https://doi.org/10.25559/SITITO.021.202501.56-75
УДК 681.3.06 (075.32)

Оригинальная статья

Аналитическое обоснование противодействия угрозам в системных процессах

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 должна поддерживаться междисциплинарной теоретической основой, методами и инструментариями исследований, основанными на моделях, позволяющих лучше понимать все более сложные системы и решения по противодействию угрозам, принимаемые в условиях неопределенности. Целью настоящей работы является демонстрация аналитического подхода, основанного на применении риск-ориентированных методов, моделей и методик, рекомендованных стандартами системной инженерии.
Применение предлагаемого подхода, применимого к системам различного назначения, позволяет осуществлять:
- прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы, интерпретация и анализ приемлемости получаемых результатов, включая сравнение с допустимыми рисками;
- определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество и/или безопасность рассматриваемой системы;
- определение и обоснование в жизненном цикле системы упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства качества и/или безопасности рассматриваемой системы при задаваемых ограничениях в задаваемый период прогноза.
Подход проиллюстрирован примерами.

Ключевые слова: модель, прогнозирование, процесс, риск, система, системная инженерия

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

Для цитирования: Костогрызов А. И. Аналитическое обоснование противодействия угрозам в системных процессах // Современные информационные технологии и ИТ-образование. 2025. Т. 21, № 1. С. 56-75. https://doi.org/10.25559/SITITO.021.202501.56-75

Original article

Analytical Justification of Countering Threats in System Processes

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

Forward-looking systems engineering should be supported by an interdisciplinary theoretical framework, research methods and tools based on models that allow for a better understanding of increasingly complex systems and decisions for countering threats made under the conditions of uncertainty. The purpose of this work is to demonstrate an analytical approach based on the use of risk-oriented methods, models and techniques recommended by the standards of system engineering.
The application of the proposed approach, applicable to systems for various purposes, allows for:
- predicting the risks associated with the critical entities of the system under consideration, interpretation and analysis of the acceptability of the results obtained, including comparison with acceptable risks;
- identification of significant threats and conditions that can negatively affect the quality and/or safety of the system under consideration in one or another development of events in the system life cycle;
- definition and justification of proactive measures in the system life cycle to counter threats and conditions that ensure the desired properties of the system quality and/or safety under the consideration of specified restrictions during a specified forecast period.
The approach is illustrated by examples.

Keywords: model, prediction, process, risk, system, system engineering

Conflict of interests: The author declares no conflict of interests.

For citation: Kostogryzov A.I. Analytical Justification of Countering Threats in System Processes. *Modern Information Technologies and IT-Education.* 2025;21(1):56-75. https://doi.org/10.25559/SITITO.021.202501.56-75

1. Введение

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]. 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 определена как комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей (согласно ISO/IEC/IEEE 15288 и его российскому аналогу – национальному стандарту ГОСТ Р 57193 «Системная и программная инженерия. Процессы жизненного цикла систем»). Примерами рассматриваемых систем могут служить системы и комплексы критической информационной инфраструктуры, иные системы, создаваемые и функционирующие в интересах органов государственной власти и корпораций, энергетических, финансово-экономических, страховых и промышленных структур, топливно-энергетического комплекса (машины, механизмы, оборудование), авиационно-космической отрасли, служб по чрезвычайным ситуациям, жилищно-коммунального хозяйства и пр. Под риском понимается сочетание вероятности нанесения ущерба и тяжести этого ущерба. В общем случае решение прикладных задач обоснования противодействия угрозам, в т.ч. в информационной сфере, осуществляется с использованием количественных показателей, методов и моделей с учетом рекомендаций стандартов, рассматриваемых в настоящем обзоре, а также ГОСТ IEC 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 и др.

В общем случае для 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[1] [2-22]. Основными решаемыми задачами для применения вероятностных методов и моделей являются:

- прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы, интерпретация и анализ приемлемости получаемых результатов, включая сравнение с допустимыми рисками;
- определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество и/или безопасность рассматриваемой системы;
- определение и обоснование в жизненном цикле системы упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства качества и/или безопасности рассматриваемой системы при задаваемых ограничениях в задаваемый период прогноза.

Применение вероятностных методов и моделей позволяет построить функцию распределения (ФР) времени до нарушения качества (безопасности) системы и ее критичных элементов (при этом понятие «нарушения качества (безопасности)» должно быть определено в терминах учитываемых показателей). Ориентируясь на построенную ФР, учитывающей характеристики угроз, функции контроля и восстановления приемлемого качества (безопасности) после нарушений или обнаружения признаков возможных нарушений (например, с помощью моделей [15-18]), с использованием аналитического обоснования противодействия угрозам в системных процессах возможно извлечение знаний, позволяющих:

- рассчитать реальную зависимость вероятности нарушения качества системы и составных подсистем от характеристик разнородных угроз и предпринимаемых мер противодействия угрозам;
- оценить точность прогнозирования по сравнению с упрощенной экспоненциальной аппроксимацией ФР, учитывающей лишь частоту нарушений;
- определить период эффективного функционирования, в течение которого нарушений качества 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) и др.

Далее для аналитического обоснования противодействия угрозам в системных процессах предлагаются показатели рисков, типовые методы, модели, перечень методик и ограничения на допустимые риски. Их практическое применение иллюстрируется на примерах анализа полноты и актуальности информации в системах, обеспечивающих проведение избирательных кампаний.

[1] 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.; 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.

2. Рекомендуемые показатели рисков, типовые методы, модели, перечень методик и ограничения на допустимые риски для аналитического обоснования

На практике при выполнении системных процессов помимо специальных показателей качества (безопасности) – например, показателей температуры, давления, производительности оборудования системы – используются вероятностные показатели рисков, такие, как риск нарушения надежности реализации рассматриваемого системного процесса как такового, риск нарушения рассматриваемого системного процесса с учетом дополнительных специфических системных требований, интегральный риск нарушения качества (безопасности) системы в течение задаваемого периода прогноза. Примеры рекомендуемых показателей рисков, типовых методов, моделей, перечни методик и ограничительные ссылки на допустимые риски для решения задач системной инженерии, в т.ч. связанных с защитой информации, отражены в таблице 1.

Таблица 1. **Перечень рекомендуемых показателей рисков, типовых методов, моделей, методик и ограничений на допустимые риски**
Table 1. **A source lists of recommended risk measures, typical methods, models, techniques and acceptable risks**

Системные процессы	**Ссылки на типовые модели, методы, допустимые риски**	**Перечень системных методик для обоснования противодействия угрозам** (в частном случае: в приложении к дополнительным специфическим требованиям по защите информации)
Процессы приобретения и поставки продукции и услуг для системы	ГОСТ Р 59329–2021, методы, модели -прил. В; допустимые риски – прил. Г	ГОСТ Р 59329–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса приобретения продукции и/или услуг для системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса приобретения продукции и/или услуг для системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса приобретения продукции и/или услуг для системы. Д.7 Методика прогнозирования риска нарушения требований по защите информации в процессе поставки продукции и/или услуг для системы. Д.8 Методика прогнозирования интегрального риска нарушения реализации процесса поставки продукции и/или услуг для системы с учетом требований по защите информации. Д.9 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации . Д.10 Методики выявления явных и скрытых недостатков процесса поставки продукции и/или услуг для системы с использованием прогнозирования рисков. Д.11 Методики обоснования предупреждающих действий, направленных на достижение целей процесса поставки продукции и/или услуг для системы и противодействие угрозам нарушения требований по защите информации. Д.12 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса поставки продукции и/или услуг для системы
Процесс управления моделью жизненного цикла системы	ГОСТ Р 59330–2021, методы, модели -прил. В; допустимые риски – прил. Г; ГОСТ Р 59992–2022, методы, модели -прил. В; допустимые риски – прил. Г	ГОСТ Р 59330–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса управления моделью жизненного цикла системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления моделью жизненного цикла системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления моделью жизненного цикла системы ГОСТ Р 59992–2022, перечень методик – прил. Д Д.4 Методики обоснования допустимых рисков для задаваемой модели угроз безопасности. Д.5 Методики определения существенных недостатков процесса управления моделью жизненного цикла системы с использованием прогнозирования рисков. Д.6 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления моделью жизненного цикла системы и противодействие угрозам. Д.7 Методики обоснования предложений по совершенствованию непосредственно самого системного анализа процесса управления моделью жизненного цикла системы

