МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО
ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН
ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
им. АБУ РАЙХАНА БЕРУНИ

На правах рукописи

КАРИМОВ Маджит Маликович

ОРГАНИЗАЦИЯ КОРПОРАТИВНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ С ИНТЕГРИРОВАННОЙ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Специальность 05.13.13 – Вычислительные машины, комплексы, системы и сети

АВТОРЕФЕРАТ

диссертации на соискание ученой степени доктора технических наук

Ташкент 2003

Работа выполнена в Ташкентском государственном техническом университете имени Абу Райхана Беруни

Официальные оппоненты:

Академик МАН ВШ,
доктор технических наук, профессор **Савельев А.Я.**

доктор технических наук, профессор **Адылова З.Т.**

доктор технических наук **Рахматуллаев Р.У.**

Ведущая организация: Национальный университет Узбекистана.

Защита состоится « 11 » октября 2003 г. в « 14 » час на заседании разового специализированного совета ТГТУ. 700095, Ташкент, ул. Университетская, 2, главный корпус, ауд. 215.
С диссертацией можно ознакомиться в библиотеке ТГТУ.

Автореферат разослан « 4 » сентября 2003 г.

Ученый секретарь
разового специализированного совета
доктор технических наук,
профессор **Хамдамов Р.Х.**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы. Постепенная интеграция в мировую экономическую систему – одна из главных задач проводимых в Республике Узбекистан за годы экономических реформ. Она позволит в обозримом будущем за счет инвестиций мирового банка развития и реконструкции, международного валютного фонда и других экономических институтов, а также национального научно-технического потенциала модернизировать эксплуатируемые и строить новые телекоммуникационные системы, корпоративные сети. В основу этого должен лечь мировой опыт проектирования и технологические решения ведущих компаний-производителей вычислительной техники, электроники, коммуникационных систем и оборудования для локальных и корпоративных компьютерных сетей, а также новые научные результаты и предложения специалистов в данной отрасли знаний.

Постепенное внедрение новейших технологий в архитектуру действующих компьютерных сетей поможет в недалеком будущем перейти на современную сетевую технологию, централизованно соединить все сети отрасли или компании в единую корпоративную сеть с гибкой системой защиты информации (СЗИ), а затем влиться в мировую информационную магистраль.

Следует отметить, что корпоративные компьютерные сети, не являющиеся больше изолированными островками, состоящими из одного или двух серверов файлов и печати и небольшого количества рабочих станций, превратились в сложные, высококритичные среды, состоящие из множества серверов различных типов, а также многочисленных рабочих групп, нуждающихся в связи друг с другом. В такой среде неоптимальность структуры топологии и отсутствие или слабость СЗИ способны привести к хаосу, прямыми последствиями которого являются снижение производительности, уменьшение надежности и ухудшение безопасности сети.

Обычно крупные сети имеют высокоскоростную магистраль, но если, например, весь сетевой трафик направляется туда, то он может исчерпать доступную пропускную способность, сводя на нет преимущества в производительности. Ввиду того, что рабочие станции взаимодействуют в основном с локальными серверами файлов и печати гораздо чаще, нежели внешними серверами Web, имеет смысл оптимизировать топологию сети, в частности, сегментировать сеть в соответствии с рабочими группами, в которых большая часть трафика не выходит за пределы локального сегмента. Кроме того, оптимизация и сегментирование структуры сети позволяют легко организовать гибкую СЗИ.

Несмотря на то, что имеется множество работ, где в той или иной мере освещены аспекты оптимального проектирования сетей, с расширением сферы использования сетей, постоянным совершенствованием сетевых технологий и повышением требований к обеспечению безопасности информации, возникает потребность в совершенствовании старых и разработке новых методов и средств синтеза компьютерных сетей.

