МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

На правах рукописи

Аль-Джабери Рамзи Хамид

Улучшение эффективности защиты корпоративных телекоммуникационных компьютерных сетей Йемена в условиях низкой определенности

Специальность 05.12.13 – Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель - профессор,
д. т. н. Галкин А.П.

г. Владимир-2015 г.

Содержание

Список сокращений

WAN- Глобальная вычислительная сеть

АБС - автоматическая биллинговая система

АКС - аппаратура конфиденциальной связи

АШКУ - абонентское шифрующее и кодирующее устройство

БД - база данных

БЗ - база знаний

ГПСПИ - генератор псевдослучайной последовательности импульсов

ЗИ – защита информации

ЗМ - защитные мероприятия

ЗУ – запоминающее устройство

ИКТ - информационные и коммуникационные технологии

ИП - информационные потоки

ИСППР - интеллектуальная система поддержки принятия решений

КИТС - корпоративная информационно-телекоммуникационная сеть

КПИ - коэффициент потерь информации

КС - корпоративные сети

КУ - канал утечки

ЛВС (LAN) - локальная вычислительная сеть

МД – множественный доступ

НСД - несанкционированный доступ

ОС - операционная система

ПИП - повторные информационные потоки

ПЭВМ - персональная ЭВМ (ПК)

СА - сетевые аномалии

СЗИ - система защиты информации

СМД - случайный множественный доступ

СОА (IDS) - систем обнаружения атак или вторжений

СОД - систем обработки данных

СППР - система поддержки принятия решений

СУБД - систе́ма управле́ния ба́зами да́нных

ТГУЙ (ТГУ) - Тайзкий государственный университет Йемена

ТКУИ - технический канал утечки информации

ТС - телекоммуникационная система

ЭС - экспертные системы

Введение

В настоящее время в Йемене продолжают широко применяться компьютерные сети, которые привели к бурному распространению глобальных информационных сетей, открывающих принципиально новые возможности информационного обмена и расцвета телекоммуникаций. Вопросами улучшения защиты сетей в Йемене уже занимались наши предшественники, Аль Муриш и Аль-Агбари, в 2007-2009 гг. [1,8,17]. В настоящее время произошло много изменений и наша задача учесть эти изменения.

В то же время, в телекоммуникациях Йемена, как и в других странах, существует угрозы использования различных приемов создания мешающих воздействий [2,7-9,85,86].

Могут создаваться опасности для людей или наступления других неадекватных последствий. Это относится к опасным угрозам государственной и общественной безопасности и всей страны и отдельных корпоративных сетей.

Перспективным направлением обеспечения работоспособности компьютерных сетей в экстремальных условиях Йемена, является разработка адаптивных отказоустойчивых систем в информационном смысле [7,9].

Корпоративная информационно-телекоммуникационная сеть (КИТС) – называемые вычислительными или компьютерными сетями, являются результатом эволюции двух научно-технических отраслей современной цивилизации - компьютерных и телекоммуникационных технологий.

В КИТС многократно затрудняется задача управления всеми процессами (неопределенность, нечеткость), - а это и есть задача для специалиста-эксперта по сетевому управлению, с применением элементов нечеткой логики[21,23].

Основными потенциально возможными требованиями для эксперта являются (табл. В.1):

Таблица В.1. Требования к эксперту проекта

Требования	Поддержка
Держать в уме всю топологию сети, понять причину и источники изменений, уметь использовать криптографию	Проект, статистика
Знать все оборудование и программное обеспечение, чтобы быстро интерпретировать изменения каких-либо параметров	Проект, администрация, статистика
На нем лежит ответственность за рациональное использование огромных ресурсов. От его работы зависит рентабельность предприятия	администрация, статистика
Когда, генерируется лавина сообщений, в том числе и ошибки, он должен уметь выделить из них самые существенные	Проект, статистика

Известные математические модели, используемые для описания структуры, поведения и управления систем защиты информации (СЗИ), в условиях некорректной постановки задач не дают хорошего результата. Необходима разработка новых, ориентированных на специфику процессов защиты информации методов и средств моделирования.

Стало быть, сложное оборудование КИТС, указывают нам на несоответствие возможностей человека требованиям эффективно ее защищать.

Эти проблемы делают неэффективным применение традиционных математических методов, в том числе методов математической статистики и теории вероятностей, а также классических методов оптимизации для решения прикладных задач защита информации в КИТС и требуют использования нечеткой логики, а в определенных случаях. применение криптографии.

Актуальность работы связана с необходимостью:

- использовать и обрабатывать качественную экспертную информацию из-за сложности процесса принятия решений, отсутствия математического аппарата, а это приводит к тому, что при оценке и выборе альтернатив возможно легко ошибиться.

- исследование применения нечеткой логики к задаче идентификации при запросах доступа к ресурсам, представляется одним из способов, позволяющих избавиться от этих недостатков.

При экспертной исходной информации и внедрении интеллектуальной системы поддержки принятия решения ИСППР для управления и диагностики состояния современной КИТС следует считать перспективным направлением разработки методики принятия решений.

Высокий уровень интеллектуализации системы и введение криптографии позволит снизить нагрузку на специалистов по управлению КИТС (сетевых администраторов), повысит эффективность их действий, увеличит надежность функционирования сети и снизит экономические риски для предприятий Йемена.

Имеется достаточно большое число структур и программных продуктов, для осуществления информационного обеспечения процессов телекоммуникационного обмена. Однако большая их часть не удовлетворяет критериям, предъявляемым к ним с точки зрения защиты от несанкционированного доступа к информации, которая может быть эффективно реализована только в условиях качественных каналов связи. Это условие выполняется еще далеко не во всех даже центральных районах, не говоря уже о периферии в Йемене (см. приложения).

Одной из первых работ посвященной этой тематике для Йемена была диссертация Аль - Муриша Мохаммеда [17] и его работы[8], 6 лет назад. С тех пор существенно изменилась технологическая база в стране, изменились КИТС. Мы рассматриваем эти проблемы уже с современных позиций и предлагаем конкретные решения, подкрепленные внедрением в сетях Йемена.

Объект исследования - корпоративные информационно-

телекоммуникационные сети, защита которых осуществляется в условиях неполной и нечеткой(низкой определенностью) информации о сетевых процессах.

Предметом исследования является разработка методик и алгоритмов обеспечения защиты информации КИТС Йемена.

Цель диссертационной работы - решение научно-технической задачи, связанной с разработка интеллектуальной СППР на базе комплексного подхода к проблеме управления информационной безопасностью и защиты информации КИТС от несанкционированного вмешательства в процесс функционирования КИТС при низкой определенности, в том числе и с применением криптографии.

Для достижения указанной в диссертации цели требуется сформулировать и решить следующие **задачи**:

1. Рассмотреть применения методов нечеткой логики к задаче по защите информации в КИТС Йемена.

2.Указать состояние проблемы управления информационной безопасностью в КИТС и выявить пути ее решения применительно к особенностям Йемена.

3.Разработать методики нечеткой идентификации, к задаче обнаружения проникновений при доступе к ресурсам КИТС.

4. Разработать программы, позволяющие реализовать интеллектуальные системы поддержки принятия решений в задачах по защите информации в КИТС, с использованием нечетких моделей.

5. Предложить подход использования криптографии в КИТС.

Методы исследования основаны на элементах нечеткой логики, дискретной математики, теории вероятностей, теории системного анализа и методах криптографии.

Научная новизна работы заключается в том, что:

1. Предложена методика управления информационной безопасностью КИТС в условиях атак злоумышленников, использующая интеллектуальные нечеткие модели.

2. Разработана методика нечеткой идентификации, к задаче обнаружения при запросах доступа к ресурсам КИТС Йемена.

3. Разработаны методики и программы, позволяющие реализовать интеллектуальные системы поддержки принятия решений в задачах по защите информации в КИТС, с использованием нечетких моделей.

4. Разработана методика использования криптографии для информационной защиты КИТС Йемена.

Практическая значимость работы заключается в том, что:

1. Разработанные и предложенные модели и алгоритмы могут быть использованы при разработке, эксплуатации и реконструкции как современных, так и устаревших КИТС Йемена.

2. Алгоритмы и методики доведены до рабочих программ и позволяют решать достаточно широкий круг научно-технических задач и позволяют сократить время проектирования в 3 раза.

3. Разработана конкретная модель действий злоумышленника в защищаемой КИТС, позволяющая оценивать качество ее функционирования системы, с повышением достоверности на 70%.

4. Разработана методика использования криптографии в КИТС Йемена.

Основные положения, выносимые на защиту:

1. Обеспечение требования безопасного функционирования КИТС в условиях атак злоумышленников на информационные ресурсы и процессы, что обосновывает применение нечеткой логики.

2. Разработка принципов функционирования и технологии создания комплексных интеллектуальных систем поддержки принятия решения, основанных на экспертных знаниях о КИТС с учетом особенностей Йемена.

3. Применения криптографии в КИТС с рациональным выбором ключей применительно к Йемену.

Достоверность научных положений, выводов и практических результатов и рекомендаций подтверждена корректным обоснованием и анализом концептуальных и математических моделей рассматриваемых способов управления информационной безопасностью и защитой информации в КИТС; наглядной технической интерпретацией моделей; данными экспериментальных исследований.

Результаты внедрения работы. Основные результаты внедрены в Таиз государственном университете (ТГУ), в Йемене, что подтверждено соответствующими документами.

Апробация работы. Основные научные и практические результаты работы докладывались и обсуждались на 4-х международных конференциях: 10-й международной научно технической конференции (НТК) «Перспективные технологии в средствах передачи информации», г. Владимир, 2013г.; 10,11-й международной научно-технической конференции «Физика и радиоэлектроника в медицине и экологии» (ФРЭМЭ), г. Владимир, 2012,2014гг.; Международной конференции НПК «Управление инновационными процессами развития региона», г. Владимир, 2012 г. межрег. науч. конф. «Инновационное развитие экономики – основа устойчивого развития территориального комплекса», на 2-м международном экономическом конгрессе,г. Владимир- г. Суздаль- г. Москва,2013.

Публикации. Основное содержание работы изложено в 12-ти статьях и трудах НТК (из них 3 из списка ВАК), в отчетах Госбюджетных НИР кафедры радиотехники и радиосистем №118 (2012-2014гг.). На международных научно-технических конференциях и семинарах сделано 5 докладов и сообщений.

Глава 1. Защита корпоративных информационно-телекоммуникационных сетей в йемене и трудности в ее решении

Сейчас состояние в Йемене характеризуется конвергенцией компьютерных и телекоммуникационных сетей (телефонных, радио, телевизионных сетей). Главный ресурс для них – информация, которую, конечно, надо защищить всемерно [28]. Все это особенно важно для Йемена, где это находится в стадии становления. Телекоммуникация и сетевые технология являются той движущей силой, которая обеспечивает прогресс всей мировой цивилизации.

Корпоративная информационно-телекоммуникационная сеть (КИТС) – называемые также вычислительными или компьютерными сетями, являются результатом эволюции двух научно-технических отраслей современной цивилизации - компьютерных и телекоммуникационных технологий [8,17,72,92].

Сложности при этом приводим в табл.1.1.

Таблица 1.1. Трудности сетевых защит в Йемене

Трудности	**особенности**	**Уровень решения**
Плохая изученность	количественная оценка ценности информации не дает возможности оценки и обоснования необходимых затрат на построение систем защиты информационных и телекоммуникационных систем	Статистика, Правительство
растущие затраты	угрозы безопасности информации КИТС и информационным технологиям [60,83]	администрация, заказчик
управление	В корпоративных сетях (КС) на	Статистика,

основано	наблюдении за сетью и сборе информации	проект
информационная безопасность	Проблема обеспечения является центральной для корпоративных сетей	администрация, заказчик
Обеспечение безопасности КС	защиту всех компонентов КС - аппаратных средств, программного обеспечения, данных и персонала; противодействия любому несанкционированному вторжению в процесс функционирования КС, а также попыткам модификации, хищения, вывода из строя или разрушения ее компонентов	администрация, заказчик, проект
управления всеми процессами в КИТС	усложняется задача трактовки результатов наблюдения - это задача для специалиста-эксперта по сетевому управлению [76]	Статистика, заказчик, проект
Известные математические модели не дают желаемого результата	в условиях некорректной постановки задач	Статистика, заказчик

Сложность процесса принятия решений, отсутствие математического аппарата приводят к тому, что просто необходимо использовать качественную экспертную информацию (применение элементов нечеткой логики).

Поэтому необходима разработка новых, ориентированных на специфику процессов защиты информации методов и средств моделирования, которым мы и посвящаем эту работу.

1.1. Классификационные признаки корпоративных сетей в Йемене

Сеть объединяет не только структурные подразделения сети, но и их региональные представительства (корпоративная информационно-телекоммуникационная сеть регионального представительства Йемена (на рис.1.1). КИТС представляет собой сложную систему (имеет дополнительные специальные средства управления) взаимосвязанных и согласованно функционирующих программных и аппаратных комплексов, к которым относятся [44-47]: рабочие станции, большие количество коммуникационного оборудования, операционные системы, сетевые приложения.

Сегодня эти КИТС стали активно внедряться в образовательные структуры в связи с массовым распространением Интернета и его доступностью. Корпоративные сети строятся на основе Интернета в отличие от банковских систем, поэтому проблемы информационной безопасности сегодня более актуальны и менее изучены именно для них[96]. Покажем это в табл.1.1.1.

Таблица 1.1.1. Классификация сетей Йемена

КИТС	**предназначенность**	**Применимость**
сети доступа	концентрации информационных потоков поступающих по каналам связи от оборудования пользователей (обыкновенных и удаленных) и передачи в узлы магистральной сети	ТВ, радио, СДО, Интернет, КИТС, телефон
Магистрали,	сети доступа, обеспечиваюшие передачу трафика между ними по высокоскоростным каналам	СДО, Интернет, КИТС

информационные центры	информационные ресурсы сети, с помощью которых осуществляется обслуживание пользователей	Интернет, КИТС, телефон

Магистральная сеть строятся на основе маршрутизаторов, многофункциональных коммутаторов и другого коммуникационного оборудования, в том числе и с применением криптографии и других сетевых инноваций.

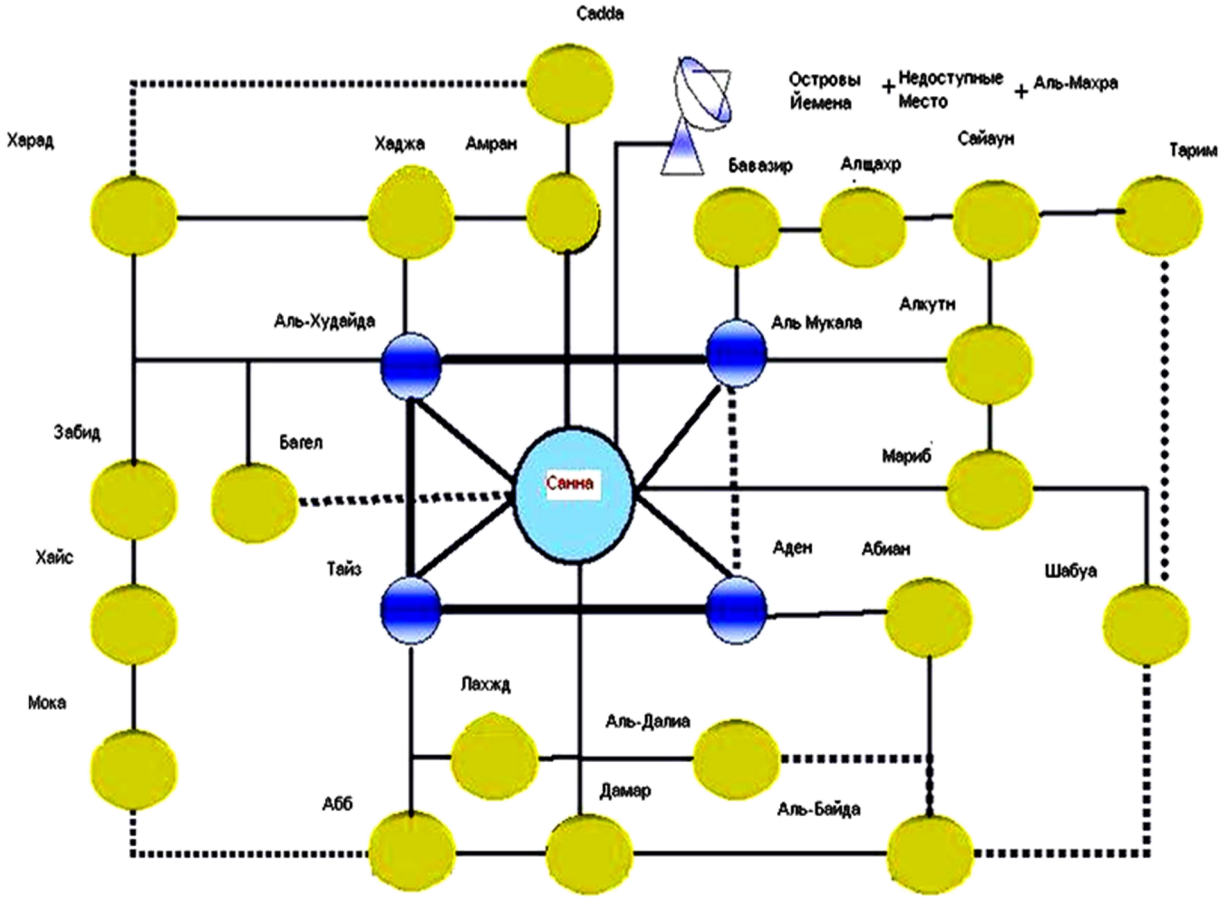


Рис.1.1. Корпоративная информационно-телекоммуникационная сеть Йемена

В соответствии с введенным определением КИТС и ее состав в общем случае образуют следующие функциональные элементы [5,14] (табл.1.1.2):

Таблица 1.1.2. Состав КИТС применительно к Йемену

элемент	**создание**	**ответственность**
абоненты	Проект, заказчик	администрация, Правительство
серверы	Проект	администрация
телекоммуникации	Проект, заказчик, Правительство	администрация, Правительство
Телеслужбы	Проект, заказчик	Правительство
управления эффективностью	Проект, заказчик	администрация
управления безопасностью	Проект, заказчик	администрация
обеспечения надежности корпоративной сети [58]	Проект, заказчик, Правительство	администрация, Правительство
диагностика и контроль [66]	Проект, заказчик	администрация
Система эксплуатации	Проект, заказчик	администрация

Информационная безопасность в КИТС в Йемене имеет свои особенности, которые мы сведем в табл.1.1.3[43], они существенно сильнее, разнообразны и острее, чем в других странах [61-66,97]:

Таблица 1.1.3. Особенности КИТС Йемена

Особенности	**Уровень**
КИТС основана на концепции «Скудного финансирования» (оборудование, кадры, нелицензионное программное обеспечение, малые скорости и память) [21, 23,24]	Правительство, заказчик
КИТС не имеют стратегических целей развития. Это значит, что топология сетей, их техническое и программное обеспечение рассматриваются с позиций текущих задач	Правительство, администрация,
КИТС обеспечивают и образовательную и научную деятельности и решение задачи управления	Правительство, администрация,

образовательным и научным процессами (АСУ «Студент», АСУ «Кадры», АСУ «Учебный процесс», АСУ «Библиотека», АСУ «НИР» АСУ «Бухгалтерия» и т.д.)	
КИТС гетерогенны как по оборудованию, так и по программному обеспечению в связи с тем, создавались в течение длительного периода времени для разных задач	администрация, проект
Планы комплексной информационной безопасности отсутствуют или не соответствуют современным требованиям	Правительство, администрация, проект, заказчик

Это можно хорошо увидеть при рассмотрении мобильности в режиме коммутации каналов, что очень характерно для сетей Йемена (табл.1.1.4).

Таблица 1.1.4.Управление мобильностью в режиме коммутации каналов и в режиме коммутации пакетов

Коммутация каналов	Коммутация пакетов
Управление мобильностью (MM) • Регистрация o Индикация открепления IMSI o Обновление местоположения • Обеспечение защиты o Аутентификация o Идентификация o Перераспределение TMSI • Управление соединением o Услуга CM o Прерывание Смешанный o Информация/статус MM	**Управление мобильностью GPRS (GMM)** • Прикрепление и открепление • Перераспределение P-TMSI • Аутентификация и шифрование • Запрос идентификации/ответ • Обновление зоны маршрутизации • Состояние/информация GMM • Запрос/Принятие/Отказ в предоставлении услуги
Управление соединениями (CC)	**Управление сеансом GPRS (SM)**

в режиме коммутации каналов • Выполнение соединения o Уведомление o Обработка/подтверждение вызова o Соединение/подтверждение соединения o Ход выполнения o Настройка • Информационная фаза соединения o Модификация o Информация пользователя o Очистка соединения o Разъединение o Освобождение/завершение освобождения • Управление дополнительными услугами o Оборудование o Удержание o Поиск • Смешанные функции o Управление перегрузкой o Уведомление o Обработка DTMF o Статус	• Активизация контекста протокола пакетных данных (PDP) • Активизация контекста вторичного PDP • Запрос активизации контекста PDP • Модификация запроса контекста PDP • Деактивизация контекста PDP • Статус SM

Организация и развитие корпоративной сети на примере высшего учебного заведения Йемена. В целом информационная система вуза представляет собой сложную систему, состоящую из нескольких

взаимодействующих уровней: корпоративная сеть, сетевая операционная система, система управления базами данных (СУБД), сервисы Интернет, приложения пользователей. В высших учебных заведениях в настоящее время широко используются современные информационные технологии, как в учебном процессе, так и в системе управления[10,41]. Последнее мы в основном и рассмотрим.

Корпоративная сеть (КС) [45] является фундаментом построения информационной системы вуза. От качества ее работы всецело зависит эффективное функционирование всей системы.

В Тайзком государственном университете Йемена (ТГУЙ, ТГУ) была создана и непрерывно совершенствуется КИТС, состоящая из компьютерной и телекоммуникационной сетей [96]. В ней мы и внедряли наши разработки. Общая структурная схема КС ТГУЙ представлена на рис.1.2.

Компьютерная сеть университета насчитывает около 1500 рабочих мест, среди которых около 750 активных компьютеров.

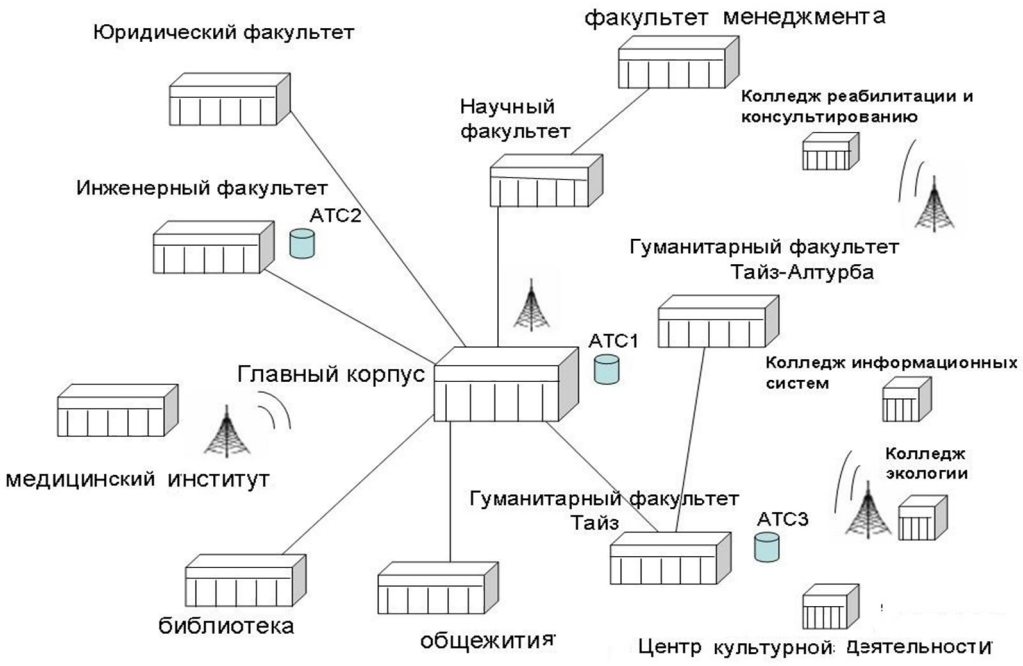


Рис.1.2. Структурная схема корпоративной сети ТГУ

Кабельная система университета включает в себя следующие подсистемы (табл.1.1.4):

Таблица 1.1.4. Кабельная система ТГУ

система	**ответственность**
подсистема пользователя	Администратор КИТС, пользователь
административная подсистема	Администратор КИТС, проект
внешняя подсистема	Администратор КИТС, проект,
горизонтальная подсистема	Администратор КИТС
вертикальная подсистема	Администратор КИТС, пользователь

Посредством указанных подсистем в университете обеспечена взаимосвязь всех учебных корпусов университета и общежитий. Центром данной магистрали является главный учебный корпус, где магистраль <<стянута в точку >> на внутренней шине головного о коммутатора с производительностью 32 Гбит/с.

Центральной административной подсистемой является подсистема главного учебного корпуса.

Опорная магистраль организована между всеми учебными корпусами университета в дуплексном режиме на скорости 100 Мбит/с.

Все подсистемы пользователя подключены к компьютерной сети на скорости 100 Мбит/с.

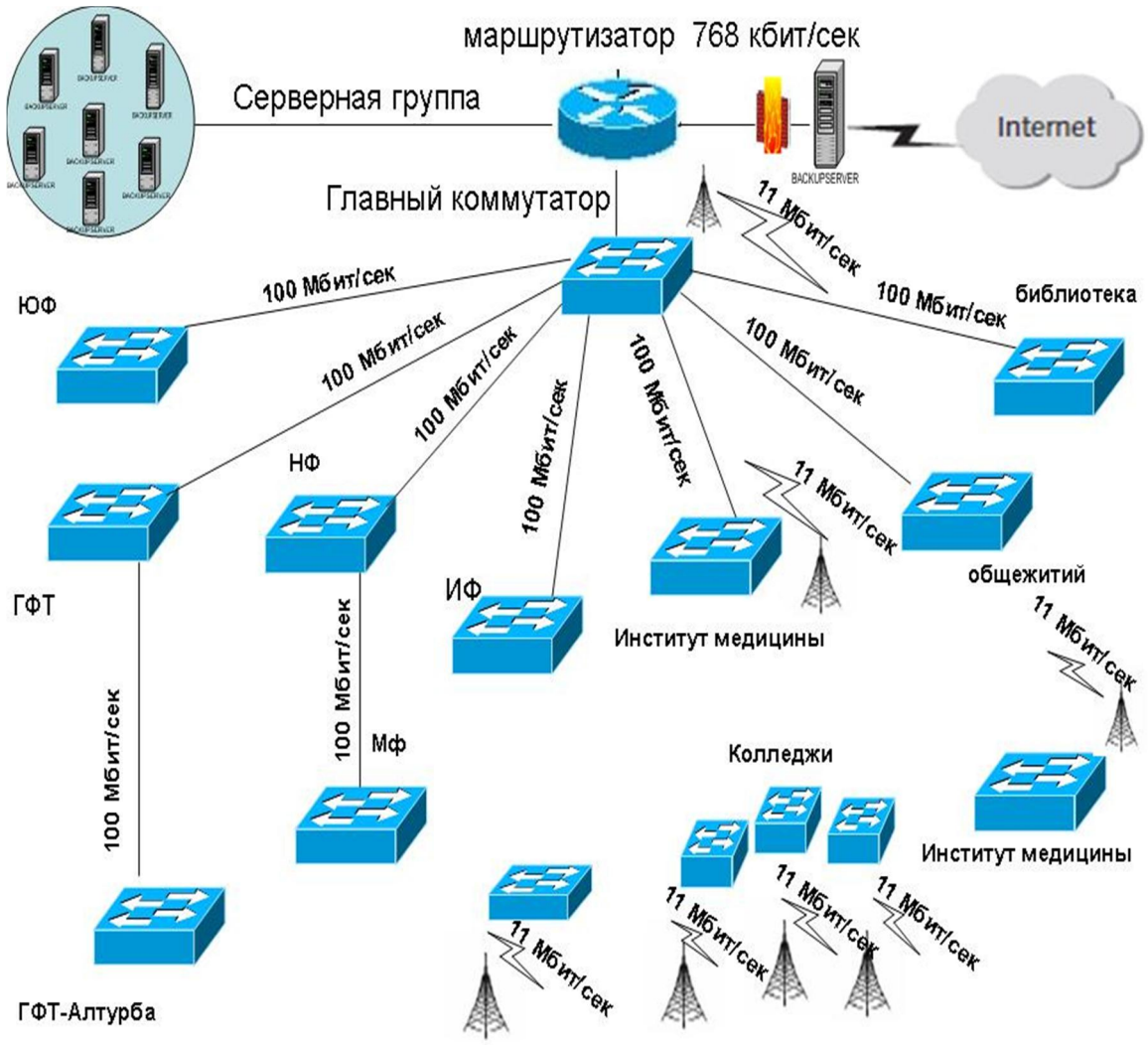


Рис.1.3. Система активного оборудования ТГУ

4900, 4400,4200, 3300, P8500. Управление данной системой осуществляется посредством Web/SNMP управления, а также посредством интеллектуальных модулей, встроенных в оборудование.

