УДК 681.3

ФУНКЦИОНАЛЬНАЯ СТАБИЛЬНОСТЬ КРИТИЧНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ: ОСНОВЫ АНАЛИЗА

Сундеев П.В. – к. т. н.
Кубанский государственный технологический университет

Анализ сложных информационных систем предполагает применение комплекса методов исследования. В работе предлагается подход системного использования методов анализа и синтеза к исследованию свойств функциональной стабильности критичных информационных систем.

Актуальность проблемы

В результате повсеместной информатизации критичные функции управления передаются под контроль автоматизированных систем (АС). Этот процесс порождает проблему обеспечения функциональной стабильности (ФС) сложных эргатических систем, использующих гибридные человеко-машинные технологии обработки информации. Особенно актуальной проблема ФС является для автоматизированных информационных систем, обеспечивающих функционирование критичных систем управления (КСУ), таких как: системы управления опасными производствами и объектами атомной энергетики; системы управления космическими полетами, воздушным или железнодорожным движением; системы управления военного назначения; системы управления органов государственной власти и другие. Большинство систем этого класса характеризуются критичностью решаемых функциональных задач, территориальной и информационной распределенностью, концентрацией информации ограниченного доступа, использованием биологических и электронных технологий обра-

ботки информации, семантической доступностью для информационного воздействия, временными ограничениями цикла управления и другими свойствами, которые определяют сложность технологических процессов обработки информации и потенциальную опасность при нарушении их ФС.

Таким образом, автоматизированные информационные системы становятся компонентом критичных систем управления, что позволяет выделить их в класс критичных информационных систем (КИС), к которым необходимо предъявлять повышенные требования по ФС из-за опасности последствий нарушения их функционирования.

Критичные информационные системы (КИС) – это класс эргатических информационных систем, реализующих информационные процессы в критичных системах управления. Критичность заключается в потенциальной опасности нарушения их функциональной стабильности, поскольку полный или частичный отказ системы может привести к значительному экономическому, политическому, военному, экологическому, моральному или другим ущербам.

Функциональная стабильность (ФС) – это свойство критичных информационных систем, заключающееся в способности реализовать заданные информационные функции (процессы обработки информации) в условиях воздействия внешних и внутренних дестабилизирующих факторов.

Обеспечение ФС КИС является сложной проблемой, требующей системного решения комплекса взаимоувязанных задач по разработке теоретических положений, методов автоматизированного моделирования и анализа сложных информационных систем, позволяющих проводить их декомпозицию, строить достоверные модели информационной архитектуры и процессов обработки информации, предъявлять требования по ФС и оценивать их реализацию.

Границы управляемости свойств ФС ИС

Границы управляемости свойств ФС ИС определяются на основе методов системного анализа диалектической взаимосвязи информационных и системных свойств материи, отношений между понятиями «функциональная стабильность», «надежность», «информационная безопасность», а также выделения класса КИС в общей иерархии сложноорганизованных информационных систем (рис. 1).

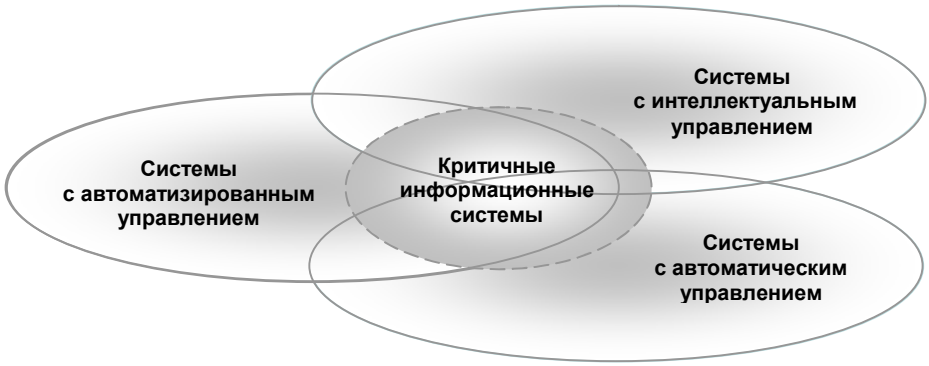


Рисунок 1 – Критичные информационные системы в иерархии сложности эргатических систем

КИС можно отнести к сложноорганизованным эргатическим информационным системам, использующим биологические и компьютерные технологии обработки информации, для которых характерно наличие технологических участков с автоматическим, автоматизированным и интеллектуальным управлением. Последнее обстоятельство усложняет анализ проблемной области, поскольку свойства ФС неоднозначны для информационных систем с разным уровнем сложности структурной организации.

ФС рассматриваемого класса систем определяется как динамическое равновесие в границах допустимых отклонений гомеокинетического плато (рис. 2) [1]. Несогласованность между субъектом и объектом управляющих воздействий, выводящих систему за границы этой области, приводит к функциональной нестабильности и информационному разрушению систе-

мы по причине неспособности к адаптации или изменения целевой функции системы в результате глобальной структурной реорганизации.

