В. Степанов, **А.А. Нистратов** [и др.] - Текст: непосредственный // Сборник трудов 7-й Международной конференции "ИТ-Стандарт 2016», М.: «TCDprint», 2016, с. 33-44

122. Kostogryzov, A. Enhancing System Preparedness by the Method of Sequence Rationale to Perform Heterogeneous Repair Works in Time. / A. Kostogryzov, P. Stepanov, **A. Nistratov** [etc.] // Proceedings of the 52nd ESReDA Seminar "Critical Infrastructures: Enhancing Preparedness & Resilience for the Security of Citizens and Services Supply Continuity" Hosted by the Lithuanian Energy Institute & Vytautas Magnus University, May 30-31, 2017, Kaunas, Lithuania, pp. 196-207,

http://www.esreda.org/

123. **Нистратов, А.А.** Подход к прогнозированию остаточного времени до нарушения целостности системных элементов на основе выявления закономерностей в их функционировании в условиях неопределенности / **А.А. Нистратов,** Г.А. Нистратов - Текст: непосредственный // Сборник трудов 8-й Международной конференции "ИТ-Стандарт 2017», М.: Издательство «Проспект», 2017, с. 96-104

124. **Нистратов, А.А.** Прогнозирование времени до нарушения целостности системных элементов в условиях неопределенности / **А.А. Нистратов А.А.,** Г.А. Нистратов - Текст: электронный // ИТ-Стандарт, 2017 №4. https://itstd-journal.ru/?page_id=1080&article=105

125. Kostogryzov, A. The method of rational dispatching a sequence of heterogeneous repair works. / A. Kostogryzov, O. Atakishchev, **A. Nistratov** [etc.] // Energetica. 2017. Vol.63, No 4, P. 154-162 www.lmaleidyka.lt/ojs/index.php/energetika/index

126. Julina, S. The probabilistic analysis of the remote monitoring systems of critical infrastructure safety. / S. Julina, T. Kuznetsova,…**A. Nistratov** [etc.] // Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars, Volume 8, Number 1, 2017, pp. 183-188 http://jpsra.am.gdynia.pl/archives/jpsra-2017-contents/

127. Kostogryzov, A. About Probabilistic Risks Analysis During Longtime Grain Storage. / A. Kostogryzov, P. Stepanov, **A. Nistratov** [etc.] // Proceedings of the 2017 2nd ACSS Internationale Conference on the Social Science and Teaching Research (ACSS-SSTR), June 28-29, 2017, Moscow, Russia. Volume 18 of Advances in Social and Behavioral Science. Edited by Harry Zhang. Copyright ©Singapore Management and Sports Science Institute, PTE.LTD . Pp.3-8

128. Kostogryzov, A. Improvement of Existing Risks Control Concept for Complex Systems by the Automatic Combination and Generation of Probabilistic Models and Forming the Storehouse of Risks Predictions Knowledge. / A. Kostogryzov, …Atakishchev O., **Nistratov A.** [etc.] // Proceedings of the 2nd International Conference on Applied Mathematics, Simulation and Modelling (AMSM 2017), August 6-7, Phuket, Thailand. DEStech Publications, Inc. pp. 279-283

129. Kostogryzov, A. Probabilistic modelling processes of mutual monitoring operators actions for transport systems /A. Kostogryzov,…G.Nistratov **A. Nistratov** [etc.]//Proceedings of the 4th International Conference on Transportation Information and Safety,ICTIS2017, Canada, Banff. pp. 865-871 https://www.engineeringvillage.com/search/expert.url?SEARCHID=322d8752M18f5M4bfeM9f03Mfa2c59de2491&COUNT=1&usageOrigin=&usageZone=

130. Kostogryzov A. Optimization of sequence of performing heterogeneous repair work for transport systems by criteria of timeliness / A. Kostogryzov, V. Panov,…**A. Nistratov A.** // Proceedings of the 4th International Conference on Transportation Information and Safety, ICTIS 2017, Canada, Banff. pp. 872-876 https://www.engineeringvillage.com/search/expert.url?SEARCHID=322d8752M18f5M4bfeM9f03Mfa2c59de2491&COUNT=1&usageOrigin=&usageZone=

131. Жулина, С.А. Вероятностный анализ качества функционирования систем дистанционного контроля промышленной безопасности. / Жулина С.А., …**Нистратов А.А.,** Нистратов Г.А. [и

др.] - Текст: непосредственный // Автоматизация, телемеханизация и связь в нефтяной промышленности № 6, 2017, с. 11-19

132. Kostogryzov, A. The probabilistic analysis of the possibilities to keep "organism integrity" by continuous monitoring. / A. Kostogryzov A., **A. Nistratov,** Nistratov G. [etc.] // Proceedings of the International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA 2018, March 25-26, Chengdu, China), Atlantis Press, Advances in Intelligent Systems Research, volume 159, 2018, pp. 432-435 doi:10.2991/mmsa-18.2018.96 https://www.atlantis-press.com/proceedings/mmsa-18/25894351

133. Kostogryzov, A. Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. / A. Kostogryzov, L. Grigoriev,…**A. Nistratov** [etc.] // Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI 2018), Beijing, China, April 22-23,2018. DEStech Publications, Inc. 2018, pp. 298-303. http://www.dpi-proceedings.com/index.php/dtcse/issue/view/279

134. Kostogryzov, A. The Experience of Probabilistic Modeling and Optimization of a Centralized Heat Supply System Which is an Object for Modernization. / A. Kostogryzov,…, S. Golovin, **A. Nistratov** [etc.] // Proceedings of the International Conference on Physics, Computing and Mathematical Modeling (PCMM 2018, April 15-16, Shanghai), DEStech Publications, Inc. 2018, pp.93-97. http://www.dpi-proceedings.com/index.php/dtcse/issue/view/273

135. Kostogryzov, A. Probabilistic estimations of increasing expected reliability and safety for intelligent manufacturing / A. Kostogryzov A., A. Rybas,…**A. Nistratov A.** [etc.] // Proceedings of the «GLOBAL SMART INDUSTRY CONFERENCE, November 13-15, 2018, Chelyabinsk, Russia. Doi: 10.1109/GloSIC.2018.8570112 https://ieeexplore.ieee.org/document/8570112

136. Kostogryzov, A. Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. / A. Kostogryzov, **A. Nistratov,** G. Nistratov - In: Sukhomlin, V., Zubareva, E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science // Communications in Computer and Information Science. – 2020. – vol 1201. Springer, Cham – P. 352-364. – https://doi.org/10.1007/978-3-030-46895-8_27. – EDN XHCTWA

137. Костогрызов, А.И. Модели системной инженерии для обоснования требований, оценки эффективности, определения «узких мест» и выработки рекомендаций по упреждающим мерам в результате прогнозной аналитической обработки данных мониторинга / А.И. Костогрызов А.И., **А.А. Нистратов,** Г.А. Нистратов // Сборник трудов IX Международной конференции «ИТ-Стандарт 2019», 11-12 марта 2019г. РТУ МИРЭА, сс. 11-24

138. Kostogryzov, A. The Approach to Probabilistic Prediction of Pipelines Safety for Quantitative Rationale Preventive Measures of Control during Design and Operation. / A. Kostogryzov,…, S. Golovin, **A. Nistratov** [etc.] // Advances in Intelligent Systems Research. 2019, Volume 165, pp. 158-161. DOI: https://doi.org/10.2991/smont-19.2019.35, https://www.atlantis-press.com/proceedings/smont-19/55917637

139. Kostogryzov, A. Probabilistic Models and Methods for Processing Data in “Smart” Monitoring System to Define Rational Preventive Measures of Supporting Reliability and Safety. / A. Kostogryzov, A. Artemyev,…**A. Nistratov** [etc.] // Critical Service continuity, Resilience and Security: 56th European Safety, Reliability & Data Association (ESReDA) Seminar. Hosted by the Johannes Kepler University, Linz, Austria, May 23-24, 2019. Publications Office of the European Union, Luxembourg, 2019, pp. 33-45. https://ec.europa.eu/jrc JRC118427, doi:10.2760/23760

140. Kostogryzov, A. Probabilistic data analysis for predicting mean time before critical integrity losses of complex system when explicit quantitative requirements to integrity are not specified. / A. Kostogryzov, **A. Nistratov,** G. Nistratov // 12-th International Conference “Computer Data Analysis & Modeling” (CDAM 2019). Stochastics and Data Science. Minsk, Belarus, September 18-22, 2019, pp. 203-206. http://www.cdam.bsu.by

