МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

на правах рукописи

ГОРШКОВ ТИМОФЕЙ ЮРЬЕВИЧ

# РАЗРАБОТКА МЕТОДИКИ ВЗАИМОДЕЙСТВИЯ УДАЛЁННЫХ ЗАЩИЩЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ ПРИ СОВМЕСТНОМ ОБСЛУЖИВАНИИ ЗАЯВКИ

Специальность 05.12.13 — Системы, сети и устройства телекоммуникаций

АВТОРЕФЕРАТ
диссертации на соискание учёной степени кандидата
технических наук

Москва — 2008

Работа выполнена на кафедре Инфокоммуникационных Систем и Сетей в Московском Физико-Техническом Институте (Государственном Университете)

Научный руководитель: доктор технических наук, профессор Буланова Татьяна Алексеевна

Официальные оппоненты: доктор технических наук, профессор Рыбин Виктор Михайлович (МИФИ)

доктор технических наук, профессор Петров Олег Михайлович (МГУПИ)

Ведущая организация: Центр Информационных Технологий и Систем органов исполнительной власти РФ (ЦИТИС)

Защита состоится 9 декабря 2008 г. в 15:30 на заседании диссертационного совета Д 212.156.04 при Московском физико-техническом институте (ГУ) по адресу: 141700, г. Долгопрудный, Московская обл., Институтский пер., д. 9, ауд. 204 Нового корпуса.

Отзывы направлять по адресу: 141700, г. Долгопрудный Московской обл., Институтский пер., д. 9, МФТИ.

С диссертацией можно ознакомиться в библиотеке МФТИ (ГУ).

Автореферат разослан "___" ноября 2008 г.

Учёный секретарь диссертационного
совета Д 212.156.04, МФТИ
к.т.н., доцент Л.П. Куклев

# Общая характеристика работы

**Актуальность темы.** Масштабность программ информатизации, высокая скорость внедрения инфокоммуникационных технологий во все сферы производства и жизнедеятельности людей, приводит к тому, что решаемые с помощью компьютерных систем задачи или разрабатываемые системы зачастую распределены и неоднородны. Одновременно растет и многообразие сетевых протоколов, обслуживающих взаимодействия систем друг с другом.

Взаимодействующие системы во многих случаях управляются различными организациями, не имеют общей цели и созданы различными разработчиками. Таким образом, при взаимодействии удаленных инфокоммуникационных систем возникает ряд новых задач, имеющих важное практическое значение в таких областях как распределенное решение сложных задач, совместное предоставление услуг, совместная распределенная разработка компьютерных программ, оптимизация бизнес-процессов и моделирование интегрированных производственных систем.

Свойства распределенности и децентрализованности в некоторых случаях дополняются свойством открытости: состав и функциональные характеристики взаимодействующих систем могут изменяться в процессе взаимодействия систем. В отсутствии единого проекта всех взаимодействующих систем, создание и развитие происходит в виде технической эволюции, поэтому аналитику или проектировщику требуются новые методы работы с такого рода системами.

Научные исследования в области взаимодействия инфокоммуникационных систем на данный момент представлены в нескольких научных направлениях: в теории операций, в теории массового обслуживания, алгоритмах маршрутизации, в исследованиях, посвященных искусственному интеллекту (в теории конечных автоматов и исследованиях по многоагентным системам). Отдельно развивается направление криптографических алгоритмов и протоколов, содержащее важные

результаты по защите информации, но данные результаты редко применяются на стадии проектирования алгоритмов взаимодействия компонент систем.

Все перечисленные направления развиваются достаточно обособлено и среди доступных работ практически отсутствуют примеры комплексной проработки вопроса взаимодействия инфокоммуникационных систем. Таким образом, проблемы организации совместного обслуживания множеством интеллектуальных агентов, возможность их координации и обеспечения защищённой работы продолжают оставаться актуальными. В данной диссертационной работе поставлена задача обобщить имеющийся опыт, предложить на его основе модель инфокоммуникационной системы и разработать методику исследования взаимодействия инфокоммуникационных систем.

Необходимо подчеркнуть важную роль алгоритмов защиты информации и установления доверия, рассмотренных в данной работе, так как их включение во взаимодействие приводит к существенным изменениям в архитектуре и алгоритмах работы. Поскольку реализация распределенной инфокоммуникационной системы, независимые агенты которой взаимодействуют через открытые каналы связи, диктует серьезные требования по информационной безопасности, то отсутствие их учета в методике рассмотренных механизмов существенно снизило бы практическую значимость предложенной методики.

Разработка технологий интеллектуальных программных агентов и создание методики их взаимодействия является одной из наиболее важных и многообещающих областей исследования в сфере информационных и коммуникационных технологий, где сегодня происходит интеграция технологий передачи данных, методов искусственного интеллекта и систем объектно-ориентированного проектирования.

Разработанная методика достаточно полно покрывает круг теоретических вопросов, возникающих при реализации защищенного взаимодействия инфокоммуникационных систем, и снабжает конструктора

или архитектора программного обеспечения моделью и набором методов для решения практических задач.

**Целью диссертационной работы** является разработка методики анализа и проектирования взаимодействия распределенных инфокоммуникационных систем, представленных в виде множества взаимодействующих агентов, построение общей модели инфокоммуникационной системы, исследование компонент инфокоммуникационных систем и алгоритмов их безопасного взаимодействия.

Поставленная цель определила необходимость решения следующих **задач**:

- Анализ преимуществ и недостатков существующих подходов интеграции удаленных инфокоммуникационных систем,
- Построение теоретической сервисной модели взаимодействия удаленных защищенных информационных систем,
- Разработка вероятностной модели обслуживания заявки и получение набора ключевых показателей для выбора стратегии поведения,
- Анализ источников угроз информационной безопасности и построение модели нарушителя в открытой многоагентной инфокоммуникационной системе,
- Разработка архитектуры и методики взаимодействия агентов удаленных инфокоммуникационных систем,
- Разработка и внедрение предложенной архитектуры и методики для взаимодействия нескольких организаций, вовлеченных в совместный процесс обслуживания заявок.

**Методологической основой исследования** являются методика исследования локально-организованных систем, описанная в работах В.Л.Стефанюка, методология агентно-ориентированного анализа и конструирования, разработанная в работах Вулдриджа, Дженнингса и Кинни,

а также методики моделирования информационной безопасности систем, изложенной в работах Гогена и Месгуера.

**Теоретическую основу исследования** составили работы по многоагентным системам Тарасова В.Б., Варшавского В.И., Поспелова Д.А., Н. Дженнингса, теории иерархических и локально-организованных систем, теории акторов и распределенных вычислений и работы по криптографическим протоколам.

