ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ РОССИЙСКОЙ АКАДЕМИИ НАУК

На правах рукописи

НИСТРАТОВ ГЕОРГИЙ АНДРЕЕВИЧ

МОДЕЛИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ КОНТРОЛЯ, МОНИТОРИНГА И ПОДДЕРЖАНИЯ ЦЕЛОСТНОСТИ В ЖИЗНЕННОМ ЦИКЛЕ СИСТЕМ

Автореферат диссертации
на соискание ученой степени кандидата технических наук
по специальности 05.13.17 «Теоретические основы информатики»

Научный руководитель:
член-корреспондент РАН
доктор технических наук
Соколов И.А.

Москва - 2007

Работа выполнена в Институте проблем информатики Российской Академии наук

Научный руководитель: член-корреспондент РАН,
доктор технических наук
Соколов Игорь Анатольевич

Официальные оппоненты: доктор технических наук, профессор,
заслуженный деятель науки РФ
Синицын Игорь Николаевич

кандидат физико-математических наук,
доцент Ищук Владимир Андреевич

Ведущая организация: Федеральное государственное унитарное предприятие «Центр информационных технологий и систем органов исполнительной власти» (ФГУП «ЦИТиС»)

Защита состоится « 22 » февраля 2007 г. в 16 часов 00 минут на заседании диссертационного совета Д002.073.01 в Институте проблем информатики РАН по адресу: 119333, г. Москва, ул. Вавилова, д.44, корп. 2

Отзыв на автореферат, заверенный печатью организации, просим направлять по вышеуказанному адресу.

С диссертацией можно ознакомиться в библиотеке Института проблем информатики РАН.

Автореферат разослан « 20 » января 2007 г.

Ученый секретарь диссертационного совета
доктор технических наук,
профессор

С.Н. Гринченко

Практика показывает, что из-за наличия различного рода угроз, сложности логической архитектуры и невозможности полной проверки программного обеспечения в компьютерных системах всегда присутствуют остаточные риски негативного развития событий. Под системой согласно ГОСТ Р ИСО/МЭК 15288 «Информационная технология (ИТ). Системная инженерия. Процессы жизненного цикла систем» понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей. Как следствие различного рода угроз и повышения технической сложности снижается качество функционирования систем, например, из-за ненадежности программно-технических средств, ненадлежащего выполнения функций человеком, несанкционированного изменения, копирования программ и данных, нарушения своевременности доступа к ним легальных пользователей и др. Под качеством функционирования системы согласно ГОСТ 15457 понимается совокупность ее потребительских свойств. Одним из необходимых условий управления качеством являются контроль и мониторинг состояний и принятие мер по поддержанию целостности системы, т.е. такого ее состояния, при котором обеспечивается достижение целей функционирования. Сегодня эффективность мер по управлению качеством функционирования систем от циркулирующей информации, принимаемых системных решений и их реализаций. Центральное место в системах занимают информационные процессы (ИП) контроля, мониторинга и поддержания целостности. Обоснование рациональных значений параметров ИП базируется на использовании теоретических основ информатики. Однако, степень теоретической проработки вопросов оценки и обеспечения эффективности ИП оказывается недостаточной для разрешения возникающих практических проблем. Так, в настоящее время Главные конструктора руководствуются в работе положениями стандартов ГОСТ Р ИСО 9001 «Системы менеджмента качества. Требования», ГОСТ 34.602 «ИТ. КСАС. Техническое задание на создание автоматизированной системы», ГОСТ РВ 51987 «ИТ. КСАС.

Типовые требования и показатели качества функционирования информационных систем. Общие положения» и др., согласно которым заказчики и разработчики систем должны использовать данные реализуемых ИП, определять критерии и методы, необходимые для обеспечения результативности и качества, осуществлять мониторинг, измерение, анализ и совершенствование протекающих процессов. Однако, в отличие от моделей надежности технических средств (рекомендуемых в стандартах), несмотря на логическую идентичность выполняемых функций ИП контроля, мониторинга и поддержания целостности, унифицированного методического аппарата их анализа, применимого к системам различного функционального назначения, не существует.

К концу 80-х годов прошлого века основные научные исследования в области качества были направлены на улучшение надежностных и вероятностно-временных показателей функционирования систем, снижение вероятности ошибки на один знак, развитие концептуальных основ обеспечения защищенности электронно-вычислительной техники от несанкционированного доступа (НСД) и характеризовали лишь отдельные важные аспекты, определяющие эффективность реализуемых ИП. Углубление научных основ обеспечения качества стало осуществляться с жестким учетом области функционального приложения систем (в частности, отдельно для АСУ технологическими процессами, АСУ предприятием с конкретной специализацией и др.). К началу 90-х годов стало очевидным, что реальное повышение эффективности ИП должно базироваться на всестороннем обеспечении качества информации, циркулирующей в системе. Созданию и практической реализации такой концепции предшествовали глубокие теоретические исследования в информатике, относящиеся к области качества информации. С появлением современных ИТ семантическое содержание систем стали определять информационные системы (ИС). В отличие от технологических систем, результатом функционирования которой могут быть конкретные действия (например,

выполнение функций робототехническими системами, управляемыми с борта космического корабля) либо какая-либо материальная продукция (например, тепло, поставляемое в дома в системе жилищно-коммунального хозяйства), входными данными и выходным результатом функционирования ИС является нематериальная информация, от качества которой зависит последующая эффективность системы в целом. Вопросы многосторонней оценки качества функционирования информационных систем, в т.ч. реализуемых в них ИП, рассматривались в работах В.А.Балыбердина, Г.В.Дружинина, В.А.Ищука, В.Ю.Королева, К.К.Колина, А.И.Костогрызова, В.В.Кульбы, В.В.Липаева, И.А.Мизина, А.П.Печинкина, И.Н.Синицына, И.А.Соколова, В.Г.Ушакова и др. В данных работах предложены теоретические подходы к методам анализа функционирования сложных систем и безопасности информации, обрабатываемой в них. Созданные модели доведены до уровня требований стандартов ГОСТ 34.602 и ГОСТ РВ 51987, однако, не в полной мере охватывают современные процессы жизненного цикла в системной инженерии (например, по ГОСТ Р ИСО/МЭК 15288). Сегодня налицо противоречие между возросшими практическими потребностями в необходимости всемерного повышения качества (в т.ч. безопасности) функционирования систем и сложившимися теоретическими возможностями информатики в удовлетворении этих потребностей за счет оптимизации реализуемых ИП. Именно необходимость разрешения этого противоречия путем обнаружения и прагматического использования новых знаний о возможностях системы по итогам моделирования ИП в жизненном цикле обусловливает **актуальность** работы.

Настоящая диссертационная работа посвящена решению **научной задачи** обоснования рациональных значений параметров ИП контроля, мониторинга и поддержания целостности в жизненном цикле систем. **Целью** исследований является повышение степени научно-методической обоснованности значений параметров ИП контроля, мониторинга и поддержания целостности в жизненном цикле систем.

