УДК 004.9, 006.074

ПОДХОДЫ К ПРОГНОСТИЧЕСКОЙ ОБРАБОТКЕ ДАННЫХ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА. ЧАСТЬ 1. О ВОЗМОЖНОСТЯХ ВЕРОЯТНОСТНЫХ МЕТОДОВ

Костогрызов А.И., Нистратов А.А.

Федеральный исследовательский центр информатики и управления Российской академии наук, 119333, г. Москва, ул. Вавилова, 44, корп.2, тел. +7(495)795-85-24, e-mail: Akostogr@gmail.com, Andrey.nistratov@gmail.com

В части 1 рассмотрены вероятностные методы решения задач прогностической обработки данных мониторинга, способствующие эффективному использованию возможностей искусственного интеллекта (ИИ). Предлагаемый подход включает в себя вероятностные модели и методы, позволяющие прогнозировать вероятности «успеха» и/или риска неудачи для сложных объектов и систем, способы решения задачи обоснования упреждающих мер противодействия угрозам и эффективного управления рисками. Достижимые эффекты разъяснены на примере интерпретации свойств функции распределения, строящейся в моделях, и применимой в предлагаемых методах.

Ключевые слова: вероятность, метод, модель, мониторинг, риск, система, технология

APPROACHES TO PREDICTIVE DATA PROCESSING IN ARTIFICIAL INTELLIGENCE SYSTEMS. PART 1. ABOUT THE POSSIBILITIES OF PROBABILISTIC METHODS

Kostogryzov A.I., 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(495)795-85-24, e-mail: Akostogr@gmail.com, *Andrey.nistratov@gmail.com*

In Part 1 probabilistic methods for solving problems of predictive processing of monitoring data are considered. The methods help to do effective use the capabilities of artificial intelligence (AI). The approach includes probabilistic models and methods that allow predicting the probability of "success" and/or the risk of failure for complex objects and systems, ways to solve the problem of justifying proactive measures to counter threats and effective risk management. The achievable effects are explained by the example of the interpretation of the properties of probability distribution function constructed in the models and applicable in the proposed methods.

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

1 Введение

В настоящей работе, состоящей из двух частей, рассматриваются различного рода объекты и системы, включающие в свой состав системы искусственного интеллекта (ИИ). Акцент сделан на приложениях, критичных с точки зрения обеспечения безопасности в зависимости от структурной сложности объектов и систем, формальных условий неопределенностей (выражаемых временными характеристиками угроз), реализуемых методов противодействия угрозам, а также условий функционирования отдельных элементов, включая робототехнические системы. Важно заметить, что функциональное назначение объектов и систем и составных элементов явно не рассматривается, оно учитывается опосредовано - лишь на уровне временных характеристик реализуемых процессов.

Примечание. Согласно ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем» под системой понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких целей (под это определение системы подпадает опасный производственный объект, промышленное оборудование какого-либо предприятия, ситуационный центр, информационная система, робот, система мониторинга и др.).

Предлагаются подходы к решению ряда аналитических задач создания и применения эффективных систем обеспечения безопасности, связанных с прогностической обработкой данных мониторинга состояний составных элементов. Под вероятностными методами прогностической обработки данных мониторинга понимаются

методы, в результате применения которых получаются прогнозы вероятности «успешного» развития событий или риска «неудачи» и для применения которых, в качестве исходных данных выступают текущие и предыдущие данные мониторинга состояний составных элементов.

Примечание - Под риском понимается 1) мера опасности с ее последствиями (по ФЗ «О техническом регулировании», ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты», ГОСТ Р 51901.1-2002 «Менеджмент риска. Анализ риска технологических систем», ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения», ГОСТ Р МЭК 61508-4-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Термины и определения» и др.) или как более общее определение - 2) эффект неопределенности в целях и/или задачах (по ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство).

Для эффективного управления используется логический переход от частных выводов, сделанных для конкретных систем, к более общим выводам относительно сложных систем и их элементов, получаемых по результатам вероятностного моделирования случайных процессов. Предлагаемые идеи, модели, методы и технологии рассчитаны на реализацию обратной связи для решения задач обоснования требований и условий, гарантирующих непревышение задаваемых приемлемых вероятностей «успеха» и/или допустимых рисков. Как частное – рассматриваются конкретные системы и отдельные их составные элементы, функционирующие в определенных условиях. Прогностическая обработка данных мониторинга для противодействия угрозам и обеспечения эффективного управления для таких систем рассмотрена в статье на многочисленных примерах. Как общее – предлагается логический переход к сложным системам с возможностями ИИ, допускающий декомпозицию систем для решения практических задач в терминах вероятности «успеха» («отсутствия нарушений целостности») или «неудачи» («нарушений целостности») в течение прогнозного периода времени. При этом под целостностью системы понимается такое ее состояние, при котором обеспечивается достижение целей ее функционирования.

В России к важным объектам и системам, использующим возможности ИИ, в первую очередь относятся:

критически важные и потенциально опасные объекты для единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, определенных Федеральным законом от 21.12.1994г. №68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»;

опасные производственные объекты 1-го и 2-го классов опасности, определенные Федеральным законом от 21.07.1997г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов»;

объекты топливно-энергетического комплекса (ТЭК), определенные Федеральным законом от 21.11.2011г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»: объекты электроэнергетики, нефтедобывающей, нефтеперерабатывающей, нефтехимической, газовой, угольной промышленности, а также объекты нефтепродуктообеспечения, теплоснабжения и газоснабжения;

объекты критической информационной инфраструктуры, определенные Федеральным законом от 26.07.2017г. №187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации": информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, транспорта, связи, энергетики, банковской сфере, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности;

объекты оборонно-промышленного комплекса, определенные Федеральным законом от 31.12.2014г. №488-ФЗ «О промышленной политике в Российской Федерации».

Некоторые примеры объектов и систем, по которым проведены исследования и на которые могут быть распространены настоящие предложения, приведен на рис. 1, а на рис. 2 представлен пример обработки данных мониторинга оборудования предприятий опасного производства с ответной реакцией. В рамках вышеуказанных систем принимаются технические решения. Примерами критически важных систем, заинтересованных в использовании возможностей ИИ для принятия политических и социально-экономических решений, могут выступать ситуационные центры Президента РФ и его администрации, ситуационные центры Правительства РФ, отдельных министерств и ведомств, ситуационные центры глав субъектов РФ, корпораций и предприятий и др. Предлагаемый подход к прогностической обработке данных мониторинга для обеспечения эффективного управления процессами применим и к такого рода системам.

Научный взгляд на процессы возникновения и реализации разнородных угроз и системное отображении реальных и возможных событий на временную ось характеризуются частотой возникновения угроз, временем их развития и системными (или нередко на практике бессистемными) мерами и технологиями противодействия угрозам. Несмотря на то, что многочисленные предпринятые в России меры противодействия угрозам разработаны на уровне федеральных законов, федеральных норм и правил, руководств по безопасности, «ручное» управление комплексной безопасностью продолжает во многих случаях оставаться главенствующим, причем так, как это субъективно понимается на ведомственном и корпоративном уровне. Учитывая, что для многих критически важных систем потенциальные ущербы и затраты на ликвидацию последствий нарушений безопасности в условиях разнородных угроз могут на порядок превышать затраты на превентивные меры, необходим поиск эффективных решений для противодействия угрозам и обеспечения эффективного управления рисками. В свою очередь, мировые тенденции развития современных систем различного функционального назначения свидетельствуют о необходимости кардинального разворота от «ручного» управления отдельными видами безопасности, основанного на выполнении устоявшихся инструкций и на экспертных оценках складывающихся ситуаций, к реализации научно обоснованных эффективных упреждающих мер на основе

вероятностного прогнозирования. Это позволяет на основе прогностического взгляда вперед превентивно предпринимать эффективные упреждающие воздействия. Такая идея красной линией проходит через все западные концепции и последние стандарты системной инженерии. Но как это сделать – остается за кадром. В мире еще нет универсального подхода к реализации этой идеи. В поиске – все ведущие страны мира. Особые надежды при этом возлагаются на применение систем ИИ для решения актуальных практических задач.