**Опытно-экспериментальной базой исследования** являлись отечественные разработки в области программных коммутаторов и алгоритмов маршрутизации голосовых соединений, интеграционные проекты по организации взаимодействия систем управления через сервисную шину, проект по реализации информационно-справочных услуг в телефоне нового поколения с помощью веб-сервисов.

**Научная новизна диссертационной работы** заключается в том, что в ней решен комплекс теоретических и практических проблем взаимодействия распределенных инфокоммуникационных систем, представленных в виде множества взаимодействующих агентов. А именно:

1. Разработана методика взаимодействия удаленных защищенных инфокоммуникационных систем, позволяющая исследовать и проектировать инфокоммуникационные системы, построенные на основе множества взаимодействующих агентов.
2. Разработана модель инфокоммуникационной системы, отражающая современные технологические тенденции создания распределенных и открытых систем. Раскрыт и обоснован состав ролей агентов в модели инфокоммуникационной системы.
3. Предложены алгоритмы взаимодействия агентов, повышающие качество обслуживания и сокращающие количество повторных посылок заявок.
4. Предложены способы защиты на основе анализа угроз безопасности, возникающих при взаимодействии агентов удаленных инфокоммуникационных систем в разработанной модели.

**Практическая значимость исследования** определена возможностью использования содержащихся в нем моделей и методов взаимодействия в практических задачах:

- интеграции разрозненных систем управления внутри одной организации,
- организации маршрутизации телефонных вызовов в пакетных сетях (IP-телефония),
- совместного предоставления услуг и построения цепочек предоставления услуг от источников к конечному потребителю составной услуги,
- предоставления информационно-справочных услуг по распределённым источникам информации.

**Основные положения, выносимые на защиту:**

1. Модель инфокоммуникационной системы на основе взаимодействующих программных агентов. Взаимодействие между агентами осуществляется в виде заявок-сообщений, которые соответствуют обращению к определенным сервисам агента.
2. Вероятностная модель обслуживания заявки и сценарии выбора времени ожидания обработки заявки, основанные на численных метриках.
3. Модель угроз информационной безопасности в инфокоммуникационной системе, являющейся открытой для подключения новых агентов.
4. Методы защиты взаимодействия агентов в виде сценариев и анализ их надежности.
5. Многоагентная архитектура инфокоммуникационной системы, основывающаяся на разделении ролей и обеспечивающая защищенное

взаимодействие компонент системы в открытой информационной среде.

6. Методика исследования и организации взаимодействия в инфокоммуникационных системах при совместном обслуживании заявки.

**Апробация и внедрение результатов исследования.** Основные результаты диссертационной работы обсуждались на 48-й и 50-й научной конференции «Современные проблемы фундаментальных и прикладных наук» (Москва, 2005, 2007) на 30-й конференции молодых ученых и специалистов ИППИ РАН «Информационные технологии и системы» (Звенигород, 2007). Результаты, связанные с обеспечением безопасности взаимодействия обсуждались на Международном форуме информатизации «Телекоммуникационные и вычислительные системы» на секции «Безопасность. Охрана и защита информации» (Москва, 2007). Разработанная методика взаимодействия обсуждалась на VII Международной научно-технической конференции «Перспективные технологии в средствах передачи информации» (Владимир-Суздаль, 2007). Внедрение результатов диссертационной работы подтверждается соответствующим актом.

**Публикации**. По теме диссертации опубликовано 9 работ. Из них 3 статьи и 6 докладов в материалах всероссийских и международных конференций.

**Объем и структура диссертации**. Диссертация содержит введение, пять глав, выводы, список литературы и приложение. Общий объем диссертации составляет 139 страниц, из них 129 - основной текст, 10 - список литературы из 78 наименований, в том числе 32 - отечественной, 46 - зарубежной. Работа содержит 54 рисунка и 4 таблицы.

# Основное содержание диссертации

**Во введении** обоснована актуальность темы исследования, сформулированы цель и задачи; определены объект, предмет и методы исследования; раскрыты научная новизна, теоретическая и практическая значимости работы, ее апробация, представлены положения, выносимые на защиту.

**В первой главе** раскрыты основные подходы к исследованию инфокоммуникационных систем в современных научных публикациях. Рассмотрены элементы общей теории систем, локально-организованных систем, многоагентных систем, модель акторов.

Проанализирован механизм контрактных сетей как способ кооперации агентов в открытой системе. Показаны его преимущества и недостатки с целью предложить в следующих главах альтернативный механизм с инфраструктурными агентами, регистрирующими предоставляемые сервисы, и механизмом вероятностной оценки времени ожидания обработки заявки.

Практическая сторона применения моделей рассмотрена в виде существующих моделей интеграции программного обеспечения.

**Во второй главе** предложена модель инфокоммуникационной системы на основе агентов, взаимодействующих между собой с помощью заявок, а также предложена вероятностная модель обработки заявки. На основе предложенных моделей рассмотрены стратегии поведения агента, в том числе проведен расчет ключевых характеристик и их последующее сравнение путем моделирования на базе показательного распределения.

Единицу построения процесса обслуживания будем называть *сервисом*. Каждый агент может предоставлять другим агентам один или более сервисов. Предоставление сервиса есть суть передача одной или более заявок (сообщений) между агентами, один из которых запрашивает сервис, а другой предоставляет. Таким образом, *сервис* — это коммуникация двух или более агентов с целью решения отдельной формализованной задачи.

Среди всего многообразия агентов выделен класс *инфраструктурных агентов*, выполняющих вспомогательные задачи по обеспечению работоспособности и связности других агентов. Примерами сервисов, предоставляемых инфраструктурными агентами, могут быть регистрация, поиск, именование, аутентификация.

Рассматриваемая система задана в виде набора взаимодействующих агентов. Функциональность каждого из агентов представлена в виде списка сервисов. Принимаемая агентом заявка чётко идентифицируется как запрос к одному из сервисов.

