

УДК 681.306 (075.32)

## **ВЕРОЯТНОСТНОЕ ПРОГНОЗИРОВАНИЕ РИСКОВ В СТАНДАРТАХ СИСТЕМНОЙ ИНЖЕНЕРИИ**

**Костогрызов А.И., Нистратов А.А.**

*Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», 119333, Россия, Москва, ул. Вавилова 44, корп.2, e-mail: Akostogr@gmail.com, Andrey.nistratov@gmail.com*

---

**Описан примерный перечень задач, для эффективного решения которых могут быть применены методы системной инженерии. Даны ссылки на типовые методы и модели, ограничения на допустимые риски и перечни методик для решения типовых задач системной инженерии. Стандартизованные методы и модели (изначально созданные и исследованные в авторских работах) предложены к использованию для вероятностного прогнозирования рисков и извлечения прагматических эффектов при решении задач обеспечения национальной безопасности.**

---

Ключевые слова: анализ, безопасность, прогнозирование, риск, система, управление.

## **PROBABILISTIC RISK PREDICTION IN SYSTEM ENGINEERING STANDARDS**

**Kostogryzov A.I., Nistratov A.A.**

*Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS), Vavilova Street 44, bld. 2, 119333 Moscow, Russia, e-mail: Akostogr@gmail.com, Andrey.nistratov@gmail.com*

---

**A list of typical tasks to be solved using system engineering method is described. References are given to standard methods and models, restrictions on admissible risks and lists of methods for solving problems of system engineering. Standardized methods and models (originally created and researched in the author's works) are proposed for use for probabilistic risks prediction and extraction of pragmatic effects in solving national security problems.**

---

Key words: analysis, control, model, prediction, risk, safety, system.

Настоящая работа посвящена краткому обзору стандартов системной инженерии, методические рекомендации которых применимы для вероятностного прогнозирования рисков при решении приоритетных задач по «Стратегии национальной безопасности РФ», утвержденной указом Президента РФ от 02.07.2021г. №400 (далее - Стратегии). Под системной инженерией понимается сосредоточение научно-технических усилий на том, как рациональным образом построить и эффективно эксплуатировать различные искусственно создаваемые системы в условиях неопределенности. Согласно ISO/IEC/IEEE 15288 и его российскому аналогу – национальному стандарту ГОСТ Р 57193 «Системная и программная инженерия. Процессы жизненного цикла систем» система определена как комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей. Примерами рассматриваемых

систем могут служить системы, создаваемые и функционирующие в интересах органов государственной власти и корпораций, энергетических, финансово-экономических, промышленных структур, топливно-энергетического комплекса, авиационно-космической отрасли, служб по чрезвычайным ситуациям, жилищно-коммунального хозяйства и пр. Тем самым понятие системы единообразно определено для исследований при решении разнородных приоритетных задач, определенных Стратегией.

Примерный перечень задач, для эффективного решения которых могут быть применены методы системной инженерии, может быть сформирован из множества приоритетных задач Стратегии [1-4] – см., например, рис. 1-2, на которых приведены практические задачи в интересах обеспечения информационной и экономической безопасности, нумерация соответствует нумерации в «Стратегии...».

СТРАТЕГИЧЕСКИЙ НАЦИОНАЛЬНЫЙ ПРИОРИТЕТ	
26.4) информационная безопасность Цель: укрепление суверенитета Российской Федерации в информационном пространстве	
<b>57. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ</b>	
1) повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования; 2) развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз; 3) предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры Российской Федерации; 4) создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий; 5) повышение защищенности и устойчивости функционирования единой сети электросвязи Российской Федерации, российского сегмента сети "Интернет", иных значимых объектов информационно-коммуникационной инфраструктуры; 6) снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений установленных российским законодательством требований по защите такой информации и персональных данных; 7) предотвращение и (или) минимизация ущерба национальной безопасности, связанного с осуществлением иностранными государствами технической разведки; 10) развитие сил и средств информационного противоборства; 12) совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления	

