На правах рукописи

Выговский Леонид Сергеевич

МЕТОД, МЕТОДИКА И СПОСОБЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ ИНТЕГРИРОВАННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Специальность: 05.13.15 — Вычислительные машины, комплексы и компьютерные сети

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург — 2011

Работа выполнена в Санкт-Петербургском государственном электротехническом университете «ЛЭТИ» им. В. И. Ульянова (Ленина).

Научный руководитель:	доктор технических наук, доцент Максимов Роман Викторович
Официальные оппоненты:	доктор технических наук, профессор Водяхо Александр Иванович
	кандидат технических наук, доцент Шкиртиль Вячеслав Иванович
Ведущая организация:	ЗАО «Интелтех»

Защита состоится «____» «_____» 2011 г. в ____ часов на заседании совета по защите докторских и кандидатских диссертаций ДС 212.238.01 Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина) по адресу: 197376, Санкт-Петербург, ул. Проф. Попова, д. 5.

С диссертацией можно ознакомиться в библиотеке университета.

Автореферат разослан «____» «_____» 2011 г.

Ученый секретарь
совета по защите докторских
и кандидатских диссертаций Щеголева Н.Л.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В настоящее время для эффективного управления и сокращения цикла принятия решений должностных лиц используются сложные информационные системы. Для создания информационных систем необходимо строить сложные компьютерные сети (КС) как государственного уровня, так и уровня предприятий. При этом сегменты КС могут находиться в разных регионах страны на значительном удалении друг от друга. Создание отдельной телекоммуникационной сети для каждой КС не представляется возможным как по экономическим, так и по техническим причинам. Таким образом, необходима интеграция с информационными системами общего пользования Единой Сети Электросвязи Российской Федерации (ЕСЭ РФ) и можно говорить о том, что подавляющее большинство современных КС является интегрированными с сетью Интернет. Это приводит к серьезному повышению риска выхода элементов системы из строя в результате воздействия преднамеренных и непреднамеренных помех (ПНП). Вледствии отказа множества элементов системы может сложиться ситуация, что система разрушится и информационный обмен прекратится.

Основными направлениями обеспечения надежности передачи информации являются: резервирование путем наращивания дополнительных ресурсов в системе передачи данных, различные способы маршрутизации, сравнительный анализ оценки надежности структур на этапе проектирования. Наращивание дополнительных ресурсов с целью резервирования канала на случай повышения количества передаваемых сообщений является дорогим решением. Маршрутизация позволяет распределять трафик по разным каналам и узлам, компенсируя его рост. Повышение трафика возможно как в результате предоставления новых информационных услуг (например, передача телевидения высокого качества), так и в силу других причин.

Существующие методы обеспечения надежности слабо адаптированы к объектам, включающим неподконтрольные владельцу (оценщику) элементы, которые представляют собой современные интегрированные компьютерные сети. Отмеченное выше позволяет выделить сложившееся противоречие между возрастающими требованиями к обеспечению надежности компьютерных сетей в условиях интеграции с ЕСЭ РФ и существующим недостаточным уровнем разработки научно-методического обеспечения и практических рекомендаций, соответствующих современным условиям надежного функционирования ИКС.

Данное противоречие позволяет констатировать **научную задачу**, заключающуюся в разработке на основе анализа функционирования ИКС, включающих в себя элементы, не контролируемые владельцем ИКС, разработать

метод оценки надежности ИКС, методику сравнительной оценки структур ИКС, получаемых в результате различных вариантов подключения к сети Интернет, и способы повышения надежности функционирования ИКС.

Выявленное противоречие и существующая научная задача обусловили выбор темы данного исследования: «Метод, методика и способы обеспечения надежности интегрированных компьютерных сетей» и ее актуальность.

Цель исследования — обеспечение надежности интегрированных компьютерных сетей.

Объект исследования — интегрированные компьютерные сети.

Предмет исследования — методы, методики и способы обеспечения надежности интегрированных компьютерных систем.

Методы исследования. Основу исследований составили научные положения о всеобщей связи, взаимной обусловленности и целостности явлений и процессов окружающего мира, общенаучные методологические подходы.

В ходе исследования были использованы следующие методы: теоретические (теория перколяции, теория графов, теория алгоритмов, теория моделирования, теория управления) и эмпирические (обобщение передового опыта в области обеспечения надежности ИКС, количественный и качественный анализ эмпирических данных, полученных в ходе исследования, опытно-экспериментальная работа по проверке исходных положений и полученных теоретических результатов).

Теоретическую основу составили работы отечественных (Рябинин И.А., Советов Б.Я., Тарасевич Ю.Ю., Ушаков И.А., Яковлев С.А.) и зарубежных (Райншке К., Мандельброт Б., Федер Е., Гриммет Г., Уилкинсон Д., Хаммерсли Дж., Кнут Д.Э., Гослинг Д., Гамма Э., Лисков Б.) ученых.

Научная новизна работы.

1. Разработан метод оценки надежности ИКС, представляющий передачу информации между абонентами ИКС как протекание одного вещества через другое, что позволяет учитывать наличие не управляемых владельцем ИКС элементов.

2. На основе предложенного метода оценки надежности разработана методика сравнительной оценки надежности ИКС, получаемых в результате подключения локальных сегментов ИКС к ССОП с помощью различных провайдеров телекоммуникационных услуг.

3. Разработан способ обеспечения надежности ИКС во время эксплуатации путем выбора альтернативного, более надежного маршрута. При этом при оценке маршрута учитывается воздействие ПНП и перспективное снижение надежности.