141. Kostogryzov A. Estimation of stakeholders satisfaction in application to socially significant systems. / A. Kostogryzov A., V. Panov,…**A. Nistratov** [etc.] // Proceedings of the 6th Inter-national Conference Actual Problems of System and Software Engineering (APSSE 2019), Moscow, Russia, 12-14 November, 2019, pp. 10-16. Published by the IEEE Computer Society. Doi:10.1109/APSSE47353.2019.00008

142. Kostogryzov, A. Probabilistic analysis of projects viability. / A. Kostogryzov, O. Atakishchev,… **A. Nistratov** [etc.] // Proceedings of the 6th International Conference Actual Problems of System and Software Engineering (APSSE 2019), Moscow, Russia, 12-14 November, 2019, Vol-2514, pp. 56-65. http://ceur-ws.org/Vol-2514/paper27.pdf , http://ceur-ws.org/Vol-2514/

143. Костогрызов, А.И. Модели системной инженерии для обоснования требований, оценки эффективности, определения "узких мест" и выработки рекомендаций по упреждающим мерам в результате прогнозной аналитической обработки данных мониторинга / А.И. Костогрызов, **А.А. Нистратов,** Г.А. Нистратов - Текст: непосредственный // ИТ-Стандарт. – 2020. – № 2(23). – С. 4-14. – EDN GYMLJY https://itstd-journal.ru/?page_id=1080&article=191

144. Kostogryzov, A. Probabilistic Comparisons of Systems Operation Quality for Uncertainty Conditions / A. Kostogryzov, P. Kanygin, **A. Nistratov** // Reliability: Theory & Applications. – 2020. – Vol. 15, No. 1(56). – P. 63-73. – DOI 10.24411/1932-2321-2020-11007. – EDN OHSZWW

145. **Нистратов, А. А.** Подход к интеграции разнородных рисков на примере анализа целей, задач и угроз по доктрине энергетической безопасности / А.А. Нистратов // Безопасные информационные технологии : Сборник трудов Одиннадцатой международной научно-технической конференции, Москва, 06–07 апреля 2021 года. – Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2021. – С. 255-262. – EDN VRTUDP

146. Авдонин, Р. Ю. Вероятностная оценка рисков для реализации процесса управления человеческими ресурсами системы / Р.Ю. Авдонин, А.И. Костогрызов А.И., **А.А. Нистратов** - Текст: непосредственный // Безопасные информационные технологии : Сборник трудов Одиннадцатой международной научно-технической конференции, Москва, 06–07 апреля

2021 года. – Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2021. – С. 2-11. – EDN ZAEYCS

147 Авдонин, Р. Ю. Методы анализа рисков для процесса управлении знаниями о системе / Р.Ю. Авдонин, А.И. Костогрызов А.И., **А.А. Нистратов** - Текст: непосредственный // Безопасные информационные технологии : Сборник трудов Одиннадцатой международной научно-технической конференции, Москва, 06–07 апреля 2021 года. – Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2021. – С. 12-19. – EDN KLQWSF

148. Kostogryzov, A.I. The estimation of probabilistic risks for the performance of system human resource management process / A.I. Kostogryzov, R.Y. Avdonin, **A.A. Nistratov** // CEUR Workshop Proceedings: BIT 2021 - Selected Papers of 11th International Scientific and Technical Conference on Secure Information Technologies, Moscow, 06–07 апреля 2021 года. – CEUR: CEUR, 2021. – P. 76-87. – EDN VSJMVK

149. Костогрызов. А. И. О приоритетных направлениях развития системной инженерии / А.И. Костогрызов, **А.А. Нистратов** - Текст: электронный // Современные информационные технологии и ИТ-образование. – 2021. – Т. 17, № 2. – С. 223-240. – DOI: 10.25559/SITITO.17.202102.223-240. – EDN OHADEB.

150. Костогрызов, А.И. Подходы к прогностической обработке данных в системах искусственного интеллекта. Часть 1. О возможностях вероятностных методов / А.И. Костогрызов, **А.А. Нистратов** - Текст: электронный // ИТ-Стандарт. – 2021. – № 4(29). – С. 4-22. – EDN KNUZYT https://itstd-journal.ru/?page_id=1080&article=244

151. **Нистратов, А. А.** Математические методы проактивного управления интегральными рисками при использовании стандартных процессов системной инженерии / **А.А. Нистратов** - Текст: электронный // ИТ-Стандарт. – 2022. – № 1(30). – С. 33-50. – EDN BTUKDT https://itstd-journal.ru/?page_id=1080&article=248

152. Костогрызов, А.И. Подходы к прогностической обработке данных в системах искусственного интеллекта. Часть 2. Достижение практических эффектов / А.И. Костогрызов, **А.А. Нистратов** - Текст: электронный // ИТ-Стандарт. - 2022, №1, с.4-23 https://itstd-journal.ru/?page_id=1080&article=250

153. Kostogryzov, A. Methodical rationale of system solutions to reduce risks and retain them within acceptable limits for knowledge management process / A.I. Kostogryzov, R.Y. Avdonin, **A.A. Nistratov** // RTA&A No4(71), Vol. 17, December 2022, pp. 50-54

154. **Нистратов, А. А.** О математических, программно-технологических и методических решениях, ориентированных на рациональное управление рисками в системной инженерии / **А.А. Нистратов** - Текст: непосредственный // Россия в XXI веке в условиях глобальных вызовов: проблемы управления рисками и обеспечения безопасности социально-экономических и социально-политических систем и природно-техногенных комплексов : сборник материалов Всероссийской научно-практической конференции, Москва, 26–27

апреля 2022 года / Российская академия наук, Международный независимый эколого-политологический университет, Государственный университет управления. Том Выпуск 1. – Москва: Государственный университет управления, 2022. – С. 251-255. – EDN KHPYGC.

155. Костогрызов, А.И. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом. / А.И. Костогрызов, **А.А. Нистратов** - Текст: непосредственный // Вопросы кибербезопасности. 2023, №5. С. 9-24 DOI:10.21681/2311-3456-2023-5-9-24

156. **Нистратов, А.А.** Вероятностное моделирование сопровождаемого цифрового двойника фрагментов магистральной трубопроводной сети для упреждающего противодействия природным угрозам. / **А.А. Нистратов** - Текст: непосредственный // Материалы XXVI Международной научной конференции «Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2023)». 25–29 сент. 2023 г., Москва / под общ. ред. В.М. Вишневского, К.Е. Самуйлова; Институт проблем управления им. В.А. Трапезникова Рос. акад. наук. –Москва : ИПУ РАН, 2023. С. 132-139.

157. **Нистратов, А.А.** Об архитектурных решениях, ориентированных на прогнозирование и рациональное управление рисками в системной инженерии / **А.А. Нистратов** - Текст: непосредственный // Материалы XXVI Международной научной конференции «Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2023)». 25–29 сент. 2023 г., Москва / под общ. ред. В.М. Вишневского, К.Е. Самуйлова; Институт проблем управления им. В.А. Трапезникова Рос. акад. наук. – Москва : ИПУ РАН, 2023. С. 139-146

158. Костогрызов, А.И. Вероятностное прогнозирование рисков в стандартах системной инженерии / А.И. Костогрызов, **А.А. Нистратов** - Текст: непосредственный // Сборник трудов XII Международной научной конференции «ИТ-Стандарт 2023». М.: Издательство «Проспект», 2023. С. 6-30. - ISBN 978-5-98597-537-6

159. **Нистратов, А.А.** Прогнозирование рисков по цифровому двойнику, сопровождаемому в процессе промышленной эксплуатации объекта / **А.А. Нистратов** - Текст: непосредственный // Сборник материалов конференции «Кибернетика и информационная безопасность». МИФИ, 2023. С.92-93

160. **Нистратов, А.А.** Человеко-машинный интерфейс для прогнозирования и рационального управления рисками в системной инженерии. / **А.А. Нистратов** - Текст: непосредственный // Сборник трудов XII международной научно-технической конференции "Безопасные информационные технологии", М.: МГТУ им. Н.Э. Баумана, 2023, С. 161-165 ISBN 978-5-6045553-8-5

161. Костогрызов, А.И. Вероятностное прогнозирование рисков в стандартах системной инженерии / А.И. Костогрызов, **А.А. Нистратов** - Текст: электронный // ИТ-Стандарт. 2023, №1, С.4-10 https://itstd-journal.ru/?page_id=1080&article=276

162. **Нистратов, А.А.** Об ожиданиях, ограничениях и прикладных возможностях

стандартизованных моделей и методов прогнозирования рисков в системной инженерии / **А. А. Нистратов** - Текст: электронный // ИТ-Стандарт. – 2024. – № 3(40). – С. 31-51. https://itstd-journal.ru/?page_id=1080&article=313

