На правах рукописи

Филиппов Михаил Николаевич

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛЕЙ И МЕТОДОВ ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ДИСПЕТЧЕРСКОГО УПРАВЛЕНИЯ

05.13.18 «Математическое моделирование, численные методы и комплексы программ»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Новосибирск — 2009

Работа выполнена в Институте автоматики и электрометрии
Сибирского отделения Российской академии наук

Научный руководитель	доктор технических наук Золотухин Юрий Николаевич
Официальные оппоненты:	доктор технических наук Резник Александр Львович
	кандидат технических наук Чейдо Геннадий Петрович
Ведущая организация	Институт систем информатики им. А. П. Ершова Сибирского отделения Российской академии наук

Защита диссертации состоится «____» *декабря* 2009 г. в ____ час. на заседании диссертационного совета Д 003.005.01 в Институте автоматики и электрометрии СО РАН по адресу: 630090, г. Новосибирск, просп. Акад. Коптюга, 1.

С диссертацией можно ознакомиться в библиотеке Института автоматики и электрометрии СО РАН.

Автореферат разослан «____» *ноября* 2009 г.

Ученый секретарь
диссертационного совета
д. ф.-м. н. Насыров К. А.

Общая характеристика работы

Актуальность работы. Среди широкого спектра автоматизированных систем диспетчерского управления (АСДУ) особое место занимают программно-аппаратные комплексы, предназначенные для использования на объектах повышенной опасности, таких как предприятия атомной и химической промышленности, транспортные комплексы, объекты военного назначения и т. п., нарушения в работе которых представляют прямую угрозу жизни и здоровью людей. Помимо высокой надежности при работе в штатном режиме подобные системы должны обеспечивать предсказуемо-безопасное поведение в случае выхода из строя отдельных компонентов.

В отличие от полностью автоматической системы АСДУ предполагает первостепенное и активное участие человека, осуществляющего функции оперативного управления, поэтому анализ отдаваемых им команд и блокирование ошибочных действий в режиме реального времени является необходимым условием обеспечения безопасности, позволяющим уменьшить влияние так называемого «человеческого фактора».

В настоящее время многие предприятия нуждаются в модернизации разработанных много лет назад и уже морально устаревших систем управления. Также не менее часто, чем отжившее свой век оборудование и программное обеспечение (ПО), на практике встречается построенная на основе достаточно современных компонентов так называемая лоскутная автоматизация, представляющая собой набор разнородных слабо связанных информационных подсистем, следствием чего является низкая скорость обмена данными, дублирование, увеличение времени обработки, снижение уровня контроля ситуации и, в конечном итоге, общая неэффективность системы управления. В то же время интенсивное усложнение и увеличение масштабов производства приводит к необходимости использования интегрированных средств, построенных на основе современных достижений вычислительной техники.

Ограничения, наиболее важные из которых перечислены выше, а также перечень требований, регламентируемых государственными, отраслевыми и внутренними стандартами предприятий, не позволяют найти приемлемое универсальное решение среди существующих, поэтому становится актуальной проблема ***разработки и исследования моделей и методов построения автоматизированных систем диспетчерского управления***, удовлетворяющих поставленным условиям, включая экономическую целесообразность.

В процессе решения основной задачи особое внимание должно быть уделено анализу различных характеристик создаваемой системы, основными из которых являются надежность, безопасность и живучесть. И если в случае аппаратной части, составленной из стандартных компонентов, можно воспользоваться предоставляемыми производителями данными о среднем времени наработки на отказ, сроке службы и т. п., то для программной части использование статистического подхода, по крайней мере на первом этапе, неприменимо ввиду уникальности разработки и планируемого штучного использования. Эти обстоятельства приводят к необходимости исследования методов оценки параметров подобных систем с учетом имеющейся зачастую косвенной или неполной информации.

Целью диссертационной работы являлись разработка и исследование методов построения автоматизированных систем диспетчерского управления повышенной надёжности. В соответствии с поставленной целью требовалось решить следующие задачи:

- исследовать типовые модели систем диспетчерского управления, выделить стандартные элементы и создать на их основе *архитектуру автоматизированной системы диспетчерского управления* с повышенным уровнем надежности и безопасности;
- *разработать открытую модульную многоплатформенную SCADA-систему* (Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных), поддерживающую предложенную архитектуру АСДУ и предназначенную для создания многоуровневых программных комплексов с распределённым резервированием;
- *осуществить анализ характеристик разработанных архитектуры и программного обеспечения* на основе предложенных способов оценки надежности, учитывающих экспертные данные и информацию о процессе создания программного обеспечения, а также разработать имитационную модель, предназначенную для анализа сценариев отказа оборудования и программного обеспечения;
- *реализовать предложенные решения в виде программных комплексов* при построении АСДУ движением поездов Новосибирского метрополитена, в частности, создать на основе разработанной SCADA-системы программное обеспечение автоматизированных рабочих мест оперативного и эксплуатационного персонала.

Научная новизна. Предложена *архитектура* АСДУ, основанная на использовании равноправных асинхронно работающих узлов и обеспечивающая высокий коэффициент готовности, многоуровневый контроль действий оператора, возможность динамического изменения конфигурации и повышенную живучесть системы.

Предложен *метод построения модульной SCADA-системы* на основе разработанной концепции динамического программного интерфейса, позволяющий создавать программные комплексы со сложными логическими зависимостями между частями, составляя динамическую конфигурацию из подгружаемых модулей, а также использовать программное обеспечение с открытым исходным кодом.

Предложен *метод обработки данных на основе варианта трёхзначной логики*, позволяющий наряду с точными данными оперировать неполной и недостоверной информацией, унифицируя и упрощая запись логических выражений.

Предложен *метод оценки основных характеристик надежности программного обеспечения по информации, сохраняемой системой управления версиями*, позволяющий учесть особенности индивидуальной истории создания продукта, такие как скорость внесения изменений в текст программы, интенсивность выявления ошибок, их тип и потребовавшееся на исправление время, полнота предоставленных спецификаций и частота появления новых требований в процессе разработки.

На основе теории нечетких множеств разработан *способ уточненной оценки коэффициента готовности системы*, учитывающий экспертные поправки к среднему времени наработки на отказ и продолжительности ремонтов.

Методы исследования. Для решения поставленных задач использовались методы теории управления, теории надежности, элементы теории нечетких множеств, математической логики и теории массового обслуживания, а также имитационное моделирование.

Практическая значимость и внедрение результатов. Разработанные архитектура и программное обеспечение могут быть использованы при создании многоуровневых распределенных автоматизированных систем диспетчерского управ-

ления с повышенными требованиями к надежности и безопасности, а также возможностью поэтапной модернизации путем интеграции с существующими программно-аппаратными комплексами.

На основе предложенной архитектуры разработана система диспетчерского управления движением поездов Новосибирского метрополитена. Программное обеспечение, созданное с помощью разработанной SCADA-системы, функционирует на станциях «Березовая роща», «Маршала Покрышкина», «Площадь Гарина—Михайловского», «Заельцовская» и «Красный проспект».