В связи с "многопользовательским" режимом работы в компьютерной сети возникает целый набор взаимосвязанных вопросов по защите информации, хранящейся в компьютерах или серверах компьютерной сети. Следует отметить, что сами сетевые операционные системы также представляют мощные средства защиты от несанкционированного доступа к сетевым ресурсам. Однако нередки случаи, когда даже такая защита не срабатывает. Практика показывает, что несанкционированный пользователь, имеющий достаточный опыт в области системного и сетевого программирования, задавшийся целью подключиться к сети, даже имея ограниченный доступ к отдельным ресурсам, рано или поздно может получить доступ к некоторым защищенным ресурсам сети. Поэтому возникает необходимость в создании дополнительных аппаратных и программных средств защиты сетевых ресурсов.

К аппаратным средствам защиты относятся различные сетевые экраны, фильтры, устройства шифрования протокола и т.д. К программным средствам защиты можно отнести: программы шифрования данных; программы слежения сетевых подключений (мониторинг сети); программы аутентификации и идентификации и т.д.

Среди всего спектра методов защиты от несанкционированного доступа особое место занимают криптографические методы. В отличие от других методов они опираются лишь на свойства самой информации и не используют свойства его материальных носителей, особенности узлов его обработки, передачи и хранения. Актуальность проблемы использования криптографических методов в информационных системах объясняется тем, что, с одной стороны, расширилось использование компьютерных сетей, в частности, глобальной сети Internet, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающие возможности доступа к ней посторонних лиц. С другой стороны, появление новых мощных компьютеров, сетевых технологий и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически нераскрываемыми.

Следовательно, для обеспечения эффективной информационной безопасности, на наш взгляд, необходимо разработать **интегрированную систему защиты информации** на основе топологического синтеза структуры,

обеспечивающую целостность представления общей картины сети с точки зрения её безопасности. В результате топологического синтеза определяется оптимальная топология сети с точки зрения минимальности диаметра и валентности структуры сети, а также удобства осуществления оперативного мониторинга сети. Кроме того, выделяются сегменты и выбираются возможные узлы установления фильтров, сетевых и межсетевых экранов.

Особое место в интегрированной системе защиты информации занимают комбинированные криптографические методы, шифрование данных в которых производится в два этапа. На первом этапе данные шифруются стандартным или модернизированным методом, а на втором – шифрованные данные подвергаются вторичному шифрованию по специальному методу. В качестве последних могут быть использованы: гаммирование; перемножение вектора шифрованных данных на матрицу; перестановки с логическими преобразованиями и т.д.

В связи с тем, что аппаратная реализация комбинированного метода приводит к увеличению аппаратных затрат, а его программная реализация существенно влияет на время шифрования и дешифрования данных, целесообразна аппаратно-программная реализация, когда один из этапов комбинированного метода необходимо реализовать аппаратно, а другой – программно.

Таким образом, разработка интегрированной системы защиты начинается с первых этапов синтеза компьютерных сетей и постоянно совершенствуется путем введения в состав системы новых специальных методов и аппаратно-программных средств защиты информации.

Вышесказанное свидетельствует о том, что работы, направленные на исследование и разработку корпоративных сетей с интегрированной системой защиты информации, являются актуальными.

Материал реферируемой диссертационной работы основан на результатах исследований, выполненных автором как самостоятельно, так и совместно со своими коллегами по работе в соответствии с Государственными научно-техническими программами ГКНТ Республики Узбекистан на 1997-99 и 2000-02 годы в рамках НИР № 14.7 «Аппаратные и программные средства накопления, обмена и защиты информации для ЛВС ВУЗа» (№ Гос. регистрации №01970006111), 4.2.1.2 «Разработка, специальных методов и аппаратно-программных средств защиты информации в компьютерных сетях» (№ Гос. регистрации №01.20008907), а также связан с планами основных научных работ кафедры «Компьютерные системы и сети» Ташкентского государственного технического университета.

Цель работы. Целью диссертационной работы является разработка теоретических основ и создание корпоративных сетей с интегрированной системой защиты информации.