Процесс управления инфраструктурой системы	ГОСТ Р 59331–2021, методы, модели -прил. В; допустимые риски – прил. Д ГОСТ Р 59993–2022, методы, модели -прил. В; допустимые риски – прил. Г	ГОСТ Р 59331–2021, перечень методик – прил. Е; Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса управления инфраструктурой системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления инфраструктурой системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления инфраструктурой ГОСТ Р 59993–2022, перечень методик – прил. Д Д.4 Методики обоснования допустимых рисков для задаваемой модели угроз безопасности (в терминах обобщенного риска нарушения реализации процесса управления инфраструктурой системы с учетом дополнительных специфических системных требований). Д.5 Методики определения существенных недостатков процесса управления инфраструктурой системы с использованием прогнозирования рисков. Д.6 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления инфраструктурой системы и противодействие угрозам. Д.7 Методики обоснования предложений по совершенствованию непосредственно самого системного анализа процесса управления инфраструктурой системы
Процесс управления портфелем проектов	ГОСТ Р 59332–2021, методы, модели -прил. В; допустимые риски – прил. Г	ГОСТ Р 59332–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты ин-формации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса управления портфе-лем проектов с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления портфелем проектов и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления портфелем проектов
Процесс управления человеческими ресурсами системы	ГОСТ Р 59333–2021, методы, модели -прил. В; допустимые риски – прил. Д	ГОСТ Р 59333–2021, перечень методик – прил. Е Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса управления человеческими ресурсами системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления человеческими ресурсами системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления человеческими ресурсами
Процесс управления качеством системы	ГОСТ Р 59334–2021, методы, модели -прил. В; допустимые риски – прил. Г ГОСТ Р 59989–2022, методы, модели -прил. В; допустимые риски – прил. Г	ГОСТ Р 59334–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса управления качеством системы с использованием прогнозируемых рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления качеством системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления качеством системы ГОСТ Р 59989–2022, перечень методик – прил. Д Д.4 Методики обоснования допустимых рисков для задаваемой модели угроз безопасности (в терминах обобщенного риска нарушения реализации процесса управления качеством системы с учетом дополнительных специфических системных требований). Д.5 Методики определения существенных недостатков процесса управления качеством системы с использованием прогнозирования рисков. Д.6 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления качеством системы и противодействие угрозам. Д.7 Методики обоснования предложений по совершенствованию непосредственно самого системного анализа процесса управления качеством системы

Процесс управления знаниями о системе	ГОСТ Р 59335–2021, методы, модели - прил. В; допустимые риски – прил. Д	ГОСТ Р 59335–2021, перечень методик – прил. Е Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса управления знаниями о системе с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления знаниями о системе и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления знаниями о системе
Процесс планирования проекта	ГОСТ Р 59336–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59336–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса планирования проекта с использованием прогнозируемых рисков. Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса планирования проекта и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса планирования проекта
Процесс оценки и контроля проекта	ГОСТ Р 59337–2021, методы, модели - прил. В; допустимые риски – прил. Г; ГОСТ Р 59990–2022, методы, модели -прил. В; допустимые риски – прил. Г	ГОСТ Р 59337–2021, перечень методик – прил. Д; ГОСТ Р 59990–2022, перечень методик – прил. Д Дополнительно к методикам, на которые сделаны ссылки в приложении Д, рекомендуется создание и применение методик, способствующих решению задач системной инженерии, в т.ч.: - методики оценки специальных показателей, связанных с критичными сущностями проекта и системы, охватываемой проектом; - методики обоснования допустимых значений специальных показателей, связанных с критичными сущностями проекта и системы, охватываемой проектом; - методики оценки интегрального риска нарушения качества, безопасности и эффективности системы, охватываемой проектом, в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза; - методики определения существенных угроз и условий для проекта с использованием специальных показателей и прогнозируемых рисков; - комплекса методик поддержки принятия решений по обеспечению качества, безопасности и эффективности системы, охватываемой проектом, в ее жизненном цикле; - методики обоснования упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства конкретных процесса, системы (и ее элементов) и проекта при задаваемых ограничениях (природных, технических, ресурсных, стоимостных, временных, социальных, экологических) в задаваемый период времени; - методики обоснования предложений по обеспечению и повышению качества, безопасности и эффективности системы, охватываемой проектом (и ее элементов); - методики решения вспомогательных задач совершенствования непосредственно системного анализа процесса оценки и контроля проекта
Процесс управления решениями	ГОСТ Р 59338–2021, методы, модели - прил. В; допустимые риски – прил. Д	ГОСТ Р 59338–2021, перечень методик – прил. Е Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса управления решениями с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления решениями и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления решениями

Процесс управления рисками для системы	ГОСТ Р 59339–2021, методы, модели -прил. В; допустимые риски – прил. Д; ГОСТ Р 59991–2022, методы, модели - прил. В; допустимые риски – прил. Д	ГОСТ Р 59339–2021, перечень методик – прил. Е, ГОСТ Р 59991–2022, перечень методик – прил. Е. Дополнительно к методикам, на которые сделаны ссылки в таблице Е, рекомендуется создание и применение методик, способствующих решению задач системной инженерии, в т.ч.: - методики оценки специальных показателей, связанных с критичными сущностями системы; - методики обоснования допустимых значений специальных показателей, связанных с критичными сущностями системы; - методики оценки интегрального риска нарушения качества системы в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза; - методики оценки интегрального риска нарушения безопасности системы в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза; - методики оценки интегрального риска нарушения эффективности системы в условиях возможных комбинаций используемых системных процессов в задаваемом периоде прогноза; - методики определения существенных угроз и условий для конкретных системных процессов, системы и/или проекта с использованием специальных показателей и прогнозируемых рисков; - комплекса методик поддержки принятия решений по обеспечению качества, безопасности и эффективности системы в ее жизненном цикле; - методики обоснования упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства конкретных процесса, системы (и ее элементов) и соответствующего проекта при задаваемых ограничениях (природных, технических, ресурсных, стоимостных, временных, социальных, экологических) в задаваемый период времени; - методики обоснования предложений по обеспечению и повышению качества, безопасности и эффективности системы (и ее элементов); - методики решения вспомогательных задач совершенствования непосредственно системного анализа процесса управления рисками для системы
Процесс управления конфигурацией системы	ГОСТ Р 59340–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59340–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса управления конфигурацией системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления конфигурацией системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления конфигурацией системы

