УДК 004.9, 006.074

О ВЕРОЯТНОСТНЫХ МОДЕЛЯХ, ПРОГРАММНЫХ, ТЕХНОЛОГИЧЕСКИХ И МЕТОДИЧЕСКИХ РЕШЕНИЯХ ДЛЯ РАЦИОНАЛЬНОГО УПРАВЛЕНИЯ РИСКАМИ В СИСТЕМНОЙ ИНЖЕНЕРИИ

Нистратов А.А.

Федеральный исследовательский центр информатики и управления Российской академии наук, 119333, г.Москва, ул. Вавилова, 44, корп.2, тел. +7(925)915-70-08, e-mail: Andrey.nistratov@gmail.com

Применительно к вычислительным системам (ВС) и компьютерным сетям (КС) обзорно изложены некоторые результаты исследований, посвященные решению научной проблемы разработки широко применимых вероятностных моделей, программных, технологических и методических решений, ориентированных на прогнозирование и рациональное управление рисками в системной инженерии. Изложение охватывает следующие вопросы: анализ существующих подходов к оценке и управлению рисками, совершенствование и стандартизация вероятностных моделей для прогнозирования и рационального управления рисками в жизненном цикле различных систем, разработка программных и технологических решений, обеспечивающих прогнозирование рисков и обоснование упреждающих мер противодействия угрозам в автономном и удаленном режиме применения ВС и КС, для этих решений - разработка типовых методик применения в ВС и КС усовершенствованных вероятностных моделей, в заключение - разработка рекомендаций и демонстрационных примеров по снижению и удержанию рисков в допустимых пределах на основе применения созданной инфраструктуры и технологии поддержки риск-ориентированной системной инженерии. Приведены отдельные иллюстрирующие примеры.

Ключевые слова: модель, метод, риск, система, системная инженерия, технология

ABOUT PROBABILISTIC MODELS, SOFTWARE, TECHNOLOGICAL AND METHODOLOGICAL SOLUTIONS FOR RATIONAL RISK MANAGEMENT IN SYSTEM ENGINEERING

Nistratov A.A.

Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Vavilova Street 44, bld. 2, 119333 Moscow, Russia, tel. +7(925)915-70-08, e-mail: Andrey.nistratov@gmail.com

In relation to computing systems (CS) and computer networks (CN), some research results devoted to solving the scientific problem of developing widely applicable probabilistic models, software, technological and methodological solutions focused on predicting and rational risk control in system engineering are reviewed. The paper covers the following issues: analysis of existing approaches to risk assessment and control, improvement and standardization of probabilistic models for predicting and rational risk control in the lifecycle of various systems, development of software and technological solutions that ensure risk prediction and justification of proactive measures to counter threats in the autonomous and remote mode of application of CS and CS, for these solutions - development of typical methods for the use of advanced probabilistic models in CS and CS, and, finally, the development of recommendations and demonstration examples for reducing and maintaining risks within acceptable limits based on the use of the created infrastructure and technology to support risk-oriented system engineering. Some illustrative examples are given.

Keywords: method, model, probability, risk, system, technology

Введение

Анализ произошедших научно-технических революций и разнородных событий природного и техногенного характера побуждает к широкомасштабному исследованию и применению концептуальных воззрений и методов системной инженерии. Системная инженерия – это в первую очередь сосредоточение научно-технических усилий на том, как рациональным образом построить и эффективно эксплуатировать различные искусственно создаваемые системы. В качестве источников системной инженерии как научно-прикладной дисциплины Международный совет по системной инженерии (INCOSE) рассматривает западные ракетные технологии и

развитие железнодорожного транспорта, системы безопасности, телефонии, вооружений (1937-1956гг.), первые технологии авиакосмической промышленности, результаты моделирования городских систем в Массачусетском технологическом институте (1957-1980гг.) [1]. В России становление системной инженерии произошло, в первую очередь, благодаря достижениям в области ракетостроения, освоения космоса и обеспечения безопасности.

Сегодня теоретические основы системной инженерии еще продолжают находиться в стадии становления. Перекрестное внедрение в различных отраслях промышленности существующих методов системной инженерии идет медленно. Наиболее узким местом отечественной системной инженерии является отсутствие доступных и широко применимых программных и технологических решений для вычислительных систем (ВС) и компьютерных сетей (КС), ориентированных на прогнозирование и рациональное управление рисками в достижении системных целей. По этой же причине сдерживается междисциплинарная интеграция научно-технических усилий, применимая в различных типовых процессах на всех этапах жизненного цикла (ЖЦ) различных систем.

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 прогнозирования и исследований, основанными на моделях, позволяющих лучше понимать все более сложные системы и решения, принимаемые в условиях неопределенности. Обеспечение и поддержание необходимой конкурентоспособности на отечественном и мировом научно-технологическом рынке должно поддерживаться эффективными инструментариями и решениями на уровне ВС и КС.

Степень разработанности проблематики. 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 Martin J., Kleinrock L., B. Boehm, H.Kumamoto, E. Henley, D. Vose, E.H. Conrow, J. Mun [2-10] и другие ученые США. 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). Вопросы многосторонней методической оценки качества и безопасности функционирования различных систем с использованием вероятностного моделирования были заложены в школах отечественных ученых Б.В. Гнеденко, Н.А. Махутова, Н.Н. Моисеева. В последние десятилетия исследования были продолжены и расширены В.А. Балыбердиным, И.В. Бычковым, В.И. Васильевым, Е.С. Вентцель, Я.Д. Вишняковым, С.А. Головиным, Л.И. Григорьевым, Г.В. Дружининым, А.А. Зацаринным, К.К. Колиным, В.Ю. Королевым, А.И. Костогрызовым, И.В. Котенко, В.В. Кульбой, В.В. Липаевым, В.В. Москвичевым, Д.А. Новиковым, Б.А. Позиным, И.Н. Синицыным, И.А. Соколовым, П.В. Степановым, А.А. Стрельцовым, В.А. Сухомлиным, 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. Анализ упомянутых и многих других исследований показывает, что в условиях разнородных неопределенностей для критичных систем тематика управления рисками сохраняет свою теоретическую и практическую важность. 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. 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 систем. За редким исключением возможности существующих Интернет-технологий не используются для вероятностного прогнозирования рисков. Тем самым в системной инженерии отсутствует широкодоступный сервис для моделирования различных систем 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. На сегодня возникло критичное методологическое и программно-технологическое противоречие между объективными потребностями в рациональном управлении рисками в системной инженерии и реальными программными и технологическими возможностями в применении в реальном времени получаемых результатов прогнозирования.

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 исследований.

Осуществляя научный поиск практических путей, способствующих устранению выявленного противоречия, в настоящей работе обзорно изложены некоторые результаты исследований, посвященные решению научной проблемы разработки широко применимых вероятностных моделей, программных, технологических и методических решений, ориентированных на прогнозирование и рациональное управление рисками в системной инженерии, см. подробнее [1-31].

Главной целью статьи является обзорное изложение основных идей предлагаемых научно обоснованных математических, программных, технологических и методических решений для ВС и КС, посвященных упреждающему выявлению «узких мест» и определению рациональных способов снижения и удержания рисков в допустимых пределах в жизненном цикле систем различного функционального назначения в условиях реальных и гипотетичных вызовов и угроз.

1. Анализ существующих подходов к оценке и управлению рисками в жизненном цикле систем

В результате анализа существующих подходов к оценке и управлению рисками в жизненном цикле различных систем осуществлен анализ роли и места системной инженерии в решении практических задач, выявлены тенденции в изменениях современных систем, проведен анализ стандартизованных процессов в жизненном цикле систем, разработаны принципы для риск-ориентированного решения практических задач с использованием вычислительных систем и компьютерных сетей, определены требования к методам системного анализа с использованием вычислительных систем и компьютерных сетей.

Показано, что в условиях неопределенностей роль системной инженерии в решении практических задач является определяющей 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.

Выявлены 10 основных тенденций в изменениях современных систем на ближайшую 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.

Установлена необходимость анализа соответствующих рисков при выполнении всех стандартизованных процессов с учетом задаваемых требований:

– 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.

При решении практических задач с использованием риск-ориентированного подхода 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.

Все применяемые принципы должны быть согласованы с принципом целенаправленности осуществляемых действий.

Научная проблема поставлена таким образом, чтобы предлагаемые новые научно обоснованные математические, программные, технологические и методические решения для ВС и КС позволяли обеспечить в жизненном цикле систем: 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. В результате решения научной проблемы ожидается прототип интеллектуального инструментария системного аналитика, опирающегося на стандартизованные модели и применимого в жизненном цикле систем различного функционального назначения для решения практических задач системной инженерии.