Для достижения поставленной цели необходимо решить следующие задачи исследования:

- обоснование принципа организации корпоративных компьютерных сетей с интегрированной системой защиты;
- разработка метода оптимального сегментирования топологии сети;
- разработка комбинаторного метода и алгоритма декомпозиции структуры компьютерной сети;
- разработка способа многопараметрической оптимизации топологии корпоративной компьютерной сети;
- разработка принципов построения оптимального дерева концентраторов и концентраторного перекрытия корпоративных сетей;
- разработка специального алгоритма мониторинга топологии сети;
- обоснование специальных и совершенствование типовых методов шифрования данных и разработка аппаратно-программных средств их реализации;
- разработка метода синтеза оптимальных структур специализированных устройств шифрования данных.

Результаты исследований могут быть использованы при организации корпоративных компьютерных сетей на основе рассредоточенных локальных сетей и отдельных рабочих станций с усиленной системой защиты информации для предприятий, ведомств, министерств, служб и комитетов. В работе сформулированная ghj,ktvf решается применительно к рассредоточенным отраслевым корпоративным сетям, имеющим точку выхода в Интернет.

Методы исследования. В работе использованы методы теории графов, теории множеств и оптимизации, методы защиты информации, криптографические методы, теория алгоритмов и программирования, теория формальных языков, методы схемотехники и системотехники.

Научная новизна работы состоит в классификации каналов утечки информации в компьютерных сетях; обосновании принципа организации структур сетей на основе объединения различных типовых топологических организаций в единую иерархическую структуру; разработке метода оптимального сегментирования топологии сети, позволяющего упростить процесс управления трафиком; разработке комбинаторного метода декомпозиции структуры сети, отличающейся от известных более высокой скоростью сходимости; разработке способа многопараметрической оптимизации структуры корпоративных компьютерных сетей на основе методов релаксации и алгоритма формирования топологии терминальной сети, позволяющего находить решение, максимально

приближённое к оптимальному; разработке алгоритма формирования топологии коммутационной сети и синтеза древовидной сети с использованием концентраторного перекрытия; обосновании методов построения комбинированных дерево-гиперкубических топологий, обладающих преимуществом двух распространённых базовых топологий; разработке базовой структуры интегрированной системы защиты информации; разработке специального алгоритма оперативного мониторинга топологии сети, обеспечивающего высокую оперативность обнаружения несанкционированных подключений к сети при минимальных вычислительных затратах; разработке специальных методов шифрования данных, отличающихся простотой аппаратно-программной реализации; построении алгебраической модели и метода синтеза оптимальных структур специализированных вычислительных устройств шифрования данных.

Основные научные положения, выносимые на защиту. Автор защищает следующие результаты и выводы, полученные в ходе выполнения диссертационной работы:

- проблемно-ориентированный подход к синтезу корпоративных компьютерных сетей, объединяющий этапы синтеза топологий компьютерных сетей и построение интегрированной системы защиты информации;
- необходимость отнесения задач синтеза структур компьютерных сетей к классу полнопереборных (NP) задач с многопараметрической оптимизацией;
- целесообразность рассмотрения проблемы сегментирования структуры слабосвязанного графа как задачи формирования минимального подмножества сочленения, решение которой обеспечивает высокую скорость сходимости;
- комбинаторный метод декомпозиции структур компьютерных сетей, реализуемый с минимальными вычислительными затратами по сравнению с существующими;
- способ многопараметрической оптимизации структуры древовидных корпоративных компьютерных сетей на заданном множестве сетевых уровней;
- алгоритмы формирования терминальной и коммутационной сетей;
- показатели эффективности топологических структур, ориентированные на массовое распараллеливание вычислительных процессов;
- основные принципы оценки уровня системы защиты информации, базирующиеся на простоте механизма защиты, закрытости всех возможных каналов утечки информации, не строгой секретности механизма защиты, разделении прав и полномочий пользователей, минимальности полномочий, максимальной обособленности механизма защиты, психологической привлекательности;

- целесообразность включения в состав системы защиты информации (наряду с типовыми средствами) специальных комбинированных средств защиты, позволяющих повысить уровень защищенности сетей,
- модифицированные методы шифрования данных, отличающиеся от существующих простотой аппаратно-программной реализации и высокой криптостойкостью процессов шифрования.