Рисунок 1 - Некоторые примеры важных объектов и систем для приложений вероятностных методов

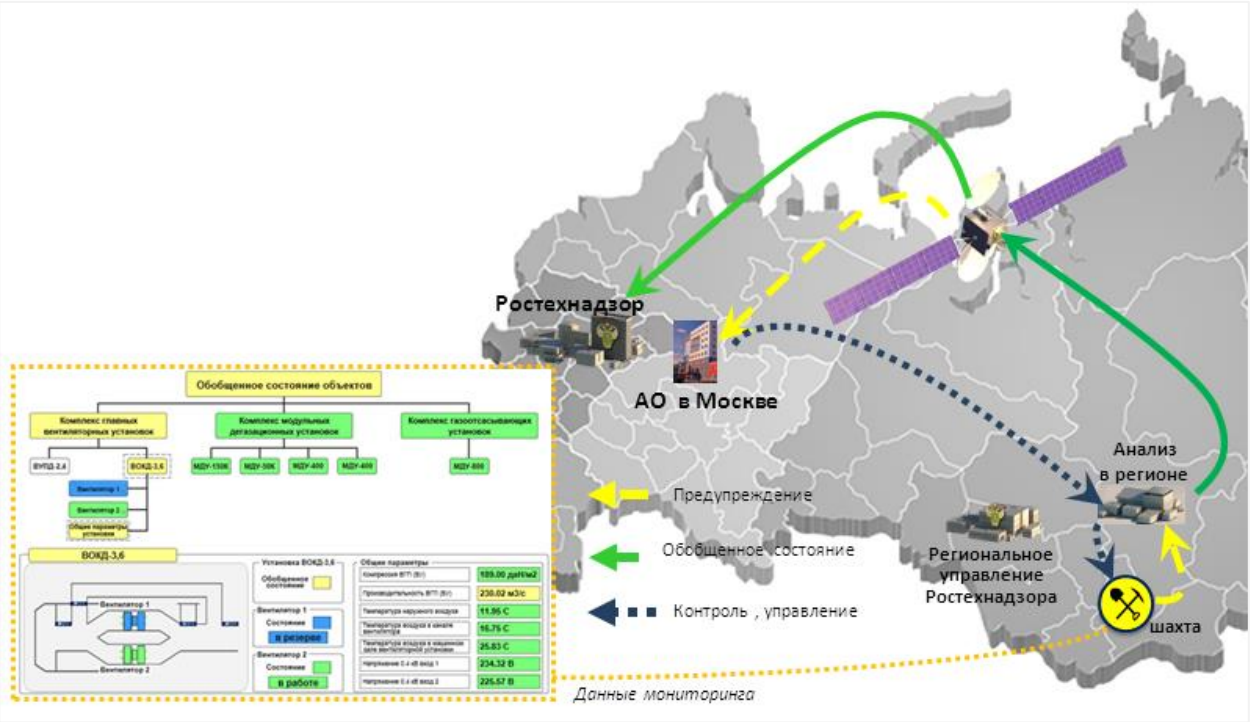


Рисунок 2 – Частный пример обработки данных мониторинга о состоянии оборудования

Если современный человеческий мозг уже обладает навыками адаптации к условиям различного рода неопределенностей окружающего мира, то системы ИИ по мере развития и расширения областей их приложения нуждаются в создании и применении всевозможных методов когнитивного решения. В настоящей работе проанализированы возможности систем ИИ для поддержки принятия решений в опасном производстве и в робототехнических системах. Для демонстрации способов построения и эффективного применения вероятностных методов из множества различных задач ИИ выбраны задачи системного планирования возможностей выполнения функций и оптимизации пути робота в пространстве.

Учитывая актуальность очерченной проблематики, в настоящей работе предлагается научно-практический подход к прогностической обработке данных мониторинга для систем ИИ. Предлагаемые вероятностные методы

развивают сложившиеся вероятностные подходы [1-17], применимые там, где имеет место некоторая похожая повторяемость событий. Их имеет смысл применять в сравнении или в комбинации, или в дополнение к существующим методам. Там, где часто требуется прогнозный анализ или где используемые подходы оказываются малоэффективными, предлагаемые методы могут быть использованы как рациональная альтернатива. В части 1 рассмотрены вероятностные методы решения задач прогностической обработки данных мониторинга, в части 2 разбираются примеры, поясняющие достижение практических эффектов.

2 Суть предлагаемого подхода к решению задач прогностической обработки данных

Мониторируемая система может сама представлять собой интересуемую систему для исследования (например, диспетчерский интеллектуальный центр) или может быть частью другой, более объемлющей интересуемой системы (например, комплексом функционально ориентированных роботов в системах безопасности). Для выполнения заданных или ожидаемых функций интересуемой системы осуществляется сбор и обработка текущей информации в реальном времени.

Предлагается осуществлять вероятностное прогнозирование развития критичных процессов во времени с тем, чтобы не только действовать согласно прогнозу, но и сравнивать прогнозы и их совпадения с последующими реалиями, накапливать и использовать эти знания. Именно в накоплении, анализе и использовании появляющихся знаний о возможной целостности системы в будущем заключается когнитивность решений задач прогностической обработки данных мониторинга.

При функционировании интересуемой системы в условиях складывающихся разнородных угроз степень приемлемости происходящих событий предлагается оценивать вероятностью «успеха» и/или «неудачи» (риском «неудачи») в течение заданного прогнозного периода времени. При этом прогнозный период времени должен задаваться таким, чтобы за это время успеть восстановить возможности, которые могут оказаться утраченными, или осуществить предстоящее действие, с которым была связана инициация решения задачи. Такое поведение означает функционирование в реальном времени. В каждом конкретном случае моделирования понятие «успеха» должно быть определено в терминах приемлемого состояния интересуемой системы для выполнения заданных или ожидаемых функций. Понятие «неудачи» означает отсутствие «успеха». В общем случае под «успешностью» функционирования интересуемой системы в течение заданного прогнозного периода времени понимается сохранение приемлемого уровня качества функционирования для выполнения заданных или ожидаемых функций (включая сохранение требуемой надежности и безопасности). Соответственно «неудача» для интересуемой системы означает наступление неприемлемого уровня качества ее функционирования в течение заданного прогнозного периода времени. Под риском «неудачи» понимается вероятностная мера «неудачи» с возможными последствиями.

Суть предлагаемого когнитивного решения задач аналитической обработки данных мониторинга, предусматривающая совершенствование, накопление, системный анализ и использование появляющихся знаний, отражена на рис. 3. При этом возможные неопределенности для заданного периода прогноза (с начальной точки t1 до момента tx в будущем) могут быть учтены с использованием излагаемых ниже подходов к моделированию, прогнозированию и оптимизации.

Рисунок 3 – Суть предлагаемого когнитивного решения задач

Аналитическое прогнозирование рисков предлагается осуществлять на основе вероятностного моделирования систем. Для практического применения рекомендуются методы и модели [1-10, 14-17] (далеко не исчерпывающие список адекватных моделей), где субъективные весовые коэффициенты исключены. Последнее – важно, т.к. продолжают широко применяться методы, базирующиеся на экспертных оценках, в т.ч. с использованием различного рода субъективно назначаемых коэффициентов. Экспертные коэффициенты еще как-то воспринималось на заре системного анализа, но сегодня их искусственное назначение является тормозом в современной науке, поскольку «эксперты» бывают разные. Человек в состоянии обозреть единицы-десятки элементов с отслеживаемыми параметрами, но не сотни-тысячи и более в их многочисленных взаимосвязях. Из-за субъективизма возможны «подгонки» под любые пожелания, ожидания и нормативы, не привязанные к конкретным методам.

Предлагаемые модели базируются на классически построенном вероятностном пространстве (Ω, B, P), где Ω – конечное пространство элементарных событий; B – класс всех подмножеств множества Ω, удовлетворяющий свойствам сигма-алгебры; P – вероятностная мера на пространстве элементарных событий. При этом, поскольку $\Omega=\{\omega k\}$ – конечное, в моделях установлено отображение $\omega k \rightarrow pk = P(\omega k)$ такое, что $pk \geq 0$ и $\sum_k p_k = 1$.

Уровень прогнозируемого качества функционирования системы предлагается оценивать вероятностью «успеха» (или «отсутствия нарушений целостности»), а прогнозируемой безопасности – вероятностью «неудачи» (или «нарушения целостности») в течение заданного периода времени для составных компонентов и системы в целом в условиях разнородных угроз. При идентичных последствиях вероятность «неудачи» характеризует риск «неудачи». Само понятие приемлемого уровня целостности (в т.ч. «успешности») должно быть определено в терминах штатного состояния системы или составных элементов. Сложная система декомпозируется до составных элементов для решения проблем применительно к каждому из элементов и подсистем и их сворачивания в систему в целом – см. рис. 4.