2. Совершенствование и стандартизация вероятностных моделей

В рамках исследований по совершенствованию и стандартизации вероятностных моделей для прогнозирования и рационального управления рисками в жизненном цикле систем сформулированы основные идеи по построению пространства элементарных событий, определены формализованные показатели для прогнозирования рисков, сделан выбор вероятностных моделей для использования в качестве базовых, сформулированы и доказаны основные теоремы 1-4 для расчетов формализованных показателей рисков в ВС и КС и совершенствования базовых моделей для анализа системных элементов, сложных систем и процессов, осуществлена реализация основных положений по моделированию, прогнозированию и упреждающему управлению рисками в национальных стандартах, сформирован концептуальный облик предлагаемых математических, программных и технологических решений для ВС и КС.

В условиях различных неопределенностей на сформулированном пространстве элементарных событий (с учетом специальных физически измеримых показателей) предложено использовать следующие показатели рисков, одинаково свойственные для любого рода систем:

– риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза при реализации основных функциональных требований, в т.ч. риски нарушения рассматриваемого системного процесса для реализации основных функциональных требований;

– риск нарушения дополнительных специфических требований к моделируемой системе в течение задаваемого периода прогноза, в т.ч. риски нарушения рассматриваемого системного процесса с учетом дополнительных специфических системных требований;

– интегральный риск нарушения целостности моделируемой системы в течение задаваемого периода прогноза при реализации основных функциональных требований и дополнительных специфических требований, как частный случай - интегральный риск нарушения комплексной безопасности системы в течение задаваемого периода прогноза.

Рассматриваются широко применимые вероятностные модели из ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы»: «Математическая модель «черного ящика» при отсутствии какого-либо контроля» (модель из приложения В.2.2) и более общая «Математическая модель «черного ящика» при реализации технологии периодического системного контроля» (модель из приложения В.2.3). Эти же модели предлагаются к использованию другими стандартами системной инженерии применительно к системам различного функционального назначения – см., например, ГОСТ Р 59329 – ГОСТ Р 59357, ГОСТ Р 59989 – ГОСТ Р 59994. Для них предлагаются следующие теоремы:

Теорема 1 (о существовании расчетного риска, зависящего от различных длительностей диагностики и восстановления нарушенной целостности, с применением модели В.2.3).

Пусть процесс функционирования системы формализован с помощью модели В.2.3 (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 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 В.2.3 по формулам (В.1) – (В.5) из ГОСТ Р 59341-2021 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 В.2.3. Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление целостности;

2-я итерация осуществляется после расчета риска $R_{.}^{(1)}$ с использованием модели В.2.3 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:

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

где $R_{неконтр.}^{(n-1)}$ вычисляется по модели В.2.3, 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: $|R_{.}^{(n)} - R_{.}^{(n-1)}| \le \varepsilon$.

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 [31]. Применительно к ВС и КС для достижения практически приемлемой адекватности минимальное значение ε установлено в численном выражении не менее, 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.

Теорема 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).

Примечание. 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.

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 универсальной вспомогательной модели показателя (УВМП, из ГОСТ Р 59349-2019 «Системная инженерия. Защита информации в процессе системного анализа»): «Приемлемое», «Приемлемое с отклонением», «Неприемлемое» - см. рис. 1.

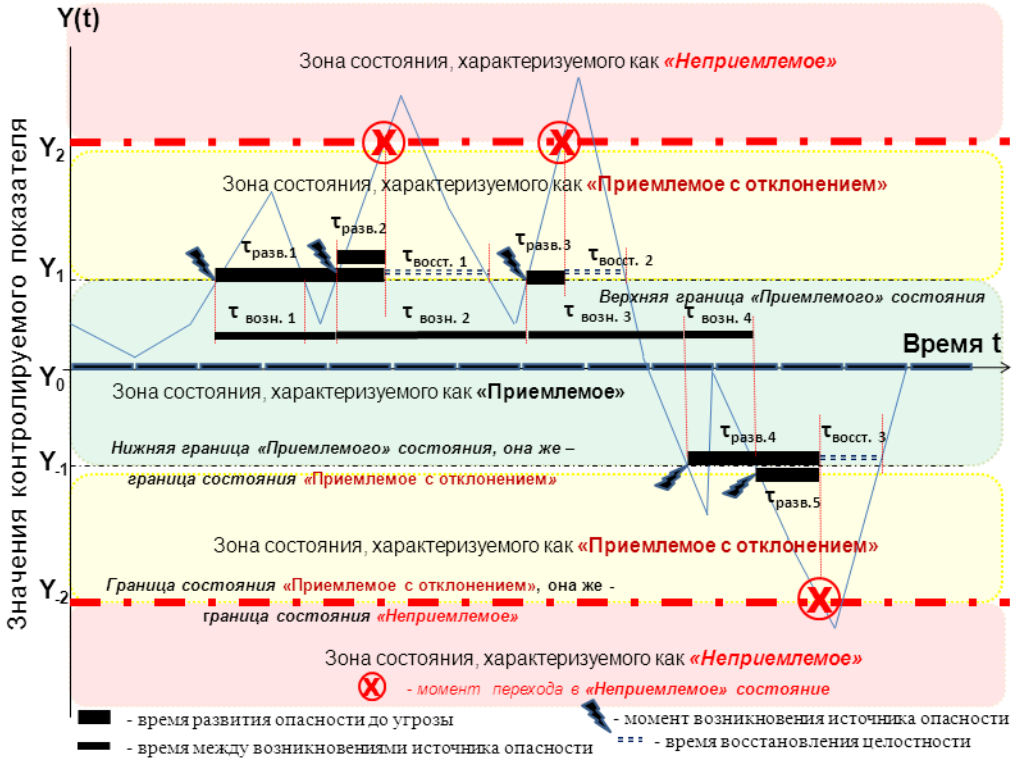

Рис. 1 – Элементарные состояния контролируемого показателя УВМП во времени и временные характеристики для прогнозирования рисков

При этом пусть 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 В.2.2 из ГОСТ Р 59341-2019) 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 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 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. Причем 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. 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. 2 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. 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 $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}) = R_{наруш}(\sigma, \beta, T_{зад})$. 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 $\Omega_{возд.}(t) = 1-\exp(-\sigma t)$ и $\Omega_{акт.}(t) = 1-\exp(-t/\beta)$. 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).

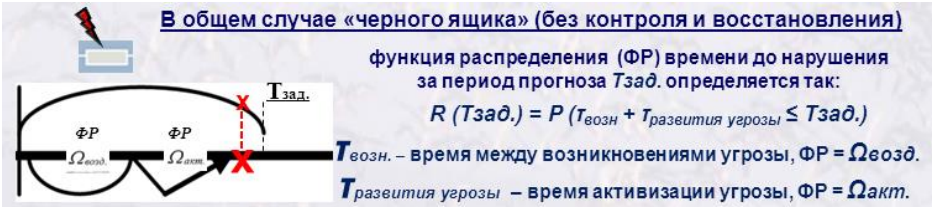

Рис. 2 – Формальный случай нарушения целостности системы за период прогноза $T_{зад}$

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 $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}) = R_{наруш}(\sigma, \beta, T_{зад})$ с вычислительной точностью ε. В свою очередь эта ФР $R_{наруш}(\sigma, \beta, T_{зад})$ строится с помощью «Модели «черного ящика» при отсутствии какого-либо контроля» по точкам расчета при $T_{зад}$, пробегающем все значения от 0 до ∞. По условиям теоремы неизвестным является не просто значение β, а такое β, которое практически совпадает с периодом прогноза $T_{зад}$. В итоге ищется значение минимального ненулевого времени развития угроз x (т.е. неизвестное x=β), когда за прогнозный период $T_{зад}$ (тоже равный неизвестному x) риск нарушения целостности моделируемой системы впервые достигнет установленного допустимого уровня риска $R_{доп}(x)$ 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

$$R_{наруш}(\sigma, x, x) = R_{доп}(x) \qquad (1)$$

относительно x с задаваемой расчетной точностью ε. Искомое неизвестное x занимает в формульном выражении $R_{наруш}(\sigma, \beta, T_{зад})$ место параметров β и $T_{зад}$.