Рис. 1 Задачи в интересах обеспечения информационной безопасности

СТРАТЕГИЧЕСКИЙ НАЦИОНАЛЬНЫЙ ПРИОРИТЕТ	
26.5) экономическая безопасность Цели: укрепление экономического суверенитета страны, повышение конкурентоспособности российской экономики и ее устойчивости к воздействию внешних и внутренних угроз, создание условий для экономического роста Российской Федерации, темпы которого будут выше мировых	
<b>67. ЗАДАЧИ, ПОДЛЕЖАЩИЕ РЕШЕНИЮ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СИСТЕМНОЙ ИНЖЕНЕРИИ</b>	
2) сохранение макроэкономической устойчивости, обеспечение сбалансированности бюджетной системы; 5) обеспечение устойчивого развития реального сектора экономики, создание высокотехнологичных производств, новых отраслей экономики, рынков товаров и услуг на основе перспективных высоких технологий; 6) повышение производительности труда путем модернизации промышленных предприятий и инфраструктуры, цифровизации, использования технологий искусственного интеллекта, создания высокотехнологичных рабочих мест; 8) укрепление достигнутых Российской Федерацией лидирующих позиций и конкурентных преимуществ в авиационной, судостроительной, ракетно-космической промышленности, двигателестроении, атомном энергопромышленном комплексе, а также в сфере информационно-коммуникационных технологий; 15) обеспечение энергетической безопасности Российской Федерации, в том числе обеспечение устойчивого тепло- и энергоснабжения населения и субъектов национальной экономики, повышение энергетической эффективности экономики и эффективности государственного управления в сфере топливно-энергетического комплекса; 19) развитие рыночной, энергетической, инженерной, инновационной и социальной инфраструктур; 20) обеспечение развития эффективной транспортной инфраструктуры и транспортной связанности страны; 23) повышение эффективности государственной макроэкономической политики путем развития системы стратегического планирования, внедрения риск-ориентированного подхода с учетом потенциальных внешних и внутренних вызовов и угроз экономической безопасности Российской Федерации; 24) совершенствование системы государственного контроля (надзора) в сфере экономической деятельности; 32) повышение эффективности использования бюджетных средств и управления принадлежащими государству активами	

Рис. 2 Задачи в интересах обеспечения экономической безопасности

Системы для решения задач обеспечения национальной безопасности, упомянутых на

рис. 1-2 согласно Стратегии, определяются непосредственно исследователем. В общем случае прогнозирование рисков в различных приложениях при решении приоритетных задач Стратегии может быть осуществлено с учетом рекомендаций множества стандартов – например, ГОСТ ИЕС 61508-3, ГОСТ Р ИСО 2859-1, ГОСТ Р ИСО 2859-3, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 14258, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59343, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508. При проведении исследований используются вероятностные показатели для прогнозирования рисков.

Примечание. Под риском понимается сочетание вероятности нанесения ущерба и тяжести этого ущерба (по ГОСТ Р 51898–2002).

Ниже более детально рассмотрены стандарты, рекомендуемые вероятностное прогнозирование рисков применительно к нескольким стандартизованным процессам технического управления: управления рисками, управления конфигурацией, управления информацией.

Содержательной основой системного прогнозирования рисков и обоснования эффективных предупреждающих мер по снижению этих рисков или их удержанию в допустимых пределах являются вероятностные методы и модели. В этом их научно - практическая роль, к примеру, основными целями их применения могут быть:

- прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы и характеризующих ее качество и/или безопасность, включая сравнение достигаемых или прогнозируемых значений показателей с допустимым уровнем на предмет выполнения задаваемых ограничений;

- определение с использованием моделирования существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество и/или безопасность рассматриваемой системы (и/или ее элементов);

- определение и обоснование с использованием моделирования в жизненном цикле системы упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства качества и/или безопасности рассматриваемой системы (и/или ее элементов) при задаваемых ограничениях в задаваемый период прогноза;

- обоснование с использованием моделирования предложений по обеспечению и повышению качества и/или безопасности рассматриваемой системы (и/или ее элементов), включая совершенствование непосредственно самого системного анализа процесса гарантии качества для системы.

Примером прогностического моделирования процессов может служить авторский подход, разработанный в конце 90-х годов [1] и доведенный до реализации на уровне типовых требований к качеству функционирования информационных систем. Подход основан на формулировании общей цели функционирования информационных систем различного назначения, а именно – обеспечение надежного и своевременного представления полной, достоверной и конфиденциальной информации для

последующего использования.

Для прогнозирования рисков, связанных с реализацией системных процессов, и обоснования эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых пределах используют устанавливаемые качественные и количественные показатели. На практике при выполнении системных процессов помимо специальных показателей качества (например, показателей температуры, давления, производительности оборудования промышленной системы) используются показатели рисков, такие, как:

- риск нарушения надежности реализации рассматриваемого системного процесса как такового (для любого из рассматриваемых процессов соглашения, процессов организационного обеспечения проекта, процессов технического управления и технических процессов);

- риск нарушения рассматриваемого системного процесса с учетом дополнительных специфических системных требований;

- интегральный риск нарушения качества системы в течение задаваемого периода прогноза.

Примеры рекомендуемых показателей рисков, ссылки на типовые методы и модели, ограничения на допустимые риски и перечни методик для решения задач системной инженерии применительно к некоторым процессам технического управления отражены в таблице.

Вышеупомянутые в таблице модели могут быть использованы для вероятностного прогнозирования рисков и извлечения прагматических эффектов при решении задач обеспечения национальной безопасности (см. рис. 1-2) методами системной инженерии. Например, с использованием упомянутых выше вероятностных моделей и методов прогнозирования рисков могут решаться задачи определения существенных угроз и условий для обеспечения качества рассматриваемой системы с использованием специальных показателей и прогнозируемых рисков, такие, как:

- задачи определения существенных факторов опасности — например, природных и человеческого факторов, факторов, связанных с новыми технологиями и несовершенством применяемых технологий;

- задачи анализа рисков нарушения качества и безопасности 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, а также интерпретацию получаемых результатов диагностики и моделирования;

- задачи системной инженерии при проектировании, испытаниях и эксплуатации системы по показателям «эффективность — стоимость».