Процесс управления информацией системы	ГОСТ Р 59341–2021, методы, модели - прил. В; допустимые риски – прил. Д	ГОСТ Р 59341–2021, перечень методик – прил. Е Е.3 Методика количественного обоснования требований к системе и необходимых условий для обеспечения надежности предоставления информации. Е.4 Методика количественного обоснования требований к системе и необходимых условий для обеспечения своевременности предоставления информации. Е.5 Методика количественного обоснования требований к системе и необходимых условий для обеспечения полноты отражения состояния всех реально существующих критичных объектов и явлений. Е.6 Методика количественного обоснования требований к системе и необходимых условий для обеспечения актуальности информации на момент ее использования. Е.7 Методика количественного обоснования требований к системе и необходимых условий для обеспечения безошибочности информации после ее контроля. Е.8 Методика количественного обоснования требований к системе и необходимых условий для получения корректных результатов обработки информации. Е.9 Методика количественного обоснования требований к системе и необходимых условий для обеспечения безошибочности действий пользователей и персонала. Е.10 Методика количественного обоснования требований к системе и необходимых условий для обеспечения отсутствия опасного программно-технического воздействия на систему в пределах допустимого риска. Е.11 Методика количественного обоснования требований к системе для обеспечения защищенности активов системы от НСД в пределах допустимого риска. Е.12 Методика количественного обоснования требований к системе для сохранения конфиденциальности информации в пределах допустимого риска. Е.13 Методика прогнозирования интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации. Е.14 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации (в терминах риска нарушения требований по защите информации и интегрального риска нарушения реализации процесса управления информацией системы с учетом требований по защите информации). Е.15 Методики выявления явных и скрытых недостатков процесса управления информацией системы с использованием прогнозирования рисков. Е.16 Методики обоснования предупреждающих мер, направленных на достижение целей процесса управления информацией системы и противодействие угрозам нарушения требований по защите информации (с использованием прогнозируемых рисков). Е.17 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса управления информацией системы (с использованием прогнозируемых рисков)
Процесс измерений системы	ГОСТ Р 59342–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59342–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса измерений системы с использованием прогнозируемых рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса измерений системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса измерений системы
Процесс гарантии качества для системы	ГОСТ Р 59343–2021 методы, модели - прил. В; допустимые риски – прил. Д; ГОСТ Р 59994–2022 методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59343–2021, перечень методик – прил. Е ГОСТ Р 59994–2022, перечень методик – прил. Д

Процесс анализа бизнеса или назначения системы	ГОСТ Р 59344–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59344–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса анализа бизнеса или назначения системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса анализа бизнеса или назначения системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса анализа бизнеса или назначения системы
Процесс определения потребностей и требований заинтересованной стороны для системы	ГОСТ Р 59345–2021, методы, модели - прил. В; допустимые риски – прил. Д	ГОСТ Р 59345–2021, перечень методик – прил. Е Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса определения потребностей и требований заинтересованной стороны для системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса определения потребностей и требований заинтересованной стороны для системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса определения потребностей и требований заинтересованной стороны для системы
Процесс определения системных требований (на примере требований по защите информации)	ГОСТ Р 59346–2021, методы, модели - приложения В, Д; допустимые риски – прил. Е	ГОСТ Р 59346–2021, методические указания – см. прил. Ж
Процесс определения архитектуры системы	ГОСТ Р 59347–2021, методы, модели - прил. В; допустимые риски – прил. Д	ГОСТ Р 59347–2021, перечень методик – прил. Е Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса определения архитектуры системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса определения архитектуры системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса определения архитектуры системы
Процесс определения проекта	ГОСТ Р 59348–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59348–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса определения проекта с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих действий, направленных на достижение целей процесса определения проекта и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса определения проекта

Процесс системного анализа	ГОСТ Р 59349–2021, методы, модели -прил. В; допустимые риски – прил. Д	ГОСТ Р 59349–2021, перечень методик – прил. Е Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемых моделей угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса системного анализа с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер для достижения целей процесса системного анализа и противодействия угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам исследований процесса системного анализа. Е.7 Методики выявлению явных и скрытых угроз нарушения надежности реализации системных процессов (по ГОСТ Р 57193) с использованием прогнозирования рисков. Е.8 Методики решения задач минимизации интегрального риска нарушения безопасности системы при кратко-, средне- и долгосрочном планировании и ограничениях (на отдельные допустимые риски реализации существенных угроз, на ресурсы, общие затраты и при иных ограничениях), учитывающих специфику системы. Е.9 Методики решения задач минимизации общих затрат на реализацию кратко-, средне- и/или долгосрочных планов при ограничениях (на интегральный риск нарушения безопасности системы, на отдельные допустимые риски реализации существенных угроз, на ресурсы и при иных ограничениях), учитывающих специфику системы
Процесс реализации системы	ГОСТ Р 59350–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59350–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса реализации системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса реализации системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса реализации системы
Процесс комплексирования системы	ГОСТ Р 59351–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59351–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз. Д.4 Методики выявления явных и скрытых недостатков процесса комплексирования системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса комплексирования системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса комплексирования системы
Процесс верификации системы	ГОСТ Р 59352–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59352–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Д.4 Методики выявления явных и скрытых недостатков процесса верификации системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса верификации системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса верификации системы
Процесс передачи системы	ГОСТ Р 59353–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59353–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз. Д.4 Методики выявления явных и скрытых недостатков процесса передачи системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса передачи системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса передачи системы

Процесс аттестации системы	ГОСТ Р 59354–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59354–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз. Д.4 Методики выявления явных и скрытых недостатков процесса аттестации системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса аттестации системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам аттестации системы
Процесс функционирования системы	ГОСТ Р 59355–2021, методы, модели - прил. В; допустимые риски – прил. Д	ГОСТ Р 59355–2021, перечень методик – прил. Е Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации (в терминах риска нарушения требований по защите информации и интегрального риска нарушения реализации процесса функционирования системы с учетом требований по защите информации). Е.4 Методики выявления явных и скрытых недостатков процесса функционирования системы с использованием прогнозирования рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса функционирования системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам функционирования системы. Е.7 Методики инструментально-расчетной оценки показателей устойчивости функционирования системы в условиях информационно-технических воздействий. Е.8 Методики обоснования способов повышения устойчивости функционирования системы в условиях информационно-технических воздействий
Процесс сопровождения системы	ГОСТ Р 59356–2021, методы, модели - прил. В; допустимые риски – прил. Д	ГОСТ Р 59356–2021, перечень методик – прил. Е Е.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз безопасности информации. Е.4 Методики выявления явных и скрытых недостатков процесса сопровождения системы с использованием прогнозируемых рисков. Е.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса сопровождения системы и противодействие угрозам нарушения требований по защите информации. Е.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса сопровождения системы
Процесс изъятия и списания системы	ГОСТ Р 59357–2021, методы, модели - прил. В; допустимые риски – прил. Г	ГОСТ Р 59357–2021, перечень методик – прил. Д Д.3 Методики обоснования допустимых рисков и нормы эффективности защиты информации для задаваемой модели угроз. Д.4 Методики выявления явных и скрытых недостатков процесса изъятия и списания системы с использованием прогнозирования рисков. Д.5 Методики обоснования предупреждающих мер, направленных на достижение целей процесса изъятия и списания системы и противодействие угрозам нарушения требований по защите информации. Д.6 Методики обоснования предложений по совершенствованию и развитию системы защиты информации по результатам системного анализа процесса изъятия и списания системы

Источник: здесь и далее в статье все таблицы и рисунки составлены автором.
Source: Hereinafter in this article all tables and figures were made by the author.