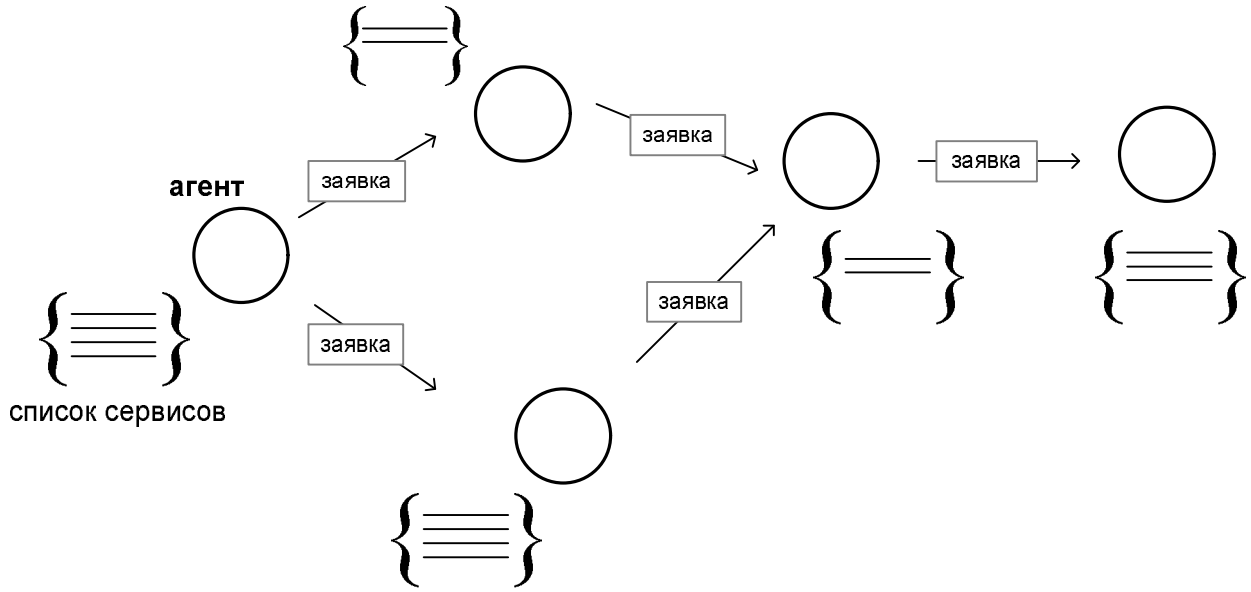


**Рис. 1. Сервисная модель взаимодействия агентов**

Передача сообщений осуществляется через среду. В модели не рассматривается возможность потерь и помех в каналах связи. Тем не менее, сами агенты при обработке заявок могут проявлять некорректное поведение: терять заявки, пытаться нарушить инструкции или видоизменить сообщения.

Внешний заказчик сервиса присылает заявку одному из агентов системы, обслуживающему заявки данного типа. Получивший агент обрабатывает заявку. Если он не в состоянии сам полностью выполнить обработку заявки, то он выбирает бизнес-процесс обработки данной заявки.

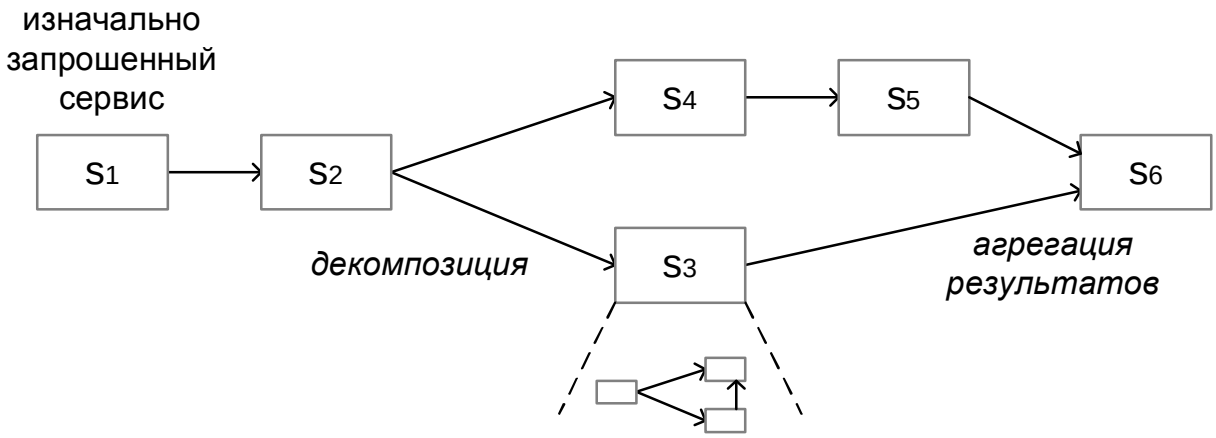


**Рис. 2. Декомпозиция на сервисы при обработке заявки**

Процесс представляется в виде ориентированного графа $W = (S,E)$, задающего последовательность вызова сервисов, где $S = \{s_1, s_2, \ldots, s_{|S|}\}$ – множество узлов, каждый из которых задает сервис, а $E \in S \leftrightarrow S$ – множество ребер, задающих последовательность вызова сервисов.

В построенном графе узлы задают только типы сервисов. Поэтому для каждой вершины графа необходимо определить список агентов, предоставляющих сервисы данного типа. Для этого агент обращается к инфраструктурным сервисам и получает списки доступных на данный момент агентов для каждого из типов сервисов.

По получению списка агент применяет правила безопасности. На этом шаге фильтруются те пары {агент, сервис}, которые не удовлетворяют правилам. Если после фильтрации для какого-то из сервисов осталось более одного агента, то этот список может быть ранжирован в соответствии с метрикой, применяемой на основе имеющейся информации об агентах. Как для принятия решений по правилам безопасности, так и при определении приоритетов пар могут проводиться запросы к инфраструктурным сервисам.

После того, как для каждого из сервисов определен приоритетный агент его исполнения, проводится посылка заявок агентам, соответствующим узлам графа $W$, и выбирается стратегия ожидания обработки заявки в зависимости от того, какую из характеристик исполнения сервиса

необходимо оптимизировать. Это может быть стоимость или надежность. Предложенная в работе модель агента адресована ситуации, когда невозможно установить предпочтения между агентами, ввиду того, что доступная информация об их параметрах ограничена и одинакова для всех агентов, оставшихся в списке после фильтрации.

Пусть для исполнения заявки доступно $N$ агентов и пусть каждое обращение к любому из агентов имеет стоимость $c$ (например, в единицах полосы пропускания или в денежном выражении). Возможны разные стратегии обращений к агентам, такие как:

- обращение к произвольно выбранному агенту для исполнения заявки и ожидание до тех пор, пока она не будет исполнена;
- рассылка заявок параллельно всем агентам с целью максимизировать вероятность успешного исполнения;
- посылка заявки одному из агентов, ожидание выбранного промежутка времени и посылка заявки следующему агенту из списка.

