УДК 681.3.06 (075.32)
DOI 10.21778/2413-9599-2017-2-91-100

А.И. Костогрызов[1], И.В. Зубарев[2]

[1] Государственный научно-исследовательский испытательный центр робототехники Министерства обороны РФ, Федеральный исследовательский центр «Информатика и управление» РАН, Москва, Россия
[2] Научно-исследовательский институт прикладной математики и сертификации, Москва, Россия

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ДЛЯ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ РИСКАМИ В ОБЕСПЕЧЕНИЕ КАЧЕСТВА И БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ И ПЕРСПЕКТИВНЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

На основе проведенного анализа тенденций выявлены принципиальные проблемы современных и перспективных систем реального времени (СРВ) – это проблема адекватного аналитического прогнозирования рисков, проблема аналитического обоснования эффективных упреждающих мер в обеспечение качества и комплексной безопасности, проблема обеспечения информационной безопасности служебной информации, проблема рационального импортозамещения программного обеспечения СРВ, проблема эффективного управления рисками в жизненном цикле системных элементов, важных объектов и систем по критериям «безопасность–эффективность–стоимость». Предложены пути решения проблем на основе системной инженерии, описаны способы моделирования процессов для прогнозирования рисков, сформулированы задачи оптимизации.

Ключевые слова: *анализ, безопасность, качество, модель, процесс, риск, система.*

Для цитирования: Костогрызов А.И., Зубарев И.В. Моделирование процессов для эффективного управления рисками в обеспечение качества и безопасности функционирования современных и перспективных систем реального времени // Радиопромышленность. 2017. № 2. С. 91–100.

A.I. Kostogryzov[1], I.V. Zubarev[2]

[1] Main Scientific Research Test Center of the Russian Ministry of Defence and Federal Research Center «Computer Science and Control» of the Russian Academy of Sciences, Moscow, Russia
[2] Research Institute of Applied Mathematics and Certification, Moscow, Russia

MODELLING OF PROCESSES FOR EFFECTIVE RISKS CONTROL TO REACH HIGH OPERATION QUALITY OF MODERN AND PERSPECTIVE SYSTEMS OF REAL TIME

Based on the analysis of trends there have been identified fundamental problems of today's and future real-time systems (RTSs) – this is a problem of adequate analytical risk prediction, the problem of analytical study of efficient preventive measures for quality assurance and integrated security, the problem of proprietary information security, the problem of rational import substitution for RTS software, a problem of efficient risk management in the life cycle of the system elements, critical facilities and systems under «safety, cost-effectiveness» criteria. Methods for solving the problems on

the basis of systems engineering are proposed, process modeling methods for risk prediction are described, and optimization tasks are formulated.

Keywords: *analysis, safety, quality, model, process, risk, system.*

For citation: Kostogryzov A.I., Zubarev I.V. Modelling of processes for effective risks control to reach high operation quality of modern and perspective systems of real time. Radiopromyshlennost, 2017, no. 2, pp. 91–100 (in Russian).

DOI 10.21778/2413-9599-2017-2-91-100

Введение

Сегодня наблюдается серьезный перекос в информационном и техническом прогрессе РФ, обострившийся в последнее время из-за санкций Запада, технологического отставания РФ в области информационных технологий (ИТ), социально-экономических кризисов и распространения терроризма, ведущих к росту разнородных неопределенностей. В итоге в России процесс создания и эксплуатации современных и перспективных систем реального времени (СРВ) различного назначения оказывается совмещенным с утратой согласованной подконтрольности отдельных элементов и систем. Это приводит к недооценке роста рисков нарушения качества и комплексной безопасности СРВ и нерациональности в решении связанных с этим системных проблем [1].

Учитывая, что потенциальные ущербы и затраты на ликвидацию последствий критичных нарушений качества и безопасности для СРВ в условиях разнородных угроз на порядок превышают затраты на превентивные меры, необходим поиск эффективных решений по комплексной безопасности. Несмотря на то, что многочисленные предпринятые в России меры противодействия угрозам разработаны на уровне федеральных законов (ФЗ), федеральных норм и правил (ФНП), руководств по безопасности (РБ), «ручное» управление качеством и комплексной безопасностью СРВ продолжает оставаться главенствующим, причем так, как это субъективно понимается на ведомственном и корпоративном уровнях. В свою очередь, мировые тенденции развития современных систем различного функционального назначения свидетельствуют о необходимости кардинального разворота от «ручного» управления качеством и отдельными видами безопасности (основанного на выполнении устоявшихся инструкций и на экспертных оценках складывающихся ситуаций) к реализации научно обоснованных эффективных упреждающих мер в жизненном цикле СРВ на основе моделирования процессов для прогнозирования рисков. Это позволяет на основе прогнозного взгляда вперед превентивно предпринимать эффективные упреждающие воздействия. Такая идея красной линией проходит через все западные концепции и последние стандарты системной инженерии. Но как это сделать – остается за кадром. В мире еще нет универсального подхода к реализации этой идеи. В поиске – все ведущие страны мира, а находки, которых не так много, обращаются в государственные, коммерческие или военные решения «ноу-хау», предопределяющие выгоды от их применения.