Здесь $R_{наруш}(\sigma, x, x) = 1 - P_{возд(1)}$. Расчет идет для случая, когда ФР времени отсутствия нарушения целостности моделируемой системы $P_{возд(1)} = P_{возд(1)}(\sigma, x, T_{меж}, T_{диаг}, x)$ выражается в виде:

$$P_{возд(1)} = \begin{cases} \left(\sigma - x^{-1}\right)^{-1}\left\{\sigma e^{-1} - x^{-1}e^{-\sigma x}\right\}, если\ \sigma \neq x^{-1}, \\ e^{-\sigma x}\left[1+\sigma x\right], если\ \sigma = x^{-1}. \end{cases} \qquad (2)$$

Решение нелинейного уравнения (1) существует, поскольку слева функция $R_{наруш}(\sigma, \beta, T_{зад})$ 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 $T_{зад}$ от нуля до бесконечности значение риска монотонно возрастает от 0 до 1 (как ФР по $t=T_{зад}$). 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 $T_{зад}$, стремящемся к ∞, нарушения за этот период прогноза неизбежны. В терминах элементарных событий по УВМП это означает, что переходы из элементарного состояния «Приемлемое» в состояние «Приемлемое с отклонением» 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» становятся реже, т.е. значения критичного параметра в основном колеблятся в «зеленой» или «желтой» зонах, не выходя в «красную» зону – см. рис. 1.

Поскольку справа в уравнении (2.9) $R_{доп}$ – это константа по оси «у» в интервале (0,1), то, при вычислениях, увеличивая от нуля $R_{доп}$ с некоторым шагом (например, с шагом $0.01R_{доп}$), определяются ближайшие точки пересечения этой горизонтальной линии (параллельной оси «х») с траекторией функции $R_{наруш}(\sigma, x, x)$, зависящей от x, а также от σ. В итоге каждому значению $R_{доп}$ из сетки на оси «у» (с шагом $0.01R_{доп}$) будет соответствовать на оси «х» одна или ряд точек x_0 пересечения $R_{доп}$ с функцией $R_{наруш}(\sigma, x, x)$ - 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 (9), 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.

Теорема 2 действует при использовании модели из В.2.2. В этом случае лицо, принимающее решение о принятии упреждающих мер, придерживается предположения о худшем развитии событий, оценивая снизу – какое можно ожидать время до 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 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»). На самом деле 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 В.2.3). Сразу возникают два практических вопроса: «Какой по длительности выбирать период между диагностиками целостности системы?» и «Каково среднее остаточное время до 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 Теорема 3.

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. (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 В.2.3 с учетом Теоремы 1). 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.

Доказательство Следствия из Теоремы 2.

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 (1) и (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 (1) и (2). Например, при $\sigma=\beta^{-1}$ выражение (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 (1), (2) построены зависимости риска нарушения целостности моделируемой системы *R* от z, точнее от $T_{зад}/\beta$ – см. рис. 3 – 7.

Примечание. Значение задаваемого допустимого уровня $R_{доп}$=0.1 непринципиально, оно выбрано лишь для иллюстрации предлагаемого подхода к определению ограничений на основе выявляемых закономерностей. Выявленные ниже закономерности позволяют установить ограничения, аналогичные по логике их определения, для любого задаваемого значения $R_{доп}$.

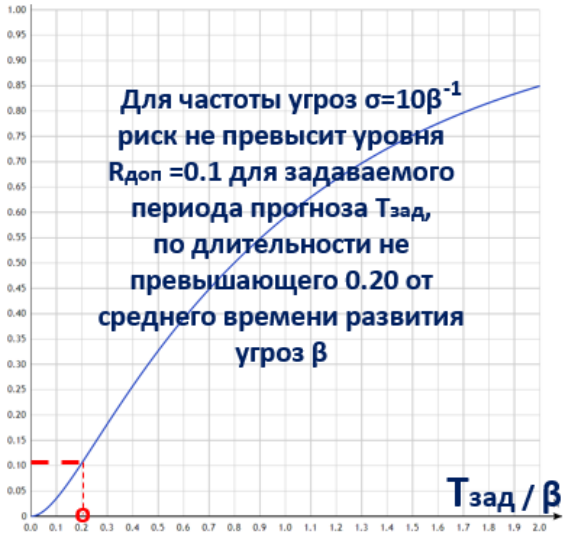

Рис. 3 – Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=10\beta^{-1}$

Рис. 4 – Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=2\beta^{-1}$

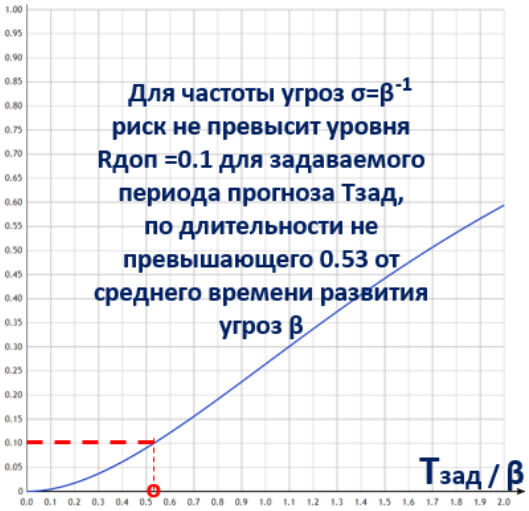

Рис. 5 – Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=\beta^{-1}$

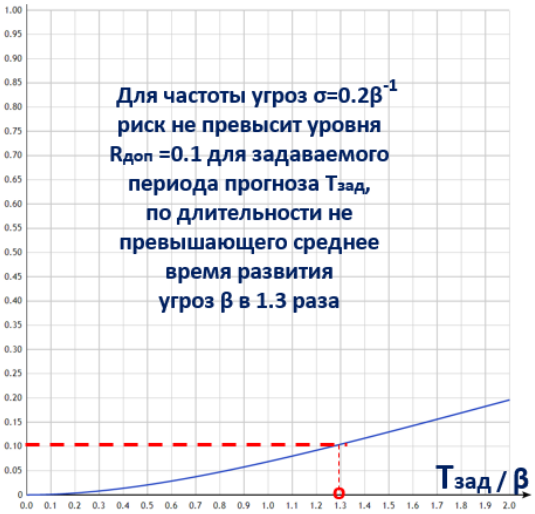

Рис. – 6 Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=0.2\beta^{-1}$

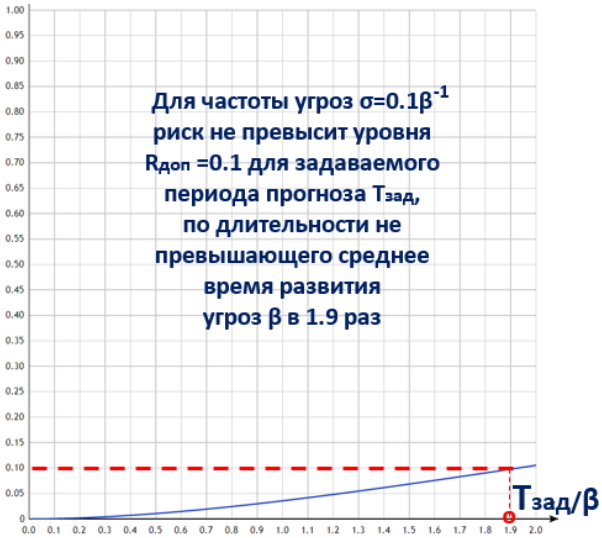

Рис. 7 – Зависимость риска от $T_{зад}/\beta$ и выявленная закономерность для $\sigma=0.1\beta^{-1}$

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. 8 – 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:

– ри 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 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. 8 представлено обобщение выявленных закономерностей.

Условия Следствия из Теоремы 2 представляют собой условия, сформулированные на рис. 3-8 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.

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

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 ГОСТ Р 59349-2021 – см. рис. 1): «Приемлемое», «Приемлемое с отклонением», «Неприемлемое». Тогда среднее остаточное время до 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, вычисляемой при использовании «Модели «черного ящика» при реализации технологии периодического системного контроля» (из В.2.3 с учетом Теоремы 1).

Доказательство Теоремы 3. Применение «Модели «черного ящика» при реализации технологии периодического системного контроля» (из В.2.3) позволяет вычислить значения $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ в последовательных K точках $T_{зад} = t_1 \geq 0, t_2, t_3, \ldots, t_{K-1}, t_K$, 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 $R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, t_K)$ достигает 1, т.е. $1-\varepsilon \leq R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, t_K) \leq 1$.

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. 3-8 позволяют установить аналогичные закономерности для любого задаваемого значения $R_{доп}$.

Это достижимо при использовании вероятностной меры, когда N – действительное число, учитывающее не только целую, но и дробную части при расчетах по формулам (3) – (5) – см. соответствующее

примечание в В.2.3: «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)».