Основными результатами, выносимыми на защиту, являются:

модели ИП контроля, мониторинга и поддержания целостности систем и их программная реализация в комплексах «Проектирование архитектуры» и «Анализ безопасности» (свидетельство Роспатента № 2004610858);

методика оценки эффективности ИП контроля, мониторинга и поддержания целостности систем;

методика обоснования рациональных значений параметров ИП контроля, мониторинга и поддержания целостности, организационно-технических мер и управляющих воздействий в жизненном цикле систем.

Научная новизна работы состоит:

в предложении оригинальных математических и программных моделей для оценки эффективности ИП контроля, мониторинга и поддержания целостности систем по интегральным показателям качества и безопасности их функционирования (без программной реализации применение предложенных математических моделей оказывается практически невозможным ввиду их высокой алгоритмической сложности);

в выработке методического подхода к обоснованию рациональных значений параметров ИП контроля, мониторинга и поддержания целостности в жизненном цикле систем.

Практическая значимость работы состоит:

в возможности практического использования предложенных моделей и методик для систем различных областей приложения (проиллюстрировано на примерах для корпоративной информационной системы, робототехнических систем и автоматизированной системы обеспечения жизнедеятельности космонавта, системы теплоснабжения г.Жуковский Московской области, подтверждено актами реализации);

в использовании комплексов для научно-исследовательских и опытно-конструкторских работ (акты 3 ЦНИИ Минобороны РФ и ЦНИИ машиностроения), в учебном процессе для проведения лабораторных работ, подготовки курсовых, дипломных работ студентами старших курсов по

специализации «Стандартизация, моделирование и сертификация» в РГУ нефти и газа им. И.М.Губкина и «Безопасность информации» в МИЭМ (подтверждено актами реализации).

Достоверность и обоснованность полученных результатов, выводов и рекомендаций обусловлена корректностью применения теоретических основ информатики, теории вероятностей, теории регенерирующих процессов, математической статистики и методов системного анализа для построения моделей и методик, а также совпадением в частных случаях полученных формул с существующими (в частности, вероятности безотказного функционирования по ГОСТ 27.301-96 и вероятности отсутствия опасного воздействия на систему по ГОСТ РВ 51987) и совпадением полученных результатов моделирования с результатами статистических экспериментов и применения других вспомогательных моделей в ходе испытаний систем.

Результаты работы реализованы:

в эскизном и техническом проектах по созданию корпоративной информационной системы;

в отчетах о НИР, связанных с анализом ИП и систем по требованиям качества и безопасности функционирования, анализом робототехнических систем и автоматизированной системы обеспечения жизнедеятельности космонавта, оптимизацией системы теплоснабжения г.Жуковский Московской области;

в учебных курсах «Стандартизация, моделирование и сертификация» в РГУ нефти и газа им. И.М.Губкина и «Безопасность информации» в МИЭМ .

Апробация работы осуществлялась на образцах сложных систем различного назначения и подтверждена актами реализации 3 ЦНИИ Минобороны России, ЦНИИ машиностроения (г.Королев), теплоэнергетической компании ЗАО "ИНГРАС-М", РГУ нефти и газа им. Губкина, МИЭМ. Программные комплексы представлялись на отечественных и международных научно-технических форумах в России, Германии, Италии, Люксембурге, Украине. Комплекс «Проектирование

архитектуры» был отмечен в конкурсе «Дебют года» почетной грамотой РАН и Федерального агенства по информационным технологиям по результатам выставки «Softool-2005». Математические и программные модели используются для лабораторных работ и расчетов курсовых, дипломных работ и диссертаций в РГУ нефти и газа им. И.М.Губкина, МИЭМ и ряде других учебных заведений.

Работа состоит из введения, 3-х разделов и заключения.

В первом разделе проведен анализ требований системообразующих международных и отечественных стандартов, проанализировано влияния ИП на качество и безопасность функционирования систем. Выявлено, что ИП контроля и мониторинга занимают центральное место и играют ключевую роль в оперативном определении готовности компонентов систем к выполнению своих функций. В совокупности с мерами анализа, принятия решений и своевременными организационно-техническими мерами и управляющими воздействиями по поддержанию целостности они являются главными компонентами управления функционированием системы, определяющими ее качество (или безопасность, как одно из важных составных свойств качества, имеющих самостоятельное значение). Предложены следующие интегральные вероятностно-временные показатели для оценки эффективности ИП:

на уровне качества функционирования системы: наработка на нарушение приемлемого качества и вероятность обеспечения приемлемого качества системы в течение заданного периода времени;

на уровне безопасности: среднее время безопасного функционирования как показатель стойкости системы к реализации угроз и вероятность обеспечения ее безопасного функционирования в течение заданного периода времени.

В завершение раздела на основе анализа существующих методов оценки эффективности систем сформулирована научная задача обоснования рациональных значений параметров ИП контроля, мониторинга и

поддержания целостности в жизненном цикле систем. Научная задача формализована (см. рис.1) как задача определения таких значений параметров ИП, организационно-технических мер и управляющих воздействий, на которых достигается минимум затрат при ограничениях на минимально допустимый уровень эффективности ИП (на этапах концепции и ТЗ, проектирования и разработки, производства и сопровождения) или максимум эффективности ИП при ограничениях на затраты (в процессе эксплуатации).

На этапах концепции и ТЗ, проектирования и разработки, производства и сопровождения системы	**В процессе эксплуатации системы**
1.1) в приложении к качеству $Z_{созд.}(Q_{рац.}) = \min_{Q} Z_{созд.}(Q)$ при ограничениях $P_{кач.} \geq P_{доп.}$ и $C_{экспл.} \leq C_{доп.}$ 1.2) в приложении к безопасности $Z_{созд.}(Q_{рац.}) = \min_{Q} Z_{созд.}(Q)$ при ограничениях $P_{безоп.} \geq P_{доп.}$ и $C_{экспл.} \leq C_{доп.}$	2.1) в приложении к качеству $T_{(с\ обсл.)}(Q_{рац.}) = \max_{Q} T_{(с\ обсл.)}(Q)$ или $P_{кач.}(Q_{рац.}) = \max_{Q} P_{кач.}(Q)$ при ограничениях $C_{экспл.} \leq C_{доп.}$ 2.2) в приложении к безопасности $T_{(стойкость)}(Q_{рац.}) = \max_{Q} T_{(стойкость)}(Q)$, или $P_{безоп.}(Q_{рац.}) = \max_{Q} P_{безоп.}(Q)$ при ограничениях $C_{экспл.} \leq C_{доп.}$