Пренебрежительное отношение к аналитическому моделированию процессов и прогнозированию рисков ведет к многомиллиардным ущербам. Для СРВ злоумышленные нарушения могут маскироваться под технические неисправности, ошибки из-за «человеческого фактора» или от воздействия анонимных хакеров. Независимо от рода реализуемых угроз это уже наносит, и, к сожалению, порой непоправимый, ущерб, вредит конкурентоспособности России, ведет к обострению социальной напряженности.

Острота перечисленных угроз усугубляется отсутствием в России требований и применяемых мер обеспечения информационной безопасности служебной информации. Возрастают риски нарушения информационной безопасности и связанных с этим других видов безопасности – промышленной, энергетической, пожарной, экологической, транспортной, антитеррористической безопасности и иных видов безопасности с использованием IT-систем.

В итоге состояние дел может быть охарактеризовано следующими положениями. Количественный прогноз рисков для качества и отдельных видов безопасности на основе моделирования различных процессов применительно к СРВ не осуществляется (например, для информационной и антитеррористической безопасности). Как исключение – прогноз рисков в интересах МЧС РФ и в некоторых случаях для Росатома, осуществляемый путем имитационного моделирования), а там, где делается (например, для промышленной безопасности) – в подавляющем большинстве случаев осуществляется при структурных и методических упрощениях, свойственных достижениям 20–30-летней давности. Отсюда из-за недопонимания требуемой глубины анализа идут грубые ошибки – для сложных систем они составляют сотни-тысячи процентов! В общем случае «допустимые риски» рассматриваются лишь как пограничная полоса. Разнородность угроз и их системное влияние на качество и комплексную безопасность СРВ не анализируются. В подавляющем

большинстве случаев требования к «допустимым» рискам научно не обосновываются или предъявляются формально для демонстрации того, что риски при таких-то условиях «не превышают допустимых» (прогнозы и устойчивость для разнородных угроз – не рассматриваются, задачи синтеза с обоснованием «что делать?» – не решаются в реальном времени). Для сложных структур предпринимаемые меры контроля, мониторинга и противодействия угрозам научно не обосновываются, хотя понятие «допустимых рисков» в мире используется в первую очередь для решения обратных задач и обоснования упреждающих мер противодействия угрозам. Эффективность отдельных упреждающих мер в комплексе мер не оценивается в терминах снижения рисков. Узкоспециализированные (и за счет этого зачастую разнонаправленные и дезинтегрированные) методические решения ведут к различающимся несравнимым интерпретациям и невозможности соизмерить результаты из различных приложений применительно к разнородным угрозам. Междисциплинарный опыт используется крайне редко. Междисциплинарные знания по прецедентам для эффективных упреждающих действий не систематизируются и не доводятся до заинтересованных лиц для учета и недопущения повторных или аналогичных ошибок. Приобретение и внедрение импортного программного обеспечения (ПО) разобщено. Доказательствам эффективности СРВ в терминах прогнозируемых рисков в условиях разнородных угроз на всех стадиях жизненного цикла (особенно на ранних) не уделяется должного внимания. Именно здесь находится источник принципиальных противоречий между требуемыми и достигаемыми качеством и комплексной безопасностью СРВ. Если сейчас не повернуться лицом к выявленным противоречиям, то по мере усложнения создаваемых важных объектов и систем, базирующихся на СРВ, будет проявляться неэффективность принимаемых несистемных решений. И наоборот, своевременное разрешение накопившихся проблем на основе моделирования и прогнозирования рисков приведет к долговременной и обоснованной реализации скрытых эффектов для СРВ.

Для СРВ различного функционального назначения выявлены следующие принципиальные проблемы обеспечения качества и комплексной безопасности, требующие приоритетного решения. В общем случае для ожидаемых условий неопределенности и разнородных угроз в приложении к объекту, системе или системному элементу, выполняющему функции СРВ, или их совокупности таковыми проблемами являются:

1. Проблема адекватного аналитического прогнозирования рисков нарушения качества и комплексной безопасности на заданный период прогноза;
2. Проблема аналитического обоснования эффективных упреждающих мер в обеспечение качества и комплексной безопасности (по результатам прогнозирования рисков);
3. Проблема обеспечения информационной безопасности служебной информации для важных объектов и систем в России и за рубежом;
4. Проблема рационального импортозамещения программного обеспечения СРВ;
5. Проблема эффективного управления рисками в жизненном цикле системных элементов, важных объектов и систем по критериям «безопасность–эффективность–стоимость».

