УДК 681.3.06(075.32)
DOI: 10.25559/SITITO.18.202202.227-240

Научная статья

К методам системной инженерии: вероятностные подходы к анализу процесса управления качеством системы

А. И. Костогрызов
ФГУ «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», г. Москва, Российская Федерация
Адрес: 119333, Российская Федерация, г. Москва, ул. Вавилова, д. 44-2
Akostogr@gmail.com

Аннотация

Перспективная системная инженерия, выходя далеко за сегодняшние рамки, должна ориентироваться на системы будущего, становящиеся более разумными, самоорганизующимися, ресурсоэффективными, безопасными, устойчивыми, а также поддерживаться междисциплинарной теоретической основой. В результате анализа прогнозов применения системной инженерии предложены вероятностные подходы к анализу процесса управления качеством системы. Предложенные вероятностные подходы позволяют оценивать риски нарушения надежности реализации процесса управления качеством системы (в т.ч. риски невыполнения необходимых действий, нарушения сроков выполнения необходимых действий процесса и/или наличия недопустимого брака в поставляемых продукции и/или услугах) без учета и с учетом дополнительных специфических системных требований. Их применение ориентировано на решение актуальных задач системной инженерии.

Ключевые слова: качество, модель, риск, система, системная инженерия

Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Костогрызов А. И. К методам системной инженерии: вероятностные подходы к анализу процесса управления качеством системы // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 2. С. 227-240. doi: https://doi.org/10.25559/SITITO.18.202202.227-240

Original article

To the Methods of System Engineering: Probabilistic Approaches to the Analysis of the System Quality Management Process

A. I. Kostogryzov
Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russian Federation
Address: 44 Vavilov St., building 2, Moscow 119333, Russian Federation
Akostogr@gmail.com

Abstract

Advanced system engineering should be based on interdisciplinary theory and focused on the systems of the future, becoming more intelligent, self-organizing, resource-efficient, safe and sustainable. As a result of the analysis of forecasts for the application of system engineering, probabilistic approaches to the analysis of the system quality management process are proposed. The proposed probabilistic approaches allow us to assess the risks of violation of the reliability of the implementation of the system quality management process (including the risks of failure to perform the necessary actions, violation of the deadlines for performing the necessary actions of the process and/or the presence of unacceptable defects in the supplied products and/or services) without taking into account and taking into account additional specific system requirements. Their application is focused on solving actual problems of system engineering.

Keywords: model, quality, risk, system, system engineering

The author declares no conflict of interest.

For citation: Kostogryzov A.I. To the Methods of System Engineering: Probabilistic Approaches to the Analysis of the System Quality Management Process. *Sovremennye informacionnye tehnologii i IT-obrazovanie = Modern Information Technologies and IT-Education.* 2022; 18(2):227-240. doi: https://doi.org/10.25559/SITITO.18.202202.227-240

1. Введение

Настоящая работа продолжает идеи, связанные с разработкой и совершенствованием методов, применимых для исследования стандартизованных процессов и решения прикладных задач системной инженерии [1-16]. Под системной инженерией понимается сосредоточение научно-технических усилий на том, как рациональным образом построить и эффективно эксплуатировать различные искусственно создаваемые системы. В свою очередь система рассматривается как комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей[1]. Примерами важных систем в России выступают: критически важные и потенциально опасные объекты для единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, определенных Федеральным законом от 21.12.1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»; опасные производственные объекты, определенные Федеральным законом от 21.07.1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов»; объекты топливно-энергетического комплекса (ТЭК), определенные Федеральным законом от 21.07.2011 г. № 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 26.07.2017 г. №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 и др.[2]

Согласно ожиданиям Международного совета по системной инженерии (INCOSE) перспективная системная инженерия должна охватывать широкий спектр областей функционального применения систем, выходя далеко за сегодняшние рамки (в т.ч. захватывая поддержку политических решений), ориентироваться на системы будущего, становящиеся более разумными, самоорганизующимися, ресурсоэффективными и безопасными, устойчивыми в эксплуатации и реагирующими на постоянно растущий и разнообразный спектр общественных потребностей. Для этого перспективная системная инженерия должна поддерживаться междисциплинарной теоретической основой, методами и инструментариями исследований, основанными на моделях, позволяющих лучше понимать все более сложные системы и решения, принимаемые в условиях неопределенности [1].

В настоящей работе внимание сосредоточено на широко применимом процессе управления качеством системы. Этот процесс является одним из 30 стандартизованных процессов в жизненном цикле любого рода систем в ISO/IEC/IEEE 15288 и ГОСТ Р 57193, более подробно процесс управления качеством описан в ГОСТ Р ИСО 9001 «Системы менеджмента качества. Требования»[3], ГОСТ Р ИСО/МЭК 20000-1 «Информационная технология. Управление услугами, Часть 1. Требования к системе управления услугами»[4]. Предлагаемые идеи применимы к системам, создаваемым человеком для любой области приложений с учетом имеющейся специфики – в интересах органов государственной власти и корпораций, энергетических, финансово-экономических, страховых и промышленных структур, предприятий оборонно-промышленного комплекса, авиационно-космической отрасли, служб по чрезвычайным ситуациям, жилищно-коммунального хозяйства и пр.

2. Характеристика процесса управления качеством системы

Процесс управления качеством системы, подлежащий системному анализу, используют на стадиях замысла, формирования требований, разработки концепции и технического задания (ТЗ), разработки, эксплуатации и сопровождения системы.

В общем случае главная цель процесса управления качеством системы состоит в том, чтобы выпускаемая продукция, выполняемые функции и услуги системы и непосредственно

[1] См. подробнее ISO/IEC/IEEE International Standard – Systems and software engineering – System life cycle processes. ISO/IEC/IEEE 15288. First edition 2015-05-15. IEEE Press, 2015. doi: https://doi.org/10.1109/IEEESTD.2015.7106435; ГОСТ Р 57193-2016 Системная и программная инженерия. Процессы жизненного цикла систем: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2016 г. № 1538-ст: введен впервые: дата введения 2017-11-01 / подготовлен ООО «ИАВЦ». М.: Стандартинформ, 2016.

[2] О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: федер. закон от 21 декабря 1994 № 68-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_5295 (дата обращения: 18.05.2022); О промышленной безопасности опасных производственных объектов: федер. закон от 21 июля 1997 № 116-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_15234 (дата обращения: 18.05.2022); О безопасности объектов топливно-энергетического комплекса: федер. закон от 21 июля 2011 № 256-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_117196 (дата обращения: 18.05.2022); О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26 июля 2017 № 187-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885 (дата обращения: 18.05.2022).

[3] ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования = ISO 9001:2015 Quality management systems – Requirements: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 сентября 2015 г. № 1391-ст: введен впервые: дата введения 2015-11-01 / подготовлен ОАО «ВНИИС», ООО «Интерсертифика – ТЮФ», ЗАО «Центр Приоритет», Ассоциации по сертификации «Русский регистр», ООО «ТЮФ Интернациональ РУС», ООО «Би-Эс-Ай Эм-Эс-Си-Ай-Эс», «AE Conformity Pty Ltd», Международной ассоциации по сертификации персонала. М.: Стандартинформ, 2020.

[4] ГОСТ Р ИСО/МЭК 20000-1-2013 Информационная технология. Управление услугами. Часть 1. Требования к системе управления услугами = ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 г. № 1543-ст: введен впервые: дата введения 2015-01-01 / подготовлен ЗАО «ИТ Эксперт», ООО «ИАВЦ». М.: Стандартинформ, 2019.

