УДК 004.9, 006.074

МОДЕЛИ И МЕТОДЫ СИСТЕМНОЙ ИНЖЕНЕРИИ ДЛЯ ОПРЕДЕЛЕНИЯ СУЩЕСТВЕННЫХ УГРОЗ И УСЛОВИЙ НАРУШЕНИЯ ИНТЕРОПЕРАБЕЛЬНОСТИ

Костогрызов А.И.

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

При решении задач системной инженерии к системам различного функционального назначения предъявляются требования обеспечения интероперабельности. Под интероперабельностью согласно ГОСТ Р 55062-2021 понимается способность двух или более систем или компонентов к обмену необходимой информацией и к использованию информации, полученной в результате такого обмена. Цель работы состоит в обзорном представлении существующих моделей и методов системного анализа интероперабельности для определения существенных угроз и условий при решении практических задач системной инженерии. По ходу обзора даются отдельные поясняющие примеры.

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

MODELS AND METHODS OF SYSTEM ENGINEERING FOR DETERMINING SIGNIFICANT THREATS AND CONDITIONS OF INTEROPERABILITY DISRUPTION

Kostogryzov A.I.

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

When solving system engineering problems, systems of various functional purposes are required to ensure interoperability. According to GOST R 55062-2021, interoperability is the ability of two or more systems or components to exchange necessary information and to use the information obtained as a result of such exchange. The purpose of this work is to provide an overview of existing models and methods of system analysis of interoperability to identify significant threats and conditions when solving practical system engineering problems. The review includes some illustrative examples.

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

Введение

При решении задач системной инженерии к системам предъявляются требования обеспечения интероперабельности. Под интероперабельностью согласно ГОСТ Р 55062-2021 «Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения» понимается способность двух или более систем или компонентов к обмену необходимой информацией и к использованию информации, полученной в результате такого обмена.

Настоящая работа охватывает системы различного функционального назначения. Например это могут быть системы в интересах органов государственной власти и корпораций, энергетических и промышленных структур (в т. ч. для отдельных предприятий, строительных, нефтегазовых и транспортных комплексов, опасного производства), предприятий атомной промышленности, служб по чрезвычайным ситуациям, информационно-управляющие системы, системы с использованием технологий искусственного интеллекта и др. Под системой понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей. Таким образом, требования интероперабельности свойственны практически для всех систем, независимо от их масштабов и функционального назначения.

В России одними из первых разработок в области интероперабельности явились работы Гуляева Ю.В., Журавлева Е.Е., Олейникова А.Я. и др. [1-4], приведшие впоследствии к появлению ряда национальных стандартов. Пример проблемно-ориентированного описания интероперабельности системы по ГОСТ Р 55062, ГОСТ Р 59797 «Информационные технологии. Сложные системы. Интероперабельность. Основные положения», ГОСТ Р 70569 «Информационные технологии. Сетецентрические информационно-управляющие

системы. Интероперабельность» с условным выделением организационного, семантического и технического уровней представлен на рис. 1.

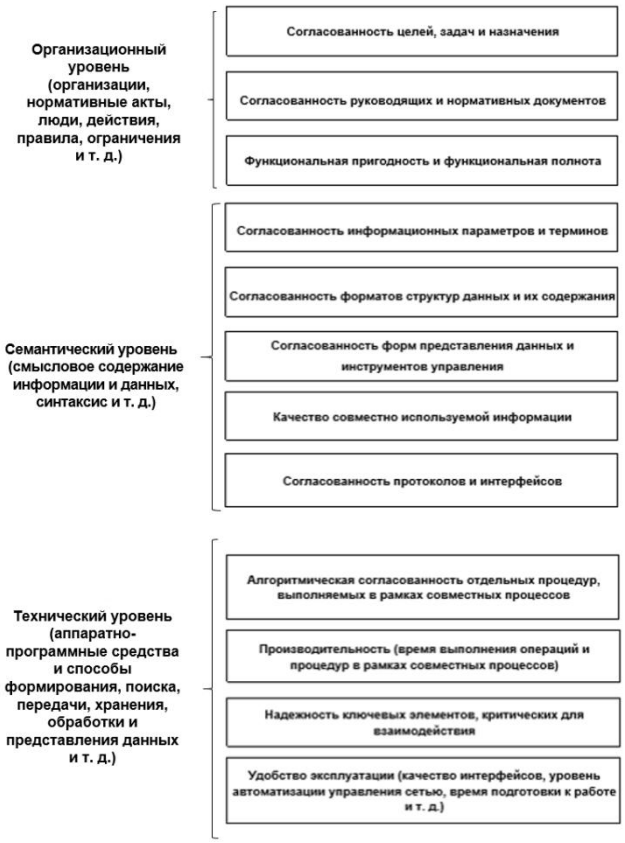

Рис.1 Пример проблемно-ориентированного описания интероперабельности системы

Для рационального выполнения требований интероперабельности и решения практических задач системной инженерии в жизненном цикле систем различного функционального назначения используют системный анализ. Под системным анализом интероперабельности понимается научный метод системного познания, предназначенный для решения практических задач системной инженерии путем представления рассматриваемых системных процессов или системы в виде приемлемой моделируемой системы, обладающей способностью к обмену необходимой информацией с другой моделируемой системой. Метод включает:

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

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

- обоснование с использованием моделирования упреждающих мер противодействия угрозам, обеспечивающих желаемые свойства рассматриваемых процесса, системы (и/или ее элементов) и/или проекта при задаваемых ограничениях в задаваемый период времени;

- обоснование с использованием моделирования предложений по обеспечению и повышению качества, безопасности и/или эффективности рассматриваемой системы (и/или ее элементов) и достижению целей системной инженерии при задаваемых ограничениях в задаваемый период времени.

К специальным критичным сущностям системы могут быть отнесены отдельные характеристики (например, физические параметры, характеристики качества, безопасности, размеры, стоимость), достигаемые эффекты, выполняемые функции, действия или защищаемые активы. При этом в состав рассматриваемых могут быть включены характеристики, эффекты, функции, действия и активы, свойственные не только самой системе, но и иным системам (подсистемам), не вошедшим в состав рассматриваемой системы. Например, это могут быть характеристики, эффекты, функции, действия и активы, свойственные обеспечивающим системам, привлекаемым информационным системам и/или базам данных, охватываемым по требованиям заказчика.

Примечание. В соответствии с ГОСТ Р 59994-2022 «Системная инженерия. Системный анализ процесса гарантии качества для системы» моделируемая система определена как система, для которой решение задач системного анализа осуществляется с использованием

ее формализованной модели, позволяющей исследовать критичные сущности системы в условиях ее создания и/или применения, учитывающей структурные связи между переменными или постоянными элементами формализованного представления, задаваемые условия и ограничения. Например, при проведении системного анализа в принимаемых допущениях, ограничениях и предположениях модель может формально описывать функциональные подсистемы и элементы, процессы, реализуемые действия, множество активов и/или выходных результатов или множество этих или иных сущностей в их целенаправленном применении в задаваемых условиях.

Цель настоящей статьи состоит в обзорном представлении существующих моделей и методов системного анализа интероперабельности для определения существенных угроз и условий при решении практических задач системной инженерии. Представленные далее модели и методы системного анализа интероперабельности вошли в проект национального стандарта ГОСТ Р «Системная инженерия. Системный анализ интероперабельности. Определение существенных угроз и условий», успешно прошедшего публичное обсуждение летом 2025г.

1. Общий методический взгляд на определение существенных угроз и условий нарушения интероперабельности

Важной задачей системной инженерии является определение существенных угроз и условий, способных при том или ином развитии событий негативно или позитивно повлиять на качество, безопасность и прогнозируемые риски относительно двух и более взаимодействующих систем. Результаты определения существенных угроз и условий подлежат использованию при решении задач системной инженерии, включая обоснование мер, направленных на эффективное противодействие угрозам и поддержание приемлемых условий использования систем в условиях ограничений на задаваемые допустимые риски, правовых, функциональных, нормативно-технических, технологических, климатических, экологических и иных ограничений на ресурсы (в т.ч. на природные, временные, стоимостные, людские, технические ресурсы). При этом важно одинаковое понимание используемых терминов и словосочетаний.