4. Разработан способ обеспечения надежности ИКС во время предна-

меренного деструктивного воздействия путем введения злоумышленника в заблуждение относительно структуры ИКС.

Научно-практическая значимость исследования заключается в возможности использования его результатов при проектировании и эксплуатации ИКС в следующих аспектах:

1. Разработанный метод оценки надежности интегрированных компьютерных сетей, позволяет получить оценки надежности ИКС, включающих элементы ССОП (Интернет).

2. Предложенная методика сравнительной оценки интегрированных компьютерных сетей, функционирующих в условиях воздействия ПНП, позволяет обоснованно выбрать альтернативные структуры ИКС, получаемые в результате выбора того или иного варианта подключения локальных сегментов ИКС к ССОП (Интернет).

3. В ходе исследования были разработаны способы обеспечения надежности интегрированных компьютерных сетей в процессе эксплуатации, а также специальное программное обеспечение для практического применения метода и методики обеспечения надежности ИКС.

Реализация. Результаты научного исследования внедрены в научно-иследовательских работах: ФГУП «НИИ «Масштаб»; Военная академия связи им. С.М. Буденова («Инспектор», «Связка», «Отвага 2010»), СПбГЭТУ “ЛЭТИ” им. В.И. Ульянова (Ленина) в рамках аналитической ведомственной целевой программы «Развитие научного потенциала высшей школы (2009-2010 годы)», о чем имеются соответствующие акты внедрения.

Достоверность полученных научных результатов обеспечена применением современной научной методологии, использованием современных математических методов, апробированных на практике, и результатами экспериментальных исследований. Новизна, практическая реализуемость и изобретательский уровень предложенных технических решений подтверждены положительными заключениями экспертизы на выдачу патентов РФ.

Апробация результатов работы. Основные научные результаты исследования апробированы путем проведения их многоступенчатой экспертизы на научно-технических и научно-практических конференциях: Всеармейской НПК “Инновационная деятельность в ВС РФ”, ВАС, СПб. (2007, 2008); научно-технической конференции СПбНОТОРЭС им. А.С. Попова посвященной дню радио, СПб, (2008, 2010); научно-технических семинарах кафедры АСОИУ СПбГЭТУ “ЛЭТИ” (2008-2010).

Публикации. Научные результаты диссертации достаточно полно изложены и опубликованы в 8 печатных научных трудах, из которых 2 статьи в изданиях, рекомендованных в действующем перечне ВАК, 2 патента РФ, 3

доклада на всероссийских научно-технических конференциях, 1 публикация в бюллетене изобретений.

Структура и объем диссертационной работы. Диссертация состоит из введения, четырех глав с выводами, заключения и списка литературы, включающего 103 наименования. Основная часть работы изложена на 163 страницах машинописного текста. Работа содержит 49 рисунков, 4 таблицы.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, определены цель, объект, предмет и задачи исследования; обозначены теоретико-методологические основы исследования научной задачи; показана его научная новизна, теоретическая и практическая значимость, а также сформулированы положения, выносимые на защиту.

В первой главе «Анализ задачи обеспечения надежности интегрированных компьютерных сетей» вводятся основные понятия и определения, анализируются возможные подходы к обеспечению надежности компьютерных сетей, интегрированных с сетью Интернет или ЕСЭ РФ. Показано, что рост потребностей общества в информационном обмене приводит к созданию крупных информационный систем, обмен данными в которых обеспечивается компьютерными сетями. В соответствии с предъявляемыми к информационным системам требованиями компьютерные сети должны быть территориально распределенными. Не существует возможности (в первую очередь по экономическим причинам) создания выделенной телекоммуникационной инфраструктуры для каждой информационной системы, что необходимо для прогнозируемого надежного функционирования компьютерной сети. Это приводит к необходимости использовать при построении компьютерной сети промежуточное оборудование провайдеров, интегрируя тем самым компьютерную сеть во всемирную сеть Интернет.

Рассмотрены способы решения задачи обеспечения надежности, которая решается как во время проектирования компьютерной сети, так и во время эксплуатации. Во время проектирования надежность обеспечивается путем сравнительной оценки альтернативных вариантов структур КС и резервирования. Стандартные методы оценки надежности включают в себя следующие этапы: сбор данных об элементе, статистическую обработку полученных данных, построение на основе обработки модели объекта, оценку надежности на основе построенной модели. Сбор данных в интегрированных компьютерных сетях существенно затруднен по следующим причинам: значительная часть ИКС не принадлежит владельцам проектируемой компьютерной сети, элементы сети постоянно меняют свои характеристики вследствие

обновления программного обеспечения, отсутствует перспективный учет повышения нагрузки. Статистическая обработка данных существенно затруднена в силу того, что компьютерное оборудование является высоконадежным оборудованием в штатных режимах работы и накапливается мало данных об отказах. Модель объекта быстро теряет актуальность, так как неконтролируемая часть ИКС постоянно меняется в силу добавления новых узлов, изменения настроек оборудования и программного обеспечения, изменения внешней среды функционирования. Таким образом, можно сделать вывод о недостаточной пригодности существующих методов оценки надежности в предметной области ИКС. Поставщики телекоммуникационных услуг, работающих в пространстве ЕСЭ РФ, являются коммерческими организациями, старающимися найти оптимальный баланс качество/стоимость. Как правило, они обеспечиваются резервированием не более 30% от штатной нагрузки на каналы. Этот метод хорошо работает в обычных условиях, в то же время при внештатной нагрузке сеть не справляется, что приводит к невозможности (или существенному ухудшению качества) передачи информационных потоков между абонентами.