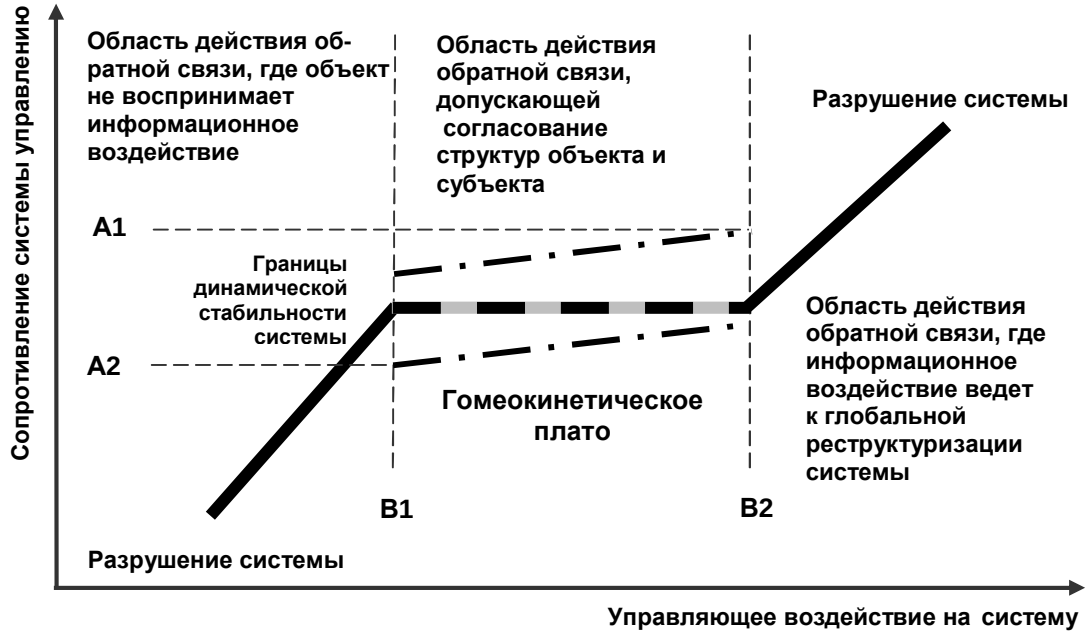


Рисунок 2 – Гомеокинетическое плато сложноорганизованной информационной системы

Область возможного управления ФС сложной ИС определяется на основе иерархической стратификации структуры сложных систем и целевых функций ее подсистем (рис. 3).

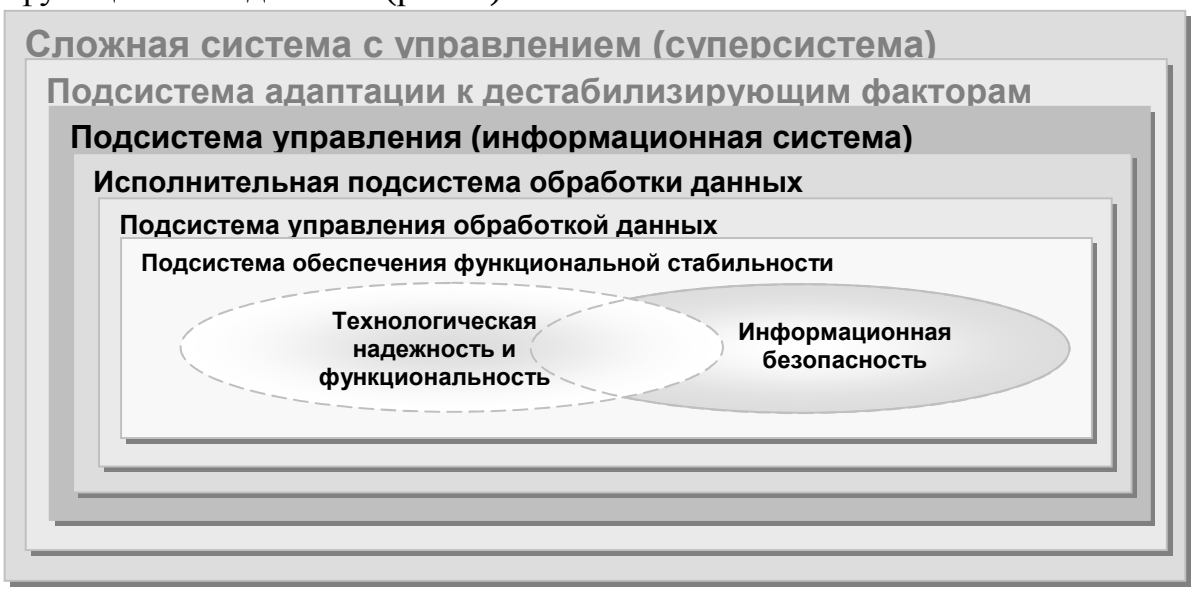


Рисунок 3 – Иерархическая стратификация структуры сложной системы с управлением

Иерархическая стратификация целевых функций подсистем сложной системы с управлением представлена в таблице.