Практическая ценность работы состоит в том, что разработанный комплекс программ позволяет проектировать проблемно-ориентированные корпоративные компьютерные сети с оптимальным концентраторным перекрытием и разбиением на сегменты. Это имеет важное практическое значение в связи с требованиями к надёжности функционирования, обеспечению эффективности использования каналов связи и информационной безопасности сети. Предложенная интегрированная система защиты информации позволяет повысить эффективность системы защиты за счет сокращения времени шифрования в 1,3 раза и увеличения криптостойкости в 1,4 раза по сравнению со стандартными методами. Предложенная алгебраическая модель и метод синтеза специализированных устройств сети могут быть применены при синтезе и выборе оптимальных структур устройств защиты информации, используемых как устройства оперативного шифрования в составе интегрированной системы защиты компьютерных сетей, так и автономно.

Реализация результатов работы. Разработанные методы и алгоритмы нашли практическое применение в Республиканском Информационно-аналитическом центре, в Государственной акционерной железнодорожной компании «Узбекистон темир йуллари», показав высокую эффективность при структурном синтезе топологии корпоротивных сетей; декомпозиции структур компьютерных сетей; организации систем защиты информации; синтезе специализированных устройств защиты информации; повышении надежности системы защиты информации компьютерных сетей.

Внедрение этих разработок обеспечило совокупной экономический эффект в размере 1 млн. 610 тыс. сумов в год.

Теоретические разделы работы вошли в программы ряда специальных дисциплин и используются в учебном процессе в Ташкентском государственном техническом университете имени Абу Райхана Беруни при чтении курсов лекций по предметам «Топология вычислительных сетей», «Безопасность информации», «Специальные средства вычислительных сетей», «Технические средства защиты информации», «Программно-аппаратная защита информации» и при выполнении диссертационных работ магистрантами специальности 5А521901-«Вычислительные машины, комплексы, системы и сети» и 5А521909-«Информационная безопасность».

Апробация работы. Основные положения диссертационной работы докладывались и обсуждались на ряде симпозиумов, совещаний и семинаров, в том числе, на ежегодных республиканских научно-теоретических и технических конференциях профессорско-преподовательского состава ТГТУ (Ташкент, 1989-2002 г.); на межвузовской научно-теоретической конференции молодых учёных (Ташкент, апрель 1987 г.г.); всесоюзной научно-технической конференции " Измерительные и информационные системы" (Ташкент, сентябрь 1987 г.); Всесоюзной научно-технической конференции «Математическое, алгоритмическое и техническое обеспечение АСУ ТП» (Ташкент, июль 1988 г.); республиканской научно-технической конференции «Применения микро ЭВМ и микропроцессоров в народном хозяйстве» (Ташкент, июль 1988 г.); республиканской научно-технической конференции «Достижения науки молодых-производству» (Ташкент, апрель 1991 г.); международной научно-технической конференции «Системный анализ, моделирование, управление сложными процессами и объектами на базе ЭВМ» (Ташкент, ноябрь 1993 г.); республиканской научно-технической конференции «Юксак малакали мутахассислар-тараккиёт омили» (Ташкент, 1998 г.); National seminar and trading course System and Network security. UNESCO (Tashkent, 1999 г.); республиканской научно-технической конференции «Моделирование и информационные технологии» (Киев, 1999 г.); World Conference on Intelligent System for Industrial Automation (WCIS 2000), (Tashkent, 2000); республиканской научно-технической конференции «Информационная и коммуникационная технология в учебном процессе» (Ташкент, 2000 г.); республиканской научной конференции «Современные проблемы автоматизации и программирования» (Ташкент, 2001 г.); республиканской научно-технической конференции профессоров и преподавателей «Технические науки и глобальные проблемы XXI века» (Ташкент, 2001 г.); республиканской научно-технической конференции «Информация, информационная технология, информационная безопасность» (Ташкент, 2002 г.); международной научно-технической конференции «Техника и технология дистанционного образования» (Ташкент, 2002 г.); XV международной научной конференции «Математические методы в технике и технологиях» (ММТТ-XV) (Тамбов, 2002 г.); Second World Conference on Intelligent System for Industrial Automation (WCIS-2002), (Tashkent, 2002)