Под существенной угрозой в работе понимается совокупность обстоятельств и факторов, создающих потенциальную или реально существующую опасность нарушения требуемой интероперабельности системы. Условие является существенным, если в контексте использования системы риск нарушения требуемой интероперабельности системы превышает задаваемый допустимый уровень. Контекст использования системы определяют ее пользователи, решаемые задачи, оборудование (аппаратные средства, программные средства, материалы), физическая и социальная среда и условия, сценарии возникновения и развития угроз нормальному использованию системы, реализуемые способы и технологии противодействия угрозам интероперабельности и восстановления необходимой целостности системы после реализации угроз. В свою очередь, под целостностью моделируемой системы понимается такое ее состояние, которое отвечает целевому назначению модели системы в течение задаваемого периода прогноза. Наконец, под риском понимается влияние неопределенности на достижение поставленных целей. При этом риск выражается через его источники, потенциальные события, их последствия и вероятность (по ГОСТ Р 51897/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения).

На практике определение существенных угроз и условий, способных при том или ином развитии событий негативно или позитивно повлиять на интероперабельность рассматриваемой системы (подсистемы или системного элемента), выполняют с использованием методов системного анализа специальных показателей интероперабельности, связанных с критичными сущностями рассматриваемой системы, в т. ч. с помощью методов прогнозирования рисков. При этом используемые методы определения существенных угроз и условий должны быть целенаправлены на раннее распознавание и оценку развития предпосылок к нарушению качества, безопасности и/или эффективности рассматриваемой системы [5-20 и др.]. Возможно рассмотрение интероперабельности одной конкретной системы, условно предполагая ее сравнение с некоторой системой-эталоном или системой-аналогом.

Для определения существенных угроз и условий при наличии достаточных фактических данных, позволяющих пренебречь условиями неопределенности, используют результаты измерений и оценок специальных показателей, связанных с критичными сущностями рассматриваемой системы и характеризующих нарушение качества, безопасности и/или эффективности (как следствие нарушения интероперабельности рассматриваемой системы). При отсутствии или недостаточности фактических данных, а также при необходимости учета различных неопределенностей на задаваемый период прогноза рассматриваемая система формально представляется в виде моделируемой системы.

2. Обобщенные рекомендации по определению существенных угроз и условий

При решении задач системной инженерии, позволяющих пренебречь последствиями неопределенности, как правило, составляют полный перечень угроз нарушения интероперабельности системы и условий использования системы, критичных с точки зрения обеспечения ее интероперабельности. Каждой угрозе и каждому условию сопоставляются соответствующие последствия от реализации этих угроз и условий. Сопоставляемые последствия характеризуют потенциальный ущерб от нарушения интероперабельности и могут быть выражены как качественно (например, «недопустимый ущерб», «большой ущерб» с использованием логических описаний последствий или «допустимый ущерб»), так и количественно (например, ущерб в рублях, часах неработоспособности или в каких-либо иных условных единицах). Причем как в качественном, так и в количественном выражениях фиксируются состояния, признаваемые с точки зрения интероперабельности как недопустимые, остальные уровни признаются допустимыми, т.е. приемлемыми для практического использования. На практике это – вырожденный случай, который возможен именно в силу пренебрежения условиями неопределенности. Случается крайне редко – например, это могут быть автоматические системы, которые предназначены для совместной работы в стабильных условиях в течение длительных периодов эксплуатации независимо от контроля человека (например, автоматические сенсорные устройства в газопроводе, обменивающиеся информацией с контрольно-диспетчерским пунктом с использованием технологий искусственного интеллекта).

В рамках составленного полного перечня угроз и условий используют следующие критерии:

- угроза нарушения интероперабельности системы признается существенной, если установленное для нее множество возможных последствий признано недопустимым;

- условие использования системы, критичное для обеспечения ее интероперабельности, признается существенным, если при осуществлении этого условия множество последствий признано недопустимым.

Ранжирование существенных угроз и условий проводится по необходимости, оно может быть осуществлено лишь в случае, когда возможно сравнение последствий: чем последствия хуже, тем опасность соответствующих угроз и условий выше.

Далее обратимся к наиболее распространенному случаю при решении задач системной инженерии, когда пренебречь условиями неопределенности невозможно. Для определения существенных угроз и условий составляют изначальный возможный перечень угроз нарушения интероперабельности системы и условий использования системы, критичных с точки зрения обеспечения ее интероперабельности. При необходимости этот перечень может расширяться и уточняться во времени и по содержанию, в т.ч. из-за изменения условий неопределенности.

Для прогнозирования рисков на практике могут быть использованы любые научно обоснованные формализованные модели и методы, обеспечивающие достижение целей и решение поставленных задач системной инженерии. Для определения существенных угроз и условий рекомендуется применение математических моделей и методов прогнозирования рисков применительно к моделируемой системе в задаваемый период прогноза, см., например, соответствующие рекомендации стандартов системной инженерии: ГОСТ Р 59329 – ГОСТ Р 59357 для различных процессов жизненного цикла систем, ГОСТ Р 59989 – ГОСТ Р 59994 для системного анализа отдельных процессов (процесса управления качеством системы, процесса оценки и контроля проекта, процесса управления рисками для системы, процесса управления моделью жизненного цикла системы, процесса управления инфраструктурой системы, процесса гарантии качества для системы), ГОСТ Р 71998 «Информационные технологии. Требования и оценка качества систем и программного обеспечения. Определение качества ИТ-услуг».

Как пример, применимы критерии:

- угроза нарушения интероперабельности системы признается существенной, если для нее прогнозное значения риска превышает установленное значение соответствующего допустимого риска;

- условие использования системы, критичное для обеспечения ее интероперабельности, признается существенным, если при осуществлении этого условия:

- прогнозное значения риска превышает установленное значение допустимого риска (при сопоставимых ущербах для различных угроз, условий и/или для различных сценариев их проявления при использовании системы);

- математическое ожидание ущерба превышает установленный допустимый уровень (при несопоставимых ущербах для различных угроз, условий и/или для различных сценариев их проявления при использовании системы).

Непревышение допустимого риска на вероятностном уровне или на уровне математического ожидания ущерба интерпретируют как несущественность рассматриваемых угроз и как соблюдение условий по удержанию риска в допустимых пределах в течение периода прогноза.

Если в приложении к моделируемой системе все расчетные риски не превышают установленных допустимых рисков, это означает, что результаты моделирования подтверждают удержание рисков в допустимых пределах, т.е. существенные угрозы и условия для системы в течение периода прогноза считаются отсутствующими. Если какие-то расчетные риски превышают максимально допустимые, это означает уязвимость рассматриваемой системы с точки зрения нарушения ее интероперабельности для соответствующих существенных угроз и условий.

Ранжирование существенных угроз и условий проводится по необходимости, оно может быть осуществлено лишь в случае, когда возможно количественное сравнение последствий (например, в условных единицах).

При сопоставимых ущербах применим следующий критерий: чем вероятностное выражение риска выше, тем более высокой считается опасность соответствующих угроз и условий (в этом случае достаточно ограничиться сравнением на вероятностном уровне). В свою очередь, при несопоставимых ущербах для различных угроз, условий и/или для различных сценариев их проявления при использовании системы необходим учет различных последствий нарушения интероперабельности. В этом случае применим следующий критерий: чем выше значение математического ожидания ущерба в задаваемый период прогноза, тем более высокой считается опасность реализации соответствующих угроз и условий в этот период.

Примечание. В одинаковых единицах измерения результат произведения вероятностного значения прогнозируемого риска в задаваемый период прогноза на количественное значение потенциального ущерба может быть интерпретировано как математическое ожидание ущерба. Тем самым ранжирование существенных угроз и условий может проводиться по шкале математического ожидания ущерба в единицах количественного измерения последствий нарушения интероперабельности.

3. Рекомендации по моделированию

3.1 Суть подхода

Для демонстрации общего подхода к применению методов и моделей системной инженерии используем типовую архитектуру системы по ГОСТ Р 59797 «Информационные технологии. Сложные системы. Интероперабельность. Основные положения» – см. рис. 2.