Иерархическая стратификация подсистем и целевых функций

Элементы иерархической структуры сложной системы с управлением	**Иерархия целевых функций**	**Иерархия информационных функций**	**Результат (цель)**
1	2	3	4
Сложная система с управлением (суперсистема)	Обеспечение структурной стабильности системы	—	Целостность системы в течение жизненного цикла
Подсистема адаптации к дестабилизирующим факторам	Адаптация системы к новым условиям с минимальными структурными изменениями	Управление свойствами суперсистемы	Суперсистема с новыми свойствами, обеспечивающими целостность
Подсистема управления (информационная система)	Моделирование суперсистемы и внешней среды	Управление информационными моделями суперсистемы и внешней среды (реализация функциональных алгоритмов)	Модель структуры суперсистемы с новыми свойствами

Продолжение таблицы

1	2	3	4
Исполнительная подсистема обработки данных	Реализация процедур по обработке информационных моделей (данных)	Управление обработкой данных (реализация исполнительных алгоритмов)	Хранение, передача, интерпретация на физическом уровне и трансляция данных
Подсистема управления обработкой данных	Моделирование процессов обработки данных	Управление исполнительной подсистемой обработки данных	Согласование процедур информационного процесса
Подсистема обеспечения функциональной стабильности информационной системы	Обеспечение обработки данных при дестабилизирующих информационных воздействиях	Управление состоянием информационной подсистемы	Функциональная стабильность информационной подсистемы
Подсистема обеспечения технологической надежности элементов	Обеспечение технологической надежности элементов	Управление надежностью элементов информационных технологий	Надежность элементов информационных технологий
Подсистема обеспечения структурной стабильности	Обеспечение структурной стабильности	Управление конфигурацией информационной архитектуры	Конфиденциальность и целостность информации

Окончание таблицы

1	2	3	4
Подсистема обеспечения эксплуатационной надежности	Обеспечение эксплуатационной надежности	Управление работоспособностью системы	Доступность информации и уменьшение простоя системы после сбоев

Анализ возможных дестабилизирующих факторов, структуры и целевых функций сложных информационных систем показал, что ФС для исследуемого класса систем зависит от двух аспектов: уровня технологической надежности и функциональности элементов и подсистем, а также состояния информационной безопасности.

Вопросы надежности и функциональности технических систем достаточно полно исследованы, изложены в теории надежности, прикладных теориях и учитываются на практике при проектировании АС. Влияние аспекта ИБ на ФС менее изучено и наиболее актуально для анализа в конфликтных средах, поскольку он связан с целенаправленным воздействием конкурирующих систем. Поэтому анализ ФС ИС целесообразно ограничить аспектами информационной безопасности с учетом требований по функциональности и надежности.

Повышение адекватности моделирования информационных процессов и систем

Одной из трудноразрешимых задач системного анализа сложных ИС является повышение адекватности моделей информационных процессов и систем их реальным прототипам.

Предлагаются три метода решения этой задачи:

- трехуровневое описание взаимодействия информационных систем;

- визуализация процесса декомпозиции исследуемых систем на основе использования современных компьютерных технологий;

- автоматизация процесса синтеза математических моделей информационных процессов и систем из объектно-ориентированных диаграмм на основе разработанного математического аппарата формального описания состояний системы.

Первый метод основан на предположении о том, что любое информационное взаимодействие между сложными системами реализуется последовательно на физическом, синтаксическом и семантическом уровнях взаимодействия (рис. 4). Причем системы должны иметь соответствующие интерфейсы для взаимодействия на каждом из уровней [2, 3]. Разделив систему на информационные объекты (функциональные модули) и описав все их интерфейсы взаимодействия, можно декларировать относительную полноту множества учитываемых отношений между элементами системы, которые определяют ее поведение и являются предметом анализа функциональной стабильности.

Второй метод повышения достоверности моделирования основан на визуализации процесса построения моделей системы в виде объектно-ориентированных диаграмм. Использование универсального языка моделирования UML и поддерживающих его программных инструментальных средств анализа и проектирования сложных систем позволяют формализовать и автоматизировать процесс синтеза интегрированных моделей системы, снизить зависимость от субъективности аналитика и его ошибок и, как следствие, повысить адекватность моделей. Для возможности декомпозиции информационных систем на информационные объекты и модули необходимо использовать метод классификации элементов системы и связей между ними по информационно-функциональному принципу [3].