Основные положения, выносимые на защиту:

- разработанная архитектура автоматизированной системы диспетчерского управления обеспечивает более высокий коэффициент готовности по сравнению с классической схемой «основной-резервный»;
- предложенный метод обработки данных на основе варианта трёхзначной логики позволяет унифицировать и упростить запись логических выражений при обработке неполной и недостоверной информации;
- разработанный метод расчета основных характеристик надежности программного обеспечения по информации, сохраняемой системой управления версиями, позволяет оценить остаточное количество ошибок ПО;
- предложенный метод оценки параметров надёжности, разработанный на основе теории нечетких множеств, позволяет наряду со статистическими распределениями учитывать предоставляемую экспертами неточную информацию.

Апробация работы. Основные результаты работы были изложены и обсуждались на следующих научно-технических конференциях и семинарах:

- VI Международный семинар «Распределенная обработка информации», Новосибирск, 1998 г.;
- the IASTED International Conference “Automation, Control, and Information Technology (ACIT 2002)”, Новосибирск, 2002 г.;
- the Second IASTED International Multi-Conference “Automation, Control, and Applications (ACIT-ACA 2005)”, Новосибирск, 2005 г.;
- VII, VIII, IX и X Международные конференции «Проблемы управления и моделирования в сложных системах», Самара, 2005–2008 гг.;
- Международная школа-конференция молодых ученых «Информационно-коммуникационные системы», Новосибирск, 2006 г.;
- научно-практическая конференция молодых ученых и студентов НГУ и ИАиЭ СО РАН «Информационно-вычислительные системы анализа и синтеза изображений», Новосибирск, 2006 г.;
- IV Всероссийская школа-семинар молодых ученых «Проблемы управления и информационные технологии», Казань, 2008 г.;
- VII Международная конференция памяти академика А. П. Ершова «Перспективы систем информатики», Новосибирск, 2009 г.

Публикации. По результатам выполненных в диссертационной работе исследований и разработок опубликовано 17 печатных работ, включая три статьи в рекомендованных ВАК журналах.

Личный вклад автора. Все выносимые на защиту положения и результаты диссертационной работы получены и разработаны автором лично или при его непосредственном участии.

Структура и объем работы. Диссертация состоит из введения, пяти глав, за-

ключения, пяти приложений и списка цитируемой литературы из 156 наименований и изложена на 162 страницах, включает 15 рисунков и 8 таблиц.

Содержание работы

Во введении обоснована актуальность темы исследования, определены цели и задачи работы, сформулированы научная новизна и практическая значимость полученных результатов, приведены основные положения, выносимые на защиту.

В первой главе представлена предложенная архитектура автоматизированной системы диспетчерского управления, в основу которой положена концепция равноправных асинхронно работающих узлов с параллельной рассылкой команд по постоянно поддерживаемым виртуальным соединениям, и приводится обоснование принятых решений.

Исследование стандартных схем построения автоматизированных систем диспетчерского управления показало, что общепризнанной с точки зрения процесса преобразования информации является распределённая многоуровневая иерархическая архитектура, включающая: уровень объекта управления (или нижний уровень), который обеспечивает получение и первичную обработку информации от внешних устройств, а также выдачу управляющих воздействий на исполнительные механизмы; опциональный уровень местного управления, позволяющий с одного или нескольких резервных автоматизированных рабочих мест (АРМ) поддерживать функционирование системы в случае потери связи с удаленным верхним уровнем, который, в свою очередь, включает рабочие места диспетчеров и средства интеграции с другими частями общей информационной системы, такие как шлюзы внешнего доступа, базы данных и серверы прочих служб.

В качестве примера представлен средний уровень АСДУ движением поездов метрополитена, одной из основных задач которого является предоставление информации поездному диспетчеру и передача команд на уровень объекта управления, причем отдаваемые команды анализируются программным обеспечением с целью предотвращения несогласованных и потенциально опасных действий, способных привести к аварийной ситуации.

Для соблюдения данного требования каждое действие оператора анализируется независимо друг от друга тремя различными подсистемами. На первом этапе проверку осуществляет программное обеспечение АРМ поездного диспетчера, которое, в отличие от ПО АРМ дежурного по станции, обладает базовой информацией о состоянии всей линии метрополитена и, в частности, о положении каждого участвующего в движении поезда в данный момент времени.

Затем получившая подтверждение команда пересылается на конкретную станцию метрополитена, где анализируется функционирующим на АРМ дежурного по станции модулем логики, в распоряжении которого находятся более полные сведения о состоянии контролируемого участка линии. На данном этапе производятся установленные регламентом проверки, связанные с безопасностью движения, такие как проверка свободности участков пути, проверка отсутствия установленных враждебных маршрутов и т. п.

На следующем этапе команда поступает в контроллер, где анализируется согласно ограниченному с целью снижения объема вычислений и повышения быстродействия набору наиболее актуальных проверок, чем обеспечивается оперативная реакция на изменение поездной ситуации. Наконец, на заключительном этапе команда, проверенная программным обеспечением всех уровней, преобразуется кон-

троллером в выходные сигналы для исполнительного оборудования. При этом многоуровневый анализ действий диспетчера производится несколькими подсистемами, которые реализованы независимыми разработчиками с использованием различных языков программирования, чем обеспечивается необходимый уровень диверсификации.

Существенным отличием предложенной архитектуры АСДУ от классической схемы с иерархией «основной-резервный» является параллельная рассылка копий команд управления по нескольким независимым каналам (рис. 1). Принимаемые команды анализируются асинхронно работающими равноправными серверами перед отправкой на низлежащий уровень (контроллер); последний, в свою очередь, выполняет первую полученную команду и запоминает ее уникальный идентификатор вместе с результатом исполнения, которые затем используются при формировании ответов на поступающие позже копии.

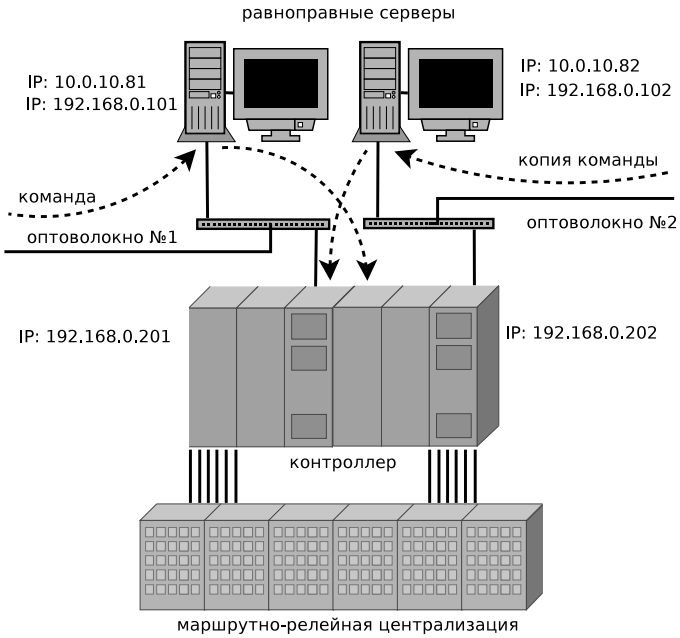

Рис. 1. Архитектура АСДУ на основе равноправных серверов

Таким образом, при выходе из строя одного из каналов доставки и обработки команд, включая компьютеры, маршрутизаторы, оптоволоконный кабель, сетевой модуль контроллера и т. п., обеспечивается выполнение задания и получение ответа на отправленный запрос. При этом отсутствуют обычные в таких случаях (и зачастую существенные) задержки на ожидание перед переключением на резервное оборудование.