163. Костогрызов, А.И. Методический подход к вероятностному прогнозированию и сравнению качества функционирования систем в условиях неопределенности / А.И. Костогрызов, **А.А. Нистратов** - Текст: непосредственный // Надежность. 2024. №1. С. 10-24 https://doi.org/10.21683/1729-2646-2024-24-1-10-24

164. Костогрызов, А.И. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 1. Общий подход / А.И. Костогрызов, **А.А. Нистратов** - Текст: непосредственный // Правовая информатика, 2024, №3, с. 13-31 DOI: 10.24682/1994-1404-2024-3-13-31

165. Костогрызов, А.И. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 2. Моделирование с использованием «черных ящиков» / А.И. Костогрызов, **А.А. Нистратов,** П.Е. Голосов - Текст: непосредственный // Вопросы кибербезопасности, 2024, №6, с. 3-28 DOI: 10.21681/2311-3456-2024-6-2-27

166. Костогрызов, А.И. Методические положения по вероятностному прогнозированию качества функционирования информационных систем. Часть 3. Моделирование сложных систем. Интегральный анализ / А.И. Костогрызов, **А.А. Нистратов,** П.Е. Голосов - Текст: непосредственный // Вопросы кибербезопасности, 2025, №2, с. 2-19. DOI: 10.21681/2311-3456-2025-2-2-19

167. **Нистратов, А.А.** О вероятностных моделях, программных, технологических и методических решениях для рационального управления рисками в системной инженерии / **А. А. Нистратов** - Текст: электронный // ИТ-Стандарт. – 2025. – № 1(42). – С. 23-49. https://itstd-journal.ru/?page_id=1080&article=329

168. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А., Нистратова Е.Н. Моделирование процессов в жизненном цикле систем "Моделирование процессов" - "ноу-хау" // Свидетельство о государственной регистрации программы для ЭВМ №2004610858.

169. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А. Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем // Свидетельство о государственной регистрации программы для ЭВМ №2006610219.

170. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А. и др. "Программно-инструментальный комплекс оценки качества функционирования информационных систем через Интернет «КОК-Интернет» // Свидетельство о государственной регистрации программы для ЭВМ №2008612348.

171. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А., Стойликович В. [и др.] "Программно-инструментальный комплекс сопровождения систем менеджмента качества «OPISys-КОК-Интернет»" // Свидетельство о государственной регистрации программы для ЭВМ

№2008614525.

172. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А., Нистратова Е.Н. Программно-вычислительный комплекс оценки качества производственных процессов // Свидетельство о государственной регистрации программы для ЭВМ № 2010614145.

173. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А., Нистратова Е.Н. Комплекс для оценки качества информационных и административно-управленческих процессов при функционировании электронного правительства (КОК-ЭП)». // Свидетельство о государственной регистрации программы для ЭВМ № 2010617017

174. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А. Удаленная аналитическая поддержка информирования о вероятностно-временных показателях функционирования системы и ее элементов при реализации риск-ориентированного подхода. // Свидетельство о государственной регистрации программы для ЭВМ №2018617949

175. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А. Удаленное обоснование требований к средствам и условиям обеспечения качества функционирования «умных» систем. // Свидетельство о государственной регистрации программы для ЭВМ №2018618572

176. Костогрызов А.И., **Нистратов А.А.,** Нистратов Г.А. Удаленное вероятностное прогнозирование качества функционирования информатизированных систем. // Свидетельство о государственной регистрации программы для ЭВМ №2018618686

177. **Нистратов А.А**. Модуль определения частоты возникновения угроз, времен развития угроз и восстановления в универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349-2021 (заявка на регистрацию программы для ЭВМ: 6390301103, 2025)

178. **Нистратов А.А**. Модуль формирования отчетности по результатам вероятностного прогнозирования рисков для сложной системы с последовательным соединением элементов (заявка на регистрацию программы для ЭВМ: 6388313200, 2025)

179. **Нистратов А.А**. Модуль проверки достаточности данных для прогнозирования рисков по статистике (заявка на регистрацию программы для ЭВМ: 6389115593, 2025)

180. **Нистратов А.А**. Модель технологической поддержки риск-ориентированной системной инженерии (заявка на регистрацию программы для ЭВМ: 6390605370, 2025)

181. Безкоровайный М.М., Костогрызов А.И., Львов В.М. [и др.] Комплекс для Оценки Качества функционирования информационных систем (КОК) - "ноу-хау". Свидетельство о государственной регистрации программы для ЭВМ №2000610272

182. Безкоровайный, М.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК. / М.М. Безкоровайный, А.И. Костогрызов, В.М. Львов - М.: Изд. «Вооружение. Политика. Конверсия», 2002.- 304 с. - Текст: непосредственный

183. Климов, Г.П. Теория вероятностей и математическая статистика. / Г.П. Климов - М.: МГУ, 1983. 328 с. - Текст: непосредственный

184. Костогрызов, А.И. Универсальный инструментально- моделирующий комплекс (КОК) –

эффективное средство заказчика, разработчика и пользователя для обеспечения и повышения качества функционирования информационных систем / А.И. Костогрызов, Н.А. Баранов, И.З. Бондарюк [и др.] - Текст: непосредственный // «Связьинформ» №1, 2001г., с.164-170.

185. Костогрызов, А.И. Математические модели инструментария КОК – основа для обоснования требований, оценки и оптимизации качества функционирования информационных систем / Безкоровайный М.М., Костогрызов А.И., Львов В.М. [и др.] - Текст: непосредственный // «Связьинформ» №3, 2001г., с.69-105

186. **Нистратов А.А.** Методика прогнозирования техногенных рисков и ее реализация с использованием Интернет-технологии : диссертация на соискание ученой степени доктора технических наук по специальности 05.13.17 «Теоретические основы информатики» / **Нистратов Андрей Андреевич** – Москва, Институт проблем информатики Российской академии наук, 2013г. – 150с. - Текст: непосредственный.

187. Вентцель, Е.С. Исследование операций: задачи, принципы, методология. / Е.С. Вентцель - Дрофа 2004.-206с. - Текст: непосредственный

188. Мачихина, Л.И. Научные основы продовольственной безопасности зерна (хранение и переработка). / Л.И. Мачихина, Л.В. Алексеева, Л.С. Львова – М.:ДеЛи принт, 2007. – 382с. - Текст: непосредственный

189. Эртель, В. Введение в искусственный интеллект. / Эртель В. -М. «Эксмо», 2019. – 448с. - Текст: непосредственный

190. Лекун, Ян Как учится машина (революция в области нейронных сетей и глубокого обучения). / Ян Лекун – М. Альпина PRO, 2021. – 335с. - Текст: непосредственный

191. Арлазаров В.В. Мобильное распознавание и его применение к системе ввода идентификационных документов : диссертация на соискание ученой степени доктора технических наук по специальности 2.3.1 / Арлазаров Владимир Викторович – Москва, ФИЦ «Информатика и управление» Российской академии наук, 2023. – 358с. - Текст: непосредственный

192. Chakraborty A., Alam M., Dey V., Chattopadhayay A.U., Yay D.M. Adversarial attacks and defences: A survey //arXiv preprint arXiv:1810.00069. – 2018

Приложение А. Доказательства Теорем 1 – 4

А.1. Доказательство Теоремы 1

(о существовании и сходимости прогнозных значений рисков, учитывающих различия во временах диагностики и восстановления целостности системы)

Рассчитываемая функция риска нарушения целостности системы по формулам (2.1) – (2.5) базовой модели 2.2.2.2 является монотонной и ограниченной на сегменте $[\min(T_{диагн.}, T_{восст}), \max(T_{диагн.}, T_{восст})]$ при действительном $N=T_{зад.}/(T_{меж.}+T_{диаг.})$. Так, при пробегании значений $T_{зад.}$ в диапазоне от 0 до ∞ расчетное значение траектории риска описывает функцию распределения времени наработки на нарушение целостности. По свойствам ФР эта траектория является монотонно неубывающей с изменением от 0 до 1, т.е. она ограниченная. Поскольку на 1-й итерации длительность контроля $T_{диагн.}^{(1)}$ не учитывает времени восстановления, то риск $R_{.}^{(1)}$, рассчитываемый с использованием модели 1, ожидается оптимистичным (т.е., если время восстановления нарушенной целостности больше времени просто диагностики, то риск нарушения целостности с нулевым временем восстановления меньше реального). В расчетных формулах значение $T_{диагн.}$ наряду с $T_{меж}$ находится на месте $T_{зад.}$ и расчет определяется лишь выражениями (2.1) при $T_{зад.} \le T_{меж.}+T_{диаг.}$ или при $T_{зад.} > T_{меж.}+T_{диаг.}$. Оба расчетных выражения носят смысл функции распределения, т.е. тоже будут монотонно неубывающими и ограниченными, изменяясь в диапазоне от 0 до 1 по параметру $T_{диагн.}$ при неизменном $T_{меж.}$.