Наиболее применяемым методом обеспечения надежности является маршрутизация информационных потоков во время эксплуатации компьютерной сети. Разработаны различные алгоритмы, которые действуют как для выбора маршрутов внутри сегментов, так и вне их. К общим недостаткам алгоритмов маршрутизации можно отнести следующее. Необходимость синхронизировать представление о сети между маршрутизаторами, что занимает время и создает служебный трафик. Расчет маршрутов осуществляется с помощью алгоритма поиска кратчайших путей Дейкстры, вычислительная сложность которого существенно увеличивается с ростом элементов сети, поэтому каждый маршрутизатор хранит в памяти относительно небольшой размер сети, что снижает качество принимаемых решений о направлении маршрутов. Алгоритмы маршрутизации накладывают единственное ограничение на используемые метрики расчета кратчайшего пути - их аддитивность, в то же время, как правило, используется только одна метрика, самая простейшая - количество узлов в маршруте.

Как показывает проведенный в диссертационном исследовании анализ, в настоящее время отсутствуют методы обеспечения надежности, подходящие для предметной области интегрированных компьютерных сетей. Для решения этой проблемы предлагается использовать модель просачивания (перколяции) для описания процесса передачи трафика между территориально распределенными сегментами ИКС. Просачивание одного вещества через другое изучается теорией перколяции. Раскрываются основные положения теории

перколяции и делается вывод о необходимости ее адаптации к предметной области ИКС. Делается вывод о необходимости на основе адаптированной теории перколяции разработать методическое обеспечение надежности ИКС, включающее в себя метод оценки надежности, методику сравнительной оценки надежности ИКС, способы обеспечения надежности ИКС.

Во второй главе «Метод оценки надежности интегрированных компьютерных сетей» теории перколяции адаптируется в предметную области ИКС и на ее основе сформулированы критерии оценки надежности.

Вводится понятие границ ИКС и критерий перколяционного кластера. Под перколяционным кластером понимается кластер, состоящий из работоспособных, связанных линиям связи элементов, который включает в себя хотя бы по одному граничному узлу из каждой территориально обособленной ЛВС ИКС. Пограничные узлы $K = \{k_i\}$ – это элементы ЛВС ИКС, с помощью которых ЛВС ИКС интегрируются с сетью Интернет. Вся совокупность узлов на одной ЛВС образует границы, из которых определяется множество границ B:

$$B = \{b_j\}, b_j \subset k_i, |b_j| > 0, \quad |B| \geq 2 \tag{1}$$

где b — граница, k — ключевой узел. Один ключевой узел принадлежит строго одной границе $\cap_j b_j = \emptyset$. При этом кластер C считается перколяционным в том и только в том случае, если он содержит хотя бы по одному узлу из каждой границы:

$$C \bigcap_j b_j \neq \emptyset. \tag{2}$$

Описывается способ моделирования передачи информации как протекание вещества (информационных потоков) через материал (сеть). Считается, что трафик может «протечь» в узел, если он является работоспособным. В том случае, если узел вышел из строя в результате воздействия преднамеренных и непреднамеренных помех, передача через него информационных пакетов невозможна. Задают исходные данные. Структура ИКС представляется в виде графа, узлами которого являются узлы ИКС, а ребрами – связи между ними. Узлы локальных сегментов, через которые осуществляется подключение к сети Интернет, определяют множество границ. Задается вероятность устойчивости узлов $p_{\text{уст}}$ к воздействию помехи, общая для всех узлов сети, и количество экспериментов. Обобщенная схема метода показана на рис. 1.

Каждому узлу сети, независимо от других, устанавливается $p_{\text{воз}}$, которая определяется по равномерному закону распределения. Узлы, у которых $p_{\text{уст}} > p_{\text{воз}}$, запоминают во множестве исправных узлов, способных передать информационный трафик. С помощью системы непересекающихся множеств получают множество кластеров, состоящих из связанных между собой ис-