В работе на основе предположений о вероятностном характере времени обработки заявки получены выражения для функции полезности $u$ для трёх приведённых стратегий:

$$u_1 = r \cdot p \cdot D(t_{\max}) - c,$$

$$u_2 = r \cdot (1 - (1 - p \cdot D(t_{\max}))^k) - k \cdot c,$$

$$u_3 = (r - \frac{c}{p \cdot D(w)}) \cdot (1 - (1 - p \cdot D(w))^m).$$

Для сравнения стратегий рассмотрим частный случай функции распределения. С точки зрения практики наиболее интересным является случай, когда время обработки отдельной заявки имеет показательное распределение

$$r(t) = m \cdot e^{-m \cdot t}.$$

В таком случае для стратегии 1 получаем вероятность успешного исполнения заявки, среднее время обработки заявки и выражение для функции полезности:

$$s = p \cdot D(t_{\max}) = p \cdot \int_0^{t_{\max}} m \cdot e^{-m \cdot t} dt = p \cdot (1 - e^{-m \cdot t_{\max}}),$$

$$\bar{d} = \int_0^{t_{\max}} t \cdot r(t) dt = \frac{1}{m} - \left( \frac{1}{m} + t_{\max} \right) e^{-m \cdot t_{\max}},$$

$$u_1 = r \cdot p \cdot D(t_{\max}) - c = r \cdot p \cdot (1 - e^{-m \cdot t_{\max}}) - c.$$

Для стратегии 2 получаем:

$$s = 1 - (1 - p \cdot (1 - e^{-m \cdot t_{\max}}))^k,$$

$$\bar{d} = \int_0^{t_{\max}} t \cdot \tilde{r}(t) dt = k \int_0^{t_{\max}} t \cdot (1 - p \cdot (1 - e^{-m \cdot t}))^{k-1} \cdot m \cdot e^{-m \cdot t} \cdot dt,$$

$$u_2 = r \cdot (1 - (1 - p \cdot (1 - e^{-m \cdot t_{\max}}))^k) - k \cdot c.$$

Для стратегии 3 получаем:

$$s = 1 - (1 - p \cdot (1 - e^{-m \cdot w}))^m,$$

$$\bar{d} = \int_0^{w} t \cdot r(t) dt + \frac{w \cdot \left( (1 - p \cdot (1 - e^{-m \cdot w})) - m(1 - p \cdot (1 - e^{-m \cdot w}))^m \right)}{1 - (1 - p \cdot D(w))^m \cdot p \cdot (1 - e^{-m \cdot w})} +$$

$$+ \frac{w \cdot \left( (m-1)(1 - p \cdot (1 - e^{-m \cdot w}))^{m+1} \right)}{1 - (1 - p \cdot D(w))^m \cdot p \cdot (1 - e^{-m \cdot w})},$$

$$t_{\max} = w \cdot m,$$

$$u_3 = \left( r - \frac{c}{p \cdot (1 - e^{-m \cdot w})} \right) \cdot (1 - (1 - p \cdot (1 - e^{-m \cdot w}))^m).$$

Для стратегии 2 возможно варьирование параметра ***k*** с целью нахождения оптимального количества заявок, которое необходимо послать

агентам-исполнителям. Для стратегии 3 для нахождения оптимального значения функции полезности возможно варьирование времени ожидания ***w*** перед посылкой заявки следующему агенту-исполнителю.

На основе данных моделирования сделан следующий вывод: при достаточно большом соотношении коэффициентов ***r/c*** и достаточном времени $t_{max}$ становится выгодным использование стратегий 2 и 3, как при низкой вероятности исполнения заявки отдельно взятым агентом, так и при высокой.

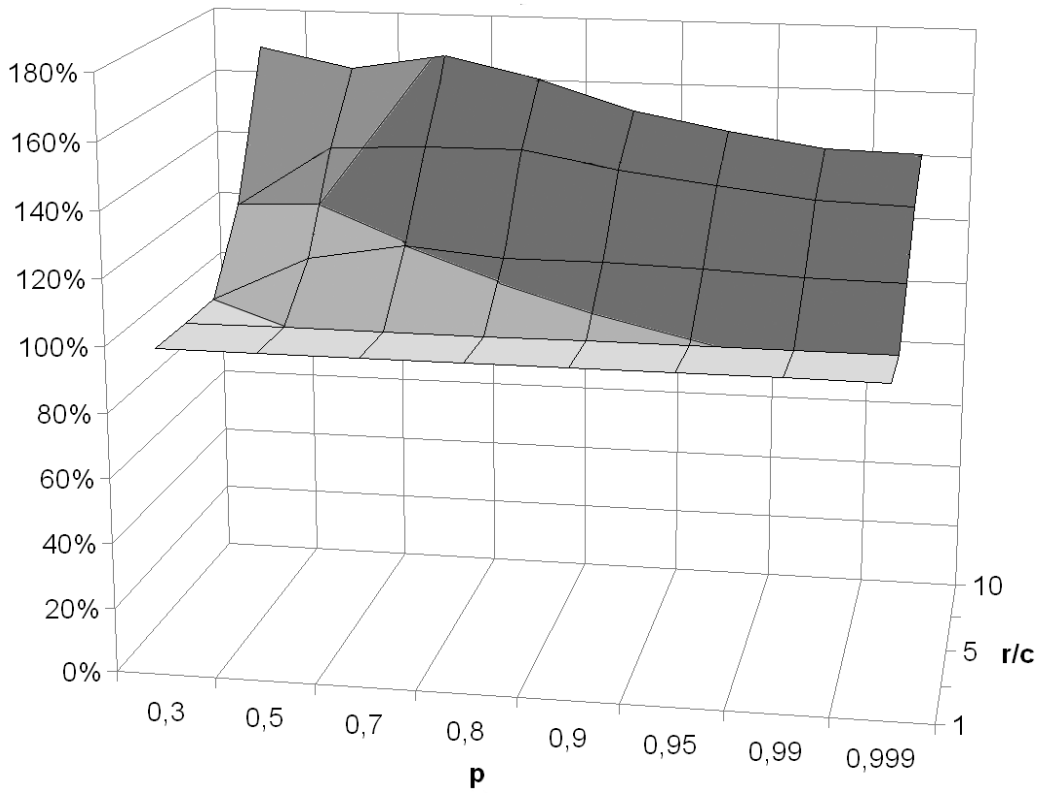


**Рис. 3. Области применимости стратегий ($T_{max}$ = 10 и μ=0.1)**

Тем не менее, использование стратегий 2 и 3 может давать отрицательный результат даже при малых параметрах ***k*** и ***m***, если соотношение ***r/c*** невелико. Таким образом, для выбора наиболее выигрышной стратегии агенту-инициатору заявок необходимо проводить оценку параметров. Значения **p** и **μ** могут вычисляться на основе статистики в конкретной рассматриваемой инфокоммуникационной системе.

**Оптимальная стратегия**

Пусть для определения времени отправки заявки агент каждый раз решает задачу по максимизации функции полезности. При наличии доступных (и ещё не опрошенных) агентов выполняется вычисление значений функции полезности для возможных моментов времени ожидания перед посылкой заявки. Из данных вычислений выбирается максимальное положительное значение. Соответствующее ему время ожидания **τ** используется как время ожидания перед отправкой заявки. Сразу после отправки заявки проводится повторное вычисление времени ожидания и так далее. При этом успешная обработка посланных заявок, произошедшая по истечении времени ожидания **τ,** также считается успешной и отслеживается.