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:

$$\text{Среднее (для отдельного элемента)} = \text{МОЖ} = \sum_{k=1}^{K} t_k R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, t_k). \quad (3)$$

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 (3) с использованием «Модели «черного ящика» при реализации технологии периодического системного контроля» (из В.2.3).

Доказательство Теоремы 3 завершено.

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. 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.

Для сложной системы возникает тот же самый актуальный вопрос: «Каково среднее остаточное время до 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 каждого составного элемента сложной системы).

Для этого случая применимо теоретическое обоснование возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых из «черных ящиков», осуществленное в В.2.4 из ГОСТ Р 59341-2021, Приложения В.

Соответствующий ответ на сформулированный выше вопрос дает предлагаемая Теорема 4.

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

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 В.2.4 из ГОСТ Р 59341-2021). 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: «Приемлемое», «Приемлемое с отклонением», «Неприемлемое». Тогда с использованием результатов Теоремы 3 среднее остаточное время до 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 В.2.3 с учетом Теоремы 1).

Доказательство Теоремы 4. Применение Теоремы 3 (с примечанием) позволяет поточечно построить по значениям в последовательных K точках $T_{\text{зад}} = t_1 \geqslant 0, t_2, t_3, \ldots, t_{K-1}, t_K$ траектории ФР времени до нарушения целостности $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$ для каждого из элементов декомпозированной системы (со своими исходными данными $\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}$ при одних и тех же значениях $t_1, t_2, t_3, \ldots, t_{K-1}, t_K$).

Примечание. Адекватность применения Теоремы 3 в частных случаях подтверждается применением инженерных способов, в частности, способом определения границ рабочего диапазона критичных параметров мониторируемого объекта – см. ГОСТ Р 58494-2019.

Использование одних и тех же значений t_1, t_2, t_3,…, t_{K-1}, t_K позволяет в полной мере использовать расчеты с использованием ВС и КС в построении ФР для интегрированной моделируемой системы, вычисляемой с использованием «Модели «черного ящика» при реализации технологии периодического системного контроля» (из В.2.3 с учетом Теоремы 1). В итоге для интегрированной моделируемой сложной системы получается поточечно построенная ФР времени до нарушения целостности системы в целом: $R_{\text{наруш}}(T_{\text{зад}})$, зависящая также от параметров σ, β, $T_{\text{меж}}$, $T_{\text{диаг}}$, $T_{\text{восст}}$ со своими значениями для каждого из элементов интегрируемой структуры при одних и тех же значениях $T_{\text{зад}} = t_1, t_2, t_3,\ldots, t_{K-1}, t_K$.

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 $R_{\text{наруш}}(T_{\text{зад}})$ поточечно описывает функцию распределения времени наработки на нарушение целостности всей интегрированной системы, монотонно возрастающую от 0 до 1.

Для этой построенной ФР $R_{\text{наруш}}(t_k)$ среднее значение остаточного времени до нарушения целостности сложной системы при своевременном принятии упреждающих мер противодействия угрозам так же, как в Теореме 3, определяется по формуле (3) 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.

Доказательство Теоремы 4 завершено.

Применения предложенных Теоремы 1, универсальной вспомогательной модели показателей (УВМП), используемой для извлечения знаний из процесса мониторинга данных, Теоремы 2, выявленных закономерностей в соотношениях исходных данных для непревышения задаваемого допустимого уровня риска и сохранения целостности моделируемой системы, Следствия из Теоремы 2, Теоремы 3, теоретического обоснования возможностей аналитической композиции прогнозируемых рисков для сложных систем, интегрируемых из «черных ящиков», и Теоремы 4 позволило осуществить теоретические усовершенствования существующих моделей и методов и тем самым сформировать базовые модели для анализа системных элементов, сложных систем и процессов с использованием ВС и КС.

С учетом основных положений Теорем 1 – 4 дополнительно наряду с рисками, определенными в разделе 1 статьи, предложено определять следующие расчетные показатели (рассчитываемые с использованием ВС и КС):

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

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

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

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.

Стандартизованные математические и методические решения из этих стандартов внедрены в практику работы национального технического комитета ТК22 «Информационные технологии» в части рекомендаций по использованию созданных методов, моделей и демонстрационных примеров системной инженерии в новых стандартах 2024г.: 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)».

3. О программных и технологических решениях

Сформированный концептуальный облик создаваемой инфраструктуры и технологии поддержки риск-ориентированной системной инженерии для решения практических задач с использованием ВС и КС отражен на рис. 9.

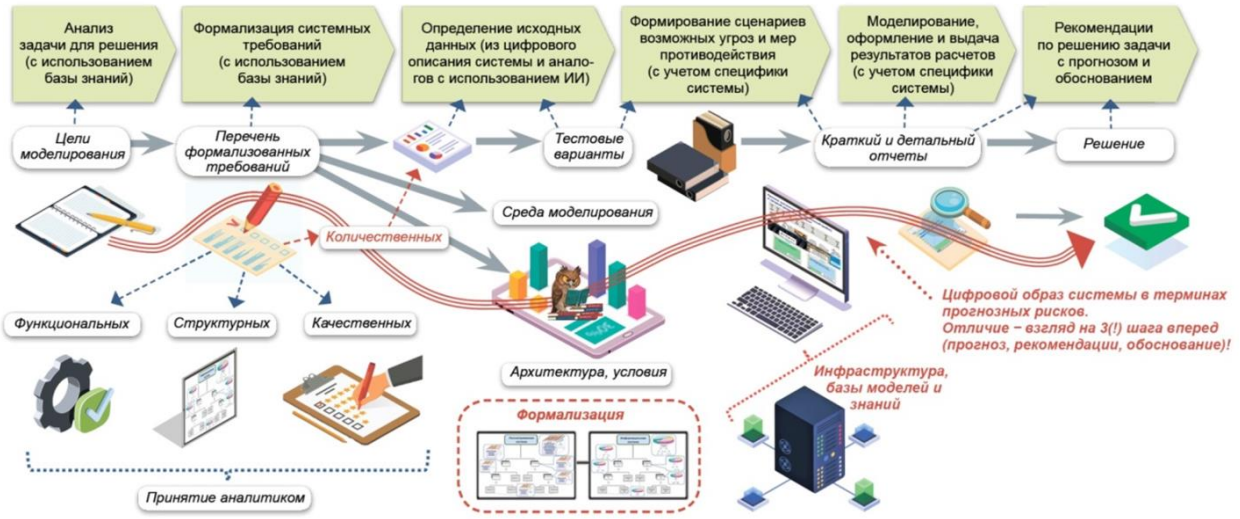

Рис. 9 – Концептуальный облик инфраструктуры и технологии поддержки риск-ориентированной системной инженерии для решения практических задач

Это позволило осуществить разработку программных и технологических решений, обеспечивающих прогнозирование рисков и обоснование упреждающих мер противодействия угрозам в автономном и удаленном режимах применения ВС и КС – см. рис. 10.