На момент получения команды внутренние состояния модулей логики серверов в общем случае различны, поскольку, работая в асинхронном режиме, они опрашивают контроллер в различные моменты времени. Как показано в разделе, посвященном оценке надежности программного обеспечения главы 4, это значительно уменьшает вероятность одновременного отказа обоих узлов в случае ошибок, проявляющихся при определенных состояниях входов системы.

Главным достоинством предложенной архитектуры является обеспечение многоуровневого анализа безопасности действий оператора, повышенной живучести системы и восстановления рабочего состояния в случае выхода из строя ее составляющих. Дополнительное преимущество схемы с равноправными серверами состоит в возможности изменения конфигурации без перезапуска остальной части системы, например, подключение дополнительных резервирующих узлов и линий связи, выключение части оборудования на профилактическое обслуживание, а также поэтапная замена программного и аппаратного обеспечения с предварительным тестированием в параллельном режиме.

Во второй главе изложены предпосылки создания и особенности реализации открытой модульной многоплатформенной SCADA-системы, поддерживающей распределённое резервирование и предназначенной для создания многоуровневых программных комплексов повышенной надежности и безопасности.

В настоящее время подавляющее большинство SCADA-систем предназначено

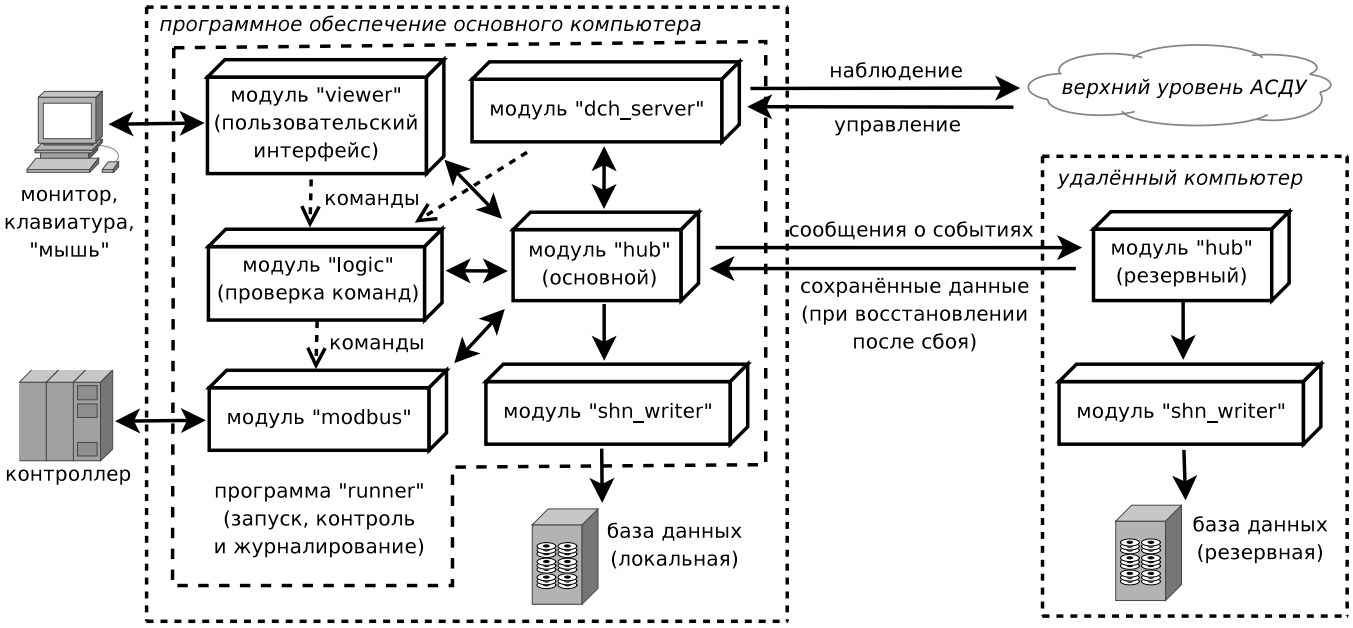

Рис. 2. Типовая конфигурация модулей ПО АРМ дежурного по станции

для использования исключительно в операционной системе Windows, а буквально единицы оставшихся либо не составляют им конкуренции в плане функциональности, либо разработаны для какой-либо конкретной операционной системы и не являются многоплатформенными. Это является серьезным препятствием при разработке распределенных систем, в которых к некоторым узлам предъявляются повышенные требования по отказоустойчивости (что требует использования хорошо зарекомендовавших себя решений на базе операционных систем QNX или GNU/Linux), а второстепенные узлы, реализующие только функции наблюдения, могут представлять собой стандартные персональные компьютеры с более привычной для пользователей и обслуживающего персонала операционной системой Windows.

Не менее важным фактором при выборе программного обеспечения является возможность доступа к исходным текстам с целью непредвзятого анализа надежности, исследования недокументированных особенностей поведения и, при необходимости, независимого от разработчика и оперативного расширения функциональности.

В рамках диссертационной работы сформулированы спецификации открытой многоплатформенной SCADA-системы. При её разработке активно использован принцип модульности для обеспечения расширяемости архитектуры, упрощения повторного использования кода, а также для повышения надежности программы.

Внутренняя архитектура подчинена разработанной концепции динамического программного интерфейса, основной идеей которого является организация всех разделяемых между частями системы точек взаимодействия в виде единой динамически изменяющейся структуры. С точки зрения модуля регистрация (или публикация) собственного интерфейса выглядит как операция создания нескольких элементов в специализированной виртуальной файловой системе, поддерживающей функции работы с объектами, организованными в виде древовидной структуры с узлами-каталогами, а в качестве имени-идентификатора выступает строка с символом-разделителем между элементами – путь от корневого каталога до конкретного объекта.

В качестве иллюстрации (рис. 2) приведена типовая конфигурация ПО АРМ дежурного по станции, состоящая из шести одновременно работающих модулей, ко-

торые взаимодействуют по протоколу TCP/IP: модуль маршрутизатора (*hub*) предназначен для пересылки сообщений между компонентами системы; модуль пользовательского интерфейса (*viewer*) обеспечивает отображение графической информации на экране оператора и передачу вводимых команд модулю логики (*logic*) для дальнейшей обработки; модуль связи (*modbus*) пересылает проверенные модулем логики команды в контроллер, а также периодически опрашивает состояние переменных контроллера и генерирует сообщения об изменениях; модуль базы данных (*shn_writer*) заносит в неё записи об изменении состояния системы; наконец, модуль *dch_server* обеспечивает связь с верхним уровнем АСДУ.