Методический подход к прогнозированию интегрального риска в сценарных условиях комбинации используемых системных процессов в течение задаваемого периода прогноза изложен в [2-22], а также приведен в ГОСТ Р 59991-2022 «Системная инженерия. Системный анализ процесса управления рисками для системы», В.4 приложения В. Интегральная вероятность сохранения качества (безопасности) системы в сценарных условиях комбинации используемых системных процессов в течение задаваемого периода прогноза вычисляется как дополнение до единицы вероятностного значения интегрального риска нарушения качества (безопасности) системы. Примеры количественного прогнозирования рисков и решения практических задач обоснования противодействия угрозам применительно к системам различного назначения приведены[2] 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.

[2] Примечание. 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 58494, 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.

Степень достижения целей при решении задач системной инженерии оценивается 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 (см. таблицу 1). Вышеизложенные идеи доведены до реализации на уровне типовых требований системной инженерии (см. ГОСТ Р 59329 – ГОСТ Р 59357, ГОСТ Р 59989 – ГОСТ Р 59994). В частности, в ГОСТ Р 59341-2021 «Системная инженерия. Защита информации в процессе управления информацией системы» предложенный подход основан на выделении и формулировании общей цели функционирования информационных систем различного назначения, а именно – обеспечение надежного и своевременного представления полной, достоверной и конфиденциальной информации для последующего использования.

Использование предложенного подхода к аналитическому обоснованию противодействия угрозам с использованием типовых методов и моделей [23-25] иллюстрируется на примерах анализа полноты и актуальности информации в системах, обеспечивающих проведение избирательных кампаний.

3. Примеры анализа полноты и актуальности информации в системах, обеспечивающих проведение избирательных кампаний

3.1 О социальной значимости качества выходной информации

При проведении избирательных кампаний сбор, обработка и передача информации базируется на широкомасштабном применении информационных технологий. Главным социальным вопросом остается доверие к результатам выборов непосредственно в день голосования и сразу после него. Для избирателей это доверие формируется на основе выходной информации о ходе и результатах выборов. Требуемое при этом качество на всех иерархических уровнях выборной системы во многом достигается за счет оперативности процессов доставки, обеспечения полноты и достоверности выходной информации (это относится к системному процессу управления информацией). Перед глазами – последние примеры обеспечения качества выходной информации о ходе и результатах второго тура выборов Президента Турции 28 мая 2023 года и Президента России 17 марта 2024 года с гласным информированием избирателей в среднем каждые 20-40 минут. Это – частные положительные примеры, но до них во всем мире было множество других примеров, где недостаточное качество информации для избирателей в день голосования служило источником социального взрыва.

Для более аргументированного ответа на вопрос о роли распределенных компьютерных и телекоммуникационных систем и сетей для обеспечения качества выходной информации о ходе и результатах выборов необходимо более детальное математическое моделирование. К сожалению, для приложений к выборным технологиям при наличии множества разнородных неопределенностей целенаправленных количественных оценок качества выходной информации практически нет (за некоторыми исключениями – см., например[3]).

Именно количественному анализу таких свойств качества выходной информации, как полнота и актуальность, применительно к системам, обеспечивающим проведение избирательных кампаний непосредственно в день выборов и при подсчете результатов выборов, посвящены нижеследующие исследования в 3.2 – 3.4.

3.2 Основные понятия, принятые положения и допущения

В примерах приняты следующие положения и допущения, касающиеся достижения цели обеспечения оперативности доставки, полноты и достоверности выходной информации о ходе и результатах выборов.

Оперативность доставки информации измеряется временем обработки бюллетеней и доведения соответствующей информации о ходе и результатах выборов до избирателей. По сравнению с ручным пересчетом бюллетеней время обработки и доведения выходной информации до избирателей объективно сокращается на порядки – до нескольких минут. По этой причине целевые эффекты, связанные с повышением оперативности доставки информации за счет применения распределенных компьютерных и телекоммуникационных систем и сетей, представляются очевидными и в работе используются лишь в контексте формирования исходных данных для математического моделирования.

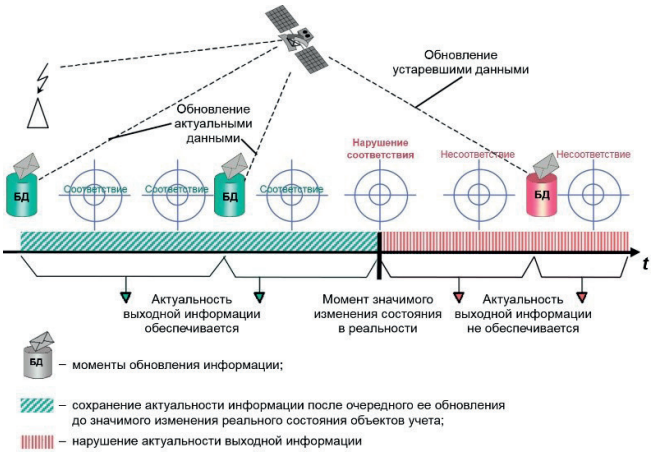
Все последующие определения адаптированы из ГОСТ Р 59341-2021, смысл других терминов, не раскрываемых ниже, сохранен согласно этому стандарту.

Под полнотой выходной информации понимается свойство предоставляемой избирателям информации отражать состояния всех впервые появляющихся фактов и объектов учета предметной области системы (например, о готовности избирательных комиссий, об открытии участков, о первых нарушениях в ходе выборов, о признании выборов состоявшимися, о первых результатах голосования и др.). Каждый случай неполноты выходной информации становится предметом особого внимания, ведь тем самым нарушается необходимая степень доверия избирателей к выборам. Здесь неопределенность заключается в наступлении моментов первого появления фактов и объектов учета предметной области системы, времени подготовки, доведения и отражения соответствующей информации в базах данных (БД) системы.

Под достоверностью выходной информации в примерах понимается свойство периодически обновляемой в БД и подлежащей доведению до избирателей выходной информации отражать реальные состояния хода выборов (по количеству проголосовавших, по количеству нарушений и пр.), промежу-

[3] 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.; 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.

точных и окончательных результатов голосования (по количеству набираемых голосов), изменяемых во времени в ходе голосования и при подсчете количества бюллетеней за кандидатов. Достоверность выходной информации определяется корректностью обработки заполненных бюллетеней, безошибочностью при хранении и передаче соответствующей информации и сохранением ее актуальности на момент использования. Под актуальностью выходной информации понимается свойство обновляемой информации, корректно обработанной из заполненных бюллетеней и подлежащей доведению до избирателей, отражать текущее состояние хода выборов и результатов выборов с соблюдением согласованности с объективной реальностью. Рассогласование реальной и хранимой в БД информации вызвано устареванием информации в результате какого-либо значимого изменения до следующего обновления этого изменения в БД – см. рис. 1, формально иллюстрирующий пространство элементарных событий при моделировании с использованием “Модели для оценки актуальности обновляемой информации” согласно приложению В.3.5 из ГОСТ Р 59341-2021.



