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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

г. Владимир-2015 г.

Работа выполнена на кафедре радиотехники и радиосистем ФГБОУ ВПО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» ВлГУ.

Научный руководитель **Галкин Александр Павлович**
доктор технических наук, профессор,
кафедры радиотехники и радиосистем
«Владимирский государственный
университет» ВлГУ (г. Владимир)

Официальные оппоненты: **Приоров Андрей Леонидович**
доктор технических наук, доцент
кафедры динамических систем,
«Ярославский государственный
университет имени Демидова»,
(г. Ярославль)

Дерябин Вячеслав Михайлович
кандидат технических наук, доцент,
заместитель начальника отдела
измерительной техники ЗАО
«Автоматика плюс», (г. Владимир)

Ведущая организация: Региональный аттестационный центр
ООО «ИнфоЦентр» (г. Владимир)

Защита состоится « 6 » октября 2015 г. в 14 ч. в ауд. 301-3 на заседании диссертационного совета Д 212.025.04 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, д. 87, корп. 3, ауд. 301.

С диссертацией можно ознакомиться в научной библиотеке ВлГУ.

Автореферат разослан « 15 » июня 2015 г.

Отзывы в двух экземплярах, заверенные печатью, просим направлять по адресу: ул. Горького, д. 87, ВлГУ, ФРЭМТ, г. Владимир, 600000.

Ученый секретарь диссертационного совета
доктор технических наук, профессор А. Г. Самойлов

Введение

В настоящее время в Йемене широко стали использоваться 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. В настоящее время произошло много изменений и наша задача учесть эти изменения.

В то же время, в телекоммуникациях Йемена потенциально существует угрозы использования различных приемов создания мешающих воздействий (проникновения, утечки и извращение информации и т.п.).

При этом преднамеренно или неумышленно могут создаваться опасность для жизни или здоровья людей или наступления других тяжких последствий, преследуются цели получения преимуществ при решении политических, экономических или социальных проблем, нарушение нормальной деятельности корпораций, банков и т.п. Это является одной из опасных преднамеренных угроз государственной и общественной безопасности и всей страны и отдельных корпоративных сетей.

Одним из перспективных направлений обеспечения работоспособности компьютерных сетей в экстремальных условиях Йемена, является разработка адаптивных отказоустойчивых систем, обеспечивающих автоматическое обнаружение, локализацию и исправление возникающих ошибок.

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 усложняется задача управления всеми процессами (большая ситуационная неопределенность, нечеткость), трактовка результатов наблюдения - это задача для специалиста-эксперта по сетевому управлению, с применением элементов нечеткой логики.

Основными потенциально возможными требованиями для эксперта явля-

ются:

- Отлично знать все используемое оборудование и программное обеспечение, чтобы быстро интерпретировать изменения каких-либо параметров.
- Держать в уме всю топологию сети, чтобы быстро определить причину и источники таких изменений при необходимости использовать криптографию.
- При нарушении нормального режима функционирования сети, обычно, генерируется лавина сообщений, в том числе и ошибки, и он должен уметь выделить из них существенные и отбросить те, которые являются следствием первых.
- Наконец, на нем лежит административный груз ответственности за эффективное использование огромных ресурсов (дорогостоящего оборудования, каналов связи, обслуживающего персонала). От его работы зависит экономическая эффективность предприятия.

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

Таким образом, сложное оборудование КИТС, большой объем поступающей информации, трудность решения плохо формализуемых и слабо структурированных задач при отсутствии полной и достоверной информации о состоянии элементов сети, короткое время на анализ проблемных ситуаций и принятие решения приводят к несоответствию возможностей человека требованиям эффективно управлять сетью.

Указанные проблемы делают практически невозможным или малоэффективным 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 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).

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 Тайзском 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. межрегиональной научной конференции «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 10 научных трудах (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.

Личный вклад автора диссертации. В диссертации использованы результаты исследований и разработок по созданию многофункциональных методик и аппаратных средств для защиты систем связи и корпоративных сетей от несанкционированного доступа к информации. При этом автор диссертации являлся непосредственным исполнителем или соавтором основополагающих разработок, алгоритмов и моделей. В статьях и в докладах выполненных в соавторстве ему принадлежит или равная часть или более того.