Решение проблем на основе системной инженерии

Научно-теоретической и практической основой решения проблем выступает системная инженерия, определяемая в современных международных стандартах как сосредоточение научно-технических усилий по рациональному построению и эффективному применению сложных систем. Рассматриваемые системы состоят из множества составных подсистем и системных элементов (их могут быть десятки, сотни, тысячи и более), для каждой из которых в общем случае должны решаться идентичные по своему содержанию проблемы 1–5 в условиях разнородных угроз нарушения качества и комплексной безопасности (рис. 1, 2). Прогнозируемые риски должны быть соизмеримыми и в жизненном цикле системных элементов и систем позволять решение прямых и обратных задач по критериям «безопасность–эффективность–стоимость».

Западный мир в той или иной степени уже приступил к решению сформулированных выше проблем. Так, США сформулировали подходы системной инженерии к обеспечению национальной безопасности после 11 сентября 2001 года. Например, реализуемые ими концепции гибридных войн настоящего и будущего предусматривают не столько чисто военные решения, сколько использование уязвимостей важных объектов и систем противника к разнородным угрозам и их неспособность противостоять явным или скрытым нарушениям промышленной, энергетической, пожарной, информационной, экологической, транспортной, антитеррористической безопасности, безопасности зданий и сооружений и/или ядерной и радиационной безопасности.

Особенности разнородных угроз для важных объектов и систем России, использующих СРВ, связаны с необходимостью преодоления технологического отставания в различных областях (в первую очередь – в области информационных технологий) и важностью всемерного развития

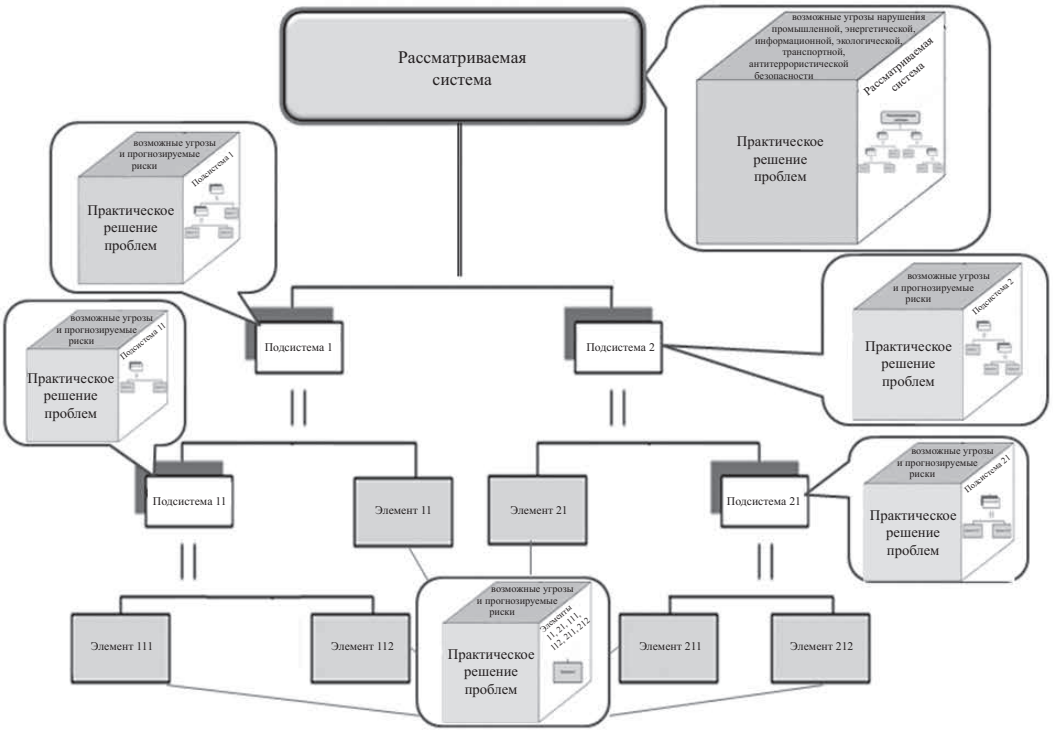


Рисунок 1. Декомпозиция сложной системы до элементов для решения проблем

научно-технологического комплекса, с рассредоточенностью в ряде случаев важных объектов информационной инфраструктуры на громадной территории РФ с различными условиями и угрозами, с поиском и освоением новых источников энергии (например, в Арктике) и расширением рынков сбыта своей продукции, с осознанием лидирующей роли и ответственности в борьбе с международным терроризмом.

Для практического управления рисками рекомендуются методы и модели (далеко не исчерпывающие список адекватных моделей [2–15]), где субъективные весовые коэффициенты исключены. Последнее – важно, т.к. продолжают широко применяться методы, базирующиеся на экспертных оценках, в т.ч. с использованием различного рода субъективно назначаемых коэффициентов (что еще как-то воспринималось на заре исследований по качеству и безопасности, но сегодня является тормозом в современной науке, поскольку «эксперты» бывают разные, человек в состоянии обозреть единицы-десятки элементов, но не тысячи в их сложных взаимосвязях). Из-за субъективизма возможны «подгонки» под любые пожелания и нормативы.