По теореме Веерштрасса всякая монотонная и ограниченная последовательность имеет предел. Таким образом, с увеличением n указанная последовательность $T_{диагн.}^{(n)}$ будет сходящейся или из нее можно выделить сходящуюся. Соответственно, последовательность значений функции $R_{.}^{(n)}(T_{диагн.}^{(n)})$ также будет сходящейся или из нее можно выделить сходящуюся, поскольку она монотонная и ограниченная. Т.е. для окончательного расчета риска по модели 1 исходным выступает усредненная длительность контроля по n-й итерации $T_{диагн.}^{(n)}$ такая, что выполняется условие: $|R_{.}^{(n)} - R_{.}^{(n-1)}| \le \varepsilon$. Это итерационное значение длительности контроля $T_{диагн.}^{(n)}$ учитывает как длительность просто диагностики $T_{диаг.}$, так и длительность восстановления нарушенной целостности $T_{восст.}$ с учетом реального риска с заданной точностью $\varepsilon>0$ (близкой к 0).

Окончательный расчет риска осуществляется для целого значения N (т.е. $N = [T_{зад}/(T_{меж}+ T_{диаг})]$ - целая часть), что дает возможность прогноза риска с учетом реальных (а не сглаженных функционально) влияний мер периодического контроля и восстановления целостности и служит аналитической основой для извлечения закономерностей.

Применительно к ВС и КС для достижения практически приемлемой адекватности минимальное значение ε установлено в численном выражении не более, чем 0.001 от задаваемого значения допустимого риска нарушения целостности системы. Это значение обосновано эмпирическим путем при решении многих десятков практических задач, выполняемое при этом количество итераций исчисляется сотнями – тысячами (в зависимости от специфики моделируемой системы могут быть исключения, основанные на более глубоких эмпирических сравнениях).

Доказательство теоремы завершено.

А.2. Доказательство Теоремы 2
(об условиях существования прогнозной нижней оценки среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта)

Для облегчения понимания доказательства имеет смысл предварительно привести следующие формальные пояснения.

В моделируемой системе, представляющей собой такую сущность, как критичный параметр мониторируемого объекта, при использовании УВМП и «Модели «черного ящика» при отсутствии какого-либо контроля» нарушение нормативного диапазона для значений критичного параметра мониторируемого объекта означает ничто иное, как нарушение целостности моделируемой системы (нарушение целостности на рис. А.1 отмечено «крестиком» X), где функция распределения (ФР) $\Omega_{возд.}(t)$ времени между возникновениями угрозы равна $\Omega_{возд.}(t) = 1-\exp(-\sigma t)$, σ – частота возникновения источников угроз в моделируемой системе, ФР $\Omega_{акт.}(t)$ времени развития (активизации) угрозы равна $\Omega_{акт.}(t) = 1-\exp(-t/\beta)$, β – среднее время развития угроз с момента возникновения источников угроз до нарушения установленных требований по обеспечению целостности моделируемой системы или до инцидента.

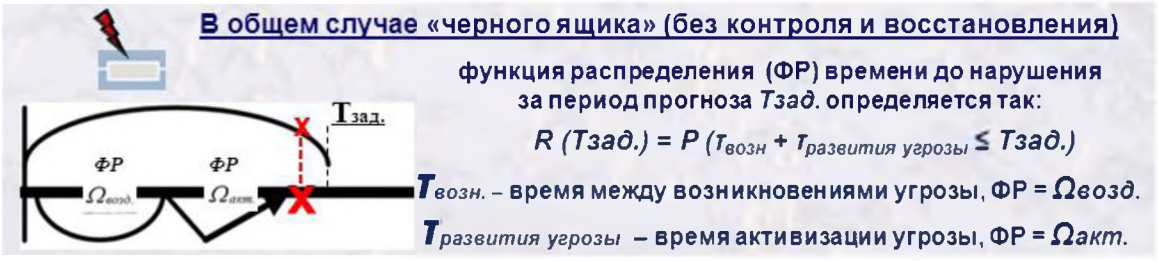


Рис. А.1 Формальный случай нарушения целостности системы за период прогноза $T_{зад}$

Такие параметры модели, как $T_{меж}$ (время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы) и $T_{диаг}$ (среднее время

системной диагностики целостности моделируемой системы) никакой роли не играют, т.к. искомая оценка для остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона достигается до наступления какой-либо очередной диагностики, т.е. ФР времени до нарушения целостности моделируемой системы $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}}) = R_{\text{наруш}}(\sigma, \beta, T_{\text{зад}})$. Именно из-за этого расчетная оценка рассматривается как оценка снизу (нижняя оценка), если учитывать дополнительные параметры и более адекватные модели (см. Теоремы 3 и 4), будут получаться более точные оценки. Далее, распределение времени до нарушения целостности моделируемой системы (т.е. до «крестика») по существу представляет собой свертку двух функций распределения $\Omega_{\text{возд.}}(t) = 1-\exp(-\sigma t)$ и $\Omega_{\text{акт.}}(t) = 1-\exp(-t/\beta)$. При возрастании t от 0 до ∞ эта свертка представляет собой монотонно возрастающую от 0 до 1 функцию (эта свертка также является функцией распределения, обладающей по определению свойствами непрерывности и монотонного возрастания по t от 0 до 1).

При использовании УВМП (см. рис. 2.12) для характеристики элементарных состояний отслеживаемого критичного параметра зона «Приемлемое» полностью идентична состоянию «В пределах рабочего диапазона» на рис. 2.16, зона «Приемлемое с отклонением» идентична состоянию «За пределами рабочего диапазона, но в пределах нормативного диапазона» на рис. 2.16, зона «Неприемлемое» идентична состоянию «За пределами нормативного диапазона» на рис. 2.16.

В приведенных формальных описаниях для прогнозной оценки среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона требуется вычисление математического ожидания ФР времени до нарушения целостности моделируемой системы $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}}) = R_{\text{наруш}}(\sigma, \beta, T_{\text{зад}})$ с вычислительной точностью ε. В свою очередь эта ФР $R_{\text{наруш}}(\sigma, \beta, T_{\text{зад}})$ строится с помощью «Модели «черного ящика» при отсутствии какого-либо контроля» по точкам расчета по формулам (1), (2) при $T_{\text{зад}}$, пробегающем все значения от 0 до ∞. По условиям теоремы неизвестным является не просто значение β, а такое β, которое практически совпадает с периодом прогноза $T_{\text{зад}}$. В итоге ищется значение минимального ненулевого времени развития угроз x (т.е. неизвестное $x=\beta$), когда за прогнозный период $T_{\text{зад}}$ (тоже равный неизвестному x) риск нарушения целостности моделируемой системы впервые достигнет установленного допустимого уровня риска $R_{\text{доп}}(x)$ с задаваемой расчетной точностью ε.

Таким образом, искомая в теореме 2 прогнозная нижняя оценка среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного

диапазона для значений критичного параметра мониторируемого объекта представляет собой решение уравнения

$$R_{\text{наруш}}(\sigma, x, x) = R_{\text{доп}}(x) \qquad \text{(A.1)}$$

относительно x с задаваемой расчетной точностью ε. Искомое неизвестное x занимает в формульном выражении $R_{\text{наруш}}(\sigma, \beta, T_{\text{зад}})$ место параметров β и $T_{\text{зад}}$.