Структура и объем диссертации. Диссертация состоит из списка сокращений, введения, 3-х глав, заключения, списка литературы и приложений. Содержит 126 стр., 108 библиографий, 28 табл., 45 рис.

Основное содержание работы

Во введении обоснована актуальность темы диссертационной работы, сформулированы цели и задача исследований, научная новизна и практическая ценность результатов диссертации.

В первой главе рассматриваются анализа современное состояние информационной безопасности корпоративных информационно-телекоммуникационных сетей (КИТС) (КИТС Йемена на рис.1). Комплексная информационная безопасность – система сохранения, ограничения и авторизованного доступа к информации, содержащейся на серверах в КИТС.

Не смотря на различия между компьютерными, телевизионными, телефонными и первичными сетями (сетями электросвязи), вес эти сети имеют сходные структуры, включающие следующие компоненты:

- сети доступа – предназначены для концентрации информационных потоков поступающих по каналам связи от оборудования пользователей (обыкновенных и удаленных) и передачи в узлы магистральной сети;
- магистраль – объединяет отдельные сети доступа, обеспечивая передачу трафика между ними по высокоскоростным каналам;

• информационные центры – это информационные ресурсы сети, с помощью которых осуществляется обслуживание пользователей.

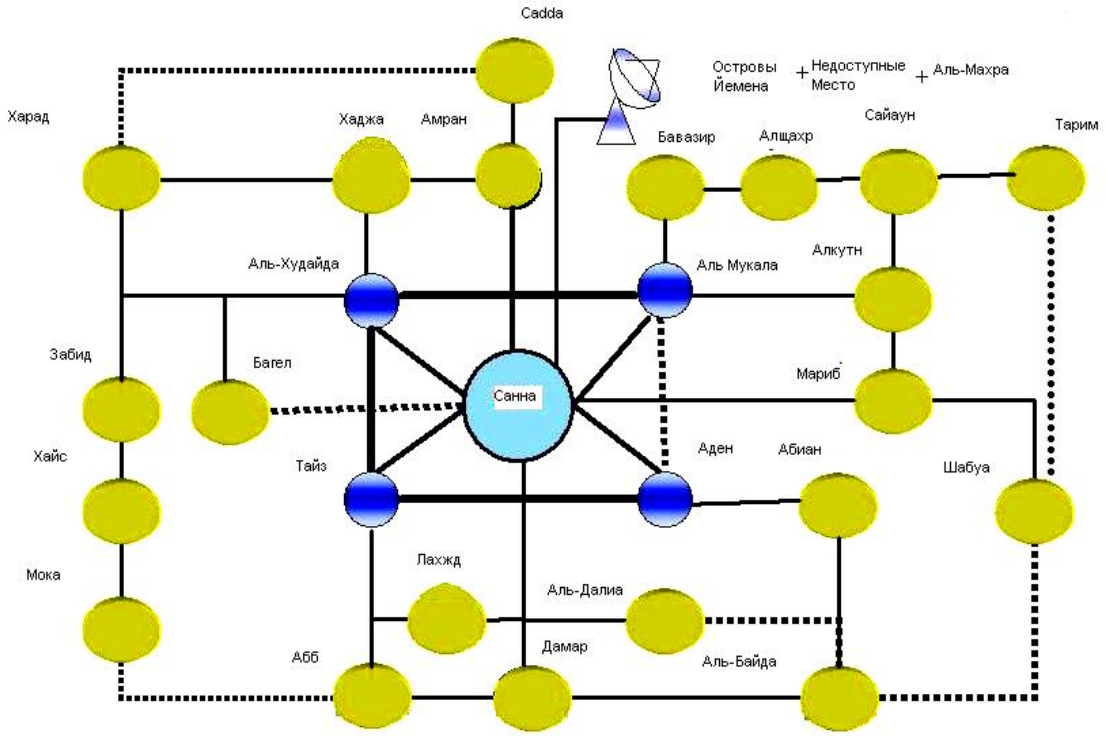

Рис.1. Корпоративная информационно-телекоммуникационная сеть Йемена

В соответствии с введенным определением КИТС и ее состав в общем случае образуют следующие функциональные элементы:

- Рабочие места (абоненты) корпорации.
- Информационные серверы корпорации.
- Средства телекоммуникации.
- Телеслужбы.
- Система управления эффективностью функционирования КИТС.
- Система управления безопасностью функционирования корпоративной сети.
- Система обеспечения надежности корпоративной сети
- Система диагностики и контроля.
- Система эксплуатации.