Публикации. Основные результаты диссертационной работы опубликованы в сорока восьми печатных работах и содержатся в трёх научно-технических отчётах по теме ГНТП ГКНТ РУз.

Структура и объём диссертации. Диссертационная работа состоит из введения, шести глав, заключения, списка литературы и приложения. Основная часть содержит 173 страницы печатного текста, 63 рисунка и 15 таблиц. Приложение содержит 46 страниц. Список литературы включает 110 наименований.

Автор выражает благодарность доктору технических наук, профессору Ганиеву С.К. за научные консультации и обсуждение результатов работы на различных этапах её выполнения.

Содержание работы

Во введении показана актуальность темы диссертации, дан краткий анализ состояния трактуемой проблемы, определены цель и задачи исследования. Охарактеризована научная новизна и показана практическая ценность результатов работы, сформулированы основные научные положения, выносимые на защиту.

В первой главе приводятся топологические структуры и параметры корпоративных компьютерных сетей, а также освещены основные подходы к построению топологии сетей и приведены результаты анализа их метрических характеристик. Рассматриваются проблемы информационной безопасности компьютерных сетей и основные функции системы защиты информации. Сформулированы принципы проблемно-ориентированного синтеза топологий компьютерных сетей с интегрированной системой защиты. Приводится модель системы защиты информации, являющиеся математической основой для разработки и исследования конкретных систем защиты информации.

Отмечено, что проблема обеспечения безопасности информации в корпоративных компьютерных сетях сложна и многогранна и требует решения ряда взаимосвязанных проблем. К их числу относятся: оптимизация топологии сети; сегментирование или декомпозиция структуры сети в соответствии с ее компонентами и с учетом уязвимых мест; построение оптимального дерева концентраторов; разработка эффективной системы защиты информации; создание методики оценивания уровня безопасности корпоративных компьютерных сетей; разработка специальных методов и средств защиты информации; обеспечение совместимости и управляемости компонентов системы защиты информации.

Эти проблемы обусловлены недостатками, присущими корпоративным сетям. качественно усложняющими обеспечение безопасности обработки по сравнению с отдельной компьютерной системой, а именно: распределенность ресурсов; «многопользовательский» режим работы; сложность операционной системы; неопределенность периферии; множественность точек атак; неизвестность траектории доступа, слабая защищенность линии связи и т.д.

Для решения задач оптимизации и сегментирования (декомпозиции) топологии сети, от которых зависят такие важные параметры сетей, как задержка при передаче сообщений, сложность алгоритмов маршрутизации, показатели отказоустойчивости, уровень системы безопасности и возможности диагностики компонентов сети, предлагается использовать дескриптивную метрику, которая включает в себя множество характеристик, определяющих, с одной стороны, возможность выбора оптимальных архитектурных решений на этапе проектирования, а с другой стороны, возможность оценки выбранной архитектуры

компьютерных сетей с точки зрения соответствия поставленным задачам. Результаты исследований на множестве топологических построений подтвердили целесообразность использования дескриптивной метрики как инструмента определения таких показателей качества сетей, как диаметр топологической организации, число коммуникационных линий, стоимость сети, время выполнения операций и оперативность обслуживания заявок.