Рис. 1 Формальная постановка научной задачи

Обозначения: в приложении к качеству $Q(S, T_{восст.}, T_{зад.}, T_{к\ ухудш.}, T_{к\ наруш.}, T_{к\ между}, C_{к\ экспл.})$ и безопасности $Q(S, T_{восст.}, T_{зад.}, Ч_{угроз}, T_{к\ стойкость}, T_{к\ монитор}, T_{к\ между}, C_{к\ экспл.})$ – характеристики ИП, орг.-технические меры и управляющие воздействия по результатам реализации ИП; $T_{зад}$ - заданный период для оценки; $Z_{созд.}$ - затраты на создание системы; $P_{кач.}$ ($P_{безоп.}$) - достигаемый уровень качества (безопасности); $C_{экспл}$ - затраты на эксплуатацию; $T_{(с\ обсл.)}$ - наработка на нарушение приемлемого качества; $Ч_{угроз}$ – частота возникновения угроз системе; $T_{стойкость}$ – стойкость системы к реализации угроз

При этом окончательный выбор интегрального показателя должен быть сделан заказчиком с учетом специфики создаваемой или эксплуатируемой системы. Варьируемыми параметрами ИП, организационно-технических мер и управляющих воздействий предложены:

<u>системные характеристики:</u> S – логическая структура архитектурного построения системы; $T_{восст.}$ – время восстановления системы; $T_{зад.}$ – задаваемый период для оценки; $P_{доп.}$ - задаваемый допустимый уровень вероятности обеспечения приемлемого уровня качества (безопасности);

<u>характеристики к-го компонента системы:</u> $T_{к\ ухудш.}$ – наработка на ухудшение функционирования с начала эксплуатации или момента

восстановления; $T_{к\ наруш.}$ – наработка на нарушение приемлемого качества с начала ухудшения функционирования; $T_{к\ стойкость}$ – стойкость меры к реализации угроз (среднее время); $T_{к\ монитор.}$ – наработка на ошибку средств мониторинга; $T_{к\ между}$ – период между моментами контроля приемлемого качества или безопасности; $C_{к\ экспл.}$ – затраты на обеспечение функционирования.

Существо нынешнего и предлагаемого подходов к использованию ИП контроля, мониторинга и поддержания целостности систем отражен в таблице 1.

Таблица 1

Существующий подход	Предлагаемый подход
1. Не ставится цели использования ИП для управления качеством (в т.ч. безопасностью) на всех этапах жизненного цикла (ЖЦ) систем 2. Как следствие – ИП реализуются на стадии эксплуатации системы для сбора данных о ее текущем состоянии и экстраполяции отслеживаемых характеристик системы в целях динамического управления **Вывод:** несмотря на логическую идентичность и ключевую роль в обеспечении качества и безопасности, отсутствуют модели, позволяющие количественно оценивать в жизненном цикле эффективность ИП по системным показателям, обосновывать рациональные значения параметров и уровни допустимых рисков	1. Осуществлять сбор тех данных, которые позволят оценивать эффективность ИП по единым системным показателям с учетом области функционального приложения 2. На всех этапах жизненного цикла систем различного назначения решать оптимизационные задачи для обеспечения эффективности планируемых и реализуемых ИП. Получаемые оценки использовать для обоснования уровня приемлемых рисков по «прецедентному принципу» **Предлагается:** использовать скрытый потенциал реализуемых ИП для целенаправленного обнаружения новых знаний о возможностях систем и эффективных способах повышения их качества и безопасности

Во втором разделе предложено развитие существующих моделей для анализа интегральных показателей. Разработаны математические модели ИП контроля, мониторинга и поддержания целостности систем и составных компонентов. Основная идея в построении моделей ИП состоит в следующем. Путем комбинации существующих моделей надежности (не учитывающих возможностей управления процессами контроля, мониторинга и поддержания целостности, но позволяющих проведение комплексных оценок для сложных структур), защищенности от опасных программно-технических воздействий и мониторинга безопасности систем (учитывающих влияние контроля, мониторинга и поддержания целостности, но не

позволяющих проведение комплексных оценок) осуществлено создание нового комплекса математических моделей для ИП, позволяющего выявлять новые знания на уровне предложенных интегральных показателей. В качестве комбинируемых выбраны следующие модели.

1. Модель для оценки надежности из ГОСТ 27.301 и ГОСТ РВ 51987 (Модель…1). Для системы из одного элемента при экспоненциальной аппроксимации распределений исходных характеристик и их независимости вероятность надежного представления информации $P_{над}$ в течение $T_{зад}$:

$$P_{над} = \frac{T_{нар}^{2}}{(T_{вос}+T_{нар})(T_{зад}+T_{нар})},$$

где $T_{нар}$ – среднее время наработки системы на отказ
$T_{вос}$ – среднее время восстановления системы после отказа
$T_{зад}$ – задаваемый период надежного функционирования системы

Для сложной системы использованы следующие результаты для функции распределения независимых случайных величин:

.Последовательное соединение	Параллельное соединение
$P(t) = P(\min(\tau_1, \tau_2) \le t) = 1 - P(\min(\tau_1, \tau_2) > t) =$ $1 - P(\tau_1 > t)\, P(\tau_2 > t) = 1 - [1-P_1(t)]\,[1-P_2(t)]$	$P(t) = P(\max(\tau_1, \tau_2) \le t) = P_1(\tau_1 \le t)\, P_2(\tau_2 \le t) =$ $= P_1(t)\, P_2(t)$

Это позволяет осуществлять расчеты для сложных последовательно-параллельных структур. При этом сделанное предположение об экспоненциальности времени с начала эксплуатации или момента восстановления всей системы до нарушение приемлемого качества аналогично предположению о пуассоновости общего потока событий (от различных компонентов), приводящих к нарушению приемлемого качества. Для сложной структуры системы этот общий поток нарушений представляет собой сумму большого числа потоков от множества компонентов. Интенсивность каждого из слагаемых потоков мала по сравнению с интенсивностью суммарного потока – в такой ситуации действует предельная теорема В. Григолиониса, согласно которой суммарный поток будет пуассоновским.

2. Модель для оценки защищенности системы от опасных программно-технических воздействий из ГОСТ РВ 51987 (Модель …2). Для варианта $T_{зад} < T_{меж} + T_{диаг}$ вероятность отсутствия опасного воздействия в течение времени $T_{зад.}$:

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

Для варианта $T_{зад} \geq T_{меж} + T_{диаг}$: $P_{возд(2)} = P_{серед} + P_{кон}$, где $P_{серед}$ – вероятность отсутствия опасного воздействия в течение всех серединных периодов между диагностиками, целиком вошедшими в $T_{зад,}$, $P_{кон}$ – вероятность отсутствия опасного воздействия в течение последней диагностики (в конце $T_{зад}$)

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

где σ^{-1} –наработка на ухудшение функционирования (в модели обозначается как $1/T_{к\ ухудш.}$ для оценки качества) или частота возникновения угроз системе ($Ч_{угроз}$ для оценки безопасности); β –наработка на нарушение приемлемого качества с начала ухудшения функционирования ($T_{к\ наруш.}$ для оценки качества) или стойкость меры к реализации угроз ($T_{к\ стойкость}$ – для оценки безопасности); $T_{меж}$ –период между моментами восстановления; $T_{диаг}$ – длительность диагностики, включая восстановление целостности, в модифицированной «Модели…2» учтено в $T_{меж}$; $T_{зад}$ –задаваемый период для оценки, N – число периодов между диагностиками, которые целиком вошли в пределы времени $T_{зад}$, с округлением до целого.