Здесь $R_{\text{наруш}}(\sigma, x, x) = 1 - P_{\text{возд}(1)}$. Расчет идет по формулам (2.1), (2.2), где ФР времени отсутствия нарушения целостности моделируемой системы $P_{\text{возд}(1)} = P_{\text{возд}(1)}(\sigma, x, T_{\text{меж}}, T_{\text{диаг}}, x)$ выражается в виде:

$$P_{возд(1)} = \begin{cases} \left(\sigma - x^{-1}\right)^{-1}\left\{\sigma e^{-1} - x^{-1}e^{-\sigma x}\right\}, если\ \ \sigma \neq x^{-1}, \\ e^{-\sigma x}\left[1+\sigma x\right] если\ \ \sigma = x^{-1}. \end{cases} \qquad \text{(A.2)}$$

Решение нелинейного уравнения (A.1) существует, поскольку слева функция $R_{\text{наруш}}(\sigma, \beta, T_{\text{зад}})$ непрерывна по всем параметрам и при возрастании β (т.е. x) от 0 до ∞ и остальных фиксированных параметрах значение риска нарушения целостности моделируемой системы монотонно убывает от положительного фиксированного значения (зависящего от σ) из интервала (0,1) до 0, а при возрастании периода прогноза $T_{\text{зад}}$ от нуля до бесконечности значение риска монотонно возрастает от 0 до 1 (как ФР по $t=T_{\text{зад}}$). Интерпретация такая: если среднее время развития угроз растет, то моменты времени до нарушения целостности моделируемой системы отодвигаются во времени вправо при любой частоте возникновения источников угроз σ, т.е. нарушения становятся реже, а при $T_{\text{зад}}$, стремящемся к ∞, нарушения за этот период прогноза неизбежны. В терминах элементарных событий по УВМП это означает, что переходы из элементарного состояния «Приемлемое» («В пределах рабочего диапазона» на рис. 2.7) в состояние «Приемлемое с отклонением» («За пределами рабочего диапазона, но в пределах нормативного диапазона» на рис. 2.7) могут случаться сколь угодно часто (это характеризуется параметром σ), но при росте среднего времени развития угроз β переходы из состояния «Приемлемое с отклонением» в состояние «Неприемлемое» («За пределами нормативного диапазона» на рис. 2.7) становятся реже, т.е. значения критичного параметра в основном колеблются в «зеленой» или «желтой» зонах, не выходя в «красную» зону – см. рис. 2.3.

Поскольку справа в уравнении (A.1) $R_{\text{доп}}$ – это константа по оси «у» в интервале (0,1), то, при вычислениях, увеличивая от нуля $R_{\text{доп}}$ с некоторым шагом (например, с шагом $0.01R_{\text{доп}}$), определяются ближайшие точки пересечения этой горизонтальной линии (параллельной оси «х») с траекторией функции $R_{\text{наруш}}(\sigma, x, x)$, зависящей от x, а также от σ. В итоге каждому значению $R_{\text{доп}}$ из сетки на оси «у» (с шагом $0.01R_{\text{доп}}$) будет соответствовать на оси «х» одна или ряд точек x_0 пересечения $R_{\text{доп}}$ с функцией $R_{\text{наруш}}(\sigma, x, x)$ - несколько точек

может совпасть с задаваемой точностью расчетов ε. Минимальное x_{0min} из этих значений $\{x_0\}$ как раз и будет определять нижнюю оценку среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта. Для некоторых значений $R_{доп}$ такой положительной точки x_{0min} может не существовать из-за того, что искомое остаточное время может оказаться практически равным 0 в условиях заданной расчетной точности ε или оказаться неизмеримо большим (именно для понимания этого в (8) справа проставлена $R_{доп}(x)$ как зависящая от x). А дополнение до 1 соответствующего точке x_{0min} значение $R_{доп.0min}$ из $\{R_{доп.0}\}$ есть ничто иное, как доверительная вероятность этой вычисленной прогнозной нижней оценки среднего остаточного времени. Множество $\{R_{доп.0}\}$ определяет по сути рассчитанную область доверительной вероятности, а $R_{доп.0min}$ – достижимую доверительную вероятность вычисления искомой точки x_{0min}. Тем самым доказана первая часть Теоремы 2, а именно: «…прогнозная оценка среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта существует в определенной рассчитываемой области доверительной вероятности».

При этом дополнение до 1 установленного допустимого уровня риска нарушения целостности моделируемой системы $R_{доп}$ может не войти в множество $\{R_{доп.0}\}$. Это будет говорить о том, что на вычислительной сетке ВС и КС в заданных жестких условиях прогноза остаточное время на принятие упреждающих мер в недопущение нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта близко к нулю или устремлено в бесконечность, т.е. необходимо смягчать условия прогноза (по значениям $R_{доп}$ и/или ε). Если же дополнение до 1 входит в рассчитанную область доверительной вероятности $\{R_{доп.0}\}$, то ему будет соответствовать единственное минимальное значение x_{0min} из-за непрерывности функции $P_{возд(1)}(\sigma, x, T_{меж}, T_{диаг}, x)$, рассчитываемой по формуле (А.2), и отсутствия константных фрагментов по x. Именно это x_{0min} будет представлять собой прогнозную нижнюю оценку среднего остаточного времени на принятие упреждающих мер в недопущение нарушения нормативного диапазона. Согласно изложенному выше алгоритму эта точка вычислена как результат решения задачи определения такого минимального среднего времени развития угроз, при котором риск нарушения целостности моделируемой системы достигает с заданной точностью ε значения установленного допустимого уровня риска $R_{доп}$. Тем самым доказано последнее утверждение Теоремы 2.

Доказательство в целом Теоремы 2 завершено.

А.3 Доказательство Следствия из Теоремы 2 (об ограничениях при выборе периода между диагностиками целостности системы, ориентированного на непревышение допустимого риска нарушения целостности системы)

Для доказательства Следствия из Теоремы 2 достаточно выявить некоторые закономерности в соотношениях исходных данных, следование которым обеспечит непревышение задаваемого допустимого уровня риска и сохранение целостности моделируемой системы ($R_{доп}$ =0.1). Для этого опять обратимся к формулам (2.1) и (2.2), использованным в Теореме 2.

Рассмотрим выборочные зависимости исходных данных σ и $T_{зад}$ от β, а именно: $\sigma=10\beta^{-1}$, $\sigma=2\beta^{-1}$, $\sigma=\beta^{-1}$, $\sigma=0.2\beta^{-1}$, $\sigma=0.1\beta^{-1}$, а также $T_{зад}$ /β. Это позволит существенно упростить выражения в (2.1) и (2.2). Например, при $\sigma=\beta^{-1}$ выражение (2.1) будет выглядеть так:

$$R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}) = R = 1 - \exp(-z)[1+z] = 1 - \exp(-T_{зад}/\beta)[1+T_{зад}/\beta] \ ,$$

где $z = \sigma T_{зад} = T_{зад}/\beta$.

С учетом этого по формулам (2.1), (2.2) построены зависимости риска нарушения целостности моделируемой системы R от z, точнее от отношения $T_{зад}/\beta$, см. рис. А.2 – А.7.