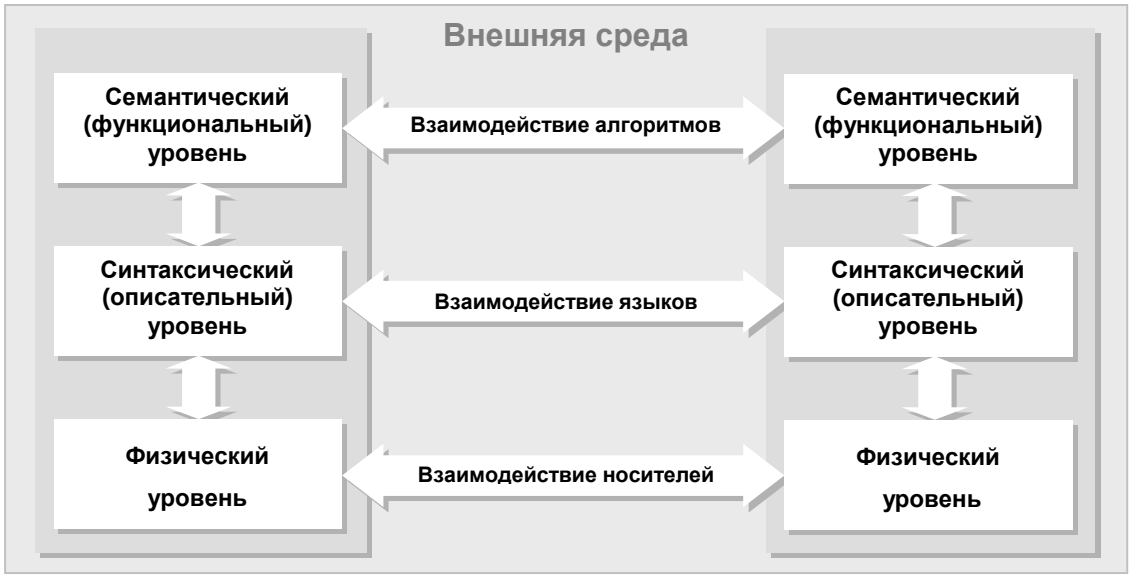


Рисунок 4 – Модель информационного взаимодействия сложных систем

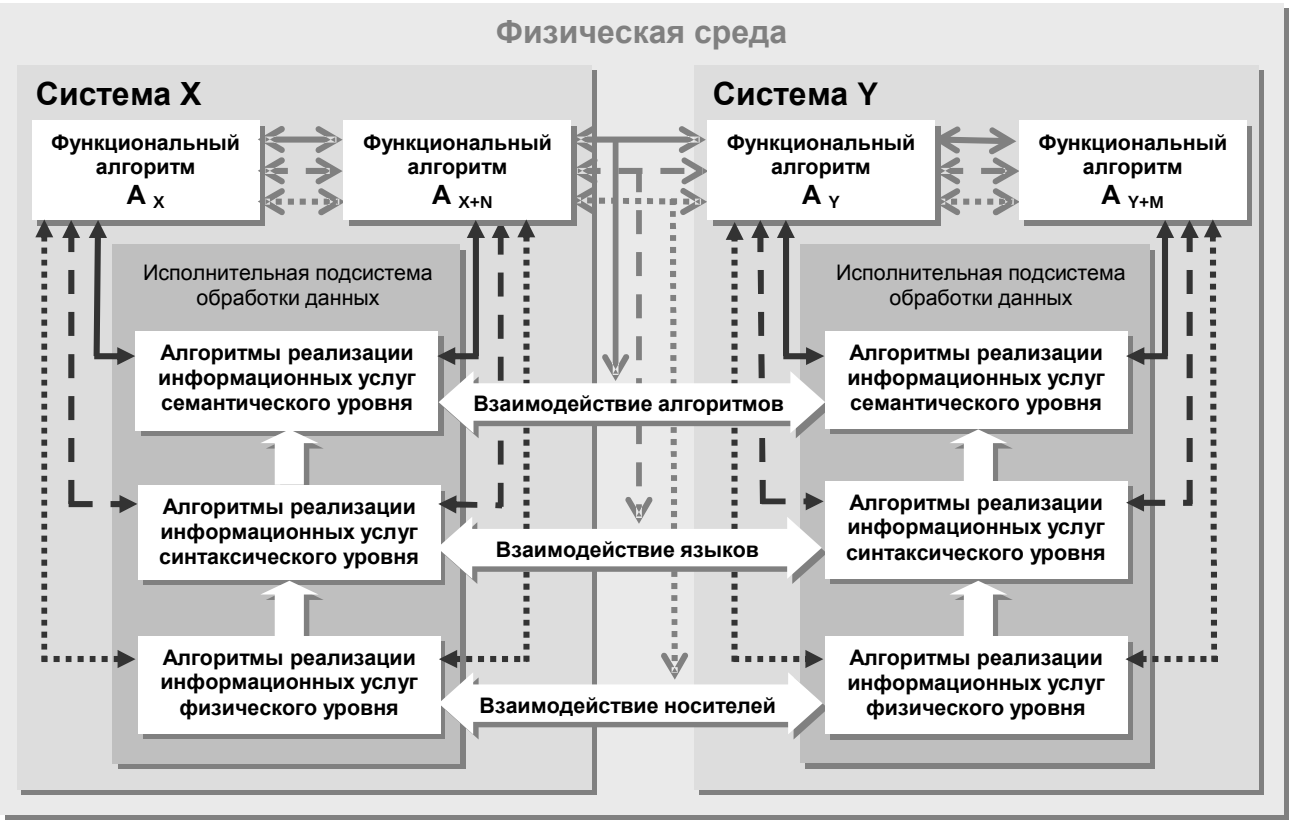
Третий метод повышения достоверности моделирования основан на генерации математических моделей информационной системы из объектно-ориентированных диаграмм. Для его реализации предлагается использовать разработанный математический аппарат формального описания состояний информационной системы [3].