Можно выделить три основных подхода к построению топологии сетей. Первый базируется на использовании двухточечных линий связи, каждая из которых объединяет только два узла сети. При этом вопросы взаимодействия узлов распределяются в пространстве. Второй подход базируется на использовании многокаскадных коммутирующих сетей и решает вопросы взаимодействия некоторого множества узлов путем распределения функций коммутации в пространстве и во времени. И, наконец, третий подход базируется на использовании общей шины, с помощью которой взаимодействия узлов распределяются во времени. Второй и третий подходы, основанные на пространственно-временном и временном распределении функций взаимодействия узлов в сети к построению коммутирующих сетей, неприемлемы и накладывают существенные ограничения на общую производительность сети. В связи с этим при структурном описании компьютерных сетей используется только первый подход, в рамках которого предложено множество различных топологических построений (линейный, двухмерный, кольцевой, звездообразный, кубический и полносвязный).

Широкое использование нашли два основных типа топологии сетей: древовидные и распределенные. Если представить топологию корпоративной компьютерной сети в виде графов, то распределенным сетям будут соответствовать циклические графы, а древовидным сетям – ациклические.

Критерии оптимальности синтеза топологии той или иной сети могут быть различными и определяются целями и задачами, стоящими перед проектировщиками сети. Синтез топологии корпоративной сети может осуществляться как по одному, так и по нескольким критериям одновременно.

Метод ветвей и границ, обеспечивающий довольно высокую точность решения, не находит широкого применения в задачах синтеза топологии корпоративных компьютерных сетей с большим количеством параметров оптимизации, поскольку при этом дерево решения растёт по экспоненциальному закону.

Установлено, что эффективные топологии корпоративных сетей могут формироваться при учете всех специфических особенностей проектируемой сети и на основе объединения различных типовых топологических организаций в единую

- иерархическую организацию, т.е. при использовании проблемно-ориентированного подхода к синтезу топологии сетей.

Разработка эффективных средств защиты информации корпоративных сетей как согласованной совокупности средств требует определения базовой модели построения системы защиты. В работе в качестве таковой выбрана модель Белла и Ла-Падула, в которой предусмотрено обязательное использование диспетчера доступа, обеспечивающее гибкость системы защиты, т.е. возможность перехода от одной платформы защиты к другой в динамическом режиме. Задачу декомпозиции топологии компьютерной сети предлагается решать как задачу определения минимального подмножества сочленения графа.

Во второй главе предлагаются комбинированный способ оптимального сегментирования топологии корпоративной сети и метод декомпозиции структуры корпоративной компьютерной сети.

Для решения задач сегментирования топологии корпоративной компьютерной сети предлагается использовать комбинированный способ, в котором сеть представляется в виде множества отдельных сегментов (подсетей), объединенных между собой шлюзами. При этом в качестве критерия оптимизации сегментирования используется отношение интенсивности внешних потоков к внутреннему. Оптимальной следует считать топологию сети с минимальным значением суммы всех внешних потоков сегментов.

Исходными данными для сегментирования являются топология сети передачи данных, задаваемая с помощью множества вершин графа сети $A=|a_{ij}|_n$ и множества его ребёр $R=|r_{ij}|_m$. Тогда интенсивность всего множества информационных потоков представляется в виде матрицы $\Lambda=|\lambda_{ij}|_n$. Далее определяется загрузка каналов передачи данных $L=|l_{ij}|_n$ и их пропускная способность $T=|t_{ij}|_n$.

При условии $R=A$ *и* $\lambda_{ij} \le t_{ij}$ справедливо равенство $A=L$, *т.*е. при совпадении структуры потоков в сети с ее топологией и отсутствии перегрузки каналов передачи данных значение их загрузки полностью совпадает с интенсивностью информационных потоков. В противном случае задаётся обводной путь передачи данных через дополнительные вершины, что приводит к увеличению загрузки сети передачи данных.