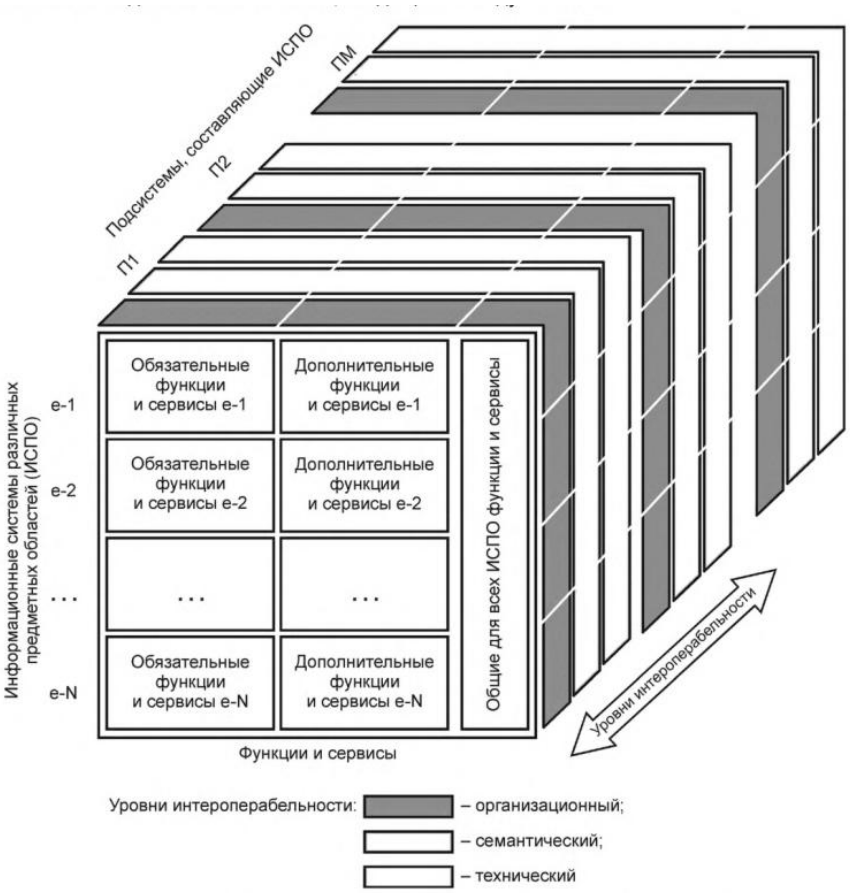

Рис. 2 Типовая архитектура системы с точки зрения интероперабельности (по ГОСТ Р 59797-2021)

В качестве оцениваемых выступает моделируемая система, представляющая собой формализованную модель рассматриваемой системы, и формализованные модели учитываемых сущностей качества информации в

условиях применения системы. Получаемые в результате моделирования результаты прогнозирования рисков и решения прикладных задач распространяются на рассматриваемую систему.

Основной целью прогнозирования рисков для моделируемой системы является установление степени вероятного нарушения требований по обеспечению интероперабельности за период прогноза (для упрощения последствия для различных типов информации и расчетных показателей на семантическом уровне полагаются сравнимыми). Цель может варьироваться в зависимости от периода прогноза и контекста предполагаемого использования моделируемой системы.

Целеполагание при прогнозировании рисков нарушения интероперабельности позволит количественно решать следующие прикладные задачи системного анализа (например, по ГОСТ Р 59991 «Системная инженерия. Системный анализ процесса управления рисками для системы»):

- прогнозирование рисков, интерпретации и анализ получаемых результатов, включая сравнение прогнозируемых значений оцениваемых показателей с допустимым уровнем на предмет выполнения задаваемых ограничений;
- обоснование допустимых рисков;
- определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно или позитивно повлиять на свойства, способных недопустимо ухудшить качество и/или безопасность и/или эффективность рассматриваемой моделируемой системы;
- определение и обоснование в жизненном цикле моделируемой системы упреждающих мер противодействия угрозам и условий снижения рисков или удержания рисков в допустимых пределах, обеспечивающих желаемый уровень интероперабельности для рассматриваемой системы при задаваемых ограничениях в период прогноза;
- обоснование рекомендаций по минимизации рисков нарушения интероперабельности моделируемой системы с учетом дополнительных специфических требований (например, требований по защите информации).

Для математической формализации приняты следующие предположения:

- в условиях неопределенностей возникновение и разрастание различных угроз и условий, критичных для обеспечения интероперабельности системы, описывается в терминах случайных событий;
- для различных вариантов развития угроз обеспечению интероперабельности средства, технологии и меры противодействия угрозам с формальной точки зрения представляют собой совокупность контрмер, предназначенных для преодоления барьеров интероперабельности и воспрепятствования реализации угроз и/или ухудшению условий использования моделируемой системы;
- в общем случае в моделируемой системе интероперабельность на семантическом уровне согласно ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы» зависит от своевременности предоставления используемой информации, полноты оперативного отражения в системе новых объектов и явлений, актуальности обновляемой информации, безошибочности информации после контроля, корректности обработки информации, обеспечения безопасности информации (включая сохранение целостности моделируемой системы в условиях опасных программно-технических воздействий, защищенность активов от несанкционированного доступа и сохранение конфиденциальности используемой информации);
- к началу периода прогноза целостность моделируемой системы обеспечена, включая изначальное выполнение требований по обеспечению интероперабельности.

Предупреждающие контрмеры характеризуются обоснованным использованием выбранных мер противодействия угрозам (и/или удержания в допустимых пределах условий, критичных для обеспечения интероперабельности). Дополнительно делается предположение о наличии возможностей по определению предпосылок к реализации угроз (и/или к ухудшению критичных условий использования системы), наличии мер противодействия угрозам (и/или удержания в допустимых пределах критичных условий использования системы), наличии способов выявления последствий следов реализации угроз (и/или последствий проявления критичных условий в недопустимых пределах), а также возможностей по приемлемому восстановлению нарушаемых условий функционирования моделируемой системы с точки зрения обеспечения ее интероперабельности.

Для определения существенных угроз и явлений могут быть использованы математические модели и методы прогнозирования рисков, изложенные в ГОСТ Р 59341, ГОСТ Р 59991 и ГОСТ Р 59994 «Системная инженерия. Системный анализ процесса гарантии качества для системы». Поэтому далее приводятся лишь ссылки на соответствующие положения в указываемых стандартах. Рекомендуемые показатели поддерживаются математическими моделями и методами, обеспечивающими проведение оценок различных частных рисков и прогнозирование интегрального риска нарушения интероперабельности моделируемой

системы. Частные показатели учитывают возможные нарушения интероперабельности подсистем в их жизненном цикле на организационном, семантическом и техническом уровнях (см. рис. 1).

Для прогнозирования рисков при сопоставимых последствиях рекомендуются следующие количественные показатели:

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на организационном уровне при выполнении обязательных функций и сервисов в течение заданного периода прогноза. Это – частный показатель;

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на семантическом уровне при выполнении обязательных функций и сервисов в течение заданного периода прогноза. Это – частный показатель;

Примечание. Для многосторонних научно-практических исследований необходимо учитывать, что в общем случае интероперабельность в моделируемой системе на семантическом уровне будет зависеть от своевременности предоставления используемой информации, полноты оперативного отражения в системе новых объектов и явлений, актуальности обновляемой информации, безошибочности информации после контроля, корректности обработки информации, обеспечения безопасности информации (включая сохранение целостности моделируемой системы в условиях опасных программно-технических воздействий, защищенность активов от несанкционированного доступа и сохранение конфиденциальности используемой информации);

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на техническом уровне при выполнении обязательных функций и сервисов в течение заданного периода прогноза. Это – частный показатель;

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на организационном уровне при выполнении дополнительных функций и сервисов в течение заданного периода прогноза. Это – частный показатель;

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на семантическом уровне при выполнении дополнительных функций и сервисов путем анализа задаваемого объема информации. Это – частный показатель;

- риск нарушения интероперабельности в моделируемой системе (подсистеме, компоненте, элементе системы) на техническом уровне при выполнении дополнительных функций и сервисов в течение заданного периода прогноза. Это – частный показатель;

- интегральный риск нарушения интероперабельности в моделируемой системе в течение заданного периода прогноза (на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов). Это – интегральный показатель, учитывающий дополнительные расчетные показатели в зависимости от индикаторных условий (α) и вероятностных значений частных показателей, определенных выше (см. соответствующие условия α из ГОСТ Р 59341, приложений В.3.2 – В.3.8, а также А.6.4).