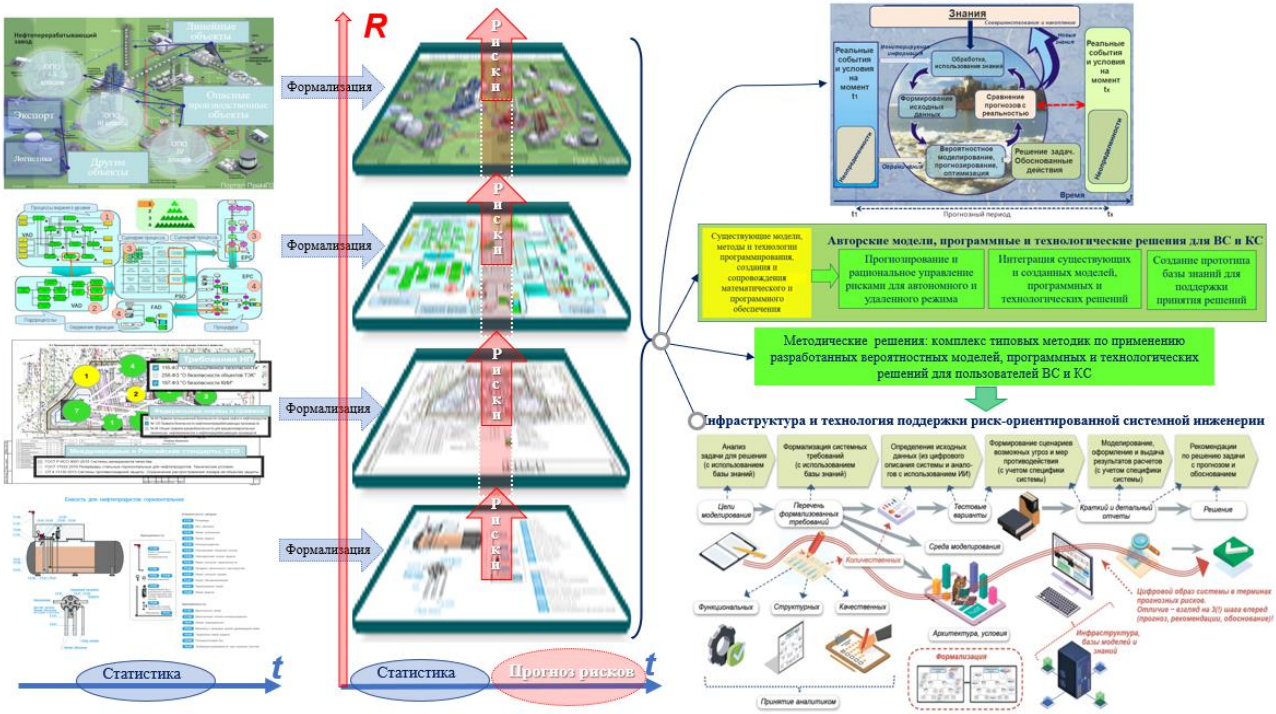

Рис. 10 – Замысел поддержки риск-ориентированной системной инженерии для решения практических задач, реализованный на уровне программных и технологических решений

4. О типовых методиках прогнозирования рисков

На основе созданных программных и технологических решений разработаны типовые методики прогнозирования рисков нарушения целостности моделируемой системы, представимой в виде «черного ящика»,

и нарушения целостности сложной моделируемой системы, применимые в жизненном цикле систем различного назначения. Разработан инженерный подход к определению границ рабочего диапазона критичных параметров мониторируемого объекта. С инженерной точки зрения применение 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).

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 промышленной безопасности и риски утраты работоспособности за сутки;

– прогнозирование рисков нарушения промышленной безопасности 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 промышленной безопасности за сутки. За год при идеальном управлении с использованием СДК риск может снизиться до уровня 0.24, что в 3 раза ниже, чем вероятность безопасного функционирования исследуемого оборудования;

– моделирование многомодального взаимодействия социокиберфизических систем в жизненном цикле обогатительной фабрики в угольной отрасли для обоснования путей усовершенствования (перевооружения) системы вентиляции, аспирации и пылеподавления. 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 12 лет 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.

Разработанные методические решения в совокупности с разработанными в разделах 1 – 3 математическими, программными и технологическими решениями для ВС и КС позволили констатировать создание в итоге практически востребованных научно-техническим сообществом инфраструктуры и технологии поддержки риск-ориентированной системной инженерии.

Пример 1. Исследуемая система - главная вентиляторная установка (ГВУ) гипотетичной угольной шахты.

Задача 1.1. Рассматривается фрагмент «дерева отказов», способных привести к аварии на опасном производственном объекте из-за отказа главной вентиляторной установки и повышенной концентрации метана. В качестве анализируемого объекта для прогнозирования рисков нарушения промышленной безопасности (ПБ) с использованием СКД выступает ГВУ с осевым двухступенчатым вентилятором (ГВУ ВОКД 3,6) – см. рис. 11.

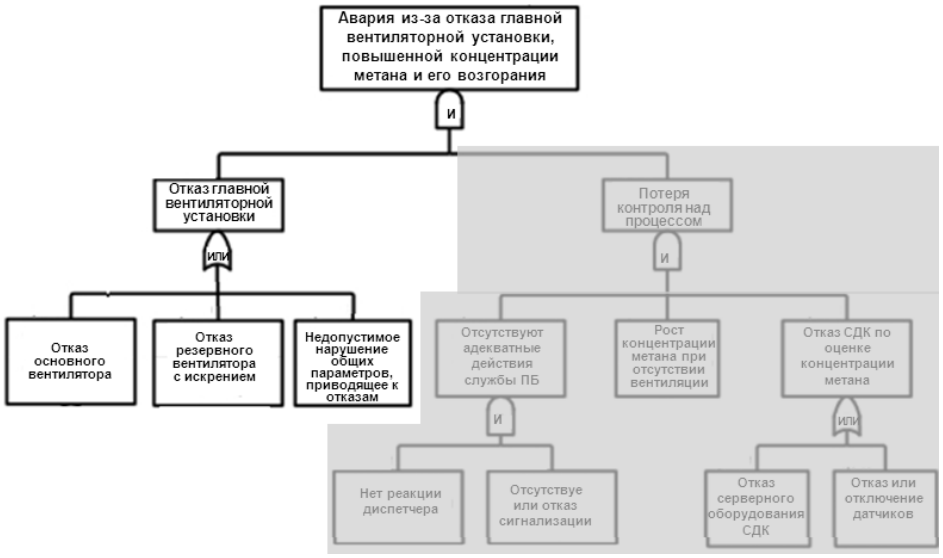

Рис. 11 – Фрагмент дерева отказов, способных привести к аварии на опасном производственном объекте из-за отказа главной вентиляторной установки (ГВУ)

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. 12.

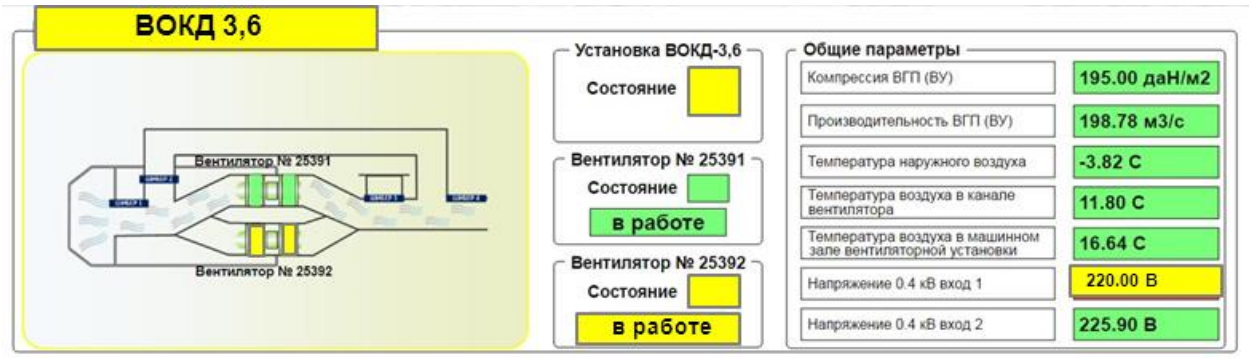

Рис. 12 – Пример состояния ВОКД 3,6

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 обычной системы контроля (СК), т.е. без использования возможностей СДК, и с осуществлением требуемых или рекомендуемых мер противодействия угрозам с использованием СДК.

Решение задачи 1.1. Формализация для прогнозирования рисков отражена на рис. 13. Представленная формализация с учетом УВМП (см. рис. 1) и логики декомпозиции и интеграции с ложных систем (см. ГОСТ Р 59341, приложение В.2.4) 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. 13 – Формализация ВОКД 3,6 в виде сложной структуры для решения задачи 1.1

Для каждого из элементов формализации определяются необходимые исходные данные для прогнозирования рисков.

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. 11, 12. 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. 14), среднее время до нарушения ПБ при этом составит 488 часов, т.е. всего 20 суток (рис. 15).

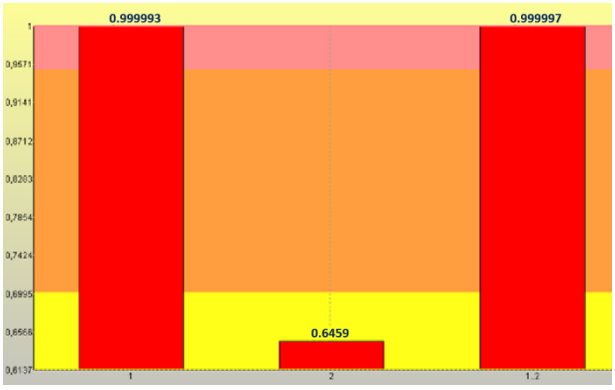

Рис. 14 – Риск критичного нарушения ПБ за год при полном бездействии (1- за 1-ю подсистему, 2- за 2-ю подсистему, 1…2 – за систему в целом)

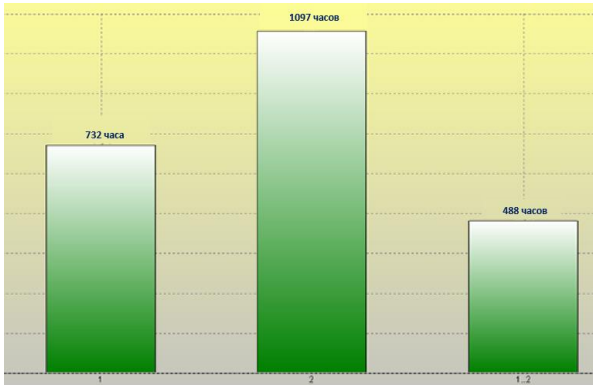

Рис. 15 – Среднее время до нарушения ПБ при полном бездействии

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, 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. 16), среднее время до нарушения ПБ при этом составит около 40 лет – это в идеале (см. рис. 17).