Р и с. 1. Иллюстрация формирования актуальности выходной информации

F i g. 1. Illustration of the formation of the relevance of output information

Актуальность выходной информации для избирателей обеспечивается путем достаточно быстрого и непротиворечивого отражения в БД объективно имевших место значимых изменений информации о ходе выборов и результатов выборов с учетом технических задержек в используемых распределенных компьютерных и телекоммуникационных системах. Оперирование неактуальной информацией в системе может быть воспринято избирателями как обман или необоснованные затяжки времени для подделки результатов голосования, вызвать недоверие к выборам и послужить источником социального взрыва. При этом вполне обоснованно можно полагать, что безошибочность входной информации из заполненных бюллетеней и корректность обработки бюллетеней обеспечиваются в результате применения на избирательных участках специальных комплексов автоматической обработки избирательных бюллетеней. Благодаря использованию самими избирателями этих комплексов осуществляется автоматический подсчет голосов, устраняются ошибки ручного подсчета голосов и предотвращаются попытки фальсификации итогов голосования. Также не без оснований полагается, что безошибочность выходной информации при ее хранении и передаче достигается применением современных компьютерных технологий обеспечения информационной безопасности. Неопределенность заключается в наступлении моментов значимого изменения состояния объектов учета в реальности, времени подготовки, доведения и отражения соответствующей информации в БД системы.

С учетом вышеизложенного из свойств, характеризующих качество выборных технологий, как наиболее критичные выбраны свойства полноты и актуальности выходной информации. Понимая, что реальные распределенные компьютерные и телекоммуникационные системы, обеспечивающие проведение избирательных кампаний, имеют сложную сетевую структуру, в настоящей работе принято следующее допущение. В целях анализа полноты и актуальности выходной информации система, обеспечивающая проведение избирательных кампаний, рассматривается как черный ящик. Сетевая структура учитывается лишь путем формирования временных исходных данных для математического моделирования.

Далее оценим функциональные возможности некоторой гипотетичной автоматизированной системы (АС), структурно представляющей собой многоуровневую территориально-распределенную систему комплексов средств автоматизации центральной избирательной комиссии (ЦИК), десятков избирательных комиссий субъектов, сотен окружных, тысяч территориальных и десятков тысяч участковых избирательных комиссий. К примеру, в ГАС «Выборы» России насчитывается более 96 тысяч участковых избирательных комиссий. Исследуемая АС может выступать как некая система-аналог для многих реальных систем, обеспечивающих проведение избирательных кампаний. Для расчетов используются модели для оценки полноты и актуальности информации, отраженные в работах[4] [2], [5], [9-11], а также в ГОСТ Р 59341-2021, в котором эти модели реализованы.

3.3 Оценка полноты выходной информации

Используемая «Модель для оценки полноты оперативного отражения в системе новых объектов и явлений» приложения В.3.4 из ГОСТ Р 59341-2021 позволяет оценить вероятность обеспечения полноты выходной информации в БД системы. Искомая вероятность вычисляется в предположении пуассоновского потока моментов появления новых фактов и объектов учета. В качестве исходных данных используется частота появления новых фактов и объектов учета в день выборов и при подсчете результатов выборов и среднее время подготовки, передачи и ввода новых объектов учета в БД.

[4] Там же.
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.

При оценке полноты речь идет о новых фактах и объектах учета – это может быть информация о готовности республиканских, окружных, территориальных и участковых избирательных комиссий, об открытии участков, о деятельности избирательных комиссий, о предполагаемой фальсификации, о принуждении к участию в голосовании, о ходе выборов, о предварительных результатах голосования и др. Пример собираемых данных (об обращениях избирателей), отображаемых на табло коллективного пользования и характеризующих полноту выходной информации в БД АС приведен на рис. 2.

Р и с. 2. Пример собираемых данных, характеризующих полноту выходной информации в БД АС

F i g. 2. An example of collected data characterizing the completeness of output information in the Automated System Database

Пусть в период выборов на одном избирательном участке в среднем 1 раз в 2 часа происходит новое важное событие, информация о котором должна быть доведена до сведения вышестоящей избирательной комиссии для принятия решения. В свою очередь, на более высокий уровень передается лишь 10% всех сообщений, поступающих от подчиненных избирательных комиссий. Остальные 90 % сообщений разрешаются в первой же более высокой инстанции. Пусть до внедрения АС на подготовку данных уходило в среднем 15 минут (печать поступивших документов на печатной машинке), на передачу (с помощью телеграмм, телефонограмм, факса) – 5 минут, прием и доведение до ЦИК – 2 минуты. В АС подготовка сократилась до 1 минуты, передача – до 3 секунд и доведения до БД ЦИК – 30 секунд. Требуется оценить степень повышения полноты выходной информации в БД АС по сравнению с неавтоматизированным режимом.

Результаты расчетов показали, что за счет внедрения АС вероятность обеспечения полноты выходной информации в БД повысится на уровне территориальных избирательных комиссий с 0.002 до 0.65, на уровне окружных избирательных комиссий с 10^{-6} до 0.34, на уровне избирательных комиссий субъектов с 0.003 до 0.66. Из-за большого количества избирательных участков информация на уровне ЦИК окажется неполной с вероятностью, близкой к 1. Неполнота будет иметь место по 3-7 объектам учета из нескольких десятков. Но избиратель привык к такой неполноте. Надо признать, что на практике из-за многоминутных задержек полнота выходной информации о ходе выборов в вероятностном выражении будет объективно низкой даже с использованием высокопроизводительных компьютерных систем. И это – нормальный результат для условий, когда неполнота не является некритичной.

Для полученных результатов оценки дальнейшее противодействие угрозам нарушения полноты оперативного отражения в системе новых объектов и явлений (по сравнению с неавтоматизированным режимом) представляется излишним, но результаты расчетов следует учесть при анализе актуальности выходной информации в АС на момент ее предоставления избирателям.

3.4 Анализ актуальности выходной информации

Используемая «Модель для оценки актуальности обновляемой информации» (приложения В.3.5 из ГОСТ Р 59341-2021) позволяет оценить вероятность сохранения актуальности выходной информации в системе на момент ее предоставления избирателям Ракт при задаваемых: среднем времени между значимыми изменениями состояния объекта учета (ξ); среднем времени подготовки информации (ω); среднем времени передачи информации (δ); среднем времени ввода информации в БД (β); дисциплине обновления в информации в системе (D). $D=D_1$ означает, что сбор информации в системе происходит «сразу по происшествии значимого изменения» состояния объектов учета. $D=D_2$ означает, что сбор происходит вне явной

зависимости от изменения состояний объектов учета. Для случая D=D2 дополнительно задается среднее время (q) между обновлениями информации

Для начала оценим актуальность информации о количестве проголосовавших, отображаемой на табло коллективного пользователя ЦИК АС в ходе выборов. Пример собираемых данных (о количестве проголосовавших), отображаемых на табло коллективного пользования и характеризующих актуальность выходной информации в БД АС в ходе выборов приведен на рис. 3.

Р и с. 3. Пример собираемых данных, характеризующих актуальность выходной информации в БД АС

F i g. 3. An example of collected data characterizing the relevance of output information in the Automated System Database

Положим, что значимые для выборов изменения происходят 1 раз в час, регламент сбора информации от избирательных участков составляет также 1 раз в час, время подготовки данных в АС – 3 минуты, время передачи от избирательных участков до ЦИК с учетом обобщения в вышестоящих округах – 10-15 минут, а время ввода в БД с учетом контроля – 5 минут. Согласно результатам моделирования вероятность того, что на табло ЦИК отражается актуальная информация о количестве проголосовавших, равна 0.35-0.58 (т.к. на практике могут быть отступления от регламент сбора информации). Таким образом, собранные данные на момент отображения существенно устаревают. Может показаться удивительным, но, похоже, из-за отсутствия необходимости высокой точности количества проголосовавших более высокая актуальность и не требуется. Она требуется лишь в случае недобора необходимого минимума проголосовавших для признания выборов состоявшимися.