В данной модели компьютерной сети логический и физический центр компьютерной сети находятся в одном месте, что позволяет равномерно распределить загрузку сетевых сегментов и обеспечить централизованное управление всей серверной системой.

Система обеспечена независимым бесперебойным питанием.

Серверная группа располагается в главной административной подсистеме главного учебного корпуса и является логическим центром компьютерной сети университета (рис.1.4).

В серверную группу входят сервера следующего назначения:

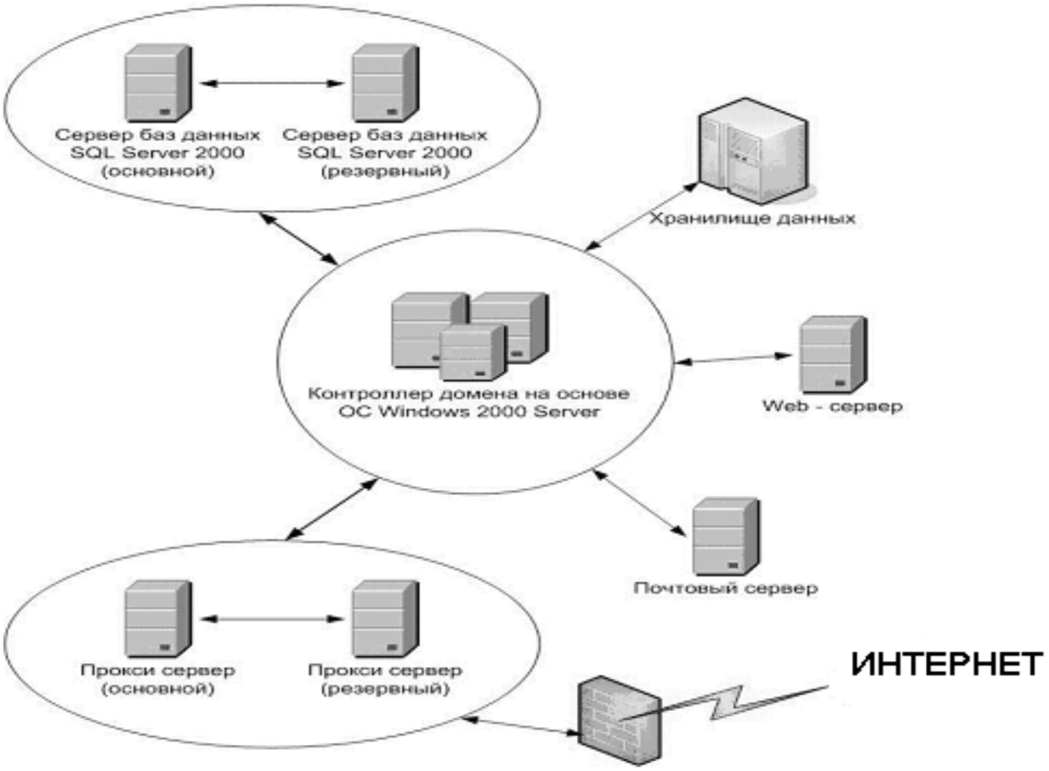


Рис.1.4. Серверная группа

1) контроллер домена – два сервера (основной и дополнительный контроллеры);

2) сервера баз данных –два сервера (основной и резервный);

3) сервера доступа в Интернет-FireWall и Proxy Server, выполнены на основе операционной системы Linux– два сервера (основной и резервный);

4) почтовый сервер – выполнен на основе операционной системы Linux (CommuniGate) с системой защиты от вирусов и спама – один сервер;

5) weЬ-сервер – выполнен на основе операционной системы Windows (IIS 5.0) один сервер;

б) система хранения данных – выполнена на основе специального оборудования фирмы RaidTec SNAZ (хранилище данных)

Телекоммуникационная сеть университета состоит из следующих подсетеи:

- учрежденческая телефонная сеть;
- сеть доступа в глобальную сеть Интернет;
- сеть оповещения гражданской обороны и пожарной безопасности.

- Также заслуживает внимания внедрение 1Р-телефонии [14] для внутренних абонентов университета.

В частности, использование технологий Wi-Fi позволит значительно упростить создание компьютерных сетей в студенческих общежитиях, так как в этом случае отпадает необходимость прокладки кабелей в жилые комнаты.

1.2. Анализ угроз информационной безопасности в КИТС и основные мероприятия по их предотвращению

Все угрозы информационной безопасности (ИБ) можно классифицировать по нескольким критериям [67-71] (табл.1.2.1.):

Таблица 1.2.1. Критерии ИБ в Йемене

критерии	**обеспечение**
аспект ИБ (доступность, целостность, конфиденциальность)	Правительство, заказчик
компонентам ИС (программное обеспечение, аппаратное обеспечение, инфраструктура, каналы связи, пользователи)	проект, администрация, заказчик
осуществления (случайные/преднамеренные действия природного/техногенного характера)	администрация, заказчик
расположение источника угроз (внутри/вне рассматриваемой ИС)	проект, заказчик

Рассмотрим классификацию угроз по компонентам ИС, а также обозначим способы защиты от возможных угроз [52,101-104] на табл.1.2.2.

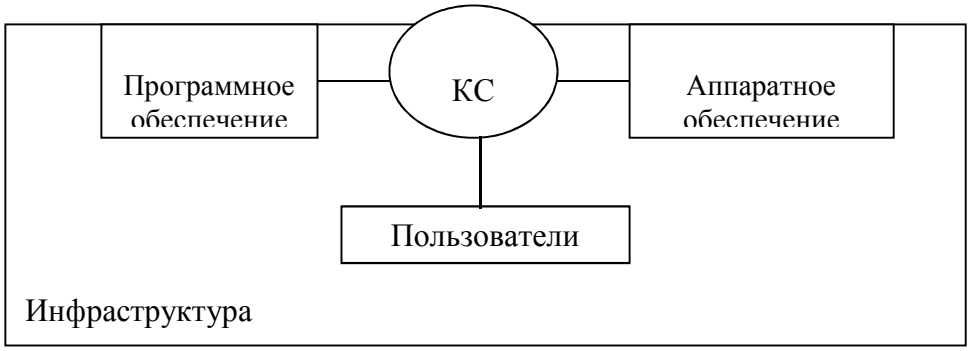


Таблица 1.2.2.

ответственность	**Вид угрозы**	**Способы защиты**
администрация, служба безопасности, тьюторы	***1.Угрозы со стороны пользователей*** – непреднамеренная (до 65% всех потерь) – неумение или отказ работы с системой – преднамеренная («обиженные сотрудники») – ошибки администрирования	1. обучение сотрудников, 2. введение пропускного режима и его соблюдение, 3. удаление учетных данных после увольнения сотрудника, 4. регулярная смена паролей 5.разграничение полномочий между сотрудниками, 6. соблюдение правил работы с конфиденциальной информацией
Правительство, администрация, служба безопасности, тьюторы	***2. Угрозы со стороны программного обеспечения***[26] – логические ошибки ПО – уязвимость ПО – вредоносное ПО	1. покупка и использование лицензионного программного обеспечения со встроенной защитой, 2. использование антивирусных программ, 3. использование сетевых экранов, 4. отслеживание уязвимостей и своевременное их устранение
администрация, служба безопасности	*3.* ***Угрозы со стороны аппаратного обеспечения***[27] – разрушение или отказ	1. использование АО со встроенными средствами защиты, 2. бесперебойное питание,

	АО – перебои напряжения	защита от скачков напряжения, 3. ремонт только в сертифицированных сервисных центрах, 4. антивандальные корпуса
администрация, служба безопасности	*4.* ***Угрозы со стороны инфраструктуры***[23-24] – пожары, наводнения, стихийные бедствия, – выход из строя систем кондиционирования, охлаждения, отопления – нарушение физических границ инфраструктуры	1. защита помещений (заборы, охрана и т.п.), 2. противопожарные системы, 3. системы охлаждения и вентиляции, 4. работа с сертифицированными охранными предприятиями
администрация, служба безопасности	***5. Угрозы со стороны КС***[4,52] – разрывы КС – искажение при передаче в КС – использование общедоступных КС	1. шифрование при передаче в «общедоступных» КС, 2. передача с избыточным копированием(дублирование), 3. использование проверки контрольных сумм, 4. физическая защита КС

Эти угрозы - общие для всех типов КИТС, но понятие «угроза» в разных ситуациях может трактоваться по-разному [30-36]. Показательно, что сайт Правительства Йемена - общедоступен, но несанкционированный доступ к этой информации, повлекший ее изменение или удаление- угроза.

1.3. Система обнаружения атак или вторжений и нарушений в корпоративной сети

Система обнаружения атак (СОА)- программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет [93-94].

СОА для Йемена[7,98] в виде типовой архитектуры системы выявления атак[85-89] приведена в табл.1.3.1:

Таблица 1.3.1. Архитектура СОА в Йемене

Архитектура	**Обеспечение**
сенсорная подсистема, предназначенная для сбора	Проект, заказчик,
событий, связанных с безопасностью защищаемой системы	администрация
подсистема анализа, предназначенная для выявления атак и подозрительных действий на основе данных сенсоров	администрация
хранилище, обеспечивающее накопление первичных событий и результатов анализа	Проект, администрация
консоль управления, позволяющая конфигурировать СОА, наблюдать за состоянием защищаемой системы и СОА, просматривать выявленные подсистемой анализа инциденты	Проект, заказчик, администрация

Система обнаружения выполняют ряд функций [57,100] (табл.1.3.2):

Таблица 1.3.2. Функции СОА

Функции	**действие**	**Ответственность**
анализ пользовательской и системной активности	Мониторинг	проект, статистика, заказчик

системная конфигурация	Аудит уязвимостей	Администрация, заказчик
целостность системных файлов	Контроль файлов данных	проект, заказчик
отражение известных атак	Распознавание шаблонов действий	проект, статистика, заказчик
нарушения политики безопасности	распознавание действий пользователя	Администрация, статистика
аномальные действия	Статистический анализ шаблонов	проект, статистика

Польза от СОА и анализа защиты [73-74] (табл.1.3.3):

Таблица 1.3.3. Улучшения от СОА

Действие	**Полезный эффект**	**Уровень**
информационная безопасность	Улучшение целостности частей инфраструктуры	КИТС
системный мониторинг	Улучшение механизмов	администрация
промежуточные воздействия	Рассмотрение действий пользователя начиная от точки входа в систему и заканчивая точкой выхода	администрация, пользователи
Исправление ошибок	Определение ошибок конфигурации системы	КИТС
системные файлы и файлы данных	Распознавание и уведомление об изменении	КИТС, администрация
изменения в программах	Уведомление персонала	администрация,

приведение персонала защиты в готовность	Распознавание специфичных типов атак	КИТС, администрация

В настоящее время существует ряд проблем, с которыми неизбежно сталкиваются организации, развертывающие у себя систему выявления атак, некоторые из них [6,37] (табл. 1.3.4):

Таблица 1.3.4. Проблемы при использовании СОА в Йемене

проблемы	**ответственность**
механизмы аутентификации и идентификации не компенсируются	Проект, администрация,
сетевые протоколы не компенсируются без человеческого участия не исследуются атаки	КИТС администрация, КИТС
большое число ложных срабатываний и несрабатываний из-за невысокой эффективности СОА Йемена	Проект, заказчик
Высокая стоимость коммерческих СОА неадекватно оценивается величина риска и обосновывается стоимость реализации контрмер для руководства из-за отсутствия в организации методики анализа и управления рисками	администрация Проект, администрация, КИТС
осуществление сетевых атак из-за недооценки рисков	Проект, заказчик
Требовательность к ресурсам и порой неудовлетворительная производительность СОА уже на 100 Мбит/с в сетях (пока максимально для Йемена)	Проект, заказчик,

Типовая архитектура системы выявления атак изображена на рис 1.5. На уровне агентов (сенсоров) может выполняться фильтрация данных с целью уменьшения их объема. Это требует от агентов некоторого интеллекта, но зато разгружает остальные компоненты системы [57]. Если в процессе статистического или экспертного анализа выявляется подозрительная

активность, соответствующее сообщение направляется решателю, который определяет, является ли тревога оправданной, и выбирает способ реагирования. Если выбор должен оставаться за человеком, то пусть он сводится к нескольким элементам меню, а не к решению концептуальных проблем.

Рис.1.5. Основные элементы архитектуры систем обнаружения вторжений

1.4. Информационная безопасность КИТС в Йемене

Управление рисками и управление проектами - аналогичны, так как они предназначены для достижения проектом своей цели в рамках заданных ограничений "сроки-бюджет-качество", а это достижимо при хорошей защите от НСД к информации КИТС.

По сложившемуся мнению экспертов в политике защиты должны быть рассмотрены, по крайней мере, следующие аспекты [30,42-43,98] (табл.1.4.1):

Таблица 1.4.1. Аспекты безопасности

Аспекты	**Обеспечение**
физическая безопасность	администрация
конфигурирование и тестирование систем	Проект, заказчик

обучение мерам безопасности	администрация
мониторинг защиты и анализ статистики	администрация
контроль прав доступа	администрация
санкционирование доступа к компьютерным системам, идентификация и аутентификация пользователя	Проект, администрация
безопасность телекоммуникационных сетей	Проект, администрация, заказчик

Внешняя сетевая безопасность подразумевает определение четких границ сети и установку в критических местах межсетевых экранов, для этого используют два типа: внутренние и лежащие на периметре сети организации - там, где происходят внешние соединения [6,82-83].

1.5. Обоснование выбора нечеткой модели представлений знаний

Сложность процесса выбора из большого объема знаний фактов и правил, их структурирование и построение из них базы знаний, заставляет использовать разработку интеллектуальной (экспертной) системы, но при этом существует проблема приобретения и представления экспертных знаний [53,59].

Мы выбрали нечеткие модели, приведенные в [3,22,39], потому что система мониторинга, анализа и диагностики КИТС в Йемене обладает следующими особенностями[1,13,16,53] (табл.1.5.1):

Таблица 1.5.1. Особенности нечетких моделей в Йемене

языки	**особенности**	**Уровень**
на естественном языке в терминах лингвистических переменных[48,51]	эксперты используют как четкие методы, так и логико-лингвистические методы	Проект, администрация, заказчик, статистика

математическими зависимостями	Значительная часть информации может быть получена только в виде экспертных данных или в виде эвристических описаний процессов. Эта информация может быть нечеткой и недостаточно определенной	Проект, администрация, статистика
плохо формализуемый, трудоемкий, дорогостоящий	О причинах сетевых аномалий, связанных с отказами и сбоями в работе оборудования, программного обеспечения, компьютерных нападениях или неправильных действиях пользователей	Проект, администрация, заказчик, статистика
сложно для практического применения	Четкая модель исследуемой системы	Проект, заказчик, статистика
информация может быть нечеткой	недостаточно определенной для того, чтобы быть выраженной математическими зависимостями [9,17-19]	Проект, заказчик, статистика
нечеткий характер [15]	Входные данные системы не являются точными	заказчик, статистика

1.6. Система подержки принятия решений для задач управления КИТС

Система поддержки принятия решений (СППР) [55,95] - это интерактивные автоматизированные системы, помогающие при принятии решения, применять данные и модели с неполной информацией.

Спецификой таких задач являются (табл.1.6.1):

Таблица 1.6.1. Специфика СППР в Йемене

задачи	**специфика**	**ответственность**
строгие алгоритмические методы и модели теории принятия решений	невозможность успешно использовать для решения таких задач	Проект, статистика, администрация
Ограничение по времени	необходимость получения решения в условиях временных ограничений	администрация
необходимость коррекции	введения дополнительной информации в процессе поиска решения	Проект, статистика, активное участие в нём ЛПР (лицо, принимающее решение)
Неопределенность ситуации	присутствие недетерминизма в процессе поиска решений	статистика, администрация
субъективная, эвристическая информация	невозможность получения объективной информации, необходимой для решения	Проект, статистика, администрация

Теоретической основой СППР становится сочетание нормативных методов, искусственного интеллекта и теории систем. Можно прогнозировать более широкое применение неструктурированной информации в СППР.

1.6.1. Модели принятия решений в задачах управления КИТС

Процесс решения задачи принятия решений понимается как оптимальный выбор метода обработки исходных структур из некоторого базового класса методов, которые хранятся в библиотеке моделей задач принятия решений. Конкретные модели ориентированы на соответствие тех

или иных методов принятия решений определенным базовым структурам.

В работах [11] по созданию модели принятия решений предлагается классификация моделей, основанная на ее формальном представлении:

$<t, X, R, A, F, G, D>$,

где:

t – постановка задачи;

X – множество допустимых альтернатив;

R – множество критериев оценки степени достижения поставленных целей;

A – множество шкал измерения по критериям;

F –отображение множества допустимых альтернатив в множество критериальных оценок;

G – система предпочтений решающего элемента;

D – решающее правило, отображающее систему предпочтений.

В основе предложенной модели лежат методы принятия решений, необходимые для решения задач управления КИТС.

Первый компонент модели предназначен для информационно несложных задач, второй – информационно сложных задач. Схемы компонентов приведены на рис. 1.6.1 и 1.6.2. В приведенных схемах в прямоугольниках описаны исходные данные, а в фигурных стрелках – методы обработки исходных данных.

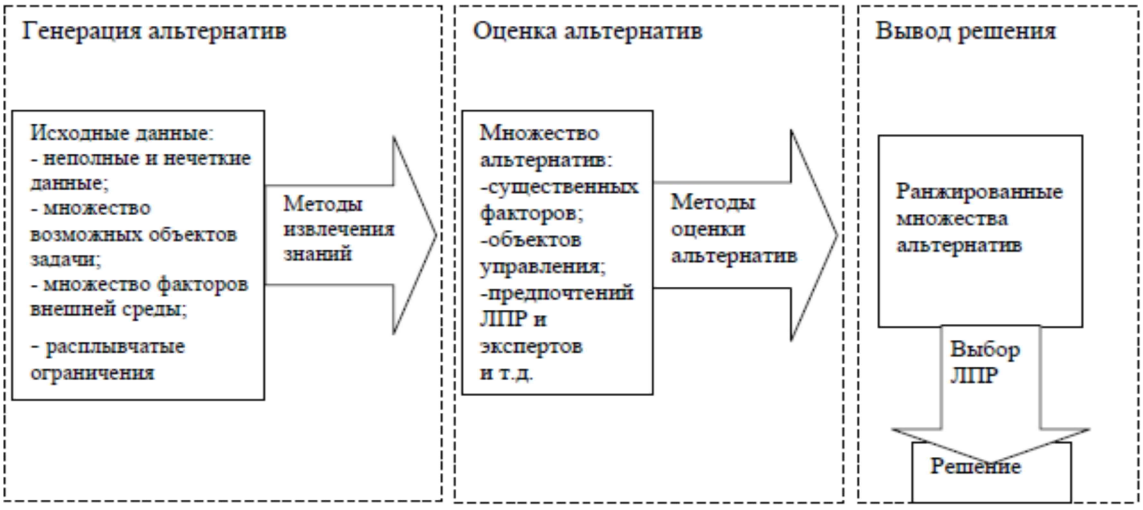


Рис.1.6.1. - Схема принятия решений для информационно несложных задач принятия решений

Рис.1.6.2. - Схема принятия решений для информационно сложных задач принятия решений

Мы предполагаем также разработать методики нечеткой идентификации и нечеткого многокритериального выбора альтернатив, а также элементы криптографии, которые нами разработаны при внедрении в ТГУ [103,104], поскольку идентификация и аутентификация обычно используется при принятии решения, можно ли разрешить доступ к системным ресурсам пользователю или процессу (см. 2-ю и 3-ю главы).

1.6.2. Применения интеллектуальной СППР в задачах управления

Одним из основных соображений, положенных в основу выбора интеллектуальной системы в качестве базы СППР, является то, какой вид практической деятельности может быть реализован с помощью такой системы.

Экспертный анализ направлений управленческой деятельности должностных лиц предприятия Тайзского университета (ТГУ) (Йемен) и форм их поддержки, показывают, что интеллектуальная составляющая занимает ведущее место в обеспечении принятия решений по управлению КИТС.

Основными направлениями применения интеллектуальной СППР для рассматриваемой предметной области могут быть (табл.1.6.2.1):

Таблица 1.6.2.1. Задачи СППР в Йемене

Задачи	**действие**	**обеспечение**
обучение обслуживающего персонала	контроль действий обучаемого, оценка его действий с указанием ошибок, выдача при необходимости методических указаний и пояснений	Администрация
Ремонт оборудования	выполнение ремонтных процедур для восстановления сети	Администрация
отладка	восстановления правильного функ-ционирования сети и оценивание их эффективности	Администрация, проект
диагностика	выдача рекомендаций по устранению нештатных ситуаций в процессе эксплуатации	проект, заказчик
мониторинг работы элементов телекоммуникационн ой сети и сетевых процессов	выбор гипотезы, выполненный с использованием данных измерений и информации, на основе которой делаются умозаключения	проект, заказчик
доступ к системным ресурсам пользователю или процессу	идентификация и аутентификация используется при принятии решения	Администрация
сложные задачи	В некоторых случаях они могут быть объединены между собой	Администрация, проект,заказчик

Выводы по главе 1

1. Показаны особенности и трудности при эксплуатации КИТС в Йемене и необходимость разработки инженерных методик по защите информации и необходимость применения ИСППР в условиях малой определенности.

2. Обоснованы главные проблемы в информационной защите КИТС в Йемене.

3. При управлении сетью надо обеспечивать централизацию информационных ресурсов в КИТС и примененять ИСППР и криптографию.

Глава 2. Методики оценки КИТС Йемена

Проектирование, организация и применение СЗИ фактически связаны с неизвестными событиями в будущем и поэтому всегда содержат элементы неопределенности. Количественная оценка эффективности. В соответствии с современной теорией оценки эффективности систем[17-22], качество любого объекта, в том числе и СЗИ, проявляется лишь в процессе его использования по назначению (целевое функционирование), поэтому наиболее объективным является оценивание по эффективности применения.

Поэтому объективной характеристикой качества СЗИ — степенью ее приспособленности к достижению требуемого уровня безопасности в условиях реального воздействия случайных факторов, может служить только вероятность, характеризующая степень возможностей конкретной СЗИ при заданном комплексе условий.

Приведем возможные подходы к оценке эффективности КИТС в случае проведения защитных мероприятий (табл.2.1-2).

Таблица 2.1. Возможные показатели эффективности средств защиты информации СЗИ

обеспечение	**Требование к СЗИ**	**Вид показателя эффективности СЗИ**
Проект	Наступление или отсутствие события	Вероятность события
Проект, заказчик	Достижение требуемых характеристик	Вероятность достижения результата не ниже требуемого уровня
заказчик	Отклонения от заданных характеристик	Средний квадрат уклонения результата от требуемого знания
Проект, администрация, заказчик	Обеспечение гарантированного уровня характеристик	Квантиль заданного уровня гарантии
Проект, заказчик	Не установлены	1.математическое ожидание результата 2.дисперсия результата

		3.средний риск

Таблица 2.2. Возможные критерии эффективности средств защиты информации СЗИ

Концепция эффективности СЗИ	**Кто проводит**	**Критерии эффективности**
Пригодность	Проект, заказчик	1.приемлемый результат 2.допустимая гарантия 3.допустимый гарантированный результат
Оптимальность	Проект, администрация, заказчик	1.наилучший результат 2. наилучший средний результат 3.наибольшая вероятность гарантии результата 4. наибольший гарантированный результат

2.1. Оценка достоверности функционирования отказоустойчивого запоминающего устройства при информационной защите телекоммуникаций

Уже указано, что одна из особенностей КИТС Йемена – применение малоразрядных итеративных кодов. Важно знать достоверность запоминающих устройств (ЗУ) в этих сетях и суметь выбрать наилучшие параметры для конкретных сетей.

В этом случае[104]:

$$\lambda_i = 1*10^{-9}\ \ 1/ч, (\ p(t) = e^{-10^{-9}*t}). \qquad (2.1.1)$$

Вероятность безотказной работы накопителя по одному выходу равна[98]:

$$p1(t) = p(t)^{6M}. \qquad (2.1.2)$$

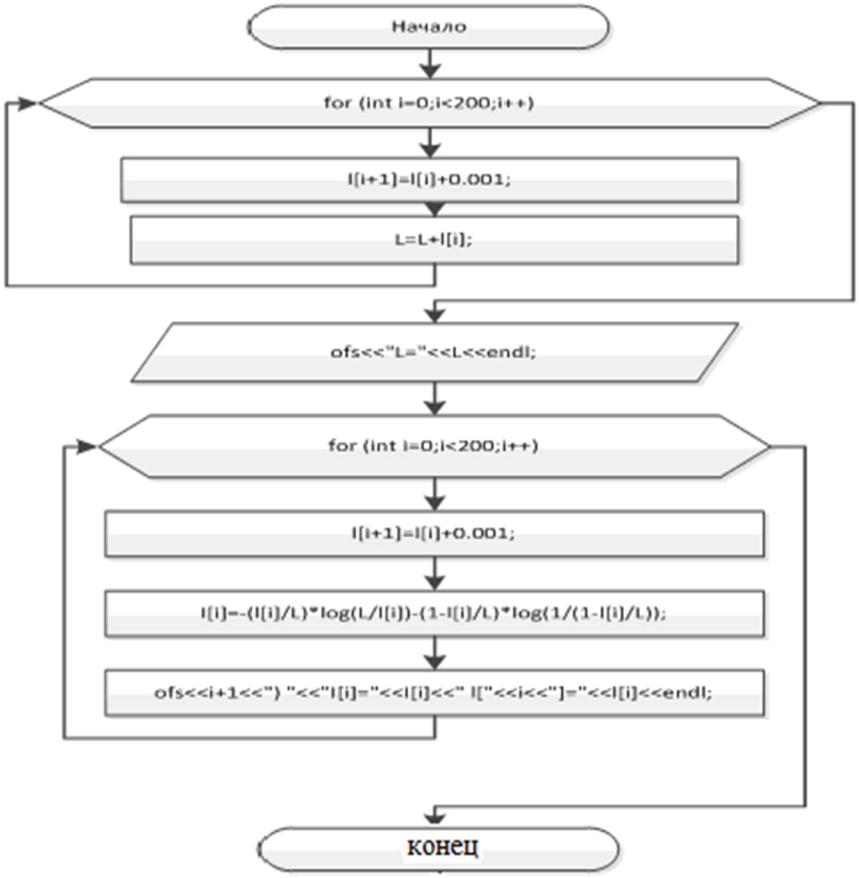
Достоверность функционирования отказоустойчивого ЗУ оценим используя выражение [104]:

$$D(t) = p_{ДЕК}(t)\sum_{i=0}^{k-1} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i + p_{ДЕК}(t)\sum_{i=1}^{n} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i - P_{ДЕК}(t)^2\sum_{i=0}^{k-1} C_n^i p1(t)^{(n-i)}[1-p1(t)]^i * \sum_{i=1}^{n} C_n^i p1(t)^{(n-i)}[1-p1(t)]. \qquad (2.1.3)$$

Проведем оценку влияния кратности исправляемой ошибки аппаратурные затраты и достоверность функционирования устройств памяти при реализации кодирования информации при различных кратностях ошибок[98].

Полученные результаты и зависимости, отображающие достоверности функционирования запоминающего устройства от времени, приведены на рис.2.1.1.

Используя данные, заданные заказчиком, рассчитаем аппаратурные затраты для построения запоминающего устройства с 4-х разрядным кодом, сложность декодирующего устройства (элементов), зависимость достоверности (2.1.3) показана на рис.2.1.1. Для расчетов применяли алгоритм:



Используя выражения (1-3) рассчитаем и проведем оценку достоверности функционирования запоминающего устройства, работающего на основе предлагаемых подходов (рис.2.1.1).

В результате, как это видно из табл.2.1.1 и (2.1.4.) и рис.2.1.1.,

достоверность отказоустойчивых ЗУ улучшается в среднем на 70%.