Кроме того, эти методы могут быть использованы для поддержки принятия решений при решении задач обеспечения национальной безопасности по Стратегии.

Примерами таковых могут служить:

- 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 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;

Таблица. Ссылки для некоторых процессов

Системный процесс. Ссылки на типовые модели, методы, допустимые риски и перечень системных методик	Вероятностные показатели риска
<p>Процесс управления рисками для системы. ГОСТ Р 59339–2021, методы, модели -приложение В; допустимые риски – приложение Д; перечень методик – приложение Е; ГОСТ Р 59991–2022, методы, модели - приложение В; допустимые риски – приложение Д; перечень методик – приложение Е</p>	<p>- для системных процессов риски по ГОСТ Р 59339–2021, 6.3 (с учетом дополнительных специфических системных требований на примере требований по защите информации); - интегральные риски нарушения качества системы в сценарных условиях комбинации используемых системных процессов в течение задаваемого периода прогноза по ГОСТ Р 59991–2022, 6.3</p>
<p>Процесс управления конфигурацией системы. ГОСТ Р 59340–2021, методы, модели - приложение В; допустимые риски – приложение Г; перечень методик – приложение Д</p>	<p>- риск нарушения надежности реализации процесса как такового (без учета дополнительных требований); - риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); - риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)</p>
<p>Процесс управления информацией системы. ГОСТ Р 59341–2021, методы, модели - приложение В; допустимые риски – приложение Д; перечень методик – приложение Е</p>	<p>- риск нарушения надежности реализации процесса как такового (без учета дополнительных требований); - риск нарушения дополнительных специфических системных требований (на примерах требований к надежности и своевременности представления, полноты и достоверности выходной информации, требований по защите информации); - риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примерах требований к надежности и своевременности представления, полноты и достоверности выходной информации, требований по защите информации)</p>

- комбинации перечисленных выше или иных оптимизационных задач применительно к системе или ее отдельным элементам.

Вышеизложенные идеи проиллюстрированы примерами решения прикладных задач в следующих стандартах системной инженерии: ГОСТ Р 58494, 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.

#### **Вместо заключения**

Описаны практические задачи, для эффективного решения которых могут быть использованы методы системной инженерии. Сами системы для решения задач обеспечения национальной безопасности определяются непосредственно исследователем.

С привязкой к некоторым стандартизованным процессам технического управления предоставлены ссылки на типовые модели, методы, допустимые риски и перечни системных методик, а также на вероятностные показатели рисков. С использованием этих ссылочных вероятностных моделей и методов прогнозирования рисков (изначально созданных и исследованных в авторских работах) приведены примеры задач, которые могут быть решены: задачи определения существенных факторов опасности, задачи анализа рисков нарушения качества и/или безопасности для сложных конструкций, задачи системной инженерии при проектировании, испытаниях и эксплуатации системы по показателям «эффективность — стоимость».

---

#### Список литературы

---

1. Костокрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем формационных систем / - М.: Изд-во ВПК, 2008. - 404 с.
2. Зацаринный А.А., Костокрызов А.И., Нистратов А.А. Приоритетные направления развития системной инженерии, предусматривающие применение риск-ориентированного подхода // Электронный научный журнал «ИТ-Стандарт». – 2021. - №4(29). – С.23-37 <https://clck.ru/34MofQ>
3. Костокрызов 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: 10.25559/SITITO.18.202202.227-240
4. Костокрызов А. И. Обзор стандартизованных риск-ориентированных методов и моделей для обеспечения гарантий качества системы // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 3. С. 483-495. doi: 10.25559/SITITO.18.202203.483-495

---

#### References

---

1. Kostogryzov A.I. Stepanov P.V. Innovative management of quality and risks in systems life cycle / - М.: Armament. Policy. Conversion, 2008 — 404p.

2. Zatsarinny A.A., Kostogryzov A.I., Nistratov A.A. Priority directions of system engineering development, providing for the use of risk-oriented approach. IT-Standard, 2021, no.4(29), pp. 23-37 clck.ru/34MofQ

3. Kostogryzov A.I. To the Methods of System Engineering: Probabilistic Approaches to the Analysis of the System Quality Management Process. Modern Information Technologies and IT-Education. 2022; 18(2):227-240. doi: [https:// doi.org/10.25559/SITITO.18.202202.227-240](https://doi.org/10.25559/SITITO.18.202202.227-240)

4. Kostogryzov A.I. The Review of Standardized Risk-Oriented Methods and Models to Ensure the Quality Assurance of the System. Modern Information Technologies and IT-Education. 2022; 18(3):483-495. doi: 10.25559/SITITO.18.202203.483-495