Такой подход позволяет максимизировать функцию полезности с точностью до шага при вычислении **τ**. Недостатком подхода является большая вычислительная нагрузка, приходящаяся на агента.

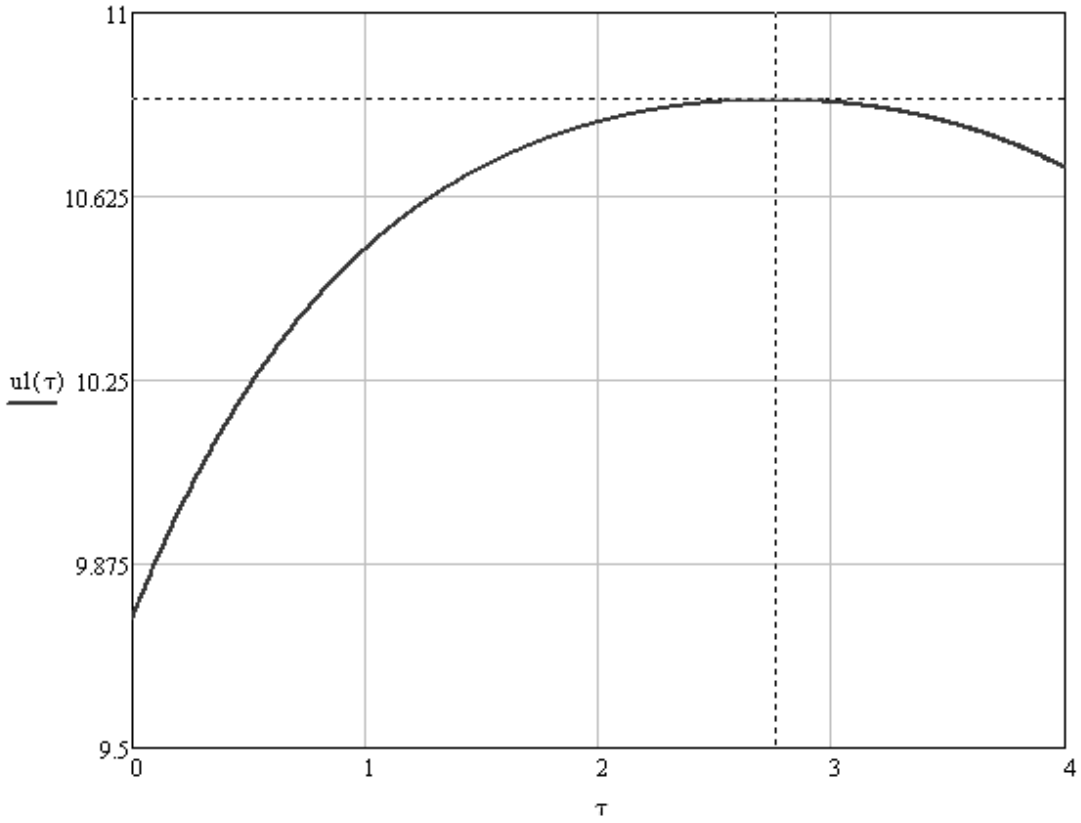


**Рис. 4. Функция полезности для оптимальной стратегии при k=1**

Приведем выражение для функции полезности на шаге **k**:

$$u_k = \int_{T_k}^{t} (r - c_k) \cdot (1 - F(t))' dt + \int_{t}^{T_{\max}} (r - c_k - c) \cdot \left(1 - F(t) \cdot \hat{f}(t - t)\right)' dt .$$

График функции полезности для k=1, r/c=10, p=0.99 и $T_{max}$ = 4 приведен на рис. 4.

Из полученного графика можно сделать вывод: оптимальный выбор времени ожидания перед посылкой второй заявки будет в точке максимума функции полезности на отрезке [0,$T_{max}$] и в приведённом примере составит 2,75 секунды.

**В третьей главе** рассмотрен вопрос обеспечения информационной безопасности при взаимодействии инфокоммуникационных систем и влияние решения вопроса безопасности на алгоритмы взаимодействия агентов, предложенных во второй главе.

Обозначим категории нарушителей в виде **A** и **B**, для внешних и внутренних нарушителей соответственно.

Сводная таблица угроз представлена в таблице 1.

**Таблица 1. Источники угроз**

| **Модель** | **Краткое описание** |
|---|---|
| *Внешние источники угрозы* | |
| **A1** | Подслушивание и анализ шаблонов трафика |
| **A2** | Подключение от имени другого агента / перехват сессии |
| **A3** | Перегрузка и отказ в обслуживании |
| **A4** | Повторные посылки заявок |
| *Внутренние источники угрозы* | |
| **B1** | Регистрация в системе в качестве шлюза к другим сервисам |
| **B2** | Сбор заявок на себя и их необслуживание |
| **B3** | Изменение маршрута заявки (если он содержится в заявке) |
| **B4** | Симуляция инфраструктурных сервисов. |
| **B5** | Нарушение конфиденциальности пользовательских данных |

Для каждой из моделей угроз в работе выполнен анализ. Так, для угрозы **B2** (сбор заявок на себя и их необслуживание) возможны минимум два варианта защиты. Общим для них является накопление информации о «благонадежности» того или иного агента. Первый вариант: каждый агент, для которого является критическим необслуживание своей заявки по определенному сервису, использует внутреннюю метрику, основанную на опыте взаимодействия с другими агентами. Второй вариант, когда подобная метрика является централизованной и является доступной в виде инфраструктурного сервиса. Возможно разделение метрик надежности агента и безопасности. Рассмотрим подробнее преимущества и недостатки централизованного и локального варианта, отражённые в таблице 2.

**Таблица 2. Сравнение локальной и централизованной метрики**

| | Локальная метрика | Централизованная метрика |
|---|---|---|
| Универсальность | Каждый агент сам определяет, насколько критичной является заявка и применяет ту метрику, которая соответствует логике работы. | Необходимо использовать алгоритм общий для всех агентов. Возможно формирование набора метрик (надежность, задержка обслуживания, доверие и т.п.) |
| Скорость работы | Быстро, локальный подсчет | Задержка из-за обращения к инфраструктурному сервису перед посылкой каждой заявки |
| Уязвимость | Мало данных по другим агентам. Атака B2 остается легко осуществимой | Возможна оперативная блокировка агента или быстрое занижение его метрики. |

При организации взаимодействия агентов через транспортные инфраструктурные узлы, данные узлы могут быть использованы для блокировки атаки на основе централизованной метрики. При этом сами транспортные узлы и сервисы метрики являются новыми объектами с

потенциальными уязвимостями, а их «взлом» приводит к дестабилизации всей инфокоммуникационной системы.