3. Модель мониторинга безопасности системы (Модель…3, [1]).

Для варианта $T_{зад.} < T_{меж.} + T_{диаг.}$ вероятность отсутствия опасных воздействий в течение периода $T_{зад.}$ при независимости исходных характеристик:

$$P_{возд.(1)}(T_{зад.}) = 1 - \int_{0}^{T_{зад.}} dA(\tau) \int_{0}^{T_{зад.}-\tau} d\,\Omega_{возд.} * \Omega_{акт.}(\theta). \qquad * \text{ - знак свертки,}$$

Для варианта $T_{зад.} \geq T_{меж.} + T_{диаг.}$

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

где $N = \lfloor T_{зад.}/(T_{меж.} + T_{диаг.}) \rfloor$ - целая часть, $T_{ост.} = T_{зад.} - N(T_{меж.} + T_{диаг.})$

Здесь $\Omega_{возд.}(t)$ - ФР времени между воздействиями на систему с целью внедрения источника опасности, для эксп. ФР $\Omega_{возд.}(t) = 1 - exp(-\sigma t)$, σ – частота воздействий; $\Omega_{акт.}(t)$ - ФР времени активизации источника опасности после его проникновения в систему, для эксп. ФР $\Omega_{акт.}(t) = 1 - exp(-t/\beta)$, β – среднее время активизации источника опасности; $A(t)$ - ФР времени наработки системы мониторинга на ошибку, для эксп. ФР $A(t) = 1 - e^{-t/Tнар}$, $T_{нар.}$ – среднее.

Суть логики предлагаемого расчета интегральных показателей для сложных структур в условиях потенциальных угроз с увеличенной (за счет поддержания целостности) наработкой мониторируемых элементов

отражена на рис. 2. В итоге для созданных «Модели…4» (программа «Анализ проекта архитектурного построения системы») предложен методический алгоритм расчета наработки на нарушение приемлемого качества и вероятности обеспечения приемлемого качества в течение заданного периода времени (см. рис.3), а для «Модели…5» («Анализ комплексной безопасности») - алгоритм расчета стойкости системы к реализации угроз и вероятности обеспечения безопасности функционирования системы в течение заданного периода времени (см. рис. 4). Приведено обоснование адекватности предложенных моделей.

Рис. 2 Суть логики предлагаемого расчета интегральных показателей для сложных структур в интересах повышения качества функционирования систем

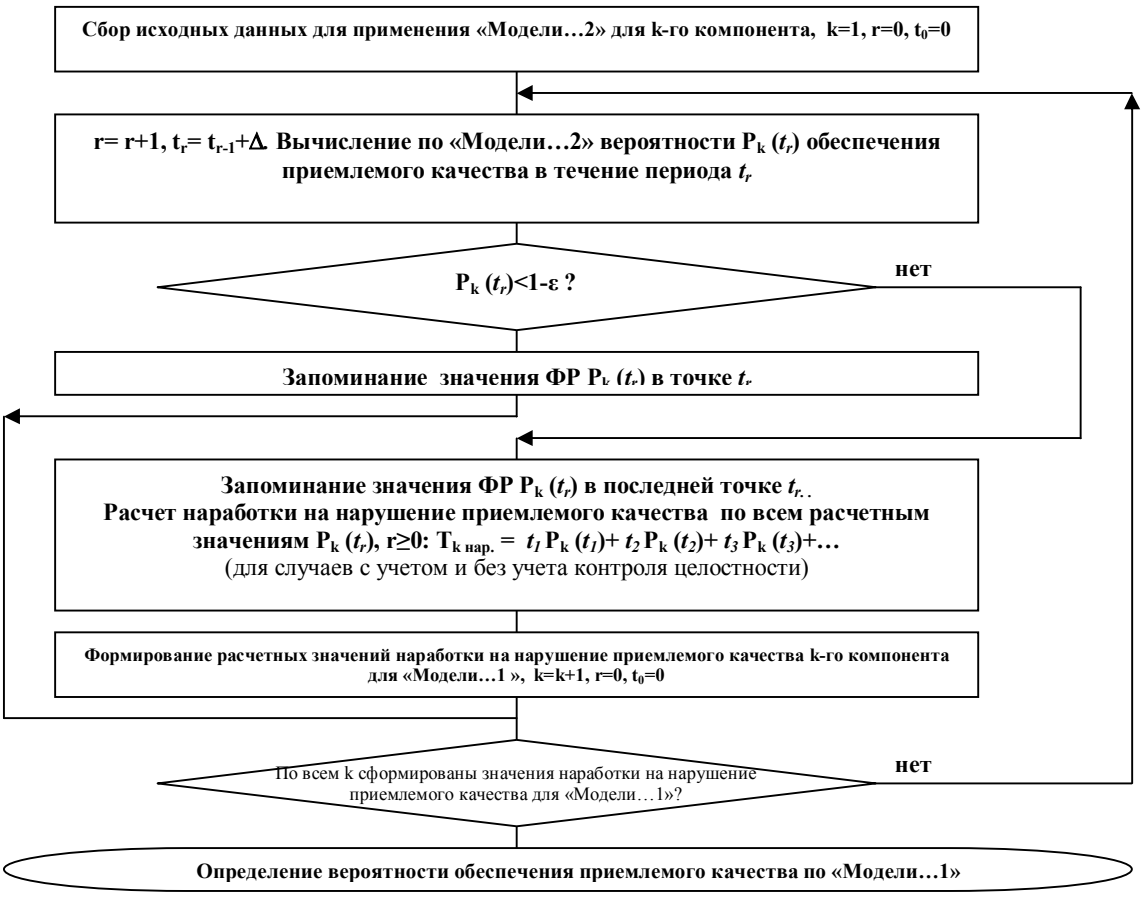


Рис. 3 Расчет показателей оценки эффективности ИП по «Модели…4» (на уровне качества)