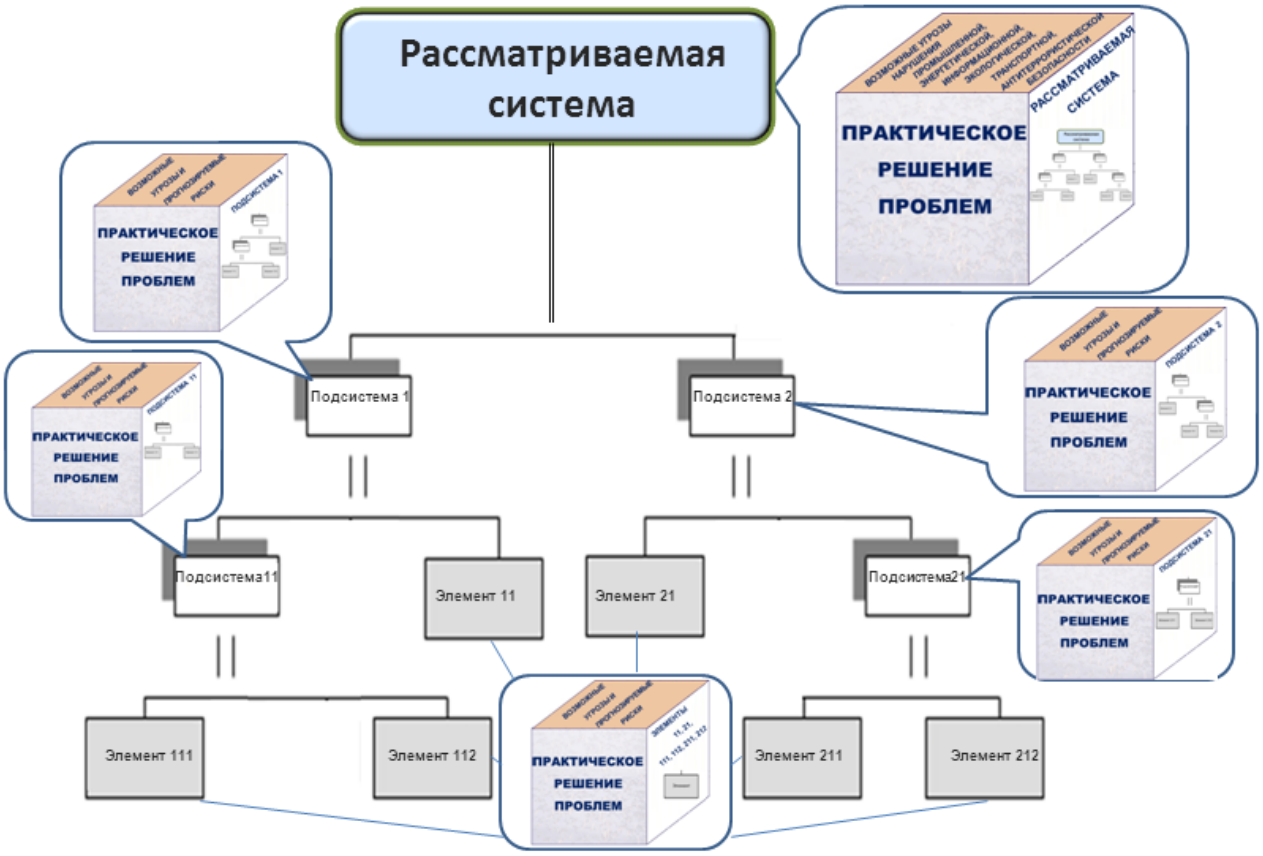


Рисунок 4 - Декомпозиция сложной системы до элементов для решения возникающих проблем

Каждый из элементов представляется в виде «черного ящика», и для него могут быть применены различные вероятностные модели для расчетов и построения искомой функции распределения (ФР) времени между соседними нарушениями целостности, учитывающие разнородные угрозы, предпринимаемые меры контроля, мониторинга и восстановления целостности. Научный взгляд на процессы реализации разнородных угроз и системное отображении событий на временную ось характеризуются частотой возникновения угроз, временем их развития и системными или бессистемными мерами и технологиями противодействия угрозам. В случайных событиях присутствуют скрытые закономерности. Современный уровень развития теории

вероятностей и теории случайных процессов независимо от природы разнородных угроз способен сформировать теоретическую и практическую базу прогнозирования целостности систем во времени (в т.ч. прогнозирования риска нарушения качества функционирования) и решения связанных с этим задач выработки и обоснования эффективных упреждающих мер. Фокусирование внимания именно на процессах позволяет использовать для их описания лишь характеристики времени (среднего времени или частоты наступления событий), безразмерные или стоимостные характеристики, свойственные для объектов и систем различных приложений. Степень достижения ожидаемых результатов оценивается вероятностными показателями (например, с помощью вероятности безотказного функционирования, риска отказа или риска нарушения безопасности в течение заданного времени), рассчитываемыми с использованием применимых вероятностных моделей.

Примером может служить авторский подход к прогностическому моделированию процессов, доведенный до реализации на уровне типовых требований системной инженерии (см. ГОСТ Р 59329 – ГОСТ Р 59357), а также в ГОСТ Р 58494-2019 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов». В частности, в ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы» предложенный подход основан на выделении и формулировании общей цели функционирования информационных систем различного назначения, а именно – обеспечение надежного и своевременного представления полной, достоверной и конфиденциальной информации для последующего использования – см. рис. 5.

Рисунок 5 - Абстрактная иллюстрация качества функционирования информационных систем

В общем случае анализ заключается во взаимоувязанной оценке показателей надежности и своевременности представления, полноты, достоверности и конфиденциальности используемой информации. С точки зрения математической формализации реализуемые процессы сбора, обработки и защиты информации вполне однотипны. В совокупности со сформулированной целью этого оказалось достаточным для формирования унифицированных системных требований и выбора сравнительно общих вероятностных показателей качества функционирования.

Этот подход применим к каждому элементу сложной структуры, формализуемому как «черный ящик», для решения вопросов оценки и обеспечения качества и рисков применительно к элементам системы, реализующим функции сбора, обработки и обеспечения безопасности информации.

Ниже приводятся обобщенные модели «черного ящика», которые предлагаются для прогнозирования рисков нарушения целостности отдельных элементов системы.

3 Предлагаемые модели для перехода от частного к общему

3.1 Математическая модель для прогноза риска нарушения целостности системы при реализации технологии профилактической диагностики

Суть модели в следующем. Предполагается изначальная целостность системы (в качестве моделируемой системы может также рассматриваться отдельный ее элемент, т.е. в этом случае система – это «черный ящик»). В процессе функционирования в результате реализации возможных угроз (природных, технических, технологических, со стороны «человеческого фактора» и др.) могут начать развиваться процессы, приводящие к нарушению целостности системы. Начало (инициирование) каждого из таких процессов служит источником потенциальной опасности для обеспечения целостности. В системе осуществляется периодический контроль целостности. Из-за различных природных, технических, технологических причин, различного уровня квалификации специалистов, привлекаемых для контроля, недостатка, неготовности или нечувствительности измерительного оборудования, неэффективных мер поддержания или восстановления штатного режима функционирования системы и пр. целостность системы может быть нарушена.

Примечание. В приложении к каждой системе (и ее критичных элементов) понятие и показатели обеспечения и нарушения целостности должны быть конкретизированы на уровне правил, инструкций по эксплуатации, обязанностей должностных лиц.

В рамках модели развитие критичных ситуаций в системе считается не нарушающим целостности в течение заданного прогнозного периода времени, если к началу периода нарушение целостности отсутствует и в течение всего периода либо источники опасности не инициируются, либо после инициации происходит их оперативное выявление и принятие адекватных мер противодействия. Предполагается, что существуют не только средства диагностики (контроля) целостности, но и способы поддержания и/или восстановления необходимой целостности системы при выявлении источников опасности или следов их инициации. Восстановление осуществляется лишь в период системного контроля.

За основу анализа принят следующий поэтапный алгоритм возникновения и реализации опасности: сначала источник опасности появляется и начинает инициироваться, а по прошествии свойственного ему периода инициации опасность разрастается до угрожающих размеров, приводящих к нарушению целостности системы. Если опасность постоянна (например, для опасного производства), выделяются приемлемый нормативный диапазон, который не должен нарушаться для показателей, характеризующих уровень опасности. Целостность считается нарушенной лишь после того, как инициировавшийся источник приводит к нарушению штатного режима функционирования системы (например, установленных пределов нормативного диапазона). Если инициировавшийся источник опасности был выявлен до наступления нештатной ситуации и приняты адекватные контрмеры, считается, что целостность системы не нарушена. Результатом применения очередной диагностики является полное восстановление нарушенной целостности системы до приемлемого уровня или подтверждение целостности при отсутствии ее нарушения.

Модель позволяет оценить вероятность нарушения целостности системы в течение заданного периода времени. Именно эта вероятность определяется как риск нарушения целостности (как для системы в целом, так и для составных подсистем и элементов) в течение заданного периода прогноза с учетом предпринимаемых мер периодического контроля и восстановления целостности, а также возможных последствий от нарушений.

Достижение приемлемого уровня риска нарушения целостности системы является следствием достаточно частого диагностирования и применения эффективных средств диагностики, контроля и восстановления целостности при существующих ограничениях.

Примечание. Существование средств гарантированного выявления источников опасности или следов их воздействия и существование способов поддержания нарушенной целостности системы являются необходимыми условиями. Их эффективность может быть оценена на основе математического моделирования или натурных испытаний в условиях типовых сценариев развития угроз.

Некоторые из моделируемых случаев соотношения между периодами диагностики, временем до начала инициации источников опасности и непосредственно их развития до размеров, угрожающих целостности, приведены на рис. 6.

Рисунок 6 - Формальные случаи сохранения и нарушения целостности

Для описания процессов возникновения и выявления опасных воздействий на объект введены обозначения:

σ – частота возникновения источника опасности;

β – среднее время инициации с разрастанием опасности до угроз, приводящих к нарушению целостности системы (например, до нарушения установленных нормативов);

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

Тдиаг– длительность диагностики, включая восстановление целостности системы;

Тзад– длительность прогнозного периода времени.

Оценка риска нарушения целостности системы $R_{наруш.}$ в течение прогнозного периода Тзад с учетом возможных ущербов осуществляется по формуле:

$$R_{наруш.} = 1 - P_{возд.}, \quad (1)$$

где $P_{возд.}$ – это вероятность отсутствия нарушений целостности в течение периода Тзад.