Таблица 2.1.1. Достоверность ЗУ в КИТС во времени

Ошибки (проникновения)	**2 сут**	**8сут**	**8 отн 2**	**Выигрыш во времени**
Отсутствуют	0,96	0,95	0,99	
Одно проникновение	0,96	0,8	0,83	0,85
Два проникновения	0,96	0,8	0,83	0,84
Три проникновения	0,95	0,8	0,84	0,84
Четыре проникновения	0,9	0,54	0,6	0,6
Пять проникновений	0,87	0,48	0,55	0,56
Шесть проникновений	0,85	0,4	0,47	0,47

$$(0,85+0,84+0,84+0,6+0,56+0,47) / 6 = 0,69 \qquad (2.1.4)$$

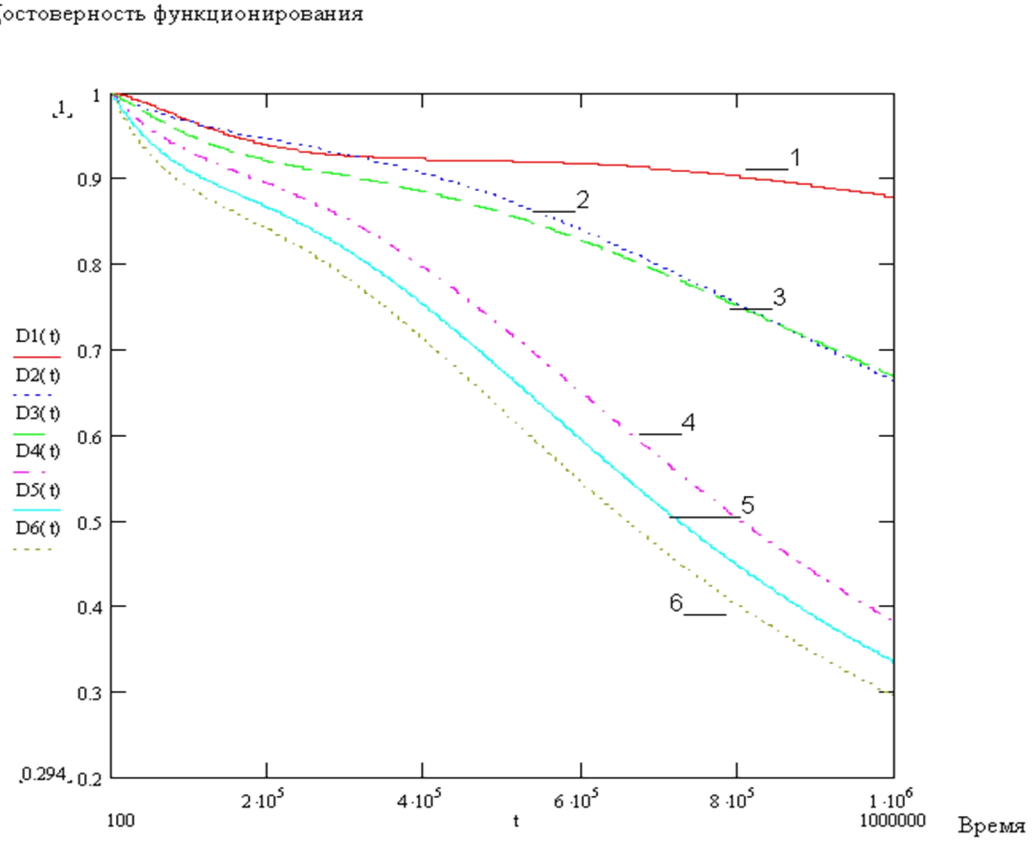


Рис.2.1.1. Выигрыщ в достоверности:1-кратность 0- проникновений; 2- 1- проникновений; 3-2- проникновений; 4- 3- проникновений; 5- 4- проникновений; 6-5- проникновений.

Лучшие характеристики с точки зрения достоверности функционирования имеет устройство, построенное на основе первого метода.

В среднем, как это видно из графика, достоверность выше на 70% чем у других методов(2.1.4.) [104]. Это объясняется использованием минимального количества простейших логических элементов для его построения [98,105]. Однако при этом процент обнаруживаемых и исправляемых ошибок (проникновений) у первого варианта (0- проникновений) – наименьший, а шестого (5- проникновений) – самый большой.

2.2.Системный уровень проектирования защищенных сетей

Разработаем для КИТС Йемена рациональный подход проектирования.Существует множество систем автоматизированного проектирования (САПР), в том числе, и для защищенных сетей (ЗС), призванных облегчить труд разработчика и ускорить процесс проектирования соответствующих объектов. Среди наиболее известных САПР следует выделить Altera, Mental Graphics, Cadence, SolidWorks 97, HP VEE, InTouch, каждая из которых ориентирована на класс задач определенной предметной области. Однако существующие САПР в основном ориентированы на проектировании SoC и не позволяют в полной мере спроектировать системы Network on Chip (NoC).

Приведем классификацию телекоммуникационных систем (ТС) по силовому деструктивному воздействию (СДВ), характерному для Йемена.

Рис.2.2.1. Классификация ТС СДВ по проводным линиям

Рис.2.2.2. Классификация ТС СДВ по эфиру (электромагнитные ТС СДВ)

Мы рассматриваем САПР, предназначенную для автоматизации труда проектировщика систем защиты информации основанных на NoC. При этом учитываем особенности Йемена (использование телефонных каналов в КИТС, малые скорости, малоразрядные коды) (см. приложения) [98]

САПР NoC состоит из различных уровней разработки и верификации СБИС NoC.

Остановимся на самых основных (см. рис.2.2.3).

Рис. 2.2.3. Общий маршрут проектирования

Системный уровень включает два подуровня функциональный и уровень транзакций(табл.2.2.1).

Таблица 2.2.1. Модели архитектуры системы

уровни	особенности	языки
функциональный уровень	создается и верифицируется математическая модель системы в целом	VHDL
уровень транзакций	моделируется архитектура системы с учетом ИСППР	VHDL, C/C++, Verilog, Matlab

Можно, разработав системную модель сложного устройства, довести отдельный его блок до вентильного и даже до топологического уровня и верифицировать системную модель, используя уже готовый блок. В этом случае может выясниться, например, что какие-либо параметры, заложенные в блок на системном уровне, не реализуются, и тогда можно изменить саму систему.

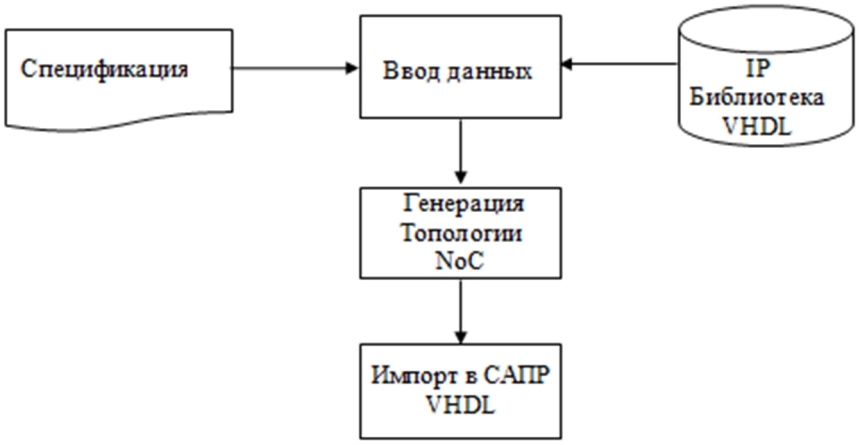


Рис. 2.2.4 Системный уровень

Причем синтезируемые XML структуры, если и превышают по числу вентилей разработанные вручную, то в среднем не более чем на 30%[98].

Для работы с ПЛИС предназначен стыкуемый с Compiler инструмент FPGA Compiler, который включает библиотеки других производителей (Altera, Xilinx, Actel, Atmel, Motorola, Intel, Lattice и т.д).

Рис. 2.2.5. Уровень регистровых передач

По завершении логического синтеза необходимо провести верификацию проекта. Для анализа временных статических характеристик предназначен пакет Prime Time[98]. Это также весьма распространенный на рынке продукт. Он позволяет получить адекватное представление о поведении схемы, проанализировать его в наилучшем и наихудших случаях, обнаружить скрытые ошибки. У этого продукта есть расширение – Prime Time SI, предназначенное для анализа топологии. Оно позволяет отслеживать взаимовлияние проводников.

Рис. 2.2.6. Уровень верификации

Уровень синтеза топологии предназначен для размещения, трассировки и оптимизации топологии.

Рис. 2.2.7. Уровень синтеза топологии

Разработанный нами подход позволил при внедрении в ТГУ (Йемен) сократить время проектирования КИТС в 3 раза (см. приложения).

2.3. Выбор рациональной информационной защиты КИТС Йемена с криптографией

При проектировании защищенных КИТС Йемена возникают проблемы выбора рациональной защиты (и бюджетной и эффективной). Обоснуем и приведем разработанный нами подход, удовлетворяющий этим условиям. Предварительно проведем целевую классификацию. Алгоритмы шифрования с использованием ключей предполагают, что данные не сможет прочитать никто, кто не обладает ключом для их расшифровки. Они могут быть разделены на два класса, в зависимости от того, какая методология криптосистем напрямую поддерживается ими [99,100].

Симметричные алгоритмы. Для шифрования и расшифровки используются одни и те же алгоритмы. Один и тот же секретный ключ используется для шифрования и расшифровки. Этот тип алгоритмов используется как симметричными, так и асимметричными криптосистемами.

Асимметричные алгоритмы используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей [99,100]. Порядок использования систем с симметричными ключами[99]:

Асимметричная (открытая) методология. В этой методологии ключи для шифрования и расшифровки разные, хотя и создаются вместе. Один ключ делается известным всем, а другой держится в тайне. Приведем [99] следующие данные об эквивалентных длинах ключей:

Таблица 2.3.1. Длина ключей

Длина симметричного ключа	Длина открытого ключа	Задание и обеспечение
56 бит	384 бит	пользователь
64 бита	512 бит	пользователь
80 бит	768 бит	администрация

		пользователь
112 бит	1792 бита	администрация пользователь
128 бит	2304 бита	администрация пользователь

Порядок использования систем с асимметричными ключами проверенный и отлаженный нами[99] , в том числе при внедрении в ТГУ, Йемен (см. приложения):

Распространение ключей. Необходимо безопасное распространение ключа[99.100] апробированное нами (табл.2.3.2):

Таблица 2.3.2. Раздача ключей

Процедура	**Комментарии**	**Обеспечение**
Физическая раздача ключей	Используется как симметричными, так и асимметричными криптосистемами.	администрация пользователь
Выдача общего ключа участникам взаимодействия центром выдачи ключей	Может использоваться как симметричными, так и асимметричными криптосистемами. Так как при данном способе каждый пользователь должен каким-то образом безопасно взаимодействовать с центром выдачи ключей в самом начале работы, то это просто еще один случай, когда начальный обмен ключами является проблемой.	администрация пользователь
Предоставление центром сертификации	Предоставление центром сертификации ключей доступа к открытым ключам пользователей и выдача секретных ключей пользователям	администрация

ключей		
Сеть доверия	Используется в асимметричных криптосистемах. Пользователи сами распространяют свои ключи и следят за ключами других пользователей	администрация пользователь
Метод Диффи-Хеллмана	Обмен секретным ключом по незащищенным каналам связи между двумя пользователями, которые до этого не имели общего секретного ключа. Уязвим к атаке "активное вмешательство в соединение".	пользователь

Изучив и апробировав вышеупомянутые методики, в компании ОАО «Ай-Ди Технологии Управления», нами [99,100] был выработан комплексный подход к защите информации в сфере электронного документооборота на платформе EMC Documentum и ее интеграцией с Системой Oracle IRM (в рамках реализации проекта по защите информации модуля «Конфиденциальная тайна» в АСУД (автоматизированная систему управления документооборотом) ОАО «ФСК ЕЭС»), который включает в себя использование криптографической шифрования документов, а так же использование электронного ключа eToken, как персональное средство авторизации, аутентификации и защищённого хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП).

Разработанное решение, позволило осуществить централизованное управление правами на документы, формирование контекстов документов КТ, в рамках которых задаются права доступа (табл.2.3.3):

Таблица 2.3.3. Права доступа

Процессы	**Ответственность**
Динамическое шифрование версий документа КТ	Администрация
Контроль доступа к набору (согласно классификации) или к любому конкретному документу, начала и конца доступа с возможность отмены права доступа в любой момент, того, как именно пользователи АСУД работают с документами на своих рабочих станциях	Администрация
Динамическое шифрование документов КТ при записи в репозитарий АСУД или когда они покидают его	Администрация, пользователь
Шифрование и снятие защиты, при движении документа по жизненному циклу в СЭД	пользователь
Полнотекстовая индексация документов КТ и версий, поиск по зашифрованным документам и версиям	Администрация, пользователь

Экспериментальная часть.

Цель: изучить аутентификации в сети GSM с использованием A3 алгоритма.

Теория:

Шифрование в сети GSM использует механизм запрос / ответ.

1. Мобильная станция (MS) признаки в сеть.

2. Подвижный центр службы коммутации (MSC) просит 5 троек из домашнего местоположения (HLR).

3. Регистр местоположения создает пять троек, использующих алгоритм A8. Эти пять троек содержат:

- 128-битный случайный вызов (RAND)
- 32-битная соответствия подписанный ответ (SRES)
- 64-битный ключ шифрования используется в качестве ключа сеанса (Кс)

4.Главная Регистрация местоположения отправляет центр переключения

мобильных услуг пяти троек.

5.Центр коммутации услуг мобильных посылает случайные вызов для базы передатчика станции (BTS).

6. Базовый передатчик станции отправляет случайный вызов от первой мобильной станции.

7.Мобильная станция получает случайный вызов от передатчика базовой станции и шифрует его с индивидуального ключа аутентификации абонента (Ki) назначенного Мобильной станцией, используя алгоритм A3.

8. Мобильная станция посылает подписанный ответ приемопередатчика базовой станции.

9. Базовая приемопередающая станция посылает подписанный ответ на мобильный Центр услуг коммутации.

10. Мобильные услуги коммутационный центр проверяет подписанный ответ.

11. Мобильная станция генерирует сессионный ключ (Kc), используя алгоритм A8, Индивидуальный ключ аутентификации подписчика (Ki), назначенный для мобильной станции, и случайный вызов, полученных от приемопередатчика базовой станции.

12. Мобильная станция посылает ключ сеанса (Kc) с базовой станции.

13. Подвижный центр службы коммутации посылает сеансовый ключ (Kc) к передатчику базовой станции.

14. Базовая приемопередающая станция получает сеансовый ключ (Kc) от мобильной Услуги коммутационный центр.

15. Базовая приемопередающая станция получает сеансовый ключ (Kc) от мобильной Станции.

16. Базовая приемопередающая станция проверяет сеансовых ключей от мобильной станции и мобильный коммутационный центр услуг.

17. Алгоритм A5 инициализируется сессионным ключом, (Kc) и количество.

18. Канал связи между мобильной станцией и базой могут быть

зашифрованы с использованием алгоритма A5.

Для проверки разработанного нами шифрования разработали алгоритм и программу и провели эксперимент при внедрении для сетей GSM Йемена(см. приложения). Блок -схема приведена на рис.2.3.1, база данных на рис .2.3.2, на рис.2.3.3.логика алгоритма, на рис.2.3.4 интерфейс.

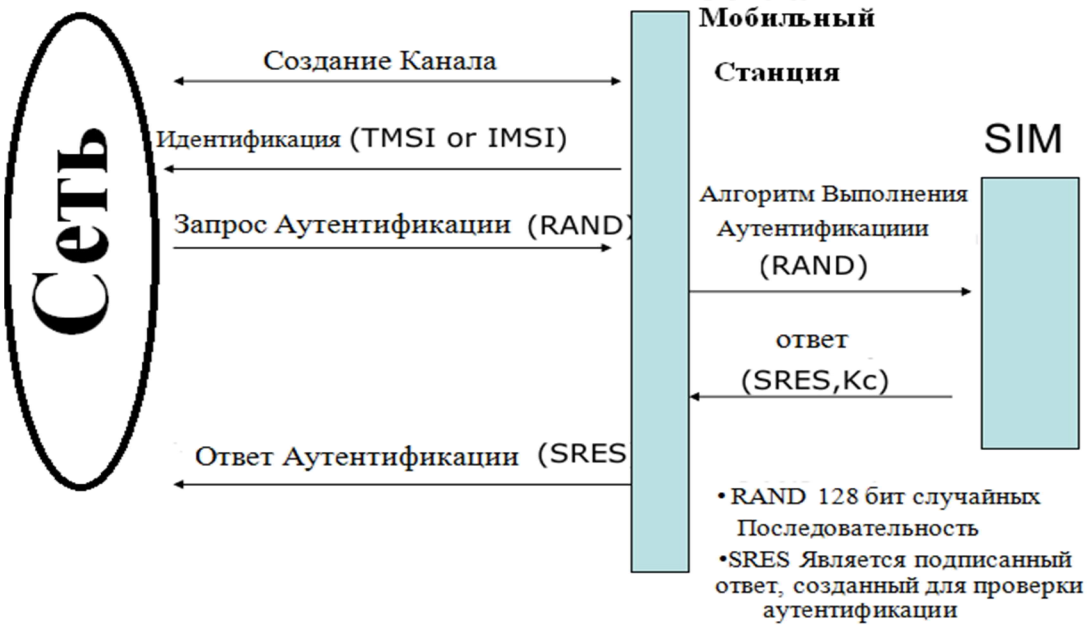


Рис.2.3.1. Блок схема сети GSM в Йемене

HLR :

id	MSISDN	IMSI	Services
1	9029326504	919029311986	CALL,SMS,GPRS
2	9209203394	919209494286	CALL,SMS

VLR :

id	IMSI	MSISDN	TMSI
1	919029311986	9029326504	919029908227
2	919209494286	9209203394	919209529393

AUC :

id	IMSI	Ki
1	919029311986	cd-e7-e1-f3-e7-ed-d3-db-d8-d0-c2-cd-dc-9c-cb-b6
2	919209494286	a2-9a-a6-ff-e2-f0-8a-db-be-aa-e7-a1-a0-c3-89-ad

Рис.2.3.2. База данных

Для реализации наших разработок были разработаны и алгоритм и программа (см. приложение 2.3.1.).

A3 Логика алгоритма:

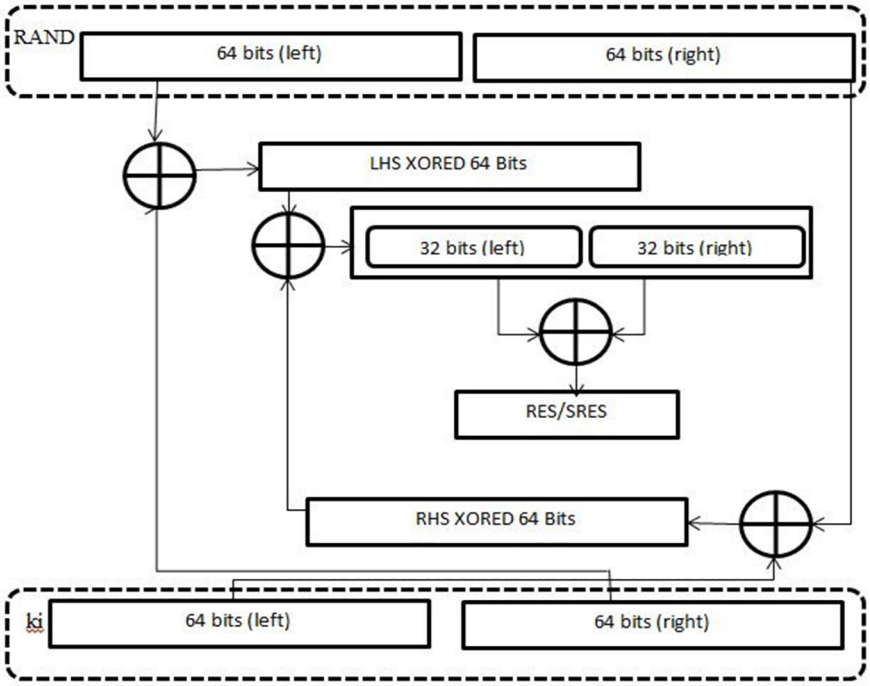


Рис.2.3.3. Логика алгоритма

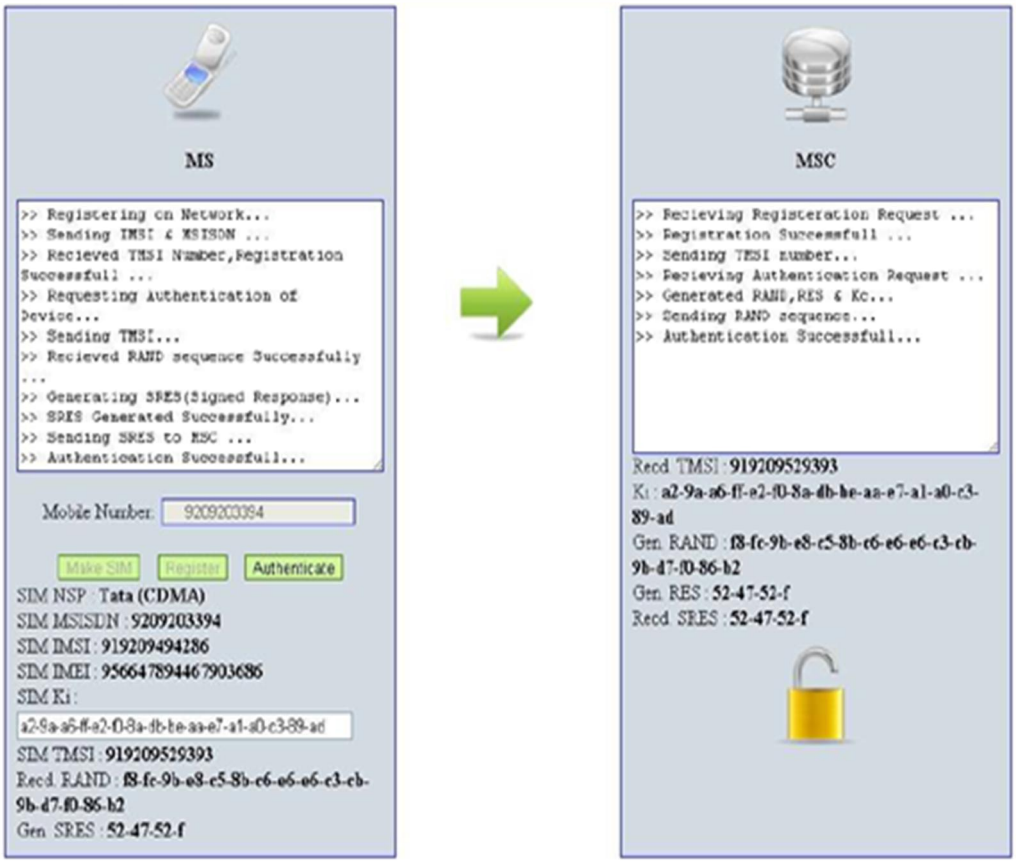


Рис.2.3.4. Графический интерфейс пользователя

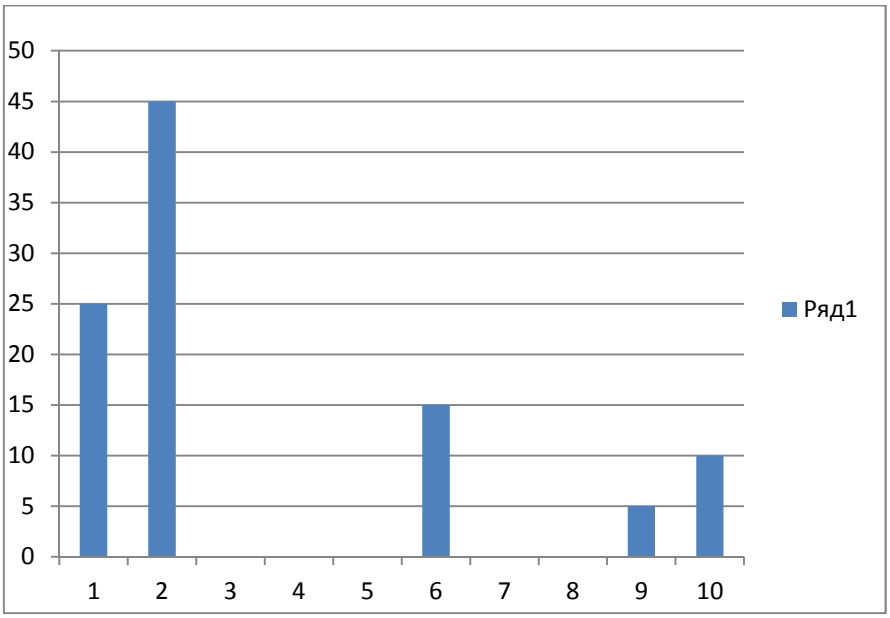


Рис.2.3.5. Зависимость числа проникновений при шифровании в КИТС ТГУ в зависимости от используемой раздачей ключей: 1- Физическая раздача ключей. 2- Выдача общего ключа участникам взаимодействия центром выдачи ключей. 6- Предоставление центром сертификации ключей. 9- Сеть доверия(наш алгоритм). 10- Метод Диффи-Хеллмана.

При проведении эксперимента при внедрении (см. приложения) мы убедились (см. рис.2.3.5), что число проникновений уменьшилось в 4 раза из-за целесообразного подбора ключей и их форматов применительно к КИТС ТГУ по нашим алгоритму и программе.

Выводы по главе 2

1.Проведена оценка достоверности функционирования отказоустойчивого запоминающего устройства при информационной защите телекоммуникаций и обосновано применение малоразрядных кодов в КИТС Йемена, что дало увеличение достоверности на 70%.

2. Разработан алгоритм обеспечения системного уровня проектирования защищенных сетей, что позволило уменьшить время проектирования в 3 раза.

3. Предложен выбор рациональной информационной защиты КИТС Йемена с криптографией, который позволил уменьшить число проникновений в 4 раза.

Глава 3. Разработка множественного доступа в беспроводных когнитивных сетях йемена

В современных телекоммуникационных системах для организации взаимодействия абонентов широко используется множественный доступ, предполагающий коллективное использование канала связи абонентами системы. При этом канал представляет собой общий ресурс, разделение которого необходимо для обеспечения эффективной работы системы связи. Такие сети целесообразны и для Йемена. Рассмотрим и разработаем основные подходы к этой проблеме.

Алгоритмы, предназначенные для такого разделения, носят название алгоритмов множественного доступа и располагаются на специальном подуровне управления доступом к среде (УДС или media access control, MAC) [21-23, 105]. В широкополосном беспроводном доступе есть два вида сред передачи данных: точка-точка и с множественным доступом (точка-многоточек). В среде точка-точка доступ возможен только с двух сторон. Проблемы синхронизации доступа там не столь сложны. Этот вид сред передачи характерен для WAN сетей.

Рассмотрим протоколы для работы с каналами с множественным доступом или, как их еще называют, протоколы со случайным доступом [23, 101,105]. Системы передачи пакетов, использующие механизм случайного множественного доступа (СМД), интенсивно исследуются и находят практическое применение в беспроводных локальных сетях, спутниковых, кабельных и оптических сетях связи.

Широкое распространение беспроводных локальных сетей, применяющих СМД, обусловлено их способностью просто и надежно поддерживать информационный обмен между большим числом пользователей (станций).

На сегодняшний день не существует идеального метода организации

доступа к общему разделяемому каналу передачи данных. С точки зрения доступа к каналу основной проблемой являются возможность возникновения конфликтов доступа к общему ресурсу в том числе и из-за несанкционированных проникновений. Механизм возникновения конфликта заключается в случайной одновременной передаче сигнала по общему разделяемому каналу, что приводит к наложению передаваемых сигналов и к искажению передаваемой информации.

Протокол множественного доступа. Для обеспечения надежной передачи данных в телекоммуникационных сетях связи требуется проведение их математического моделирования с целью определения оптимальных характеристик передающего оборудования и разработки алгоритмов, гарантирующих доставку сообщений за приемлемое время. Эта проблема наиболее актуальна для сетей случайного доступа, в которых наблюдается существенная нерегулярность функционирования в условиях повышенной загрузки канала связи.

Для стабилизации таких сетей связи предлагаются различные модификации протоколов случайного доступа [21-23]. Динамический протокол дает эффективные результаты при стабилизации сетей связи, но технически не реализуемы, так как каждая абонентская станция должна иметь информацию об общем количестве заявок, требующих повторной передачи.

3.1. Разновидности множественного доступа в беспроводных сетях

Одной из проблем управления доступом в беспроводных сетях является эффективное разделение их ресурсов между множеством независимо функционирующих узлов, что предполагает применение на канальном уровне соответствующих методов доступа (МД), к которым предъявляются следующие основные требования: децентрализованное функционирование, высокая пропускная способность, малая задержка передачи, а также ряд дополнительных - передача неоднородного (данные, речь, видео) и приоритетного трафика, использование направленных антенн, управление

очередностью передач.