Дальнейший анализ проведен уже в приложении к информации о результатах выборов, когда скорость нужна не только для понимания «кто побеждает», но и для отсутствия социально критичных подозрений о подтасовке результатов выборов. Автоматизация процесса подсчета и регистрации голосов позволяет обновлять информацию в режиме реального времени. Пример предварительных итогов голосования, отображаемых на табло коллективного пользования и характеризующих актуальность выходной информации в БД АС, приведен на рис. 4 (иллюстрирует вариант формы представления объекта оценки при моделировании).

Р и с. 4. Пример предварительных итогов голосования, характеризующих актуальность выходной информации в БД АС

F i g. 4. An example of preliminary voting results characterizing the relevance of the output information in the Automated System Database

Пусть на подготовку сообщения о промежуточных результатах уходит 5 минут, на передачу данных от избирательного участка через всю цепочку иерархии 10-15 минут, на контроль и ввод данных – 5 минут. На рис. 5 представлен пример результатов голосования в другой форме представления объекта оценки, нежели на рис. 4, это – то, что видит избиратель. Положим в качестве допустимой вероятности сохранения актуальности выходной информации уровень 0.7, что эквивалентно установлению допустимого риска нарушения актуальности информации на уровне 0.3 (0.3=1–0.7). Это вполне обосновано с учетом предыдущих исследований в 3.3, 3.4. Тогда реально могут быть аналитически обоснованы следующие действенные меры противодействия угрозам устаревания отображаемой информации во время голосования. На рис. 6 – результаты моделирования в обобщенном виде, т.е. то, что избиратель не видит, доверяя разработчикам АС в вопросах противодействия угрозам качеству потребляемой информации, в частности в том, что выходная информация в БД сохраняет свою актуальность на момент ее вывешивания на табло коллективного пользования. Именно эти расчетные результаты характеризуют аналитические усилия по обеспечению требуемой актуальности отображаемых итогов выборов (поскольку эти итоги и являются главной востребованной выходной информацией для избирателей).

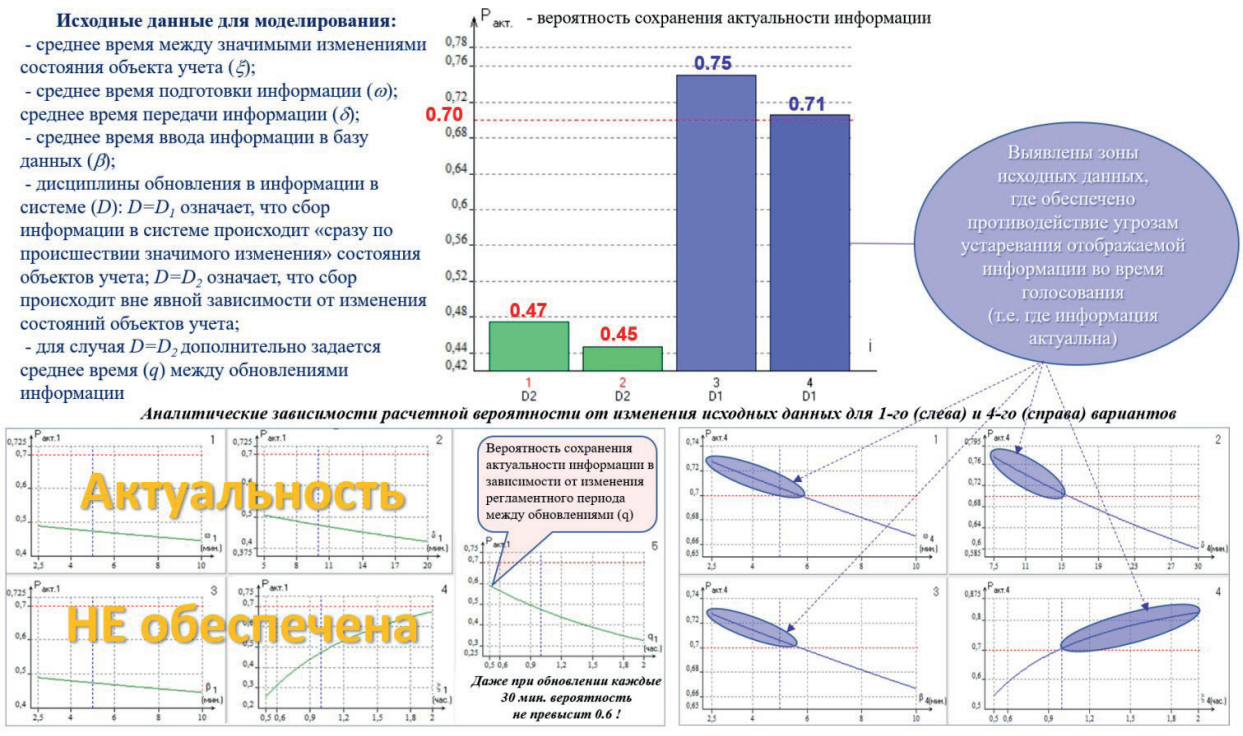
Обобщенные результаты расчетов показывают, что регламентный сбор информации (т.е. дисциплина D2, i = 1,2) существенно хуже по сравнению со сбором «сразу по изменении» (дисциплина D1, i = 3,4). Более того, при регламентном сборе информации от источников с периодом от 30 минут и более вероятность сохранения актуальности выходной информации для избирателей не будет обеспечена никогда (см. зависимости на рис. 6 внизу слева при изменении исходных данных в диапазоне -50% - +100%). Повышения актуальности с достижимого уровня 0.70-0.75 до более высокого уровня можно добиться, если от участковых избирательных комиссий результаты будут направлены в оригинале по иерархии, и одновременно – непосредственно в ЦИК (технически это возможно).

ВЫБОРЫ 19 СЕНТЯБРЯ 2021

ДИСТАНЦИОННОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ – РЕЗУЛЬТАТЫ ГОЛОСОВАНИЯ
ВЫБОРЫ ДЕПУТАТОВ ГОСУДАРСТВЕННОЙ ДУМЫ ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ВОСЬМОГО СОЗЫВА