Отношение $k_{ij}=l_{ij}/t_{ij}$ представляет собой коэффициент использования каналов передачи данных и является характеристикой эффективности загрузки сети передачи данных, среднее значение которой определяется как

$$k_{ср} = \sum_{ij} k_{ij} / m.$$

Задачу определения минимального подмножества сочленения можно сформулировать следующим образом: для произвольных вершин A_i *и* A_j графа

$G(A,R)$, входящих в подмножество $a_i \in A_1$ $a_j \in A_2$, найти подмножество B, обеспечивающее

1) $A_1 \cap B = \varnothing$;
2) $A_2 \cap B = \varnothing$;
3) $A_1 \cap A_2 = \varnothing$;
4) $A_1 \cup A_2 = A$;
5) $B = min$.

Соотношение между рассматриваемыми подмножествами определяется выражением:

$$B = A - (A_1 \cup A_2).$$

Очевидно, подмножество B будет минимальным при максимальных подмножествах A_1 и A_2. Таким образом, задача определения минимального подмножества B может быть сведена к определению максимальных подмножеств A_1 и A_2.

При увеличении размерности исходной матрицы инцидентности значительно возрастают затраты на перебор всех вариантов. Поэтому предлагается алгоритм решения задачи, основанный на формировании полной подматрицы, у которой $l = min$. При этом используется правило эквивалентной перестановки строк и столбцов матрицы инцидентности, при котором не нарушается топология графа.

Согласно алгоритму сегментирования вначале выбирается i-я строка с $\max \sum_{j=1}^{n} a_{ij}$ и переставляется с первой строкой, соответственно переставляются и одноименные столбцы.

Затем выбирается k-я строка по условию

$$\max \sum_{j=1}^{n} (a_{ij} \bigcap a_{kj}),$$

которая меняется со второй строкой, а при наличии нескольких строк с одинаковой суммой выбирается строка с $max\ a_{kj}$.

Предложенный алгоритм матричных преобразований приводит исходную матрицу смежности к виду, близкому к блочному.

Анализ полученной матрицы позволяет определить локальные зоны и связывающие их ребра. Однако в случае сильно связного графа возникает необходимость перераспределения потоков с последующим удалением остальных ребер графа. В этом случае среди выбранных множеств сочленения определяется множество с минимальным значением V и $\overline{l_i}$. Дальнейший процесс оптимизации заключается в удалении одного или нескольких ребер l_{ij} и перераспределении нагрузки до тех пор, пока не будет выполняться условие

$$\sum_{i=1}^{V} l_{ij} \geq \sum_{i=1}^{V} \overline{l_{ij}}.$$

В реальных условиях корпоративные компьютерные сети представляют собой совокупность локальных сетей, для которых характерно ограничение на диаметр сети. В работе предлагается алгоритм декомпозиции топологии сети, отличающийся от известных тем, что учитывается ограничение на диаметр сети. При этом задачу формирования полной подматрицы решают относительно "полных" нулевых подматриц. При наличии подмножества сочленения матрица инцидентности исходного графа может быть представлена в виде следующей блочной матрицы:

M_{11}	M_{12}	M_{13}
M_{21}	M_{22}	M_{23}
M_{31}	M_{32}	M_{33}

Здесь подматрицы $|M_{11}|_{mxm}$ и $|M_{33}|_{lxl}$ определяют подграфы $G_1\{A_1,S_1\}_m$ и $G_3\{A_3,S_3\}_{kl}$, а подматрица $|M_{22}|_{lxl}$ соответствует подмножеству сочленения исходного графа. Величина I определяется из соотношения $I=n-(m+k)$. В свою очередь, подматрица определяет ребра между подграфом и подмножеством сочленения. Совокупность ребер образует соответствующий разрез, а подматрица определяет связи и разрез между подграфами, вошедшими в подмножество сочленения. Таким образом, можно утверждать, что для подграфа размерностью R в матрице инцидентности исходного графа может быть выделена нулевая подматрица размером mxk, а также две подматрицы сочленения размером (mxl) и (lxk), где $I=n-(m+k)$. При $I=0$ графы распадаются на два несвязанных подграфа.