В работе представлены методы и сценарии взаимодействия, направленные на защиту от проанализированных возможных угроз. Предложенные сценарии абстрактных протоколов используют как пример средства криптографии с открытым ключом.

**В четвертой главе** введены роли взаимодействующих агентов и на их основе построена обобщенная архитектура взаимодействия инфокоммуникационных систем.

При разработке архитектуры и методики взаимодействия инфокоммуникационная система рассматривалась как набор ролей, взаимодействующих друг с другом. Роли характеризуют функции агентов независимо от их внутренней структуры и определяются с помощью полномочий, ответственности и протоколов.

По ролевому признаку можно вычленить следующие основные виды агентов в инфокоммуникационных системах:

1. Агент-транспорт, обеспечивающий связанность между другими агентами
2. Агент-реестр, регистрирующий сервисы, предоставляемые в системе
3. Агент-гарант, осуществляющий проверки корректности данных и доверия к их источнику
4. Агент-шлюз, осуществляющий фильтрующий и транслирующий заявки
5. Агент-заказчик, рассылающий заявки на выполнение некоторого задания другим агентам
6. Агент-исполнитель, выполняющий заявку и отправляющий ответ-результат
7. Агент-координатор, выбирающий процесс обработки заявки другими агентами.

Из перечисленных ролей первые четыре можно отнести к инфраструктурным ролям, так как они носят универсальных характер и слабо зависят от предметной области, с которой работает инфокоммуникационная система. Три последние роли непосредственно вовлечены в функциональные процессы. Дл каждой из ролей в работе приведены полномочия, ответственности и протоколы взаимодействия.

Агент — предоставляет и/или использует сервисы, получает заявки, обрабатывает их и отправляет другим агентам (ответ или задание).

Можно считать, что инфокоммуникационная система с единой транспортной средой имеет одну компоненту связности. Если различные агенты используют разные транспортные среды или если из соображений безопасности необходимо разделить транспортную среду на безопасно взаимодействующие сегменты, следует вводить несколько компонент связности, разделённые агентами-шлюзами. Ниже на рис. 5 показан пример двух инфокоммуникационных систем, взаимодействующих через внешнюю общую транспортную среду.

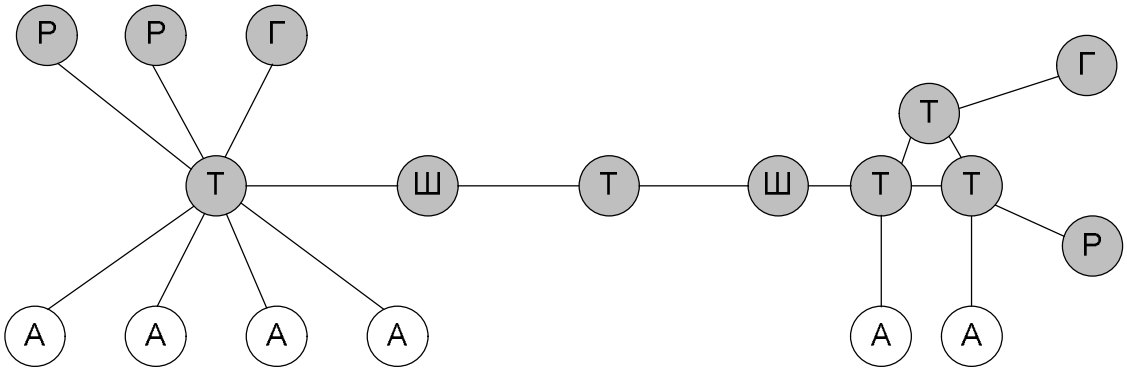


**Рис. 5. Взаимодействие двух инфокоммуникационных систем**

Взаимодействие между агентом-заказчиком и агентом-исполнителем состоит из трёх этапов: «подготовка – отправка заявки – прием результата». На этапе подготовки агент-заказчик направляет запросы инфраструктурным сервисам, для выбора подходящего агента-исполнителя. Условия выполнения сервиса агентом-исполнителем описываются в реестре, а потому в отличие от контрактных сетей переговоры не проводятся. На втором этапе происходит

отправка заявки агенту-исполнителю. Затем агент-заказчик начинает ожидать результата работы. Агент-исполнитель выполняет работу и окончив ее, докладывает агенту-заказчику о завершении. Агент-заказчик решает, удовлетворяет ли его результат и в зависимости от этого предпринимает дальнейшие шаги. Адекватная модель взаимодействия – конечный автомат с фиксированным пространством состояний.

Приведём определение и модель инфокоммуникационной системы, уточнённой по результатам глав 1-4 работы.

*Инфокоммуникационная система A* — это локально-организованная система, состоящая из неоднородной группы агентов $A_i$, взаимодействующих через одну или более сетевых сред путем обмена информацией в виде заявок, каждый из которых может в свою очередь представлять собой локально- или глобально-организованную инфокоммуникационную систему. Взаимодействующие агенты могут быть географически удалены друг от друга и иметь связь через цепочку других агентов.

Рассмотрим инфокоммуникационную систему A, состоящую из группы агентов $A_i$ и взаимодействующую с внешними инфокоммуникационными системами B, C, D,…