	Курская область	Мурманская область	Нижегородская область	Ростовская область	Ярославская область	Город Севастополь
1. Политическая партия "КОММУНИСТИЧЕСКАЯ ПАРТИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ"	6 491	5 476	18 446	24 502	11 754	1 754
2. Политическая партия "Российская экологическая партия "ЗЕЛЁНЫЕ"	788	1 193	2 268	3 631	1 850	814
3. Политическая партия ЛДПР – Либерально-демократическая партия России	4 376	4 654	9 634	19 586	6 103	1 793
4. Политическая партия "НОВЫЕ ЛЮДИ"	5 365	5 352	10 563	14 209	8 104	1 399
5. Всероссийская политическая партия "ЕДИНАЯ РОССИЯ"	21 893	18 789	50 003	186 052	31 855	10 016
6. Партия СПРАВЕДЛИВАЯ РОССИЯ – ЗА ПРАВДУ	3 211	4 691	12 915	11 488	14 589	1 560
7. Политическая партия "Российская объединенная демократическая партия "ЯБЛОКО"	358	615	1 931	2 925	1 411	143
8. Всероссийская политическая партия "ПАРТИЯ РОСТА"	245	316	1 510	1 496	495	83
9. Политическая партия РОССИЙСКАЯ ПАРТИЯ СВОБОДЫ И СПРАВЕДЛИВОСТИ	427	569	1 013	1 797	861	131
10. Политическая партия КОММУНИСТИЧЕСКАЯ ПАРТИЯ КОММУНИСТЫ РОССИИ	711	658	1 380	2 353	1029	112
11. Политическая партия "Гражданская Платформа"	284	125	151	273	141	19
12. Политическая партия ЗЕЛЕНАЯ АЛЬТЕРНАТИВА	663	971	1 599	2 535	1 018	266
13. ВСЕРОССИЙСКАЯ ПОЛИТИЧЕСКАЯ ПАРТИЯ "РОДИНА"	299	356	1 050	2 698	547	144
14. ПАРТИЯ ПЕНСИОНЕРОВ	1 843	2 230	3 612	4 313	1 989	387
ВСЕГО	46 954	45 995	116 075	277 858	81 746	18 621

Р и с. 5. Пример результатов голосования (то, что видит избиратель)
F i g. 5. Example of voting results (what the voter sees)



Р и с. 6. Аналитические зависимости для выявления действенных мер противодействия угрозам сохранения актуальности выходной информации (то, что избиратель не видит, полагаясь на разработчиков АС)
F i g. 6. Analytical dependencies for identifying effective measures to counter threats to maintaining the relevance of output information (what the voter does not see, relying on the AS developers)

Так будет улучшена «прозрачность» выборов, доверие к их результатам будет повышено, избиратели смогут в режиме реального времени наблюдать актуальную информацию. При этом выявлены зоны исходных данных, где обеспечено противодействие угрозам устаревания отображаемой информации во время голосования (т.е. где информация актуальна). Так, для 4-го варианта (см. рис. 6 внизу справа) при неизменных остальных исходных данных допустимое среднее время подготовки информации (ω_4) может составлять от 2.5 до 5.5 минут, допустимое среднее время передачи информации (δ_4) – от 7.5 до 15 минут, допустимое среднее время ввода информации в БД (β_4) – от 2.5 до 5.5 минут, но при этом среднее время между значимыми реальными изменениями состояния объектов учета (ξ_4) не должно быть менее 1 часа. Для других исходных данных результаты моделирования будут иными.

3.5 Некоторые выводы по примерам

Проведенный анализ влияния современных информационных технологий на качество выходной информации в системах, обеспечивающих проведение избирательных кампаний, показал следующее:

- по сравнению с неавтоматизированным голосованием вероятность обеспечения полноты выходной информации в БД в день голосования повысится до уровня 0.34-0.66. Из-за большого количества избирательных участков информация на уровне ЦИК окажется неполной с вероятностью, близкой к 1 (т.е. в масштабах системы отображаемая информация оказывается заведомо неполной). На первый несистемный взгляд может показаться странным, но такой невысокий вероятностный уровень полноты информации в БД, отображаемый на табло, имеет смысл признать приемлемым, т.к. выше не только не достижимо, но и не нужно, поскольку человек привык адаптироваться к подобным условиям неполноты используемой им информации (т.е. для выборных технологий рассмотренный показатель полноты информации для избирателя имеет глубоко второстепенное значение);
- отображаемая на табло ЦИК информация о количестве проголосовавших в период между обновлениями оказывается актуальной с вероятностью 0.35-0.58 (на практике более высокая актуальность и не требуется);
- вероятность сохранения актуальности выходной информации на табло ЦИК о результатах выборов («кто побеждает») может достигать уровня 0.70-0.75. Повышения актуальности до более высокого уровня можно добиться, если от участковых избирательных комиссий результаты будут направлены в оригинале по иерархии, и одновременно – непосредственно в ЦИК. Похоже, уровень 0.7 – это разумный допустимый уровень, достижимый применительно к современным АС. Требовать уровень вероятности «соответствия реальности» 0.999 (сравнимого с показателями надежности) – это неразумно и технически недостижимо, а с учетом ментального восприятия избирателями такой высокий уровень просто не требуется.

Заключение

Предложен аналитический подход к обоснованию противодействия угрозам в системных процессах, основанный на применении риск-ориентированных методов, моделей и методик, рекомендованных стандартами системной инженерии. Применение подхода к системам различного назначения позволяет осуществлять:

- прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы, интерпретация и анализ приемлемости получаемых результатов, включая сравнение с допустимыми рисками;
- определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество и/или безопасность рассматриваемой системы;
- определение и обоснование в жизненном цикле системы упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства качества и/или безопасности рассматриваемой системы при задаваемых ограничениях в задаваемый период прогноза.

Использование предложенного подхода проиллюстрировано на примерах анализа полноты и актуальности информации в системах, обеспечивающих проведение избирательных кампаний (применительно к процессу управления информацией согласно ГОСТ Р 59341-2021).

Список использованных источников

[1] Костогрызов А. И., Нистратов А. А. О приоритетных направлениях развития системной инженерии. Современные информационные технологии и ИТ-образование. 2021. Т. 17, № 2. С. 223-240. 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 // Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science ; ed. by V. Sukhomlin, E. Zubareva. Vol. 1201. Cham: Springer, 2020. P. 352-364. https://doi.org/10.1007/978-3-030-46895-8_27

[3] Костогрызов 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. https://doi.org/10.25559/SITITO.18.202203.483-495

[4] Костогрызов А. И., Нистратов А. А. Вероятностное прогнозирование рисков в стандартах системной инженерии // ИТ-Стандарт. 2023. № 1(34). С. 4-10. EDN: ZMRLUM

[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). Dallas, USA: Engineering and Technical Management Symposium, 2000. P. 63-70.

[6] 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 / A. Kostogryzov [et al.] // Proceedings of the 2nd International Conference on Applied Mathematics, Simulation and Modelling (AMSM). Phuket, Thailand: DEStech Publications Inc.; 2017. P. 279-283. https://doi.org/10.12783/dtetr/amsm2017/14857

[7] Akundi A., Lopez V. A Review on Application of Model Based Systems Engineering to Manufacturing and Production Engineering Systems // Procedia Computer Science. 2021. Vol. 185. P. 101-108. https://doi.org/10.1016/j.procs.2021.05.011

[8] Kołowrocki K., Soszyńska-Budny J. Modeling Reliability and Safety of Multistate Systems with Ageing Components // Reliability and Safety of Complex Technical Systems and Processes. Springer Series in Reliability Engineering. London: Springer, 2011. P. 1-52. https://doi.org/10.1007/978-0-85729-694-8_1

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

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

[11] Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes / A. Kostogryzov [et al.] // American Journal of Operations Research. 2013. Vol. 3, no. 1A. P. 217-244. https://doi.org/10.4236/ajor.2013.31A021

[12] Kołowrocki K., Soszyńska-Budny J. Prediction of critical infrastructures safety // The 10th International Conference on Digital Technologies 2014. Zilina, Slovakia: IEEE Press, 2014. P. 130-138. https://doi.org/10.1109/DT.2014.6868704

[13] Zio E. An Introduction to the Basics of Reliability and Risk Analysis. World Scientific Publishing Co Pte Ltd, 2007. 236 p. https://doi.org/10.1142/6442