Здесь же обосновывается применение аппарата нечеткой логики.

Во второй главе оценивается достоверность функционирования отказоустойчивого запоминающего устройства при информационной защите телекоммуникаций и предлагается системный уровень проектирования защищен-

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

Мы рассматриваем САПР, предназначенную для автоматизации труда проектировщика систем защиты информации основанных на NoC. При этом учитываем особенности Йемена.

Рис.2. Классификация ТС СДВ по проводным линиям

Рис.3. Классификация ТС СДВ по эфиру (электромагнитные ТС СДВ)

Системный уровень включает два подуровня функциональный и уровень транзакций. На функциональном уровне (уровне алгоритмов) создается и верифицируется математическая модель системы в целом. На уровне транзакций можно моделировать архитектуру системы. Очень важно, что уже на системном уровне возможно совместное моделирование аппаратной и программной частей системы, определение их оптимального соотношения.

Рис. 4. Общий маршрут проектирования

Разработанное нами криптографическое решение, позволило осуществить централизованное управление правами на документы, формирование контекстов документов, в рамках которых задаются права доступа, а именно:

- Динамическое шифрование документов при записи в репозитарий АСУД (системы электронного документооборота) или когда они покидают его.
- Динамическое шифрование версий документа.
- Полнотекстовая индексация документов и версий, поиск по зашифрованным документам и версиям.
- Шифрование и снятие защиты, при движении документа по жизненному циклу в СЭД;
- 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.

Третья глава посвящена многостанционному доступу в когнитивных сетях и разработке методик оценок этого с помощью аппарата нечеткой логики. 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. Измерение состояния канала проводится в разных интервалах времени τ1, τ2,.. τn, где τ- длительность цикла.

τ = 8Δt, Δt=[t, t + 1] требуемый интервал времени для передачи одного пакета.

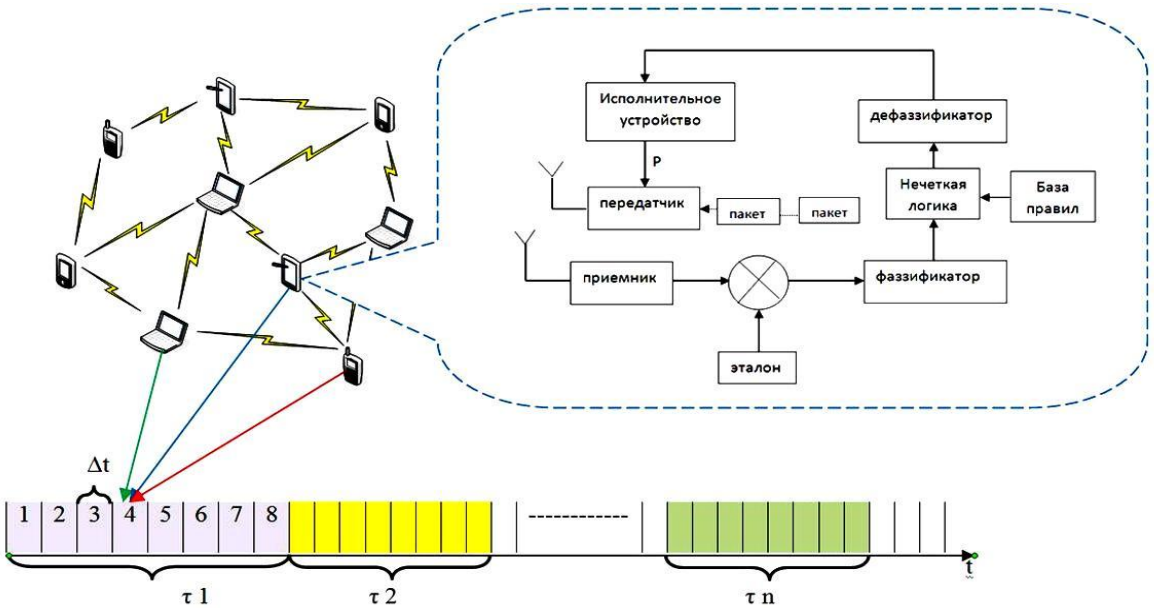

Рис.5. Схема когнитивного абонентского терминала на примере ТГУ

Как показано на рис.5 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.