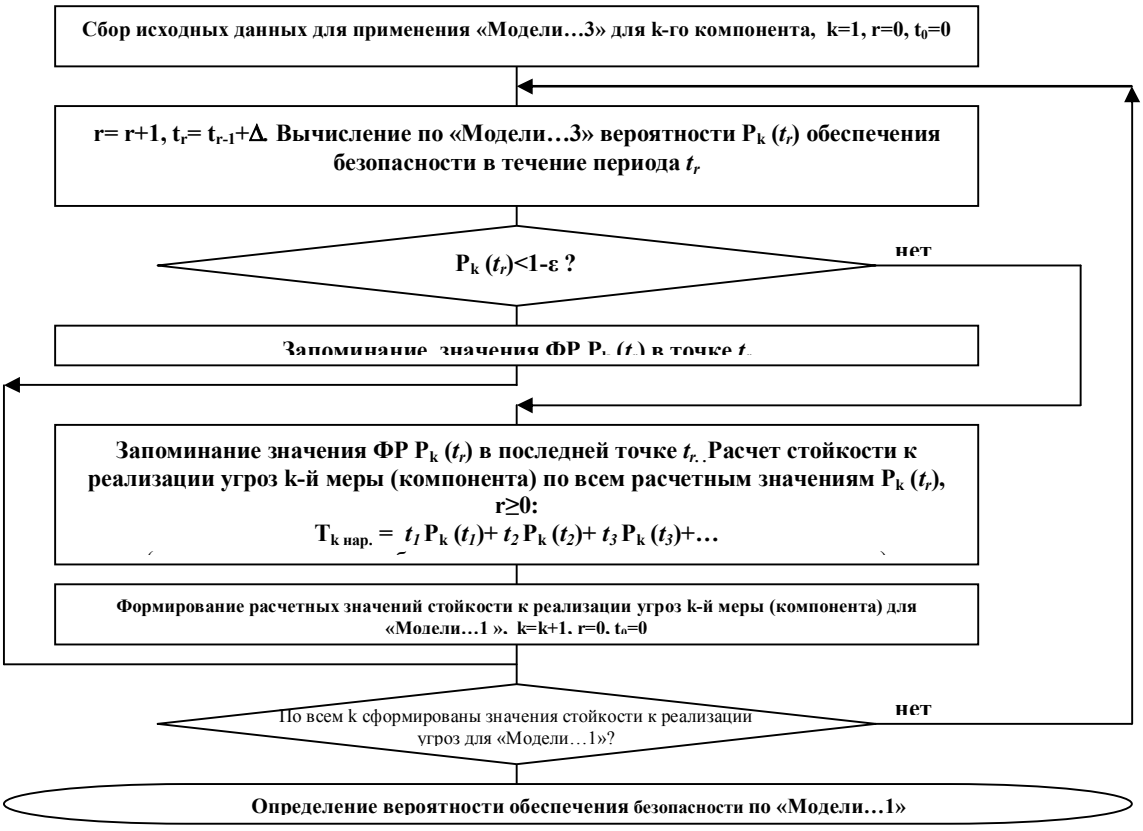
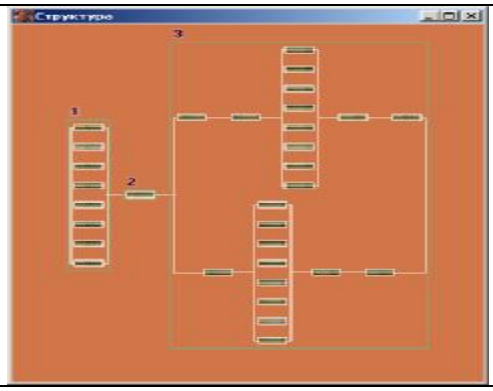


Рис. 4 Расчет показателей оценки эффективности ИП по «Модели…5» (на уровне безопасности)

Математические модели реализованы в программных комплексах «Проектирование архитектуры» и «Анализ безопасности» (на рис. 5 – представление системы из 3-х подсистем, характеристики 1-й подсистемы – из табл.2).



Пример конструируемой структуры (для исходных данных табл. 2)

Рис. 5 Пример конструируемой структуры в комплексе «Анализ безопасности» (для исходных данных табл. 2)

Таблица 2. Пример характеристики сценария угроз несанкционированного доступа и системы защиты для фрагмента оцениваемой корпоративной ИС (1-я подсистема)

Преграда	Частота смены значения параметра преграды	Среднее время преодоления преграды	Возможный способ преодоления преграды
1. Охраняемая территория со сменой охраны	через 2 часа	30 мин.	Скрытое проникновение на территорию
2. Пропускная система в здание, где располагается АИС и рабочие места пользователей со сменой службы контроля	через 1 сутки	10 мин.	Подделка документов, сговор, обман
3. Электронный ключ для включения компьютера	через 5 лет (до замены)	1 неделя	Кража, принудительное изымание ключа, сговор
4. Пароль для входа в систему	через 1 мес.	1 мес.	Подсматривание, принудительное выпытывание, сговор, подбор пароля
5. Пароль для доступа к программным устройствам	через 1 мес.	10 суток	—II—
6. Пароль для доступа к требуемой информации	через 1 мес.	10 суток	—II—
7. Зарегистрированный внешний носитель информации для записи	через 1 год	1 сутки	Кража, принудительная регистрация, сговор
8. Подтверждение подлинности пользователя в процессе сеанса с телемониторингом	через 1 мес.	1 сутки	Подсматривание, принудительное выпытывание, сговор

Предложенная «Методика оценки эффективности ИП контроля, мониторинга и поддержания целостности систем» определяет порядок применения созданных моделей 4 и 5, основанных на комбинации существующих моделей 1-3 и реализованных в программных комплексах «Проектирование архитектуры» и «Анализ безопасности».

Третий раздел посвящен разработке «Методики обоснования рациональных значений параметров ИП контроля, мониторинга и

поддержания целостности, организационно-технических мер и управляющих воздействий» в жизненном цикле систем. Решение поставленной научной задачи с использованием методики на этапах концепции и ТЗ, проектирования и разработки, производства и сопровождения системы (по показателям качества) проиллюстрировано на рис. 6. Для полного решения поставленной научной задачи в жизненном цикле систем разработаны аналогичные алгоритмы по показателям качества и безопасности.