Способы моделирования процессов

Суть предложений по развитию существующего научно-методического потенциала – в разработке и использовании вероятностных моделей для расчетов показателей качества функционирования и рисков применительно к сложным системам. Модели базируются на классически построенном вероятностном пространстве (Ω, B, P), где Ω – конечное пространство элементарных событий; B – класс всех подмножеств множества Ω, удовлетворяющий свойствам сигма-алгебры; P – вероятностная мера на пространстве элементарных событий. При этом, поскольку пространство $\Omega=\{\omega_k\}$ – конечное, в моделях установлено отображение $\omega_k \to p_k = P(\omega k)$ такое, что $p_k \geq 0$ и $\sum_k p_k = 1$.

Примером является моделирование процессов для оценки качества функционирования СРВ, являющихся информационными системами. Основная идея для достижения качества и безопасности функционирования таких СРВ – обеспечение информацией, для которой уровень риска нарушения качества функционирования системы не превышает допустимого (рис. 2).

Для расчета вероятностных показателей рекомендуется ряд вероятностных моделей:

- модель процессов выполнения функций системой в условиях ненадежности комплексируемых компонентов;
- комплекс моделей процессов обработки запросов в системе;
- модель процессов отражения в системе новых объектов учета предметной области;
- комплекс моделей процессов сбора информации от источников;

Рисунок 2. Абстрактный пример реально получаемой информации с учетом разнородных угроз

- модель процессов анализа информации;
- комплекс моделей опасных воздействий на защищаемую систему;
- комплекс моделей процессов несанкционированного доступа к ресурсам системы и др. (публикации [2–11]).

В приложении к более общему случаю (рис. 1) для моделирования используются следующие рассуждения.

Каждый из элементов представляется в виде «черного ящика», и для него могут быть применены различные вероятностные модели для расчетов и построения искомой функции распределения (ФР) времени между соседними нарушениями целостности, учитывающие разнородные угрозы, предпринимаемые меры контроля, мониторинга и восстановления целостности. Научный взгляд на процессы реализации разнородных угроз и системное отображение событий на временную ось характеризуются частотой возникновения угроз, временем их развития и системными или бессистемными мерами и технологиями противодействия угрозам. В случайных событиях присутствуют скрытые закономерности. Современный уровень развития теории вероятностей и теории случайных процессов независимо от природы разнородных угроз способен сформировать теоретическую и практическую базу для прогнозирования рисков (в т.ч. риска нарушения качества функционирования) и решения связанных с этим задач выработки и обоснования эффективных упреждающих мер. Фокусирование внимания именно на процессах позволяет использовать для их описания лишь характеристики времени (среднее время или частоту наступления событий), безразмерные или стоимостные характеристики, свойственные для объектов и систем различных приложений. Степень достижения ожидаемых результатов оценивается вероятностными показателями (например, с помощью вероятности успеха или риска нарушения безопасности в течение заданного времени), рассчитываемыми с использованием применимых вероятностных моделей. На рис. 3 отражено абстрактное представление процессов возникновения и реализации угроз с учетом мер противодействия для построения методов прогнозирования рисков на заданный период прогноза. Собственно, эта идея реализована для технологий контроля (без непрерывного мониторинга событий в модели опасных воздействий на защищаемую систему в стандарте ГОСТ РВ 51987). Предлагаемые методы расчета приведены в [2–14].

Для сложных структур предлагается метод комбинации моделей, позволяющий вручную или в автоматическом режиме генерировать новые модели, за счет чего оказывается возможным расчет формализованных показателей рисков. При этом появляется возможность аналитического учета разнородных угроз с учетом предпринимаемых

Рисунок 3. Абстрактное представление процессов возникновения и реализации угроз с учетом мер противодействия для построения методов прогнозирования рисков на заданный период прогноза

технологических мер контроля, мониторинга и восстановления целостности (как системы в целом, так и составных подсистем).

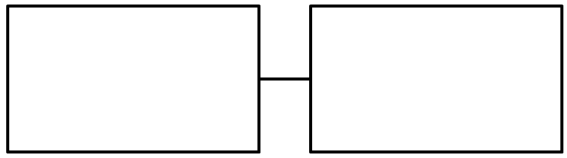
Основные идеи комбинации и, как следствие, автоматической генерации новых моделей для комплексных исследований заключаются в следующем:

1-я идея. Поскольку модели математические, то путем смыслового переобозначения исходных данных и, соответственно, расчетных показателей возможно использование одних и тех же моделей для оценки разных показателей. Идея упомянута лишь для понимания логики в генерации моделей.