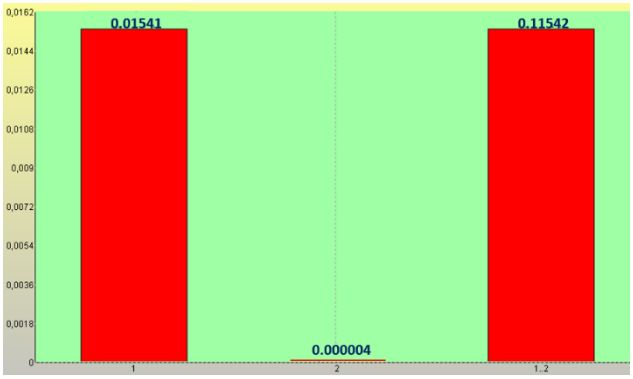

Рис. 16 – Риск критичного нарушения ПБ за год при идеальном управлении (1- за 1-ю подсистему, 2- за 2-ю подсистему, 1…2 – за систему в целом)

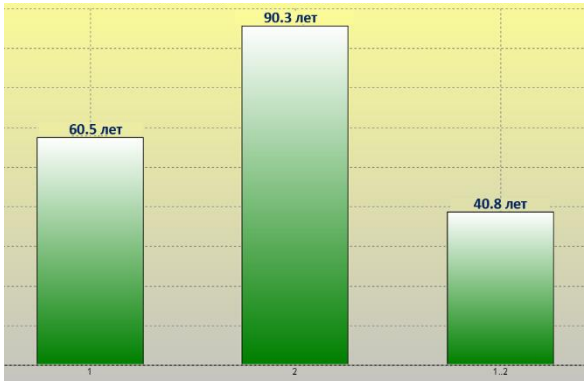

Рис. 17 – Среднее время до нарушения ПБ при идеальном управлении (в годах)

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 СК (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 без использования возможностей СДК.

Вывод по задаче 1.1. Для главной вентиляторной установки использование возможностей СДК позволяет в 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).

5. Рекомендации и демонстрационные примеры

На основе применения возможностей созданной инфраструктуры и технологии поддержки риск-ориентированной системной инженерии разработаны рекомендации и демонстрационные примеры по снижению и удержанию рисков в допустимых пределах в жизненном цикле различных систем – см. [14-17, 19-29, 31].

Продемонстрирован способ логического преобразования изначального вербального описания сложной системы к формализованному виду, позволяющему использовать предложенные математические, программные, технологические и методические решения для ВС и КС. В качестве системы без ограничения общности рассмотрен технический облик гипотетичной многоуровневой системы управления рисками, подлежащей созданию в интересах обеспечения энергетической безопасности согласно "Доктрине энергетической безопасности Российской Федерации". Сведение вербального описания сложной системы к формализованному

виду позволяет применять возможности созданной инфраструктуры и технологии для формальной постановки и решения практических задач:

– минимизации риска нарушения надежности обеспечения энергетической безопасности макрорегиона государства или отдельно взятого субъекта энергетической безопасности в топливно-энергетическом комплексе (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 могут быть использованы для обеспечения баланса по критерию «эффективность – стоимость» при кратко-, средне- и/или долгосрочном планировании на уровне макрорегиона государства или отдельно взятого субъекта энергетической безопасности.

Ниже на примере 2 продемонстрировано применение разработанных математических, 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), что обеспечивает прослеживаемость и аналитическую зависимость прогнозных рисков от влияющих факторов.

Пример 2. В качестве области приложения разработанных математических, 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 математические, 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. 18, в каждой точке – данные, в т.ч. привязанные ко времени измерения и сравнения с нормативными границами (например, по УВМП).

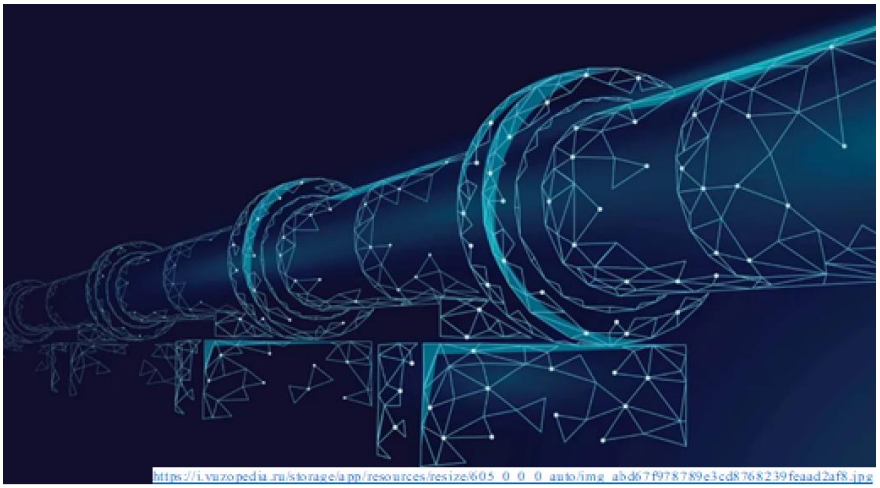

Рис. 18 – Пример цифрового двойника фрагмента магистральной трубы

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 осуществить системное обоснования 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 методик предлагается использовать рекомендованные базовые вероятностные модели и методы (см. разделы 2 – 4), отраженные в авторских работах [14-17, 19-29, 31], 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 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. 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 1 – 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	3года

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. 19, 20. Анализ зависимости показывает, что лишь для прогнозного периода 1 год интегральный риск составит около 0.1 (на рис. 5.9).

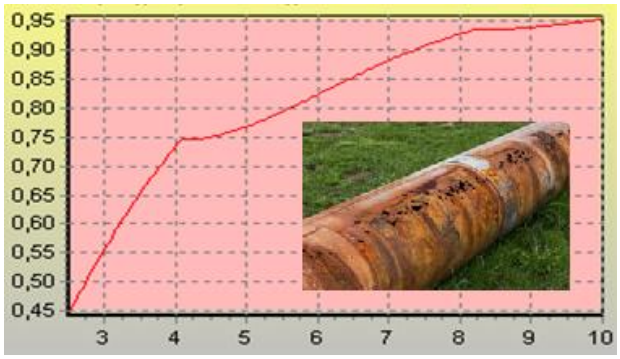

Рис. 19 – Зависимость интегрального риска от периода прогноза, изменяемого в диапазоне от 2.5 до 10 лет

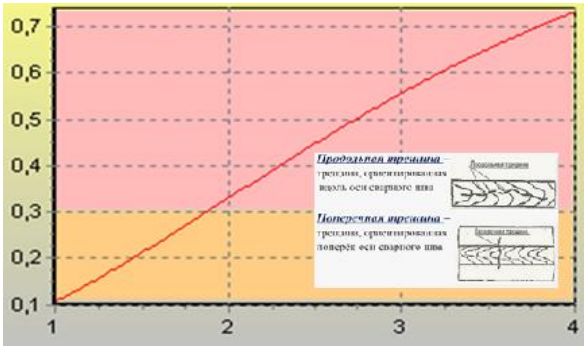

Рис. 20 – Зависимость интегрального риска от периода прогноза, изменяемого в диапазоне от 1 до 4-х лет

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. 21 – 22 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.