В условиях неопределенности для оценки частных и интегрального рисков нарушения интероперабельности моделируемой системы далее применяются математические модели, рекомендованные ГОСТ Р 59341, ГОСТ Р 59991 и ГОСТ Р 59994. Применяемые модели ориентированы на возможные угрозы нарушения интероперабельности системы и условия использования системы, критичные с точки зрения обеспечения ее интероперабельности (см. раздел 4 статьи).

3.2. Оценка риска нарушения интероперабельности на организационном уровне

Для оценки риска нарушения интероперабельности в моделируемой системе на организационном уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза применяются «Модели для оценки безошибочности действий пользователей и персонала системы» из ГОСТ Р 59341, приложения В.3.8. В качестве исходных данных для расчетов выступают:

σ – частота возникновения источников угроз с точки зрения нарушения интероперабельности на организационном уровне;

β – среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий пользователей и персонала);

$T_{меж}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{восст}$ – среднее время восстановления нарушаемой целостности моделируемой системы;

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

В общем случае такие исходные данные, как $T_{меж}$ и $T_{диаг}$, на практике определяются в руководствах по контролю целостности системы или путем измерений. В свою очередь для определения σ, β, $T_{восст}$

рекомендуется использование универсальной вспомогательной модели показателя (УВМП) – см., например, ГОСТ Р 59349. Значения σ, β, $T_{восст}$, получаемые по результатам анализа данных мониторинга (или пересчета этих параметров на уровне УВМП), являются исходными данными для формального описания моделируемой системы с учетом возможности прогнозирования динамики разнородных событий. В общем случае показатель УВМП может быть использован при формировании исходных данных и применении моделей для семантического и технического уровней интероперабельности.

3.3. Оценка риска нарушения интероперабельности на семантическом уровне

Для оценки риска нарушения интероперабельности в моделируемой системе на семантическом уровне при выполнении обязательных и дополнительных функций и сервисов применяются различные частные показатели, призванные охарактеризовать качество используемой информации в системе:

1) для оценки своевременности предоставления используемой информации - «Модель для оценки своевременности предоставления информации» из ГОСТ Р 59341, приложения В.3.3, характеризуемая исходными данными для расчетов:

T_i, и $|(T_i^2 - T_{i2})|^{0,5}$ – соответственно среднее время и среднеквадратичное отклонение времени реакции системы при обработке запросов *i*-го типа (т. е. полного времени пребывания на обработке с учетом ожидания в очередях), T_{i2} – второй момент времени реакции. Чаще в качестве исходных данных формируют целиком именно среднеквадратичное отклонение, не опускаясь до отдельных измерений второго момента;

– для каждого из значимых типов информации (с привязкой к выполняемым функциональным задачам, источникам и получателям информации) требования к своевременности обработки запросов в системе (касающиеся как запрашиваемой, так и выдаваемой принудительно информации) указывается один из двух критериев:

- критерий своевременности по среднему времени реакции: среднее время обработки запросов *i*-го типа T_i должно быть не более задаваемого $T_{зад\,i}$ (далее условие этого критерия упоминается как условие своевременности α_1);

- вероятностный критерий: вероятность своевременной обработки запросов *i*-го типа в системе $P_{св\,i}(T_{зад\,i}) = P_{св\,i}(\tau_i \le T_{зад\,i})$ за заданное время $T_{зад\,i}$ должна быть не ниже задаваемой $P_{св\,зад\,i}$ (далее условие этого критерия упоминается как условие своевременности α_2), где τ_i – случайная величина, означающая время реакции системы при обработке запросов *i*-го типа;

2) для оценки полноты оперативного отражения в системе новых объектов и явлений - «Модель для оценки полноты оперативного отражения в системе новых объектов и явлений» из ГОСТ Р 59341, приложения В.3.4, характеризуемая исходными данными для расчетов:

λ — частота появления новых объектов и явлений в процессе функционирования системы;

$T_{база\ данных}$ — среднее время подготовки, передачи и ввода новых объектов учета в БД системы;

3) для оценки актуальности обновляемой информации - «Модель для оценки актуальности обновляемой информации» из ГОСТ Р 59341, приложения В.3.5, характеризуемая исходными данными для расчетов:

ξ — среднее время между значимыми изменениями реальной информации относительно информации, хранимой в системе (т. е. ξ^{-1} — частота значимого изменения);

$T_{база\ данных}$ — среднее время подготовки, передачи и ввода в БД данных от источников информации;

q — среднее время между соседними обновлениями данных (т. е. q^{-1} — частота обновления данных) в системе при обновлении ее по регламенту;

4) для оценки безошибочности информации после контроля - «Модель для оценки безошибочности информации после контроля» из ГОСТ Р 59341, приложения В.3.6, характеризуемая исходными данными для расчетов:

V — объем контролируемой информации;

μ – доля первоначальных ошибок в контролируемой информации в объеме V (до контроля), т. е. произведение $V \cdot \mu$ принимает безразмерное значение от 0 до 1;

ν — средняя скорость контроля информации;

n — частота ошибок контроля 1-го рода (когда реальное отсутствие ошибки истолковывается как наличие ошибки);

$T_{нар}$ — среднее время наработки контролера на ошибку 2-го рода, после истечения которого первая же реальная ошибка в контролируемом объеме информации оказывается пропущенной (для программно-технических средств — это время наработки на отказ);

$T_{непр}$ — период непрерывной работы контролера;

$T_{зад}$ — задаваемое время на контроль информации;

5) для оценки корректности обработки информации - «Модель для оценки корректности обработки информации» из ГОСТ Р 59341, приложения В.3.7, характеризуемая исходными данными для расчетов:

V – объем информации, подлежащий обработке (анализу);

μ – часть важной для принятия решения информации, которая должна быть объективно использована при обработке (анализе) информации объема V, т. е. произведение $V \cdot \mu$ принимает безразмерное значение от 0 до 1;

ν – скорость обработки (анализа);

n – частота ошибок обработки (анализа) 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной);

$T_{нар}$ – среднее время наработки на алгоритмическую ошибку (когда объективно важная для принятия решения информация игнорируется, это – аналог ошибки контроля 2-го рода);

$T_{непр}$ – период непрерывной работы аналитика (в качестве аналитика могут выступать программно-математические средства или пользователь системы);

$\boldsymbol{T}_{зад}$ – задаваемое время на обработку (анализ) информации;

6) для оценки безопасности информации в части сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий - «Модель для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий» из ГОСТ Р 59341, приложения В.3.9.2, характеризуемая исходными данными для расчетов:

σ – частота возникновения источников угроз в виде источников опасных программно-технических воздействий на моделируемую систему;

β – среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий процесса или защищаемых активов, используемых при выполнении действия) в результате опасных программно-технических воздействий;

$T_{меж}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{восст}$ – среднее время восстановления нарушаемой целостности моделируемой системы;

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

7) для оценки безопасности информации в части защищенности активов от несанкционированного доступа - «Модель для оценки защищенности активов от несанкционированного доступа» из ГОСТ Р 59341, приложения В.3.9.3, характеризуемая исходными данными для расчетов:

M – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы;

$\boldsymbol{f_m}$ – среднее время между соседними изменениями параметров защиты m-й преграды;

u_m – среднее время преодоления (вскрытия значений параметров защиты) m-й преграды;

8) для оценки безопасности информации в части сохранения конфиденциальности используемой информации - «Модель для оценки сохранения конфиденциальности используемой информации» из ГОСТ Р 59341, приложения В.3.9.3, характеризуемая исходными данными для расчетов:

M – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы;

$\boldsymbol{f_m}$ – среднее время между соседними изменениями параметров защиты m-й преграды;

u_m – среднее время преодоления (вскрытия значений параметров защиты) m-й преграды;

$T_{конф}$ - период объективной конфиденциальности используемой информации.

3.4. Оценка риска нарушения интероперабельности на техническом уровне

Для оценки риска нарушения интероперабельности в моделируемой системе на техническом уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза применяются «Модели для оценки надежности предоставления информации» из ГОСТ Р 59341, приложения В.3.2, «Модель для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий» из ГОСТ Р 59341, приложения В.3.9.2 (для программно-технических аспектов, влияющих на интероперабельность). В качестве исходных данных для расчетов выступают:

σ – частота возникновения источников угроз с точки зрения нарушения интероперабельности на техническом уровне;

β – среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы с точки зрения нарушения интероперабельности на техническом уровне;

$T_{меж}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{диаг}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{восст}$ – среднее время восстановления нарушаемой целостности моделируемой системы;

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

Примечание. Несмотря на фактическую повторяемость некоторых названий исходных данных (поскольку используются одни и те же модели), их значения при моделировании для технического уровня при выполнении дополнительных функций и сервисов, возможно, будут отличны от значений при использовании моделей при выполнении обязательных функций и сервисов, а также в сравнении с организационным и семантическим уровнями, поскольку различны их природа, причины формирования значений, интерпретация и области приложений. Соответственно разными могут быть и расчетные риски.