Основные положения теории ФС

Теория ФС позволяет обосновать принципы построения и критерии оценивания функционально стабильных информационных систем в аспекте информационной безопасности. Основой эти положений являются: модель реализации угроз ФС, особенности информационных технологий и концепция построения функционально стабильных систем.

Модель реализации угроз функциональной стабильности при информационном взаимодействии систем демонстрируют отношения на трех уровнях взаимодействия, через которые возможна дестабилизация системы (рис. 5).

Существенным фактором, представленным в модели, является выделение в структуре информационной системы функциональных алгоритмов, предназначенных для интерпретации семантики объектов управления, и исполнительной подсистемы обработки данных, направленной на реализацию информационных услуг по хранению, передаче и преобразованию данных по запросам функциональных алгоритмов. Реализация угроз может осуществиться на любом уровне взаимодействия. Кроме того, взаимодействие функциональных алгоритмов возможно, если они имеют интерфейсы и функции, характерные для исполнительной подсистемы по обработке данных.



Отношения между алгоритмами на семантическом, синтаксическом и физическом уровнях, реализующие информационный процесс

Возможные отношения между алгоритмами на семантическом, синтаксическом и физическом уровнях, дестабилизирующие систему

Рисунок 5 – Модель реализации угроз функциональной стабильности при информационном взаимодействии систем

Представленная модель позволяет ввести систему воздействия дестабилизирующих факторов для анализа ФС КИС.

Особенности используемых технологий обработки информации оказывают существенное влияние на функциональную стабильность КИС.

В КИС используются две полнофункциональные технологии обработки информации: биологическая и электронная. Различием между ними, с точки зрения обеспечения ФС, является способ представления знаний и данных.

Рассмотренная ранее интерпретация модели угроз ФС характерна для технологий обработки информации, представленной на контекстно-независимых языках. В этом случае в системе существуют отдельные информационные объекты, с которыми возможно взаимодействие через несанкционированные информационные каналы. Такими объектами являются технологические участки КИС, использующие компьютерные технологии обработки данных.

Для систем с контекстно-зависимым представлением информации, к которым относятся человек и перспективные интеллектуальные компьютерные системы, основанные на нейросетевых технологиях, внешнее дестабилизирующее информационное воздействие можно реализовать только через штатные входы и выходы системы. Угрозы, направленные на дестабилизацию исполнительной подсистемы обработки данных, для этого случая не актуальны, если она реализована по принципу иерархического предоставления информационных услуг и выполнены требования по информационной безопасности.

Концепция построения функционально стабильных информационных систем основана на стратегии ограничения и контроля доступа к функциональным интерфейсам информационных объектов. Структура концепции и взаимосвязь ее элементов с разрабатываемой методологией

анализа ФС представлены на рисунке 6. Очевидно, что функциональная стабильность системы может быть обеспечена при учете параметров информационного взаимодействия, параметров ФС и системы дестабилизирующих факторов.

Рисунок 6 – Общая структура концепции функциональной стабильности критичных информационных систем

Методология анализа ФС должна предоставить требования к ним и оценить их реализацию при создании функционально стабильных КИС.

Стратификация требований по ФС позволяет выделить уровень, на котором возможно управление свойствами ФС (рис. 7).

Требования к функциональной стабильности КИС можно условно стратифицировать на макросистемный, системный и микросистемный уровни. На макроуровне требования формируются системой управления, в

интересах которой создается информационная подсистема, и определяются информационной политикой, разрабатываемой для поддержки решения функциональных задач, решаемых системой.