реализация процесса управления качеством системы удовлетворяли организационным и проектным целям в области качества с достижением требуемой удовлетворенности заказчика и пользователей системы.

Основные усилия системной инженерии при проведении системного анализа процесса управления качеством системы сосредотачивают на:

- определении выходных результатов и действий, предназначенных для достижения целей процесса;
- определении потенциальных угроз и определении возможных сценариев возникновения и развития угроз для качества системы и процесса управления качеством системы;
- измерениях и оценках специальных показателей, связанных с критичными сущностями системы и характеризующих ее качество;
- определении и прогнозировании рисков, подлежащих системному анализу;
- получении результатов системного анализа в виде, пригодном для решения задач системной инженерии, включая обоснование мер, направленных на практическое противодействие угрозам качеству системы и достижение поставленных целей.

Основными выходными результатами процесса управления качеством системы являются цели управления качеством, критерии и методы оценки качества, ресурсы и информация для поддержки и контроля действий в процессе, результаты оценки процесса, корректируемая политика и процедуры по управлению качеством. Для получения выходных результатов процесса управления качеством системы в общем случае выполняют следующие основные действия:

- планирование управления качеством (включая определение целей, политики и процедур по управлению качеством, определение обязанностей и полномочий для реализации управления качеством, определение критериев и методов оценки качества, обеспечение ресурсами и информацией для управления качеством);
- оценку управления качеством (включая сбор и анализ результатов оценки процесса управления качеством в соответствии с определенными критериями, оценку удовлетворенности заказчика, периодический анализ действий по обеспечению качества выполнения проектов, контроль улучшений качества для процессов, продукции и услуг);
- выполнение корректирующих и упреждающих действий по управлению качеством, в т.ч. планирование корректирующих действий для достижения целей управления качеством, планирование упреждающих мер при определении недопустимого риска нарушения надежности реализации процесса управления качеством, осуществление корректирующих действий для достижения целей управления качеством[5].

Для анализа достижимости требуемого качества системы, прогнозирования рисков, связанных с реализацией системных процессов, и обоснования эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых пределах используют вероятностные показатели и методы их расчетов. Эти методы применяются для расчетов при решении различных задач системной инженерии. При этом сам перечень востребованных для решения задач системной инженерии формируется в жизненном цикле рассматриваемой системы с учетом ее масштабов, имеющих место вызовов и возможных угроз[6].

3. Примеры задач системной инженерии, при решении которых используются вероятностные методы

Задачи системной инженерии, при решении которых используются вероятностные методы, условно могут быть сгруппированы по критериям оценки и обоснования допустимых значений показателей, определения существенных угроз и условий, поддержки принятия решений в системной инженерии и совершенствования непосредственно самого системного анализа процесса.

Примерами первой группы задач выступают задачи оценки специальных показателей, связанных с критичными сущностями рассматриваемой системы, характеризующими ее качество. Оценки осуществляются для предотвращения ущерба и уменьшения размеров возможных негативных последствий. К таким задачам могут быть отнесены:

- задачи обработки и контроля данных о состоянии качества системы;
- построение деревьев событий, связанных с нарушением качества, прогнозированием технического состояния и выработкой планов обеспечения качества и безопасности (см., например, ГОСТ IEC 61508-3, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 56939, ГОСТ Р 57272.1, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7);
- задачи оценки прямых и косвенных экономических, экологических и социальных ущербов из-за нарушения реализации процесса управления качеством системы.

Вторую группу задач, при решении которых используются вероятностные методы, образуют задачи обоснования допустимых значений специальных показателей, связанных с критичными сущностями рассматриваемой системы, и допустимых рисков, например, допустимых рисков по показателям надежности (см., например, ГОСТ Р ИСО 13379-1, ГОСТ Р 51901.1,

[5] Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа / А. И. Костогрызов, А. В. Петухов, А. М. Щербина. М.: Изд. Вооружение. Политика. Конверсия, 1994. 278 с.; Сертификация функционирования автоматизированных информационных систем / А. И. Костогрызов, В. В. Липаев. М.: Изд. Вооружение. Политика. Конверсия, 1996. 280 с.; Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК. 150 задач анализа и синтеза и примеров их решения / М. М. Безкоровайный, А. И. Костогрызов, В. М. Львов. М.: Изд. Вооружение. Политика. Конверсия, 2002. 304 с.

[6] Костогрызов А. И., Нистратов Г. А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М.: Вооружение. Политика. Конверсия, 2005. 395 с.; Костогрызов А. И., Степанов П. В. Инновационное управление качеством и рисками в жизненном цикле систем. М.: Изд. Вооружение. Политика. Конверсия, 2008. 404 с.

ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р МЭК 61069-5).

К третьей группе могут быть отнесены задачи определения существенных угроз и условий для обеспечения качества рассматриваемой системы с использованием специальных показателей и прогнозируемых рисков. Примерами таких задач могут быть:

- задачи определения существенных факторов опасности – например, природных и человеческого факторов, факторов, связанных с новыми технологиями и несовершенством применяемых технологий;
- задачи анализа рисков нарушения качества для сложных конструкций, включая декомпозицию конструкции на составляющие элементы, детализацию и обобщение информации с учетом ее неполноты и недостоверности, выбор критериев риска, диагностика и моделирование применения конструкции во времени с учетом случайных факторов в среде эксплуатации (в нагрузках, механических воздействиях, прочности и дефектности материалов, напряженности, деформируемости и трещиностойкости как для отдельных элементов, так и для конструкции в целом), а также интерпретацию получаемых результатов диагностики и моделирования;
- задачи системной инженерии при проектировании, испытаниях и эксплуатации системы по показателям «эффективность – стоимость» [17].

К четвертой группе задач, при решении которых используются вероятностные методы, может быть отнесен комплекс задач поддержки принятия решений в системной инженерии (в части обеспечения качества системы в ее жизненном цикле). Примерами могут служить задачи обоснования требований к приемлемым условиям и мерам противодействия угрозам качеству системы по какому-либо из критериев оптимизации:

- задачи обоснования требований к приемлемым условиям и мерам противодействия угрозам качеству системы по критерию минимизации обобщенного риска нарушения реализации процесса управления качеством моделируемой системы с учетом дополнительных специфических системных требований в течение года при ограничениях на ресурсы, затраты и допустимые риски реализации отдельных существенных угроз, а также при иных корректных ограничениях;
- задачи обоснования требований к приемлемым условиям и мерам противодействия угрозам качеству системы по критерию минимизации общих затрат на реализацию кратко-, средне- и/или долгосрочных планов технического обслуживания системы при ограничениях на допустимый риск нарушения реализации процесса управления качеством моделируемой системы с учетом дополнительных специфических системных требований, а также при иных корректных ограничениях;
- комбинации перечисленных выше или иных оптимизационных задач применительно к системе или ее отдельным элементам.

Наконец, пятую группу образуют вспомогательные задач системного анализа, включающие задачи совершенствования непосредственно самого системного анализа процесса управления качеством системы. К таким задачам относятся, например:

- задачи программно-целевого планирования системного анализа процесса управления качеством системы;
- задачи оценки влияния процесса управления качеством системы на ее безопасность и эффективность;
- задачи обоснование способов повышения эффективности процесса управления качеством системы.

Степень достижения целей при решении задач системной инженерии оценивают с помощью методов формализации неопределенностей и специальных количественных показателей, которые позволяют спрогнозировать представление о возможных причинах недопустимого снижения качества системы, начиная с самых ранних этапов, когда можно успеть предпринять предупреждающие меры.