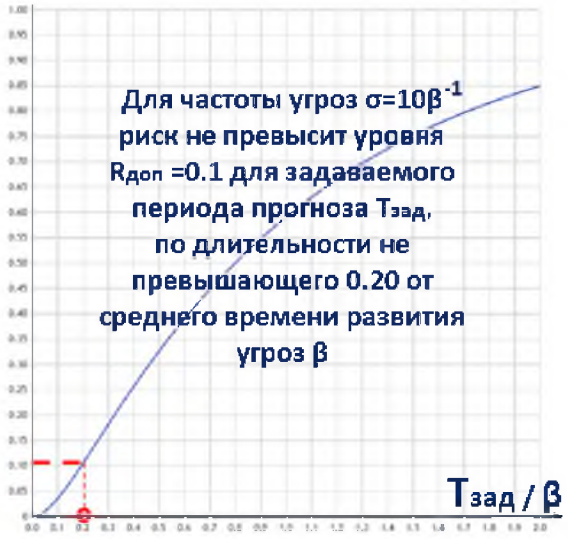


Рис. А.2 Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=10\beta^{-1}$

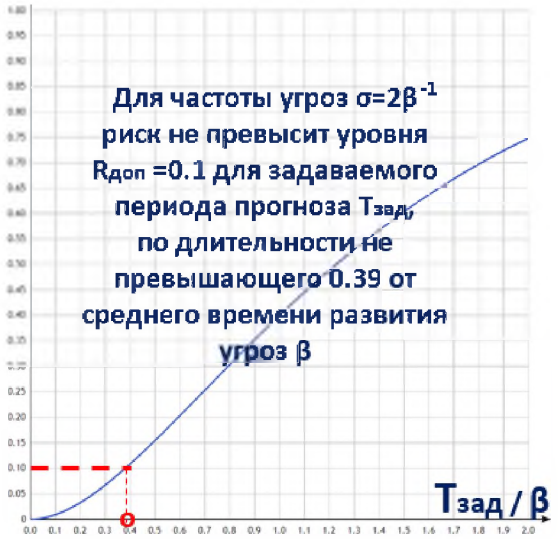


Рис. А.3 Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=2\beta^{-1}$

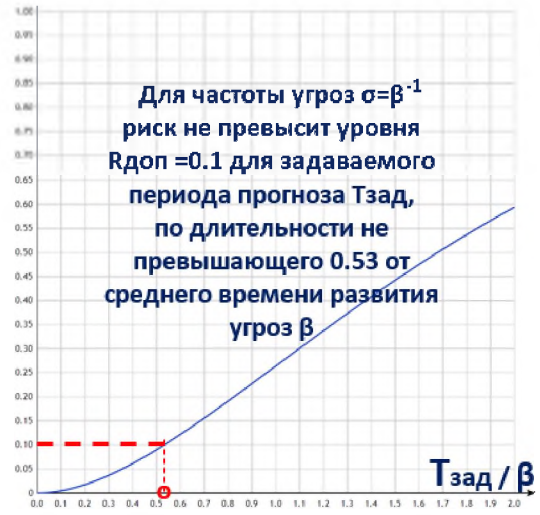


Рис. А.4 Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=\beta^{-1}$

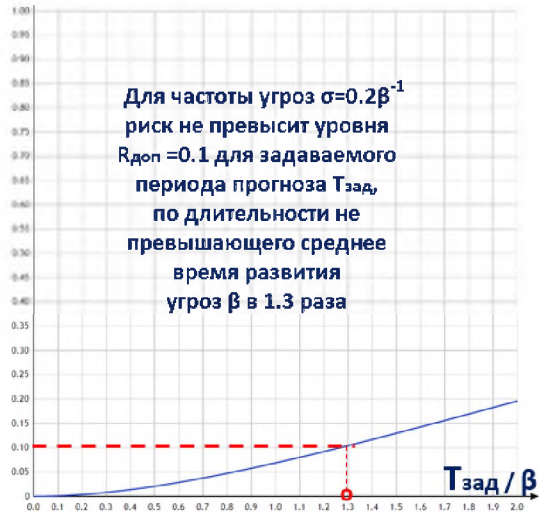


Рис. А.5 Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=0.2\beta^{-1}$

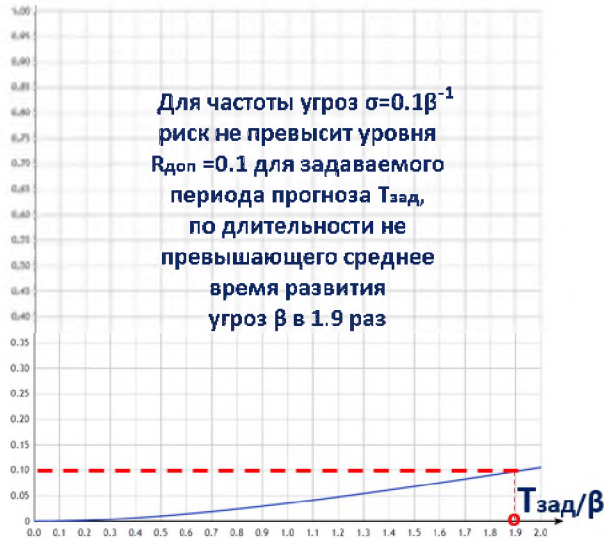


Рис. А.6 Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=0.1\beta^{-1}$

Обобщенные условия для $R_{доп}=0.1$

Условие по соотношению частоты возникновения угроз σ со средним временем развития угроз β	Условие по соотношению длительности периода прогноза $T_{зад}$ со средним временем развития угроз β
$\sigma=10\ \beta^{-1}$	$T_{зад} \leq 0.20\ \beta$
$\sigma=2\ \beta^{-1}$	$T_{зад} \leq 0.39\ \beta$
$\sigma=\beta^{-1}$	$T_{зад} \leq 0.53\ \beta$
$\sigma=0.2\ \beta^{-1}$	$T_{зад} \leq 1.3\ \beta$
$\sigma=0.1\ \beta^{-1}$	$T_{зад} \leq 1.9\ \beta$

Рис. А.7 Обобщение выявленных закономерностей

Выявленные закономерности заключаются в следующих выборочных условиях в соотношениях исходных данных для непревышения задаваемого допустимого уровня риска и сохранения целостности моделируемой системы:

- при условии, когда средний период между моментами возникновения угроз σ^{-1} на порядок меньше среднего времени развития угроз β (т.е. для частоты возникновения угроз $\sigma=10\beta^{-1}$) риск нарушения целостности моделируемой системы не превысит уровня $R_{доп}=0.1$, только если задаваемый период прогноза $T_{зад}$ не превысит 0.2 от среднего времени развития угроз β;

- при условии, когда средний период между моментами возникновения угроз σ^{-1} вдвое меньше среднего времени развития угроз β (т.е. для частоты возникновения угроз $\sigma=2\beta^{-1}$) риск нарушения целостности моделируемой системы не превысит уровня $R_{доп}=0.1$, только

если задаваемый период прогноза $T_{зад}$ не превысит 0.39 от значения среднего времени развития угроз β;

- при условии, когда средний период между моментами возникновения угроз σ^{-1} равен среднему времени развития угроз β (т.е. для частоты возникновения угроз $\sigma=\beta^{-1}$) риск нарушения целостности моделируемой системы не превысит уровня $R_{доп}=0.1$, только если задаваемый период прогноза $T_{зад}$ не превысит 0.53 от среднего времени развития угроз β;

- при условии, когда средний период между моментами возникновения угроз σ^{-1} в 5 раз больше среднего времени развития угроз β (т.е. для частоты возникновения угроз $\sigma=0.2\beta^{-1}$) риск нарушения целостности моделируемой системы не превысит уровня $R_{доп}=0.1$, только если задаваемый период прогноза $T_{зад}$ по длительности не превысит среднего времени развития угроз β в 1.3 раза;

- при условии, когда средний период между моментами возникновения угроз σ^{-1} на порядок больше среднего времени развития угроз β (т.е. для частоты возникновения угроз $\sigma=0.1\beta^{-1}$) риск нарушения целостности моделируемой системы не превысит уровня $R_{доп}=0.1$, только если задаваемый период прогноза $T_{зад}$ по длительности не превысит среднего времени развития угроз β в 1.9 раза.

На рис. 2.14 представлено обобщение выявленных закономерностей.

Примечание. Значение допустимого уровня $R_{доп}=0.1$ непринципиально, оно выбрано лишь для иллюстрации предлагаемого подхода к выявлению закономерностей (кроме того, такой уровень рекомендуется ГОСТ Р 59991-2022). Результаты расчетов на рис. А.2 – А.7 позволяют установить аналогичные закономерности для любого задаваемого значения $R_{доп}$.

Условия Следствия из Теоремы 2 представляют собой условия, сформулированные на рис. 2.9 – 2.14 с заменой задаваемого периода прогноза $T_{зад}$ на нижние оценки среднего остаточного времени на принятие упреждающих мер x_{0min}, вычисляемые в результате применения Теоремы 2. Поскольку результатом применения Теоремы 2 являются нижние оценки, то ориентация на эти значения как на верхние с точки зрения длительности выбираемого периода между диагностиками целостности моделируемой системы $T_{между}$ гарантирует, что ожидаемый расчетный риск нарушения целостности системы не превысит заданного допустимого уровня с учетом того, что в результате диагностики целостность системы полагается сохраненной (если не было нарушений) или восстановленной (если нарушения имели место быть).

Доказательство Следствия из Теоремы 2 завершено.

А.4. Доказательство Теоремы 3

(о среднем остаточном времени до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам)

Применение «Модели «черного ящика» при реализации технологии периодического системного контроля» (из 2.2.2.2) позволяет вычислить значения $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}})$ в последовательных K точках $T_{\text{зад}} = t_1 \geq 0, t_2, t_3, \ldots, t_{K-1}, t_K$, принимающих значения от 0 до условной вычислительной бесконечности, точнее, до такого значения t_K, при котором с задаваемой расчетной точностью ε, соизмеримой со значением ε из Теоремы 2, расчетное значение $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, t_K)$ достигает 1, т.е. $1 - \varepsilon \leq R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, t_K) \leq 1$. Это достижимо при использовании вероятностной меры, когда N – действительное число, учитывающее не только целую, но и дробную части при расчетах по формулам (2.3) – (2.5) – см. соответствующее примечание в 2.2.2.2: «… в этом случае пилообразность исчезнет, получится классическая функция распределения».

Таким образом, при пробегании значений $T_{\text{зад.}}$ по точкам $\{t_1, t_2, t_3, \ldots, t_{K-1}, t_K\}$ расчетное значение траектории функции $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, t)$ поточечно описывает функцию распределения времени наработки на нарушение целостности, монотонно возрастающую от 0 до 1.