Метолы доступа можно классифицировать по следующим признакам (рис.3.1.1):

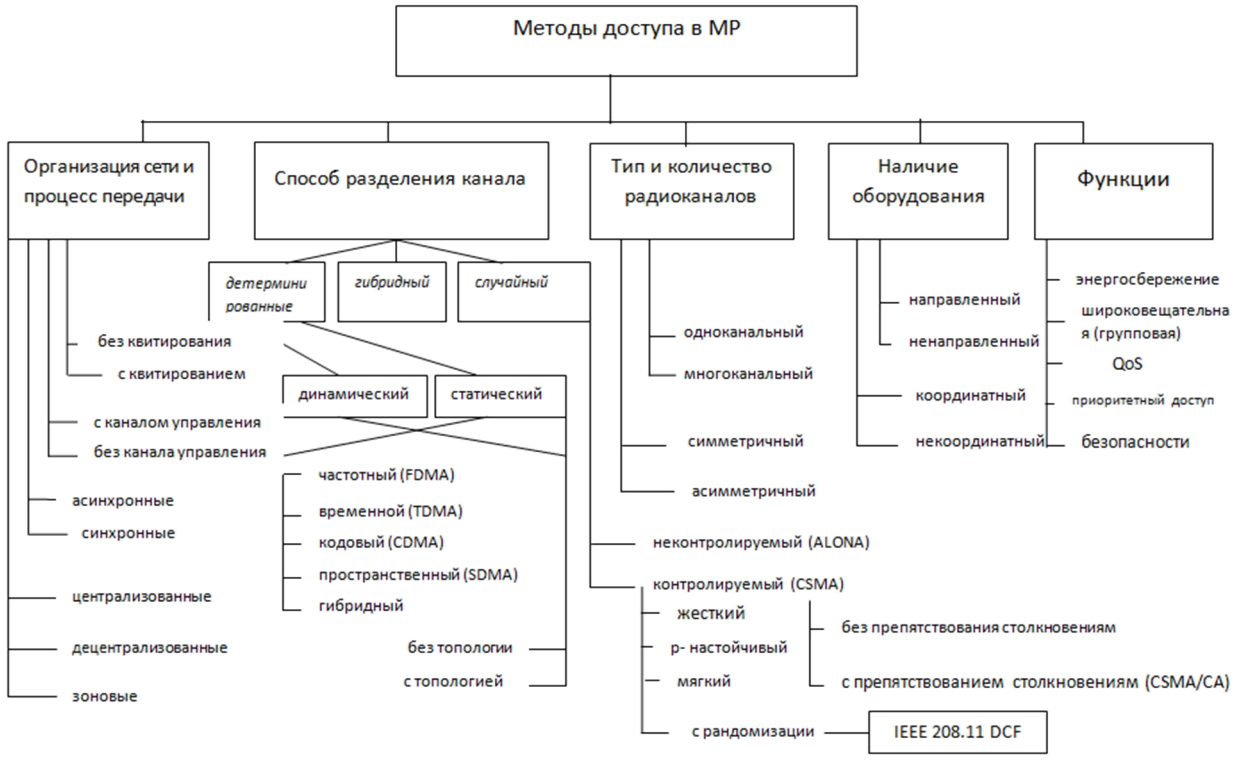


Рис.3.1.1. Классификация доступа в беспроводной сети

- по организации сети и процесса перелачи сообщений — централизованные, децентрализованные и зоновые: синхронные или асинхронные, с выделенным каналом управления или без него; с квитированием или без него;
- по способу разделения канала — детерминированные (статические или динамические), случайные (неконтролируемые и контролируемые) и гибридные (их комбинация):
- по количеству и типу используемых радиоканалов в сети одноканальные и многоканальные, симметричные и асимметричные;
- по использованию в узлах сети оборудования позиционирования (координатные и некоординатные) и антенн с изменяющейся диаграммой направленности (направленные или ненаправленные);
- по реализации функций (дополнительных сервисов) - энергосбережение;

широковещательная (групповая) передача; передача с заданным качеством обслуживания (QoS); передача приоритетного трафика, безопасность.

Зоновая организация сети, предполагающая разбиение ее на зоны (кластеры) с выделением в каждой зоне главных и простых узлов, а также шлюзов (для связи между зонами), является комбинацией централизованного (в зонах) и децентрализованного (между главными узлами) способов управления.

Узлы могут функционировать в *синхронном* или *асинхронном* режиме. Синхронизация предполагает, что радиоканал сегментирован на дискретные интервалы времени (слоты), объединенные в повторяющиеся фрагменты. Регулярность и однородность слотов позволяет реализовать передачу с заданным качеством обслуживания , так как задержка, пропускная способность легко управляются посредством назначения временных слотов. Сложность процесса синхронизации зависит от организации сети, в централизованной сети. Узлы каждой соты легко синхронизируются базовой станцией, которая широковещательно передает сигнал, указывающий на начало временного фрагмента. В узлах процесс синхронизации значительно сложнее и может быть осуществлен за счет временных сигналов глобальной системы позиционирования (GPS). В свою очередь, асинхронный режим не предполагает глобальной синхронизации узлов и поэтому не требует дополнительного оборудования, однако определяет сложность в передаче данных (например, интегрального трафика) из-за случайного характера обмена информацией.

Организация сети тесно взаимосвязана со способами разделения канала: *детерминированным, случайным* и *гибридным.*

Реализация детерминированных методов доступа заключается в планировании (резервировании) ресурса сети для передачи сообщений. В качестве ресурса могут выступать частота (FDMA), время (TDMA), коды (CDMA), пространство (SDMA) или их сочетание (гибридные МД, например TDMA/CDMA или STDMA). Планирование может осуществляться как с учетом, так и без учета текущей топологии сети.

Статические детерминированные МД являются централизованными (предполагают наличие информации обо всей сети) и осуществляют фиксированное планирование ресурсов сети до начала передач узлов.

Динамические детерминированные МД для планирования используют информацию о нагрузке и топологии сети. Здесь задача распределения ресурсов усложняется из-за отсутствия глобальной информации о сети (обычно каждый узел собирает информацию на расстоянии ретрансляций), поэтому предлагаемые решения для узлов в указанной области имеют целью получение субоптимальных децентрализованных решений.

Большинство известных детерминированных МД ориентировано на распределение временного ресурса, что возможно только в синхронных сетях. Соответствующие методы являются преимущественно бесконфликтными, т. е. длина передаваемого пакета меньше длительности слота (последние могут иметь фиксированную или переменную длину).

Рассмотрим *случайные МД,* большинство из которых функционируют в условиях асинхронной сети. Исторически первым считается метод *ALOHA,* не предполагающий взаимной координации узлов. Любой узел *i*, подготовив пакет к передаче узлу *j,* в произвольный момент времени начинает передачу. Передав пакет, узел *i* определенное время ожидает прием квитанции от узла *j*. Если квитанция не получена, то через случайный промежуток времени передача начинается вновь. Очевидно, что вероятность столкновений у этого метода очень велика (максимальная пропускная способность для полносвязной сети (*S*= 0.18). Повысить пропускную способность сети можно сегментированием сети - *S-ALOHA (S = 0.36*) [2,78].

Для снижения вероятности столкновений пакетов применяют методы доступа с контролем несущей (МДКН) или CSMA, т. е, методы, основанные на предварительной проверке состояния радиоканала. В простейшем случае перед передачей пакета абонент контролирует состояние канала (наличие несущей или самой передачи). Если канал занят, абонент откладывает передачу на более позднее время. При освобождении канала его передача

может начинаться различными способами: сразу («жесткий» МДКН), через случайный интервал времени *(*«мягкий»), с вероятностью p (p-настойчивый) или с рандомизацией времени передачи на сегменты.

Основным препятствием успешной передаче пакета при МДКН являются так называемые проблемы скрытого и открытого терминалов, т. е. возможность столкновения пакетов из-за распределенности процесса принятия решения на передачу (рис. 3.1.2). Проблема «скрытого терминала» (рис.3.1.2, *а)* заключается в том, что абонент *a* не находится в пределах радиодоступности с абонентом *c* и, соответственно, не может прослушивать его передачи. Поэтому при передаче пакета от узла *a* к узлу *b* узел *c* в это же время может передать свой пакет (например, узлу *d*). В результате возникает столкновение пакетов. В данном случае узел *c* является скрытым узлом относительно узла *a.*

Проблема «открытого терминала» (рис. 3.1.2. б) такова: узел *c* передает пакет узлу *d* и блокирует на время передачи узел *b,* который намеревается осуществить передачу узлу *a* (хотя процесс данной передачи бесконфликтен).

Рис. 3.1.2. Иллюстрация проблем «скрытого» (а) и «открытого» (б) терминалов

Эффективность метода доступа в беспроводной сети зависит не только от входной нагрузки, но и от мобильности узлов, используемого метода маршрутизации и текущей топологии сети и текущего состояния канала[2,105].

Для эффективного использования ресурсов беспроводной сети необходимо предусмотреть возможность применения метаметодов, т.е. совокупности методов доступа в узлах сети. Выбор конкретного метода доступа зависит от текущей цели управления сетью, состояния последней и принятых решений на других уровнях эталонной модели. Для окончательного

решения в пользу конкретного МД целесообразно используются методы, основаны на нечеткой логике и нечеткой системе управления[23,24].

3.2. Нечеткий алгоритм управления доступом в КИТС

Важными проблемами в области обеспечения качества обслуживания являются проблемы управления доступом. Для дальнейшего улучшения качества и эффективности передачи данных в беспроводных сетях требуется разработка нового алгоритма управления доступом, который позволит использовать полосу пропускания канала более эффективно для разных типов трафика и ограничения числа конфликтов с целью предотвращения возможности переполнения и блокировки низкоприоритетных потоков. Это особенно важно, учитывая особенности сетей Йемена [1,17,61-66]. Для анализа и расчета оптимальных условий доступа в беспроводных сетях к общему ресурсу предлагаем применить нечеткую логику и нечеткую систему управления.

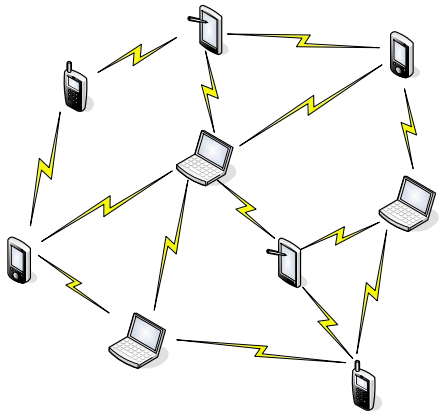


Рис.3.2.1. Соединение между абонентскими терминалами

Структура системы управления доступом к каналу на основе математического аппарата нечеткой логики представлена на рис3.2.2.

Рис.3.2.2. Схема нечеткого управления допуском

Модель системы на основе сети ТГУ. Мы рассмотрим и изучим вариант модели системы нечеткого случайного множественного доступа на примере сети ТГУ [63]. В системе имеется бесконечное число абонентов и канал связи, вход и выход которого доступны всем абонентам. У абонентов возникают пакеты, которыми они обмениваются, используя канал связи. Предполагается, что все пакеты имеют одинаковую длину.

Мы наложим ряд предположений на функционирование канала связи и способ доступа вызовов к нему, сходные с условиями работы [1,17,23,24,61-66,105].

Абонент запоминает пакет *x* в буфере и, начиная с окна $t_x + 1$, использует значение *x* для принятия решения о том в каких окнах пакет *x* будет передаваться. Обозначим через $\nu_i^{(x)}$ индикатор события {пакет *x* передавался в окне *i*}. Последовательность $\nu^{(x)}(t) = \{\nu_0^{(x)}, \ldots \nu_t^{(x)}\}$ будем называть историей пакета *x* к окну *t*. Если в окне *t* происходит передача пакета *x*, т.е. $\nu_t^{(x)}=1$, и если других пакетов не передается, т.е. $\theta_t = 1$, то по завершении этого окна считается, что пакет *x* в успешно передан, и он удаляется из системы.

Пакеты, имеющие единичную длину, могут передаваться станциями лишь на временных интервалах (t, t+1), $t = \{0, 1, \ldots\} = I_0$, которые называются окнами.

Число станций, передающих пакеты по каналу, достаточно велико, так что его можно считать бесконечным. На каждой станции в любой момент времени находится не более одного требующего передачи пакета.

Моменты возникновения на всех станциях новых готовых для передачи пакетов образуют суммарный поток, который является пуассоновским и обозначается X*. Последовательные моменты возникновения пакетов обозначаются $x_1^* <: x_2^* <: \ldots$, $x_i^* \in R_+$, где R_+, - множество действительных неотрицательных чисел. Таким образом, $X^* = \{x_1^*, x_2^*, \ldots\}$, и разности $x^*_{i+1} - x^*_i$, $i \in I_1$, являются независимыми одинаково распределенными случайными

величинами с распределением $Pr\{ x^*_{i+1} - x^*_i > x\} = e^{-\lambda x}$, $x_i^* \in R_+$, где λ - интенсивность потока X*.

В любом окне (t, t+1) может произойти одно из n+1 событий: пустое окно - ни одна из станций не передавала пакет в этом окне (это событие обозначается $\theta_{t+1}=0$); успешная передача *i* пакетов - в окне передавали пакеты i, 1<i<n-1 , станций ($\theta_{t+1}=1$); конфликт - в окне передавали пакеты n или более станций ($\theta_{t+1}=n$). Каждой станции системы к началу каждого окна становится известным, какое из этих n событий произошло в предыдущем окне. Станции запоминают эти сведения, так что к началу любого окна (t, t+1) каждой станции известны события $\theta(t) = (\theta_1 \ldots , \theta_t)$, происходившие во всех предыдущих окнах. Успешно переданные пакеты покидают систему. Пакеты, попавшие в конфликт, требуют повторной передачи и покидают систему лишь получив, наконец, успешную передачу.

Если станция в момент t, $t \in I_0$, имеет требующий передачи пакет, то она передает его по каналу в окне (t, t+l) или молчит в этом окне в зависимости от того, что предписывает ей нечеткий алгоритм передачи, используя при этом общую для всех абонентов историю канала θ(t − 1) и индивидуальную историю пакета $\nu^{(x)}(t-1)$.

Абонентский терминал (АТ) все время будет проводить изучение и измерение состояния канала, прежде чем передает свои пакеты.

Считается, что бесконечное число АТ, которые передают по каналу пакеты равной длины. Все время передачи по каналу разделено на окна. Длина окна равна длине пакета и принята за единицу времени. Считается, что на станции системы в течение любого окна Δt извне поступает суммарный пуассоновский поток интенсивности λ; при этом каждая станция в любой момент имеет не более одного требующего передачи пакета [2,23].

Измерение состояния канала проводится в разных интервалах времени τ1, τ2,.. τn, где τ- длительность цикла. где, τ = 8Δt Δt=[t, t + 1] требуемый интервал времени для передачи одного пакета.

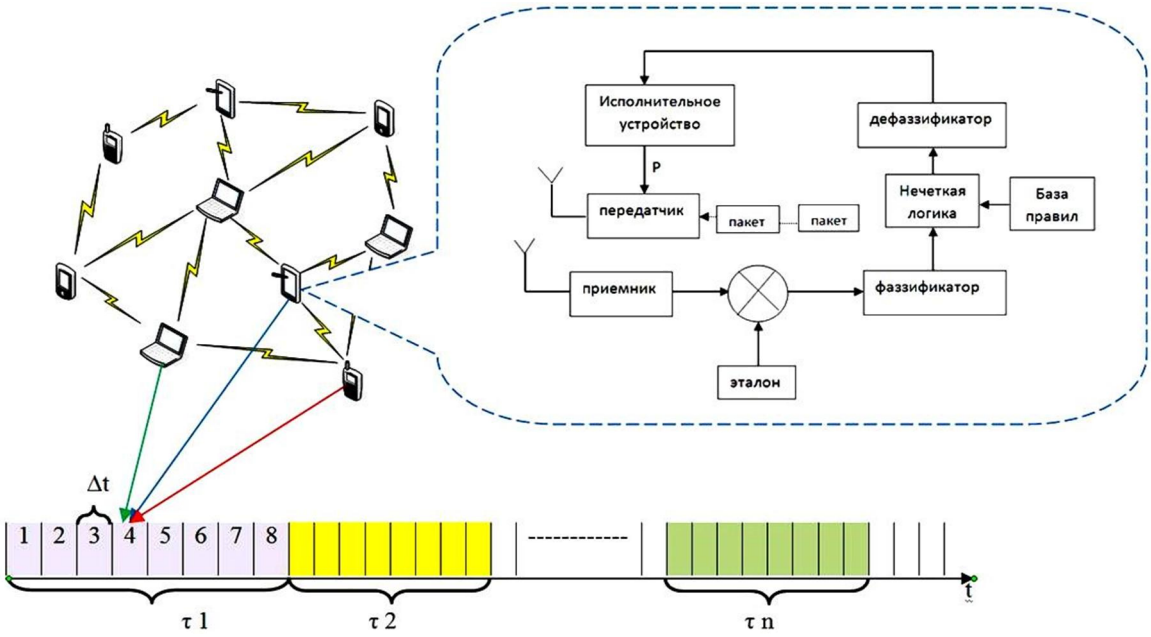


Рис.3.2.3. Схема когнитивного абонентского терминала на примере ТГУ

Как показано на рис.3.2.3 приемник когнитивного абонентского терминала осуществляет измерения состояния канала. Результаты измерения поступает на устройство сравнения, которое определяет степень текущей загруженности канала и насколько изменилось состояние канала в τ_n по сравнению с предыдущим состоянием в τ_{n-1}.

Значение состояния канала (количество свободных окон) и изменение степени загрузки канала подаются из устройства сравнения на вход контроллера, который проводит фаззификацию всех значений и затем в соответствии с установленной базой правил выполняет операцию нечеткого вывода.

Результат нечеткого вывода передается в деффазификатор, который преобразует нечеткие значения в четкие решения, которые передаются на вход исполнительного устройства. В соответствии с результатом решения нечеткой логики, исполнительное устройство устанавливает вероятность, с которой будет передаваться поступивший пакет в канал.

3.3. Применение нечеткой логики для управления множественным доступом

Математическая теория нечетких множеств (fuzzy sets) и нечеткая логика (fuzzy logic) являются обобщениями классической теории множеств и

классической формальной логики. Популярность теории нечетких множеств в проектировании в арабском мире объясняется тем, что нечеткие системы разрабатываются быстрее, они получаются проще и дешевле четких аналогов[23]. При разработке нечетких систем необходимо пройти следующие этапы проектирования (табл. 3.3.1):

Таблица 3.3.1. Этапы нечетких систем

Этапы	**Задание**
Определить входы и выходы создаваемой системы	Проект
Задать для каждой из входных и выходных переменных функции принадлежности с термами	Проект, заказчик
Разработать базы правил выводов для реализуемой нечёткой системы	заказчик
Провести дефаззификацию	Проект
Программная реализация нечеткого регулятора на конкретном микроконтроллере	Проект
Провести настройку и анализ адекватности разработанной модели реальной системе	Проект, администрация

Фаззификация и разработка нечетких правил вывода. Нечетким логическим выводом (fuzzy logic inference) называется аппроксимация зависимости Y = f(X1,X2…Xn) каждой выходной лингвистической переменной от входных лингвистических переменных и получение заключения в виде нечеткого множества, соответствующего текущим значениям входов, с использованием нечеткой базы знаний и нечетких операций. Максимально приближаемся к ТГУ [63].

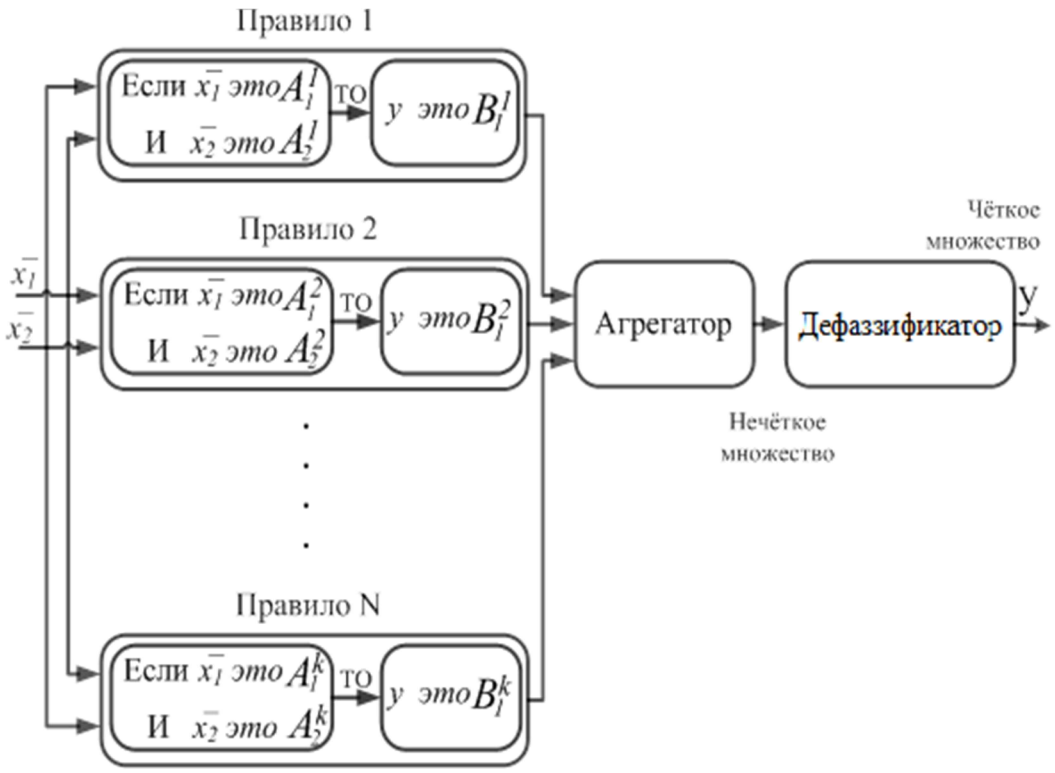


Рис.3.3.1. Система нечеткого логического вывода. Где $\bar{x}1$ – состояние канала; $\bar{x}2$ – скорость изменения состояния канала; У-рейтинг канала; К=1..N

Фаззификатор выдает три терма состояния канала Т(С): «канал загружен», «канал в норме», «канал незагружен».

Как показано на рис.3.2.3 мы предлагаем, если во время передачи пакета были свободные из 8 окна (тактовых интервалов времени) Δt:

(0…2) Δt, канал загружен,

(3…5) Δt – канал в норме,

(6..8) Δt – канал незагружен.

В качестве входной переменной используется С- число свободных окон (состояние канала), которое меняется с [0..8] и терма множества Т(С) которого имеет вид: «канал загружен (П)», «канал в норме (Н)» и «канал незагружен (Х)». Функция принадлежности $\mu(C)$ имеет вид треугольную форму как на рис.3.3.2 .

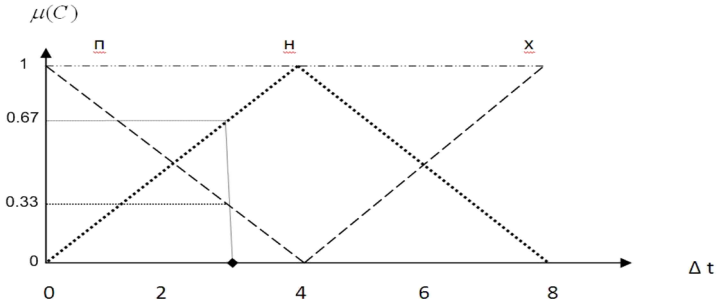


Рис.3.3.2. Функция принадлежность состояния канала

Состояние канала будет менять через случные моменты времени. Скорость изменения состояния канала обозначаем через скорость изменения степени загруженности канала dX/dt и мы считаем ее второй входной переменной нечеткого алгоритма управления. dX/dt может принимать значения от минуса 8 до плюса 8 единиц.

Для перехода к нечетким переменным скорости изменения степени загруженности канала примем форму функции принадлежности с термами: снижает (М), в норме (Н) и повышает (В) (рис. 3.3.3).

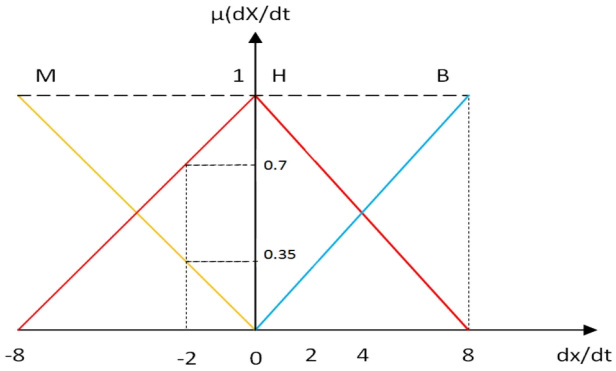


Рис.3.3.3. Функция принадлежность изменения загруженности канала

В качестве Т-нормы используется операция минимум, в качестве S-нормы – операция максимум:

$$\mu_A(x) *^T \mu_B(x) = \min(\mu_A(x), \mu_B(x)).$$
$$\mu_A(x) *^S \mu_B(x) = \max(\mu_A(x), \mu_B(x)).$$

$$\mu_{A\to B}(x,y) = \mu_R(x,y) = \mu_A(x) \cap \mu_B(y) = \min(\mu_A(x), \mu_B(y)),$$

$$\mu_{B'}(y) = \max_{k=1\ldots N}\{\min[\mu_{A_1^k}(\overline{x}_1), \mu_{A_2^k}(\overline{x}_2), \mu_{B_1^k}(y)]\},$$

где $\overline{x}_1$, $\overline{x}_2$ соответственно входные переменные (число свободных окон и скорость изменения степени загруженности канала), A_1^k и A_2^k -

соответствующие им нечеткие множества, к=1,…..,N- правила нечеткого вывода.

Совокупность всех правил удобно представить в виде табл.3.3.1.

Таблица 3.3.1.Рейтинг канала при всех значениях (C и dx/dt)

C	dX\dt	Y(centroid)	Y(bisector)	Y(mom)	Y(lom)	Y(som)
0	-8	50,0	50,0	50,0	50,0	50,0
0	-7	46,1	48,0	50,0	52,0	48,0
0	-6	43,1	46,0	50,0	55,0	45,0
0	-5	40,6	43,0	50,0	57,0	43,0
0	-4	38,3	38,0	38,0	60,0	16,0
0	-3	35,9	33,0	26,0	33,0	19,0
0	-2	33,4	30,0	25,5	30,0	21,0
0	-1	30,3	28,0	25,0	27,0	23,0
0	0	26,3	26,0	25,0	25,0	25,0
0	1	25,2	26,0	25,0	27,0	23,0
0	2	23,9	25,0	25,5	30,0	21,0
0	3	22,4	23,0	26,0	33,0	19,0
0	4	20,8	21,0	18,8	36,0	0,0
0	5	19,0	18,0	3,5	7,0	0,0
0	6	16,5	12,0	2,5	5,0	0,0
0	7	12,8	8,0	1,0	2,0	0,0
0	8	6,3	5,0	0,0	0,0	0,0
1	-8	56,6	54,0	50,0	55,0	45,0
1	-7	52,7	52,0	50,0	55,0	45,0
1	-6	49,7	50,0	50,0	55,0	45,0
1	-5	47,3	47,0	50,0	57,0	43,0
1	-4	45,3	44,0	38,0	60,0	16,0
1	-3	43,5	39,0	26,0	33,0	19,0
1	-2	41,8	34,0	25,5	30,0	21,0
1	-1	38,1	32,0	25,5	30,0	21,0
1	0	33,4	30,0	25,5	30,0	21,0
1	1	32,1	29,0	25,5	30,0	21,0
1	2	30,8	28,0	25,5	30,0	21,0
1	3	29,6	28,0	26,0	33,0	19,0
1	4	28,5	27,0	18,8	36,0	0,0
1	5	27,7	25,0	3,5	7,0	0,0
1	6	26,8	23,0	2,5	5,0	0,0
1	7	22,6	17,0	2,5	5,0	0,0
1	8	16,5	12,0	2,5	5,0	0,0
2	-8	61,3	61,0	61,2	83,0	40,0
2	-7	57,1	58,0	61,2	83,0	40,0
2	-6	53,9	55,0	61,2	83,0	40,0
2	-5	51,4	52,0	61,2	83,0	40,0
2	-4	49,5	49,0	48,7	83,0	16,0

2	-3	47,7	47,0	38,0	60,0	16,0
2	-2	45,3	44,0	38,0	60,0	16,0
2	-1	42,2	41,0	38,0	60,0	16,0
2	0	38,3	38,0	38,0	60,0	16,0
2	1	36,9	37,0	38,0	60,0	16,0
2	2	35,4	36,0	38,0	60,0	16,0
2	3	33,9	34,0	38,0	60,0	16,0
2	4	32,6	33,0	31,2	60,0	0,0
2	5	30,9	30,0	18,8	36,0	0,0
2	6	28,5	27,0	18,8	36,0	0,0
2	7	25,3	24,0	18,8	36,0	0,0
2	8	20,8	21,0	18,8	36,0	0,0
3	-8	66,3	70,0	75,0	79,0	71,0
3	-7	61,1	68,0	75,0	79,0	71,0
3	-6	57,1	65,0	75,0	79,0	71,0
3	-5	55,5	59,0	75,0	81,0	69,0
3	-4	53,9	55,0	61,2	83,0	40,0
3	-3	52,0	52,0	50,0	57,0	43,0
3	-2	49,7	50,0	50,0	55,0	45,0
3	-1	46,8	48,0	50,0	55,0	45,0
3	0	43,1	46,0	50,0	55,0	45,0
3	1	41,5	45,0	50,0	55,0	45,0
3	2	39,6	44,0	50,0	55,0	45,0
3	3	37,5	41,0	50,0	57,0	43,0
3	4	35,4	36,0	38,0	60,0	16,0
3	5	33,2	31,0	26,0	33,0	19,0
3	6	30,8	28,0	25,5	30,0	21,0
3	7	27,9	27,0	25,5	30,0	21,0
3	8	23,9	25,0	25,5	30,0	21,0
4	-8	75,0	75,0	75,0	75,0	75,0
4	-7	69,9	73,0	75,0	77,0	73,0
4	-6	66,3	70,0	75,0	79,0	71,0
4	-5	63,6	67,0	75,0	81,0	69,0
4	-4	61,3	61,0	61,2	83,0	40,0
4	-3	59,1	57,0	50,0	57,0	43,0
4	-2	56,6	54,0	50,0	55,0	45,0
4	-1	53,5	52,0	50,0	52,0	48,0
4	0	50,0	50,0	50,0	50,0	50,0
4	1	46,1	48,0	50,0	52,0	48,0
4	2	43,1	46,0	50,0	55,0	45,0
4	3	40,6	43,0	50,0	57,0	43,0
4	4	38,3	38,0	38,0	60,0	16,0
4	5	35,9	33,0	26,0	33,0	19,0
4	6	33,4	30,0	25,5	30,0	21,0
4	7	30,3	28,0	25,0	27,0	23,0
4	8	26,3	26,0	25,0	25,0	25,0