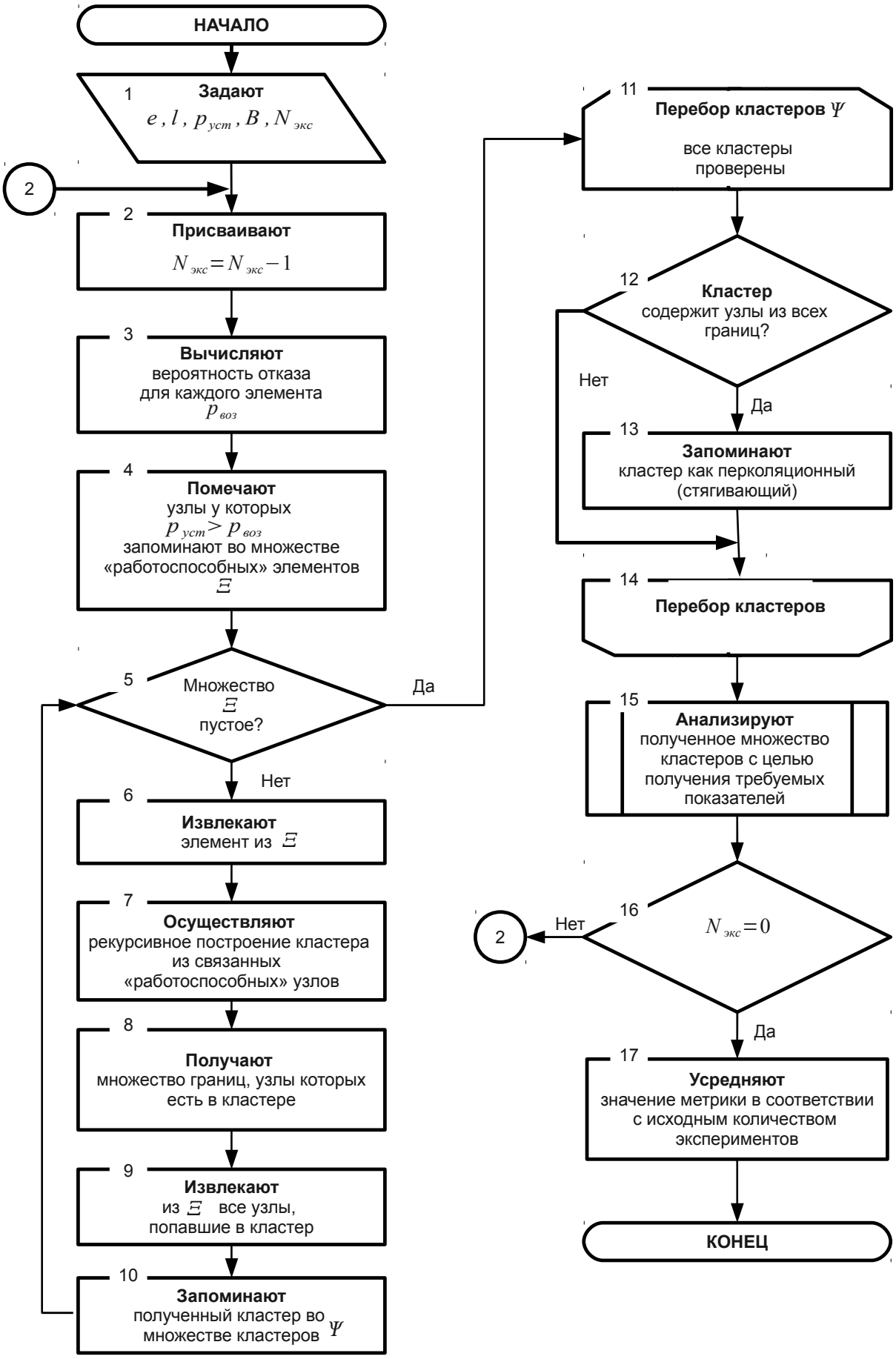
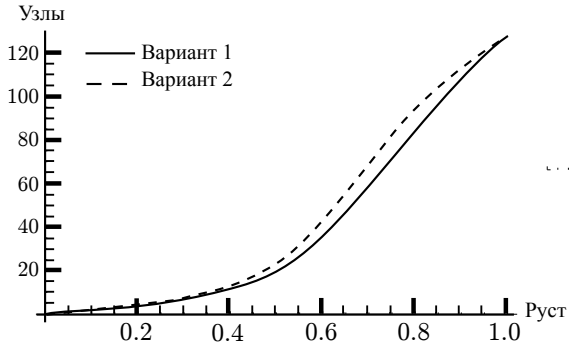


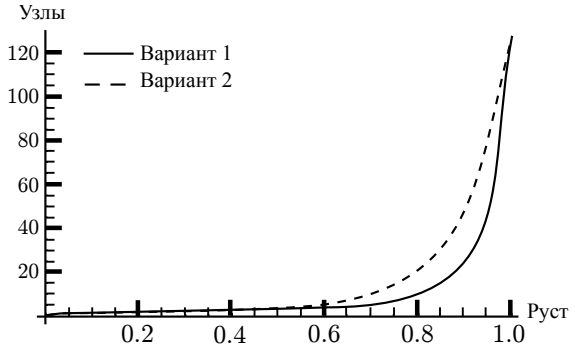
Рис. 1. Блок-схема обобщенного алгоритма, определяющая последовательность действия для реализации методики

правных узлов.

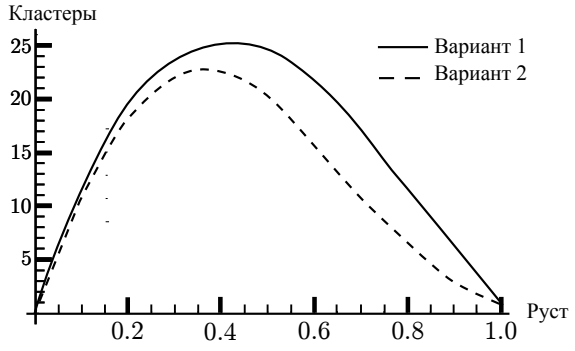
По указанному ранее критерию выделяют множество перколяционных кластеров и осуществляется расчет необходимых метрик.