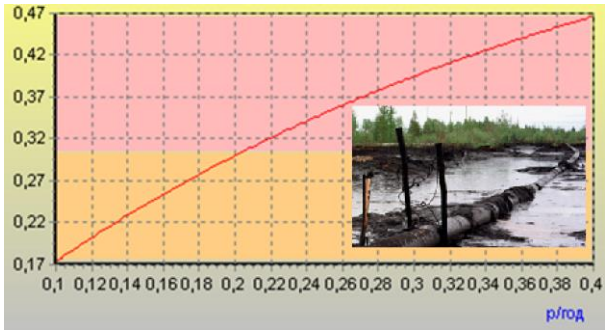

Рис. 21 – Зависимость риска нарушения целостности от «частоты возникновения угроз» для фрагмента 5 при прогнозе на 5 лет

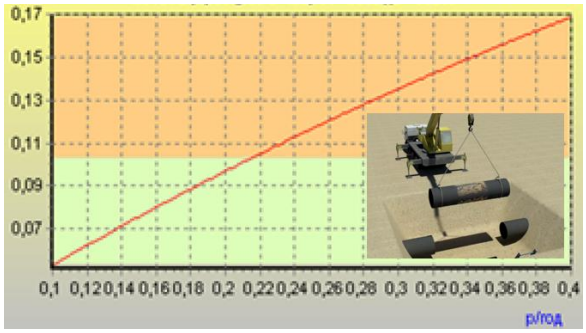

Рис. 22 – Зависимость риска нарушения целостности от «частоты возникновения угроз» для фрагмента 5 при прогнозе на 2 года

На рис. 23, 24 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.

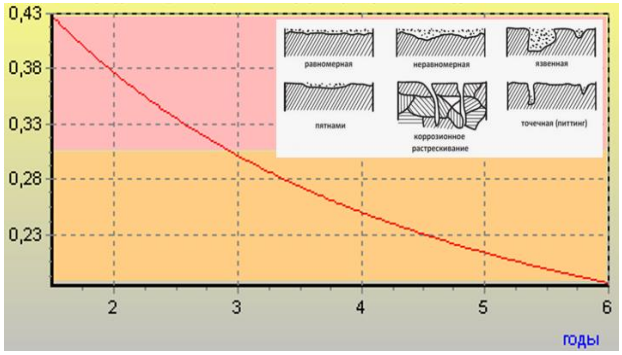

Рис. 23 – Зависимость риска нарушения целостности от «среднего времени развития угроз» для фрагмента 5 при прогнозе на 5 лет

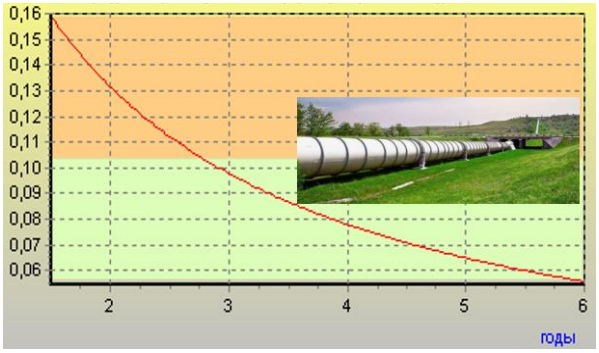

Рис. 24 – Зависимость риска нарушения целостности от «среднего времени развития угроз» для фрагмента 5 при прогнозе на 2 года

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 при выявлении для этих прогнозных сроков 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 дополнением к техническим мерам, востребуемым по итогам регулярного внутритрубного диагностирования реальных сетей. Важно подчеркнуть, что за счет использования возможностей созданной инфраструктуры и технологии 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.

Таким образом применение предложенных математических, 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) привели к удовлетворению важной аналитической потребности. А именно: их применение обеспечивает прослеживаемость и аналитическую 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.

Для другой области приложения, связанной с обеспечением качества хранимого зерна, с использованием предложенных базовых моделей 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 [31].

Продемонстрирована способность расширения аналитических возможностей созданной инфраструктуры и технологии риск-ориентированной системной инженерии путем добавления другой модели. Еще для иной области приложения в интересах демонстрации 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 и дообучения (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 проиллюстрирована количественными примерами [26].

Разностороннее использование возможностей созданной инфраструктуры и технологии 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 к каждой из служб организационного управления. Сформулированы условия (определяемые главным образом ответственностью и высокой квалификацией работников предприятия, формализуемые с помощью временных характеристик реакции на угрозы) при активном управлении и эффективной поддержке со стороны Руководства предприятия. На примерах показано, что с высокой вероятностью именно соблюдения этих обоснованных условий обеспечит сохранение бизнеса в долговременной перспективе.

Сформулированы перспективные направления исследований [29].

Заключение

В приложении к применению в вычислительных системах и компьютерных сетях обзорно изложены новые научно обоснованные математические, программные, технологические и методические решения, реализованные в рамках созданной инфраструктуры и технологии риск-ориентированной системной инженерии. Место и роль проведенных исследований и авторский вклад в науку на рис. 25.

Вклад в математические решения задач системной инженерии позволил усовершенствовать существующую концепцию управления рисками и состоит: в формулировке и доказательстве теорем 1-4; в усовершенствовании на основе теорем базовых вероятностных моделей и методов повышения адекватности вероятностного моделирования с использованием ВС и КС 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 в ВС и КС.

Вклад в программные и технологические решения задач системной инженерии состоит в расширении для ВС и КС практических возможностей по: прогнозированию и рациональному управлению рисками в автономном и удаленном режимах; интеграции существующих и созданных моделей, программных и технологических решений; созданию прототипа базы знаний для поддержки принятия решений.

Вклад в методические решения задач системной инженерии состоит в создании комплекса типовых методик по применению разработанных вероятностных моделей, программных и технологических решений для пользователей ВС и КС и разработке типовых примеров демонстрации работоспособности и обоснования рекомендаций по снижению и удержанию рисков в допустимых пределах.

Рис. 25 – Место и роль проведенных исследований и вклад в науку

Применение в жизненном цикле систем различного функционального назначения предлагаемых новых научно обоснованных математических, программных, технологических и методических решений для ВС и КС позволит обеспечить упреждающее выявление «узких мест» и определение рациональных способов снижения и удержания рисков в допустимых пределах в условиях реальных и гипотетичных вызовов и угроз.

Список литературы

1. Systems Engineering Handbook. A Guide for System Life Cycle Processes and Activities. Fifth Edition. 2023. INCOSE-TP-2003–002-05
2. Винер Н. Кибернетика или Управление и связь в животном и машине. Изд.2-е. М.: Сов.радио, 1968. - 326с.
3. Гуд Г.Х., Макол Р.З. Системотехника: Введение в проектирование больших систем. – М.: Советское радио, 1962. – 383 с.
4. Martin J. System Analysis for Data Transmission. V. II, IBM System Research Institute. Prentice Hall, Inc., Englewood Cliffs; New Jersey. 1972
5. Kleinrock L. Queueing systems, V.2: Computer applications, John Wiley & Sons; New York. 1976
6. Boehm, B. 1989. *Software Risk Management.* Los Alamitos, CA; Tokyo, Japan: IEEE Computer Society Press, p. 115-125.
7. Kumamoto, H. and E. Henley. 1996. *Probabilistic Risk Assessment and Management for Engineers and Scientists,* 2nd ed. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers (IEEE) Press.
8. Vose, D. 2000. *Quantitative Risk Analysis,* 2nd ed. New York, NY, USA: John Wiley & Sons.
9. Conrow, E.H. 2003. *Effective Risk Management: Some Keys to Success,* 2nd ed. Reston, VA, USA: American Institute of Aeronautics and Astronautics (AIAA).
10. Mun, J. 2010. *Modeling Risk,* 2nd ed. Hoboken, NJ, USA: John Wiley & Sons.
11. Eid M, Rosato V. Critical Infrastructure Disruption Scenarios Analyses via Simulation. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, SpringerOpen, 2016. 43-62.

12. Zio En. An Introduction to the Basics of Reliability and Risk Analysis, World Scientific Publishing Co.Pte.Ltd; 2006.

13. Kolowrocki K, Soszynska-Budny J. Reliability and Safety of Complex Technical Systems and Processes, Springer-Verlag London Limited. 2011.

14. Kostogryzov A., Nistratov G., Nistratov A. (2012) Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, 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

15. Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. (2013) Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes, DOI: 10.4236/ajor.2013.31A021, American Journal of Operations Research, 2013, 3, p.217-244, http://www.scirp.org/journal/ajor/

16. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G. Prediction and optimization of system quality and risks on the base of modelling processes. American Journal of Operation Researches, Special Issue, Volume 1, 2013, pp. 217-244. http://www.scirp.org/journal/ajor/

17. Andrey Kostogryzov, Andrey Nistratov, George Nistratov The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields. International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 3, September 2013, pp. 146-155. http://www.ijeit.com/archive.php

18. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности./Под ред. Махутова Н.А. – М.:МГОФ «Знание», 2015, - 936с.