При разработке нечетких систем необходимо пройти следующие этапы проектирования (после изучения основных понятий нечетких множеств и систем): определить входы и выходы создаваемой системы; задать для каждой из входных и выходных переменных функции принадлежности с термами; разработать базы правил выводов для реализуемой нечёткой системы; провести дефаззификацию; провести настройку и анализ адекватности разработанной модели реальной системе; программная реализация нечеткого регулятора на конкретном микроконтроллере.

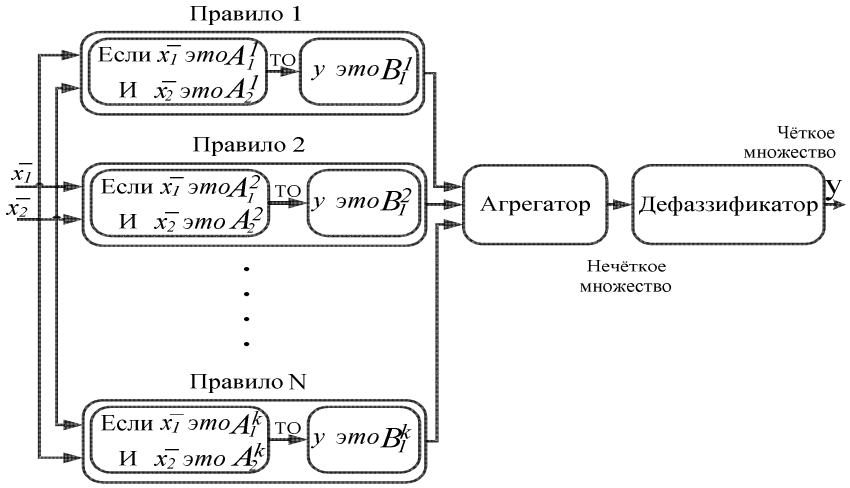

Рис.6. Система нечеткого логического вывода.

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.

Фаззификатор выдает три терма состояния канала T(C): «канал загружен», «канал в норме», «канал незагружен». Как показано на рис.5 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 C- 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.7 .

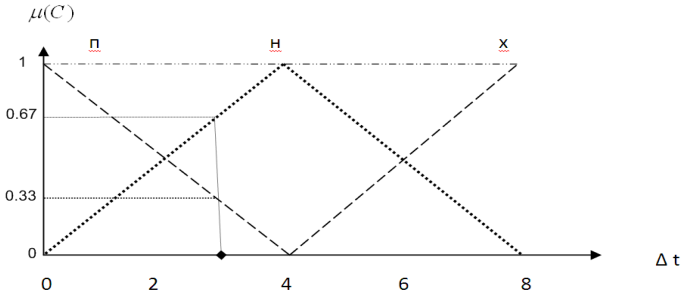

Рис.7. Функция принадлежность состояния канала

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. 8).

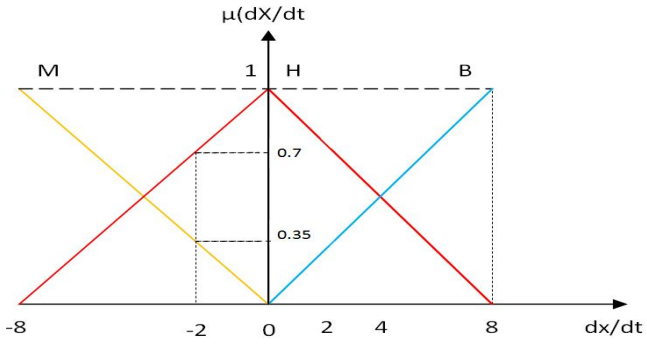

Рис.8. Функция принадлежность изменения степени загруженности канала

В качестве функций принадлежности для каждого терма всех лингвистических переменных выбирали треугольные функции принадлежности, поскольку, как показывает практика и исследования, они хорошо подходят для использования при решении широкого круга проблем управления. Процесс вычисления нечеткого правила называется нечетким логическим выводом и подразделяется на два этапа: обобщение и заключение. Важной характеристикой нечеткой логики является то, что любая переменная может быть фаззифицирована, т. е. обобщена путем замены понятия четкого множества понятием нечеткого мно-

жества.