Все конфигурационные файлы системы, включая описания отображаемых на экране объектов, основаны на формате XML, что предоставляет разработчику возможность выбора не только оптимального в каждом конкретном случае приложения-редактора, но и системы управления версиями для работы со всеми файлами программного продукта, включая графическую информацию.

Интегрированная поддержка сценариев позволяет реализовать концепцию выработки для конкретной задачи предметно-ориентированного языка и значительно сократить объем работы программиста, а также повысить надежность программного обеспечения благодаря корректной обработке интерпретатором типичных ошибок исполнения (например, деление на нуль или выход за границы массива) – это не приводит к краху программы, а позволяет получить в обработчике исключения полную информацию о конкретной строчке кода, вызвавшей сбой.

Предложенная архитектура позволяет разрабатывать программные комплексы со сложными логическими зависимостями между частями, составляя динамическую конфигурацию из подгружаемых модулей. К настоящему времени на основе разработанной SCADA-системы создано программное обеспечение АСДУ Новосибирского метрополитена.

При разработке систем управления сложными объектами, как правило, возникает необходимость обеспечить предсказуемо-безопасное поведение в условиях поступающей неполной или недостоверной информации. В первую очередь это относится к распределённым системам с большим количеством входных датчиков и линий связи различной степени надежности; для корректной обработки получаемых данных в этом случае требуется использование специальных математических методов.

С этой целью **в третьей главе** предложен метод обработки данных на основе варианта трёхзначной логики, представляющего собой расширение классической бинарной логики дополнительным истинностным значением, которое интерпретируется как отсутствие в данный момент информации о точном значении переменной или нарушение одного из заданных ограничений значения переменной во время вычисления выражения. Преимуществом данного метода является то, что он позволяет наряду с точными данными оперировать неполной и недостоверной информацией, унифицируя и существенно упрощая при этом запись логических выражений.

В рамках предложенного математического аппарата обработка данных производится в соответствии с логическими выражениями, записанными с помощью стандартного набора операторов, которые определены на расширенном истинностным значением «неизвестно» множестве возможных значений аргументов и результата таким образом, что сохраняют при этом классический результат вычисления, если все аргументы определены («истина» или «ложь»).

Таблицы истинности логических операторов, в соответствии с которыми производится обработка троичных данных, представлены в табл. 1; два наиболее существенных принципа их построения:

- сводимость к классической двузначной логике в случае, когда все аргументы функции принимают значения только «истина» (t) или «ложь» (f) ($F_{ternary}(x_1, x_2, \dots) \equiv F_{binary}(x_1, x_2, \dots)$, если все $x_i \in \{t,f\}$);
- если аргумент функции «неизвестен» (u), и при его изменении как на «истину», так и на «ложь» значение функции не изменяется (C), то результат вычисления принимается равным данной константе (если $F(\dots, t, \dots) \equiv F(\dots, f, \dots) \equiv C$, то $F(\dots, u, \dots) \equiv C$), в противном случае результат вычисления также «неизвестен» ($F(\dots, u, \dots) \equiv u$).

Табл. 1. Основные логические операторы

x	$\neg x$
t	f
f	t
u	u

$\vee$	t	f	u
t	t	t	t
f	t	f	u
u	t	u	u

$\wedge$	t	f	u
t	t	f	u
f	f	f	f
u	u	f	u

$\rightarrow$	t	f	u
t	t	f	u
f	t	t	t
u	t	u	u

$\equiv$	t	f	u
t	t	f	u
f	f	t	u
u	u	u	u

Полученный математический аппарат использован при создании SCADA-системы, предназначенной для разработки автоматизированных систем управления повышенной надежности. Программная среда предоставляет разработчику стандартный набор функций, позволяющий записывать выражения в привычном виде при операциях как с логическими (*not, and, or,* == и т. д.), так и с численными (<, <=, ==, *!=*, >, >= и т. п.) переменными, существенно облегчая тем самым обработку неполной и недостоверной информации в соответствии с описанными выше принципами.

Предложенный подход позволяет снизить сложность программного обеспечения и тем самым добиться повышения надёжности, что особенно актуально при создании автоматизированных систем управления, насчитывающих значительное количество входных сигналов, а поступающая информация обрабатывается логическими условиями со множеством аргументов. При этом программная реализация обеспечивает механизм автоматического переключения на работу в безопасном режиме тех подзадач, для корректного выполнения которых в данных момент недостаточно информации, а также позволяет локализовать некоторые типичные ошибки программирования и спецификаций аппаратной части.

Практическое применение метода, основанного на использовании описанного варианта трёхзначной логики и унифицирующего обработку наряду с точными данными неполной и недостоверной информации, позволяет упростить разработку программного обеспечения, а также обеспечить корректное поведение и повысить надёжность всей системы управления.

В четвертой главе представлены разработанные методы оценки основных характеристик надежности, а также имитационная модель предложенного программно-аппаратного комплекса системы управления.

Известен ряд методов оценки надежности программного обеспечения (модели Холстеда, Нельсона, Джелински—Моранды и др.), учитывающих широкий спектр различных параметров, таких как размер исходных текстов и используемые языки программирования, количество модулей и связей между ними, интенсивность выявления ошибок в процессе тестирования, эффективность организации управления проектом и уровень квалификации сотрудников и т. п., но при этом в большин-

стве моделей не уделяется должного внимания существенным факторам, играющим свою роль во время создания данного конкретного продукта, в первую очередь, это полнота предоставленных спецификаций и частота появления новых требований в процессе реализации и тестирования, тип выявленных ошибок и потребовавшееся на исправление время, скорость внесения изменений в текст программы и прочие характеристики индивидуальной истории разработки.

С другой стороны, создание масштабного программного продукта коллективом разработчиков сегодня практически невозможно представить без использования современных систем управления версиями, существенно облегчающих работу с изменяющейся информацией, автоматизируя хранение исходных текстов и сопутствующей документации.

В первом параграфе четвёртой главы представлен разработанный метод оценки основных характеристик надёжности программного обеспечения, позволяющий учесть особенности индивидуальной истории создания программы, заключающийся в выявлении зависимости количества значимых изменений кода от фактического времени разработки по предоставляемой журналом системы управления версиями информации и экстраполяции полученной функции с целью получения числовых оценок остаточного количества ошибок и скорости их обнаружения.

Представлен пример практического применения разработанного метода для оценки характеристик программного обеспечения системы управления движением поездов станции «Заельцовская» Новосибирского метрополитена.

На рис. 3 приведён построенный по записям журнала системы управления версиями график времени выпуска версии программы, начиная с момента получения предварительных спецификаций 28 сентября 2007 г. и заканчивая установкой программы на станции в режим опытной эксплуатации 21 мая 2008 г.; всего за этот период в исходный текст программы было внесено 407 изменений. В нижней части рисунка для удобства дальнейшего рассмотрения исключены наиболее заметные интервалы времени, в течение которых разработка программы была приостановлена по различным причинам, таким как участие сотрудников в других проектах и конференциях, праздничные дни, дни отпуска и т. п.