5	-8	77,9	77,0	75,0	79,0	71,0
5	-7	72,7	74,0	75,0	79,0	71,0
5	-6	69,3	72,0	75,0	79,0	71,0
5	-5	66,7	69,0	75,0	81,0	69,0
5	-4	64,5	64,0	61,2	83,0	40,0
5	-3	62,5	59,0	50,0	57,0	43,0
5	-2	60,4	55,0	50,0	55,0	45,0
5	-1	58,4	55,0	50,0	55,0	45,0
5	0	56,6	54,0	50,0	55,0	45,0
5	1	52,7	52,0	50,0	55,0	45,0
5	2	49,7	50,0	50,0	55,0	45,0
5	3	47,3	47,0	50,0	57,0	43,0
5	4	45,3	44,0	38,0	60,0	16,0
5	5	43,5	39,0	26,0	33,0	19,0
5	6	41,8	34,0	25,5	30,0	21,0
5	7	38,1	32,0	25,5	30,0	21,0
5	8	33,4	30,0	25,5	30,0	21,0
6	-8	81,1	81,0	82,9	100,0	67,0
6	-7	75,5	77,0	82,9	100,0	67,0
6	-6	71,7	74,0	82,9	100,0	67,0
6	-5	69,1	71,0	82,9	100,0	67,0
6	-4	67,4	68,0	68,8	100,0	40,0
6	-3	66,1	66,0	61,2	83,0	40,0
6	-2	64,5	64,0	61,2	83,0	40,0
6	-1	62,8	62,0	61,2	83,0	40,0
6	0	61,3	61,0	61,2	83,0	40,0
6	1	57,1	58,0	61,2	83,0	40,0
6	2	53,9	55,0	61,2	83,0	40,0
6	3	51,4	52,0	61,2	83,0	40,0
6	4	49,5	49,0	48,7	83,0	16,0
6	5	47,7	47,0	38,0	60,0	16,0
6	6	45,3	44,0	38,0	60,0	16,0
6	7	42,2	41,0	38,0	60,0	16,0
6	8	38,3	38,0	38,0	60,0	16,0
7	-8	85,3	89,0	97,5	100,0	95,0
7	-7	77,9	84,0	97,5	100,0	95,0
7	-6	73,2	77,0	97,5	100,0	95,0
7	-5	72,5	75,0	96,5	100,0	93,0
7	-4	71,7	74,0	82,9	100,0	67,0
7	-3	70,6	73,0	75,0	81,0	69,0
7	-2	69,3	72,0	75,0	79,0	71,0
7	-1	67,8	71,0	75,0	79,0	71,0
7	0	66,3	70,0	75,0	79,0	71,0
7	1	61,1	68,0	75,0	79,0	71,0
7	2	57,1	65,0	75,0	79,0	71,0
7	3	55,5	59,0	75,0	81,0	69,0

7	4	53,9	55,0	61,2	83,0	40,0
7	5	52,0	52,0	50,0	57,0	43,0
7	6	49,7	50,0	50,0	55,0	45,0
7	7	46,8	48,0	50,0	55,0	45,0
7	8	43,1	46,0	50,0	55,0	45,0
8	-8	93,7	94,0	100,0	100,0	100,0
8	-7	88,6	92,0	99,0	100,0	98,0
8	-6	85,3	89,0	97,5	100,0	95,0
8	-5	83,0	84,0	96,5	100,0	93,0
8	-4	81,1	81,0	82,9	100,0	67,0
8	-3	79,5	78,0	75,0	81,0	69,0
8	-2	77,9	77,0	75,0	79,0	71,0
8	-1	76,4	76,0	75,0	77,0	73,0
8	0	75,0	75,0	75,0	75,0	75,0
8	1	69,9	73,0	75,0	77,0	73,0
8	2	66,3	70,0	75,0	79,0	71,0
8	3	63,6	67,0	75,0	81,0	69,0
8	4	61,3	61,0	61,2	83,0	40,0
8	5	59,1	57,0	50,0	57,0	43,0
8	6	56,6	54,0	50,0	55,0	45,0
8	7	53,7	52,0	50,0	52,0	48,0
8	8	50,0	50,0	50,0	80,0	50,0

расчетные методики (обозначения)

centroid	центр тяжести	**C**	состояние канала
bisector	медиана	**dX/dt**	скорость изменения сост. канала
lom	наибольший из максимумов	**Y**	рейтинг канала
som	наименьший из максимумов		
mom	центр максимумов		

Приведена диаграмма (рис. 3.3.4) рейтингов канала полученных методом центра тяжости и как видно, чем больше свободных окон(С) и меньше скорости изменения степени загруженности канала (dx\dt), тем больше рейтинг канала.

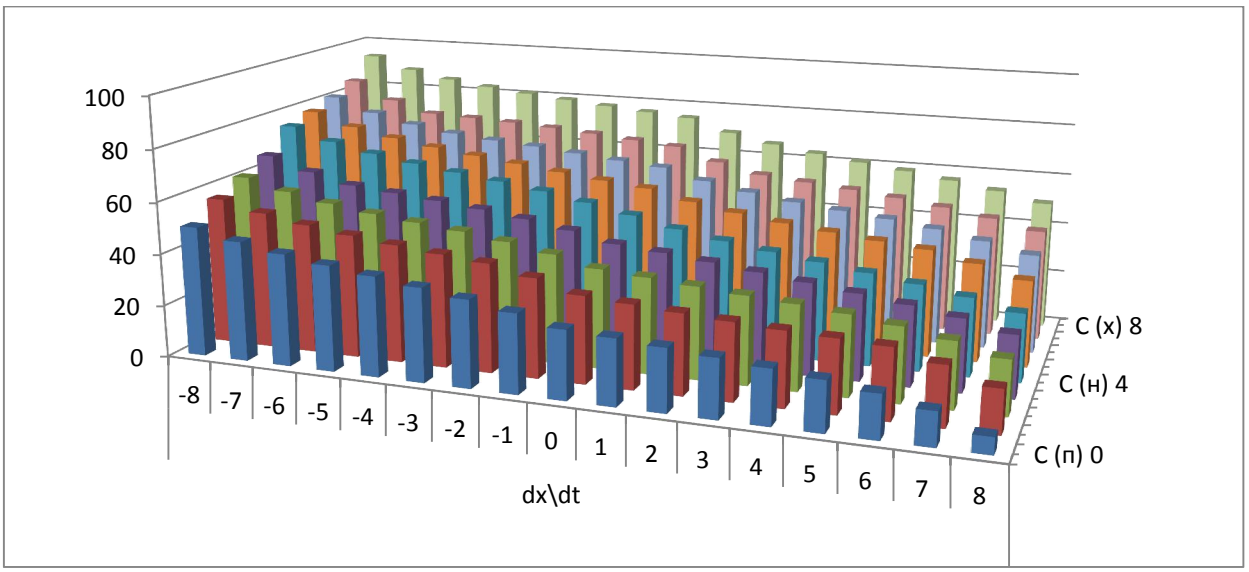


Рис.3.3.4.

Приводим алгоритм и листинг разработанной нами программы, обеспечивающей этот расчет(см. приложение 3.3)

Для примера мы допустим что, число свободных окон при передаче пакета были 3 и степень загруженности канала изменился на минус 2 по сравнению с предыдущим состоянием. В этом случае термы П и Н состояние канала как показано на рис.3.3.2 имеют степень принадлежности 0,33 и 0,67

соответственно, а термы М и Н скорости изменения степени загруженности канала на рис.3.3.3 равны 0,35и 0,7.

Приведем интерфейсные рисунки иллюстрирующие действие нашей программы.

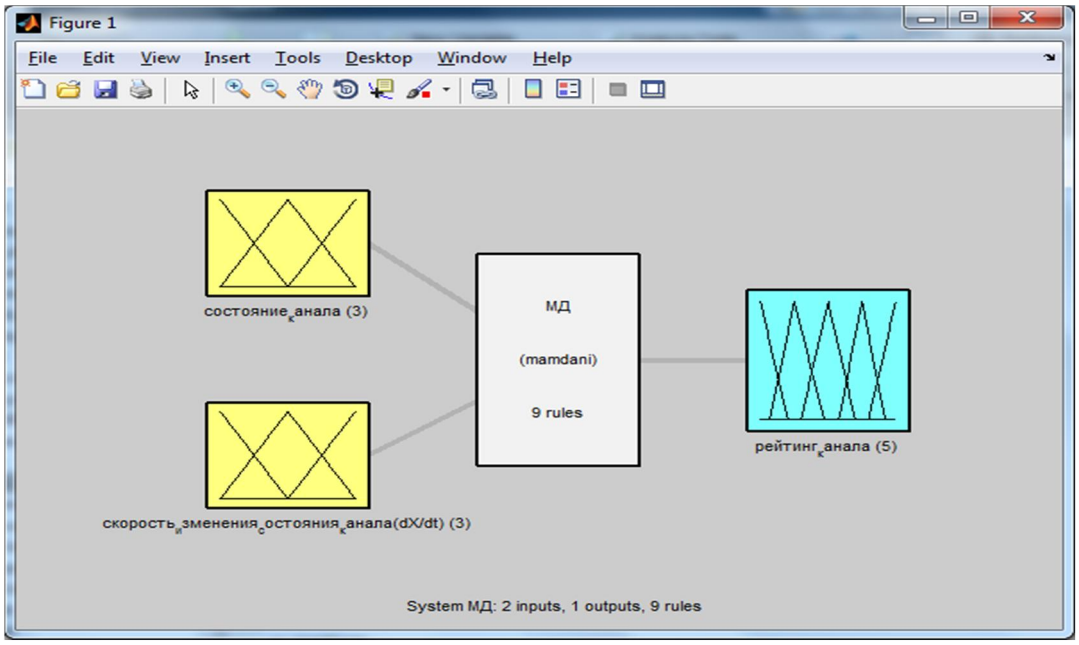


Рис.3.3.5. Система множественного доступа

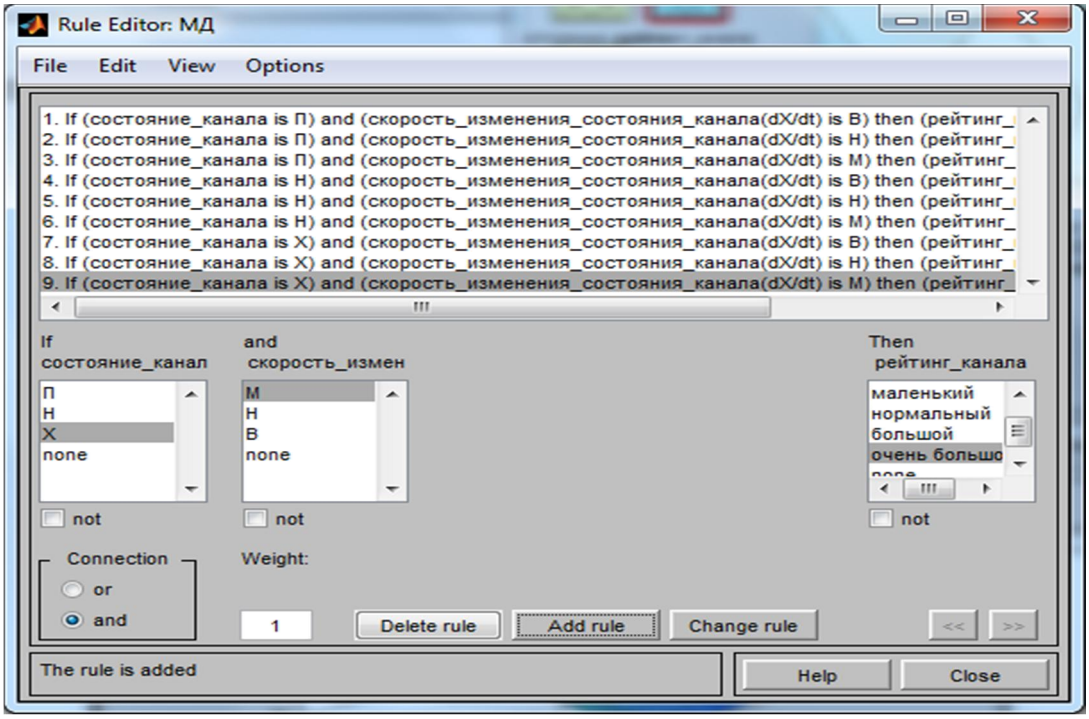


Рис.3.3.6. Правила нечеткого вывода

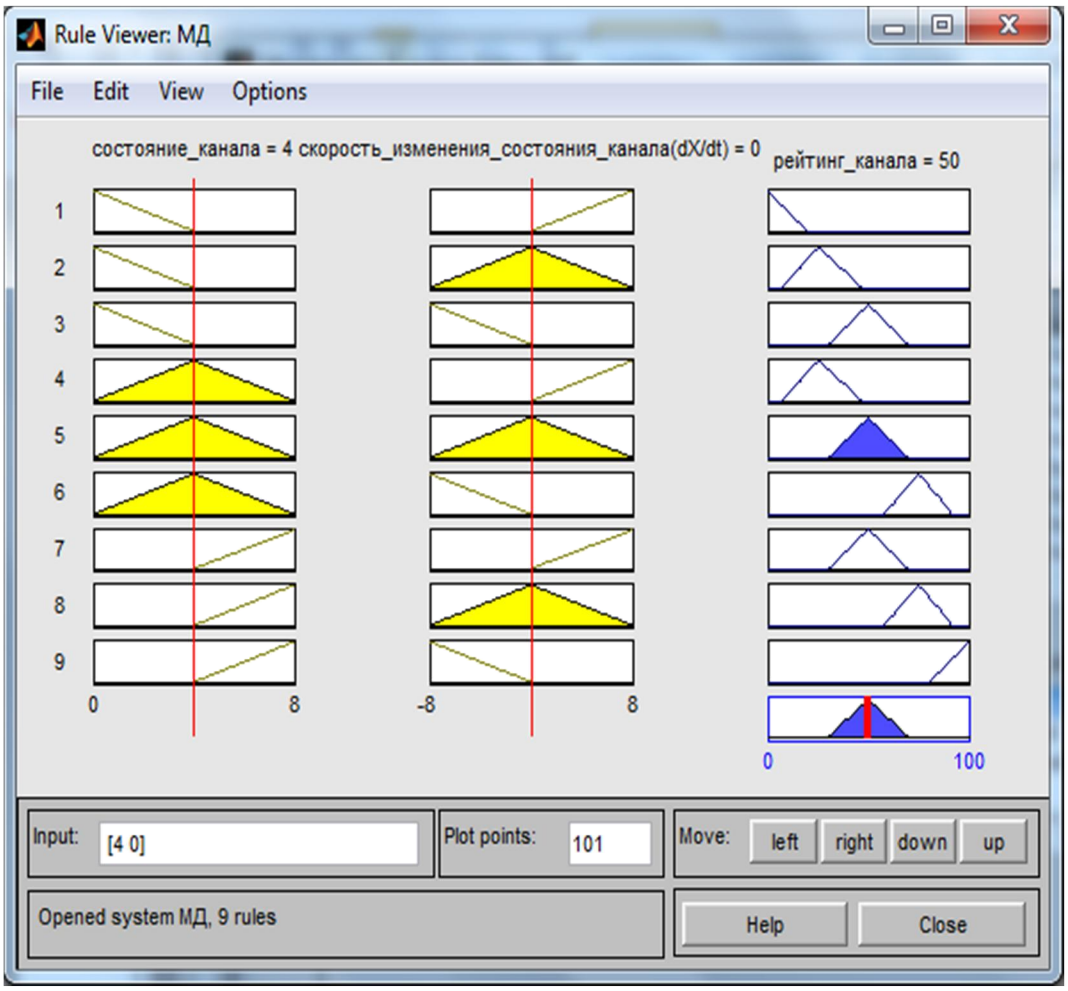


Рис.3.3.8. Просмотр правила нечёткого вывода

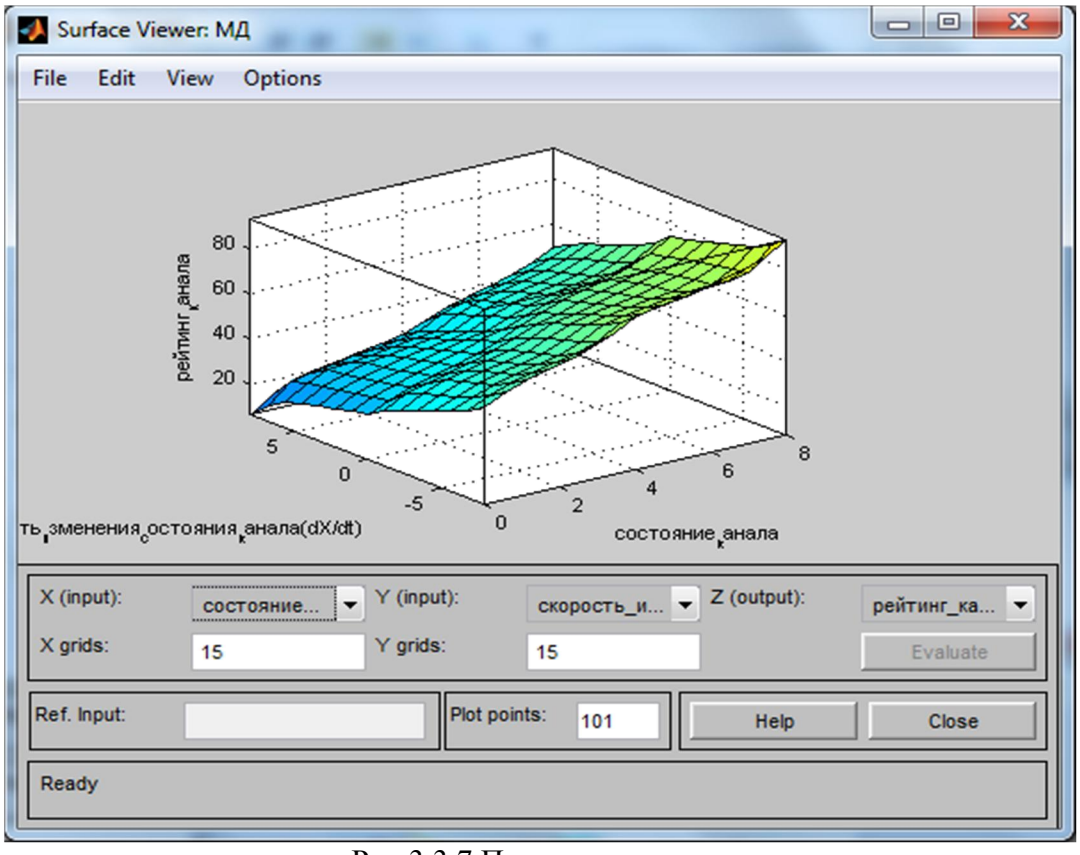


Рис.3.3.7.Поверхности просмотра

Формула дефаззификации по методу центра тяжести (см. раздел 3.2):

$$Y = \frac{y1\mu OM + y2\mu M + y3\mu H + y4\mu B + y5\mu OB}{\mu OM + \mu M + \mu H + \mu B + \mu OB}$$

Подставив в формулу численные значения, получим:

$$Y = \frac{0 \cdot 0 + 25 \cdot 0.33 + 50 \cdot 0.67 + 75 \cdot 0.35 + 0 \cdot 0}{0 + 0.33 + 0.67 + 0.35 + 0} = 47$$

Получено значение рейтинга канала управления в сети ТГУ, что позволяет нам оценить конкуретный уровень наших разработок по сравнению с другими КИТС.

Моделирование алгоритма МД в сети ТГУ. Рассмотрим сеть [63] (см. приложение), состоящую из пяти станций, передающих пакеты по коллективно используемому каналу связи. Канал может находиться в одном из трех состояний: П, Н, Х. Пакет, попавший в конфликт, должен согласно алгоритму передаваться повторно до тех пор, пока не будет передан успешно. Число попавших в некоторый конфликт пакетов называется кратностью этого конфликта. Когда канал находится в состоянии П, в сети действует синхронизация, в результате каждый отрезок времени, в течение которого канал находился в состоянии П, разбивается на целое число равных интервалов, называемых окнами. Длина окна принимается за единицу измерения времени. Как на рис. 3.3.8 первые два окна были свободные, через случайный момент времени на третьем окно появились 3 пакета из трех абонентов, в результате возникает конфликт.

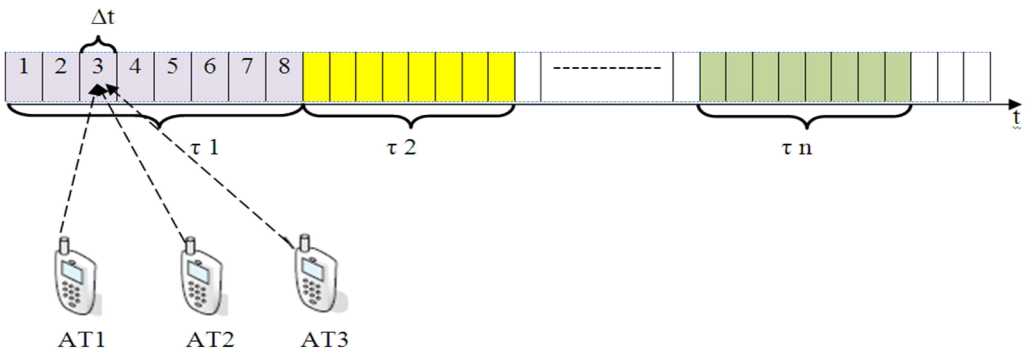


Рис.3.3.9. Окна и пакеты сети ТГУ

В результате использование нами нечеткой логики в абонентских

терминалах сети ТГУ позволяет учитывать параметры состояния каналов связи при выборе оптимального канала для передачи пакетов без конфликтов. Это позволило увеличить эффективность защиты в сети ТГУ (см. Приложения).

3.4. Разработка методики маршрутизации в мобильных беспроводных ad-hoc сетях на основе аппарата нечеткой логики

Основной проблемой является сложность построения точной математической модели сети по многим причинам, основной из которых является сложная система взаимного влияния параметров. Существующие [47] подходы к маршрутизации в беспроводных ad hoc сетях не позволяют учитывать все множество факторов, влияющих на распределение трафика в сети и на передачу пакетов между двумя узлами.

Предлагаем новый подход к решению задач маршрутизации в сетях MANET , основан на применение математической теории нечетких множеств в частности поиск наиболее пригодных маршрутов на нечетких графах, с учетом особенностей ТГУ [63].

3.4.1. Анализ существующих методов маршрутизации в сетях Йемена

Разработанные протоколы маршрутизации для MANET сетей классифицируются соответственно стратегии обнаружения и поддерживания маршрутов на три класса: проактивные, реактивный, и гибрид как показано на рис. 3.4.1 [52].

Рис.3.4.1. Классификация протоколов маршрутизации в MANET сетях

Рассмотрим несколько методов, которые являются наиболее широко

распространенными и используемыми (табл.3.4.1.1):

Таблица 3.4.1.1. Протоколы сетей в Йемене

действие	**протоколы**	**особенности**
Оптимизированная маршрутизация по состоянию каналов связи) [47,52]	OLSR (Optimized Link State Routing,	оптимизация обычного протокола маршрутизации по состоянию каналов связи LSR (Link State Routing, Маршрутизация по состоянию каналов связи) для беспроводных сетей.
запрашивает маршрут до узла, до которого еще нет маршрута в таблице, узел широковещательно рассылает запрос на поиск маршрута.	AODV this On-Demand routing protocol is essentially a combination of DSR and Destination Sequenced Distance Vector (DSDV)	Маршруты поддерживаются в таблице маршрутизации до тех пор, пока они используются. AODV строит маршруты, используя цикл "запрос-ответ"
Динамическая маршрутизация от источника	DSR (Dynamic Source Routing,	отсутствуют «маяки» и следовательно не требует периодической передачи пакета приветствия, которые используются узлом, чтобы сообщить соседям о его присутствии.
Маршрутизация с учетом качества обслуживания при	Application Aware QoS Routing	полагается на транспортный уровень. Данный подход предполагает использование

участии приложения [47,52]		транспортного протокола реального времени (RTP, Real-time Transport Protocol) [23]
Кроссуровневая маршрутизация по требованию с управлением сессиями) [47, 52, 98, 102]	Cross Layer ACOR (Cross Layer Admission Control enabled On-demand Routing,	предоставление маршрута, удовлетворяющего двум критериям: доступной пропускной способности и задержки передачи пакета до узла назначения

Оценкой пригодности канала связи по его доступной пропускной способности является:

$$F_b = \frac{B}{B_{max} - (B_{res} + B)},$$

где B - запрашиваемая пропускная способность, B_{max} - максимальная пропускная способность канала связи, например, 2Мбит/с, 5Мбит/с, B_{res} - доступная пропускная способность.

Чтобы установить сессию передачи данных, протокол ACOR проверяет неравенство

$$B_{res} + B \leq B_{max}.$$

Для оценки задержки передачи пакета протокол ACOR использует следующий алгоритм. Пакет "Hello" используется для оценки задержки до соседнего узла. Когда узел передает пакет Hello, он запускает локальный таймер $d_{scheduled}$ для ожидания подтверждения получения Hello от соседа. Поэтом узел-отправитель пакета Hello записывает время отправления своего пакета Hello, d_1. После приема подтверждения источник записывает вновь время получения d_2. Время d_1 - d_2 и есть время оборота пакета (RTT, Round trip time).

Однако, чтобы точно оценить задержку передачи авторы вводят фактор вероятности ошибки D_e, который сравнительно мал, и представляет задержку

на пребывание пакета в очереди на каждом перенаправляющем узле, время передачи пакета и время продвижения пакета. Поэтому оцениваемая задержка на узле *i* составляет D_i= RTT + D_e. Оценочная функция при этом:

$$F_d = \frac{D}{D_{max} - (\sum_{i=1}^{j} D_i + D)},$$

где D - оцененная задержка на следующем узле, D_{max} - верхняя граница задержки, поддерживаемой сессий данных, $\sum_{i=1}^{j} D_i$ - суммарная задержка от узла *i* до узла *j*. Кроме того, перед установлением сессии передачи данных необходимо проверить следующее неравенство:

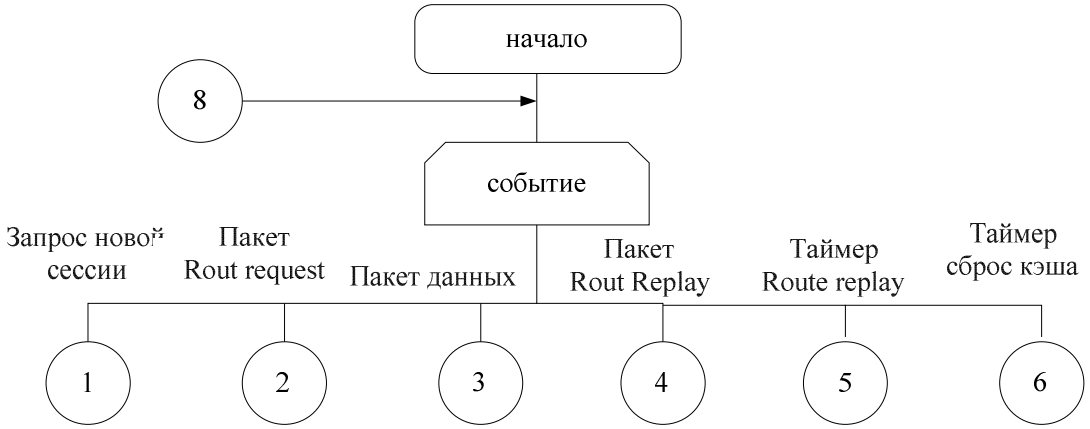
$$D_{max} \geq \sum_{i=1}^{j} D_i + D.$$

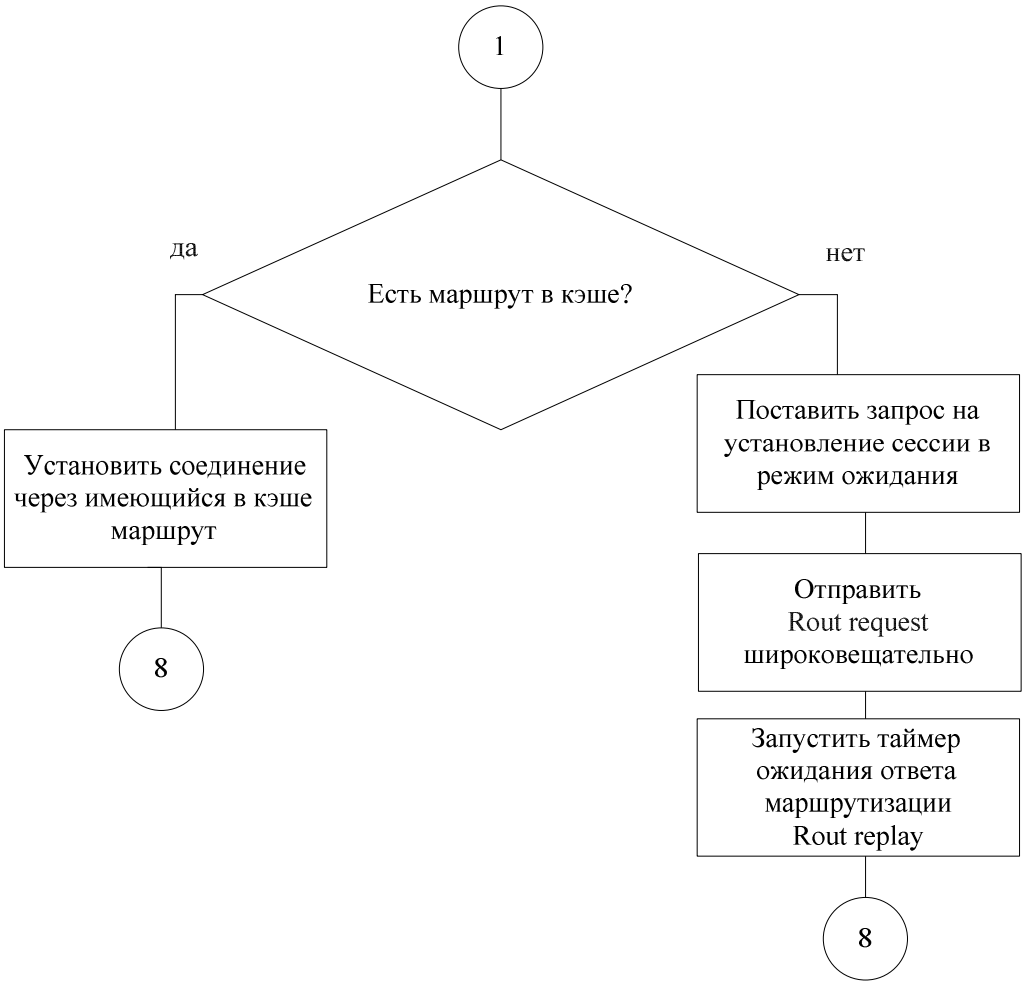
Полная функция оценки пригодности маршрута Fg является суммой функций Fb и Fd, и вычисляется на каждом узле, участвующим в процессе обнаружения маршрута. Высокое значение Fg говорит о том, что данный маршрут перегружен.