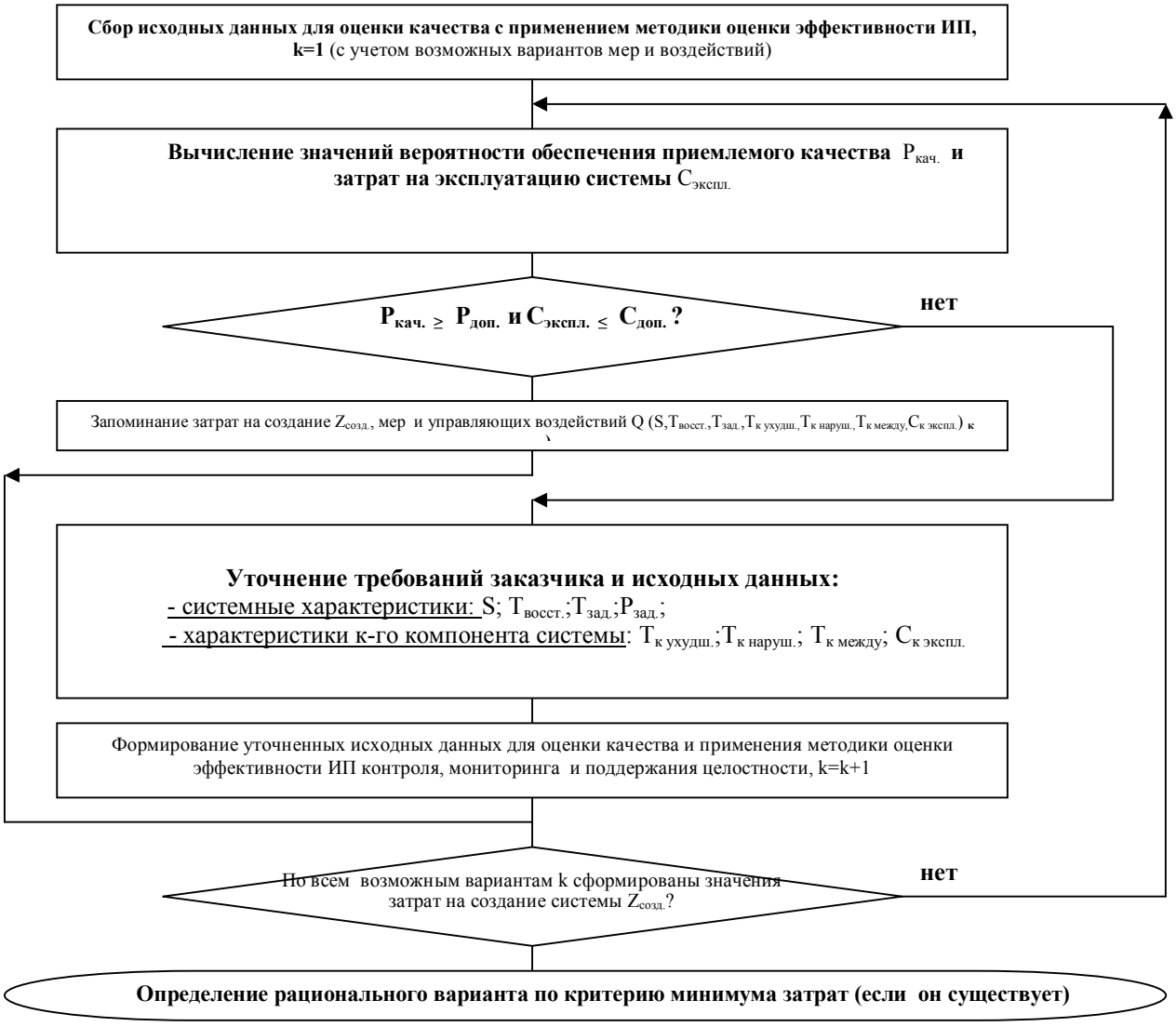


Рис. 6 Алгоритм решения поставленной задачи на этапах концепции и ТЗ, проектирования и разработки, производства и сопровождения системы (по показателям качества)

Работоспособность моделей и методик проиллюстрирована на примерах корпоративной информационной системы (КИС), робототехнических систем, автоматизированной системы обеспечения жизнедеятельности космонавта,

системы теплоснабжения. Показана возможность целенаправленного повышения качества и безопасности функционирования систем на основе практической реализации в жизненном цикле рациональных организационно-технических мер и управляющих воздействий, обоснованных с применением предлагаемых моделей и методик.

Так, если для анализа ИП контроля, мониторинга и поддержания целостности отдельной подсистемы с преградами из табл. 2 по показателям информационной безопасности наряду с предложенными применимы существующие модели (например, комплекс «КОК», свидетельство Роспатента №2000610272), то для количественной оценки безопасности всей системы сложной структуры ни один из созданных ранее комплексов не оказался практически применимым (оцениваемая система состоит из трех подсистем – см. рис. 5: 1-я подсистема – это фрагмент КИС с преградами из табл. 2, в рамках 3-й подсистемы таких фрагментов два с прежними характеристиками, а. 2-я подсистема – это подсистема передачи информации с использованием криптографических средств). Предложенная в диссертации модель 5 и созданный программный комплекс «Анализ безопасности» позволили провести оперативные расчеты комплексной безопасности системы. Анализ результатов расчетов (см. рис. 7) свидетельствует, что узким местом являются подсистемы 1 и 3. Стойкость этих подсистем существенно уступает в стойкости 2-й подсистеме. В итоге предлагаемый комплекс мер безопасности оказался несбалансированным. При этом было выявлено, что планируемые меры контроля и мониторинга весьма слабо влияют на комплексную безопасность, т.е. эти меры неэффективны, а затраты могут оказаться напрасными! Для обеспечения комплексной безопасности потребовался дополнительный поиск эффективных вариантов построения системы в части защиты от НСД. Результаты исследований были учтены на последующих этапах создания КИС для построения более эффективных ИП контроля, мониторинга и поддержания целостности.

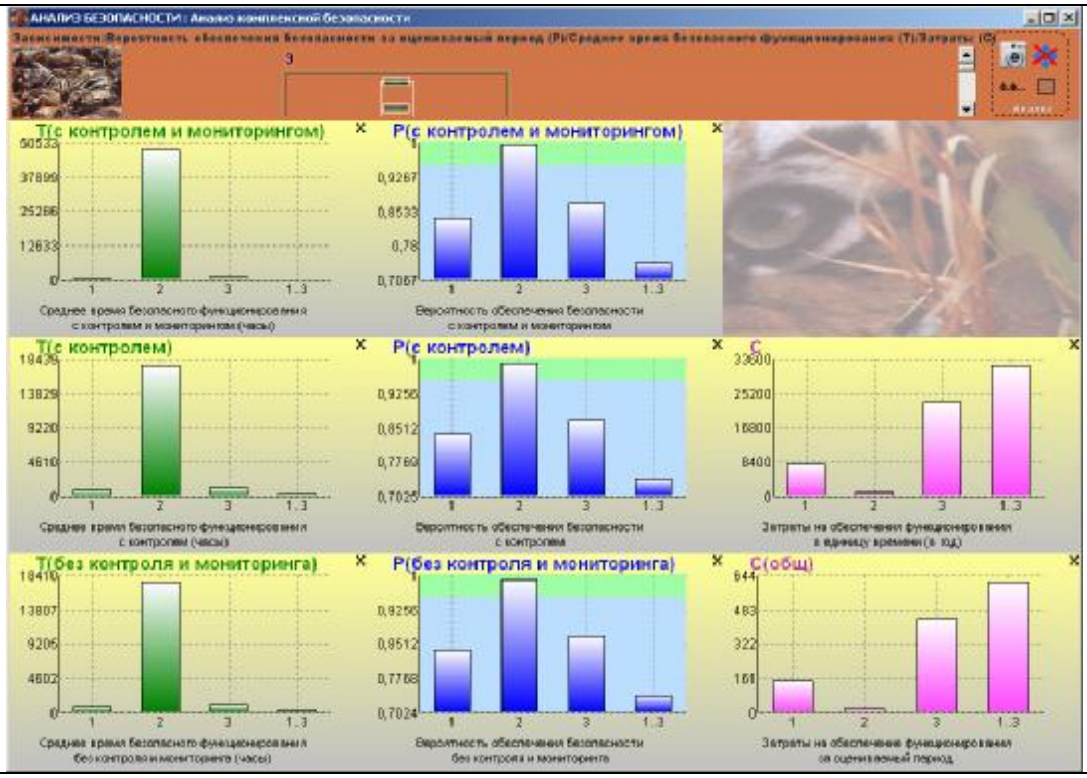
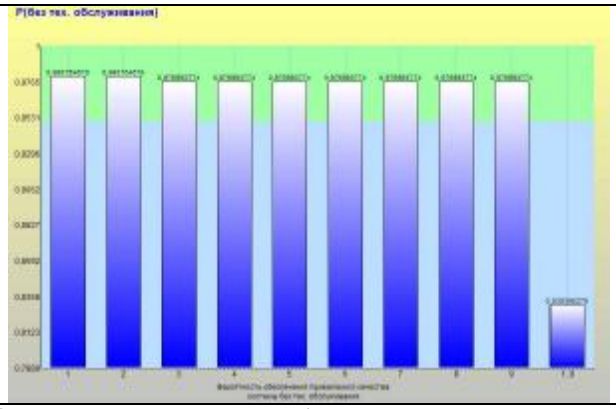
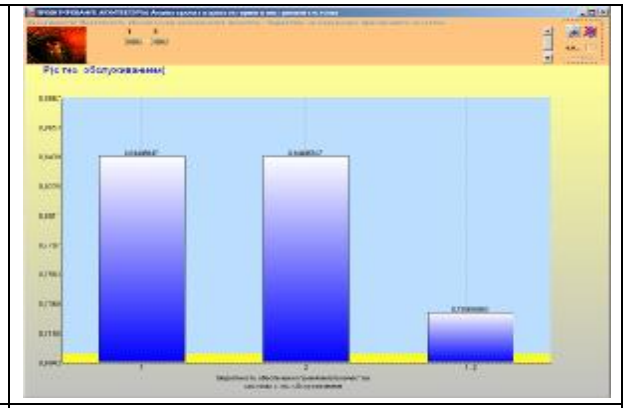