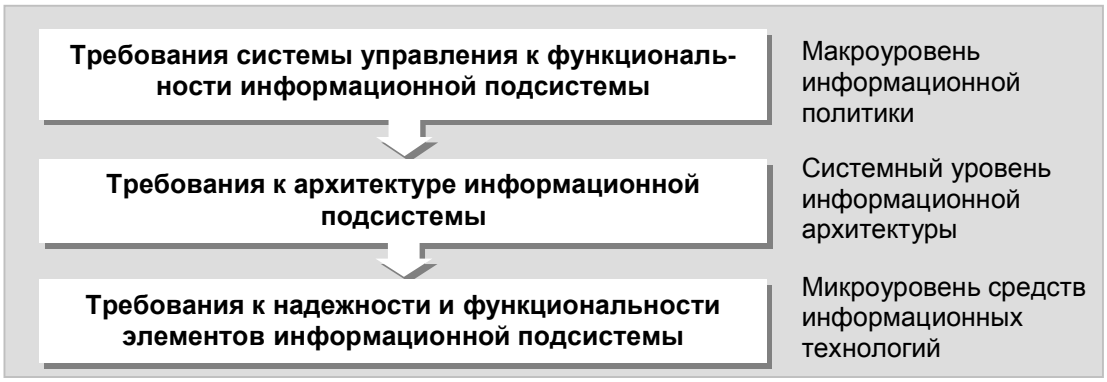


Рисунок 7 – Стратификация требований к функциональной стабильности критичных информационных систем

На микроуровне требования предъявляются к надежности и функциональности элементов информационной системы и определяются развитием технологий. Характеристики информационной системы на макро- и микроуровнях являются слабоуправляемыми. Таким образом, управление ФС информационной системы возможно, в основном, на системном уровне, на котором предъявляются требования к информационной архитектуре и технологии обработки данных, при условии обеспечения надежности элементов системы и корректности требований системы управления. Поэтому анализ ФС целесообразно проводить на системном уровне, т. е. на уровне информационной архитектуры.

Стратегия контроля доступа к функциональным интерфейсам информационных объектов определяет принципы построения архитектуры и организации информационного процесса для функционально стабильных систем.

В системе выделяются информационные объекты, способные выполнять стандартные функции по обработке информации на трех уровнях ин-

формационного взаимодействия. Функциональность объектов определяется наличием у них открытых интерфейсов для каждого из уровней. Возможность взаимодействия определяется нахождением объектов в одной зоне доступа и наличием у них парных интерфейсов. Поскольку уровни взаимодействия иерархичны, то возможность взаимодействия на вышестоящем уровне реализуется в зависимости от наличия его на всех нижестоящих уровнях. Зоны физического, синтаксического или семантического доступа характеризуются архитектурой системы и средствами разграничения доступа на соответствующих уровнях.

Система считается функционально стабильной, если в ходе информационного процесса ее информационные объекты находятся в разрешенных для них зонах доступа. Система считается функционально нестабильной, если в ходе информационного процесса в зону возможного взаимодействия попадают объекты, отношения между которыми считаются опасными для функционирования системы. Эти положения являются критерием оценки ФС КИС, основанным на регламентации логики взаимодействия функциональных элементов и подсистем.

Анализ ФС на системном уровне заключается в поиске траекторий перехода системы в опасные состояния, что является основной проблемой при проектировании, эксплуатации и модернизации КИС, которые должны иметь определенный уровень функциональной стабильности. Для определения всех или почти всех (т. е. относительно полного множества) траекторий перехода системы в опасные состояния необходима методология, позволяющая моделировать архитектуру и информационные процессы систем, формализовать состояния любых информационных систем, проводить анализ функциональной стабильности.

Методологический подход к автоматизации анализа ФС КИС

Методология построения моделей и анализа ФС КИС включает несколько этапов (рис. 8).

Рисунок 8 – Последовательность анализа ФС КИС

На первом этапе проводится информационное и техническое обследование системы управления с целью выявления информационных объектов и отношений между ними, описания информационных интерфейсов на трех уровнях взаимодействия.

Содержательный анализ информационной архитектуры системы проводится с целью структуризации исходных данных для последующего моделирования.

Сложность объекта исследования и размерность модели требуют применения специальных методов моделирования. Наиболее перспективным для данного случая является использование методологий функционально-структурного и объектно-ориентированного моделирования и анализа сложных систем, поддерживаемых CASE-средствами, которые позволяют визуализировать и автоматизировать процесс построения модели.

Технология автоматизации анализа и моделирования сложных информационных систем

Построение интегрированных визуальных моделей информационной системы основано на возможности представления ее архитектуры в виде мультиграфа, который изображается как объектно-ориентированные диаграммы (рис. 9).