Возможны два варианта:

- вариант 1 – заданный оцениваемый период Тзад меньше периода между окончаниями соседних диагностик (Тзад<Тмеж+ Тдиаг);
- вариант 2 - заданный оцениваемый период Тзад больше или равен периоду между окончаниями соседних диагностик (Тзад≥Тмеж+ Тдиаг), т.е. за это время заведомо произойдет одна или более диагностик.

Для варианта 1 при условии независимости исходных характеристик вероятность $P_{возд}(1)$(σ, β, Тмеж, Тдиаг, Тзад) отсутствия нарушений целостности в течение периода Тзад. вычисляют по формуле (как распределение от суммы времен возникновения и инициации опасности на момент завершения периода прогноза Тзад – см. рис. 6):

$$P_{возд(1)} = \begin{cases} \left(\sigma - \beta^{-1}\right)^{-1}\left\{\sigma e^{-T_{зад}/\beta} - \beta^{-1} e^{-\sigma T_{зад}}\right\}, если\ \ \sigma \neq \beta^{-1}, \\ e^{-\sigma T_{зад}}\left[1 + \sigma T_{зад}\right], если\ \ \sigma = \beta^{-1}. \end{cases} \quad (2)$$

Примечание - Эту же формулу используют для оценки вероятности отсутствия нарушений целостности без какой-либо диагностики в предположении, что к началу Тзад целостность системы обеспечена.

Для варианта 2 при условии независимости исходных характеристик для расчетов возможны различные вероятностные меры.

Так, согласно первой мере вероятность отсутствия нарушений целостности в течение периода Тзад. может быть вычислена по формуле:

$$P_{возд(2)} = P_{серед} + P_{кон}, \quad (3)$$

где $P_{серед}$ – вероятность отсутствия нарушений целостности в течение всех периодов между диагностиками, целиком вошедшими в Тзад. С учетом доли этих периодов $\frac{N\left(T_{меж} + T_{диаг}\right)}{T_{зад}}$ в общем оцениваемом периоде Тзад, расчет осуществляют по формуле

$$P_{серед} = \frac{N\left(T_{меж} + T_{диаг}\right)}{T_{зад}} \cdot P^{N}_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж} + T_{диаг}), \quad (4)$$

N – число периодов между диагностиками, которые целиком вошли в пределы времени Тзад, с округлением до целого числа, N=[Тзад/(Тмеж+ Тдиаг)] - целая часть.;

$P_{возд}(1)$(σ, β, Тмеж, Тдиаг, Тмеж+Тдиаг) – вероятность отсутствия нарушений целостности за один период между диагностиками, целиком вошедший в пределы времени Тзад, вычисляют по формуле (2);

$P_{кон}$ – вероятность отсутствия нарушений целостности после последней диагностики (в конце Тзад). С учетом доли остатка Тост=Тзад - N(Тмеж+Тдиаг) в общем прогнозном периоде Тзад расчет осуществляют по формуле

$$P_{кон} = \frac{T_{ост}}{T_{зад}} \cdot P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{ост}); \quad (5)$$

Значение $P_{возд(1)}$(σ, β, Тмеж, Тдиаг, Тост) для остатка от задаваемого прогнозного периода вычисляют по формуле (2) с тем отличием, что вместо Тзад стоит Тост.

Выражение (3) логически объясняется так: нарушения, если они появляются, могут наблюдаться либо на «серединном» участке заданного прогнозного периода Тзад (нормированный вес этого участка равен N(Тмеж+Тдиаг)/Тзад), либо на «конечном» участке после последней диагностики целостности (нормированный вес этого участка равен Тост/Тзад). При этом на обоих участках должно наблюдаться отсутствие нарушений целостности, что оценивается выражениями (4) и (5). Достоинство этой меры в том, что при целом N возможно оценить отклонения расчетной вероятности за счет более частого контроля и восстановления целостности, а при нецелом N (равном Тзад/(Тмеж+ Тдиаг)) получаемые зависимости от Тзад в полной мере характеризуют функцию распределения наработки на нарушение целостности для выбранной вероятностной меры.

Другая возможная вероятностная мера для оценки вероятности отсутствия нарушений целостности в течение периода Тзад. может быть вычислена по формуле:

$$P_{возд\ (2)} = P_{серед} \cdot P_{кон}, \quad (6)$$

где вероятность отсутствия нарушений целостности в течение всех периодов между диагностиками Рсеред, целиком вошедшими в Тзад , вычисляется по формуле

$$P_{\text{серед}} = P^{N}_{\text{возд (1)}}\left(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{меж}} + T_{\text{диаг}}\right), \quad (7)\ (E.31)$$

а вероятность отсутствия нарушений целостности Ркон после последней диагностики (в конце Тзад) равна

$$P_{\text{кон}} = P_{\text{возд (1)}}\left(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{ост}}\right). \quad (8)$$

Выражение (6) логически объясняется так: для отсутствия нарушений целостности за весь период прогноза требуется отсутствие нарушений целостности на каждом из участков – будь то середина или конец периода прогноза Тзад. Достоинство этой меры в том, что при целом N сразу получается классическая функция распределения наработки на нарушение целостности для выбранной вероятностной меры. Однако, в отличие от меры (3) отклонения расчетной вероятности за счет более частого контроля и восстановления целостности практически трудноразличимы, что способствует сокрытию эффективности этих мер противодействия в управлении рисками для аналитика.

Таким образом, вероятность отсутствия нарушений целостности в течение периода Тзад. определяется аналитическими выражениями (2), (3) или (6) в зависимости от варианта соотношений между исходными данными и выбранной вероятностной меры. Это позволяет вычислить по формуле (1) искомый риск нарушения целостности системы *Rнаруш.* в течение заданного периода прогноза Тзад с учетом предпринимаемых технологических мер периодического системного контроля и восстановления целостности и возможных последствий.

3.2 Математическая модель для прогноза риска нарушения целостности системы при реализации технологии мониторинга

Технология мониторинга целостности является более общим случаем по сравнению с технологией профилактической диагностики. Она характеризуется тем, что между системными контролями целостности, осуществляемыми периодически, реализуется непрерывный мониторинг состояния системы силами каких-либо операторов (в качестве таковых могут выступать автоматические сканеры, человек за экраном монитора, на котором фиксируются показания датчиков и др.). В идеале это позволяет сразу же при обнаружении угрозы (возникновения источника опасности) приступать к восстановлению целостности системы. В моменты системного контроля также происходит восстановление функциональных возможностей системы и операторов - например, путем штатной смены человека-оператора или подтверждением работоспособности датчиков и пр. Однако, операторам, в т.ч. автоматам, тоже свойственные ошибки, безошибочность их действий характеризуется временем наработки на ошибку, что является аналогом наработки на отказ.

Примечание. В приложении к каждой системе (и ее критичным элементам) понятия и показатели обеспечения и нарушения целостности, ошибки оператора-человека должны быть конкретизированы на уровне правил распознавания ситуаций при мониторинге и контроле, инструкций по эксплуатации, обязанностей должностных лиц.

За основу анализа принят следующий поэтапный алгоритм возникновения опасности: сначала источник опасности появляется и начинает инициироваться, а по прошествии свойственного ему периода инициации опасность разрастается до угрожающих размеров, способных привести к нарушению целостности системы. Целостность считается нарушенной лишь после того, как инициировавшийся источник приводит к нештатной ситуации (т.е. к нарушению штатного режима функционирования системы). Если инициировавшийся источник опасности был выявлен до наступления нештатной ситуации и приняты адекватные контрмеры восстановления, считается, что целостность системы не нарушена. Результатом применения очередной диагностики является полное восстановление нарушенной целостности системы до приемлемого уровня или подтверждение целостности при отсутствии ее нарушения. Кроме того, между диагностиками реализуется мониторинг состояний системы (аналог того, если диагностика осуществляется через короткие промежутки времени, стремящиеся к 0). Формально с учетом этих дополнительных мер целостность системы может быть нарушена лишь в случае, если наработка на отказ средств мониторинга окажется меньше, нежели период между диагностиками и именно в это оставшееся до следующей диагностики время произойдет инициация проникших источников опасности. Тем самым в рамках модели учитываются возможности к сканированию ситуаций, оперативному выявлению потенциальных опасностей и восстановлению нарушаемой целостности – см. рис. 7.

Модель позволяет оценить вероятность нарушения целостности системы в течение заданного периода времени. Именно эта вероятность с учетом последствий определяется как риск нарушения целостности системы в течение заданного периода прогноза с учетом предпринимаемых технологических мер периодического контроля, мониторинга и оперативного восстановления целостности. За основу берется аналогичная модель, разработанная и исследованная ранее (см., например, в [1, 4, 6]).

С учетом возможных последствий оценка риска нарушения целостности системы *Rнаруш.* в течение прогнозного периода Тзад осуществляется по формуле (1).

Возможны те же два варианта, что и выше:

вариант 1 – заданный оцениваемый период Тзад меньше периода между окончаниями соседних диагностик (Тзад<Тмеж+ Тдиаг);

вариант 2 - заданный оцениваемый период Тзад больше или равен периоду между окончаниями соседних диагностик (Тзад≥Тмеж+ Тдиаг), т.е. за это время заведомо произойдет одна или более диагностик.