Одним из основных методов представления знаний в экспертных системах являются продукционные правила, позволяющие приблизиться к стилю мышления человека. При построении нечеткого логического вывода исходят из предположения, что эксперты в состоянии сформировать базу правил, обычно продукционное правило записывается в следующем виде:

«ЕСЛИ (посылка_1) (связка) (посылка_2) (св) …(св) (посылка_n), ТО (заключение)». и базы данных с функциями принадлежности для предпосылок ***μ(x)*** и выводов ***μ(y)***, т.е. определить все необходимые лингвистические правила с лингвистическими переменными и термами. Типичное продукционное правило состоит из ***антецедента*** (часть ЕСЛИ …) и ***консеквента*** (часть ТО …). Антецедент может содержать более одной посылки. В этом случае они объединяются посредством логических связок И или ИЛИ. В качестве Т-нормы используется операция минимум, в качестве S- нормы – операция максимум:

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

Правило нечеткой импликации задается правилом:

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

где A и B - нечеткие множества $A \subseteq X, B \subseteq Y$, отношение R определено на X * Y. В результате получаем, что:

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

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, N- количество правил нечеткого вывода(N= 3*3=9, поскольку каждая из двоя лингвистических переменных может принимать три разных значений), у- выходная переменная (рейтинг канала), В- соответствующее ей множество. Если канал находится в хорошем состоянии и его степень загруженности уменьшается по сравнению с предыдущим состоянием, то рейтинг канала будет очень большим. Через нечеткие переменные это правило можно записать следующим образом: если C = X и dX/dt = M, то P = OB. Если канал находится в нормальное состояние и его

степень перегрузки по сравнению с предыдущим состоянием увеличится, то рейтинг канала уменьшается. Через нечеткие переменные это правило можно записать так: если С = Н и dX/dt = В, то Р = М.

Совокупность всех правил удобно представить в виде таблицы, в которой столбцы соответствуют условиям одного параметра, строки - условиям другого параметра, а на их пересечениях записываются выводы, соответствующие этим условиям.

Состояние канала (С)	Скорость изменения состояния канала (dX/dt)		
	В	Н	М
П	ОМ	М	Н
Н	М	Н	В
Х	Н	В	ОВ

Выводом каждого правила импликации является лингвистическая переменная “ рейтинг канала”, множество значений которой состоит из пяти термов Т(Р): очень маленький (ОМ), маленький (М), норма (Н), большой (В) и очень большой (ОВ) .

Результат работы системы нечеткого вывода будет определяться нечеткой базой знаний, а точнее продукционными правилами, на которых построен нечеткий вывод. 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.

Основные результаты и выводы

В ходе проведенных исследований получены следующие основные результаты:

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.

Список публикаций по теме диссертации

- в изданиях по перечню ВАК:

1. Аль-Джабери Р.Х. Системный уровень проектирования защищённых сетей / Обади Х.М., Галкин А.П., Ковалёв М.С., Амро М.М.// Изв. института инженерной физики. 2013. №4. С. 10-12. (35%)

2. Аль-Джабери Р.Х. Выбор рациональной информационной защиты корпоративных сетей с криптографией/ Галкин А.П., Обади Х.М., Ковалёв М.С., Суслова Е.Г.// Изв. института инженерной физики. 2014. №3(33), С. 7-12.(30%)

3. 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. (35%)

- в других изданиях:

4. Аль-Джабери Рамзи Когнитивное радио-важное направление в инновационном развитии здравоохранении / 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. (30%)

5. Аль-Джабери Р.Х. Проблемы информационной безопасности и инновационные пути их решение/ Галкин А.П., Дарахма И., Альджарадат М.М. //«Инновационные развития экономики – основа устойчивого развития территориального комплекс» Матер. Всероссийской научн. прак. конф. Владимир - Москва, 2012. С.172-176.(30%)

6. 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., книга 2, С. 49-52.(30%)

7. 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.(30%)

8. 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.(30%)

9. 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. (40%).

10. 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. Том 2 С. 112-114. (90%)

Подписано в печать 02.06.2015г.
Формат 60×84/16. Усл. печ. л. 1,39. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.