Рис. 7 Результаты расчетов комплексной безопасности КИС

В приложении к системе теплоснабжения г. Жуковский Московской области для домов с индивидуальным отоплением доказана возможность безаварийного теплоснабжения в течение года с вероятностью 0.73 при реализации еженедельного технического обслуживания (см. рис. 8). Для централизованного теплоснабжения обоснован вариант модернизации до уровня вероятности безаварийного теплоснабжения 0.41 против существующего уровня 0.008 и 0.014 для первоначального проекта, разработанного без применения предложенных моделей.



Вероятность надежного теплоснабжения в течение отопительного сезона для идеальной системы
1-й компонент – идеальные котельные; 2-й компонент – идеальный центральный тепловой пункт и надземные бойлерные установки; компоненты с 3-го по 8-й - это с 1-го по 7-й лучи теплотрассы, 9-й компонент, характеризует вероятность надежного теплоснабжения всей сети (идеальные – т.е. на базе нового оборудования)



Вероятность надежного (безаварийного) теплоснабжения с техобслуживанием для домов с индивидуальным теплоснабжением
1 – для источника тепла, 2 - для тепловых сетей, 1..2 - для источника тепла и тепловых сетей

Рис. 8 Расчетный фрагмент надежности теплоснабжения

ЗАКЛЮЧЕНИЕ

Решена научная задача обоснования рациональных значений параметров ИП контроля, мониторинга и поддержания целостности в жизненном цикле систем, имеющая существенное значение для развития теоретических основ информатики. Основные результаты:

1. Научная задача обоснования рациональных значений параметров ИП контроля, мониторинга и поддержания целостности в жизненном цикле систем формализована как задача определения таких значений параметров ИП, организационно-технических мер и управляющих воздействий, на которых достигается минимум затрат при ограничениях на допустимый уровень эффективности ИП (на этапах выработки концепции и ТЗ, проектирования и разработки, производства и сопровождения) или максимум эффективности ИП контроля, мониторинга и поддержания целостности системы при ограничениях на затраты (в процессе эксплуатации).

В качестве интегральных показателей эффективности ИП контроля, мониторинга и поддержания целостности системы предложены:

на уровне качества функционирования системы: наработка на нарушение приемлемого качества и вероятность обеспечения приемлемого качества системы в течение заданного периода времени;

на уровне безопасности: среднее время безопасного функционирования как показатель стойкости системы к реализации угроз и вероятность обеспечения ее безопасного функционирования в течение заданного периода времени.

2. Путем комбинации существующих моделей надежности (не учитывающих возможностей управления процессами контроля, мониторинга и поддержания целостности, но позволяющих проведение комплексных оценок для сложных структур), защищенности от опасных воздействий и мониторинга безопасности систем (учитывающих влияние контроля, мониторинга и поддержания целостности, но не позволяющих проведение комплексных оценок) создан принципиально новый комплекс математических моделей ИП контроля, мониторинга и поддержания целостности систем, позволяющий решить поставленную научную задачу в приложении к сложным системам, логически представимым в виде параллельно-последовательных структур. Предложенные модели доведены

до уровня программной реализации в комплексах «Проектирование архитектуры» и «Анализ безопасности» (свидетельство Роспатента №2004610858).

3. Разработаны методики оценки эффективности ИП и обоснования рациональных значений параметров ИП контроля, мониторинга и поддержания целостности, организационно-технических мер и управляющих воздействий. В качестве оптимизируемых параметров ИП, организационно-технических мер и управляющих воздействий, влияющих на значения интегральных показателей эффективности и варьируемых для решения поставленной задачи, предложены и используются:

системные характеристики: логическая структура архитектурного построения системы; время восстановления системы;

характеристики к-го компонента системы: наработка на ухудшение функционирования с начала эксплуатации или момента восстановления и наработка на нарушение приемлемого качества с начала ухудшения функционирования (для моделей качества); стойкость меры к реализации угроз (среднее время); наработка на ошибку средств мониторинга (для моделей безопасности); период между моментами контроля приемлемого качества или безопасности; затраты на обеспечение функционирования.

4. На примерах корпоративной информационной системы, робототехнических систем, автоматизированной системы обеспечения жизнедеятельности космонавта, системы теплоснабжения города доказана возможность целенаправленного повышения качества и безопасности функционирования систем на основе практической реализации в жизненном цикле рациональных значений параметров ИП, организационно-технических мер и управляющих воздействий, обоснованных с применением предлагаемых моделей и методик. В результате обеспечено повышение степени научно-методической обоснованности характеристик анализируемых ИП в жизненном цикле систем различного приложения, что отвечает цели диссертационных исследований.

5. По итогам практического применения предложенных моделей и методик в качестве направлений дальнейших научных исследований предложены:

вероятностный анализ инцидентов для различного рода систем критических приложений (информационных, нефтегазовых, систем обеспечения безопасности аэропортов, вокзалов, транспортных путей в условиях террористических угроз, систем перевозки пассажиров и грузов, систем опасного производства и хранения, например, угольных шахт, складов горючих материалов и др.) и формирование базы данных результатов анализа в зависимости от реализуемых на практике ИП контроля, мониторинга и поддержания целостности, организационно-технических мер и управляющих воздействий;

обоснование уровней приемлемых рисков и рекомендаций по обеспечению безопасности для различного рода систем критических приложений с учетом затрат, математического ожидания предотвращенных ущербов и возможной коммерческой выгоды.