3.5. Оценка интегрального риска

В качестве исходных данных для оценки интегрального риска нарушения интероперабельности моделируемой системы в течение заданного периода прогноза (на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов) используются расчетные показатели, рассчитываемые в зависимости перечисленных выше исходных данных по «Алгоритму расчета интегрального риска нарушения реализации процесса с учетом требований по защите информации» из ГОСТ Р 59341, приложения В.3.10:

$Z_{над\ предст}(T_{зад})$ — вероятностный коэффициент надежности предоставления информации, учитывающий вероятность надежного предоставления информации в системе в течение заданного периода прогноза $T_{зад}$ и соответствующие условия α, определяется по модели В.3.2 из ГОСТ Р 59341;

$Z_{своевр}$ — вероятностный коэффициент своевременности обработки запросов, учитывающий относительную долю своевременно обработанных в системе запросов и соответствующие условия α, определяется по модели В.3.3 из ГОСТ Р 59341;

$Z_{полн}$ — вероятностный коэффициент полноты оперативного отражения в системе новых объектов и явлений, учитывающий вероятность того, что в системе полностью отражены состояния всех реально существующих критичных объектов и явлений, и соответствующие условия α, определяется по модели В.3.4 из ГОСТ Р 59341;

$Z_{акт}$ — вероятностный коэффициент актуальности информации в системе, учитывающий вероятность сохранения актуальности информации на момент ее использования и соответствующие условия α, определяется по модели В.3.5 из ГОСТ Р 59341;

$Z_{безош}$ — вероятностный коэффициент безошибочности информации в системе, учитывающий вероятность отсутствия ошибок в информации после ее контроля и соответствующие условия α, определяется по модели В.3.6 из ГОСТ Р 59341;

$Z_{корр}$ — вероятностный коэффициент корректности обработки информации в системе, учитывающий вероятность получения корректных результатов обработки информации и соответствующие условия α, определяется по модели В.3.7 из ГОСТ Р 59341;

$Z_{чел}$ $(T_{зад})$ — вероятностный коэффициент безошибочных действий пользователей и персонала системы, учитывающий вероятность безошибочных действий пользователей и персонала в течение заданного периода прогноза и соответствующие условия α, определяется по модели В.3.8 из ГОСТ Р 59341;

$P_{возд}(T_{зад})$ — вероятность отсутствия опасного программно-технического воздействия на систему в течение заданного периода прогноза $T_{зад}$, определяемая по рекомендациям В.3.9.2 из ГОСТ Р 59341;

$P_{НСД}$ $(T_{зад})$ — вероятность обеспечения защищенности активов системы от НСД в течение заданного периода прогноза $T_{зад}$ (или без привязки к этому периоду - $P_{НСД}$), определяемая по рекомендациям В.3.9.3 из ГОСТ Р 59341;

$P_{конф}(T_{конф})$ — вероятность сохранения конфиденциальности используемой информации в течение периода объективной конфиденциальности $T_{конф}$, определяемая по рекомендациям В.3.9.4 из ГОСТ Р 59341 (период $T_{конф}$ может играть роль периода прогноза $T_{зад}$ – см. последнее примечание в 3.9.4).

4. Использование интегрального риска

Интегральный риск используется для сравнения весомости прогнозируемых частных рисков, выявления существенных угроз и поддержки принятия решений для задач системного анализа при разработке и эксплуатации системы в сопоставлении с возможным ущербом. Как пример, интегральный риск нарушения интероперабельности в моделируемой системе в течение заданного периода прогноза на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов $\boldsymbol{R}_{\text{интегр}}(\boldsymbol{T}_{\text{зад}})$ для прогнозного периода $\boldsymbol{T}_{\text{зад}}$ может быть определен по формуле (согласно ГОСТ Р 59991, приложению В):

$$R_{\text{интегр}}\ (T_{\text{зад}}) = 1 - [1 - R_{\text{наруш}}(T_{\text{зад}})]\ [1 - R_{\text{надежн}}\ (T_{\text{зад}})], \qquad (1)$$

где $\boldsymbol{R}_{\text{наруш}}(\boldsymbol{T}_{\text{зад}})$ — риск нарушения безопасности информации (включая сохранение целостности моделируемой системы в условиях опасных программно-технических воздействий, защищенность активов от несанкционированного доступа и сохранение конфиденциальности используемой информации) в течение периода прогноза $\boldsymbol{T}_{\text{зад}}$. Показатель $\boldsymbol{R}_{\text{наруш}}(\boldsymbol{T}_{\text{зад}})$ относится к семантическому уровню интероперабельности и может быть рассчитан по моделям и рекомендациям ГОСТ Р 59341, приложению В:

$$\boldsymbol{R}_{\text{наруш}}\ (\boldsymbol{T}_{\text{зад}}) = 1 - P_{\text{возд}}\ (T_{\text{зад}}) \cdot P_{\text{НСД}}\ (T_{\text{зад}}) \cdot P_{\text{конф}}(T_{\text{конф}}); \qquad (2)$$

$\boldsymbol{R}_{\text{надежн}}(\boldsymbol{T}_{\text{зад}})$ — обобщенный виртуальный показатель для организационного, семантического и технического уровням, учитывающий в течение задаваемого периода прогноза $\boldsymbol{T}_{\text{зад}}$ надежность и своевременность предоставления используемой информации, полноту оперативного отражения в системе новых объектов и явлений, актуальность обновляемой информации, безошибочность информации после контроля, корректность обработки информации и безошибочность действий пользователей и персонала системы. Этот виртуальный показатель для моделируемой системы может быть рассчитан по моделям и рекомендациям ГОСТ Р 59341, приложению В:

$$\boldsymbol{R}_{\text{надежн}}\ (\boldsymbol{T}_{\text{зад}}) = \mathbf{1} - Z_{\text{над предст}}(T_{\text{зад}}) \cdot Z_{\text{своевр}} \cdot Z_{\text{полн}} \cdot Z_{\text{акт}} \cdot Z_{\text{безош}} \cdot Z_{\text{корр.}} \cdot Z_{\text{чел}}(T_{\text{зад}}). \qquad (3)$$

Здесь к организационному уровню интероперабельности относится $Z_{\text{чел}}(T_{\text{зад}})$, к семантическому уровню - показатели $Z_{\text{своевр}}$, $Z_{\text{полн}}$, $Z_{\text{акт}}$, $Z_{\text{безош}}$, $Z_{\text{корр.}}$, а также $P_{\text{возд}}\ (T_{\text{зад}}) \cdot P_{\text{НСД}}\ (T_{\text{зад}}) \cdot P_{\text{конф}}(T_{\text{конф}})$, к техническому уровню относится $Z_{\text{над предст}}(T_{\text{зад}})$.

При этом на организационном уровне интероперабельности для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп чел}}\ (T_{\text{зад}})$ и условие α. Условие α касается безошибочности действий пользователей и персонала системы и формулируется в виде ограничений: $P_{\text{чел}}\ (T_{\text{зад}}) \geq P_{\text{доп чел}}\ (T_{\text{зад}})$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента безошибочных действий пользователей и персонала системы $Z_{\text{чел}}\ (T_{\text{зад}})$

$$Z_{\text{чел}}(T_{\text{зад}}) = \begin{cases} 1, & \text{если условие безошибочности действий } \alpha \text{ выполнено,} \\ P_{\text{чел}}(T_{\text{зад}}), & \text{если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

На семантическом уровне интероперабельности для оценки своевременности предоставления информации используется вспомогательное понятие относительной доли своевременно обработанных в системе запросов $C_{\text{своевр.}}$ Этот вспомогательный показатель охватывает лишь те типы запросов, для которых выполнены требования потребителя информации, этот показатель вычисляют по формуле

$$C_{\text{своевр}} = \sum_{i=1}^{I} \lambda_i P_{\text{св}\ i}\ (T_{\text{зад}\ i})[Ind\ (\alpha_1) + Ind\ (\alpha_2)] \Big/ \sum_{i=1}^{I} \lambda_i, \qquad 4)$$

где λ_i — частота поступления на обработку запросов i-го типа;

Критерии своевременности обработки каждого типа запросов устанавливают с использованием индикаторной функции $Ind\ (\alpha)$:

$$Ind(\alpha) = \begin{cases} 1, & \text{если условие } \alpha \text{ истинно,} \\ 0, & \text{если условие } \alpha \text{ ложно.} \end{cases}$$

При этом для i-го типа запросов условие своевременности α с учетом возможных ущербов определяют одним из условий α_1 или α_2:

- α_1 – условие, когда для i-го типа запросов задан критерий своевременности по среднему времени реакции и $T_i \leq T_{\text{зад}\ i}$.