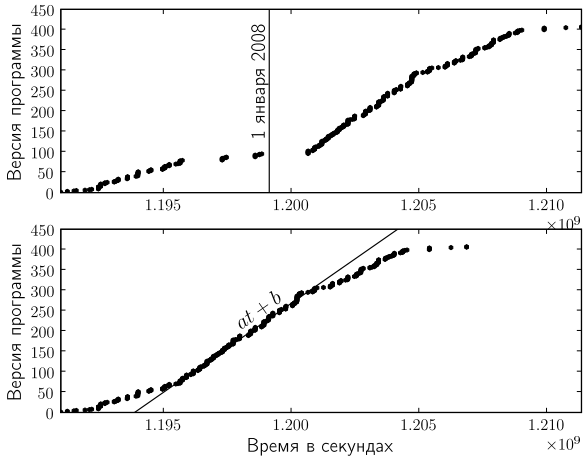

Рис. 3. Версия программы от времени разработки

При анализе данного графика целесообразно выделить три основные части: первая соответствует начальному периоду разработки, во время которого проводится уточнение спецификаций, планируется внутренняя архитектура ПО и создаются прототипы основных модулей. На данном этапе скорость внесения изменений относительно невелика, затем она постепенно увеличивается и достигает максимального значения к средней части графика.

В течение следующего периода, который соответствует времени активной разработки, кривая подчиняется простой линейной зависимости $at + b$. Объясняется это тем, что, несмотря на готовый план работы и четкие спецификации программ-

ных интерфейсов, скорость внесения изменений ограничена производительностью труда коллектива разработчиков.

Наконец, последняя часть графика вновь демонстрирует уменьшение скорости внесения изменений и отражает плавный переход от активной разработки к процессу тестирования, описываемому принципиально другой зависимостью (рис. 4), которая и представляет наибольший интерес с точки зрения оценки основных характеристик надежности поступающего в эксплуатацию программного обеспечения. Наблюдаемые данные на этом участке хорошо аппроксимируются зависимостью

$$N(1 - e^{-(t/\lambda)^k}).$$

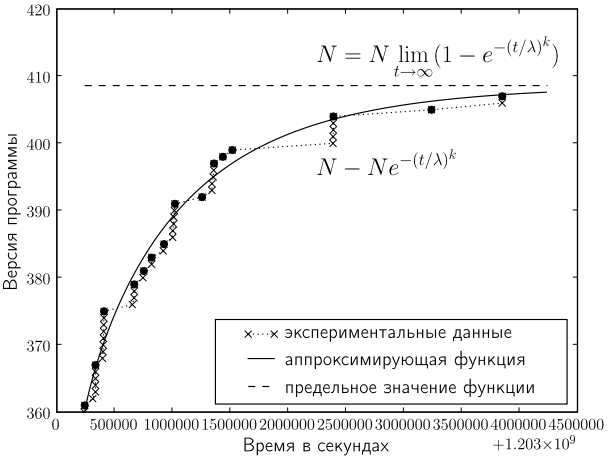

Рис. 4. Версия программы от времени тестирования

Исследование ряда других программ с сохранившимися журналами системы управления версиями подтвердило, что выявленная закономерность с хорошей степенью точности описывает период заключительного тестирования программного обеспечения, непосредственно предшествующий сдаче его в эксплуатацию.

При этом получаемые по методу наименьших квадратов коэффициенты позволяют оценить количество ошибок на момент начала тестирования, эффективность выбранных методик тестирования и практическую скорость выявления ошибок, а также качество конечного продукта по оценке количества ошибок, оставшихся невыявленными к моменту окончания работ, которая на основании существующего предела полученной функции имеет вид

$$n(t) = Ne^{-(t/\lambda)^k}. \tag{1}$$

Для получения количественных характеристик надежности, в частности среднего времени наработки до отказа, использована модель нестационарного пуассоновского процесса. После ряда преобразований полученная из зависимости (1) интенсивность обнаружения ошибок имеет вид

$$\mu(t) = k/t^{1-k}\lambda^k. \tag{2}$$

Для передаваемой в эксплуатацию программы можно оценить среднее время наработки до отказа (MTTF), воспользовавшись тем, что на анализируемом участке $\mu(t)$ является медленно убывающей функций; с достаточной степенью точности её можно считать постоянной до момента обнаружения следующей ошибки: $\mu(t) = \mu(T_0)$, где T_0 – время начала эксплуатации, откуда $\text{MTTF} = 1/n(T_0)\mu(T_0)$.

Предложенный метод позволяет получить числовые оценки основных характеристик надежности программного обеспечения, таких как количество невыявленных ошибок, среднее время наработки на отказ, коэффициент готовности системы, вероятность опасного отказа за интересующий период времени и т. д., по информации, сохраняемой системой управления версиями; дополнительно продемонстрирован способ оценки количества времени, необходимого для поиска и исправления ошибок с целью достижения требуемых эксплуатационных характеристик.

Во втором параграфе представлена имитационная модель, разработанная для анализа сценариев отказа оборудования и программного обеспечения, которая учитывает влияние внешних факторов на надежность аппаратного и программного

обеспечения, использование которой позволяет получить числовые оценки таких параметров, как максимальное и среднее времена потери управления, количество и продолжительность сбоев различного типа, влияние диверсификации ПО на коэффициент готовности системы и т. д.

С целью оценки устойчивости имитационной модели к малым изменениям начальных параметров и определения времени перехода к стационарному состоянию в рамках теории массового обслуживания построена упрощенная математическая модель среднего уровня АСДУ (рис. 1) и рассмотрен процесс $M|M|1$ для системы из двух одинаковых серверов с постоянными интенсивностями отказов λ и ремонта μ, обслуживаемых одним ремонтником (рис. 5).

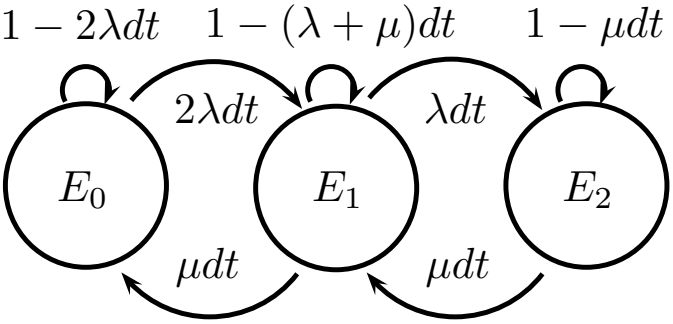

Рис. 5. Модель $M|M|1$: два сервера, один ремонтник

Из уравнений Колмогорова для состояния статистического равновесия получены следующие вероятности безотказной работы обоих серверов $\pi_0 = \lim_{t\to\infty} P_0(t)$; отказа одного сервера $\pi_1 = \lim_{t\to\infty} P_1(t)$; отказа обоих серверов $\pi_2 = \lim_{t\to\infty} P_2(t)$ в зависимости от коэффициента нагрузки $\rho = \lambda/\mu$:

$$\pi_0 = \frac{1}{1+2\rho+2\rho^2},\ \ \pi_1 = \frac{2\rho}{1+2\rho+2\rho^2},\ \ \pi_2 = \frac{2\rho^2}{1+2\rho+2\rho^2}. \qquad (3)$$

Испытания имитационной модели продемонстрировали соответствие результатов полученным аналитическим зависимостям и позволили оценить количество итераций, необходимое для получения желаемой степени точности (рис. 6), а также показали, что состояния статистического равновесия достигаются за времена, уменьшающиеся вместе с ρ и сравнимые со средним временем наработки до отказа одного сервера (рис. 7).