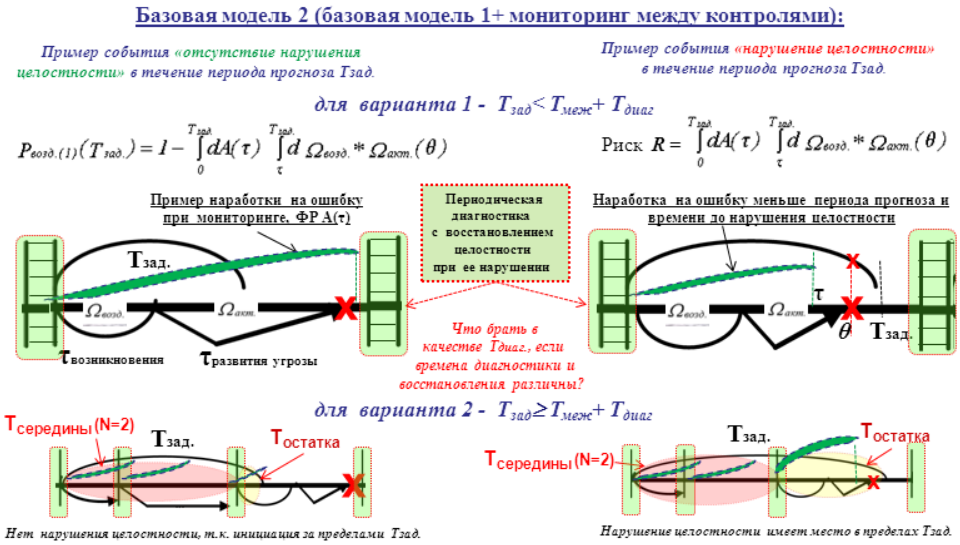


Рисунок 7 - Формальные случаи сохранения и нарушения целостности

Для варианта 1 при условии независимости исходных характеристик вероятность Рвозд(1)(σ, β, Тмеж, Тдиаг, Тнар, Тзад) отсутствия нарушений целостности в течение периода Тзад. вычисляют по формуле:

$$P_{возд.(1)}(T_{зад.}) = 1 - \int_0^{T_{зад.}} dA(\tau) \int_0^{T_{зад.}-\tau} d\,\Omega_{возд.} * \Omega_{акт.}(\theta). \qquad (9)$$

где * – знак свертки;

Ωвозд.(t) – функция распределения (ФР) времени между возникновениями источника опасности, в инструментариях *Ωвозд.(t)=1-exp(-σt), σ* – частота возникновения источника опасности;

Ωакт.(t) – ФР времени инициации источника опасности до угрожающих размеров, приводящих к нарушению целостности системы, в инструментариях Ωакт.(t) =1-exp(-t/β), β – среднее время инициации;

A(t) – ФР времени наработки оператора на ошибку, в инструментариях

A(t)=1-e-t/Тнар, Тнар. – среднее.

Выражение для вероятности нарушения целостности $\int_0^{T_{зад.}} dA(\tau) \int_\tau^{T_{зад.}} d\,\Omega_{возд.} * \Omega_{акт.}(\theta)$ читается так: нарушение происходит тогда, когда инициация опасности происходит в момент θ, который наступает на полусегменте (τ, Тзад.], а в свою очередь, первая ошибка оператора произойдет в момент τ, который также наступит раньше истечения периода прогноза Тзад.

Для варианта 2 при условии независимости исходных характеристик также, как и для модели подраздела 3.1, для расчетов возможны различные вероятностные меры.

Согласно первой мере вероятность отсутствия нарушений целостности в течение периода Тзад. может быть вычислена по формуле (3), где Рсеред – вероятность отсутствия нарушений целостности в течение всех периодов между диагностиками, целиком вошедшими в Тзад. С учетом доли этих периодов $\frac{N(T_{меж}+T_{диаг})}{T_{зад}}$ в общем оцениваемом периоде Тзад, расчет осуществляют по формуле

$$P_{возд.(2)}(T_{зад.}) = \frac{N(T_{меж.}+T_{диаг.})}{T_{зад.}} \cdot P^{N}_{возд.(1)}(T_{меж.}+T_{диаг.}) + \frac{T_{ост.}}{T_{зад.}} P_{возд.(1)}(T_{ост.}), \qquad (10)$$

где *N*=[*Тзад./(Тмеж.+ Тдиаг.)*] – целая часть, *Тост. = Тзад. – N(Тмеж.+ Тдиаг.).*

Доказательство – аналогично модели 3.1.

Замечание. Для первого периода Рнач. =

Другая возможная вероятностная мера для оценки вероятности отсутствия нарушений целостности в течение периода Тзад. может быть вычислена по формуле (6), где

вероятность отсутствия нарушений целостности в течение всех периодов между диагно-стиками Рсеред, целиком вошедшими в Тзад, вычисляется по формуле, аналогичной (7), а вероятность отсутствия нарушений целостности Ркон после последней диагностики (в конце Тзад) – по формуле, аналогичной (8), но здесь Рвозд.(1) вычисляется уже по формуле (9), т.е.

$$P_{возд.(2)}(T_{зад.}) = P^{N}_{возд.(1)}(T_{меж.}+T_{диаг.}) \cdot P_{возд.(1)}(T_{ост.}),$$

где *N*=[*Тзад./(Тмеж.+ Тдиаг.)*] - целая часть, *Тост. = Тзад. - N(Тмеж.+ Тдиаг.).*

Таким образом, вероятность отсутствия нарушений целостности в течение периода Тзад. определяется аналитическими выражениями (9) и (6) в зависимости от варианта соотношений между исходными данными. Это

позволяет вычислить по формуле (4) искомый риск нарушения целостности системы *Rнаруш.* в течение заданного периода прогноза Тзад с учетом предпринимаемых технологических мер контроля, мониторинга и восстановления целостности.

Если в моделях подразделов 3.1 и 3.2 построить зависимость функции Рнаруш. (Тзад) в точках расчета, когда Тзад. пробегает значения от 0 до бесконечности (с заданной точностью), то эта зависимость будет характеризовать ФР времени нарушения целостности. Известный вид этой ФР, построенной по точкам, позволяет традиционными методами математической статистики определить среднюю наработку до нарушения целостности.

Точность моделей может быть повышена с помощью учета различий во времени диагностики и восстановления целостности составных элементов, что также рекомендовано этим стандартом.

3.3 Метод повышения адекватности моделей

Этот метод в дополнение к возможностям моделей подразделов 3.1 и 3.2 позволяет повысить адекватность моделирования за счет дополнительного учета времени на восстановление после нарушения целостности. В моделях 3.1 и 3.2 время системного контроля по составному элементу одинаково и равно в среднем Tдиаг.. Вместе с тем, если по результатам контроля требуются дополнительные меры восстановления нарушенной целостности в течение времени Tвосст , то для расчетов усредненное время контроля Tдиаг должно быть увеличено. При этом усредненное время контроля вычисляется итеративно с заданной точностью:

1-я итерация определяет $T_{\text{диаг}}^{(1)} = T_{\text{диаг}}$, задаваемое на входе модели. Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление нарушаемой целостности;

2-я итерация осуществляется после расчета риска $R_{\text{неконтр}}^{(1)}$ по исходным данным после 1-й итерации

$$T_{\text{диаг}}^{(2)} = T_{\text{диаг}}^{(1)} \cdot \left(1 - R_{\text{неконтр}}^{(1)}\right) + R_{\text{неконтр}}^{(1)} \cdot T_{\text{восст}},$$

где $R_{\text{неконтр}}^{(1)}$ – риск нарушения целостности с исходным значением $T_{\text{диаг}}^{(1)}$, вычисляемый с использованием соответствующих моделей 3.1 или 3.2. Здесь, поскольку на 1-й итерации $T_{\text{диаг}}^{(1)}$ не учитывает времени восстановления, риск $R_{\text{неконтр}}^{(1)}$, рассчитываемый с использованием моделей 3.1, 3.2, ожидается оптимистичным (т.е. меньше реального),

… r-я итерация осуществляется после расчета риска $R_{\text{неконтр}}^{(r-1)}$ по исходным данным после $(r-1)$-й итерации:

$$T_{\text{диаг}}^{(r)} = T_{\text{диаг}}^{(r-1)} \cdot \left(1 - R_{\text{неконтр}}^{(r-1)}\right) + R_{\text{неконтр}}^{(r-1)} \cdot T_{\text{восст}},$$

где $R_{\text{неконтр}}^{(r-1)}$ вычисляется по-прежнему по моделям 3.1, 3.2, но уже в качестве исходного выступает $T_{\text{диаг}}^{(r-1)}$, рассчитанное на предыдущем шаге итерации. Здесь уже в большей степени учитывается время восстановления с частотой, стремящейся к реальной. Соответственно риск $R_{\text{неконтр}}^{(r-1)}$ также приближается к реальному.

С увеличением r указанная последовательность $T_{\text{диаг}}^{(r)}$ сходится, и для дальнейших расчетов используют значение, отличающееся от точного предела $T_{\text{диаг}}^{(\infty)}$ на величину, пренебрежимо малую с задаваемой изначально точностью итерации ε :

$$\left|R_{\text{неконтр}}^{(r)} - R_{\text{неконтр}}^{(r-1)}\right| \leq \varepsilon.$$

Примечание ─ Способ итеративного применения процессов рекомендован ГОСТ Р 57102-2016, ГОСТ Р 58494-2016.