4. О формализации неопределенностей и выборе количественных показателей рисков

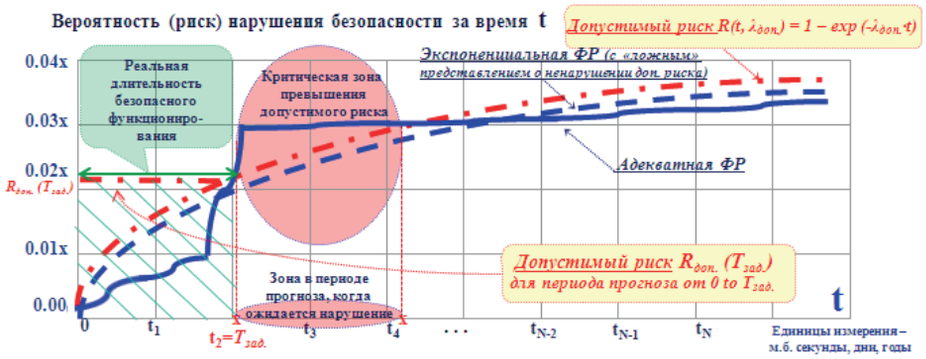
В формализации неопределенностей наивысшим достижением моделирования является построенное вероятностное пространство, позволяющее вычислять вероятность нарушения целостности системы (например, по показателям качества) за время *t*. Именно такой взгляд во многом позволяет осуществлять прогноз в системной инженерии. Если время *t* распространить на всю временную ось, то речь идет о функции распределения (ФР) времени до нарушения целостности системы. На рис. 1 проиллюстрированы ограничения к допустимым рискам, экспоненциальная и некая более адекватная ФР времени между соседними нарушениями системной целостности с одинаковой частотой нарушений $\boldsymbol{\lambda}$ (на примере нарушения безопасности) – см. подробнее[7] [2-16].

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 скудные извлекаемые знания…

Ориентируясь на более адекватную ФР (например – с помощью моделей [10-13]), если при ее создании для каждого критичного составного элемента задавались характеристики угроз и предпринимаемые меры противодействия угрозам, возможно извлечение следующих знаний:

- 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;

[7] Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности / Н. В. Абросимов, А. И. Агеев, В. В. Адушкин [и др.]; под ред. Н. А. Махутова. М.: МГОФ «Знание», 2015. 936 с.; Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Техногенная, технологическая и техносферная безопасность / Н. В. Абросимов, А. И. Агеев, Е. О. Адамов [и др.]; под ред. Н. А. Махутова. М.: МГОФ «Знание», 2018. 1016 с.



Р и с. 1. Фрагменты ФР, демонстрирующие возможные варианты зависимостей ограничений на допустимый риск, экспоненциальную и более адекватную аппроксимацию ФР

F i g. 1. Distribution function fragments demonstrating possible variants of the dependencies of the restrictions on the tolerable risk, exponential and more adequate approximation of the distribution function

- 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.

Кроме того, построив более адекватную ФР, возможно обычными расчетными методами извлечь дополнительные знания – см, например, [1; 9-16]:

- 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.

Построение и оперирование более адекватной ФР позволяет выявить и познать какие-либо закономерности в ожидаемом поведении систем и выработать логичные решения. Именно поэтому поиск новых вероятностных подходов является актуальным для системной инженерии.

Для решения задач системного анализа на практике помимо специальных показателей, связанных с критичными сущностями рассматриваемой системы (например, характеристиками качества продукции или показатели функционирования производственного оборудования, оцениваемые с использованием измерений) предлагается использовать:

- прогнозируемый риск нарушения надежности реализации процесса управления качеством системы как такового без учета дополнительных специфических системных требований;
- прогнозируемый обобщенный риск нарушения реализации процесса управления качеством системы с учетом дополнительных специфических системных требований [18; 19].

Именно для оценки прогнозируемых рисков применимы вероятностные модели и методы.

При этом под «успешностью» функционирования рассматриваемой системы в течение заданного прогнозного периода времени понимается сохранение приемлемого уровня ее качества. Под риском «неудачи» («нарушения успешного функционирования») понимается вероятностная мера «неудачи» в сопоставлении с возможными последствиями.

«Успешность» подразумевает главным образом выполнение необходимых действий процесса (1), выполнение их в срок (2) и при отсутствии недопустимого брака в поставляемых продукции и/или услугах (3). Учитывая это, риск нарушения надежности реализации процесса управления качеством системы без учета дополнительных специфических системных требований предлагается характеризовать:

- риском невыполнения необходимых действий процесса, определяемым вероятностью невыполнения необходимых действий процесса (1);
- риском нарушения сроков выполнения необходимых действий процесса, определяемым вероятностью нарушения сроков выполнения необходимых действий процесса (2);
- риском наличия недопустимого брака в поставляемых продукции и/или услугах (в том числе внутри системы для обеспечения ее качества), определяемым вероятностью наличия недопустимого брака в поставляемых продукции и/или услугах[8] (3).

Для моделируемой системы нарушение реализации процес-

[8] Вероятностные оценки обеспечивают уровень адекватности, достаточный для решения задач системного анализа, при условии многократной повторяемости анализируемых событий или в предположении такой повторяемости.

са управления качеством системы с учетом дополнительных специфических системных требований характеризуется переходом системы в такое элементарное состояние, при котором имеет место или оказывается возможным ущерб по следующим причинам: из-за невыполнения необходимых действий процесса либо из-за нарушения сроков выполнения необходимых действий, либо из-за наличия недопустимого брака в поставляемых продукции и/или услугах, либо из-за нарушения дополнительных специфических системных требований, либо из-за комбинации перечисленных причин.

Выполнение или невыполнение действий и требований процесса при моделировании отслеживается с использованием индикаторной функции , которая позволяет учесть критичность последствий, связанных с невыполнением заданных условий согласно собираемой статистике:

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

Условие α, используемое в индикаторной функции, формируют путем анализа выполнения конкретных условий.

5. Вероятностные методы для анализа рисков

Надежность реализации процесса управления качеством системы без учета дополнительных специфических системных требований представляет собой свойство процесса сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнения необходимых действий процесса с обеспечением сроков выполнения необходимых действий и качества поставляемых продукции и/или услуг (в том числе внутри системы для обеспечения ее функционирования) [20].

При проведении оценок расчетных показателей на заданный период прогноза предполагается усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для моделируемой системы или для системы, выбранной в качестве аналога. Для исследования запроектных сценариев развития угроз, связанных с нарушением качества системы, при моделировании могут быть использованы гипотетичные исходные данные.

Таким образом, используется предположение, что нарушение надежности реализации процесса управления качеством системы (т.е. «нарушение успешного функционирования» моделируемой системы) без учета дополнительных специфических системных требований является следствием невыполнения необходимых действий и/или нарушения сроков выполнения необходимых действий процесса и/или наличия недопустимого брака в поставляемых продукции и/или услугах [21; 22].

В 5.1 – 5.4 предлагаемые методы расчета риска относятся к случаю представления моделируемой системы в виде «черного ящика». В 5.5 изложены способы расчетов для сложной системы, логически представимой в виде параллельно-последовательной структуры, в которой каждый составной элемент рассмотрен как «черный ящик», в 5.6 изложен способ расчета обобщенного риска.

5.1 Расчет риска невыполнения необходимых действий процесса

В реализуемом процессе должны быть выполнены необходимые действия. Невыполнение или незавершение выполнения необходимых действий процесса управления качеством системы – это угроза возможного ущерба. С точки зрения тяжести ущерба в случае невыполнения необходимых действий процесса, поставляемые системой продукция и/или услуги (в том числе внутри системы), могут быть условно сгруппированы по *K* типам, *K ≥ 1*. В общем случае для каждого типа требования к выполнению процесса управления качеством системы формулируют на уровне инструкций должностных лиц, участвующих в реализации процесса.