2-я идея. Для комплексной оценки в приложении к системам сколь угодно сложной параллельно-последовательной структуры существующая модель может быть развита традиционными методами теории вероятностей. Сложность оценивается количеством составных элементов. Для этого надо знать наработку на нарушение целостности каждого из элементов. Далее достаточно логического переопределения понятия наработки (например, для анализа надежности это наработка на отказ, а для анализа качества функционирования или безопасности – наработка на нарушение целостности). В качестве логических элементов могут выступать отдельные составные элементы системы.

Для простейшей структуры из двух независимых элементов, соединенных последовательно, что означает логическое соединение «И» (рис. 4), или параллельно, что означает логическое соединение «ИЛИ» (рис. 5), в условиях независимости выражения для ФР – классические (для i-го элемента ФР обозначается как $B_i(t)$). Тогда логическая интерпретация элементарного события «нарушение безопасности» для представления системы в виде последовательного соединения следующая: чтобы система, состоящая из подсистем, находилась в течение времени прогноза в состоянии безопасности, необходимо, чтобы все подсистемы («И» 1-я, «И» 2-я,…, «И» последняя) находились все это время в состоянии безопасности. Логическое выражение «ИЛИ» используется, если есть резервирование.

Исходные ФР $B_i(t)$ рассчитываются по адекватным моделям (например, по формулам из стандарта ГОСТ РВ 51987 или [2–11]) или, при упрощенном варианте, аппроксимируются экспоненциальным распределением. Применяя приведенные рекуррентные соотношения (рис. 4, 5), можно получать соответствующие оценки для сколь угодно сложной логической структуры с параллельно-последовательным соединением элементов. Для новой структуры – это уже новые вероятностные модели,



Функция распределения времени наработки

$$B(t) = 1 - [1 - B_1(t)][1 - B_2(t)]$$

Рисунок 4. Система из последовательно соединенных элементов

Функция распределения времени наработки

$$B(t) = B_1(t) B_2(t)$$

Рисунок 5. Система из параллельно соединенных элементов

генерируемые по формулам на рис. 4, 5. Именно эти соотношения реализованы в программных инструментариях, поддерживающих прогнозирование рисков и обоснование эффективных упреждающих мер в обеспечение качества функционирования АСУ РВ [13–15].

3-я идея. На выходе моделирования системы существует вероятность нарушения целостности в течение заданного прогнозного периода времени. В рамках предлагаемых технологий ожидается численный просчет этой вероятности для всех точек заданного периода прогноза ($T_{зад.}$) от нуля до бесконечности для каждого элемента. В итоге будут получены траектории ФР времени сохранения целостности по каждому из элементов в зависимости от реализуемых мер контроля, мониторинга и восстановления целостности. В свою очередь, известный вид этой ФР, построенной по точкам с использованием программных комплексов, позволит традиционными методами математической статистики определить среднее время сохранения целостности каждого из элементов системы. А это – необходимые исходные данные для применения генерируемых моделей и, соответственно, оценки показателей функционирования некой системы параллельно-последовательной структуры любой степени сложности.

Например, логическая интерпретация элементарных состояний: интегрированная система находится в состоянии «отсутствия нарушений целостности», если «И» система слева, «И» система справа находятся в состоянии «отсутствия нарушений целостности» (рис. 6).

Предложенный подход применим для анализа, сравнения и оптимизации функционирования разнородных систем. Для этого достаточно установить пространство элементарных событий и логическую структуру, позволяющую генерацию моделей для расчета интегральных показателей. Например, для триады «Разведка – Управление – Поражение» возможны различные комбинации логических представлений, позволяющие решение прямых и обратных задач как для интегрированной системы в целом, так и для составных систем, в т.ч. АСУ реального времени (рис. 7).

Задачи оптимизации

Зафиксировав уровни «допустимых рисков» для системы и составных подсистем, а также считая неизменными все параметры, за исключением

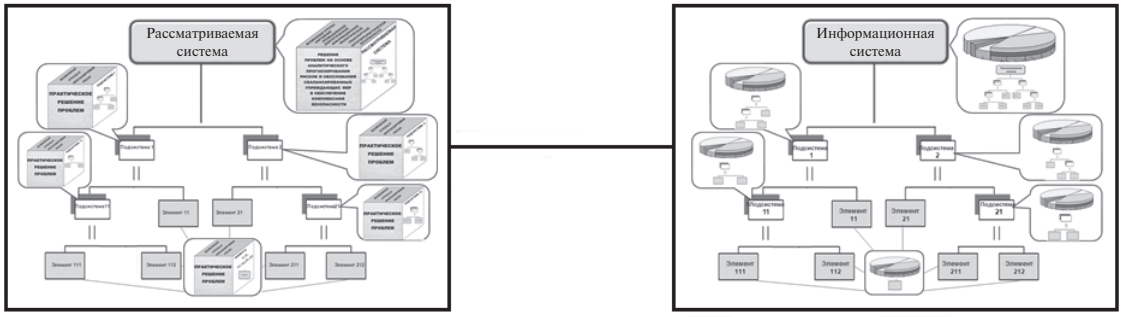


Рисунок 6. Пример логического последовательного объединения двух разнородных систем (подсистем)