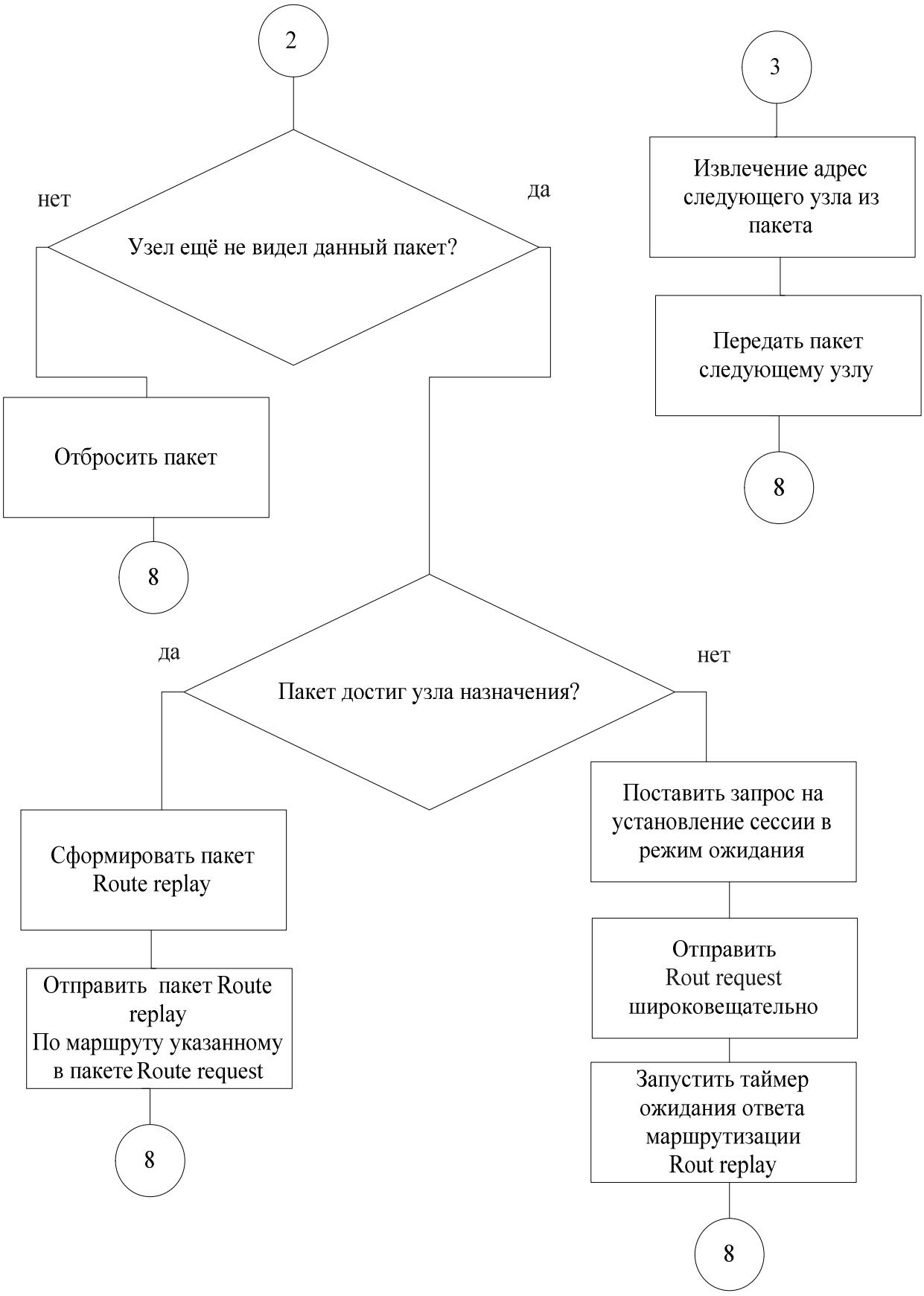
3.4.2. Разработка протокола маршрутизации для мобильной беспроводной ad hoc сети (MANET)

Разрабатываемая методика маршрутизации должна отвечать следующим требованиям, приведенным в [47,102].

Алгоритм работы предложенного протокола показан на рис.3.4.2. После включения питания узла запускается бесконечный цикл ожидания событий, относящихся к процессу маршрутизации, например, получение пакета или срабатывания установленного таймера. Для наших условий применительно к особенностям КИТС Йемена [61,62, 64-66] и конкретно в качестве примера на структуре ТГУ [83], нами разработан алгоритм:


начало
8
событие
Запрос новой сессии
Пакет Rout request
Пакет данных
Пакет Rout Replay
Таймер Route replay
Таймер сброс кэша
1
2
3
4
5
6


1
Есть маршрут в кэше?
да
нет
Установить соединение через имеющийся в кэше маршрут
8
Поставить запрос на установление сессии в режим ожидания
Отправить Rout request широковещательно
Запустить таймер ожидания ответа маршрутизации Rout replay
8


2
3
нет
да
Узел ещё не видел данный пакет?
Извлечение адрес следующего узла из пакета
Передать пакет следующему узлу
Отбросить пакет
8
8
да
нет
Пакет достиг узла назначения?
Сформировать пакет Route replay
Поставить запрос на установление сессии в режим ожидания
Отправить пакет Route replay По маршруту указанному в пакете Route request
Отправить Rout request широковещательно
Запустить таймер ожидания ответа маршрутизации Rout replay
8
8

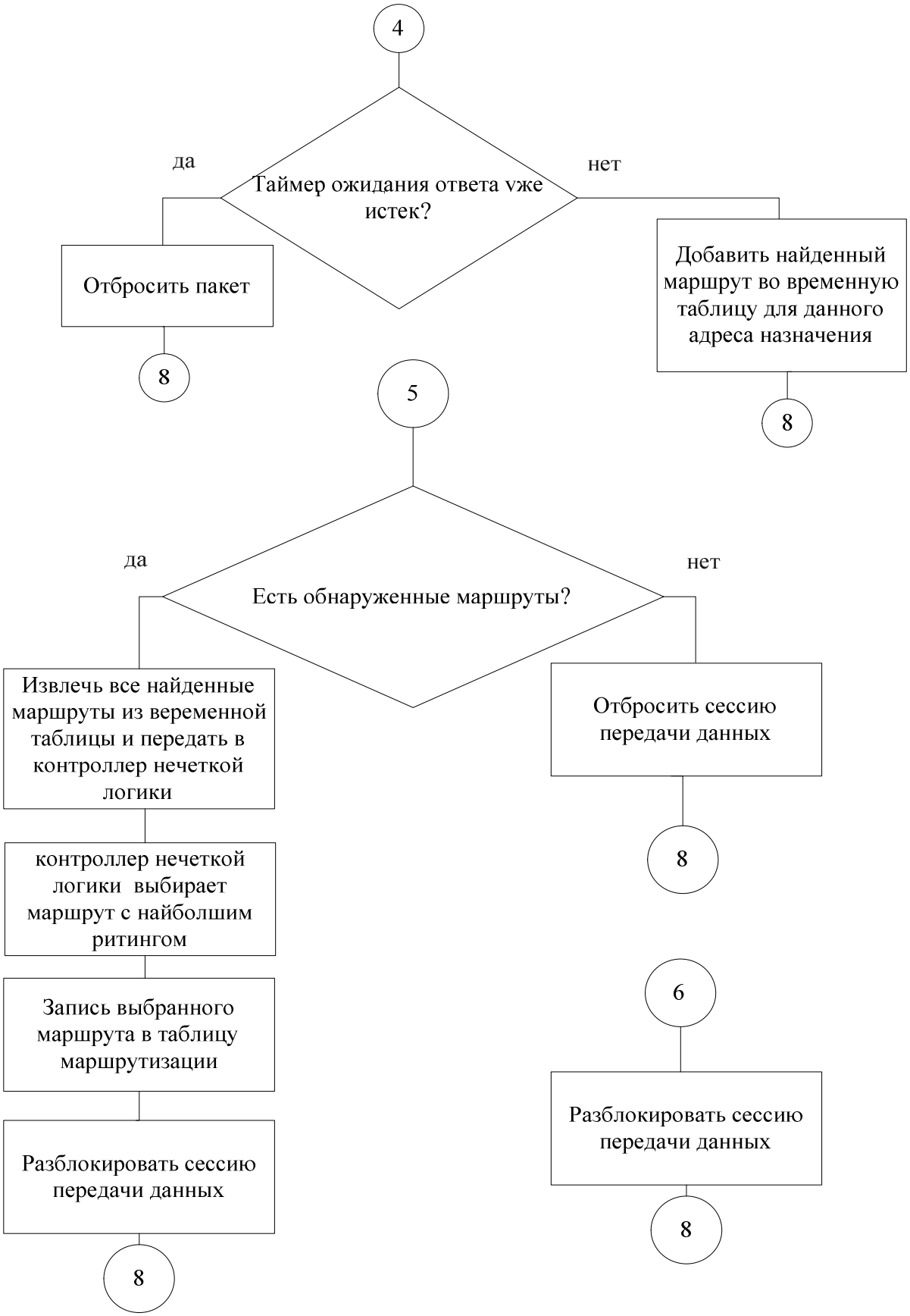


Рис. 3.4.2. Алгоритм работы предложенного протокола для ТГУ.

3.4.3. Аппарат нечеткой логики

Правила нечеткой логики в нашем случае выглядят следующим образом[17,21,23,24]. В качестве блока принятия решения по выбору оптимального маршрута и двух запасных маршрута предлагается использовать контроллер нечеткой логики.

3.4.4. Разработка блока принятия решения для метода маршрутизации на основе контроллера нечеткой логики

Таким образом, предлагаемая нами маршрутизация в MANET сетях состоит из двух компонент:

• На первом этапе разработанный реактивный протокол маршрутизации по требованию приложения запускает процедуру обнаружения возможных маршрутов до узла назначения, при этом контрольные пакеты маршрутизации также передают параметры состояния узлов и каналов связи и тоже передается степень изменение характеристики маршрута в обратном пути по сравнению с прямым путем (под изменению характеристики маршрута мы понимаем так, если пакет пришел в обратном пути быстрее чем в прямом пути значит характеристика маршрута улучается, в противном случае- ухудшается). После завершения данной процедуры (по таймеру) собранные данные подаются на вход контроллера нечеткой логики.

• На втором этапе для каждого из обнаруженных маршрутов проводится вычисление его рейтинга. Значения параметров состояния каждого маршрута подаются на вход контроллера нечеткой логики, который проводит фаззификацию всех значений и затем в соответствии с установленной базой правил выполняет операцию нечеткого вывода. На выходе контроллера мы получаем четкий (численный) рейтинг каждого маршрута. Маршрут с наибольшим рейтингом считается оптимальным.

• На третьем этапе из множества остальных маршрутов выбирается два маршрута с наибольшим рейтингом, которые и становятся запасными маршрутами.

В результате работы предлагаемого алгоритма, на этапе установления

соединения «по запросу» формируется три маршрута (один основной и два резервных). В процессе ведения информационного обмена осуществляется динамическая оценка рабочего маршрута.

В случае снижения характеристик основного маршрута ниже порогового значения из-за повышенной мобильности узлов или из-за плохих погодных условий, или в случае узел или часть узлов может покинуть маршрут осуществляется уточнение характеристик двух оставшихся (запасных) маршрутов и осуществляется выбор лучшего из них.

Если среди оставшихся (запасных) маршрутов не находится подходящего по качеству, осуществляется повторное (трех этапное) восстановление соединения.

Ниже будет рассмотрен предлагаемый контроллер нечеткой логики для метода маршрутизации: будут определены входные и выходные параметры, база правил нечеткого вывода и блок дефаззификации.

3.4.4.1 Входные параметры контроллера и блок фаззификации

Очевидно, что учет большего количества параметров состояния узлов и каналов связи позволяет лучше оценить картину распределения трафика в сети и выбрать более подходящий маршрут, в обход "заторов" в сети.

Прежде чем получить доступ к среде передачи, узел должен "прослушать" среду на предмет уже идущей передачи данных на данной частоте. Если среда свободна, узел пытается "захватить" частоту для передачи, используя механизм RTS-CTS, описанный в предыдущей главе. После этого узел захватывает среду для передачи данных, как показано на рисунке 3.4.3.

Время захвата среды $T_{occupation}$ для передачи блока данных равно:

$$T_{occupation} = T_{rts} + T_{cts} + \frac{L}{B} + T_{ack} + 3T_{sifs} + T_{difs} + T_{backoff} \qquad (3.4.1)$$

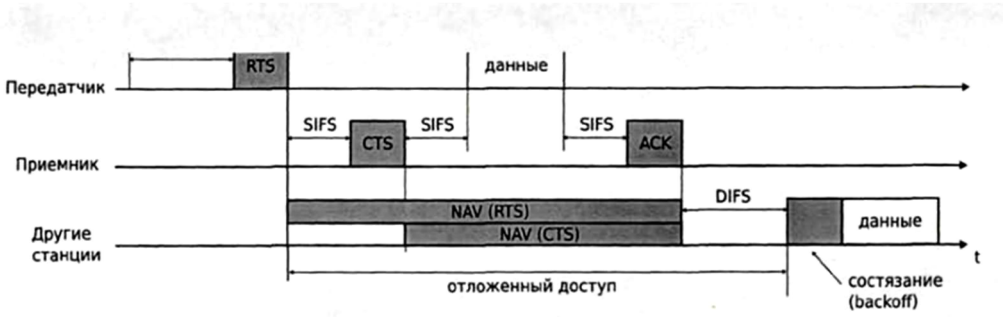


Рис. 3.4.3. Работа механизма RTS-CTS

Таким образом, доступная пропускная способность для узла составляет:

$$B_{res} = \frac{B_{nom} \cdot (T_{watch} - T_{busy} - T_{trans} - T_{recv} - T_{noisy})}{T_{watch}}, \qquad (3.4.2)$$

где -B_{res} - доступная пропускная способность канала, B_{nom} - номинальная пропускная способность канала, T_{watch} - период мониторинга состояния среды, T_{busy} - период занятости среды, T_{trans} - период передачи данных, T_{rec}, - период приема данных, T_{noisy} - период, когда сигнал детектируется, но не может быть декодирован.

Однако данная оценка является неточной по той причине, что она не учитывает интерференцию от соседних узлов. Рассмотрим ситуацию, изображенную на рис.3 4.4.

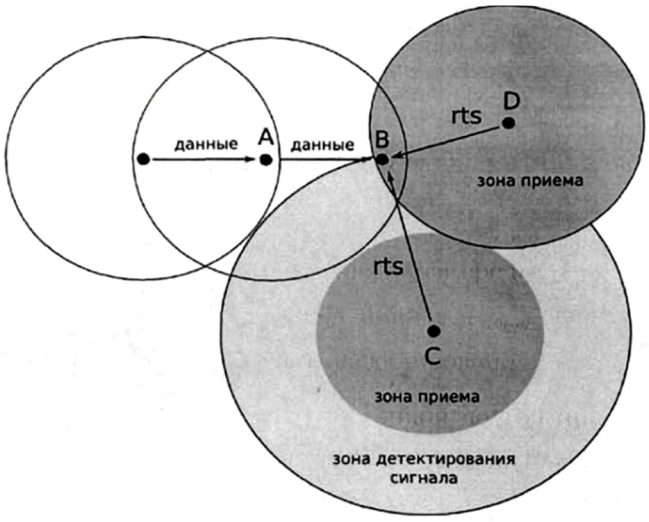


Рис. 3.4.4. Расчет доступной пропускной способности

Узел A в данном сценарии передает данные узлу B. Узел B может обмениваться данными с узлом D (оба узла находятся в зоне приема относительно друг друга), но может лишь детектировать сигналы от узла C (но не может с ним обмениваться данными). Если узел D начинает обмен данными с каким-нибудь узлом, он резервирует среду передачи данных через механизм RTS-CTS. Следовательно доступная пропускная способность канала связи между A и B вычисляется как:

$$B_{res} = \frac{B_{nom} \cdot (T_{watch} - T_{busy} - T_{trans} - T_{recv} - T_{noisy} - T_{node-noisy})}{T_{watch}}, \qquad (3.4.3)$$

Пусть маршрут состоит из n промежуточных узлов. Обозначим вместительность пакетного буфера *i*-того узла B_i, текущее количество пакетов в буфере - N_i. Тогда загруженность буфера *i*-того узла составляет:

$$l_i = \frac{N_i}{B_i} . \qquad (3.4.4)$$

Суммарная загруженность буферов на маршруте выражается как:

$$L = \sum_{i=1}^{n} l_i . \qquad (3.4.5)$$

Весовой коэффициент для загруженности каждого узла в отдельности в составе суммарной загруженности:

$$\lambda_i = \frac{l_i}{L} . \qquad (3.4.6)$$

Относительная загруженность пакетных буферов узлов на маршруте вычисляется как:

$$\overline{l} = \sum_{i=1}^{n} l_i * \lambda_i . \qquad (3.4.7)$$

Предлагаемая оценочная функция позволяет учитывать относительную загруженность пакетного буфера каждого из узлов на маршруте. Например для ТГУ (см. приложения), пусть маршрут состоит из четырех узлов и оценка загруженности маршрута даст следующее (табл.3.4.1):

Таблица 3.4.1

узел	1	2	3	4	
l_i	0.9	0.2	0.1	0.1	L=1.3
λ_i	0.69	0.15	0.08	0.08	
$l_i * \lambda_i$	0.621	0.03	0.008	0.008	$\overline{l}$ =0.668

Для сравнения среднее значение загруженности пакетных буферов дало бы значение $\frac{0.9+0.2+0.1+0.1}{4}=0.325$. Предлагаемая же оценочная функции отражает тот факт, что пакетный буфер одного из узлов практически полный.

Скорость изменения характеристики обратного пути по сравнению с прямым путем. Под изменению характеристики маршрута мы понимаем: если пакет пришел в обратном пути быстрее чем в прямом пути, это значит характеристика маршрута улучается, в противном случае - ухудшается. Это параметр учитывается в момент принятия решения выбора оптимального маршрута.

Количество промежуточных узлов. При прочих равных условиях более короткие маршруты могут оказаться предпочтительнее, поскольку передача через меньшее количество узлов оказывает меньшее влияние на текущую картину передачи радиосигналов между узлами сети. Данный параметр является аддитивным, его значение легко вычислить, поскольку ответ маршрутизации содержит список всех- промежуточных узлов до узла назначения.

Таким образом, было выделено множество из пяти параметров состояния узлов и каналов связи, по которым оценивается пригодность того или иного маршрута для передачи данных. В результате, после получения узлом источником ответа маршрутизации, значения перечисленных параметров извлекаются из пакета и подаются на вход контроллера нечеткой логики. Поскольку мы не получаем зашумленные данные на входе (нет аналоговых преобразований), в блоке фаззификации используется метод синглтон.

В качестве функций принадлежности для каждого терма всех лингвистических переменных мы выбираем треугольные функции принадлежности, поскольку, как показывает практика и исследования и опыт нашего внедрения [21,102,106], они хорошо подходят для использования при решении широкого круга проблем управления.

На рисунке(3.4.5) показан пример построения функций принадлежности для всех термов лингвистической переменной "Загруженность пакетного буфера узла".

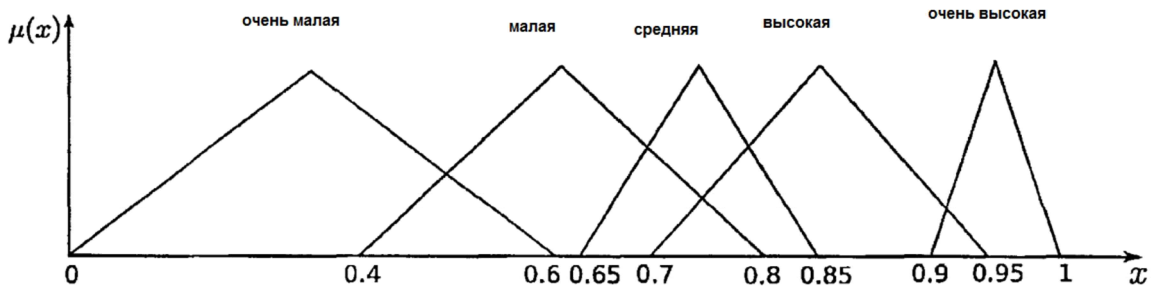


Рис.3.4.5. пример функций принадлежности термов переменной “Загруженность пакетных буферов”

На выходе контроллера нечеткой логики мы получаем точный рейтинг маршрута, который получается в результате операции дефаззификации выходного нечеткого множества. В качестве Т-нормы будем использовать операцию minimum, в качестве S-нормы - операцию maximum:

$$\mu_A(x) *^T \mu_B(x) = \min(\mu_A(x), \mu_B(x)). \qquad (3.4.8)$$

$$\mu_A(x) *^S \mu_B(x) = \max(\mu_A(x), \mu_B(x)). \qquad (3.4.9)$$

Правило нечеткой импликации мы задаем правилом Мамдани:

$$\mu_{A\to B}(x,y) = \mu_R(x,y) = \mu_A(x) \cap \mu_B(y) = \min(\mu_A(x), \mu_B(y)),$$

Где А и В- нечеткие множества $A \subseteq X, B \subseteq Y,$ отношение R определено на X x Y.

Поскольку на выходе блока выработки решения мы получаем одно нечеткое множество $\overline{B}^k \subseteq Y$ (рейтинг маршрута), то нечеткий вывод определяется таким образом:

$$\begin{aligned}
&\textit{Условие}:\ X=(x_1,x_2,x_3,x_4,x_5)^T \textit{ это } A'\\
&A'=A'_1\times(A'_2\times A'_3\times A'_4\times A'_5)\\
&\textit{Импликация}:\bigcup_{k=1}^{N}R^{(k)},R^{(k)}:A^{(k)}\to B^{(k)}\\
&\textit{вывод}: y \textit{ это } B',
\end{aligned} \qquad (3.4.10)$$

где $\bar{x}_1$, $\bar{x}_2$, $\bar{x}_3$, $\bar{x}_4$, $\bar{x}_5$ соответственно входные переменные (доступная пропускная способность, задержка передачи пакета, загруженность пакетных буферов, качество связи, количество промежуточных узлов), $R^{(k)}$, k = 1...N

- правила нечеткого вывода, B' - выходное нечеткое множество, определяющее рейтинг маршрута. Количество правил в базе правил составляет, как уже было указано выше, 3125.

Таким образом, выходной рейтинг' маршрута вычисляется как:

$$B'=A'\circ\bigcup_{k=1}^{N}R^{(K)} \qquad (3.4.11)$$

Так как правило нечеткой импликации мы определили Т-нормой типа min, то выполняется:

$$B'=A'\circ\bigcup_{k=1}^{N}R^{(K)}=\bigcup_{k=1}^{N}R^{(K)}\circ A' \qquad (3.4.12)$$

Следовательно, функция принадлежности нечеткого множества B' равна:

$$\mu_{B'}(y)=\max_{k=1\ldots N}\mu_{\bar{B}^k}(y), \qquad (3.4.13)$$

Таким образом, на вход контроллера нечеткой логики подается сигнал $\bar{x}=(\bar{x}_1$, $\bar{x}_2$, $\bar{x}_3$, $\bar{x}_4$, $\bar{x}_5)$. Исходя из (3.4.13), получаем:

$$\mu_{\bar{B}^k}(y)=\mu_{A^{(k)}\to B^{(k)}}(\bar{x},y)=\mu_{(A_1^k\times A_2^k\times A_3^k\times A_4^k\times A_5^k)\to B^k}(\bar{x}_1,\bar{x}_2,\bar{x}_3,\bar{x}_4,\bar{x}_5,y) \qquad (3.4.14)$$

Так как в качестве нечеткой импликации мы используем правило типа minimum, а декартово произведение нечетких множеств задается также операцией minimum, получаем:

$$\begin{aligned}
&\mu_{\bar{B}^k}(y)=\min[\mu_{(A_1^k\times A_2^k\times A_3^k\times A_4^k\times A_5^k)}(\bar{x}_1,\bar{x}_2,\bar{x}_3,\bar{x}_4,\bar{x}_5,\mu_B^k(y)]=\\
&\min[\mu_{A_1^k}(\bar{x}_1),\mu_{A_2^k}(\bar{x}_2),\mu_{A_3^k}(\bar{x}_3),\mu_{A_4^k}(\bar{x}_4),\mu_{A_5^k}(\bar{x}_5),\mu_B^k(y)]
\end{aligned}, \qquad (3.4.15)$$

В результате, используя выражение (3.4.13), получаем:

$$\mu_{B'}(y)=\max_{k=1\ldots N}\{\min[\mu_{A_1^k}(\bar{x}_1),\mu_{A_2^k}(\bar{x}_2),\mu_{A_3^k}(\bar{x}_3),\mu_{A_4^k}(\bar{x}_4),\mu_{A_5^k}(\bar{x}_5),\mu^k{}_B(y)]\}, \qquad (3.4.16)$$

На рис.3.4.6 представлена графическая интерпретация полученного выражения нечеткого вывода (для наглядности используются только две переменные x_1 и x_2 и два правила нечеткого вывода).

Ранее было установлено, что функции принадлежности входных и выходных переменных являются симметричными треугольными функциями принадлежности (рис.3.4.6).

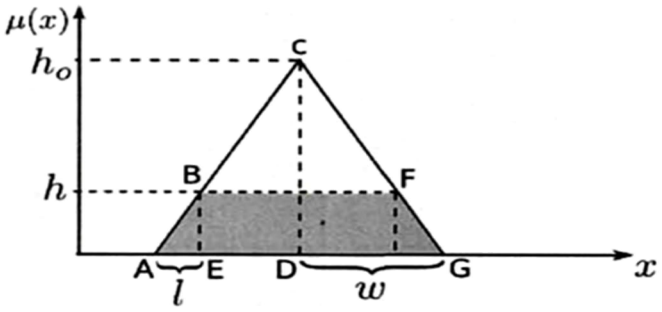


Рис. 3.4.6. Вычисление площади фигуры, образованной выходным нечетким множеством

На рис.3.4.7 показана структура разработанного контроллера нечеткой логики для предлагаемого метода маршрутизации.

Рис. 3.4.7. Разработанный контроллер нечеткой логики

Таким образом, мы определили общую (неизменяемую) структуру контроллера и его настраиваемые параметры (параметры функций принадлежности и значения выходной переменной для всех правил нечеткого вывода).

От настраиваемых параметров и зависит, как метод маршрутизации на основе представленного контроллера нечеткой логики будет функционировать в той или иной ситуации.

В ходе внедрения в ТГУ нами было проверено эффективность

нескольких подходов.

Безотказность и аутентификации отправителя за счет использования тройного DES и RSA, хотя следует учитывать с помощью SHA-256 для проверки сообщений в будущих версиях. Что касается технической возможности, TSIK, как представляется, жизнеспособным и конкурентоспособным вариантом в защите веб-основе бизнес-взаимодействия.