Таким образом, предложенные выше модели позволяют построить более адекватные ФР времени нарушения целостности отдельного элемента за счет дополнительного учета возможностей периодического системного контроля, мониторинга состояний и восстановления целостности. Что это позволяет для прогностической обработки данных?

4 Какие скрытые знания могут быть извлечены из более адекватной функции распределения?

На рис. 8 проиллюстрированы ограничения к допустимым рискам, экспоненциальная и некая более адекватная ФР времени между соседними нарушениями системной целостности с одинаковой частотой нарушений λ.

Ориентируясь на простейшую аппроксимацию экспоненциальной ФР (с одним параметром), можно легко констатировать выполнение или невыполнение задаваемых требований к уровню допустимых рисков. Ниже «пограничной полосы» - требование выполнено, выше – не выполнено! И это – все извлекаемые знания… Из «плюсов» - лишь удобство сравнения. И все…

Ориентируясь на более адекватную ФР (например – с помощью моделей 3.1 и 3.2), если при ее создании для каждого критичного составного элемента задавались характеристики угроз и предпринимаемые меры противодействия угрозам, возможно извлечение следующих знаний - см. рис. 8:

- рассчитать реальную зависимость вероятности нарушения целостности системы и составных подсистем от характеристик разнородных угроз и предпринимаемых мер противодействия угрозам;

- оценить точность прогнозирования по сравнению с экспоненциальной аппроксимацией ФР;

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

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

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

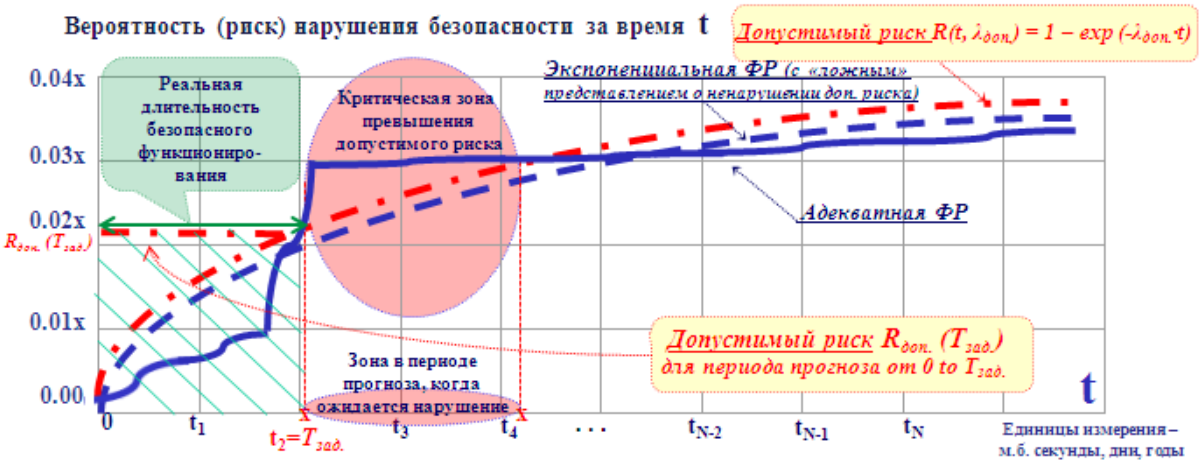


Рисунок 8 - Фрагменты ФР, демонстрирующие возможные варианты зависимостей ограничений на допустимый риск, экспоненциальную и более адекватную аппроксимацию ФР

Кроме того, построив более адекватную ФР, возможно обычными расчетными методами извлечь дополнительные знания - см, например, [6-17]:

- рассчитать среднюю наработку на нарушение и, как обратную к ней величину - частоту нарушений целостности системы и составных подсистем в условиях задаваемых разнородных угроз и предпринимаемых мер противодействия угрозам;

- сравнить среднюю наработку на нарушение целостности или частоту нарушений целостности системы (и подсистем) со средней наработкой или частотой нарушений целостности при экспоненциальной аппроксимации ФР.

Кроме этого, зафиксировав уровни «допустимых рисков» для системы и составных подсистем, а также считая неизменными все параметры, за исключением одного, возможно решение различные оптимизационных задач, связанных с обоснованием эффективных упреждающих мер обеспечения целостности системы в условиях разнородных угроз. Классическими задачами являются максимизация эффекта (выгоды, уровня качества или безопасности и др.) или минимум рисков при ограничениях или минимизация затрат при ограничениях на допустимые риски и иных ограничениях.

5 Интеграция для сложных структур, комбинация и генерации новых моделей

Предложенные в подразделах 3.1 – 3.3 модели пригодны для проведения автономных оценок системы, представимой в виде отдельного «черного ящика» (причем для случая, когда времена диагностики и восстановления нарушенной целостности совпадают). Для комплексной оценки требуется развитие моделей. При комбинации моделей потенциально оказывается возможным расчет показателей рисков в условиях угроз возможного возникновения и развития нештатных ситуаций с учетом предпринимаемых технологических мер контроля, мониторинга и восстановления целостности (как системы в целом, так и составных подсистем).

Важно определить способы корректного сворачивания расчетных показателей к интегральному виду. Определение таких возможностей позволило бы без расширения множества требуемых для расчетов исходных данных использовать принципы целенаправленности, стандартизации, унификации и модульности в оценке защищенности отдельного элемента и совокупности элементов.

Основные идеи интеграции, комбинации и генерации новых моделей для аналитического прогнозирования рисков заключаются в следующем.

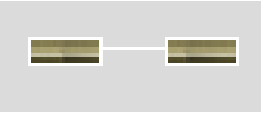
1-я идея. Поскольку модели математические, то путем смыслового переобозначения исходных данных и, соответственно, расчетных показателей возможно использование одних и тех же моделей для оценки разных показателей. Идея упомянута лишь для понимания дальнейшей логики в построении моделей.

2-я идея. Для комплексной оценки в приложении к системам сколь угодно сложной параллельно-последовательной структуры предлагается использовать следующий алгоритм генерации новых моделей.

Сложность системы оценивается количеством составных элементов. Для этого надо знать наработку на нарушение целостности каждого из элементов. С учетом идеи 1 далее достаточно логического переопределения понятия наработки (например, для анализа надежности это – наработка на отказ, а для безопасности – наработка на нарушение целостности).

Примечание. В качестве логических элементов могут выступать отдельные составные элементы системы, системы или отдельные объекты или совокупности объектов.

Рассмотрим простейшую структуру из двух независимых элементов, соединенных последовательно, что означает логическое соединение «И» (рис. 9), или параллельно, что означает логическое соединение «ИЛИ» (рис. 10). Предположение независимости имеет место быть.



ФР времени наработки на нарушение целостности B(t) =1–[1-B1(t)][1- B2(t)]

Рисунок 9 - Система из последовательно соединенных элементов

ФР времени наработки на нарушение целостности B(t) = B1(t)B2(t)

Рисунок 10 - Система из параллельно соединенных элементов

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

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

$$B(t) = P(\min(\tau 1, \tau 2) \le t)=1- P(\min(\tau 1, \tau 2) > t)=1-P(\tau 1 > t)P(\tau 2 > t)= 1 - [1-B1(t)]\,[1- B2(t)], \quad (11)$$

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

$$B(t) = P(\max(\tau 1, \tau 2) \le t)= P(\tau 1 \le t)\, P(\tau 2 \le t)= B1(t)\, B2(t). \quad (12)$$

Применяя приведенные рекуррентные соотношения (11) – (12), можно получать соответствующие оценки для сколь угодно сложной логической структуры с параллельно-последовательным соединением элементов.
Именно эти соотношения реализуются в инструментариях, поддерживающем модели - см. [11-13].

3-я идея. На выходе моделирования системы – вероятность сохранения целостности в течение заданного периода времени. Если для каждого элемента просчитать эту вероятность для всех точек Тзад. от нуля до бесконечности, то получится траектория ФР времени сохранения целостности по каждому из элементов в зависимости от реализуемых мер контроля, мониторинга и восстановления целостности. В свою очередь, известный вид этой ФР, построенной по точкам с использованием программных комплексов, позволяет традиционными методами математической статистики определить среднее время сохранения целостности каждого из элементов системы. А это – необходимые исходные данные для применения других моделей и, соответственно, оценки показателей функционирования системы параллельно-последовательной структуры любой степени сложности.

4-я идея. Возможно поддержание и/или восстановление целостности по одному или нескольким элементам. При этом расчет среднего времени восстановления группы из двух элементов осуществляется:
для последовательно соединенных элементов - см. рис. 9:

$$Твосст = Твосст1((1/Тнар1)/(1/Тнар1+Тнар2))+Твосст2((1/Тнар2)/(1/Тнар1+1/Тнар2)); \quad (13)$$

для параллельно соединенных элементов - см. рис. 10:

$$Твосст = Твосст1((1/Тнар2)/(1/Тнар1+1/Тнар2))+Твосст2\ ((1/Тнар1)/(1/Тнар1+1/Тнар2)). \quad (14)$$

Рекуррентное применение формул (13) – (14) позволяет вычислить среднее время восстановление целостности за всю систему, состоящую из множества элементов.