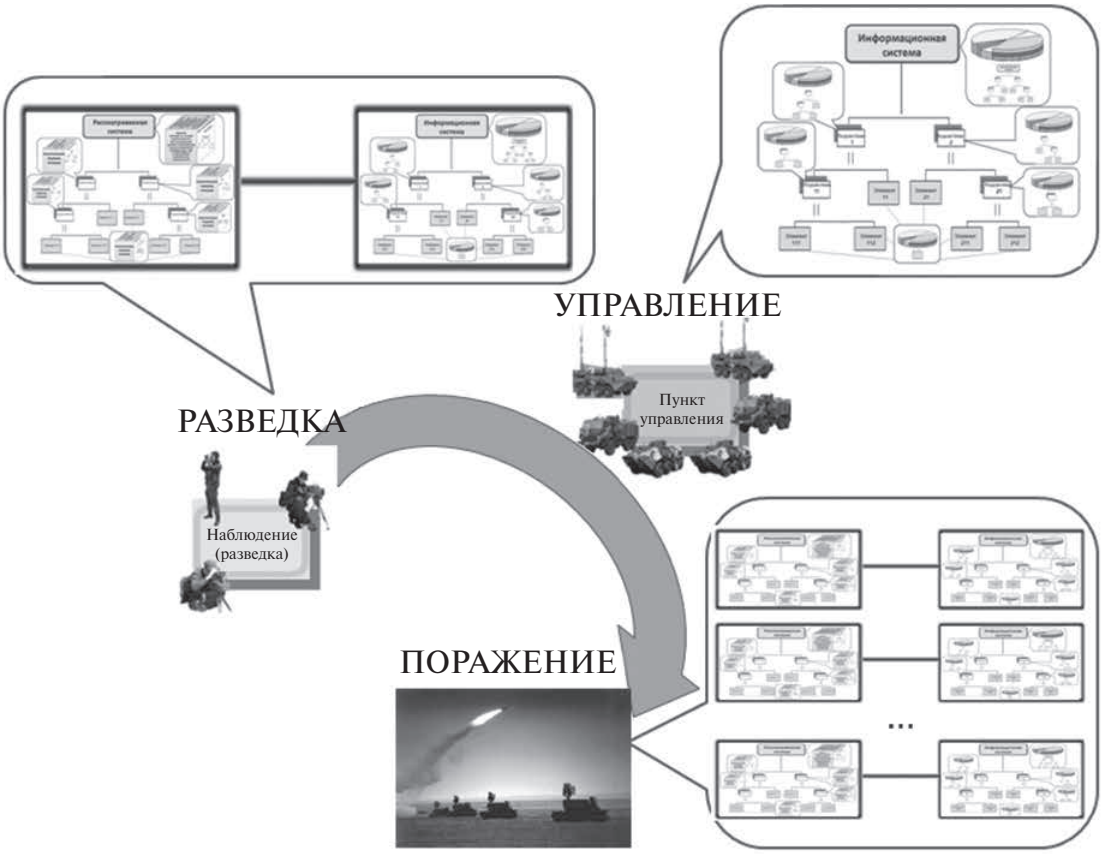


Рисунок 7. Логическая структура для моделирования процессов функционирования интегрирующей системы в замкнутом контуре «Разведка – Управление – Поражение»

одного, возможно решение различных оптимизационных задач, связанных с обоснованием эффективных упреждающих мер обеспечения целостности системы в условиях разнородных угроз [16]. Классическими задачами являются максимизация эффекта (уровня качества или безопасности и др.), или минимум рисков при ограничениях, или минимизация затрат при ограничениях на допустимые риски и иных ограничениях.

Для расчетов могут быть использованы модели, поддерживаемые инструментально-моделирующими комплексами «Моделирование процессов», свидетельство Роспатента № 2006610219, «Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем», свидетельство Роспатента № 2006610219, «Программно-вычислительный комплекс оценки качества производственных процессов», свидетельство Роспатента № 2010614145 [13–15].

Сбалансированное упреждающее управление процессами возникновения, развития, контроля и нейтрализации возможных угроз осуществляется в рамках формальных постановок оптимизационных задач путем целенаправленного использования моделей и выбранных критериев рациональности при ограничениях на ресурсы и варианты реализации процессов.

Смысл применения оптимизационных постановок задач в следующем – за счет упреждающего выбора рациональных значений управляемых параметров анализируемых сценариев угроз и реализуемых мер упреждения и реакции:

- избежать излишних затрат при допустимых рисках и заданных критичных ограничениях на этапах концепции и технического задания (ТЗ), разработки, производства, эксплуатации и сопровождения СРВ и отдельных ее подсистем и элементов;
- минимизировать риски в процессе эксплуатации СРВ и отдельных ее подсистем и элементов при заданных критичных ограничениях.