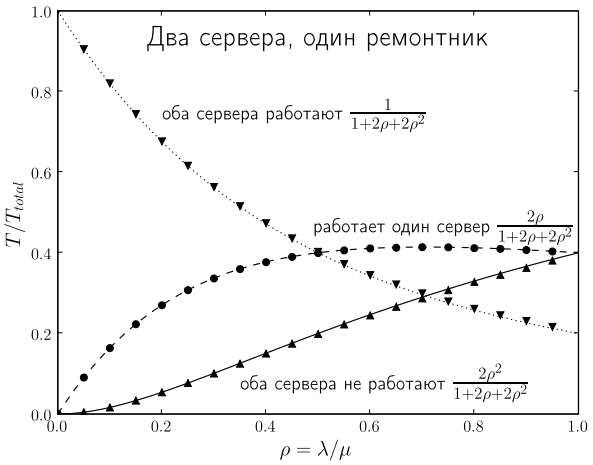

Рис. 6. Время работы серверов от ρ

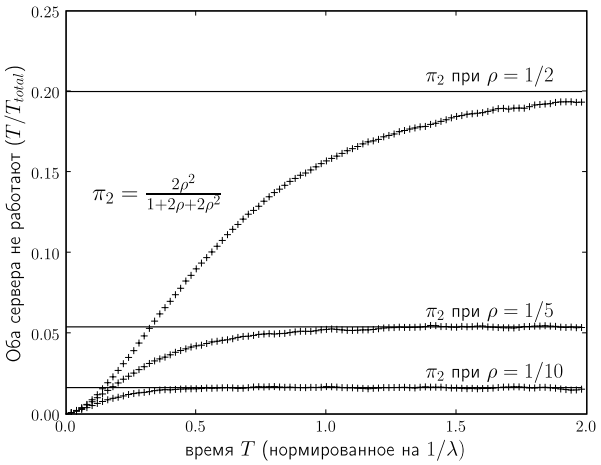

Рис. 7. Время потери управления от ρ

Для уточнения результатов моделирования в алгоритм внесён ряд изменений:

- общая интенсивность отказов λ разделена на две составляющие, соответствующие аппаратной части – $\lambda_{hardware}$ и программному обеспечению – $\lambda_{software}$; интенсивность отказов программного обеспечения $\lambda_{software}$ заменена полученной в предыдущем параграфе зависимостью $\mu(t)$ (2);
- введен алгоритм с интервальными ограничениями показательного распределе-

ния времени обслуживания: если продолжительность ремонта больше определенного времени T_{repair}, то ремонт производится в течение времени $T_{replace}$;
- снято требование о независимости отказов серверов ($P_{simultaneous} > 0$).

Если предположение о независимости отказов аппаратной части подтверждается практикой, то для ПО следует ожидать, что некоторое количество сбоев, вызванных непредусмотренными в программе состояниями входов системы, будет происходить на обоих серверах одновременно. Для учета этой ситуации введена вероятность одновременного выхода из строя программного обеспечения $P_{simultaneous}$. Для разработанной архитектуры АСДУ эта вероятность не равна 1, поскольку серверы работают независимо друг от друга, самостоятельно опрашивая контроллер в разное время, и на входах у них, в общем случае, разные значения.

Моделирование продемонстрировало важность учета $P_{simultaneous}$ при оценке надежности системы: на рис. 8 изображена полученная зависимость общего времени потери управления станцией (оба сервера вышли из строя по причине сбоя аппаратной части или ПО) от относительного среднего времени наработки до отказа программного обеспечения ($\text{MTTF}_{software}/\text{MTTF}_{hardware}$). Из графика видно, что среднее время потери управления станцией быстро растёт с увеличением вероятности одновременного выхода из строя ПО на обоих серверах.

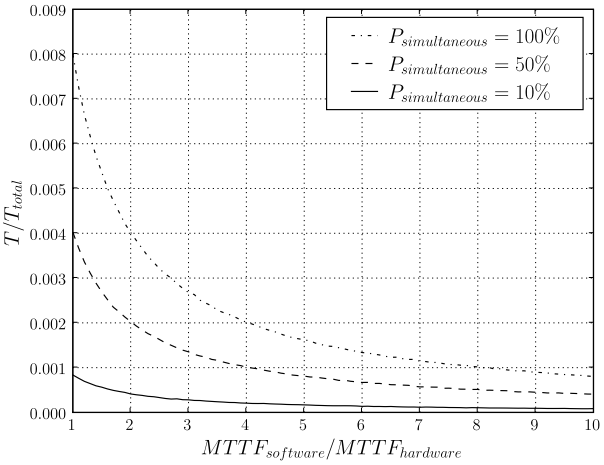

Рис. 8. Время потери управления при различных $P_{simultaneous}$

Моделирование также показало, что по сравнению с классической схемой (основной сервер и горячий резерв) предложенная архитектура с двумя независимыми узлами демонстрирует более высокий уровень готовности, поскольку система управляется одновременно по двум каналам, и отсутствует время переключения (зачастую существенное – до нескольких секунд) на резервный сервер в случае отказа основного.

Созданная имитационная модель позволила учесть зависимость надежности аппаратного и программного обеспечения от внешних факторов, проанализировать параметры предложенной архитектуры и получить числовые оценки, а также рассмотреть различные варианты улучшения характеристик системы.

В третьем параграфе представлен разработанный на основе теории нечетких множеств метод оценки характеристик надёжности, позволяющий наравне с известными статистическими распределениями учитывать предоставляемую экспертами неточную информацию различной степени достоверности.

Зачастую фактическая вероятность выхода оборудования из строя заметно отличается от вычисленной на основе заявленных в документации параметров надежности аппаратных комплектующих, таких как среднее время наработки до отказа за первый год, коэффициент изменения интенсивности отказов от времени и т. п. В первую очередь это объясняется разницей между реальными условиями эксплуатации и условиями тестирования на испытательном стенде.

При этом количество находящихся в эксплуатации одинаковых компонент не позволяет накопить достаточный статистический материал для самостоятельного

построения функции распределения вероятностей и определения необходимых характеристик надежности. В сложившейся ситуации наиболее целесообразным представляется использование экспертных оценок, которые позволяют учесть при анализе не только измеримые параметры системы, но и трудноформализуемые опыт, знания и интуицию специалистов.