При оценке риска вычисляется вероятность невыполнения необходимых действий процесса управления качеством по отдельной группе продукции и/или услуг или по всему множеству типов продукции и/или услуг в сопоставлении с возможным ущербом.

На основе применения статистических данных вероятность невыполнения необходимых действий процесса для продукции и/или услуги *k*-го типа за задаваемое время $T_{\text{зад } k}$ определяется по формуле

$$R_{\text{действий } k}(T_{\text{зад } k}) = G_{\text{наруш } k}(T_{\text{зад } k})/G_k(T_{\text{зад } k}),$$

где $G_{\text{наруш } k}(T_{\text{зад } k})$ и $G_k(T_{\text{зад } k})$ – соответственно количество случаев невыполнения необходимых действий процесса и общее количество необходимых действий процесса, подлежащих выполнению за заданное время $T_{\text{зад } k}$ для продукции и/или услуги *k*-го типа согласно статистическим данным.

Вероятность невыполнения необходимых действий процесса по всему множеству продукции и/или услуг различных типов согласно статистическим данным определяется по формулам: - для случая, когда учитывают все поставки (как с завершенным выполнением всех необходимых действий процесса, так и с их невыполнением)

$$R_{\text{действий}}(T_{\text{зад}}) = 1 - \sum_{k=1}^{K} W_k[1 - R_{\text{действий } k}(T_{\text{зад } k})] \Big/ \sum_{k=1}^{K} W_k; \quad (3)$$

- для случая, когда учитывают лишь те поставки, для которых необходимые действия процесса не были выполнены или завершены требуемым образом (именно они определяют возможные ущербы от нарушения реализации процесса):

$$R_{\text{действий}}(T_{\text{зад}}) = \quad (4)$$

$$= 1 - \sum_{k=1}^{K} W_k[1 - R_{\text{действий } k}(T_{\text{зад } k})]\ Ind_{\text{действий}}(\alpha_k) \Big/ \sum_{k=1}^{K} W_k.$$

где $\boldsymbol{T}_{\text{зад}}$ – задаваемое суммарное время на реализацию процесса для всего множества продукции и/или услуг различных типов, включающее в себя все частные значения $\boldsymbol{T}_{\text{зад } k}$ с учетом их наложений,

W_k – количество учитываемых поставок продукции и/или услуг *k*-го типа при многократных поставках.

Для продукции и/или услуг *k*-го типа учитывают требование к выполнению действий процесса с использованием индикаторной функцией $\boldsymbol{Ind}\ (\boldsymbol{\alpha}) = \boldsymbol{Ind}_{\text{действий}}(\boldsymbol{\alpha}_k)$. Индикаторная функция $\boldsymbol{Ind}\ (\boldsymbol{\alpha}) = \boldsymbol{Ind}_{\text{действий}}(\boldsymbol{\alpha}_k)$ позволяет учесть последствия, связанные с невыполнением необходимых действий процесса. Условие $\boldsymbol{\alpha}_k$ означает совокупность условий выполнения в требуемом объеме и завершения всех действий процесса при соблюдении ограничений на задаваемое время $\boldsymbol{T}_{\text{зад } k}$ для их выполнения[9].

[9] При соблюдении всех условий вероятностные оценки рисков по формулам (3), (4) совпадают.

5.2 Оценка нарушения сроков выполнения необходимых действий процесса

Каждая поставка продукции и/или услуги, осуществляемая в интересах системы (в том числе промежуточных результатов внутри системы), чтобы избежать ущербов, должна быть выполнена в приемлемые сроки. Нарушение сроков выполнения необходимых действий процесса – это угроза возможного ущерба. С точки зрения важности, срочности действий и тяжести ущерба в случае нарушения сроков выполнения необходимых действий поставляемые продукция и/или услуги могут быть условно сгруппированы по I типам, $I \geq 1$. В общем случае для каждого типа требования к своевременности поставки продукции и/или услуги формулируют в виде: срок поставки продукции и/или услуги i-го типа должен быть не более задаваемого $T_{\text{зад } i}$, $i = 1,\ldots,I$. Неприемлемость нарушения задаваемых сроков выполнения необходимых действий фиксируют в виде штрафных санкций, особых условий страхования ответственности и иных обязательств, направленных на недопущение нарушений сроков поставки в процессе управления качеством системы.

При оценке риска вычисляется вероятность нарушения сроков выполнения необходимых действий с (2) однократной и множественными поставками для разнородных продукции и/или услуг.

На основе применения статистических данных вероятность нарушения сроков выполнения необходимых действий с однократной поставкой для продукции и/или услуги i-го типа за задаваемое время $T_{\text{зад } i}$ определяется по формуле

$$R_{\text{св } i}(T_{\text{зад } i}) = N_{\text{наруш } i}(T_{\text{зад } i})/N_i(T_{\text{зад } i}),$$

где $\boldsymbol{N}_{\text{наруш } i}(\boldsymbol{T}_{\text{зад } i})$ и $\boldsymbol{N}_i(\boldsymbol{T}_{\text{зад } i})$ – соответственно количество нарушений сроков выполнения необходимых действий и общее количество необходимых действий за заданное время $\boldsymbol{T}_{\text{зад } i}$, предусматривающих поставки продукции и/или услуг i-го типа согласно статистическим данным.

Вероятность нарушения сроков выполнения необходимых действий по всему множеству поставляемых продукции и/или услуг различных типов, реализуемых в процессе согласно статистическим данным (с учетом множественности поставок, характеризуемых исходными данными по каждому из типов продукции и/или услуг), определяется по формулам:

- для случая, когда учитывают все поставки (как с выполненными, так и с нарушенными сроками выполнения необходимых действий)

$$R_{\text{св}}(T_{\text{зад}}) = 1 - \sum_{i=1}^{I} M_i[1 - R_{\text{св } i}(T_{\text{зад } i})] \Big/ \sum_{i=1}^{I} M_i; \quad (6)$$

- для случая, когда учитывают лишь те поставки, для которых сроки выполнения необходимых действий были нарушены (именно они определяют возможные ущербы от несвоевременной поставки):

$$R_{\text{св}}(T_{\text{зад}}) = 1 - \sum_{i=1}^{I} M_i[1 - R_{\text{св } i}(T_{\text{зад } i})]Ind_{\text{св}}(\alpha_i) \Big/ \sum_{i=1}^{I} M_i, \quad (7)$$

где $T_{\text{зад}}$ – задаваемое суммарное время для поставки всего множества продукции и/или услуг различных типов, включающее в себя все частные значения $T_{\text{зад } i}$ с учетом их наложений,

M_i – количество учитываемых поставок продукции и/или услуг i-го типа при многократных поставках.

Для продукции и/или услуги i-го типа учитывают требование к срокам выполнения необходимых действий с использованием индикаторной функции $Ind(\alpha) = Ind_{\text{св}}(\alpha_i)$. Индикаторная функция $Ind(\alpha) = Ind_{\text{св}}(\alpha_i)$ позволяет учесть последствия, связанные с несоблюдением сроков выполнения необходимых действий. Условие α_i означает совокупность условий по ограничениям на задаваемые сроки[10] $T_{\text{зад } i}$.