СПИСОК ЛИТЕРАТУРЫ

1. Системный подход к управлению рисками инновационных проектов на предприятиях оборонно-промышленного комплекса / А.М. Батьковский, А.В. Коновалова, П.В. Кравчук, А.В. Фомина // Вопросы радиоэлектроники. 2016. № 2. С. 133–144.
2. Костогрызов А.И., Петухов А.В., Щербина А.М. Основы оценки, обеспечения и повышения качества выходной информации в АСУ организационного типа. М.: Изд-во «Вооружение, политика и конверсия», 1994. 278 с.
3. Костогрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. М.: Изд-во «Вооружение. Политика. Конверсия», 1996. 280 с.
4. Kostogryzov A.I. Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ). Proceedings of the 34th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium (Sept. 25–29, 2000, USA, Dallas), pp. 63–70.
5. Безкоровайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК: 150 задач анализа и синтеза и примеров их решения. М.: Изд-во «Вооружение. Политика. Конверсия», 2002. 304 с.
6. Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М.: Изд-во «Вооружение. Политика. Конверсия», 2005. 395 с.
7. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем. М.: Изд-во «Вооружение. Политика. Конверсия», 2008. 404 с.
8. Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems. Proceedings of the 1st Intern. Conf. on Transportation Information and Safety, ICTIS, June 30 – July 2, 2011, Wuhan, China, 2011, pp. 845–854.
9. Kostogryzov A., Nistratov G., Nistratov A. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, DOI: 10.5772/46106, Total Quality Management and Six Sigma, InTech, 2012, pp. 127–196. Available at: http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management
10. Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes. DOI: 10.4236/ajor.2013.31A021, American Journal of Operations Research, 2013, no. 3, pp. 217–244, Available at: http://www.scirp.org/journal/ajor/
11. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности / В.А. Акимов, А.И. Костогрызов, Н.А. Махутов, В.Е. Фортов, С.К. Шойгу и др.; под ред. Н.А. Махутова. М.: МГОФ «Знание», 2015. 936 с.
12. Свидетельство о государственной регистрации программы для ЭВМ № 2004610858. Моделирование процессов в жизненном цикле систем (Моделирование процессов) – ноу-хау / Костогрызов А.И., Нистратов Г.А., Нистратова Е.Н., Нистратов А.А.; заявл. 25.03.2004, опубл. 08.04.2004.
13. Свидетельство о государственной регистрации программы для ЭВМ № 2006610219. Комплекс для анализа и управления качеством и рисками при создании и эксплуатации автоматизированных систем / Костогрызов А.И., Нистратов Г.А.; заявл. 27.10.2005 опубл. 10.01.2006.
14. Программно-вычислительный комплекс оценки качества производственных процессов. Свидетельство о государственной регистрации программы для ЭВМ № 2010614145.
15. Безопасность России. Правовые, социально-экономические и научно-технические аспекты // Фундаментальные и прикладные проблемы комплексной безопасности / Н.В. Абросимов, А.И. Костогрызов, Н.А. Махутов, В.Е. Фортов, С.К. Шойгу и др.; под ред. Н.А. Махутова. М.: МГОФ «Знание», 2017. 992 с.
16. Батьковский А.М., Фомина А.В. Инструментарий оптимизации решения актуальных задач управления развитием предприятий оборонно-промышленного комплекса // Вопросы радиоэлектроники. 2016. № 3. С. 146–157.

REFERENCES

1. Batkovskiy A.M., Konovalova A.V., Kravchuk P.V., Fomina A.V. Systemic approach to risk management of innovative projects of military-industrial complex enterprises. *Voprosy radioelektroniki,* 2016, no. 2, pp. 133–144 (In Russian).
2. Kostogryzov A.I., Petuhov A.V., Shcherbina A.M. *Osnovy ocenki, obespechenija i povyshenija kachestva vyhodnoj informacii v ASU organizacionnogo tipa* [Basics of assessment, provision of and improvement of quality of output information in the organizational-type APCS]. Moscow, Vooruzhenie, politika i konversiya Publ., 1994, 278 p. (In Russian).
3. Kostogryzov A.I., Lipaev V.V. *Sertifikacija funkcionirovanija avtomatizirovannyh informacionnyh system* [Certification of the functioning of automated information systems]. Moscow, Vooruzhenie, politika i konversiya Publ., 1996, 280 p. (In Russian).
4. Kostogryzov A.I. Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ). *Proceedings of the 34th Annual Event of the Government Electronics and Information Association (GEIA). Engineering and Technical Management Symposium* (Sept. 25–29, 2000, USA, Dallas), pp. 63–70.
5. Bezkorovayny M.M., Kostogryzov A.I., Lvov V.M. *Instrumentalno-modelirujushhij kompleks dlja ocenki kachestva funkcionirovanija informacionnyh sistem KOK* [150 problems of analysis and synthesis and examples of their solutions]. Moscow, Vooruzhenie, politika i konversiya Publ., 2002, 304 p. (In Russian).
6. Kostogryzov A.I., Nistratov G.A. *Standartizacija, matematicheskoe modelirovanie, racional'noe upravlenie i sertifikacija v oblasti sistemnoj i programmnoj inzhenerii* [Standardization, mathematical modeling, rational management and certification in the field of system and software engineering]. Moscow, Vooruzhenie, politika i konversiya Publ., 2005, 395 p. (In Russian).