(a) Максимальный размер



(b) Средний размер кластеров



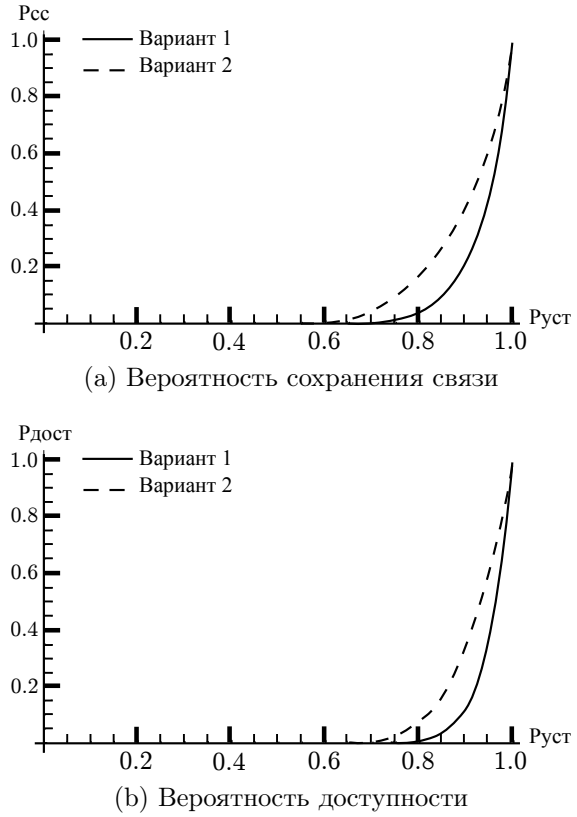
(c) Количество кластеров

Рис. 2. Количественные метрики надежности ИКС

Вводятся количественные оценки работоспособного кластера. В результате воздействия преднамеренных и непреднамеренных помех элементы сети могут выходить из строя. Это означает, что «протекание» через них информации невозможно. Работоспособные кластеры образуют новую структуру (или структуры), которую можно оценить по следующим параметрам: максимальный размер образовавшегося кластера (рис. 2, a), средний размер образовавшихся кластеров (рис. 2, b), количество образовавшихся кластеров (рис. 2, c).

Вводятся вероятностные оценки сохранения связи работоспособных узлов. Рассматривается вероятность сохранения связи между территориально распределенными сегментами ИКС и вероятность доступности произвольного узла. В результате воздействия помехи образовавшийся работоспособный кластер может включать в себя хотя бы по одному узлу из каждой границы. В этом случае можно говорить о том, что информационное взаимодействие между сегментами ИКС возможно. В ином случае ИКС не может выполнять свое функциональное назначение. Вероятность сохранения связи (рис. 3, a) рассчитывается как отношение количества образовавшихся перколяционных кластеров к количеству проведенных экспериментов. Вероятность одновременного образования двух перколяционных кластеров на одной решетке пренебрежительно мала. Вероятность доступности (рис 3, b) произвольного выбранного ресурса из ИКС определяется как соотношение размера образовавшегося перколяционного кластера к количеству узлов в решетке.

Вводится оценка надежности интегрированной компьютерной сети в условиях распространения помехи. С помощью перколяции строится кластер из узлов, через которые могут распространяться информационные потоки в определенный момент времени. Каждому элементу, вошедшему в перколяционный кластер, сопоставляется комплексный показатель устойчивости к ПНП. За один шаг моделирования помеха «просачивается» из зараженных точек в связанные с ними незараженные. При этом правило заражения может меняться в зависимости от типа моделируемой помехи. В процессе моделирования выполняют расчет размера кластера из подверженных помехе узлов и расчет движения поверхности, разделяющей сферы влияния работающих и поврежденных сторон по мере того, как логическая помеха распространяет свое влияние на узлы и каналы ИКС.



(a) Вероятность сохранения связи

(b) Вероятность доступности

Рис. 3. Вероятностные метрики надежности ИКС

В третьем разделе «Методика сравнительной оценки интегрированных компьютерных сетей» описывается методика сравнительной оценки различных структур ИКС, которые получаются при выборе альтернативных вариантов подключения локальных сегментов к ССОП (Интернету).

Целью методики является повышение надежности ИКС путем сравнительной оценки различных структур ИКС, получаемых в результате выбора того или иного оператора связи. Исходными данными методики являются множество пограничных узлов и альтернативные варианты подключения к сети Интернет. Основным показателем является вероятность сохранения связи между территориально разнесенными сегментами ИКС, через которые осуществляется взаимодействие региональных локально-вычислительных сетей, входящих в ИКС. Ограничения методики заключаются в следующем. Система считается квазиоднородной (вероятность устойчивости к воздействию ПНП у всех узлов одинакова) и невосстанавливаемой.

Методика включает в себя три последовательно выполняемые процедуры: вскрытие структуры ИКС для различных вариантов подключения к сети Интернет; анализ полученных вариантов ИКС с целью определения их устой-