5-я идея. Время диагностики по составному элементу или группе элементов каждый раз приблизительно одинаково и равно в среднем Тдиагн.. Вместе с тем, если по результатам диагностики требуются дополнительные

меры восстановления нарушенной целостности, то это время увеличивается. При этом усредненное время диагностики может быть вычислено итеративно с заданной точностью, а именно:

1-я итерация:

Тдиагн. (1) = Тдиагн., задаваемое на входе модели. Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление целостности.

2-я итерация осуществляется после расчета риска Rнеконтр.(1) по исходным данным после 1-й итерации:

Тдиагн. (2) = Тдиагн. (1) (1 – Rнеконтр.(1)) + Rнеконтр.(1) Твосст ,

где Rнеконтр.(1) – риск нарушения целостности с исходным значением Тдиагн. (1). Здесь, поскольку на 1-й итерации Тдиагн. (1) не учитывает времени восстановления, то риск Rнеконтр.(1) , рассчитываемый с использованием моделей, предлагаемых в подразделах 3.1 – 3.2, ожидается оптимистичным, т.е. меньше реального.

…

n-я итерация осуществляется после расчета риска Rнеконтр.(n-1) по исходным данным после (n-1)-й итерации:

Тдиагн. (n) = Тдиагн. (n-1) (1 – Rнеконтр.(n-1)) + Rнеконтр.(n-1) Твосст , (15)

где Rнеконтр.(n-1) вычисляется по-прежнему по моделям подразделов 3.1 – 3.2, но уже в качестве исходного выступает Тдиагн. (n-1), рассчитанное на предыдущем шаге итерации. Здесь уже в большей степени учитывается время восстановления с частотой, стремящейся к реальной, следовательно риск Rнеконтр.(n-1) также будет приближаться к реальному.

По теореме Веерштрасса с увеличением n указанная последовательность Тдиагн. (n) будет сходящейся и для дальнейших расчетов используется его значение, отличающееся от точного предела Тдиагн. (∞) на величину, пренебрежимо малую с заданной по изменению рисков точностью ε.

Т.е. для дальнейшего применения комбинируемых моделей (например, из 3.1- 3.3) исходным выступает время диагностики n-й итерация Тдиагн. (n) , для которого выполняется условие:

$$\left| R_{неконтр.}(n) - R_{неконтр.}(n-1) \right| \le \varepsilon. \qquad (16)$$

Таким образом, применяя идеи 1-5, оказывается возможным для аналитического прогнозирования рисков для системы, состоящей из множества составных подсистем и элементов использовать те же комплексные показатели, что и для отдельного элемента.

В рамках комбинации моделей предлагается алгоритм прогноза риска нарушения целостности в течение заданного периода для системы, представимой в виде сложной структуры или одного элемента.

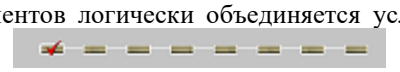
6 Предлагаемый алгоритм для аналитического прогнозирования рисков

Для указанного множества подсистем и элементов, обеспечивающих функционирование анализируемой системы, оценивается интегральный показатель - риск нарушения целостности как системы в целом, так и составных подсистем - с учетом предпринимаемых технологических мер контроля, мониторинга и восстановления целостности. И далее, исходя из этого показателя для различных значений Тзад , рассчитывается средняя наработка системы до нарушения целостности.

Предлагаемый алгоритм предусматривает выполнение следующих действий:

1. Выбирается само множество подсистем (всего – N, N≥1 подсистем, обеспечивающих функционирование анализируемого системы), по которым выполняется прогноз интегрального показателя. В самом общем случае рассматривается полное множество используемых подсистем.

2. Для каждой подсистемы из всего множества по п.1 настоящего алгоритма применяется следующий порядок действий:

2.1. Множество выбранных подсистем и/или элементов логически объединяется условием «И» и тем самым представимы в виде последовательной цепочки  (или при наличии резервирования - условие «ИЛИ» с представлением).

2.2. По каждому элементу для последующих расчетов определяются следующие исходные данные для применения моделей из 3.1 - 3.3.

2.3. С учетом идей 3 и 5 применительно к каждому из элементов выбирается и применяется для Тзад в точках от 0 до ∞ модель из подразделов 3.1 (если реализуется технология профилактической диагностики, т.е. периодический системный контроль имеет место, а мониторинг состояний между контролями отсутствует) или 3.2 (если реализуется технология мониторинга, т.е. имеет место не только периодический системный контроль, но и мониторинг состояний между контролями) с учетом подходов 3.3. С использованием идеи 1 по формулам (1)- (3), (5)-(6), (9) моделей вычисляется Rнаруш. – риск нарушения целостности в течение периода Тзад.. В итоге численных расчетов в точках Тзад от 0 до ∞ получается функция распределения.

Примечание. Это действие может быть выполнено, например, с использованием подсистем прогноза рисков из существующих инструментариев [11-13].

3. Имея в результате выполнения п. 2.3 алгоритма значения ФР по каждой подсистеме, используются формулы (11), (12) для построения ФР за систему в целом (т.е. по всему комплексу подсистем). Исходя из полученного вида ФР обычным статистическим способом вычисляется среднее время наработки до нарушения целостности, свойственное задаваемым условиям контроля, мониторинга и восстановления целостности.

Предложенный алгоритм применим для решения практических задач в приложении к отдельным элементам, подсистемам и к системе в целом, комплексируемым из разнородных систем в их жизненном цикле, в т.ч. создаваемым с разными целями в разные сроки, но объединяемые в какое-то время для решения общих или пересекающихся задач (т.е. к так называемым системам систем).

Примечание. Подробнее о системах систем и процессах жизненного цикла – см. ГОСТ Р 57193-2016 «Системная и программная инженерия. Процессы жизненного цикла систем».

В этом случае, опять-таки, используя предложенные выше модели и идеи возможна логическая интеграция системы как объединение двух последовательно соединенных систем (подсистем или элементов - см. рис. 9). Например, слева – рассматриваемая система без учета средств автоматизации, а справа – ИС, поддерживающая функции автоматизации – см. рис. 11. Логическая интерпретация элементарных состояний: интегрированная система находится в состоянии «отсутствия нарушений целостности», если «И» система слева, «И» система справа находятся в состоянии «отсутствия нарушений целостности».

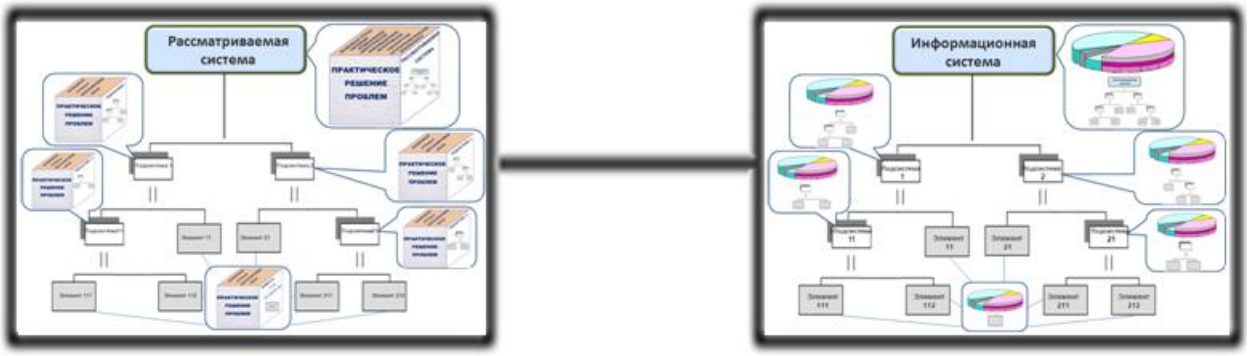


Рисунок 11 - Пример логического последовательного объединения двух разнородных систем (подсистем, элементов), при этом генерация моделей – с использованием формул (11) – (12)

Примером сложной подсистемы слева может служить фрагмент подсистемы безопасности угольной шахты, состоящий из комплексов главных вентиляторных установок, модульных дегазационных установок и газоотсасывающих установок и представленный в виде сложной параллельно-последовательной структуры – см. рис. 12.