- α_2 – условие, когда для i-го типа запросов задан вероятностный критерий своевременности и $P_{\text{св}\ i}(\tau_i \leq T_{\text{зад}\ i}) \geq P_{\text{св зад}\ i}$.

Для оценки интегрального риска условие своевременности предоставления информации α формулируют в виде условий α_1 или α_2 с добавлением, что в случае их нарушения возможный ущерб не превышает допустимого (это – формулировка условия α по всем типам запросов). Учет результатов моделирования осуществляют с использованием индикаторного коэффициента своевременности обработки запросов $Z_{\text{своевр}}$:

$$Z_{\text{своевр}} = \begin{cases} 1, & \text{если условия своевременности } \alpha \text{ выполнены для всех типов запросов,} \\ & C_{\text{своевр}} \text{ по (4), если хотя бы одно условие не выполнено.} \end{cases}$$

Для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп полн}}$ и условие α. Условие α касается полноты оперативного отражения в системе новых объектов и явлений и формулируется в виде ограничений: $P_{\text{полн}} \geq P_{\text{доп полн}}$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием вероятностного коэффициента полноты оперативного отражения в системе новых объектов и явлений $Z_{\text{полн}}$:

$$Z_{\text{полн}} = \begin{cases} 1, & \text{если условие полноты отражения в системе объектов и явлений } \alpha \text{ выполнено,} \\ & \text{Рполн, если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп акт}}$ и условие α. Условие α касается сохранения актуальности информации в системе на момент ее использования и формулируется в виде ограничений: $P_{\text{акт}} \geq P_{\text{доп акт}}$ и возможный ущерб от нарушения не превышает допустимого (это – формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента актуальности информации в системе $Z_{акт}$:

$$Z_{\text{акт}} = \begin{cases} 1, & \text{если условие сохранения актуальности информации в системе } \alpha \text{ выполнено,} \\ & P_{\text{акт}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп безош}}$ и условие α. Условие α касается обеспечения безошибочности информации после контроля и формулируется в виде ограничений: $P_{\text{безош}} \geq P_{\text{доп безош}}$ и возможный ущерб от нарушения не превышает допустимого (это – формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента безошибочности информации в системе $Z_{\text{безош}}$

$$Z_{\text{безош}} = \begin{cases} 1, & \text{если условие безошибочности информации после контроля } \alpha \text{ выполнено,} \\ & P_{\text{безош}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп корр}}$ и условие α. Условие α касается обеспечения корректности обработки информации и формулируется в виде ограничений: $P_{\text{корр}} \geq P_{\text{доп корр}}$ и возможный ущерб от нарушения не превышает допустимого (это формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента корректности обработки информации в системе $Z_{\text{корр}}$

$$Z_{\text{корр}} = \begin{cases} 1, & \text{если условие обеспечения корректности обработки информации } \alpha \text{ выполнено,} \\ & P_{\text{корр}}, \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

На техническом уровне интероперабельности для системного анализа результатов моделирования в оценках интегрального риска задают допустимый уровень $P_{\text{доп над}}(T_{\text{зад}})$ и условие α. Условие α касается надежности предоставления информации и формулируется в виде ограничений $P_{\text{над предст}}(T_{\text{зад}}) \geq P_{\text{доп над}}(T_{\text{зад}})$ и возможный ущерб от нарушения не превышает допустимого (это – формулировка условия α). Учет результатов моделирования в оценках интегрального риска осуществляют с использованием индикаторного коэффициента надежности предоставления информации $Z_{\text{над предст}}$ $(T_{\text{зад}})$

$$Z_{\text{над предст}}(T_{\text{зад}}) = \begin{cases} 1, & \text{если условие надежности предоставления информации } \alpha \text{ выполнено,} \\ & P \text{ над предст}(T\text{зад}), \text{ если условие } \alpha \text{ не выполнено или не задано.} \end{cases}$$

Сопоставление с возможным ущербом позволяет рассматривать дополнение до единицы произведения упомянутых коэффициентов $(1 - Z_{...})$ в качестве вероятностного выражения соответствующего риска.

Примечания:

1 Другие возможные показатели, модели, методы и рекомендации по оценке рисков см. в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р МЭК 61069-1 – ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 – ГОСТ Р МЭК 61508-7.

2 Примеры прогнозирования рисков и решения задач системного анализа, связанные с прогнозированием рисков в процессах, приведены в ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

5. Примеры определения существенных угроз и условий

5.1. Определение возможных угроз

Перечень возможных угроз нарушения интероперабельности системы может включать:

- природные и природно-техногенные угрозы (например, по ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 54124, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7;
- угрозы со стороны человеческого фактора (например, по ГОСТ Р МЭК 62508);
- угрозы безопасности информации, качеству и безопасности функционирования программного обеспечения, оборудования и коммуникаций, используемых в процессе работы (например, по ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275, ГОСТ Р 51583, ГОСТ Р 54124, ГОСТ Р 56939, ГОСТ Р 58412, ГОСТ Р 59329–ГОСТ Р 59357, ГОСТ Р 59989–ГОСТ Р 59994);
- угрозы компрометации информационной безопасности приобретающей стороны (заказчика) (например, по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005–2010, приложение С;
- угрозы возникновения ущерба репутации и/или потери доверия поставщика (производителя) к конкретному заказчику, системы которого были скомпрометированы;
- прочие соответствующие угрозы качеству, безопасности и эффективности системы, связанные с нарушением интероперабельности на организационном, семантическом или техническом уровнях при выполнении обязательных и дополнительных функций и сервисов в системе (например, по ГОСТ Р 59989 – ГОСТ Р 59994, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ IEC 61508-3, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 62508, ГОСТ Р 71303, ГОСТ Р 71438, ГОСТ Р 71440, ГОСТ Р 71998).

Возможные угрозы характеризуются частотой их возникновения и средним временем развития до нарушения требуемой интероперабельности (если на них никак не реагировать) – например, с использованием универсальной вспомогательной модели показателя (УВМП) по ГОСТ Р 59349. Существенность угроз определяется на основе моделирования и использования выбранных критериев системного анализа.

5.2. Определение существенных условий

Перечень существенных условий использования системы, критичных с точки зрения обеспечения ее интероперабельности, может включать условия, характеризующие такой контекст использования моделируемой системы, при котором расчетный риск превышает задаваемого допустимого при прочих неизменных параметрах. Эти условия могут быть сформированы на основе решения обратных задач.

Так, условия в части управления риском нарушения интероперабельности в моделируемой системе на организационном уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза при ограничениях в виде задаваемого условия α (применяется модель из 3.2):

– частота возникновения источников угроз с точки зрения нарушения интероперабельности на организационном уровне (σ) не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий пользователей и персонала) (β) должно составлять не менее минимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы ($T_{меж}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время системной диагностики целостности моделируемой системы ($T_{диаг}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время восстановления нарушаемой целостности моделируемой системы ($T_{восст}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

Условия в части управления рисками нарушения интероперабельности в моделируемой системе на семантическом уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза при ограничениях в виде задаваемых условий α (применяются модели из 3.3).