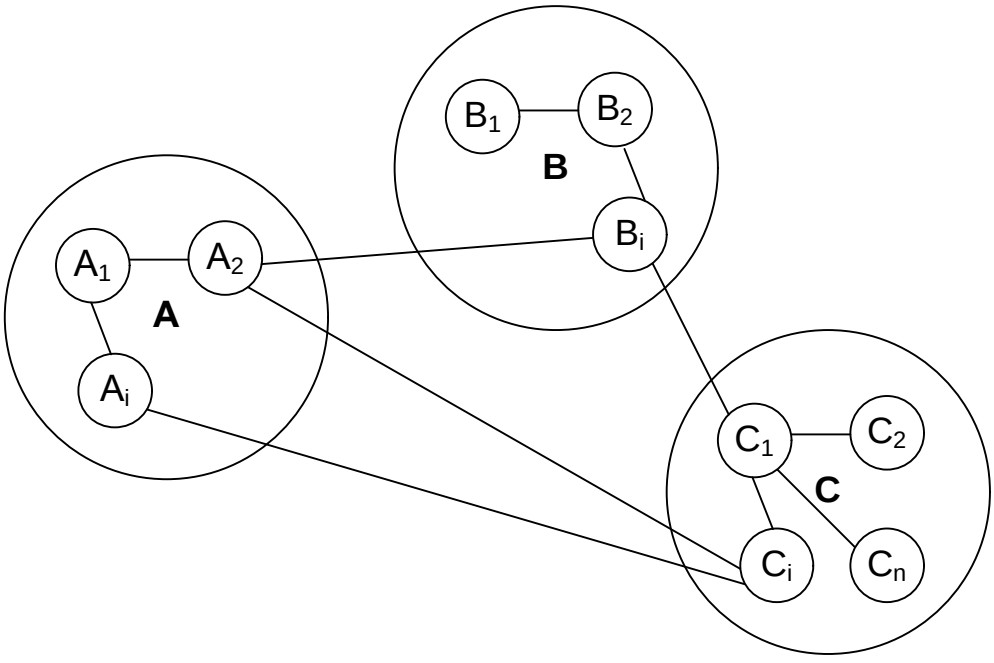


**Рис. 6. Модель инфокоммуникационной системы**

Каждый агент $A_i$ из системы A стремится достичь своей цели $G_i$ независимо от действий остальных агентов. Инфокоммуникационная система A может иметь общую цель, заданную при проектировании, тем не менее, в общем случае она имеет только локальные цели, определенные лишь для её агентов. Целью всей системы можно считать обеспечение возможности функционирования её подсистем $A_i$, обеспечение связности агентов, открытость к вхождению новых агентов, устойчивость и живучесть по отношению к атакам нарушителей и случайным ошибкам.

Взаимодействие между агентами, как внутри системы A, так и вне её, осуществляется путем посылки заявок-сообщений q. Пусть функциональность каждого из агентов представлена в виде списка сервисов $\{S_i\}$. Принимаемая агентом заявка чётко идентифицируется как запрос к одному из сервисов. Результатом обработки заявки является выполнение каких-либо действий и в большинстве случаев возврат сообщения-результата $r_i(q,t)$.

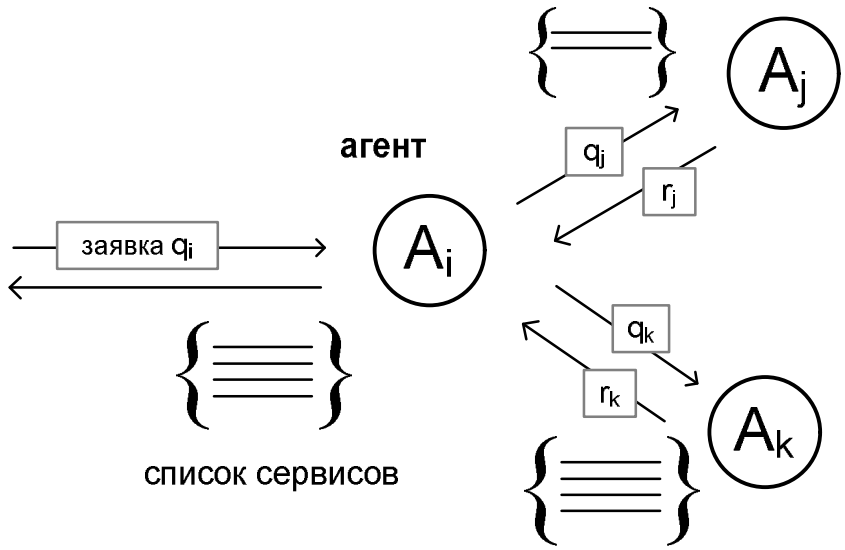


**Рис. 7. Взаимодействие агентов**

Обрабатывая заявку $q_i$, агент $A_i$ рассылает заявки на дополнительные сервисы: $q_i(t) = q_i(q_{i1}(t), q_{i2}(t),\ldots, q_{in}(t))$ , где $q_{ij}(t)$ — заявка, посылаемая агентом $A_i$ агенту $A_j$ в момент времени t. Пусть к моменту времени t вектор результатов обработки посланных агентом $A_i$ заявок: $r_i(t) = r_i(r_{i1}(t), r_{i2}(t),\ldots, r_{in}(t))$ , где $r_{ij}(t)$ — результат, получаемый агентом $A_i$ от агента $A_j$ в момент

времени t. Таким образом, взаимодействие агентов описывается двумя множествами векторов $q_i(t)$ и $r_i(t)$.

Методика организации анализа и проектирования удаленных защищённых инфокоммуникационных систем, совместно обслуживающих заявки сводится к следующим основным этапам:

I. Определение внешних систем, с которыми будут взаимодействовать агенты анализируемой инфокоммуникационной системы A;
II. Определение транспортных сред, в которых возможно взаимодействие между агентами как внутри инфокоммуникационной системы, так и с внешними агентами;
III. Определение возможных (необходимых, целевых) действий агентов и формирование списка предоставляемых сервисов, путем задания $q_i(t)$ и $r_i(t)$;
IV. Применение ролевой модели для выделения инфраструктурных ролей (транспорт, реестр, гарант, шлюз) и группировки возможных действий по агентам;
V. Указание модели взаимодействия агентов в части использования инфраструктурных сервисов;
VI. Определение списка предоставляемых сервисов на основе возможных действий, отнесённых к агенту $A_i$;
VII. Указание модели взаимодействия i-ого агента с остальными агентами как в рамках системы A (конечный автомат и его варианты реализации в протоколах);
VIII. Указание для каждого i-ого агента целевой функции $G_i(S_i, r_i(t))$ и построение алгоритма функционирования, включая модели выбора агента для исполнения сервисов и модели ожидания ответов $r_i(t)$ на посылаемые заявки $q_i(t)$;
IX. Анализ защищенности агентов и передаваемых ими данных относительно модели угроз для инфокоммуникационной системы;

X. Анализ функционирования системы А как совокупного результата действий её подсистем $A_i$, i=1…n по алгоритмам, построенным на этапах V-VIII;

XI. Определение сред, агентов, действий и протоколов, несоответствующих целевому функционированию системы;

XII. Возврат к этапу I и пересмотр выборов на каждом из этапов;

XIII. Если результат удовлетворительный, то реорганизация системы А в соответствии с результатами исследования.

**В пятой главе** разработанная методика применена для практических задач предоставления услуг связи на базе IP-сети при наличии большого количества взаимодействующих агентов. Предложены механизмы повышения эффективности и защищенности взаимодействия.