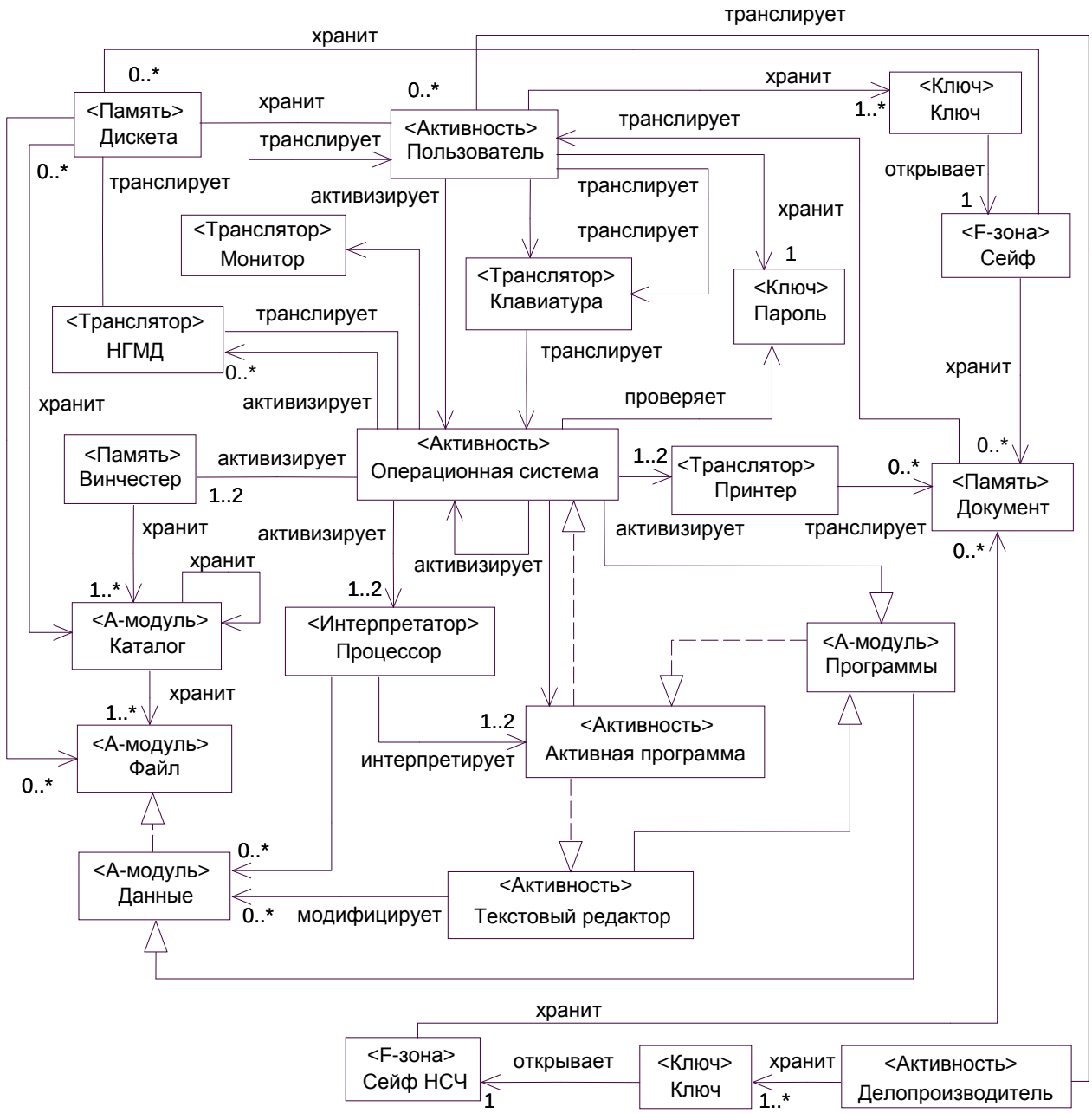


Рисунок 9 – Упрощенный фрагмент диаграммы для сегмента ИС после определения стереотипов для классов, объектов и зависимостей

Вершинами графа являются информационные объекты и классы системы, дуги нагружаются информационными отношениями.

Взаимодействие объектов и классов в ходе информационного процесса ограничивается архитектурой системы, интерфейсами объектов и средствами разграничения доступа, которые логически или физически разделяют систему на физические, синтаксические и семантические зоны. Нахождение информационных объектов в одной зоне доступа при совпадении соответствующих интерфейсов предполагает возможность их взаимодействия и, следовательно, изменения состояния системы.

Формальное описание информационной архитектуры системы и процессов обработки информации

Задачей анализа ФС КИС является нахождение всех возможных траекторий информационного процесса, способных привести систему в опасные состояния. Для ее решения необходимо перевести визуальные диаграммы КИС на язык математической логики, описав объекты, их интерфейсы, опасные и безопасные состояния и правила перехода состояний в виде предложений формальной логики исчисления предикатов первого порядка.