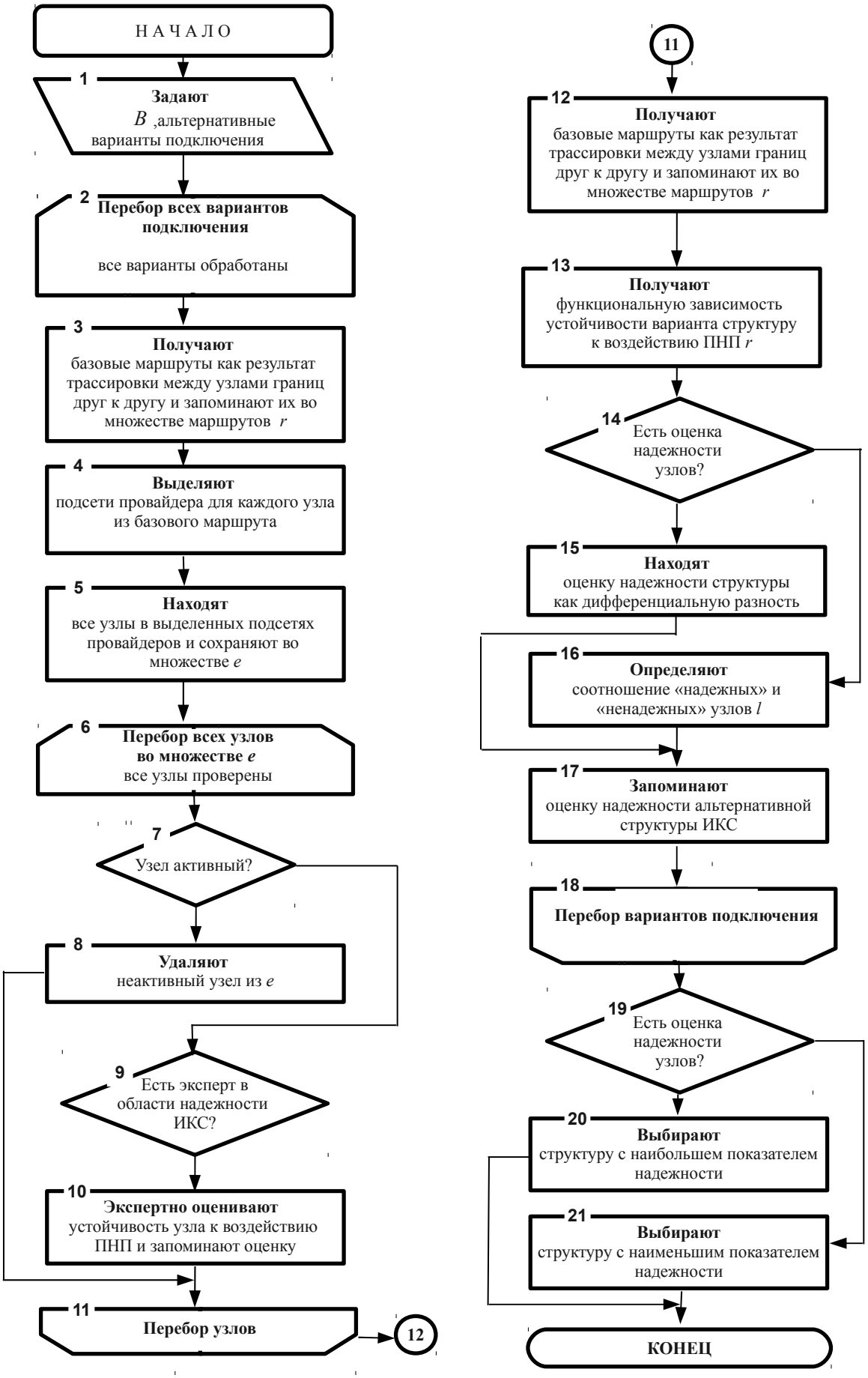


Рис. 4. Блок-схема обобщенного алгоритма, определяющая последовательность действия для реализации методики

чивости к ПНП; сравнительный анализ полученных метрик. Схема методики представлена на рис. 4.

Структуру ИКС выявляют путем анализа специализированного ПО, раскрывающего маршруты с узла пользователя до какого-либо другого узла ССОП. Осуществляется поиск базовых маршрутов, через которые передается трафик в обычном режиме эксплуатации ИКС. Для кажого узла, входящего в базовый маршрут, определяют провайдера и подсеть. Осуществляется поиск маршрутов до всех узлов провайдера. При наличии эксперта в области компьютерной безопасности и надежности сетей возможно осуществить вскрытие использующегося на узле программного обеспечения, а также топологическую схему ССОП. На основе этих данных может быть дана экспертная оценка надежности узлов, входящих в граф альтернативных вариантов подключения.

Процедура анализа включает в себя оценки вариантов структур с помощью предложенного во второй главе метода. Для этого осуществляют моделирование воздействия помехи на каждый альтернативный вариант ИКС. Задают устойчивость к помехе (одно значение для всех элементов сети). Для каждого узла, независимо от других, моделируется воздействие помехи путем генерации случайного числа по равномерному закону распределения. Полученное значение помехи сравнивается с заранее заданной устойчивостью узлов. В случае, если значение воздействия помехи превышает устойчивость узла, узел считается вышедшим из строя. Связанные работоспособные узлу образуют кластеры, в которых возможна передача информации между элементами. В случае, если образовался кластер включающий в себя хотя бы по одному узлы из каждой границы, можно говорить о том, что ИКС оказалась устойчивой к воздействию ПНП.

Для получения функциональной зависимости и учета перспективного снижения устойчивости узлов (повышение деструктивного воздействия) $p_{\text{уст}}$ изменяется в диапазоне от 0 (все узлы выходят из строя) до 1 (все узлы абсолютно надежны). На рис. 5 в графическом виде показаны функциональные зависимости для двух вариантов подключения к ССОП. В случае, если экспертная оценка надежности узлов не проводилась, вычисляют показатель надежности π для каждого ва-

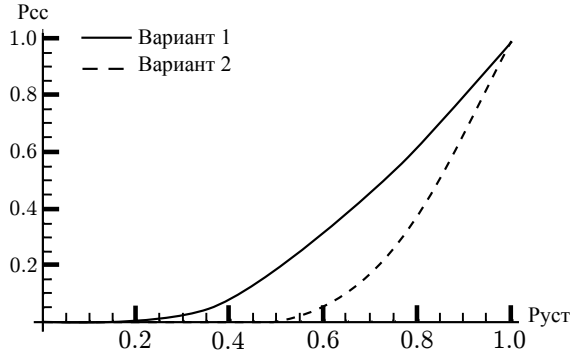


Рис. 5. Функциональные зависимости сохранения связи двух вариантов подключения к ССОП

рианта структуры как дифференциальную разность между $p_{\text{сс}}(p_{\text{уст}}) = 1$ и полученной функциональной зависимостью. Наиболее надежным считается вариант, которому соответствует минимальное значение π.