5.3. Оценка наличия недопустимого брака

При реализации каждого процесса поставляемые продукция и/или услуги должны удовлетворять требованиям по качеству. Нарушение качества поставляемой продукции и/или услуги в системе – это угроза возможного ущерба. В общем случае под выполнением требований по качеству понимают поставки продукции и/или услуг без брака или с допустимым уровнем брака, оговоренным в договорных условиях. С точки зрения нарушения качества поставляемых продукции и/или услуг и тяжести возможного ущерба поставляемые продукция и/или услуги могут быть условно сгруппированы по J типам, $J \geq 1$. В общем случае для каждого типа количественные условия к отсутствию недопустимого брака формулируются в одном из двух видов:

- условие 1: количество единиц брака в j – й поставке продукции и/или услуг $H_{\text{брака } j}(T_{\text{зад } j})$ не должно превышать задаваемого уровня $H_{\text{брака зад } j}(T_{\text{зад}j}) \geq 0$, зависящего в общем случае от объема и сроков выполнения необходимых действий $T_{\text{зад } j}$, ($j = 1,\ldots,J$). Для больших объемов поставки значение $H_{\text{брака зад } j}(T_{\text{зад } j})$ может быть по согласию заинтересованных сторон интерпретировано как количество допустимого брака в некоторых выборках;
- условие 2: допустимая вероятность брака $R_{\text{брака } j}(T_{\text{зад } j})$ в j – й поставке продукции и/или услуг не должна превышать $R_{\text{брака зад } j}(T_{\text{зад } j}) > 0$, т. е. задается максимально допустимый уровень $R_{\text{брака зад } j}(T_{\text{зад}j})$, такой чтобы $R_{\text{брака } j}(T_{\text{зад } j}) \leq R_{\text{брака зад } j}(T_{\text{зад } j})$.

Неприемлемость нарушений задаваемых ограничений фиксируется в виде штрафных санкций, особых условий страхования ответственности и иных обязательств, направленных на недопущение брака в процессе управления качеством.

При оценке риска вычисляется вероятность наличия брака при однократной и множественных поставках для разнородных продукции и/или услуг.

На основе применения статистических данных вероятность наличия брака при однократной поставке продукции и/или услуг j-го типа за задаваемое время $T_{\text{зад } j}$ определяется по формуле

$$R_{\text{брака } j}(T_{\text{зад } j}) = H_{\text{наруш}j}(T_{\text{зад } j})/H_j(T_{\text{зад } j}), \quad (8)$$

где $\boldsymbol{H}_{\text{наруш}\boldsymbol{j}}(\boldsymbol{T}_{\text{зад } \boldsymbol{j}})$ и $\boldsymbol{H}_{\boldsymbol{j}}(\boldsymbol{T}_{\text{зад } \boldsymbol{j}})$ – соответственно количество поставок с недопустимым браком и общее количество поставок за заданное время $\boldsymbol{T}_{\text{зад } \boldsymbol{j}}$ для продукции и/или услуг j-го типа согласно статистическим данным.

[10] При соблюдении всех условий вероятностные оценки рисков по формулам (6), (7) совпадают.

Вероятность наличия брака по всему множеству продукции и/или услуг различных типов, реализуемых согласно статистическим данным в процессе приобретения с учетом множественности поставок, характеризуемых исходными данными по каждому из типов продукции и/или услуг, определяется по формулам:

- для случая, когда учитывают все поставки (как с выполненными, так и с нарушенными количественными условиями по отсутствию недопустимого брака)

$$R_{\text{брака}}(T_{\text{зад}}) = 1 - \sum_{j=1}^{J} L_j[1 - R_{\text{брака } j}(T_{\text{зад } j})] / \sum_{j=1}^{J} L_j ; \quad (9)$$

- для случая, когда учитывают лишь те поставки, для которых условия по отсутствию недопустимого брака были нарушены (именно они определяют возможные ущербы от наличия брака)

$$R_{\text{брака}}(T_{\text{зад}}) = 1 - \sum_{j=1}^{J} L_j[1 - R_{\text{брака } j}(T_{\text{зад.}j})]\, Ind_{\text{брака}}(\alpha_j) / \sum_{j=1}^{J} L_j , \quad (10)$$

где $T_{\text{зад}}$ – задаваемое суммарное время поставки всего множества продукции и/или услуг различных типов, включающее в себя все частные значения $T_{\text{зад } j}$ с учетом их наложений,

L_j – количество учитываемых поставок продукции и/или услуг j-го типа при многократных поставках.

Индикаторная функция $Ind(\alpha) = Ind_{\text{брака}}(\alpha_j)$ позволяет учесть последствия, связанные с наличием брака в поставках – см. формулу (В.1). Условие α_j, используемое в индикаторной функции, формируют из договорных документов путем анализа задаваемых условий 1 или 2 к отсутствию недопустимого брака при поставках[11].

5.4. Прогнозирование риска нарушения дополнительных специфических системных требований

Прогнозирование рисков нарушения дополнительных специфических системных требований осуществляют на основе применения специальных математических моделей, учитывающих специфику системы, самих требований, а также технологий, мер и способов их выполнения. Примером специфических требований выступают требования по защите информации.

Для прогноза риска нарушения целостности системы предлагается к использованию следующая модель, формализующая технологию профилактической диагностики – см. [1], [2], [9-16], а также, например, ГОСТ Р 59341, ГОСТ Р 59347.

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[12].

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.

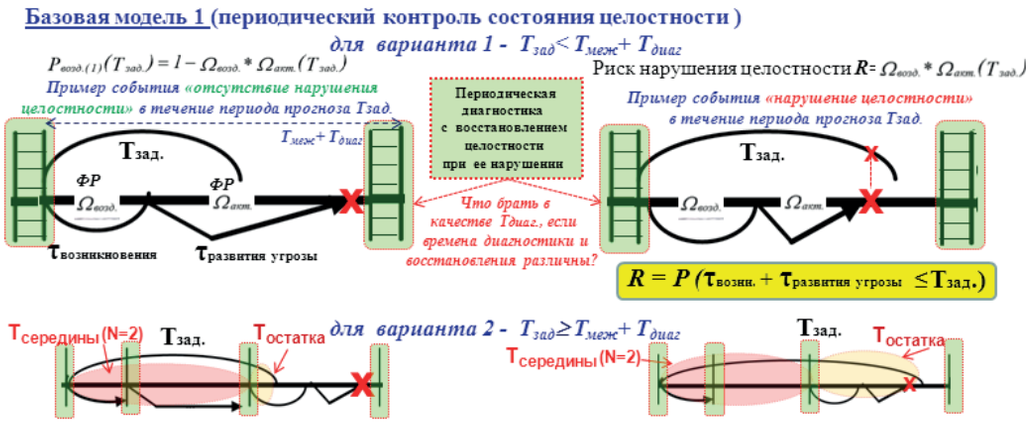
Модель позволяет оценить вероятность нарушения целостности системы в течение заданного периода времени. Именно эта вероятность определяется как риск нарушения целостности (как для системы в целом, так и для составных подсистем и элементов) в течение заданного периода прогноза с учетом предпринимаемых 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[13].

[11] При соблюдении всех условий вероятностные оценки рисков по формулам (9), (10) совпадают.

[12] 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.

[13] 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.