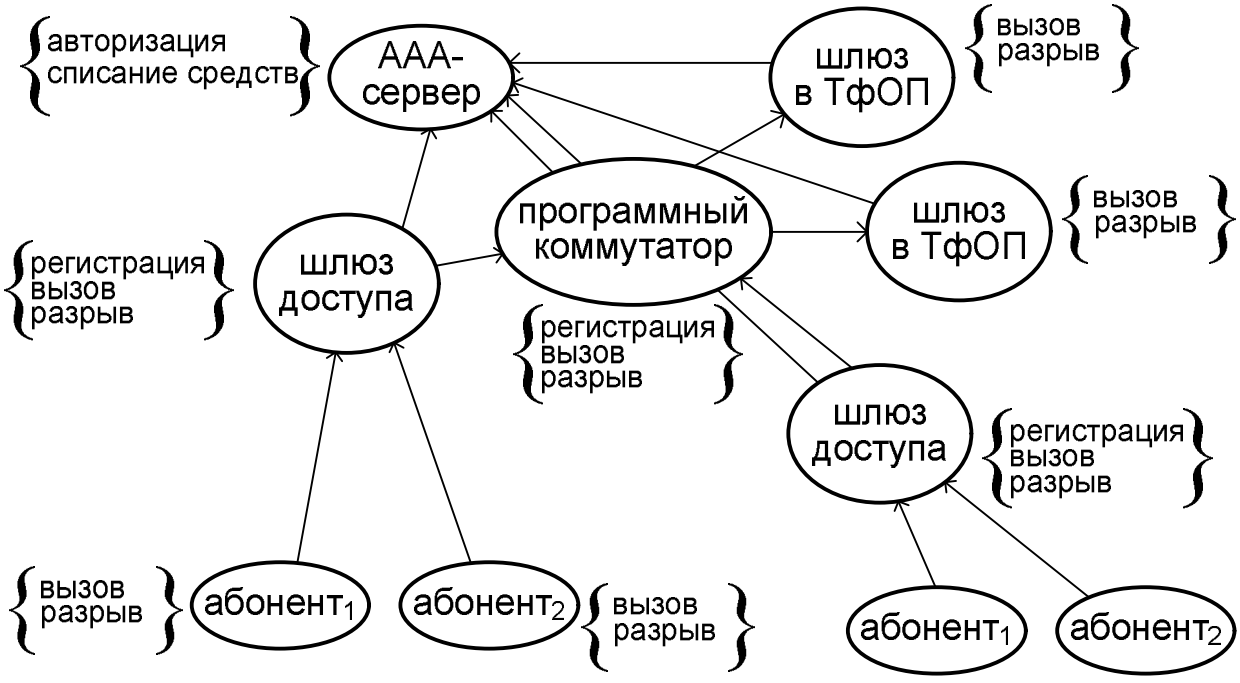


**Рис. 8. Модель системы ЦПГК**

В работе рассматривается инфокоммуникационная система — Центр Пакетной Голосовой Коммутации (ЦПГК), построенный на базе протокола SIP. На базе данной сети предоставляются услуги связи: голосового и видео-звонка, выход в телефонную сеть общего пользования (ТфОП).

За целевую функцию абонента взято его желание получить установленное соединение за комфортное время ожидания. Комфортным является время, не превышающее 5-7 секунд. В формализованном виде это можно записать как

$$G_{абонента}(t) = \begin{cases} 1, & 0 \le t \le T_{max} \\ 0, & t \ge T_{max} \end{cases} .$$

В процессе анализа системы было выявлено несколько мест, в которых можно провести улучшение исследуемой системы (ЦПГК) и сделать её более защищённой:

1. Было определено, что для программного коммутатора можно повысить вероятность успешного установления соединений без дублирования всех вызовов. Для этого необходимо внести коррективы в логику его работы, добавив реализацию динамического принятия решения о необходимости посылки заявки на второй и последующие шлюзы.
2. Ввиду низкой защищённости системы в целом, необходимо введение защиты сети Центра Пакетной Голосовой Коммутации на транспортном уровне, обеспечивающей шифрование всех передаваемых заявок между узлами сети. Абонентское подключение к шлюзу доступа рекомендуется защитить либо, внеся изменения в протоколы взаимодействия SIP и RTP (по сценариям, предложенным в части 3.4 работы), либо дополнив процедуру подключения абонента к шлюзу установлением выделенного соединения VPN.
3. Расширение функциональности программного коммутатора в части определения количества потенциальных агентов для отправки заявки и использование алгоритмов ожидания с учетом вероятности установления соединения по тому или иному направлению, полученному через сбор статистики успехов и неуспехов.

**В выводах** обобщены положения, вынесенные на защиту в каждой из глав, проанализирована применимость предложенного подхода и возможности практической реализации и намечены перспективы дальнейшего исследования рассматриваемой проблемы.

## Список работ, опубликованных по теме диссертации

1. Горшков Т.Ю. Методика взаимодействия защищенных удаленных инфокоммуникационных систем при совместном обслуживании заявки // *Инженерная Физика*, №4. – 2008.
2. Буланова Т.А. , Горшков Т.Ю. Методы защиты информации при взаимодействии инфокоммуникационных систем // *Инженерная Физика*, №4. – 2008.
3. Горшков Т.Ю. Модель взаимодействия удаленных инфокоммуникационных систем // *Приборы и Системы. Управление. Контроль. Диагностика*, №2. – 2008. – С.12-16.
4. Горшков Т.Ю. Источники угроз и модель нарушителя в открытой многоагентной инфокоммуникационной системе // *Международный форум информатизации (МФИ-2007): Труды конференции «Телекоммуникационные и вычислительные системы»*. –М.: МТУСИ. – 2007. – С. 203 - 205.
5. Горшков Т.Ю. Сервисная модель взаимодействия защищенных удаленных инфокоммуникационных систем // *Международный форум информатизации (МФИ-2007): Труды конференции «Телекоммуникационные и вычислительные системы»*. –М.: МТУСИ. – 2007. – С. 200 - 203.
6. Горшков Т.Ю. Модель взаимодействия многоагентных систем при совместном обслуживании заявки // *Сборник трудов конференции «Информационные технологии и системы» (ИТиС-2007).* – г.Звенигород: ИППИ. – 2007. – С. 162 - 165.

7. Горшков Т.Ю. Разработка методики взаимодействия защищенных инфокоммуникационных систем при совместном обслуживании заявки // *Тр. VII международной научно-технической конференции «Перспективные технологии в средствах передачи информации - ПТСПИ'2007»*. – Владимир: «РОСТ», – 2007.
8. Горшков Т.Ю. Методика взаимодействия инфокоммуникационных систем при совместном обслуживании заявки // *Труды 50-й юбилейной научной конференции «Современные проблемы фундаментальных и прикладных наук». Часть 1.* – М.: МФТИ. – 2007. – С. 31-33.
9. Горшков Т.Ю. Модель логики и методы доказательства в семантической сети // Труды 48-й научной конференции «Современные проблемы фундаментальных и прикладных наук». Часть1. – М.: МФТИ. – 2005. – С. 31-33.