Печатные работы по теме диссертации:

1. Монография: Нистратов Г.А., Костогрызов А.И. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М. Изд.”Вооружение, политика, конверсия”, 2004, 2-е изд.-2005, 395с. (Личный вклад диссертанта: методики оценки эффективности информационных процессов контроля, мониторинга, поддержания целостности, алгоритмы; программная реализация комплексов «Анализ безопасности» и «Проектирование архитектуры», расчетные примеры, 8 п.л. из 17 п.л.)

2. Нистратов Г.А. Математические модели и программные комплексы для оценки различных процессов в жизненном цикле сложных систем. Труды пятой Международной научно-практической конференции Современные информационные и электронные технологии СИЭТ-2005, Одесса, 23-27 мая 2005г. Украина, с. 162 (Личный вклад диссертанта: 100%, 0.4 п.л.)

3. Нистратов Г.А., Костогрызов А.И. Моделирование – неизбежный комплекс работ для обеспечения эффективности современных информационных систем – Материалы первого общероссийского научно-практического семинара «Электронная Земля. Электронная Россия. Электронная Москва, Методологии и технологии», Москва, ИПИ РАН, 21-22

мая 2002г., с. 112-131. (Личный вклад диссертанта: контрольные примеры, 0.1 п.л. из 0.2 п.л.)

4. Нистратов Г.А., Костогрызов А.И., Пучков О.П. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК и его приложения – Труды Международной научной конференции «Информационные технологии в естественных науках, экономике и образовании», Саратов-Энгельс, 2002г., с. 377-379. (Личный вклад диссертанта: описание программы, расчет контрольных примеров, 0.05 п.л. из 0.12 п.л.)

5. Нистратов Г.А., Григорьев Л.И., Костогрызов А.И., Стрельченко В.В. Оценки уязвимости морских нефтегазодобывающих систем в условиях террористических угроз. Труды международной конференции RAO-03, Санкт-Петербург, 2003г. (Личный вклад диссертанта: описание программы, примеры и расчет, 0.1 п.л. из 0.4 п.л.)

6. Нистратов Г.А., Костогрызов А.И., Резников Г.Я. Проблемы стандартизации и моделирования информационных систем - Наукоемкие технологии, №7, 2004, с.7-26. (Личный вклад диссертанта: описание моделирующих комплексов, 0.1 п.л. из 0.8 п.л.)

7. Нистратов Г.А., Костогрызов А.И. Проблемы моделирования информационных систем – Корпоративные системы (Украина), №4, 2004, с. 69-74;№5, 2004, с. 15-19. (Личный вклад диссертанта: описание программы, контрольные примеры и расчет, 0.05 п.л. из 0.2 п.л.)

8. G.A. Nistratov, L.I.Grigoriev, A.I. Kostogryzov Mathematical Modeling of processes in system life cycle According International standards requirements - Proceeding of the VI International Congress in Mathematical Modelling, Nigny Novgorod, 2004. (Личный вклад диссертанта: контрольные примеры для комплексов «Анализ безопасности» и «Проектирование архитектуры», 0.1 п.л. из 0.4 п.л.)

9. Нистратов Г.А., Костогрызов А.И. Математическое моделирование процессов в жизненном цикле систем в контексте требований системообразующих стандартов. Сб. трудов 4-й Всероссийской практической конференции «Стандарты в проектах современных информационных систем», 21-22 апреля 2004г., с. 27-28 (Личный вклад диссертанта: контрольные примеры, 0.1 п.л. из 0.2 п.л.)

10. Нистратов Г.А., Костогрызов А.И. 100 математических моделей для эффективного управления информационно-коммуникационными технологиями в контексте требований системообразующих стандартов. Труды XII Всероссийской научно-методической конференции «Телематика'2005», т.1, с.145 (Личный вклад диссертанта: контрольные примеры, 0.05 п.л. из 0.1 п.л.)

11. Nistratov G.A., Kostogryzov A.I. 100 Mathematical Models of System Processes According International Standards Requirements. Transaction of the XXV International Seminar on Stability Problems for the Stochastic Models. Maiority, Italy, September 20-24,2005, University of Solerno, Italy p. 196-201 (Личный вклад диссертанта: описание программы, расчет контрольных примеров, 0.05 п.л. из 0.12 п.л.)

12. Нистратов Г.А. , Костогрызов А.И., Лазарев В.М. Математические модели для эффективного контроля и управления качеством компьютеризированных систем в контексте требований системообразующих стандартов, Материалы семинара «Научные основы национальной безопасности Российской Федерации», Комитет Совета Федерации по обороне и безопасности, НИЦ ФСБ России, Москва, 2005г., с. 290-311 (Личный вклад диссертанта: описание моделирующих комплексов, 0.1 п.л. из 0.8 п.л.)

13. Нистратов Г.А. , Костогрызов А.И., Лазарев В.М. 100 Математических моделей для эффективного контроля и управления качеством компьютеризированных систем, «Инфофорум. Бизнес и безопасность в России», сентябрь 2005г., с. 105-117. (Личный вклад диссертанта: контрольные примеры, 0.2 п.л. из 0.5 п.л.)

14. Нистратов Г.А., Костогрызов А.И. 100 Математических моделей стандартизованных процессов в жизненном цикле систем. Труды международной конференции RAO-05, Санкт-Петербург, 2005г. (Личный вклад диссертанта: описание программы, примеры и расчет, 0.1 п.л. из 0.4 п.л.)

15. Nistratov G., Kleshchev N., Kostogryzov A. Mathematical Models and Software Tools to Support an Assessment of Standard System Processes. Proceedings of the 6th International SPICE Conference on Process Assessment and Improvement (SPICE-2006), Luxembourg, 2006, p. 63-68 (Личный вклад

диссертанта: описание программы, контрольные примеры и расчет, 0.05 п.л. из 0.2 п.л.)

16. Нистратов Г.А., Костогрызов А.И. Эффективные модели для анализа процессов в жизненном цикле систем. Труды научно-технической конференции с международным участием «Перспективные информационные технологии в научных исследованиях, проектировании и обучении – ПИТ-2006», Самара 29-30 июня 2006г., с.21-30. (Личный вклад диссертанта: контрольные примеры, 0.1 п.л. из 0.2 п.л.)

17. Nistratov G., Kostogryzov A. Mathematical Models and Software Tools for Analyzing System Quality and Risks according to standard requirements. Proceedings of the 6th International scientific school "MODELLING and ANALYSIS of SAFETY and RISK in COMPLEX SYSTEMS" (MASR – 2006), SAINT-PETERSBURG, RUSSIA, July 4 - 8, 2006 (Личный вклад диссертанта: описание моделирующих комплексов, 0.1 п.л. из 0.8 п.л.)