Р и с. 2. Формальные случаи сохранения и нарушения целостности

F i g. 2. Formal Cases of Integrity Preservation and Integrity Violation

При этом для расчета вероятностных показателей используются исходные данные, формально определяемые применительно к процессу управления качеством системы следующим образом:

σ – частота возникновения источников угроз нарушения дополнительных специфических системных требований в рассматриваемом процессе;

β – среднее время развития угроз с момента возникновения источников угроз до нарушения нормальных условий (например, до нарушения установленных дополнительных специфических системных требований в системе или до инцидента);

$T_{меж}$ – среднее время между окончанием предыдущей и началом очередной диагностики возможностей по обеспечению выполнения дополнительных специфических системных требований в моделируемой системе;

$T_{диаг}$ – среднее время системной диагностики возможностей по обеспечению выполнения дополнительных специфических системных требований;

$T_{восст}$ – среднее время восстановления нарушенных возможностей по обеспечению выполнения дополнительных специфических системных требований в моделируемой системе;

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

Расчетные показатели:

$P_{возд}$ $(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ – вероятность отсутствия нарушений дополнительных специфических системных требований в моделируемой системе в течение периода прогноза $T_{зад}$;

$\boldsymbol{R}_{наруш}$ $(\sigma, \beta, \boldsymbol{T}_{меж}, \boldsymbol{T}_{диаг}, \boldsymbol{T}_{восст}, \boldsymbol{T}_{зад})$ — вероятность нарушения дополнительных специфических системных требований в моделируемой системе в течение периода прогноза $\boldsymbol{T}_{зад}$.

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

$$R_{наруш.} = 1 - P_{возд.}, \quad (11)$$

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

Возможны два варианта:

вариант 1 – заданный оцениваемый период $T_{зад}$ меньше периода между окончаниями соседних диагностик ($T_{зад} < T_{меж} + T_{диаг}$);

вариант 2 - заданный оцениваемый период $T_{зад}$ больше или равен периоду между окончаниями соседних диагностик ($T_{зад} \geq T_{меж} + T_{диаг}$), т.е. за это время заведомо произойдет одна или более диагностик.

Для варианта 1 при условии независимости исходных характеристик вероятность $P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ отсутствия нарушений целостности в течение периода $T_{зад.}$ вычисляют по формуле (как распределение от суммы времен возникновения и инициации опасности на момент завершения периода прогноза $T_{зад}$ – см. рис. 2):

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

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 $T_{зад.}$ может быть вычислена по формуле:

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

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

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

N – число периодов между диагностиками, которые целиком вошли в пределы времени $T_{зад}$, с округлением до целого числа, $N=[T_{зад}/(T_{меж}+T_{диаг})]$ - целая часть.;

[14] Эту же формулу используют для оценки вероятности отсутствия нарушений целостности без какой-либо диагностики в предположении, что к началу $T_{зад}$ целостность системы обеспечена.

$P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж}+T_{диаг})$ – вероятность отсутствия нарушений целостности за один период между диагностиками, целиком вошедший в пределы времени $T_{зад}$, вычисляют по формуле (12);

$P_{кон}$ – вероятность отсутствия нарушений целостности после последней диагностики (в конце $T_{зад}$). С учетом доли остатка $T_{ост}=T_{зад}- N(T_{меж}+T_{диаг})$ в общем прогнозном периоде $T_{зад}$ расчет осуществляют по формуле

$$P_{кон} = \frac{T_{ост}}{T_{зад}} \cdot P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{ост}); \quad (15)$$

Значение $P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{ост})$ для остатка от задаваемого прогнозного периода вычисляют по формуле (12) с тем отличием, что вместо $T_{зад}$ стоит $T_{ост}$.

Выражение (13) логически объясняется так: нарушения, если они появляются, могут наблюдаться либо на «серединном» участке заданного прогнозного периода $T_{зад}$ (нормированный вес этого участка равен $N(T_{меж}+T_{диаг})/T_{зад}$), либо на «конечном» участке после последней диагностики целостности (нормированный вес этого участка равен $T_{ост}/T_{зад}$). При этом на обоих участках должно наблюдаться отсутствие нарушений целостности, что оценивается выражениями (14) и (15). 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 $T_{зад}/(T_{меж}+ T_{диаг})$) получаемые зависимости от $T_{зад}$ 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 $T_{зад.}$ может быть вычислена по формуле:

$$P_{возд\,(2)} = P_{серед} \cdot P_{кон}, \quad (16)$$

где вероятность отсутствия нарушений целостности в течение всех периодов между диагностиками $P_{серед}$, целиком вошедшими в $T_{зад}$, вычисляется по формуле

$$P_{серед} = P^{N}_{возд\,(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж} + T_{диаг}), \quad (17)$$

а вероятность отсутствия нарушений целостности $P_{кон}$ после последней диагностики (в конце $T_{зад}$) равна

$$P_{кон} = P_{возд\,(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{ост}). \quad (18)$$

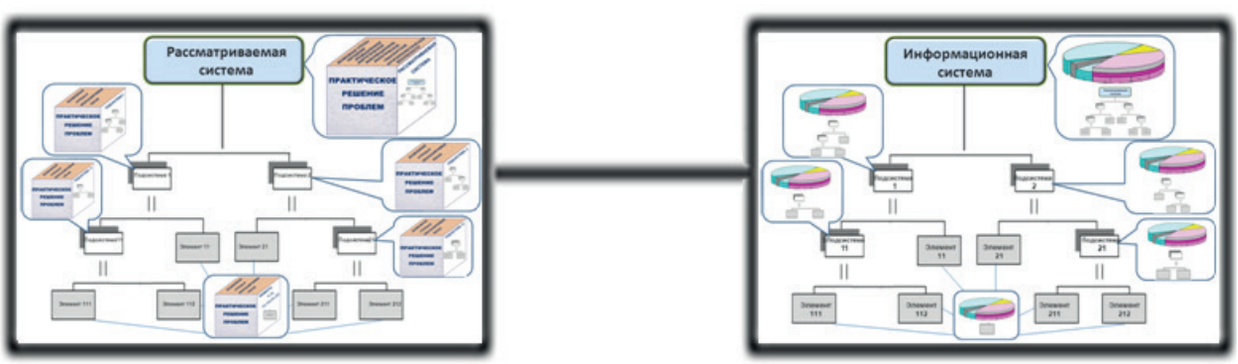
Выражение (6) логически объясняется так: для отсутствия нарушений целостности за весь период прогноза требуется отсутствие нарушений целостности на каждом из участков – будь то середина или конец периода прогноза $T_{зад}$. Достоинство этой меры в том, что при целом N сразу получается классическая функция распределения наработки на нарушение целостности для выбранной вероятностной меры. Однако, в отличие от меры (13) 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 $T_{зад.}$ определяется аналитическими выражениями (12), (13) или (16) в зависимости от варианта соотношений между исходными данными и выбранной вероятностной меры. Это позволяет вычислить по формуле (11) искомый риск нарушения целостности системы $R_{наруш.}$ в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления целостности и возможных последствий.

Расчет вероятности нарушения дополнительных специфических системных требований для процесса управления качеством системы в течение периода прогноза $\boldsymbol{R}_{наруш}(\boldsymbol{T}_{зад}) = \boldsymbol{R}_{наруш}(\sigma, \beta, \boldsymbol{T}_{меж}, \boldsymbol{T}_{диаг}, \boldsymbol{T}_{восст}, \boldsymbol{T}_{зад})$ осуществляют как дополнение до единицы значения $\boldsymbol{P}_{возд}(\sigma, \beta, \boldsymbol{T}_{меж}, \boldsymbol{T}_{диаг}, \boldsymbol{T}_{восст}, \boldsymbol{T}_{зад})$.

5.5. Расчет рисков для сложной системы

Пример декомпозиции сложной системы до составных элементов для решения поставленных проблем применительно к каждому из элементов и подсистем представлен на рис. 3. Эта декомпозиция применима также для последующего расчета интегральных показателей рисков на основе аналитического сворачивания показателей, свойственных элементам и подсистемам (см., например, ГОСТ Р 58494-2019 «Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов», ГОСТ Р 59329 – ГОСТ Р 59357-2021, посвященных решению задач защиты информации в стандартных процессах жизненного цикла систем.