Условия из 3.3.1) в части управления своевременностью предоставления используемой информации с помощью «Модели для оценки своевременности предоставления информации» из ГОСТ Р 59341, приложения В.3.3: частота поступления на обработку запросов запросов i-го типа в системе, $i \geq 1$ (касающиеся как запрашиваемой, так и выдаваемой принудительно информации) и среднее время их обработки для каждого из значимых типов информации (с привязкой к выполняемым функциональным задачам, источникам и получателям информации) не должны превышать максимальных расчетных значений (влияющих на расчетные значения T_i, и $|(T_i^2 - T_{i2})|^{0,5}$, которые в свою очередь могут быть оценены на основе применения моделей массового обслуживания разнотипных запросов в системе и/или методом натурных испытаний и/или имитационного моделирования), для которых при прочих неизменных исходных данных по каждому i-му типу запросов выполняется один из установленных критериев:

- критерий своевременности по среднему времени реакции: среднее время обработки запросов i-го типа T_i должно быть не более задаваемого $T_{зад\,i}$ (это - условие своевременности α_1);

- вероятностный критерий: вероятность своевременной обработки запросов i-го типа в системе $P_{св\,i}(T_{зад\,i}) = P_{св\,i}(\tau_i \leq T_{зад\,i})$ за заданное время $T_{зад\,i}$ должна быть не ниже задаваемой $P_{св\,зад\,i}$ (это - условие своевременности α_2), где τ_i – случайная величина, означающая время реакции системы при обработке запросов i-го типа;

Условие из 3.3.2) в части управления полнотой оперативного отражения в системе новых объектов и явлений с помощью «Модели для оценки полноты оперативного отражения в системе новых объектов и явлений» из ГОСТ Р 59341, приложения В.3.4 (для каждого из различных типов информации): среднее время подготовки, передачи и ввода новых объектов учета в БД системы ($T_{база\ данных}$) должно составлять не более максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого.

Примечание. Необходимо учесть, что в реальности возможности влияния на частоту появления новых объектов и явлений в процессе функционирования системы (λ) практически отсутствуют.

Условия из 3.3.3) в части управления актуальностью обновляемой информации с помощью «Модели для оценки актуальности обновляемой информации» из ГОСТ Р 59341, приложения В.3.5 (для каждого из различных типов информации):

— среднее время подготовки, передачи и ввода в БД данных от источников информации ($T_{база\ данных}$) должно составлять не более максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— частота обновления данных в системе при обновлении ее по регламенту (q^{-1}) должна составлять не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого.

Примечание. Необходимо учесть, что в реальности возможности влияния на частоту значимого изменения реальной информации относительно информации, хранимой в системе (ξ^{-1}) практически отсутствуют.

Условия из 3.3.4) в части управления безошибочностью информации после контроля с помощью «Модели для оценки безошибочности информации после контроля» из ГОСТ Р 59341, приложения В.3.6 (для каждого из различных типов информации):

— объем контролируемой информации (V) должен составлять не более максимального расчетного значения (если это практически возможно), для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

– доля первоначальных ошибок в контролируемой информации в объеме V (до контроля - μ) должно составлять не более максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— средняя скорость контроля информации (ν) должна быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— частота ошибок контроля 1-го рода (когда реальное отсутствие ошибки истолковывается как наличие ошибки - n) не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— среднее время наработки контролера на ошибку 2-го рода, после истечения которого первая же реальная ошибка в контролируемом объеме информации оказывается пропущенной ($T_{\text{нар}}$), должно быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— период непрерывной работы контролера ($T_{\text{непр}}$) не должен превышать максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— задаваемое время на контроль информации ($T_{\text{зад}}$) должно быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого.

Примечание. Необходимо учесть, что в реальности возможности влияния на период непрерывной работы контролера ($T_{\text{непр}}$) могут быть ограничены различными эргономическими требованиями

Условия из 3.3.5) в части управления корректностью обработки информации с помощью «Модели для оценки корректности обработки информации» из ГОСТ Р 59341, приложения В.3.7 (для каждого из различных типов информации):

— объем информации, подлежащий обработке или анализу (V) должен составлять не более максимального расчетного значения (если это практически возможно), для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

– часть важной для принятия решения информации, которая должна быть объективно использована при обработке или анализе информации объема V (μ) должна составлять не более максимального расчетного значения (если это практически возможно), для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— скорость обработки или анализа информации (ν) должна быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— частота ошибок обработки (анализа) 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной - n) не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— среднее время наработки на алгоритмическую ошибку, когда объективно важная для принятия решения информация игнорируется ($T_{\text{нар}}$), должно быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— период непрерывной работы аналитика ($T_{\text{непр}}$) не должен превышать максимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого;

— задаваемое время на обработку или анализ информации ($T_{\text{зад}}$) должно быть не менее минимального расчетного значения, для которого при прочих неизменных исходных данных соответствующий расчетный риск не превышает допустимого.

Условие из 3.3.6) по управлению безопасностью информации в части сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий с помощью «Модели для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий» из ГОСТ Р 59341, приложение В.3.9.2:

– частота возникновения источников угроз в виде источников опасных программно-технических воздействий на моделируемую систему (σ) не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время развития угроз с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий процесса или защищаемых активов, используемых при выполнении действия)

в результате опасных программно-технических воздействий (β) должно составлять не менее минимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы ($T_{меж}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время системной диагностики целостности моделируемой системы ($T_{диаг}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время восстановления нарушаемой целостности моделируемой системы ($T_{восст}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого.

Условие из 3.3.7) по управлению безопасностью информации в части защищенности активов от несанкционированного доступа с помощью «Модели для оценки защищенности активов от несанкционированного доступа» из ГОСТ Р 59341, приложения В.3.9.3: количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы (M), среднее время между соседними изменениями параметров защиты m-й преграды ($\boldsymbol{f_m}$) и среднее время преодоления (вскрытия значений параметров защиты) m-й преграды ($\boldsymbol{u_m}$) в комплексе должны быть таковыми, чтобы соответствующий расчетный риск не превышал допустимого. Из альтернативных вариантов предпочтение отдается тому варианту, для которого расчетный риск минимален при ограничениях на затраты и ресурсы.

Условие из 3.3.8) по управлению безопасностью информации в части сохранения конфиденциальности используемой информации с помощью «Модели для оценки сохранения конфиденциальности используемой информации» из ГОСТ Р 59341, приложения В.3.9.3: для задаваемого периода объективной конфиденциальности используемой информации ($\boldsymbol{T}_{конф}$) количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам системы (M), среднее время между соседними изменениями параметров защиты m-й преграды ($\boldsymbol{f_m}$) и среднее время преодоления (вскрытия значений параметров защиты) m-й преграды ($\boldsymbol{u_m}$) в комплексе должны быть таковыми, чтобы соответствующий расчетный риск не превышал допустимого. Из альтернативных вариантов предпочтение отдается тому варианту, для которого расчетный риск минимален при ограничениях на затраты и ресурсы.

Условия в части управления риском нарушения интероперабельности в моделируемой системе на техническом уровне при выполнении обязательных и дополнительных функций и сервисов в течение заданного периода прогноза при ограничениях в виде задаваемого условия α (применяются «Модель для оценки надежности предоставления информации» из ГОСТ Р 59341, приложения В.3.2, «Модель для оценки сохранения целостности моделируемой системы в условиях опасных программно-технических воздействий» из ГОСТ Р 59341, приложения В.3.9.2 – см. А.6.3):

– частота возникновения источников угроз с точки зрения нарушения интероперабельности на техническом уровне (σ) не должна превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы с точки зрения нарушения интероперабельности на техническом уровне (β) должно составлять не менее минимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы ($T_{меж}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время системной диагностики целостности моделируемой системы ($T_{диаг}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

– среднее время восстановления нарушаемой целостности моделируемой системы ($T_{восст}$) не должно превышать максимального расчетного значения, для которого при прочих неизменных исходных данных расчетный риск не превышает допустимого;

Примечание. Необходимо учесть, что в реальности из определяемых в Б.2 условий с учетом специфики системы возможности управленческих воздействий на перечисленные характеристики могут быть практически ограничены, например, некоторые из средств, способов и действий, влияющих на выполнение условий могут оказаться технически не реализуемыми. Это означает, что в управлении

контекстом использования системы эти условия игнорируются, применению подлежат лишь те условия, позволяющие удерживать риски в допустимых пределах, которые практически реализуемы.