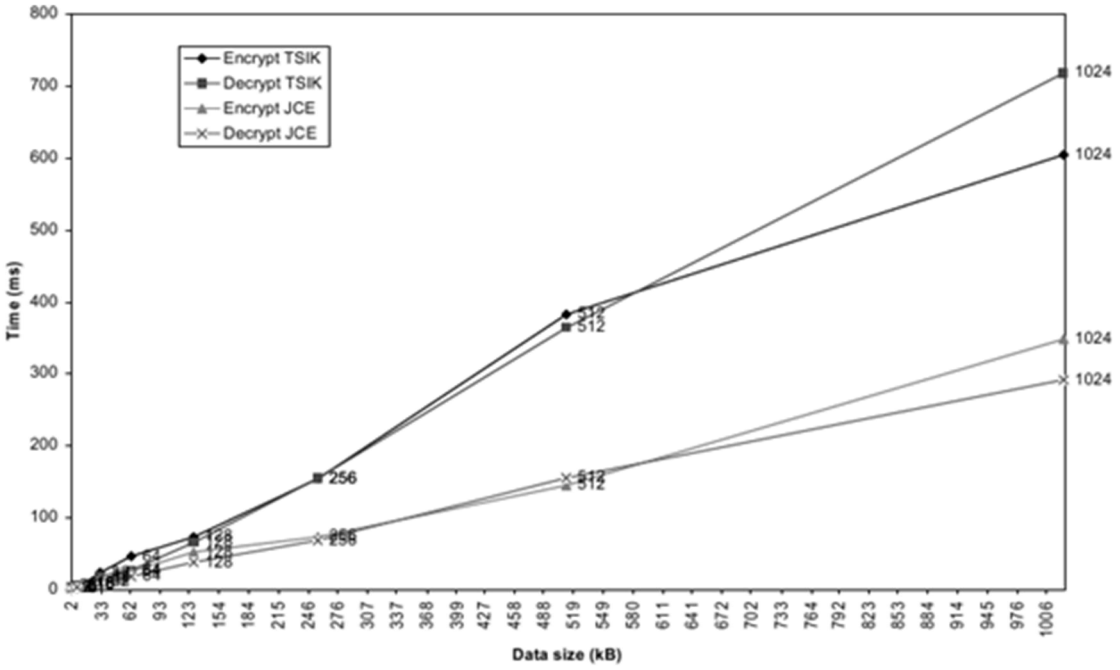


Рис.3.4.8. Вариант DES: время шифрования

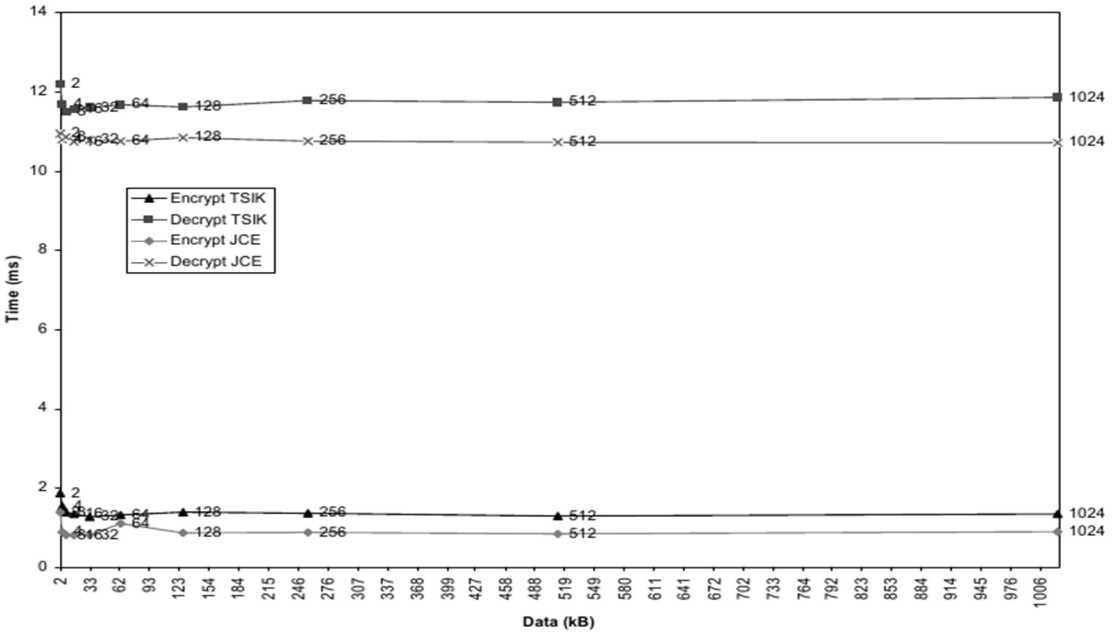


Рис.3.4.9. RSA-1024 время шифрования 168 битным ключом DES

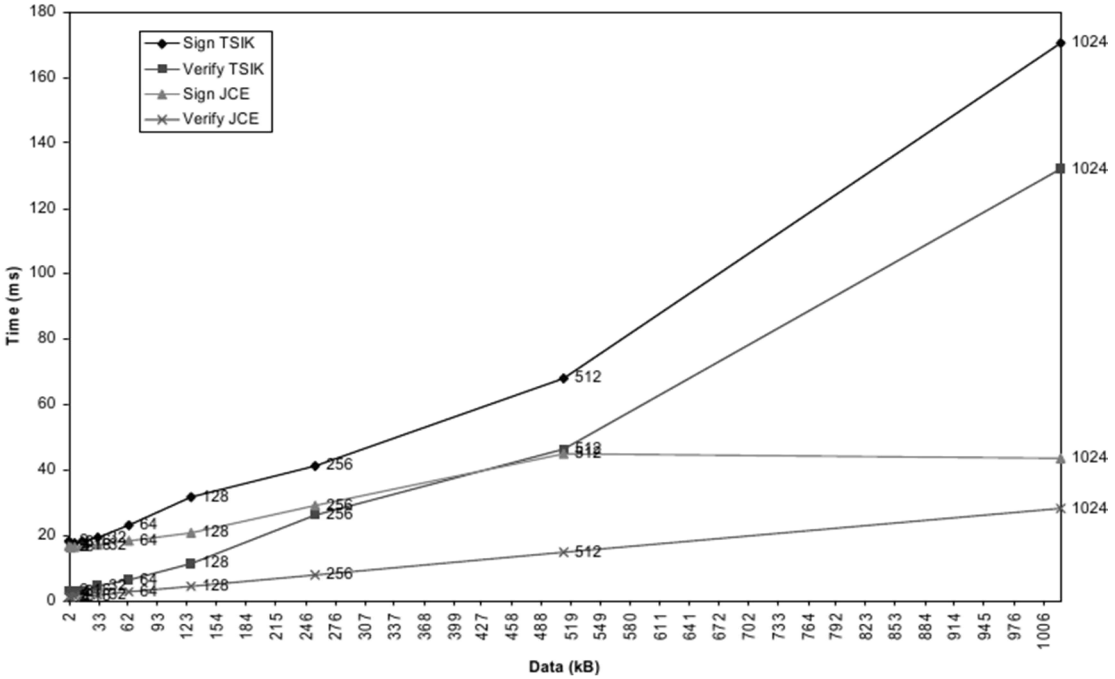


Рис.3.4.10. Проверки (с использованием SHA-1 и RSA-1024)

Для расчетов элементов нечеткой логики нами разработана программа:

```
procedure pursue(var f_objec:word_string);
        var
        f_value:word_string;
        curr_objec:objec_ptr;
        curr_value:value_ptr;
        curr_rule:rule_ptr;
        curr_prem:prem_ptr;
        bad:boolean;
        solved:boolean;
        lowest:integer;
 begin
  curr_objec:=find_objec(f_objec);
  if curr_objec=NIL then
  begin
   make_node(curr_objec);
  end;
  curr_objec^.objecx:=f_objec;
```

```
if(curr_objec^.sought<>TRUE) then
begin
 solved:=FALSE;
 curr_objec^.sought:=TRUE;
 curr_rule:=find_rule(f_objec,top_rule);
 while ((curr_rule<>NIL) and (ok_add(f_objec,DEFINITE)=TRUE)) do
 begin
  curr_prem:=curr_rule^.prem;
  bad:=FALSE;
  lowest:=DEFINITE;
 while ((curr_prem<>NIL) and (bad=FALSE)) do
  begin
   pursue(curr_prem^.objecx);
   curr_value:=test(curr_prem^.objecx,curr_prem^.value);
   if curr_value=NIL
     then bad:=TRUE
     else if curr_value^.cert<lowest
          then lowest:=curr_value^.cert;
    curr_prem:=curr_prem^.next
  end;
  if (bad=FALSE) then
   begin
    if(explain=TRUE) then
           explain_how(curr_rule);
    conclude(curr_rule,lowest);
    solved:=TRUE;
   end;
  curr_rule:=find_rule(f_objec,curr_rule^.next);
 end;
 if (solved=FALSE) then
```

```
    begin
      if(explain<>TRUE) then
            explain_why(f_objec);
     ask(f_objec,f_value);
     add_objec(f_objec,f_value);
     add_cf(f_objec,f_value,DEFINITE);
    end;
  end;
end;{pursue}
```

Все наши методики при внедрении в ТГУ (см. приложения) мы учли в табл. 3.4.2.

Таблица 3.4.2. Параметры КИТС ТГУ с учетом применения разработанных нами методик

КИТС ТГУ	С использованием наших методик	Время проектирования, дней	Число проникновений в месяц
«кадры»		9	15
«финансы»	«финансы»	3	1
«студент»		10	21
«СДО»		3	2
«документооборот»		12	8
«логистика»		15	11
«капитальное строительство»		12	7

Среднее число проникновений в месяц

Пр =(15+1+21+2+8+11+7) / 7 = 9,3.

Среднее время проектирования КИТС, дней

Вр =(9+3+10+3+12+15+12) / 7 = 9,1.

Эти методики, программы и ключи проверены нами при внедрении в ТГУ (см. приложения) и позволила сократить время проектирования КИТС

«Финансы» в 3 раза и увеличить эффективность защиты уменьшением числа проникновений в 9 раз.

Выводы по главе 3

1. Рассмотрены разновидности множественного доступа в беспроводных сетях, разработаны нечеткий алгоритм управления доступом в КИТС и методики применения нечеткой логики для управления множественным доступом.
2. Нами предложена методика проектирования защищенной сети на аппарате нечеткой логики и разработана программа для облегчения расчетов.
3. Эта методика и программа проверены нами при внедрении в ТГУ и позволила сократить время проектирования сети в 3 раза и увеличить эффективность защиты уменьшением числа проникновений в 9 раз.

Заключение

1. Показаны главные трудности при эксплуатации КИТС в Йемене и необходимость разработки инженерных методик по защите информации.

2. Рассмотрены основные подходы к информационной защите КИТС в Йемене.

3.Корпоративные сети ВУЗа является важнейшей составляющей общей информационной системы и наиболее информационно емкой.

4.Для эффективного управления сетью необходимо стремиться к централизации информационных ресурсов в рамках предприятия. Распыленность указанных ресурсов по различным подразделениям может привести к разрывам информационных потоков.

5. Проведена оценка достоверности функционирования отказоустойчивого запоминающего устройства при информационной защите телекоммуникаций и обосновано применение малоразрядных кодов в КИТС Йемена, что дало увеличение достоверности на 70%.

6. Разработан алгоритм для системного уровня проектирования защищенных сетей, что позволило уменьшить время проектирования в 3 раза.

7. Предложен выбор рациональной информационной защиты КИТС Йемена с криптографией, что позволило уменьшить число проникновений в 4 раза.

8. Рассмотрены разновидности множественного доступа в беспроводных сетях, разработаны нечеткий алгоритм управления доступом в КИТС и методики применения нечеткой логики для управления множественным доступом.

9. Предложенная нами методика проектирования защищенной сети на аппарате нечеткой логики проверена при внедрении в ТГУ и позволила сократить время проектирования сети в 3 раза и увеличить эффективность защиты уменьшением числа проникновений с криптографией в 9 раз.

Литература

1. Аль-Агбари Мохаммед. Защита телекоммуникаций систем дистанционного обучения Йемена от несанкционированного доступа к информации// Диссертация на соискание ученой степени кандидата технических наук/ Научный руководитель: Доктор технических наук, профессор Галкин А.П./ Владимирский государственный университет. г. Владимир-2008 – 170 с.
2. Галкин А.П. Проектирование эффективной сети связи с учетом срывов.\ Проектирование и технология электронных средств.-2003-№1, с.9-11.
3. Галкин А. П. Целесообразность информационной защиты предприятия./ Материалы 3-ей Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир, 1999, с.64-67.
4. Галкин А.П. Защита каналов связи предприятий и учреждений от несанкционированного доступа к информации./Уч. пос.- Владимирский государственный университет.- г. Владимир-2003. 126 с.
5. Галкин А.П. Радиосистемы для защиты каналов связи от несанкционированного доступа к информации./Уч. пос.- Владимирский государственный университет.- г. Владимир-2003. 104 с.
6. Галкин А. П. Оценка необходимости защиты информации предприятия.«Вестник ассоциации Русская оценка»,1999-1, с.55-58.
7. Галкин А. П. Зависимость эффективности сети связи от срывов. / Материалы 4-ой Международной НТК «Перспективные технологии в средствах передачи информации», г. Владимир-Суздаль, 2001, с.72-77.
8. Галкин А.П., Аль-Муриш Мохаммед, Тахаан Осама. Обнаружения атак и нарушений в корпоративной сети./ Экономические проблемы ресурсного обеспечения инновационного развития региона. Матер.междунар. научн. конф. Владимир, 2009. С.15-19.
9. Галкин А.П., Аркадьева М.С., Тахаан Осама. Кризис, безработица и информационная безопасность предприятия./ Экономические проблемы

ресурсного обеспечения инновационного развития региона. Матер.междунар. научн. конф. Владимир, 2009. С.20-24.

10. Галкин А.П., Тахаан Осама. Информационная защита корпоративной сети системой обнаружением атак с нечеткой логикой./ Известия института инженерной физики. 2009-№4. С. 2-4.
11. Галкин А.П., Тахаан Осама. Выбор комплекса защиты информации для корпоративных информационно-телекоммуникационных сетей./ Известия института инженерной физики. 2010-№2. С. 2-6.
12. Гришин В.Ю., Зубов Н.Н., Смаглий А.М. Принципы построения перспективных отказоустойчивых бортовых вычислительных систем управления космическими аппаратами с длительным сроком активного существования // Сборник докладов международной НТК “ Актуальные проблемы анализа и обеспечения надежности и качества приборов, устройств и систем”, Пенза, 1998, С. 22-23.
13. Галкин А.П. Информационная безопасность и целесообразные пути ее улучшения/ Palmarium Academic Publishing - Saarbrucken, Deuchland - 2014.75 с.
14. Дементьев В.А. Комплексное проектирование систем управления и контроля ЛА. М.: Машиностроение,1980. 256 с.
15. Авакян А.А., Искандаров Р.Д. Супернадежный высокопроизводительный вычислитель для бортовых автоматов// Информационные технологии в проектировании и производстве. 1996, вып.1- 2. С. 24-32.
16. Амато В. Основы организации сетей Cusco, том 1.-М.; Издательский дом “Вильямс”, 2002, 512 с.
17. Аль-Муриш Мохаммед Хашим. Повышение эффективности информационной защиты корпоративных телекоммуникационных сетей Йемена**//** Диссертация на соискание ученой степени кандидата технических наук/ Научный руководитель: Доктор технических наук, профессор Галкин А.П./ Владимирский государственный университет. г. Владимир-2009 – 170 с.

18. Барановская Т.П., Лойко В.И., Семенов М.И., Трубилин А.И. Архитектура компьютерных систем и сетей. - М.: Финансы и статистика, 2003, 256 с.
19. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации./ Учебник для вузов. 2-е изд. - СПб.: Питер, 2006, - 703 с
20. Бройдо В. Вычислительные системы, сети и телекоммуникации. / Учебник для вузов. 3-е изд.- СПб.: Питер, 2008, -768 с.
21. Блейхут Р. Теория и практика кодов контролирующих ошибки. М.: Мир, 1986, 522 с.
22. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971, 346 с.
23. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды. М.: Связь,1976, 410 с.
24. Блох Э.Л., Зяблов В.В. Линейные каскадные коды. М.: Наука, 1982, 350 с.
25. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986, 576 с.
26. Гост 27.002-89, Надежность в технике. Термины и определения. - М.: Стандарты, 1989.
27. Казарин О.В., Лагутин В.С., Петраков А.В. Защита достоверных цифровых электрорадио сообщений. Учебное пособие.-М,: РИО МГУ СИ, 1997. - 68 с.
28. Калинцев Ю.К. Криптозащита сообщений в системах связи. Учебное пособие.-М.: МТУСИ, 2000.- 236 с.
29. Кнопелько В.К., Лосев В.В. Наднжное хранение информации в полупроводниковых запоминающих устройствах.М.:Радио и связь,1987,238 с
30. Лонгботом Р. Надежность вычислительных систем. М.: Энергоатомиздат, 1985, 284 с.
31. Мак-Вильямс Ф.Дж., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. М.: 1979. 156 с.
32. Максимов Н.В. Компьютерные сети. М.: изд. Форум, 2007, 448 с.
33. Мырова Л.О., Чпиженко А.З. Обеспечение стойкости аппаратуры связи к

ионизирующим и электромагнитным излучениям. М.: Радио и связь, 1988. 296 с.

34. Мырова Л.О., Попов В.Д. Анализ стойкости систем связи к воздействию излучений. М.: Радио и связь, 1993. С.21-28.
35. Мур М, Притск Т., Риггс К., Сауфвик П. и др. Телекоммуникации. СПб.: БХВ - Петербург, 2005. - 624 с.
36. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.: Мир, 1976, 380 с.
37. Поваляев Э.И., Щербаков Ю.И. Аппаратно-ориентированный метод решения системы уравнений двоичных кодов БЧХ для процедуры параллельной коррекции трехкратных ошибок. // Автоматика и вычислительная техника. 1987. № 3. С. 66-71.
38. Половко А.М. Основы теории надежности. М.: Наука, 1964, 356 с.
39. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы сети и телекоммуникации./Учебник для ВУЗов. М.; Финансы и статистика, 2003, 560 с.
40. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях,-М.:Радио и связь,1999.-328 с.
41. Дементьев В.А., Крылов Л.Н., Осипов В.П. и др. Теория и синтез дискретных автоматов. М.: МО СССР, 1979.379 с.
42. Денисова А., Вихарев И., Белов А., Наумов Г. Интернет. 2-е изд. – СПб. Питер. 2004.– 368 с.
43. Давыдов А.А., Дрожжина-Лабинская А.Ю. Дополнительные корректирующие возможности кодов БЧХ, исправляющих двойные и обнаруживающие тройные ошибки. // Вопросы кибернетики. Комплексное проектирование элементно-конструкторской базы супер-ЭВМ. М.: ВИНИТИ, 1988. С. 86-112.
44. Доманицкий С.М. Построение надежных логических устройств. М.: Энергоатомиздат, 1986, 480 с.

45. Дружинин Г.В. Надежность автоматизированных производственных систем. М.: Энергоатомиздат, 1986, 480 с.

46. Дж. Уолренд Телекоммуникационные и компьютерные сети. М.: Постмаркет. 2001, 480 с.

47. Закон Российской Федерации "Об оперативно-розыскной деятельности в РФ", 1992.

48. Емелин Н.М., Новиков Н.Н., Павлов А.А. и др. Принцип агрегатно-модульной адаптации интеллектуальных систем к контролю технического состояния сложных объектов. // Измерительная техника. 1999, № 5. С. 43-46.

49. Зайцев Г.В., Зиновьев В.А., Семаков Н.В. Коды с минимальной плотностью проверок для исправления байтовых ошибок, стираний, дефектов. // Проблемы передачи информации. 1983. Т. 19. № 3. С. 29-37

50. Защита от несанкционированного доступа к информации. Термины и определения. Руководящий документ Гостехкоммиссии России. М.: Военное издательство, 1992.

51. Обухов В.Е., Павлов В.В. Синтез избыточных дискретных устройств с реконфигурацией структуры. Киев: Наукова думка,1979,154 с.

52. Олифер В.Г, Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. СПб. Питер, 2004– 864 с.

53. Пархоменко П.П. Основы технической диагностики. Кн. 1.-М.: Энергия, 1976. 464 с.

54. Павлов А.А. Повышение достоверности функционирования микропроцессорных средств измерительной техники. // Измерительная техник. 1999, №4. С. 28-33.

55. Павлов А.А. Повышение достоверности функционирования устройств памяти ЭВМ на основе использования корректирующих кодов с апостериорной коррекцией ошибок.// КомпьюЛог. 1998, № 5,6 (29,30) С. 6-9.

56. Павлов А.А., Кузнецов А.Н. Метод построения отказоустойчивых

дискретных устройств на основе корректирующих кодов повышенной обнаруживающей способности. // КомпьюЛог. 1998, № 4(28) С. 49-51.

57. Павлов А.А., Павлов А.А. Концептуальные основы построения отказоустойчивых запоминающих устройств с апостериорной коррекцией ошибок. // КомпьюЛог. 1999, № 1(31) С. 34-37.
58. Павлов А.А., Гориш А.В., Милов Ю.Г. Метод защиты памяти ЭВМ на основе корректирующих кодов с апостериорной коррекцией ошибок // Экология, мониторинг и рациональное природопользование. Научн. тр. Вып. 302(11)-М.: МГУЛеса, 1999, С.259-264.
59. Петраков А.В. Основы практической защиты информации М.: Радио и связь, 1999.- 368 с.
60. Петров Б.М. Рассмотрение основных показателей радиационной стойкости, позволяющих анализировать безотказность микропроцессорных устройств при радиационном воздействии // Сборник докладов международной НТК “Актуальные проблемы анализа и обеспечения надежности и качества приборов, устройств и систем”, Пенза, 1998, С. 325-327.
61. http://www.yemen.gov.ye/portal/ .
62. http://www.cso-yemen.org/content.php?lng=arabic&id=296 .
63. http://taiz.edu.ye/ .
64. http://www.yemen-nic.info/sectors/information/ .
65. https://ru.wikipedia.org/wiki/%D0%99%D0%B5%D0%BC%D0%B5%D0%BD#.D0.9D.D0.B0.D1.81.D0.B5.D0.BB.D0.B5.D0.BD.D0.B8.D0.B5
66. http://www.post.ye/?page_id=127 .
67. Зыль С.Н. Повышение отказоустойчивости сетевых приложений реального времени./ Сети и системы связи. 2005, №6. с 33 -37.
68. Иванов М.А., Кларин А.П. Сигнатурный анализ в задачах контроля и диагностики цифровых устройств. М.: Изд. МИФИ, 1986, 26 с.
69. Иуыду К.А. Надежность, контроль и диагностика вычислительных машин и систем. М.: Высшая школа, 1989, 215 с.

70. Каган Б.М., Мкртумян И.Б. Основы эксплуатации ЭВМ. М.: Энергоатомиздат, 1988, 430 с.

71. Щербаков Н.С. Самокорректирующееся дискретные устройства. М.: Машиностроение, 1975, 214 с.

72. Щербаков Н.С. Достоверность работы цифровых устройств. М.: Машиностроение, 1989, 224 с.

73. Яблонский С. В. Введение в дискретную математику. М.: Наука,1979, 272 с.

74. Aichelmann F. J.Jr. Local paging memory buffer forminimizing Concurrence of hard and soft data errors. // IBM Tech. Disclosure Bull. 1980.№ 11. P. 4931-4932.

75. Blaum M. Systematic unidirectional burst detecting codes. //IBM RJ 5662 (57161), May 1987.

76. Bose B. On systematic SEC/MUED code. // Proc. FTCS. June 1981.V.11 P. 265-267.

77. Bose B. Systematic unidirectional error - detecting codes. //IEEE Trans. Computere. Nov. 1985. V.c-34 P. 1026-1032.

78. Chen C.L. Error correcting codes with Byte Error detection capability //IEEE Trans. Cjmpputere. July 1983. V.c-32 p. 615-621.

79. Libson M. R., Harvey H.E. A general-purpose memory reliability simulation. // IBM J. Res. Develop. 1984/ v.28. P. 196-206.

80. Meyer J.F., Wei L. Influence of workload on error recovery in random access memories. // IEEE Trans. Comput. 1988. V.37.№4. P, 500-507.

81. Nrener R., Fujiwara E., Agarwal V.K. Low Overhead, High Coverage Built-in Self-Test PLA Desidn/FTCS-15. 1985. P. 37-41.

82. Руководство по поиску неисправностей в объединенных сетях Cusco Systems. М.: Издательский дом “Вильямс”, 2003, 1040 с.

83. Саголович Ю.Л. Кодовая защита оперативной памяти ЭВМ от ошибок.// Автоматика и телемеханика, 1991, № 5, С. 4-40.

84. Сапожников В.В., Сапожников В.В, Методы синтеза надежных автоматов. Л.:Энергия, 1980, 94 с.

85. Хорев А.А. Способы и средства защиты информации.- М.: МО РФ,2001.- 316с.

86. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1.Технические каналы утечки информации. Учебное пособие.М.:Гостехкомиссия РФ, 1998-320 с.

87. Согомонян Е.С., Слабоков Е.В. Самопроверяемые устройства и отказоустойчивые системы. М.: Радио и связь, 1989, 207 с.

88. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Термины и определения. Руководящий документ Гостехкоммиссии России. М.: Военное издательство, 1992.

89. Самофалов К.Г., Корнейчук В.И., Городний А.В. Структурно-логические методы повышения надежности запоминающих устройств. М.: Машиностроение, 1976, 350 с.

90. Суворов А.Б. Телекоммуникационные системы, компьютерные сети и Интернет./Учебное пособие для вузов. М.: Феникс, 2007, 384 с.

91. Терминологический словарь «Бизнес-Безопасность-Телекоммуникации» - Учебное пособие / Составители А.А.Аржанов, Е.Г.Новикова, А.В.Петраков, С.В. Рабовский.- М.: РИО МТУСИ, 2000.- 304 с.

92. Толстяков В.С. Обнаружение и исправление ошибок в дискретных устройствах. М.: Советское радио,1972, 288 с.

93. Шеннон К. Работы по теории информации и кибернетике. -М.: ИИЛ, 1963.- 829 с.

94. Халяпин Д. Б., Ярочкин В. И. Основы защиты промышленной и коммерческой информации. Термины и определения. М.: ИПКИР, 1994, 231 с.

95. Хетагуров Я.А., Руднев Ю.Л. Повышение надежности цифровых устройств методами избыточного кодирования. М.: Энергия,1974, 370 с.

96. Хестер Н. Frontpage 2002 для Windows: Пер. С англ. - М.: ДМК Пресс, 2002. – 448с.

97. Аль-Джабери Р.Х. Проблемы информационной безопасности и инновационные пути их решения/ Галкин А.П., Дарахма И., Альджарадат М.М. //«Инновационные развития экономики – основа устойчивого развития территориального комплекса»Матер. Всероссийской научн. прак. конф. Владимир- Москва, 2012. С.172-176.

98. Аль-Джабери Р.Х. Достоверность функционирования отказоустойчивого запоминающего устройства при информационной защите с итеративным кодом / Галкин А.П., Бадван Ахмед,Обади Хезам,// Труды X Международной научной конференции «Перспективные технологии в средствах передачи информации»/ Владимир-Суздаль, 2013 г., кн. 2, с. 49-52.

99. Аль-Джабери Р.Х. Технико- экономическое обоснование сетей для развития регионов республики Йемена / Галкин А.П., Обади Хезам., Бадван Ахмед // 2-ой российский экономический конгресс/ г.Суздаль,18-22.02.2013. С. 109-111.

100. Al-Gaberi R.H. Projection Network-on-Chip as a System-on-Chip platform for safe information / Galkin A.P., Obadi H.M. Amro M.M.// INDIAN SCINCE CRUISER Volume 27 Number 6 November 2013. С. 35-38.

101. Аль-Джабери Р. Х. Проектирование медицинских защищенных сетей на системном уровне/ Галкин А.П. , Обади Х. М// МНК ФРЭМЭ-2014-Владимир-Суздаль, 1-3.07.2014. Том 2. С.152-154.

102. Аль-Джабери Р.Х. Системный уровень проектирования защищённых

сетей / Обади Х.М., Галкин А.П., Ковалёв М.С., Амро М.М.// Известия института инженерной физики.2013. №4. С. 10-12.

103. Аль-Джабери Р.Х. Выбор рациональной информационной защиты корпоративных сетей с криптографией/ Галкин А.П., Обади Х.М., Ковалёв М.С., Суслова Е.Г.// Известия института инженерной физики. 2014.№3(33), С. 7-12.

104. Аль-Джабери Р.Х. Выбор рациональной информационной защиты корпоративных сетей для улучшения конкурентоспособности/ Галкин А.П., Обади Хезам, Суслова Е.Г.// Известия ВУЗов/Технология текстильной промышленности. 2014. № 4(352), С. 135-137.

105. Аль-Джабери Рамзи. Когнитивное радио-важное направление в инновационном развитии здравоохранения / Галкин А.П., Бадван Ахмед, Обади Хезам// Труды X Международной научной конференции «Физика и радиоэлектроника в медицине и экологии»/ Владимир-Суздаль, 2012 г., книга 2, С. 176-178.

106. Аль-Джабери Р. Х. Выбор рациональной информационной защиты беспроводных сетей для улучшения конкурентоспособности// «обеспечение устойчивого развития регионально экономике в условиях инновационный модернизации производства», Владимир-2015г.

107. Аль-Джабери Р.Х. Нечеткий алгоритм управления множественным доступом в беспроводных корпоративных сетях/ Галкин А.П. // 3-я Международная молодежная научная конференция «Будущее науки – 2015»/ Юго-Западный государственный университет, г. Курск, 23-25 апреля 2015г.

108. Аль-Джабери Р.Х. Экспертные системы в экономике //5-я Международная научно-практическая конференция «актуальные вопросы развития современного общества»/ Юго-Западный государственный университет (г. Курск, Россия), апрель 2015г.