Граф состояний модели КИС представляет собой направленный граф переходов, отображающий изменения состояния исследуемой КИС, т. е. ее поведение, определяемое архитектурой системы и технологией обработки данных. Вершинами этого графа являются элементы из множества состояний, а ребра нагружены событиями из множества событий (рис. 10).

Решение прямой задачи анализа ФС КИС состоит в определении отсутствия траекторий, приводящих систему в опасные состояния, при установлении конкретных типов информационных отношений между информационными объектами.

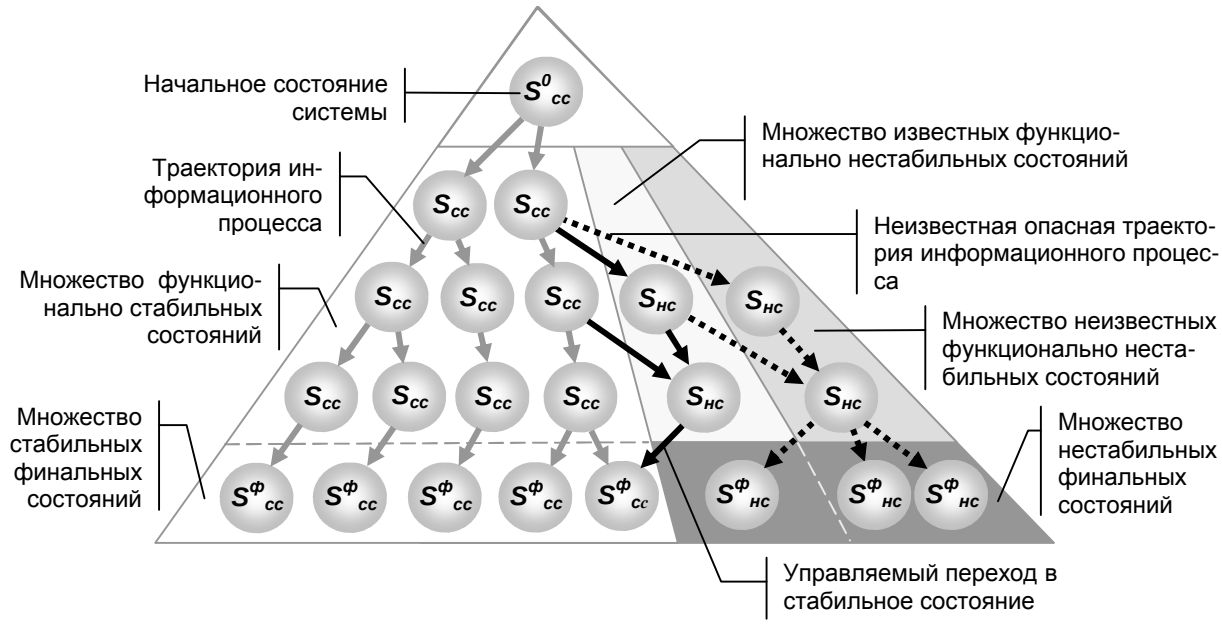


Рисунок 10 – Граф возможных состояний критичной информационной системы

Общая последовательность описания ситуации и доказательства ФС КИС в указанном смысле представлены в [3, 4].

Генерация теорем и аксиом в виде формальных высказываний математической логики исчисления предикатов может осуществляться автоматически из объектных диаграмм и диаграмм классов на основе исходных данных о структуре ориентированного графа, свойствах его вершин и дуг, полученных на этапе объектно-ориентированного анализа КИС, при наличии совместимого с CASE-средством (например, Rational Rose) компилятора для языка типа Пролог.

Научно-методический аппарат, объединяющий в рамках единой методологии основные положения теории ФС КИС, методы формализации состояний, автоматизации моделирования и поиска функционально нестабильных состояний с формальным доказательством отсутствия запрещенных траекторий, приводящих систему в опасные состояния, позволяет проводить объективную оценку и гарантировать функциональную стабильность информационных систем, используемых в критичных приложениях.

Список литературы

1. Лачинов В.М. Информодинамика или путь к миру открытых систем / В.М. Лачинов, А.О. Поляков. Изд. 2, перераб. и доп. – Спб.: Изд-во СпбГТУ, 1999.

2. Сундеев П.В. Построение информационной модели функционирования обобщенной системы управления и обоснование фундаментальных принципов информационного взаимодействия сложных систем // Межвузовский сборник научных трудов. – Краснодар: КВИ, 2000.

3. Симанков В.С. Системный анализ функциональной стабильности критичных информационных систем: Монография / В.С. Симанков, П.В. Сундеев. – Краснодар: Институт современных технологий и экономики, 2003. – 132 с.

4. Сундеев П.В. Автоматизация анализа функциональной стабильности критичных информационных систем // Научный журнал КубГАУ. – 2004. – № 3. – http//ej.kubagro.ru.