Среди нескольких активно развиваемых сегодня направлений математики, предлагающих формализованный аппарат для работы с неопределённостями субъективной природы, наиболее целесообразным в рамках поставленной задачи представляется использование теории нечетких множеств, оперирующей так называемыми функциями принадлежности, которые позволяют эксперту не только численно оценить *точечное* значение требуемого параметра, но и выразить степень своей уверенности для всех возможных значений ($\mu(x) \in [0, 1]$).

В диссертационной работе предложен метод, позволяющий воспользоваться преимуществами как вероятностного подхода, так и экспертных оценок, который состоит в использовании предложенных экспертами нечётких параметров и корректирующих коэффициентов в расчетах, проводимых в соответствии с классической теорией вероятностей. Необходимый математический аппарат для обработки нечёткой информации наряду с точными данными получен на основе принципа обобщения Заде (пусть $f : X \to Y$ – отображение из X в Y, причем $y = f(x)$ – образ элемента x, и A – нечеткое множество в X. Тогда отображение f порождает нечеткое множество B в Y с функцией принадлежности, задаваемой соотношением $\mu_B(y) = \sup_{x \in f^{-1}(y)} \mu_A(x)$).

В качестве примера рассмотрена полученная в предыдущем параграфе зависимость (3) вероятности потери управления (выход из строя обоих серверов) $\pi_2(\lambda, \mu) = \frac{2(\lambda/\mu)^2}{1+2(\lambda/\mu)+2(\lambda/\mu)^2}$ от интенсивностей отказа λ и ремонта μ. Для неё получена функция принадлежности π_2: $\alpha_{\pi_2}(x) = sup_{x=\pi_2(x_1,x_2)} min(\alpha_\lambda(x_1), \alpha_\mu(x_2))$, которая по заданным характеристическим функциям α_λ и α_μ позволяет определить степень уверенности эксперта в том или ином значении вероятности выхода из строя всей системы. Функции принадлежности α_λ и α_μ получены по определяемым экспертом нечетким значениям среднего времени наработки до отказа MTTF одного сервера и среднего времени ремонта MTTR (рис. 9). Результат вычислений представляет собой нечёткую оценку вероятности одновременного отказа обоих серверов, для которой удобна следующая интерпретация: ядро нечеткого множества – оптимистическая оценка (вероятность менее $0.4 \cdot 10^{-7}$); носитель – пессимистическая (вероятность достигает $1.8 \cdot 10^{-7}$).

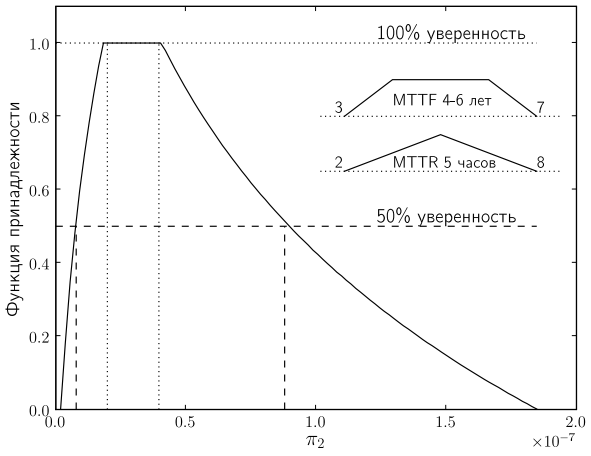

Рис. 9. Уверенность эксперта в различных значениях вероятности потери управления

Таким образом, разработанный на основе теории нечетких множеств метод формирует полный спектр возможных значений, а не только нижнюю и верхнюю границы, позволяя при этом использовать разнотипные статистические и экспертные данные; дополнительно метод предоставляет эксперту возможность отразить сте-

пень своей уверенности при оценке разброса параметров. Благодаря использованию нечетких множеств получаемый результат характеризуется низкой чувствительностью к малым изменениям входных параметров.

В пятой главе представлены общая архитектура автоматизированной системы управления движением поездов Новосибирского метрополитена, исторические предпосылки разработки, а также технические ограничения, наложенные на принятые архитектурные решения.

В рамках модернизации системы управления движением поездов Новосибирского метрополитена разработанные средства введены в постоянную эксплуатацию на станциях «Березовая роща» (с 2005 года), «Маршала Покрышкина», «Площадь Гарина—Михайловского», «Заельцовская» и «Красный проспект».

В заключении сформулированы основные результаты диссертации и выводы, в том числе:

1. На основе типовых элементов, выделенных из классических схем построения распределённых систем, разработана архитектура автоматизированной системы диспетчерского управления с повышенными требованиями к надежности и безопасности.
2. Продемонстрированы преимущества предложенной архитектуры АСДУ, в частности показано, что данная схема обеспечивает более высокий коэффициент готовности, чем классические системы с иерархией «основной-резервный», многоуровневый анализ безопасности действий оператора, возможность динамического изменения конфигурации и повышенную живучесть системы.
3. На основе разработанной концепции динамического программного интерфейса предложен метод построения модульной SCADA-системы, позволяющий создавать программные комплексы со сложными логическими зависимостями между частями, составляя динамическую конфигурацию из подгружаемых модулей.
4. На основе предложенного метода разработана открытая модульная многоплатформенная SCADA-система, поддерживающая распределенное резервирование и предназначенная для создания многоуровневых программных комплексов повышенной надежности и безопасности.
5. Предложен метод обработки данных на основе варианта трёхзначной логики, позволяющий наряду с точными данными оперировать неполной и недостоверной информацией, унифицируя и упрощая при этом запись логических выражений.
6. Предложен метод оценки основных характеристик надежности программного обеспечения по информации, сохраняемой системой управления версиями. Метод позволяет учесть особенности индивидуальной истории создания продукта, такие как практическая скорость внесения изменений в текст программы, интенсивность выявления ошибок, их тип и потребовавшееся на исправление время, полнота предоставленных спецификаций и частота появления новых требований в процессе разработки и тестирования.
7. С целью детального исследования сценариев отказа оборудования и программного обеспечения создана имитационная модель, позволяющая получить численные оценки максимального и среднего времён потери управления, количества и продолжительности сбоев различного типа, влияния диверсификации программного обеспечения на коэффициент готовности системы.
8. На основе теории нечетких множеств разработан способ оценки характеристик системы, в частности коэффициента готовности, учитывающий экспертные по-

правки к таким параметрам, как среднее время наработки на отказ и интенсивность ремонта.

9. Предложенные решения внедрены при построении автоматизированной системы диспетчерского управления движением поездов Новосибирского метрополитена; система функционирует на станциях «Березовая роща», «Маршала Покрышкина», «Площадь Гарина—Михайловского», «Заельцовская» и «Красный проспект».

В приложениях представлены дополнительные схемы и таблицы, а также акт о внедрении результатов диссертационной работы в практику производственной деятельности Новосибирского метрополитена.