В случае, если каждому узлу сопоставлена экспертная оценка надежности, устанавливают минимально допустимую надежность узлов. После этого рассчитывают отношение «надежных» (экспертная оценка больше минимально допустимой) к общему числу сети, находя тем самым вероятность устойчивости узла в сети к воздействию ПНП. Далее полученное значение подставляется в функциональную зависимость, получая тем самым метрику оценки надежности ИКС. Альтернативные варианты ИКС ранжируются по этой метрике и выбирается вариант с наибольшим значением.

В четвертой главе «Способы повышения надежности интегрированных компьютерных сетей» разработаны научно-технические способы обеспечения надежности ИКС во время эксплуатации.

В первом предложенном способе обеспечение надежности достигается за счет выбора наиболее надежного маршрута передачи сообщения из альтернативных. Предложенный способ позволяет учитывать устойчивость узлов к ПНП. Для этого в разработанном способе предварительно задают параметры ИКС и формируют ее схему. В качестве параметров задают идентификаторы узлов сети, наличие связи между ними, параметры надежности. Вычисляют комплексный показатель надежности для каждого узла как нормированное численное значение свертки параметров надежности, характеризующий устойчивость элемента к ПНП. Расчет может быть осуществлен суммированием, перемножением, или средним арифметическим, или какой-либо другой функцией от значения параметров надежности ОИ. Дополнительно задается минимально допустимое значение показателя надежности.

Из сформированной схемы ИКС выделяют альтернативные маршруты передачи информационного потока между абонентами, узлы которых определяются идентификаторами. Найденные альтернативные варианты маршрута передачи трафика сохраняют в памяти. Далее сравнивают значение ранее вычисленного комплексного показателя устойчивости каждого узла с предварительно заданным минимально допустимым значением. Если показатель узла меньше допустимого уровня, узел запоминается как «ненадежный», иначе – как надежный. В зависимости от соотношения надежных узлов к ненадежным связь между абонентами может отсутствовать, при этом критическое соотношение для разных структур различно. Учет перспективного снижения надежности узлов достигается последовательным уменьшением соотношения «надежных» и «ненадежных узлов» до того момента, как образующийся кластер «надежных» узлов перестанет включать в себя абонентов. После на-

хождения критического соотношения включения абонентов в кластер, альтернативные варианты ранжируют по нему и выбирают вариант с меньшем значением, который является более надежным.

Таким образом достигается повышение достоверности результатов сравнительной оценки структур ИКС при увеличении количества элементов и в условиях воздействия преднамеренной и непреднамеренной помехи.

Разработан способ повышения надежности интегрированных компьютерных сетей в условиях воздействия преднамеренной помехи. В частном случае разработанный метод оценки надежности сетей позволяет повышать надежность ИКС, позволяет обеспечивать надежность в случае воздействия преднамеренных помех. Для повышения эффективности воздействия преднамеренных помех злоумышленник должен знать структуру сети. Вскрытие сети можно осуществить с помощью процедуры вскрытия сети, описанной в методике сравнительной оценки ИКС. Построенная таким образом схема позволяет выявить узлы, целенаправленное и успешное деструктивное воздействие на которые воспрепятствует передаче информационного трафика между абонентами.

Для снижения эффективности воздействия преднамеренной помехи злоумышленника вводят в заблуждение относительно истинной структуры ИКС путем создания виртуальных (несуществующих физически) сегментов ИКС. При этом синтезировать структуру виртуальных сегментов предлагается исходя из метода оценки надежности ИКС, описанного в диссертационном исследовании. Для этого получают истинные оценки надежности для всех альтернативных маршрутов передачи информационного трафика и находят их усредненное значение. После этого в ИКС добавляют виртуальные узлы, образующие новые сегменты, изменяющие характеристики маршрутов. Для определения конфигураций добавляемых виртуальных сегментов могут быть использованы генетические алгоритмы, принимающие в качестве целевой функции усредненный показатель и структуру ИКС в качестве начальной популяции. При этом определяется достаточно широкий диапазон показателя, при вхождении в который генетический алгоритм прекращает работу. Это вносит элемент случайности в показатели, тем самым снижая демаскирующий признак однородности виртуальных сетей. Помимо повышения сложности решения задачи выбора объекта воздействия преднамеренной помехи путем усреднения показателей, можно создать виртуальные сегменты с крайними показателями устойчивости к воздействиям преднамеренных помех.

После определения требуемой топологии моделируемых объектов информатизации осуществляется их виртуализация на специально выделяемых узлах ИКС. Предлагается три варианта реализации способа. В первом спо-

собе предварительно задают опорные идентификаторы санкционированных соединений, содержащие сокеты отправителя и получателя потоков. Задают базу из ложных адресов абонентов. Кроме того, задаются эталоны идентификаторов типа протокола взаимодействия и время задержки отправки пакетов. Из канала связи принимают пакет сообщений от отправителя и выделяют из заголовка идентификационные признаки, в качестве которых рассматривают идентификатор информационного потока. Затем проверяют наличие выделенного идентификатора в множестве предварительно заданных опорных идентификаторов. Наличие идентификатора в списке опорных означает, что пакет является санкционированным и переданный пакет разрешается доставить получателю. В ином случае ИП считается несанкционированным и переходят к сравнению адреса отправителя (нарушителя) с адресами отправителей, указанными в опорных идентификаторах санкционированных ИП. В случае совпадения адреса отправителя (нарушителя) принятого пакета сообщений также ищут адрес получателя принятого пакета во множестве опорных идентификаторов санкционированных получателей. Если адрес не был обнаружен в множестве допустимых адресов получателей, делают проверку в заранее заданном множестве ложных получателей. В случае, если адрес отсутствует в этих трех множествах, передача пакета блокируется. В случае, если отправитель принятого сообщения не найден во множестве опорных санкционированных отправителей или адрес получателя найден в списке опорных санкционированных получателей или адрес получателя найден в списке ложных идентификаторов определяют протокол взаимодействий принятого пакета сообщений и формируют ответный пакет сообщения. Сформированный пакет отправляется отправителю с заданной задержкой.