Р и с. 3. Пример сложной системы, логически интегрируемой из двух сложных разнородных систем

F i g. 3. An example of a complex system logically integrated from two complex heterogeneous systems

Интеграция рассматриваемой системы может быть логически интерпретирована как объединение двух последовательно соединенных систем (подсистем или элементов). Например, слева – рассматриваемая система без учета средств автоматизации, а справа – рассматриваемая информационная система, поддерживающая функции автоматизации. Логическая интерпретация элементарных состояний такова: интегрированная система находится в состоянии «отсутствия нарушений целостности», если «И» система слева, «И» система справа находятся в состоянии «отсутствия нарушений целостности

Для сложных систем применимы методы декомпозиции и интеграции, описанные в [1], [2], [9-16], а также в ГОСТ Р 58494, ГОСТ Р 59329 – ГОСТ Р 59357.

5.6. Прогнозирование обобщенного риска

Прогнозирование обобщенного риска нарушения реализации процесса управления качеством системы с учетом дополнительных специфических системных требований $R_{\text{ообобщ}}(T_{\text{зад}})$ применяют при решении задач системного анализа – см. 3. Обобщенный риск оценивают с использованием расчетных вероятностей невыполнения необходимых действий процесса, нарушения сроков выполнения необходимых действий, наличия недопустимого брака в поставляемых продукции и/или услугах и нарушения дополнительных специфических системных требований в сопоставлении с возможным ущербом [23-25].

Вероятность $R_{\text{без}}(T_{\text{зад}})$ нарушения надежности реализации процесса управления качеством системы без учета дополнительных специфических системных требований определяются по формулам:

- для случая, когда учитываются все действия и поставки (как с выполненными, так и с нарушенными условиями по выполнению необходимых действий процесса, срокам выполнения необходимых действий, отсутствию недопустимого брака)

$$R_{\text{без}}(T_{\text{зад}}) = 1 - \{\sum_{k=1}^{K} W_k[1 - R_{\text{действий }k}(T_{\text{зад }k})] + \sum_{i=1}^{I} M_i[1 - R_{\text{св }i}(T_{\text{зад }i})] + \sum_{j=1}^{J} L_j[1 - R_{\text{брака }j}(T_{\text{зад }j})]\} \Big/ (\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i + \sum_{j=1}^{J} L_j); \quad (19)$$

- для случая, когда учитываются лишь те поставки, для которых условия по выполнению необходимых действий процесса, срокам выполнения необходимых действий, отсутствию недопустимого брака были нарушены (именно они определяют возможные ущербы от наличия брака)

$$R_{\text{без}}(T_{\text{зад}}) = 1 - \{\sum_{k=1}^{K} W_k[1 - R_{\text{действий }k}(T_{\text{зад }k})]\, Ind_{\text{действий}}(\alpha_k) + \sum_{i=1}^{I} M_i[1 - R_{\text{св }i}(T_{\text{зад }i})] Ind_{\text{св}}(\alpha_i) + \sum_{j=1}^{J} L_j[1 - R_{\text{брака }j}(T_{\text{зад }j})]\, Ind_{\text{брака}}(\alpha_j)\} \Big/ (\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i + \sum_{j=1}^{J} L_j), \quad (20)$$

где $T_{\text{зад}}$ – задаваемое общее время для выполнения всех действий, включающее в себя все частные значения $T_{\text{зад }k}$, $T_{\text{зад }i}$, $T_{\text{зад }j}$ с учетом их наложений – см. формулы (2) — (10)[15].

Обобщенная вероятность нарушения реализации процесса управления качеством системы с учетом дополнительных специфических системных требований $R_{\text{ообобщ}}(T_{\text{зад}})$ вычисляется по формуле

$$R_{\text{ообобщ}}(T_{\text{зад}}) = 1 - [1 - R_{\text{без}}(T_{\text{зад}})] \cdot [1 - R_{\text{наруш}}(T_{\text{зад}})]. \quad (21)$$

Здесь вероятность нарушения надежности реализации процесса в течение периода прогноза без учета дополнительных специфических системных требований $R_{\text{без}}(T_{\text{зад}})$ рассчитывается по формулам (19) или (20) в зависимости от целей системного анализа. Вероятность нарушения дополнительных специфических системных требований в системе в течение периода прогноза $R_{\text{наруш}}(T_{\text{зад}}) = R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$, ее рассчитывают по рекомендациям 5.5 для выбранной структуры системы при проведении системного анализа.

Обобщенный риск нарушения реализации процесса управления качеством системы с учетом дополнительных специфических системных требований определяется путем сопоставления расчетной обобщенной вероятности нарушения реализации процесса в течение периода прогноза, рассчитанной по формуле (21), с возможным ущербом за этот период.

Изложенные идеи доведены до уровня реализации в ГОСТ Р 59989 «Системная инженерия. Системный анализ процесса управления качеством системы»[16].

Заключение

Предложенные вероятностные подходы к анализу процесса управления качеством системы, позволяют оценивать риски нарушения надежности реализации процесса управления качеством системы (в т.ч. риски невыполнения необходимых действий, нарушения сроков выполнения необходимых действий процесса и/или наличия недопустимого брака в поставляемых продукции и/или услугах) без учета и с учетом дополнительных специфических системных требований.

Применение результатов расчетов позволяет повысить адекватность моделирования на уровне функции распределения до наступления во времени элементарного события – «нарушения успешного функционирования системы». За счет этого становится возможным осуществление прогнозирования рисков для критичных сущностей системы, определение существенных угроз и условий, способных при том или ином развитии событий негативно повлиять на качество рассматриваемой системы, обоснование упреждающих мер противодействия угрозам качеству рассматриваемой систем, обоснование предложений по обеспечению и повышению качества рассматриваемой системы и достижению целей системной инженерии при задаваемых ограничениях в задаваемый период времени. Изложенные идеи доведены до уровня реализации в ГОСТ Р 59989 «Системная инженерия. Системный анализ процесса управления качеством системы»[17].

[15] При соблюдении всех условий вероятностные оценки рисков по формулам (19), (20) совпадают.

[16] ГОСТ Р 59989-2022 Системная инженерия. Системный анализ процесса управления качеством системы: национальный стандарт РФ: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 17 августа 2022 г. № 769-ст.: введен впервые: дата введения 2022-11-30. М.: РСТ, 2022.

[17] Там же.

References

[1] Kostogryzov A.I., Nistratov A.A. About the Promising Directions of System Engineering Development. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = *Modern Information Technologies and IT-Education.* 2021; 17(2):223-240. (In Russ., abstract in Eng.) doi: https://doi.org/10.25559/SITITO.17.202102.223-240

[2] Kostogryzov A., Nistratov A., Nistratov G. Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds.) *Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science.* Vol. 1201. Springer, Cham; 2020. p. 352-364. (In Eng.) doi: https://doi.org/10.1007/978-3-030-46895-8_27

[3] Kostogryzov A., Panov V., Stepanov P., Grigoriev L., Nistratov A., Nistratov G. Optimization of sequence of performing heterogeneous repair work for transport systems by criteria of timeliness. *2017 4th International Conference on Transportation Information and Safety (ICTIS).* IEEE Press Banff, AB, Canada; 2017. p. 872-876. (In Eng.) doi: https://doi.org/10.1109/ICTIS.2017.8047870

[4] Kostogryzov A., Stepanov P., Grigoriev L., Atakishchev O., Nistratov A., Nistratov G. Improvement of Existing Risks Control Concept for Complex Systems by the Automatic Combination and Generation of Probabilistic Models and Forming the Storehouse of Risks Predictions Knowledge. *Proceedings of the 2nd International Conference on Applied Mathematics, Simulation and Modelling (AMSM).* DEStech Publications Inc., Phuket, Thailand; 2017. p. 279-283. (In Eng.) doi: https://doi.org/10.12783/dtetr/amsm2017/14857

[5] 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; 2000. p. 63-70. (In Eng.)