Для определения сбалансированных условий системной инженерии решению подлежат различные оптимизационные задачи. Например, постановка задачи может заключаться в определении таких условий использования моделируемой системы, для которых при задаваемых ограничениях достигается минимум интегрального риска нарушения интероперабельности в моделируемой системе в течение заданного периода прогноза на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов $R_{\text{интегр}}(T_{\text{зад}})$ с использованием выражений (1) – (3).

При решении задач системной инженерии возможны другие постановки оптимизационных задач системного анализа, связанные, например, с максимизацией качества и/или безопасности и/или эффективности системы по показателям более высокого мета-уровня, когда расчетные значения интегрального риска нарушения интероперабельности в моделируемой системе в течение заданного периода прогноза на организационном, семантическом и техническом уровнях при выполнении обязательных и дополнительных функций и сервисов фигурируют в ограничениях, т.е. учитывается требование к допустимому значению интегрального риска: $R_{\text{интегр}}(T_{\text{зад}}) \leq R_{\text{доп}}(T_{\text{зад}})$.

При этом могут быть использованы любые научно обоснованные формализованные модели и методы, обеспечивающие достижение целей и решение поставленных задач системной инженерии.

Заключение

Обзорно представлены существующие модели и методы системного анализа интероперабельности для определения существенных угроз и условий при решении практических задач системной инженерии. Охвачены системы различного функционального назначения.

Для определения существенных угроз и явлений в условиях неопределенности предложено использовать стандартизованные математические модели и методы прогнозирования рисков согласно ГОСТ Р 59341 «Системная инженерия. Защита информации в процессе управления информацией системы», ГОСТ Р 59991 «Системная инженерия. Системный анализ процесса управления рисками для системы» и ГОСТ Р 59994 «Системная инженерия. Системный анализ процесса гарантии качества для системы». Рекомендованные показатели рисков обеспечивают проведение оценок различных частных рисков и прогнозирование интегрального риска нарушения интероперабельности моделируемой системы. Частные показатели учитывают возможные нарушения интероперабельности подсистем в их жизненном цикле на организационном, семантическом и техническом уровнях.

Представленные модели и методы системного анализа интероперабельности вошли в проект национального стандарта ГОСТ Р «Системная инженерия. Системный анализ интероперабельности. Определение существенных угроз и условий», успешно прошедшего публичное обсуждение летом 2025г.

Список литературы

1. Гуляев Ю.В.. Олейников А.Я. Стандартизация информационных технологий в фундаментальных исследованиях. Стандарты информационных технологий от «нано» до GRIDZ/Мир стандартов. 2008. № 8. С. 12—25

2. Гуляев Ю.В.. Журавлев Е.Е.. Олейников А.Я. Методология стандартизации для обеспечения интероперабельности информационных систем широкого класса. Аналитический обзор // Журнал радиоэлектроники. 2012. № 3.

3. Каменщиков А.А., Олейников А.Я., Широбокова Т.Д. Исследование особенностей проблемы интероперабельности в крупномасштабных информационных системах // Информационные технологии и вычислительные системы. 2018, N3. стр. 16—21

4. Башлыкова А.А.. Козлов С.В., Макаренко С И.. Олейников А.Я., Фомин И.А. Подход к обеспечению интероперабельности в сетецентрических системах управления // Журнал радиоэлектроники. 2020. № 6.

5. 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.

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

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

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

10. 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

11. 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

12. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, Combinatorics and Control, InTechOpen, 2020. DOI: http://dx.doi.org/10.5772/intechopen.89168

13. 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

14. 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

15. Костогрызов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии //Вопросы кибербезопасности. 2022, №6(52), с.71-82.

16. 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

17. 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.

18. 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

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

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

21. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Тематический блок "Национальная безопасность". Системная инженерия в проблемах национальной безопасности / А. В. Анищенко, В. Б. Артемьев, М. К. Бондарева [и др.]. Научный рук. – Махутов Н.А. - Москва: МГОФ «Знание», 2025. - 904 с.

References

1. Gulyaev Yu.V., Oleynikov A.Ya. Standardization of information technologies in fundamental research. Information technology standards from "nano" to GRID // Mir Standartov [World of Standards]. 2008. No. 8. P. 12–25.

2. Gulyaev Yu.V., Zhuravlev E.E., Oleynikov A.Ya. Standardization methodology for ensuring interoperability of a wide class of information systems. Analytical review // Zhurnal Radioelektroniki [Journal of Radio Electronics]. 2012. No. 3.

3. Kamenshchikov A.A., Oleynikov A.Ya., Shirobokova T.D. Study of the features of the interoperability problem in large-scale information systems // Informatsionnye Tekhnologii i Vychislitel'nye Sistemy [Information Technologies and Computing Systems]. 2018, No. 3. pp. 16–21.

4. Bashlykova A.A., Kozlov S.V., Makarenko S.I., Oleynikov A.Ya., Fomin I.A. An approach to ensuring interoperability in network-centric control systems // Zhurnal Radioelektroniki [Journal of Radio Electronics]. 2020. No. 6.

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

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

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

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. Bezopasnost' Rossii. Pravovye, sotsial'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Nauchnye osnovy tekhnogennoi bezopasnosti [Safety of Russia. Legal, socio-economic and scientific-technical aspects. Scientific foundations of technogenic safety]. / Ed. by N.A. Makhutov. – M.: MGOF "Znanie", 2015. – 936 p.

10. Kostogryzov A.I., Stepanov P.V., Nistratov A.A., Grigoriev L.I., Chervyakov L.M. Forecasting risks to ensure information quality in complex systems // Sistemy Vysokoi Dostupnosti [High Availability Systems]. 2016, No. 3, Vol. 2, pp. 25–37.

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

12. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, Combinatorics and Control, InTechOpen, 2020. DOI: http://dx.doi.org/10.5772/intechopen.89168

13. Nistratov A.A. Analytical forecasting of the integral risk of violating acceptable execution of a set of standard processes in the life cycle of high availability systems. Part 1. Mathematical models and methods // Sistemy Vysokoi Dostupnosti [High Availability Systems]. 2021. Vol. 17, No. 3, pp. 16–31. Part 2. Software and technological solutions. Examples // Sistemy Vysokoi Dostupnosti [High Availability Systems]. 2022. Vol. 18, No. 2, pp. 42–57.

14. Nistratov A.A. On mathematical, software-technological and methodological solutions focused on rational risk management in systems engineering. Collection of materials of the All-Russian Scientific-Practical Conference "Russia in the XXI Century under Global Challenges: Problems of Risk Management and Ensuring the Safety of Socio-Economic and Socio-Political Systems and Natural-Technogenic Complexes", April 26-27, 2022, Presidium of the Russian Academy of Sciences. Ed. by Prof. Ya.D. Vishnyakov. – M.: State University of Management. 2022. pp. 251–255.

15. Kostogryzov A.I. On models and methods of probabilistic analysis of information protection in standardized processes of systems engineering // Voprosy Kiberbezopasnosti [Cybersecurity Issues]. 2022, No. 6(52), pp. 71–82.

16. 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

17. Kostogryzov A.I., Nistratov A.A. Methodological approach to probabilistic forecasting and comparison of system operation quality under uncertainty // Nadezhnost' [Reliability]. 2024, Vol. 24, No. 1. pp. 10–24.

18. Nistratov, A.A. On expectations, limitations and applied capabilities of standardized risk forecasting models and methods in systems engineering // IT-Standard. – 2024. – No. 3(40). – pp. 31–51. – EDN BDXEGY.

19. Kostogryzov A.I., Nistratov A.A. Analysis of trends in the development of systems engineering // IT-standart. 2024, No. 3, pp. 4–20.

20. Sukhomlin V.A., Romanov V.Yu., Gapanovich D.A. Vvedenie v model'no-orientirovannuyu sistemnuyu i programmnuyu inzheneriyu (MBSSE) [Introduction to Model-Based Systems and Software Engineering (MBSSE)]. MAKS Press, 2024, 672 p.

21. Bezopasnost' Rossii. Pravovye, sotsial'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Tematicheskii blok "Natsional'naya bezopasnost'". Sistemnaya inzheneriya v problemakh natsional'noi bezopasnosti [Safety of Russia. Legal, socio-economic and scientific-technical aspects. Thematic block "National Security". Systems engineering in problems of national security] / A. V. Anishchenko, V. B. Artemiev, M. K. Bondareva [et al.]. Scientific supervisor – N.A. Makhutov. - Moscow: MGOF "Znanie", 2025. - 904 p.