Основные положения и результаты диссертации изложены в следующих публикациях

Статьи в рекомендованных ВАК журналах:

1. Нечеткое управление подачей воздуха в топку парового котла / Е.П. Бакулин, В.Д. Бобко, Ю.Н. Золотухин, М.А. Золотухина, А.А. Нестеров, В.Я. Пивкин, М.Н. Филиппов, А.П. Ян // *Автометрия*. — 2002. — Т. 6. — С. 36–44.
2. *Белоконь С.А., Филиппов М.Н.* Метод построения многоплатформенной открытой модульной SCADA-системы // *Вестник НГУ. Серия: Физика*. — 2008. — Т. 3, выпуск 1. — С. 115–125.
3. *Филиппов М.Н.* Метод обработки неполных данных на основе трёхзначной логики // *Автометрия*. — 2009. — Т. 45, № 5. — С. 124–131.

Материалы научных мероприятий:

4. *Филиппов М.Н.* Метод контроля сходимости выводов нечеткой экспертной системы // *В кн. Труды VI Международного семинара «Распределенная обработка информации», 23–25 июня 1998 г., Новосибирск*. — 1998. — С. 343–347.
5. Fuzzy technology based combustion process optimization / E.P. Bakulin, V.D. Bobko, A.A. Nesterov, V.Ya. Pivkin, M.N. Filippov, A.P. Yan, Yu.N. Zolotukhin, M.A. Zolotukhina // *In: Proc. of the IASTED International Conference "Automation, Control, and Information Technology (ACIT 2002)", June 10–13, 2002, Novosibirsk*. — 2002. — Pp. 167–169.
6. Automated System of Supervisor Subway Traffic Control / A.I. Abramov, S.A. Belokon', R.R. Kogler, S.F. Markov, Yu.I. Micheev, V.M. Plotnikov, M.A. Sobolev, M.N. Filippov, V.V. Vasil'ev, A.P. Yan, Yu.N. Zolotukhin // *In: Proc. of the Second IASTED International Multi-Conference "Automation, Control, and Applications (ACIT-ACA 2005)", June 20–24, 2005, Novosibirsk*. — 2005. — Pp. 198–200.
7. Автоматизированная система диспетчерского управления движением поездов на Дзержинской линии Новосибирского метрополитена / А.И. Абрамов, С.А. Белоконь, В.В. Васильев, Ю.Н. Золотухин, Р.Р. Коглер, С.Ф. Марков, Ю.И. Михеев, В.М. Плотников, М.А. Соболев, М.Н. Филиппов, А.П. Ян // *В кн. Труды VII Международной конференции «Проблемы управления и моделирования в сложных системах», 27 июня–1 июля 2005 г., Самара*. — 2005. — С. 157–161.
8. Модернизация системы диспетчерского управления движением поездов метрополитена / А.И. Абрамов, С.А. Белоконь, В.В. Васильев, Ю.Н. Золотухин, Р.Р. Коглер, С.Ф. Марков, Ю.И. Михеев, В.М. Плотников, М.А. Соболев, М.Н. Филиппов, А.П. Ян // *В кн. Труды VIII Международной конференции «Проблемы управления и моделирования в сложных системах», 24 июня–28 июня 2006 г., Самара*. — 2006. — С. 269–273.

9. *Белоконь С.А., Филиппов М.Н.* Разработка и реализация открытой SCADA-системы // *В кн. Информационно-коммуникационные системы. Сборник тезисов докладов Международной школы-конференции молодых ученых «Информационно-коммуникационные системы», 17–24 сентября 2006 г., Новосибирск* — 2006. — С. 21–24.
10. *Белоконь С.А., Филиппов М.Н.* Открытая SCADA-система: разработка и реализация прототипа // *В кн. Материалы научно-практической конференции молодых ученых и студентов НГУ и ИАиЭ СО РАН «Информационно-вычислительные системы анализа и синтеза изображений», 19–21 сентября 2006 г., Новосибирск*. — 2006. — С. 45–48.
11. Моделирующий комплекс для разработки супервизорных систем управления движением поездов в метро / А.И. Абрамов, С.А. Белоконь, В.В. Васильев, М.А. Соболев, М.Н. Филиппов // *В кн. Материалы научно-практической конференции молодых ученых и студентов НГУ и ИАиЭ СО РАН «Информационно-вычислительные системы анализа и синтеза изображений», 19–21 сентября 2006 г., Новосибирск* — 2006. — С. 22–25.
12. *Белоконь С.А., Филиппов М.Н.* Открытая модульная SCADA-система: метод построения и особенности реализации // *В кн. Труды IX Международной конференции «Проблемы управления и моделирования в сложных системах», 22–28 июня 2007 г., Самара*. — 2007. — С. 225–233.
13. *Белоконь С.А., Филиппов М.Н.* Открытая модульная многоплатформенная SCADA-система: разработка и реализация // *В кн. Материалы конференции IV Всероссийская школа-семинар молодых ученых «Проблемы управления и информационные технологии», 23–28 июня 2008 г., Казань*. — 2008. — С. 20–23.
14. *Белоконь С.А., Филиппов М.Н.* Эффективный метод реализации открытой модульной SCADA-системы // *В кн. Труды X Международной конференции «Проблемы управления и моделирования в сложных системах», 23–25 июня 2008 г., Самара*. — 2008. — С. 259–262.
15. Автоматизированная система диспетчерского управления движением поездов в Новосибирском метрополитене / С.А. Белоконь, В.В. Васильев, Ю.Н. Золотухин, М.А. Соболев, М.Н. Филиппов, А.П. Ян // *В кн. Материалы конференции IV Всероссийская школа-семинар молодых учёных «Проблемы управления и информационные технологии», 23–28 июня 2008 г., Казань*. — 2008. — С. 28–31.
16. *Белоконь С.А., Васильев В.В., Филиппов М.Н.* Программное обеспечение автоматизированной системы диспетчерского управления Новосибирского метрополитена // *В кн. Материалы VII международной конференции памяти академика А. П. Ершова «Перспективы систем информатики», 15–19 июня 2009 г., Новосибирск*. — 2009. — С. 52–56.
17. *Белоконь С.А., Филиппов М.Н.* Архитектура высоконадёжной открытой системы автоматизированного диспетчерского управления: SCADA-система // *В кн. Материалы VII международной конференции памяти академика А. П. Ершова «Перспективы систем информатики», 15–19 июня 2009 г., Новосибирск*. — 2009. — С. 57–61.

Филиппов Михаил Николаевич

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛЕЙ И МЕТОДОВ ПОСТРОЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ДИСПЕТЧЕРСКОГО УПРАВЛЕНИЯ

Автореферат диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать «2» ноября 2009 г.

Формат бумаги 60x84 1/16, Объем 1 печ. л.
Бумага офсетная. Тираж 100 экз. Заказ № 97

Типография Института катализа им. Г. К. Борескова СО РАН
630090, г. Новосибирск, проспект Академика Лаврентьева, 5.