[6] Kostogryzov A.I., et al. Mathematical Models and Applicable Technologies to Forecast, Analyze, and Optimize Quality and Risks for Complex Systems. *Proceedings of the First International Conference on Transportation Information and Safety (ICTIS).* American Society of Civil Engineers, Wuhan, China; 2011. p. 845-854. (In Eng.) doi: https://doi.org/10.1061/41177(415)107

[7] Kostogryzov A., Nistratov G., Nistratov A. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management. In: Aized T. (ed.) Total Quality Management and Six Sigma. IntechOpen, London; 2012. p. 127-196. (In Eng.) doi: http://dx.doi.org/10.5772/46106

[8] Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes. *American Journal of Operations Research*. 2013; 3(1A):217-244. (In Eng.) doi: https://doi.org/10.4236/ajor.2013.31A021

[9] Artemyev V., Kostogryzov A., Rudenko J., Kurpatov O., Nistratov G., Nistratov A. Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. *2017 2nd International Conference on System Reliability and Safety (ICSRS).* IEEE Press, Milan, Italy; 2017. p. 368-373. (In Eng.) doi: https://doi.org/10.1109/ICSRS.2017.8272850

[10] Kostogryzov A., Grigoriev L., Golovin S., Nistratov A., Nistratov G., Klimov S. Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. *Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI).* DEStech Publications Inc., Beijing, China; 2018. p. 298-303. (In Eng.) doi: https://doi.org/10.12783/dtcse/cnai2018/24174

[11] Kostogryzov A., Grigoriev L., Kanygin P., Golovin S., Nistratov A., Nistratov G. The Experience of Probabilistic Modeling and Optimization of a Centralized Heat Supply System Which is an Object for Modernization. *International Conference on Physics, Computing and Mathematical Modeling (PCMM).* DEStech Publications Inc., Shanghai; 2018. p. 93-97. (In Eng.) doi: https://doi.org/10.12783/dtcse/pcmm2018/23643

[12] Artemyev V., Rudenko J., Nistratov G. Probabilistic Methods and Technologies of Risk Prediction and Rationale of Preventive Measures by Using "Smart Systems": Applications to Coal Branch for Increasing Industrial Safety of Enterprises. In: Kostogryzov A. (ed.) *Probabilistic Modeling in System Engineering.* IntechOpen, London; 2018. p. 23-51. (In Eng.) doi: http://dx.doi.org/10.5772/intechopen.75109

[13] Kershenbaum V., Grigoriev L., Kanygin P., Nistratov A. Probabilistic Modeling Processes for Oil and Gas. In: Kostogryzov A. *Probabilistic Modeling in System Engineering*. IntechOpen, London; 2018. p. 55-79. (In Eng.) doi: http://dx.doi.org/10.5772/intechopen.74963

[14] Kostogryzov A., Nistratov A., Nistratov G., Atakishchev O., Golovin S., Grigoriev L. The Probabilistic Analysis of the Possibilities to Keep "Organism Integrity" by Continuous Monitoring. *Proceedings of the 2018 International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA 2018).* Atlantis Press, Chengdu, China; 2018. p. 432-435. (In Eng.) doi: https://doi.org/10.2991/mmsa-18.2018.96

[15] Kostogryzov A., Korolev V. Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. In: Kostogryzov A., Korolev V. (eds.) *Probability, Combinatorics and Control.* IntechOpen, London; 2019. p. 3-34. (In Eng.) doi: http://dx.doi.org/10.5772/intechopen.89168

[16] Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic Predictive Modelling for Complex System Risk Assessments. In: Abdalla R., El-Diasty M., Kostogryzov A., Makhutov N.A. (ed.) *Time Series Analysis – New Insights*. London: IntechOpen; 2022. (In Eng.) doi: http://dx.doi.org/10.5772/intechopen.106869

[17] Akundi A., Lopez V. A Review on Application of Model Based Systems Engineering to Manufacturing and Production Engineering Systems. *Procedia Computer Science*. 2021; 185:101-108. (In Eng.) doi: https://doi.org/10.1016/j.procs.2021.05.011

[18] Kołowrocki K., Soszyńska-Budny J. *Reliability and Safety of Complex Technical Systems and Processes. Springer Series in Reliability Engineering.* Springer London; 2011. 405 p. (In Eng.) doi: https://doi.org/10.1007/978-0-85729-694-8

[19] Kołowrocki K., Soszyńska-Budny J. Prediction of critical infrastructures safety. *The 10th International Conference on Digital Technologies 2014.* IEEE Press; 2014. p. 130-138. (In Eng.) doi: https://doi.org/10.1109/DT.2014.6868704

[20] Zio E. An Introduction to the Basics of Reliability and Risk Analysis. World Scientific Publishing Co Pte Ltd; 2007. 236 p. (In Eng.) doi: https://doi.org/10.1142/6442

[21] Eid M., Rosato V. Critical Infrastructure Disruption Scenarios Analyses via Simulation. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds.) *Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control.* Vol. 90. Springer, Cham; 2016. p. 43-61. (In Eng.) doi: https://doi.org/10.1007/978-3-319-51043-9_3

[22] Gneiting T., Balabdaoui F., Raferty A.E. Probabilistic forecasts, calibration and sharpness. *Journal of the Royal Statistical Society. Series B (Statistical Methodology).* 2007; 69(2):243-268. (In Eng.) doi: https://doi.org/10.1111/j.1467-9868.2007.00587.x

[23] Meridji K., Issa G. A development approach of software requirements for renewable energy applications using fundamental principles of software engineering. *2013 1st International Conference & Exhibition on the Applications of Information Technology to Renewable Energy Processes and Systems.* IEEE Press; 2013. p. 107-112. (In Eng.) doi: https://doi.org/10.1109/IT-DREPS.2013.6588162

[24] Wisniewski M., Gladysz B., Ejsmont K., Wodecki A., Van Erp T. Industry 4.0 Solutions Impacts on Critical Infrastructure Safety and Protection – A Systematic Literature Review. *IEEE Access*. 2022; 10:82716-82735. (In Eng.) doi: https://doi.org/10.1109/ACCESS.2022.3195337

[25] Shah L., Siadat A., Vernadat F. Maturity assessment in risk management in manufacturing engineering. *2009 3rd Annual IEEE Systems Conference*. IEEE Press; 2009. p. 296-301. (In Eng.) doi: https://doi.org/10.1109/SYSTEMS.2009.4815815

Поступила 18.05.2022; одобрена после рецензирования 27.06.2022; принята к публикации 10.07.2022.
Submitted 18.05.2022; approved after reviewing 27.06.2022; accepted for publication 10.07.2022.

Об авторе:

Костогрызов Андрей Иванович, главный научный сотрудник, ФГУ «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (119333, Российская Федерация, г. Москва, ул. Вавилова, д. 44-2), доктор технических наук, профессор, **ORCID: https://orcid.org/0000-0002-0254-5202,** Akostogr@gmail.com

Автор прочитал и одобрил окончательный вариант рукописи.

About the author:

Andrey I. Kostogryzov, Chief Researcher, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, (44 Vavilov St., building 2, Moscow 119333, Russian Federation), Dr.Sci. (Tech.), Professor, **ORCID: https://orcid.org/0000-0002-0254-5202,** Akostogr@gmail.com

The author has read and approved the final manuscript.