[14] Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems / V. Artemyev, A. Kostogryzov [et al.] // 2017 2nd International Conference on System Reliability and Safety (ICSRS). Milan, Italy: IEEE Press, 2017. P. 368-373. https://doi.org/10.1109/ICSRS.2017.8272850

[15] Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space / A. Kostogryzov, L. Grigoriev [et al.] // Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI). Beijing, China: DEStech Publications Inc., 2018. P. 298-303. https://doi.org/10.12783/dtcse/cnai2018/24174

[16] The Experience of Probabilistic Modeling and Optimization of a Centralized Heat Supply System Which is an Object for Modernization / A. Kostogryzov [et al.] // International Conference on Physics, Computing and Mathematical Modeling (PCMM). Shanghai: DEStech Publications Inc., 2018. P. 93-97. https://doi.org/10.12783/dtcse/pcmm2018/23643

[17] 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 // Probabilistic Modeling in System Engineering ; ed. by A. Kostogryzov. London: IntechOpen; 2018. p. 23-51. http://dx.doi.org/10.5772/intechopen.75109

[18] Kershenbaum V., Grigoriev L., Kanygin P., Nistratov A. Probabilistic Modeling Processes for Oil and Gas // Probabilistic Modeling in System Engineering ; ed. by A. Kostogryzov. London: IntechOpen, 2018. P. 55-79. http://dx.doi.org/10.5772/intechopen.74963

[19] The Probabilistic Analysis of the Possibilities to Keep „Organism Integrity" by Continuous Monitoring / A. Kostogryzov [et al.] // Proceedings of the 2018 International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA 2018). Chengdu, China: Atlantis Press, 2018. P. 432-435. https://doi.org/10.2991/mmsa-18.2018.96

[20] Kostogryzov A., Korolev V. Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems // Probability, Combinatorics and Control ; ed. by A. Kostogryzov, V. Korolev. London: IntechOpen, 2019. P. 3-34. http://dx.doi.org/10.5772/intechopen.89168

[21] 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. https://doi.org/10.25559/SITITO.18.202202.227-240

[22] Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic Predictive Modelling for Complex System Risk Assessments // Time Series Analysis – New Insights ; ed. by R. Abdalla, M. El-Diasty, A. Kostogryzov, N.A. Makhutov. London: IntechOpen, 2022. P. 73-105. http://dx.doi.org/10.5772/intechopen.106869

[23] Намиот Д. Е., Ильюшин Е. А. О киберрисках генеративного Искусственного Интеллекта // International Journal of Open Information Technologies. 2024. Т. 12, № 10. С. 109-119. EDN: JZCUQS

[24] Костогрызов А. И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии // Вопросы кибербезопасности. 2022. № 6(52). С. 71-82. https://doi.org/10.21681/2311-3456-2022-6-71-82

[25] Kostogryzov A., Avdonin R., Nistratov A. Methodical rationale of system solutions to reduce risks and retain them within acceptable limits for knowledge management process // Reliability: Theory & Applications. 2022. Vol. 17, no. 4. P. 50-64. https://doi.org/10.24412/1932-2321-2022-471-50-64

Поступила 14.12.2024; одобрена после рецензирования 21.02.2025; принята к публикации 13.03.2025.

Об авторе:

Костогрызов Андрей Иванович, Заслуженный деятель науки Российской Федерации, 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.

References

[1] Kostogryzov A.I., Nistratov A.A. About the Promising Directions of System Engineering Development. *Modern Information Technologies and IT-Education*. 2021;17(2):223-240. (In Russ., abstract in Eng.) 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 Scienc*e. Vol. 1201. Cham: Springer; 2020. p. 352-364. https://doi.org/10.1007/978-3-030-46895-8_27

[3] 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. (In Russ., abstract in Eng.) https://doi.org/10.25559/SITITO.18.202203.483-495

[4] Kostogryzov A.I., Nistratov A.A. Probabilistic Risk Prediction in System Engineering Standards. *IT-Standard*. 2023;(1):4-10. (In Russ., abstract in Eng.) EDN: ZMRLUM

[5] Kostogryzov A. I. Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ). In: Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA). Dallas, USA: Engineering and Technical Management Symposium; 2000. p. 63-70.

[6] 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. In: Proceedings of the 2nd International Conference on Applied Mathematics, Simulation and Modelling (AMSM). Phuket, Thailand: DEStech Publications Inc.; 2017. p. 279-283. https://doi.org/10.12783/dtetr/amsm2017/14857

[7] 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. https://doi.org/10.1016/j.procs.2021.05.011

[8] Kołowrocki K., Soszyńska-Budny J. Modeling Reliability and Safety of Multistate Systems with Ageing Components. In: Reliability and Safety of Complex Technical Systems and Processes. *Springer Series in Reliability Engineering*. London: Springer; 2011. p. 1-52. https://doi.org/10.1007/978-0-85729-694-8_1

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

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

[11] 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. https://doi.org/10.4236/ajor.2013.31A021

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

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

[14] 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. In: 2017 2nd International Conference on System Reliability and Safety (ICSRS). Milan, Italy: IEEE Press; 2017. p. 368-373. https://doi.org/10.1109/ICSRS.2017.8272850

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

[16] 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. In: International Conference on Physics, Computing and Mathematical Modeling (PCMM). Shanghai: DEStech Publications Inc.; 2018. p. 93-97. https://doi.org/10.12783/dtcse/pcmm2018/23643

[17] 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: Ed. by Kostogryzov A. Probabilistic Modeling in System Engineering. London: IntechOpen; 2018. p. 23-51. http://dx.doi.org/10.5772/intechopen.75109

[18] Kershenbaum V., Grigoriev L., Kanygin P., Nistratov A. Probabilistic Modeling Processes for Oil and Gas. In: Ed. by Kostogryzov A. Probabilistic Modeling in System Engineering. London: IntechOpen; 2018. p. 55-79. http://dx.doi.org/10.5772/intechopen.74963
[19] 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. In: Proceedings of the 2018 International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA 2018). Chengdu, China: Atlantis Press; 2018. P. 432-435. https://doi.org/10.2991/mmsa-18.2018.96
[20] 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. London: IntechOpen; 2019. p. 3-34. http://dx.doi.org/10.5772/intechopen.89168
[21] 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. (In Russ., abstract in Eng.) https://doi.org/10.25559/SITITO.18.202202.227-240
[22] 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. (eds.) Time Series Analysis – New Insights. London: IntechOpen; 2022. p. 73-105. http://dx.doi.org/10.5772/intechopen.106869
[23] Namiot D.E., Ilyushin E.A. On Cyber Risks of Generative Artificial Intelligence. *International Journal of Open Information Technologies*. 2024;12(10):109-119. (In Russ., abstract in Eng.) EDN: JZCUQS
[24] Kostogryzov A.I. On models and methods of probabilistic analysis of information security in standardized processes of system engineering. *Voprosy kiberbezopasnosti* = Cybersecurity issues. 2022;(6):71-82. (In Russ., abstract in Eng.) https://doi.org/10.21681/2311-3456-2022-6-71-82
[25] Kostogryzov A., Avdonin R., Nistratov A. Methodical rationale of system solutions to reduce risks and retain them within acceptable limits for knowledge management process. *Reliability: Theory & Applications*. 2022;17(4):50-64. https://doi.org/10.24412/1932-2321-2022-471-50-64

Submitted 14.12.2024; approved after reviewing 21.02.2025; accepted for publication 13.03.2025.

About the author:

Andrey I. Kostogryzov, Honored Scientist of the Russian Federation, 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.