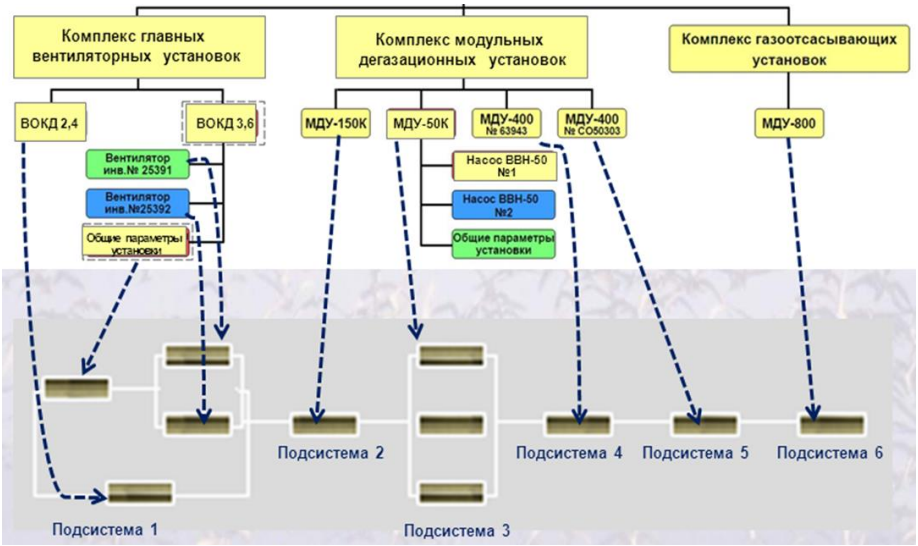


Рисунок 12 – Пример практического представления фрагмента подсистемы в формализованном виде, подготовленном для использования предложенного аналитического подхода

Таким образом, далеко не исчерпывая всего множества возможных подходов, для общего случая продемонстрированы современные способы построения вероятностных моделей для прогнозирования рисков применительно к сложным системам различного назначения.

7 Решение задач обоснования упреждающих мер

Зафиксировав уровни «допустимых рисков» для системы и составных подсистем, а также, считая неизменными все параметры, за исключением одного, возможно решение различные оптимизационных задач, связанных с обоснованием эффективных упреждающих мер обеспечения целостности системы в условиях разнородных угроз. Классическими задачами являются максимизация эффекта (уровня качества или безопасности и др.) или минимум рисков, возможных ущербов при ограничениях или минимизация затрат при ограничениях на допустимые риски и иных ограничениях. Пример предлагаемых классических постановок задач управления рисками в жизненном цикле систем приведен на рис. 13.

Для расчетов могут быть использованы модели, поддерживаемые инструментально-моделирующими комплексами [11-13].

Рисунок 13 - Постановки задач управления рисками в жизненном цикле систем

Сбалансированное упреждающее управление процессами возникновения, развития, контроля и нейтрализации возможных угроз осуществляется в рамках формальных постановок оптимизационных задач путем целенаправленного использования моделей и выбранных критериев рациональности при ограничениях на ресурсы и варианты реализации процессов. Смысл применения оптимизационных постановок задач в следующем – за счет упреждающего выбора рациональных значений управляемых параметров анализируемых сценариев угроз и реализуемых мер упреждения и реакции:

избежать излишних затрат при допустимых рисках и заданных критичных ограничениях на этапах концепции и технического задания (ТЗ), разработки, производства, эксплуатации и сопровождения системы и отдельных ее подсистем и элементов;

минимизировать риски в процессе эксплуатации системы и отдельных ее подсистем и элементов при заданных критичных ограничениях.

Описанные выше подходы зафиксированы на уровне национального стандарта ГОСТ Р 58494 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов (ОПО)». Применение этого стандарта в жизненном цикле ОПО обеспечивает: раннее распознавание и оценку развития предпосылок к инцидентам и нарушению нормальных условий функционирования ОПО; прогнозирование рисков, выявление явных и скрытых недостатков и угроз, поддержку принятия решений по предотвращению в режиме реального времени

возникновения на ОПО предаварийных и аварийных условий функционирования; определение сбалансированных мер обеспечения безопасности при средне- и долгосрочном планировании; обоснование предложений по совершенствованию и развитию многофункциональных систем безопасности по результатам системного анализа информации мониторинга.

Продолжение (часть 2) – в следующем номере.

Список литературы

1. Костогрызов А.И., Петухов А.В., Щербина А.М. «Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа». М.: Изд. «Вооружение, политика и конверсия , 1994.- 278с.
2. Костогрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. М.: Изд. «Вооружение. Политика. Конверсия», 1996.- 280 с.
3. Kostogryzov A.I. “Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ).” Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium, USA, Dallas, pp.63-70, 2000.
4. Безкоровайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК. 150 задач анализа и синтеза и примеров их решения. М.: Изд. «Вооружение. Политика. Конверсия», 2002.- 304 с.
5. Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М. Изд.”Вооружение, политика, конверсия”, 2004, 2-е изд.-2005.- 395с.
6. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд.”Вооружение, политика, конверсия”, 2008. – 404с.
7. Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. (2011) Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems, Proceedings of the 1st Intern.Conf. on Transportation Information and Safety, ICTIS, June 30-July 2,2011, Wuhan, China, p. 845-854
8. 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
9. 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/
10. Акимов В.А.,…,Костогрызов А.И., Махутов Н.А., Фортов В.Е., Шойгу С.К. и др. /Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности. М.: МГОФ «Знание», 2015, - 936с.
11. Моделирование процессов в жизненном цикле систем "Моделирование процессов" - "ноу-хау" // Свидетельство о государственной регистрации программы для ЭВМ №2004610858
12. Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем // Свидетельство о государственной регистрации программы для ЭВМ №2006610219
13. Программно-вычислительный комплекс оценки качества производственных процессов // Свидетельство о государственной регистрации программы для ЭВМ №2010614145.
14. Абросимов Н.В.,…,Костогрызов А.И., Махутов Н.А., Фортов В.Е., Шойгу С.К. и др. /Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Техногенная, технологическая и техносферная безопасность. М.:МГОФ «Знание», 2018, - 1016с. ISBN 978-5-87633-173-1.
15. 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. ISBN: 978-1-5386-3321-2
16. Probabilistic modeling in system engineering. InTechOpen, Edited by A. Kostogryzov, 2018, 279p. ISBN: 978-1-78923-775-7
17. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, Combinatorics and Control, InTechOpen. DOI: http://dx.doi.org/10.5772/intechopen.89168

References

1. Kostogryzov A.I., Petuhov A.V., SHCHerbina A.M. «Osnovy ocenki, obespecheniya i povysheniya kachestva vyhodnoj informacii v ASU organizacionnogo tipa». M.: Izd. «Vooruzhenie, politika i konversiya , 1994.-278s.
2. Kostogryzov A.I., Lipaev V.V. Sertifikaciya funkcionirovaniya avtomatizirovannyh informacionnyh sistem. M.: Izd. «Vooruzhenie. Politika. Konversiya», 1996.- 280 s.
3. Kostogryzov A.I. “Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ).” Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium, USA, Dallas, pp.63-70, 2000.
4. Bezkorovajnyj M.M., Kostogryzov A.I., L'vov V.M. Instrumental'no-modeliruyushchij kompleks dlya ocenki kachestva funkcionirovaniya informacionnyh sistem KOK. 150 zadach analiza i sinteza i primerov ih resheniya. M.: Izd. «Vooruzhenie. Politika. Konversiya», 2002.- 304 s.
5. Kostogryzov A.I., Nistratov G.A. Standartizaciya, matematicheskoe modelirovanie, racional'noe upravlenie i sertifikaciya v oblasti sistemnoj i programmnoj inzhenerii. M. Izd.”Vooruzhenie, politika, konversiya”, 2004, 2-e izd.- 2005.- 395s.
6. Kostogryzov A.I., Stepanov P.V. Innovacionnoe upravlenie kachestvom i riskami v zhiznennom cikle sistem – M.: Izd.”Vooruzhenie, politika, konversiya”, 2008. – 404s.
7. Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. (2011) Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems, Proceedings of the 1st Intern.Conf. on Transportation Information and Safety, ICTIS, June 30-July 2,2011, Wuhan, China, p. 845-854
8. 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
9. 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/
10. Akimov V.A.,…,Kostogryzov A.I., Mahutov N.A., Fortov V.E., SHojgu S.K. i dr. /Pod red. Mahutova N.A./ Bezopasnost' Rossii. Pravovye, social'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Nauchnye osnovy tekhnogennoj bezopasnosti. M.: MGOF «Znanie», 2015, - 936s.
11. Modelirovanie processov v zhiznennom cikle sistem "Modelirovanie processov" - "nou-hau" // Svidetel'stvo o gosudarstvennoj registracii programmy dlya EVM №2004610858
12. Kompleks dlya analiza i upravleniya kachestvom i riskami pri sozdanii i ekspluatacii avtomatizirovannyh sistem // Svidetel'stvo o gosudarstvennoj registracii programmy dlya EVM №2006610219
13. Programmno-vychislitel'nyj kompleks ocenki kachestva proizvodstvennyh processov // Svidetel'stvo o gosudarstvennoj registracii programmy dlya EVM №2010614145.
14. Abrosimov N.V.,…,Kostogryzov A.I., Mahutov N.A., Fortov V.E., SHojgu S.K. i dr. /Pod red. Mahutova N.A./ Bezopasnost' Rossii. Pravovye, social'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Tekhnogennaya, tekhnologicheskaya i tekhnosfernaya bezopasnost'. M.:MGOF «Znanie», 2018, - 1016s. ISBN 978-5-87633-173-1.
15. 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. ISBN: 978-1-5386-3321-2
16. Probabilistic modeling in system engineering. InTechOpen, Edited by A. Kostogryzov, 2018, 279p. ISBN: 978-1-78923-775-7
17. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, Combinatorics and Control, InTechOpen. DOI: http://dx.doi.org/10.5772/intechopen.89168