Второй вариант способа отличается от первого варианта тем, что дополнительно считают полученные пакеты и удаляют каждый i-й пакет, моделируя тем самым плохой канал связи. Третий вариант способа дополняет второй вариант тем, что запоминают отправителей несанкционированных потоков и пропускают значительное число проверок идентификаторов и протоколов.

Таким образом, в предложенном способе достигается оперативное выявление несанкционированных воздействий и введение злоумышленника в заблуждение как относительно качества канала связи, так и структуру ИКС.

Разработанное на платформе Java программное обеспечение Jerco позволяет применять метод и методику на практике. Приложение состоит из двух частей: библиотеки jerco-api с реализацией перколяции на произвольном графе (реализация метода) и приложения jerco-gui с оконными формами и расчетами метрик методики (поддержка методики). Ядро системы предоставляет необходимые функции по представлению ИКС в виде произвольного

графа и осуществлению моделирования перколяционных процессов. Библиотека может быть использована при работе в таких приложениях, как Wolfram Mathematica, Matlab, Maple или при разработке других Java-приложений.

Для практического применения конечным пользователем разработано программное обеспечение с графическим интерфейсом пользователя jerco-gui, использующее jerco-api в качестве подключаемой библиотеки. По результатам моделирования осуществляется построение графиков количественных и вероятностных метрик введенных в методе оценки надежности ИКС. Дополнительно поддерживается экспорт результатов экспериментов в текстовый файл для дальнейшей обработки в специализированном программном обеспечении.

В заключении сформулированы основные научные и практические результаты, полученные на основе проведенных в диссертационной работе исследований.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В ходе диссертационного исследования получены следующие основные результаты:

1. Произведен анализ требований к компьютерным сетям, показана необходимость создания территориально распределенных компьютерных сетей и тем самым интеграция с ССОП (Интернет). Интеграция с Интернет приводит к наличию в составе ИКС значительной доли не принадлежащих владельцу ИКС элементов. Выявлено противоречие между существующем методическим обеспечением надежности интегрированных компьютерных сетей, учитывающих наличие не принадлежащих владельцу элементов, и требованиям предъявляемым к надежности.

2. Разработан метод оценки надежности интегрированных компьютерных сетей. При этом процесс передачи информационного потока между территориально распределенными сегментами ИКС моделируется как процесс просачивания одного вещества (информационного потока) через другое (компьютерная сеть). Элементы компьютерной сети могут перестать пропускать через себя трафик в результате воздействия преднамеренной и непреднамеренной помехи. Введены количественные оценки работоспособного кластера, сохранившегося после воздействия ПНП, и вероятностные оценки сохранения связи между элементами ИКС.

3. Разработана методика сравнительной оценки различных альтернативных структур ИКС, получаемых в результате выбора того или иного оператора телекоммуникационных услуг.

4. Разработаны способы обеспечения надежности ИКС во время эксплуатации: способ обеспечения надежности путем выбора альтернативного

маршрута, который является наиболее устойчивым к воздействию преднамеренных и непреднамеренных помех; способ обеспечения надежности в случае воздействия преднамеренной помехи путем введения злоумышленника в заблуждение относительно структуры сети.

5. Разработано программное обеспечение для практического применения метода и методики.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях, рекомендованных ВАК России:

1. Выговский Л.С., Максимов Р.В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи [Текст] // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. СПб. 2008. Вып. 60. С. 166–173.

2. Выговский Л.С. Модель и метод оценки интегрированных объектов информатизации в условиях воздействия преднамеренных и непреднамеренных помех [Текст] // Известия СПбГЭТУ «ЛЭТИ». СПб. 2010. Вып. 7. С. 26–30.

Патенты:

3. Л.С. Выговский, Р.В. Максимов, Д.А. Кожевников и др. Способ (варианты) защиты вычислительных сетей Патент РФ №2307392 от 27.09.2007.

4. Л. С. Выговский, Р.В. Максимов, К.М. Зорин и др. Способ сравнительной оценки структур информационно-вычислительной сети. Патент РФ по заявке № 2009129726 03.08.2009.

Публикации в других изданиях:

5. Выговский Л.С., Максимов Р.В., Кожевников Д.А. и др. Способ (варианты) защиты вычислительных сетей (статья) [Текст] // Бюллетень «Изобретения. Полезные модели» №27 от 27.09.2007.

6. Выговский Л.С., Максимов Р.В. Модель распространения вредоносного программного обеспечения [Текст] // Сб. тр. 63 науч.-техн. конф. СПбНОТОРЭС им. А.С. Попова, посвященной дню радио, СПб. 2008г. С. 133.

7. Выговский Л.С., Максимов Р.В. Способ сравнительной оценки устойчивости информационной структуры интегрированных систем связи [Текст] // Тр. всеармейской НПК «Инновационная деятельность в ВС РФ». СПб. 2008. С. 188-194

8. Выговский Л.С. Модель доступности интегрированного объекта информатизации органов государственной власти в условиях воздействия преднамеренной и непреднамеренной помехи [Текст] // Сб. тр. 65 науч.-техн. конф. СПбНОТОРЭС им. А.С. Попова, посвященной дню радио, СПб. 2010г.