7. Kostogryzov A.I., Stepanov P.V. *Innovacionnoe upravlenie kachestvom i riskami v zhiznennom cikle sistem* [Innovative management of quality and risks in the life cycle of systems]. Moscow, Vooruzhenie, politika i konversiya Publ., 2008, 404 p. (In Russian).
8. Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems. *Proceedings of the 1st Intern. Conf. on Transportation Information and Safety, ICTIS,* June 30 – July 2, 2011, Wuhan, China, 2011, pp. 845–854.
9. Kostogryzov A., Nistratov G., Nistratov A. [Some Applicable Methods to Analyze and Optimize System Processes in Quality Management], DOI: 10.5772/46106, Total Quality Management and Six Sigma, InTech, 2012, pp. 127–196. Available at: http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management
10. Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. [Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes], DOI: 10.4236/ajor.2013.31A021, *American Journal of Operations Research,* 2013, no. 3, pp. 217–244. Available at: http://www.scirp.org/journal/ajor/
11. Akimov V.A., Kostogryzov A.I., Mahutov N.A., Fortov V.E., Shoygu S.K. at al. *Bezopasnost Rossii. Pravovye, social'no-jekonomicheskie i nauchno-tehnicheskie aspekty* [Security of Russia. Legal, social & economic and scientific & technical aspects. Scientific foundations of man-made security.] In: N.A. Mahutov ed. Moscow, MGOF «Znanie» Publ., 2015, 936 p. (In Russian).
12. Certificate of state registration of the computer program No. 2004610858. Modeling of processes in the life cycle of Process Modeling – systems know-how. Kostogryzov A.I., Nistratov G.A., Nistratova E.N., Nistratov A.A.; zajavl. 25.03.2004, opubl. 08.04.2004 (In Russian).
13. Certificate of state registration of the computer program No. 2006610219. Complex for analysis and management of quality and risks in design and operation of automated systems. Kostogryzov A.I., Nistratov G.A.; zajavl. 27.10.2005, opubl. 10.01.2006 (In Russian).
14. Certificate of state registration of the computer program No. 2010614145. Programming and computing suite for evaluation and evaluation of products quality. (In Russian).
15. Abrosimov N.V., Kostogryzov A.I., Mahutov N.A., Fortov V.E., Shoygu S.K. *Bezopasnost Rossii. Pravovye, sotsial'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Fundamental'nye i prikladnye problemy kompleksnoi bezopasnosti.* [Security of Russia. Legal, social & economic and scientific & technical aspects. Fundamental and Applied Problems of Complex Security]. In: N.A. Mahutov ed. Moscow, MGOF «Znanie» Publ., 2017, 992 p. (In Russian).
16. Batkovskiy A.M., Fomina A.V. Tools to optimize the solution topical the tasks of management by development of enterprises of the military-industrial complex. *Voprosy radioelektroniki,* 2016, no. 3, pp. 146–157 (In Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Костогрызов Андрей Иванович, д.т.н., профессор, старший научный сотрудник, Государственный научно-исследовательский испытательный центр робототехники Министерства обороны РФ, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» РАН, 119333, Москва, ул. Вавилова, д.44, корп. 2, тел.: 8 (495) 795-85-24, e-mail: akostogr@gmail.com.

Зубарев Игорь Витальевич, к.т.н., доцент, главный научный сотрудник НИИ прикладной математики и сертификации, 107564, Москва, ул. Краснобогатырская, д.2, стр. 2, тел.: 8 (916) 410-31-61, e-mail: zubarev-i@bk.ru.

AUTHORS

Kostogryzov Andrey, Dr., professor, senior researcher fellow, Test Center of the Russian Ministry of Defence; main scientific research, Federal Research Center «Computer Science and Control» of the Russian Academy of Sciences, 44, bldg. 2, Vavilova st., Moscow, 119333, Russian Federation, tel.: +7 (495) 795-85-24, e-mail: akostogr@gmail.com.

Zubarev Igor, Dr., associate professor, chief scientific officer, Research Institute of Applied Mathematics and Certification, 2, bldg. 2, Krasnobogaryrskaya st., Moscow, 107564, Russian Federation, tel.: +7 (916) 410-31-61, e-mail: zubarev-i@bk.ru.