Для этой построенной ФР среднее значение времени наработки на нарушение целостности определяется по классической формуле для математического ожидания (МОЖ) как сумма произведений всех значений случайной величины $\{t_1, t_2, t_3, \ldots, t_{K-1}, t_K\}$ на соответствующие им вероятности:

$$\text{Среднее (для отдельного элемента)} = \text{МОЖ} = \sum_{k=1}^{K} t_k R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, t_k). \quad \text{(А.3)}$$

Тем самым среднее остаточное время до нарушения нормативного диапазона для значений критичного параметра мониторируемого объекта при своевременном принятии упреждающих мер противодействия угрозам может быть вычислено в явном виде по формуле (А.3) с использованием «Модели «черного ящика» при реализации технологии периодического системного контроля» (из 2.2.2).

Доказательство Теоремы 3 завершено.

А.5. Доказательство Теоремы 4

(о среднем остаточном времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам)

Применение Теоремы 3 позволяет поточечно построить по значениям в последовательных K точках $T_{зад} = t_1 \geq 0, t_2, t_3, \ldots, t_{K-1}, t_K$ траектории ФР времени до нарушения целостности $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ для каждого из элементов декомпозированной системы (со своими исходными данными $\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}$ при одних и тех же значениях $t_1, t_2, t_3, \ldots, t_{K-1}, t_K$). Использование одних и тех же значений $t_1, t_2, t_3, \ldots, t_{K-1}, t_K$ позволяет в полной мере использовать алгоритмические выражения (2.7) – (2.8) для построения ФР для интегрированной моделируемой системы, вычисляемой с использованием «Модели «черного ящика» при реализации технологии периодического системного контроля» (из 2.2.2.2 с учетом 2.2.3, 2.2.4). В итоге для интегрированной моделируемой сложной системы получается поточечно построенная ФР времени до нарушения целостности системы в целом: $R_{наруш}(T_{зад})$, зависящая также от параметров σ, β, $T_{меж}$, $T_{диаг}$, $T_{восст}$ со своими значениями для каждого из элементов интегрируемой структуры при одних и тех же значениях $T_{зад} = t_1, t_2, t_3, \ldots, t_{K-1}, t_K$.

Таким образом, при пробегании значений $T_{зад.}$ по точкам $\{t_1, t_2, t_3, \ldots, t_{K-1}, t_K\}$ расчетное значение траектории функции $R_{наруш}(T_{зад})$ поточечно описывает функцию распределения времени наработки на нарушение целостности всей интегрированной системы, монотонно возрастающую от 0 до 1.

Для этой построенной ФР $R_{наруш}(t_k)$ среднее значение остаточного времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам так же, как в Теореме 3, определяется по классической формуле для математического ожидания как сумма произведений всех значений случайной величины $\{t_1, t_2, t_3, \ldots, t_{K-1}, t_K\}$ на соответствующие им вероятности - см. (А.3):

$$\text{Среднее (для интегрированной сложной системы)} = \text{МОЖ} = \sum_{k=1}^{K} t_k R_{наруш}(t_k),$$

где $R_{наруш}(t_k)$ относится уже к системе в целом.

Тем самым среднее остаточное время до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам может быть вычислено в явном виде по этой формуле с использованием «Модели «черного ящика» при реализации технологии периодического системного контроля» (из 2.2.2 с учетом 2.2.3, 2.2.4).

Доказательство Теоремы 4 завершено.

Приложение Б. Копии некоторых свидетельств Роспатента на разработанные программы для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

РОССИЙСКОЕ АГЕНТСТВО ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ (РОСПАТЕНТ)

СВИДЕТЕЛЬСТВО

Об официальной регистрации программы для ЭВМ

№ 2004610858

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

№ 2008612348

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

№ 2008614525

СВИДЕТЕЛЬСТВО

№ 2010614145

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2010617017

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018617949

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018618572

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018618686

Приложение В. Акты о реализации

РЕДАКЦИОННЫЙ СОВЕТ МНОГОТОМНОГО ИЗДАНИЯ

БЕЗОПАСНОСТЬ РОССИИ

Правовые, социально-экономические и научно-технические аспекты

119991 Москва, Ленинский просп., 32-а; Президиум РАН, к. 17-18. Тел.: (495) 930-80-78; e-mail: kel51@mail.ru

Акт

об использовании результатов диссертационной работы Нистратова Андрея Андреевича по теме «Вероятностные модели, программные, технологические и методические решения для рационального управления рисками в системной инженерии» на соискание ученой степени доктора технических наук по специальности 2.3.5 «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»

Настоящий акт свидетельствует о том, что теоретические и методические результаты диссертационных исследований, а также программные и технологические решения, созданные Нистратовым А.А., использованы в следующих разделах изданного тома «Безопасность России. Правовые, социально-экономические и научно-технологические аспекты. Тематический блок «Национальная безопасность». Системная инженерия в проблемах национальной безопасности»:

- в разделе III «Основные положения системной инженерии для решения проблем обеспечения национальной безопасности» (стр. 136 – 161 в части характеристики современной системной инженерии, примеров и описания складывающихся тенденций, стр. 190 – 238 в части обзора методов и моделей, типовых подходов, примеров и описания перспективной технологии решения задач системной инженерии);
- в разделе VIII «Приложения системной инженерии к национальному приоритету по обеспечению экономической безопасности» (стр. 561 – 574 в части расчетных примеров рациональных решений в нефтегазовой отрасли);
- в разделе IX «Приложения системной инженерии к национальному приоритету по обеспечению научно-технологического развития» (стр. 643 – 679 в части применения методов системной инженерии для анализа безопасности систем искусственного интеллекта).

Многотомное издание «Безопасность России. Правовые, социально-экономические и научно-технологические аспекты» выходит с 1998 года, издано 70 томов. Работа выполняется Российской Академией наук, МЧС РФ, издается Международным гуманитарным фондом «Знание» им. академика К.В. Фролова (МГОФ «Знание»). В рамках издания сконцентрированы актуальные достижения отечественной, а также зарубежной науки и практики, мировой опыт решения различных проблем безопасности. Серия «Безопасность России» приобрела межведомственный и межотраслевой характер, что соответствует уровню и задачам энциклопедического издания и фундаментального научного труда. В число руководителей, членов редакционного совета, разработчиков проблем и авторов вышедших блоков томов и отдельных томов входили руководители и члены Совета Безопасности и Российской академии наук, видные отечественные ученые.

Нистратов А.А. является одним из соавторов изданной монографии «Безопасность России. Правовые, социально-экономические и научно-технологические аспекты. Тематический блок «Национальная безопасность». Системная инженерия в проблемах национальной безопасности», изданного издательством МГОФ «Знание», 2025. – 904с.

Председатель Комиссии РАН по техногенной безопасности,
научный руководитель издания «Безопасность России»
член-корреспондент РАН Н.А. Махутов

«25» июня 2025г.

УТВЕРЖДАЮ

Директор

ФБУ «НТЦ Энергобезопасность»

Доктор экономических наук

_____ П.С. Каныгин

"04" 03 2021 г.

А К Т

о внедрении результатов диссертационной работы Нистратова Андрея Андреевича, посвященной разработке программно-технологических и методических решений по прогнозированию и рациональному упреждающему управлению рисками для приложений системной инженерии, на соискание ученой степени доктора технических наук по специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Настоящий акт свидетельствует о том, что программно-технологические и методические решения, разработанные Нистратовым А.А. в рамках диссертационных исследований, были реализованы в следующих стандартах системной инженерии, в которых ФБУ «НТЦ Энергобезопасность» выступало в качестве соразработчика:

ГОСТ Р 59329-2021 «Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы»;

ГОСТ Р 59331-2021 «Системная инженерия. Защита информации в процессе управления инфраструктурой системы»;

ГОСТ Р 59333-2021 «Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы»;

ГОСТ Р 59334-2021 «Системная инженерия. Защита информации в процессе управления качеством системы»;

ГОСТ Р 59335-2021 «Системная инженерия. Защита информации в процессе управления знаниями о системе»;

ГОСТ Р 59336-2021 «Системная инженерия. Защита информации в процессе планирования проекта»;

ГОСТ Р 59337-2021 «Системная инженерия. Защита информации в процессе оценки и контроля проекта»;

ГОСТ Р 59338-2021 «Системная инженерия. Защита информации в процессе управления решениями»;

ГОСТ Р 59339-2021 «Системная инженерия. Защита информации в процессе управления рисками для системы»;

ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы»;

ГОСТ Р 59342-2021 «Системная инженерия. Защита информации в процессе измерений системы»;

ГОСТ Р 59347-2021 «Системная инженерия. Защита информации в процессе определения архитектуры системы»;

ГОСТ Р 59356-2021 «Системная и программная инженерия. Защита информации в процессе сопровождения системы»;

ГОСТ Р 59349-2021 «Системная инженерия. Защита информации в процессе системного анализа»;

ГОСТ Р 59355-2021 «Системная и программная инженерия. Защита информации в процессе функционирования системы»;

ГОСТ Р 59353-2021 «Системная инженерия. Защита информации в процессе передачи системы»;

ГОСТ Р 59354-2021 «Системная инженерия. Защита информации в процессе аттестации системы»;

ГОСТ Р 59357-2021 «Системная инженерия. Защита информации в процессе изъятия и списания системы».