19. Костогрызов А.И., Степанов П.В., Нистратов А.А., Григорьев Л.И., Червяков Л.М. Прогнозирование рисков для обеспечения качества информации в сложных системах. Системы высокой доступности №3, т.2, 2016, с. 25-37

20. V. Artemyev, A. Kostogryzov, Ju. Rudenko, O. Kurpatov, G. Nistratov, A. Nistratov, Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, December 20-22, 2017, pp. 368-373.

21. Vsevolod Kershenbaum, Leonid Grigoriev, Petr Kanygin and Andrey Nistratov / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, P. 55-79. http://dx.doi.org/10.5772/intechopen.74963

22. Kostogryzov A., Grigoriev L., Golovin S., Nistratov A., Nistratov G., Klimov S. (2018). Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI), Beijing, China. DEStech Publications, Inc., 298-303.

23. 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 // Системы высокой доступности. 2021. Т.17 №3, с. 16-31, Часть 2. Программно-технологические решения. Примеры // Системы высокой доступности. 2022. Т.18 №2, с. 42-57

24. Нистратов А.А. О математических, программно-технологических и методических решениях, ориентированных на рациональное управление рисками в системной инженерии. Сборник материалов Всероссийской научно-практической конференции «Россия в XXI веке в условиях глобальных вызовов: проблемы управления рисками и обеспечения безопасности социально-экономических и социально-политических систем и природно-техногенных комплексов», 26-27.04.2022, Президиум РАН. Под общ. ред. Проф. Я.Д. Вишнякова. – М.: Государственный университет управления. 2022. С. 251-255

25. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments. 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

26. Костогрызов А.И., Нистратов А.А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом. // Вопросы кибербезопасности. 2023, №5. С. 9-24.

27. Костогрызов А.И., Нистратов А.А. Методический подход к вероятностному прогнозированию и сравнению качества функционирования систем в условиях неопределенности // Надежность. 2024, том 24, №1. С. 10-24.

28. Нистратов, А.А. Об ожиданиях, ограничениях и прикладных возможностях стандартизованных моделей и методов прогнозирования рисков в системной инженерии / А. А. Нистратов // ИТ-Стандарт. – 2024. – № 3(40). – С. 31-51. – EDN BDXEGY

29. Костогрызов А.И., Нистратов А.А. Анализ тенденций в развитии системной инженерии // ИТ-стандарт . 2024, №3, с. 4-20

30. Сухомлин В.А., Романов В.Ю., Гапанович Д.А. Введение в модельно-ориентированную системную и программную инженерию (MBSSE). МАКС Пресс, 2024, 672с.

31. Нистратов А.А. Методика прогнозирования техногенных рисков с помощью Интернет-технологии (на примерах систем различного функционального назначения). Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.17 «Теоретические основы информатики». Защищена в Институт проблем информатики Российской академии наук (ИПИ РАН) 24.06.2013г.

References

1. Systems Engineering Handbook. A Guide for System Life Cycle Processes and Activities. Fifth Edition. 2023. INCOSE-TP-2003–002-05

2. Wiener N. Cybernetics or Control and communication in an animal and a machine. Ed.2-E. M.: Soviet radio, 1968. -326s.

3. Good G.H., Makol R.Z. System engineering: An introduction to the design of large systems. – M.: Soviet radio, 1962. – 383 p.

4. Martin J. System Analysis for Data Transmission. V. II, IBM System Research Institute. Prentice Hall, Inc., Englewood Cliffs; New Jersey. 1972

5. Kleinrock L. Queueing systems, V.2: Computer applications, John Wiley & Sons; New York. 1976

6. Boehm, B. 1989. Software Risk Management. Los Alamitos, CA; Tokyo, Japan: IEEE Computer Society Press, p. 115-125.

7. Kumamoto, H. and E. Henley. 1996. Probabilistic Risk Assessment and Management for Engineers and Scientists, 2nd ed. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers (IEEE) Press.

8. Vose, D. 2000. Quantitative Risk Analysis, 2nd ed. New York, NY, USA: John Wiley & Sons.

9. Conrow, E.H. 2003. Effective Risk Management: Some Keys to Success, 2nd ed. Reston, VA, USA: American Institute of Aeronautics and Astronautics (AIAA).

10. Mun, J. 2010. Modeling Risk, 2nd ed. Hoboken, NJ, USA: John Wiley & Sons.

11. Eid M, Rosato V. Critical Infrastructure Disruption Scenarios Analyses via Simulation. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, SpringerOpen, 2016. 43-62.

12. Zio En. An Introduction to the Basics of Reliability and Risk Analysis, World Scientific Publishing Co.Pte.Ltd; 2006.

13. Kolowrocki K, Soszynska-Budny J. Reliability and Safety of Complex Technical Systems and Processes, Springer-Verlag London Limited. 2011.

14. Kostogryzov A., Nistratov G., Nistratov A. (2012) Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, 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

15. Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. (2013) Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes, DOI: 10.4236/ajor.2013.31A021, American Journal of Operations Research, 2013, 3, p.217-244, http://www.scirp.org/journal/ajor/

16. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G. Prediction and optimization of system quality and risks on the base of modelling processes. American Journal of Operation Researches, Special Issue, Volume 1, 2013, pp. 217-244. http://www.scirp.org/journal/ajor/

17. Andrey Kostogryzov, Andrey Nistratov, George Nistratov The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields. International Journal of Engineering and Innovative Technology (IJEIT), Volume 3, Issue 3, September 2013, pp. 146-155. http://www.ijeit.com/archive.php

18. Russia's security. Legal, socio-economic, scientific and technical aspects. Scientific foundations of technogenic safety./Edited by Makhutova N.A.– Moscow: MGOF Znanie, 2015, 936s.

19. Kostogryzov A.I., Stepanov P.V., Nistratov A.A., Grigoriev L.I., Chervyakov L.M. Forecasting risks to ensure information quality in complex systems. High Availability Systems No. 3, vol.2, 2016, pp. 25-37

20. V. Artemyev, A. Kostogryzov, Ju. Rudenko, O. Kurpatov, G. Nistratov, A. Nistratov, Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, December 20-22, 2017, pp. 368-373.

21. Vsevolod Kershenbaum, Leonid Grigoriev, Petr Kanygin and Andrey Nistratov / Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, P. 55-79. http://dx.doi.org/10.5772/intechopen.74963

22. Kostogryzov A., Grigoriev L., Golovin S., Nistratov A., Nistratov G., Klimov S. (2018). Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI), Beijing, China. DEStech Publications, Inc., 298-303.

23. Nistratov A.A. Analytical forecasting of the integral risk of violation of acceptable performance of a set of standard processes in the lifecycle of high availability systems. Part 1. Mathematical models and methods // High availability systems. 2021. Vol.17 No. 3, pp. 16-31, Part 2. Software and technological solutions. Examples // High availability systems. 2022. Vol.18 No. 2, pp. 42-57

24. Nistratov A.A. On mathematical, software, technological and methodological solutions focused on rational risk management in system engineering. Collection of materials of the All-Russian Scientific and Practical Conference "Russia in the XXI century in the context of global challenges: problems of risk management and ensuring the safety of socio-economic and socio-political systems and natural and man-made complexes", 26-27.04.2022, Presidium of the Russian Academy of Sciences. Under the general editorship . Prof. Ya.D. Vishnyakova, Moscow: State University of Management. 2022. pp. 251-255

25. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments. 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

26. Kostogryzov A.I., Nistratov A.A. Threat analysis of malicious modification of the machine learning model for artificial intelligence systems. // Cybersecurity issues. 2023, No. 5. pp. 9-24.

27. Kostogryzov A.I., Nistratov A.A. Methodological approach to probabilistic forecasting and comparison of the quality of functioning of systems in conditions of uncertainty. Reliability. 2024, volume 24, No. 1. pp. 10-24.

28. Nistratov, A.A. On the expectations, limitations and application possibilities of standardized risk forecasting models and methods in system engineering / A. A. Nistratov // IT Standard. – 2024. – № 3(40). – Pp. 31-51. – EDN BDXEGY

29. Kostogryzov A.I., Nistratov A.A. Analysis of trends in the development of system engineering // IT-standard. 2024, No. 3, pp. 4-20

30. Sukhomlin V.A., Romanov V.Yu., Gapanovich D.A. Introduction to model-oriented system and software engineering (MBSE). MAKS Press, 2024, 672-31.

31. Nistratov A.A. Methodology for forecasting technogenic risks using Internet technology (using examples of systems for various functional purposes). Dissertation for the degree of Candidate of Technical Sciences in specialty 05.13.17 "Theoretical foundations of computer Science". Defended at the Institute of Computer Science Problems of the Russian Academy of Sciences (IPI RAS) on 24.06.2013.