Приложения

Приложение 1. Йемен и его телекоммуникации

Йемен, Йеменская республика, государство на юго-западе Аравийского полуострова. Площадь Йемена 537 тыс. кв. км. Оно граничит на севере с Саудовской Аравией, а на востоке с Оманом. На юге Йемен омывается водами Аравийского моря и Аденского залива, а на западе – Красного моря . Йемену принадлежат острова Камаран, Перим, Сокотера и др. Йеменская республика была образована 22 мая 1990 в результате объединения Йеменской арабской республики (ЙАР, или Северный Йемен) и Народной Демократической Республики Йемен (НДРЙ, или Южный Йемен). Столица Сана.

Природные условия

Около 2/3 территорий Йемена – сильно пересеченная горная страна (Джабель), состоящая из высоких (до 2-3 тыс. м) плато, расчлененных глубокими долинами, и обрывающаяся на Западе и Юге многоступенчатым сильно эродированным уступом.

На территории Йемена находятся величественные горы, прибрежная низменность Тихама, засушливые пустынные плоскогорья, изредка разделенные более плодородными долинами. В стране осутствуют постоянные водотоки. Территория бывшей ЙАР занимает восточную, самую высокую часть Западно-Аравийского нагорья, которая представляет собой приподнятый, сильно расчлененный край Аравийского щита, частично перекрытый древними лавовыми отложениями. Низменность Тихама, шириной от 30 км до 80 км, сложена аллювиальными и щебнистыми отложениями. Равнина упирается в горы, круто поднимающиеся до высоты 2000-3000 м, где расположено обширное холмистое плоскогорье, пересеченное обычно сухими вади и высокими кряжами; здесь находится самая высокая точка страны – гора Эн-Наби-Шаиб (3660 м). Восточный склон Западно-Аравийского нагорья, обращенный к пустыне Руб-эль-Хали,

занимающей большую половину южной части Аравийского полуострова, более пологий, чем склон, обращенный к низменности Тихама, но более крутой, чем северный склон, обращенный к Неджу. Западная оконечность Руб-эль-Хали возвышается на 900-1200 м над уровнем моря.

Низменность Тихама – жаркий, засушливый район с редкой растительностью. Летние температуры здесь достигают 45 С; осадков выпадает от 150 мм до 400 мм в год. В горных долинах, спускающихся террасами к морю, осадки выпадают более регулярно и составляют более 500 мм в год. В высокогорьях выпадает до 1000 мм осадков. Восточная часть региона отличается засушливым климатом. Для плоскогорий в центре страны характерны теплое лето (до 33С) и прохладная сухая зима.

На территории бывшей НДРЙ большая часть ресурсов, в том числе сельскохозяйственные угодья, сосредоточены в районе Адена. Исключение составляет Хадрамаут, регион в восточной части страны, представляющий собой широкую долину – вади, протянувшуюся параллельно берегу и поворачивающую затем на юг, к морю. Прибрежная низменность на юге простирается на 5-65 км в глубину страны. Внутренняя часть региона представляет собой пересеченное плоскогорье, расчлененное долинами вади. Климат прибрежной полосы такой же жаркий, как и в низменности Тихама, но отличается еще большей сухостью. В некоторых восточных районах выпадает не более 50 мм осадков в год. Климат гор и предгорий восточной части Йемена более умеренный, временами в горах отмечаются заморозки.

Население

Население Йемена состоит в основном из арабских племен, исповедающих ислам. в основном арабы, небольшое число афро-арабских мулатов и индийцев. По оценке на 2011г., население составляет 24 млн. человек.

Телекоммуникации Йемена

Эта часть экономики развивается динамичнее остальных.

Исторически проводной телефонии в стране было мало и поэтому сейчас

сектор мобильной связи приобрел решающее значение.

В Йемене есть одна государственная компания (CDMA) yemenmobile и в феврале 2001г. было запущена первая частная комапния по сотовым связам (GSM) ,в настояще время уже три компании:

1.MTN (Spestel). 2. Sabafon 3. Y.

Мобильная связь в Йемене в периоде (2005-2013гг.)

год\параметр	количество пользователей	Плотность телефонных линий связи (на 100 жителей)
2005	2,277,553	11.4
2006	2,977,781	14.46
2007	4,348,264	20.5
2008	6,445,033	29.5
2009	8,312,773	36.96
2010	11,085,344	47.88
2011	12,349,860	51.82
2012	13,893,265	56.64
2013	17,423,000	69.04

Информационные центры в Йемене

№	**количество**	**Нозвание учерждении**
1	22	Информационные центры ,иследовании **легализаци**
2	98	Центры информации, статистических данных и государственных архивов
3	51	общедоступные библиотеки
4	727	Другие библиотеки
5	32	Издательства
6	5	Научные общества

Показатель \год	2007	2008	2009	2010	2011	2012	2013
количество установленных линий	1,326,125	1,337,122	1,336,824	1,353,839	1,360,373	1,364,582	1,380,901

Плотность телефонных линий связи (на 100 жителей)	4.8	4.4	4.4	4.5	4.5	4.5	4.3
Количество свободных линий	304,137	376,534	341,343	307,576	285,061	260,775	287,596
количество рабочих линий	1,021,988	960,588	996,981	1,046,263	1,075,312	1,103,807	1,093,305
Увеличение количества линий	53,660	61,400-	36,393	49,282	29,049	28,495	-10,502
Количество основных телефонных станций	49	49	49	48	49	49	49
Количество воспомогательных телефонных станций	229	225	226	236	237	238	236

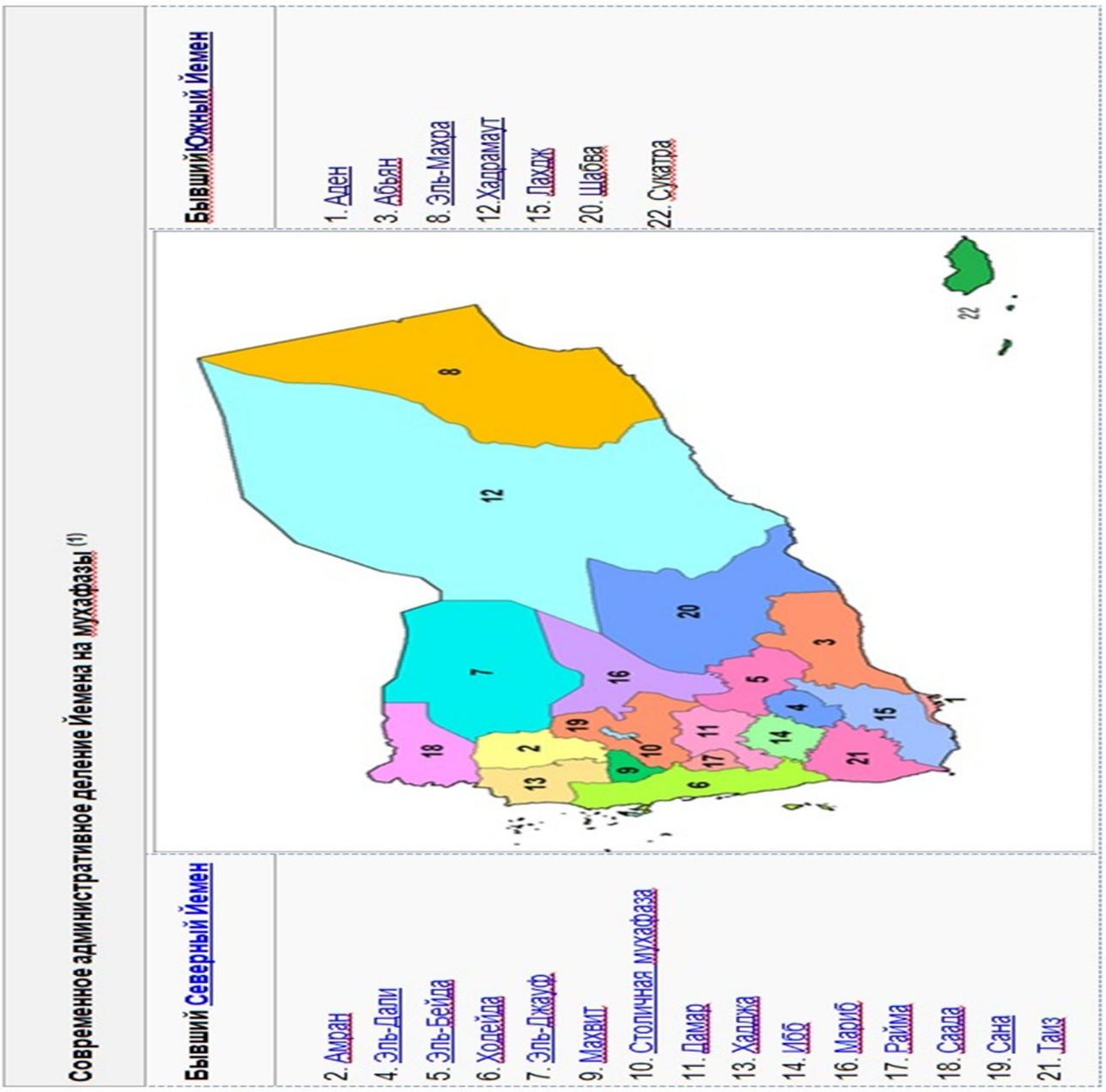
Интернет был запущен в Йемене в 1996 году одного поставщика (Йемен Телеком (Teleyemen)), число абонентов интернет услуг, дошло до (1093492) в 2013 году. Каждый год увеличивается число интернет-кафе и коммуникационных центров, где число интернет-кафе по всей республике около (1163) кафе до 2013 года, из которых (407) кафе в столице.

Интернет в Йемене в периоде (2005-2013гг.)

параметр \год	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**
количество абонентов	109127	155812	205613	305762	455429	581822	810750	857,970	1,093,492
Плотность интернет линийй (на 100 жителей	0.55	0.76	0.97	1.39	2.02	2.51	3.4	3.5	4.33
количество пользователей	-	779,060	1,028,065	1,528,810	2,260,660	1,341,530	1,787,043	2,363,769	2,607,089
количество интернет кофе	753	836	925	973	989	1004	1034	1099	1163
Переговорные пункты	10,367	12,348	13,769	14,757	15,245	15,768	16,075	16,374	16,034

Административное деление Йемена

Йемен делится на 22 мухафазу, они подразделены на 333 района (muderiah), которые подразделены на 2210 подрайонов, и затем на 38 284 деревни (на 2001).



Приложение 2

بسم الله الرحمن الرحيم

The republic of Yemen
Taiz University – turba branch
Faculty of Computer Seience
and information technology

الجمهورية اليمنية
جامعة تعز – فرع التربة
كلية الحاسبات وتقنية المعلومات

Date: 15-10-2012

The certificate of introduction

Results received from Mr. Ramzi Hamid alghabri performance of dissertational work are introduced at our University enterprises in the form of settlement techniques and of economic feasibility of improve protection of the information networks . Check of presence of possible ways and methods of penetration in a communication systems of our University enterprises .

Recommendation of improve safe of computers and telecommunication networks are used .

Chairman Department
Dr. Mohamed Ibrahim Al-aghbari

Dean Faculty
Dr. Abdulkarim Shamsan Aluosofi

Email: doc_mohebrahim2012@yahoo.com

Республика Йемен
Университет Таиз – Филиал Турба
Факультет информатики и информационных технологий
Дата: 15-10-2012

Акт внедрения

Результаты, полученные г-ном. Аль-Джабери Рамзи Хамид при выполнении диссертационной работы внедрены в нашем университете в виде расчётных методик с расчётом экономической целесообразности улучшения защиты информации сетей. Проведена проверка на наличие возможных путей и методов проникновения в системы связи нашего университета, использованы рекомендации по улучшению защиты компьютерных и телекоммуникационных сетей.

Заведующий кафедрой:
к.т.н. Аль-Агбари Мохаммед Ибрагим
Подпись
Печать :(кафедра информатики)
e-mail: doc_mohebrahim2012@yahoo.com

декан факультета:
к.т.н. Аль-Юсофи Абдулкарим Шамсан
подпись
печать: (Университет Таиз)

Перевод с английского языка на русский язык сделан переводчиком:
Аль-Хайдри Валид Ахмед

Город Владимир, Владимирская область, Российская Федерация.
Двадцать шестого ноября две тысячи четырнадцатого года.

Я, Васильева Юлия Николаевна, временно исполняющий обязанности нотариуса нотариального округа города Владимир Селезневой Жанны Игоревны, свидетельствую подлинность подписи, сделанной переводчиком Аль-Хайдри Валид Ахмед Ахмед в моем присутствии. Личность его установлена.

Зарегистрировано в реестре за № **10-7547**.

Взыскано по тарифу: 300 руб. 00 коп.
В том числе взыскано за услуги правового
и технического характера: 200 руб. 00 коп.

Временно исполняющий обязанности
нотариуса нотариального округа
города Владимир Селезневой Ж. И. Васильева Ю. Н.

Прошито, пронумеровано и скреплено печатью на 2 (двух) листах

Временно исполняющий обязанности
нотариуса нотариального округа
города Владимир Селезневой Ж. И. Васильева Ю. Н.

Компьютерная система "Экспресс"

Приложение 2.3.1. Программа выбора стратегии шифрования :

внутренний интерфейс PHP програмы.

```
<?php
include_once('Database.class.php');
define("MSCTBL","msc");
$db = new Database('localhost', 'root', 'test123', 'mscsim');
//connect to the server
$db->connect();
if($_GET['action']=='register' && !empty($_POST['MSISDN']) &&
!empty($_POST['IMSI'])){
$preMSISDN =
$_POST['MSISDN'][0].$_POST['MSISDN'][1].$_POST['MSISDN'][2].$_POST['
MSISDN'][3];
$data['TMSI'] = "91".$preMSISDN.rand('199999','999999');
$sql = "SELECT * FROM ".MSCTBL." WHERE `MSISDN` =
'".$_POST['MSISDN']."'";
$row = $db->query_first($sql);
if(empty($row)){
$error_dat['status'] = "error";
$error_dat['reason'] = "Registration Failed...";
}else{
$db->query_update(MSCTBL,$data," `MSISDN` = '".$_POST['MSISDN']."' ");
$error_dat['regdata'] = $row;
$error_dat['regdata']['TMSI'] = $data['TMSI'];
$error_dat['status'] = "success";
$error_dat['reason'] = "Registration Complete...";
}
sleep(3);
echo json_encode($error_dat);
}elseif($_GET['action']=='makesim' && !empty($_POST['MSISDN'])){
```

```
$preMSISDN =
$_POST['MSISDN'][0].$_POST['MSISDN'][1].$_POST['MSISDN'][2].$_POST['
MSISDN'][3]
;
$data['IMSI'] = "91".$preMSISDN.rand('199999','999999');
$data['IMEI'] = "956647"."894467".rand('199999','999999');
$data['Ki'] = genRandKey(128);
$data['NSP'] = getNSP($preMSISDN);
$sql = "SELECT * FROM ".MSCTBL." WHERE `MSISDN` =
'".$_POST['MSISDN']."'";
$row = $db->query_first($sql);
if(empty($row)){
$data['MSISDN'] = $_POST['MSISDN'];
$db->query_insert(MSCTBL,$data);
}else{
$db->query_update(MSCTBL,$data," `MSISDN` = '".$_POST['MSISDN']."' ");
$data['MSISDN'] = $_POST['MSISDN'];
}
echo json_encode($data);
}elseif($_GET['action']=='authenticate' && !empty($_POST['MSISDN']) &&
!empty($_POST['TMSI'])){
$sql = "SELECT * FROM ".MSCTBL." WHERE `MSISDN` =
'".$_POST['MSISDN']."'
AND `TMSI` = '".$_POST['TMSI']."'";
$row = $db->query_first($sql);
if(empty($row)){
$error_dat['status'] = "error";
$error_dat['reason'] = "Device Not Registered...";
}else{
$error_dat['RAND'] = genRandKey(128);
```

```
$error_dat['RES'] = resGen($error_dat['RAND'],$row['Ki'],128);
$error_dat['status'] = "success";
$error_dat['reason'] = "RAND Generation Complete...";
}
sleep(3);
echo json_encode($error_dat);
}elseif($_GET['action']=='gensres' && !empty($_POST['RAND']) &&
!empty($_POST['Ki'])){
$error_dat['SRES'] = resGen($_POST['RAND'],$_POST['Ki'],128);
$error_dat['status'] = "success";
$error_dat['reason'] = "RAND Generation Complete...";
sleep(3);
echo json_encode($error_dat);
}elseif($_GET['action']=='sendsres' && !empty($_POST['SRES']) &&
!empty($_POST['RES'])){
if($_POST['SRES']==$_POST['RES']){
$error_dat['status'] = "success";
$error_dat['reason'] = "Authentication Successfull...";
}else{
$error_dat['status'] = "error";
$error_dat['reason'] = "Authentication Failed...";
}
sleep(3);
echo json_encode($error_dat);
}
function genRandKey($length=128){
$count = round($length/8);
$binData = "";
for($i=1;$i<=$count;$i++){
$binData .= dechex(rand('128','255'))."-";
```

```
}
$binData = trim($binData,"-");
return $binData;
}
function getNSP($preMSISDN){
$NSP = array('9821'=>'Loop Mobile','9870'=>'Loop Mobile','9773'=>'Loop
Mobile',
'9664'=>'Loop Mobile','8082'=>'Loop Mobile',
'9819'=>'Vodafone','9820'=>'Vodafone','9833'=>'Vodafone',
'9920'=>'Vodafone','9930'=>'Vodafone','9769'=>'Vodafone',
'9619'=>'Vodafone','9167'=>'Vodafone','8879'=>'Vodafone',
'7506'=>'Vodafone Essar Ltd',
'9029'=>'Tata GSM','8097'=>'Tata GSM','8976'=>'Tata GSM',
'7208'=>'Tata GSM','8655'=>'Tata GSM',
'9869'=>'MTNL','9969'=>'MTNL','9757'=>'MTNL',
'9022'=>'Reliance (GSM)','9699'=>'Reliance
(GSM)','8080'=>'Reliance (GSM)',
'7666'=>'Reliance (GSM)','8767'=>'Reliance
(GSM)','7303'=>'Reliance (GSM)',
'9867'=>'Airtel','9892'=>'Airtel','9967'=>'Airtel','9987'=>'Airtel',
'9004'=>'Airtel','7738'=>'Airtel',
'9702'=>'Idea','9594'=>'Idea','8108'=>'Idea','8652'=>'Idea',
'7302'=>'Idea',
'9768'=>'Aircel','8898'=>'Aircel','8286'=>'Aircel',
'9076'=>'Videocon','8828'=>'Videocon','8268'=>'Videocon',
'9320'=>'Reliance(CDMA)','9321'=>'Reliance(CDMA)',
'9322'=>'Reliance(CDMA)',
'9323'=>'Reliance(CDMA)', '9324'=>'Reliance(CDMA)',
'7498'=>'Reliance(CDMA)',
'8448'=>'Reliance(CDMA)',
```

```
'9220'=>'Tata (CDMA)','9221'=>'Tata (CDMA)','9222'=>'Tata
(CDMA)',
'9223'=>'Tata (CDMA)','9224'=>'Tata (CDMA)','9209'=>'Tata
(CDMA)'
);
if($NSP[$preMSISDN]){
return $NSP[$preMSISDN];
}else{
return "Other";
}
}
function resGen($rand,$ki,$length=128){
$count = round($length/16);
$rand_arr = explode("-",$rand);
$ki_arr = explode("-",$ki);
for($i=0;$i<$count;$i++){
$left = hexdec($rand_arr[$i]) ^ hexdec($ki_arr[$i+$count]);
$right = hexdec($ki_arr[$i]) ^ hexdec($rand_arr[$i+$count]);
$res64[$i] = $left ^ $right;
}
$count2 = round($count/2);
for($i=0;$i<$count2;$i++){
$res32[$i] = dechex($res64[$i] ^ $res64[$count2+$i]);
}
return implode('-',$res32);
}
?>
```

b) Frontend HTML & Javascript :

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN">
```

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Cp1252">
<link type="text/css" href="style.css" rel="stylesheet" />
<script type="text/javascript" src="jquery.js"></script>
<script type="text/javascript">
jQuery(document).ready(function() {
////////////////////////////////////////////////////////
////////////////////// Making Sim ////////////////////////////
////////////////////////////////////////////////////////
$('#mkSIM').removeAttr('disabled');
$('#msisdn').removeAttr('disabled');
$('#register').attr('disabled','disabled');
$('#authenticate').attr('disabled','disabled');
$('#mearea').attr('value','');
$('#mscarea').attr('value','');
$('#direcImg').css('display','none');
$('#mkSIM').click(function(){
var simMSISDN = $('#msisdn').attr('value');
$.post('functions.php?action=makesim',{'MSISDN':simMSISDN},function(data){
$('#simvars').css('display','block');
$('#simMSISDN span').html(data.MSISDN);
$('#simIMSI span').html(data.IMSI);
$('#simIMEI span').html(data.IMEI);
$('#simKival').attr('value',data.Ki);
$('#simKiMSC span').html(data.Ki);
$('#simNSP span').html(data.NSP);
$('#mkSIM').attr('disabled','disabled');
$('#register').removeAttr('disabled');
$('#msisdn').attr('disabled','disabled');
```

```
},"json");
});
////////////////////////////////////////////////////////////
////////////////// Registering on Netwrok ////////////////
////////////////////////////////////////////////////////////
$('#register').click(function(){
var temp = $('#mearea').attr('value');
$('#register').attr('disabled','disabled');
$('#mearea').attr('value',temp + '>> Registering on
Network...');
$('#direcImg').css('display','block');
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>> Sending IMSI & MSISDN
...');
var simMSISDN = $('#simMSISDN span').html();
var simIMSI = $('#simIMSI span').html();
var temp = $('#mscarea').attr('value');
$('#mscarea').attr('value',temp + '>> Recieving Registeration
Request ...');
$('#regvars').css('display','block');
$('#recdMSISDN span').html(simMSISDN);
$('#recdIMSI span').html(simIMSI);
$.post('functions.php?action=register',{'MSISDN':simMSISDN,'IMSI':simIMSI},f
unc
tion(data){
$('#direcImg').attr('src','left.png');
var temp = $('#mscarea').attr('value');
$('#mscarea').attr('value',temp + '\n>> Registration
Successfull ...');
var temp = $('#mscarea').attr('value');
```

```
$('#mscarea').attr('value',temp + '\n>> Sending TMSI
number...');
$('#simTMSI span').html(data.regdata.TMSI);
$('#genTMSI span').html(data.regdata.TMSI);
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>> Recieved TMSI
Number,Registration Successfull ...');
$('#authenticate').removeAttr('disabled');
},"json");
});
////////////////////////////////////////////////////////
////////////////// Authenticating on Netwrok ///////////////
////////////////////////////////////////////////////////
$('#authenticate').click(function(){
var temp = $('#mearea').attr('value');
$('#authenticate').attr('disabled','disabled');
$('#mearea').attr('value',temp + '\n>> Requesting
Authentication of Device...');
$('#direcImg').attr('src','right.png');
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>> Sending TMSI...');
var simTMSI = $('#simTMSI span').html();
var simMSISDN = $('#simMSISDN span').html();
var temp = $('#mscarea').attr('value');
$('#mscarea').attr('value',temp + '\n>> Recieving
Authentication Request ...');
$('#regvars').css('display','none');
$('#authvars').css('display','block');
$('#recdTMSI span').html(simTMSI);
$.post('functions.php?action=authenticate',{'MSISDN':simMSISDN,'TMSI':simT
```

```
MSI},
function(data){
$('#direcImg').attr('src','left.png');
var temp = $('#mscarea').attr('value');
$('#mscarea').attr('value',temp + '\n>> Generated RAND,RES
& Kc...');
var temp = $('#mscarea').attr('value');
$('#mscarea').attr('value',temp + '\n>> Sending RAND
sequence...');
$('#genRAND span').html(data.RAND);
$('#simRAND span').html(data.RAND);
$('#genRES span').html(data.RES);
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>> Recieved RAND
sequence Successfully ...');
var simRAND = $('#genRAND span').html();
var simKi = $('#simKival').attr('value');
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>> Generating
SRES(Signed Response)...');
// generate SRES
$.post('functions.php?action=gensres',{'RAND':simRAND,'Ki':simKi},function(da
ta
){
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>> SRES Generated
Successfully...');
$('#simSRES span').html(data.SRES);
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>> Sending SRES to
```

```
MSC ...');
//// Sending SRES
mscRES = $('#genRES span').html();
$('#recdSRES span').html(data.SRES);
$('#direcImg').attr('src','right.png');
$.post('functions.php?action=sendsres',{'SRES':data.SRES,'RES':mscRES},functio
n
(data){
$('#authImg').css('display','block');
if(data.status == 'success'){
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>>
'+data.reason);
$('#authImg img').attr('src','unlocked.png');
var temp = $('#mscarea').attr('value');
$('#mscarea').attr('value',temp + '\n>>
'+data.reason);
}else{
var temp = $('#mearea').attr('value');
$('#mearea').attr('value',temp + '\n>>
'+data.reason);
$('#authImg img').attr('src','locked.png');
var temp = $('#mscarea').attr('value');
$('#mscarea').attr('value',temp + '\n>>
'+data.reason);
}
},"json");
},"json");
$('#authenticate').removeAttr('disabled');
},"json");
```

```
});
});
</script>
<title>MCS-Expt3 | Authentication in GSM Network</title>
</head>
<body>
<div style="width: 100%;border:1px solid
blue;background:#D3DCE3;height: 20px;">
<div style="width: 50%;float: left;text-align: center;">MCS-Expt.
No. 3 | Authentication in GSM Network using A3 Algorithm</div>
<div style="width: 50%;float: right;text-align: right;">Shiburaj
Pappu   </div>
</div>
<div class="col1">
<div class="box">
<div><img src="phone.png" width="80" height="80" /></div>
<div><h4>MS</h4></div>
<div><textarea id="mearea" class="codearea"
readonly="readonly">hi</textarea></div><br />
<div>Mobile Number:
<input type="text" name="msisdn" id="msisdn" /><br /><br />
<input type="button" id="mkSIM" class="btn" value="Make
SIM" />  
<input type="button" id="register" class="btn"
value="Register" />  
<input type="button" id="authenticate" class="btn"
value="Authenticate" />
</div>
<div id="simvars">
<div id="simNSP">SIM NSP : <span>--</span></div>
```

```
<div id="simMSISDN">SIM MSISDN : <span>--</span></div>
<div id="simIMSI">SIM IMSI : <span>--</span></div>
<div id="simIMEI">SIM IMEI : <span>--</span></div>
<div id="simKi">SIM Ki : <input type="text" name="simKival"
value="" id="simKival" /></div>
<div id="simTMSI">SIM TMSI : <span>--</span></div>
<div id="simRAND">Recd. RAND : <span>--</span></div>
<div id="simSRES">Gen. SRES : <span>--</span></div>
</div>
</div>
</div>
<div class="col2">
<div><img id="direcImg" src="right.png" width="80" height="80"
/></div>
</div>
<div class="col3">
<div class="box">
<div><img src="msc.png" width="80" height="80" /></div>
<div><h4>MSC</h4></div>
<div><textarea id="mscarea" class="codearea"
readonly="readonly"></textarea></div>
<div id="regvars">
<div id="recdMSISDN">Recd. MSISDN : <span>--</span></div>
<div id="recdIMSI">Recd. IMSI : <span>--</span></div>
<div id="genTMSI">Gen. TMSI : <span>--</span></div>
</div>
<div id="authvars">
<div id="recdTMSI">Recd. TMSI : <span>--</span></div>
<div id="simKiMSC">Ki : <span>--</span></div>
<div id="genRAND">Gen. RAND : <span>--</span></div>
```

```
<div id="genRES">Gen. RES : <span>--</span></div>
<div id="recdSRES">Recd. SRES : <span>--</span></div>
</div>
<div id="authImg"><img src="locked.png" width="80" height="80"
/></div>
</div>
</div>
</body>
</html>
```

Приложение 3.3

List program

```
[System]
Name='МД'
Type='mamdani'
Version=2.0
NumInputs=2
NumOutputs=1
NumRules=9
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'

[Input1]
Name='состояние_канала'
Range=[0 8]
NumMFs=3
MF1='П':'trimf',[-4 0 4]
MF2='Н':'trimf',[0 4 8]
MF3='Х':'trimf',[4 8 12]

[Input2]
Name='скорость_изменения_состояния_канала(dX/dt)'
```

```
Range=[-8 8]
NumMFs=3
MF1='M':'trimf',[-16 -8 0]
MF2='H':'trimf',[-8 0 8]
MF3='B':'trimf',[0 8 16]

[Output1]
Name='рейтинг_канала'
Range=[0 100]
NumMFs=5
MF1='очень_маленький':'trimf',[-20 0 20]
MF2='маленький':'trimf',[7 25 47]
MF3='нормальный':'trimf',[30 50 70]
MF4='большой':'trimf',[58 75 92]
MF5='очень большой':'trimf',[80 100 120]

[Rules]
1 3, 1 (1) : 1
1 2, 2 (1) : 1
1 1, 3 (1) : 1
2 3, 2 (1) : 1
2 2, 3 (1) : 1
2 1, 4 (1) : 1
3 3, 3 (1) : 1
3 2, 4 (1) : 1
3 1, 5 (1) : 1
```