Вышеперечисленные стандарты внедрены в состав нормативно-методической базы, используемой в практике ФБУ «НТЦ Энергобезопасность».

Заместитель директора
кандидат технических наук — Ф.В. Матвеенков

2

Федеральное агентство по техническому регулированию и метрологии

Национальный и межгосударственный технический комитет по стандартизации
Информационные Технологии
(ТК-МТК-022)

109544, г. Москва, ул. Краснобогатырская, д.6.
E-mail: tk22@itstandard.ru
www.cksit-rspp.ru
тел: 8(495) 165-55-41

исх. № 025/06 от 24 июня 2025 г.

АКТ

внедрения результатов диссертационной работы Нистратова Андрея Андреевича по теме «Программные, технологические и методические решения для упреждающего управления рисками в приложениях системной инженерии» на соискание ученой степени доктора технических наук по специальности 2.3.5 «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»

Настоящий акт свидетельствует о том, что стандартизованные вероятностные модели и методические решения по прогнозированию рисков, реализованные в национальных стандартах системной инженерии ГОСТ Р 59329-2021 – ГОСТ Р 59357-2021, в разработке которых от ФБУ НТЦ «Энергобезопасность» принимал участие Нистратов Андрей Андреевич, внедрены в практику работы национального технического комитета ТК22 «Информационные технологии» в части ссылок на них и рекомендаций по использованию созданных методов, моделей и прикладных примеров системной инженерии в новых национальных стандартах 2024-2025 года:

ГОСТ Р 56920-2024 «Системная и программная инженерия. Тестирование программного обеспечения. Общие положения (ISO/IEC/IEEE 29119-1:2022, NEQ)»;

ГОСТ Р 71303-2024 «Системная и программная инженерия. Возможности программных инструментариев для организационного управления инцидентами. Общие положения (ISO/IEC 23531:2020, NEQ)»;

ГОСТ Р 71304-2024 «Системная и программная инженерия. Гарантии обеспечения качества систем и программных средств. Основные понятия и термины (ISO/IEC/IEEE 15026-1:2019, NEQ)»;

ГОСТ Р 71438-2024 «Информационные технологии. Оценка процессов. Система измерения процессов для оценки их возможностей (ISO/IEC 33020:2019, NEQ)»;

ГОСТ Р 71439-2024 «Системная и программная инженерия. Методы и инструментарии продуктовой линейки программных средств и систем. Общие положения (ISO/IEC 26580:2021, NEQ)»;

ГОСТ Р 71440-2024 «Информационные технологии. Оценка процессов. Руководство по определению рисков в процессах (ISO/IEC TR 33015:2019, NEQ)»;

ГОСТ Р 57193-2025 «Системная и программная инженерия. Процессы жизненного цикла систем (ISO/IEC/IEEE 15288:2021, NEQ)»

ГОСТ Р 71998-2025 «Информационные технологии. Требования и оценка качества систем и программного обеспечения. Определение качества ИТ-услуг (ISO/IEC TS 25025:2021, NEQ)».

Все вышеперечисленные стандарты – действующие.

Председатель ТК 22 «Информационные технологии»,
доктор технических наук, профессор

С.А. Головин

Ответственный секретарь ТК 22 «Информационные технологии»

О.К. Гудкова

М.п.

Научно-исследовательский институт
прикладной математики и сертификации
107564, г. Москва, ул. Краснобогатырская 2, стр. 2
телефон (495)795-85-24, телефакс (495)931-54-17
e-mail: RIAMC@matmodels.net

« » 20 г.
№
На № от

от 14.06.2021г. №1-06

АКТ РЕАЛИЗАЦИИ РЕЗУЛЬТАТОВ ДИССЕРТАЦИОННЫХ ИССЛЕДОВАНИЙ

Нистратова Андрея Андреевича на соискание ученой степени доктора технических наук, посвященных разработке и применению математических, программных, технологических и методических решений для управления рисками

Настоящий акт свидетельствует о том, что математические, программные, технологические и методические решения, разработанные в диссертационных исследованиях Нистратова Андрея Андреевича, реализованы при выполнении практических работ в интересах генерального заказчика АО «СУЭК-Кузбасс» по созданию и эксплуатации программного прототипа подсистемы поддержки принятия решений по управлению рисками в рамках системы дистанционного контроля промышленной безопасности (СДК ПБ) на угольных шахтах: в 2016г. на тему «Прогнозирование рисков нарушения промышленной безопасности функционирования опасного производственного объекта и оценки качества функционирования СДК ПБ», в 2017г. – «Создание прототипа подсистемы поддержки принятия решений по управлению рисками при развитии прототипа СДК ПБ», в 2018г. – «Развитие прототипа подсистемы поддержки принятия решений по управлению рисками при развитии прототипа СДК ПБ», в 2019г. – «Тиражирование прототипа подсистемы поддержки принятия решений по управлению рисками при тиражировании прототипа СДК ПБ», а также в ГОСТ Р 58494-2019 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов». При разработке ГОСТ Р 58494-2019 ООО Научно-исследовательский институт прикладной математики и сертификации выступал головным исполнителем, стандарт внесен техническим комитетом по стандартизации ТК 269 «Горное дело», утвержден приказом Федерального агентства по техническому регулированию и метрологии 22.08.2019 №522-ст, введен впервые в действие с 01.01.2020г. и находится в открытом доступе.

Генеральный директор Э.В. Григорьев

Директор-научный руководитель,
доктор технических наук, профессор А.И. Костогрызов

ПРАНАФАРМ
фармацевтическое производство

ООО «ПРАНАФАРМ»
ул. Ново-Садовая, дом 106, корпус 81, г. Самара, 443068, Россия
Тел. (846) 334-52-32, 207-12-61, (846) 335-15-61, 207-41-62
http://www.pranapharm.ru/
E-mail: info@pranapharm.ru

АКТ

реализации результатов диссертационной работы Нистратова Андрея Андреевича на соискание ученой степени доктора технических наук (по специальности 2.3.5), посвященной разработке и применению программных, технологических и методических решений для упреждающего управления рисками в системной инженерии

№ 387/2025 «25» июня 2025 г.

Настоящий акт свидетельствует о том, что в проектных оценках рисков для производственного фармацевтического предприятия ООО «Пранафарм», были реализованы научно обоснованные рекомендации, полученные в период 2022 – 2025 гг. на основе применения разработанной в диссертации Нистратова Андрея Андреевича инфраструктуры и технологии поддержки риск-ориентированной системной инженерии. Рекомендации, полученные в удаленном режиме, использованы при решении следующих практических задач:

1) анализа и организации на предприятии системных процессов:

- процесса системного анализа - для удовлетворения аналитических потребностей заинтересованных сторон в поддержке принятия актуальных решений;

- процесса управления человеческими ресурсами - для выявления приемлемых условий организационного резервирования, учитывающего область ответственности и квалификацию должностных лиц предприятия;

- процесса управления качеством - для обоснования необходимой и достаточной степени организационного резервирования действий должностных лиц предприятия;

- процесса управления рисками - для своевременной идентификации рисков, обоснования и реализации эффективных упреждающих мер по снижению рисков или их удержанию в допустимых пределах;

2) прогнозирования на срок до 2037 года и удержания в допустимых пределах различных рисков разрушения бизнеса (потери инвестиций) применительно к фармацевтическому предприятию.

Реализация полученных рекомендаций позволила количественно обосновать системные требования к организационному резервированию для служб предприятия с количественными оценками на уровне прогнозируемых рисков.

Приблизительный годовой экономический эффект оценивается в 3 млн. руб. (за счет оптимизации организационного резервирования при ограничениях на допустимые риски и затраты).

Примечание. Производственное фармацевтическое предприятие ООО «Пранафарм» (ОГРН 1026301157915, ИНН 6316059876, КПП 631601001) функционирует в г. Самаре, ул. Ново-Садовая, д. 106, корп. 81 в соответствии с лицензией Л012-00102-77/00006728, выданной решением Министерства промышленности и торговли РФ от 28.11.2024 № 5591, состав продукции определяется 37 регистрационными удостоверениями Министерства здравоохранения РФ.

Председатель Совета директоров
ООО «Пранафарм»,
доктор технических наук Г.Я. Резников

Генеральный директор ООО «Пранафарм»,
доктор медицинских наук Е.А. Мишина

М.П.