Следовательно, оптимальным разбиением графа G на два подграфа G1 и G2 следует считать такое разбиение, при котором множество сочленения B→min, при k→m и m+k→n.

Целесообразность такого подхода определяется особенностью структуры матрицы инцидентности несвязного графа. Исключить операции перестановки строк и столбцов можно за счет представления строк матрицы в виде множеств и выполнения операций над множествами.

Основной операцией алгоритма является последовательное объединение множеств A_i между собой. В качестве исходного множества A_O выбирается множество A_i, образующееся путем объединения Ao с максимальным множеством A_i. Определяется число $r_i = k + m$, где k- количество объединенных множеств, m-размер множества A_m. После первого шага величина $r=2+m$.

На втором и последующих шагах аналогичным образом осуществляется объединение множества A_m с остальными $A_m = (A_0 \cap A_i)$. На каждом i-ом шаге вычисляется соответствующее значение ri. Процесс объединения заканчивается при $(k+m)=n$ или $i=n$. В этом случае исходный граф представляет собой два

подграфа, первый из которых содержит k, а второй m вершин. Вершины второго графа определяются множеством A_m, а первого – множеством A-A_m.

По сравнению с известными, данный алгоритм не использует матричного представления графа. Здесь исключены операции перестановки строк и столбцов матрицы.

Поскольку формирование подмножества A_m начинается с вершины, имеющей минимальное число ребер, количество операции на каждом шаге вычисления не превышает среднего числа ребер графа (r). В этом случае можно считать, что общее число операций не превышает величины (nxr)/2, что меньше, чем число операций в известных алгоритмах.

Третья глава посвящена вопросам проблемно-ориентированной организации корпоративных компьютерных сетей. Предлагается комбинированный метод синтеза топологии корпоративных компьютерных сетей, основа которого состоит в использовании классических математических методов –релаксации и градиента Лагранжиана. Рассматриваются вопросы синтеза топологии терминальной и коммутационной сетей. Кроме того, анализируется задача выбора эффективной структуры сети управляющих компьютеров.

Предложен комбинированный метод синтеза топологии корпоративной компьютерной сети, основанный на использовании двух классических методов релаксации и множителей Лагранжиана по критерию "стоимости" структуры древовидных сетей на заданном множестве сетевых уровней. Сущность подхода заключается в следующем: поставлена задача оптимизировать функционал $f(x)$, решение x которого лежит в области Ra с условием $R_a \subset R$. Ослабление имеет только однонаправленный характер, то-есть при округлении полученного результата мы можем сместиться с точки оптимума в большую сторону. Округляя решения к точке, в которой функционал имеет максимальную скорость нарастания, получаем целочисленное значение, наиболее близкое к оптимальному.

Лемма. При условии пологости функционала, решение, в котором он достигает значения, наиболее близкого к оптимальному, получается при округлении в точке, где имеет место максимальная скорость нарастания.

Доказательство. Известно, что скорость нарастания функции (т.е. первая производная) тождественно равна градиенту функции в этой точке:

$$\nabla_x f(x) = \frac{df(x)}{dx}$$

Данное выражение справедливо для любой точки x на всем диапазоне числовых значений функции $f(x)$, согласно которому прирост функции определяется как:

$$df(x) = \nabla_x f(x) dx.$$

Чтобы получить минимальное значение прироста функции, необходимо определить значения функционала

$$df(x) = \inf_{x}(|\nabla_x f(x)|dx).$$

Следовательно, минимальное значение прироста функции достигается при минимальном значении градиента функции в точке x и при одновременном минимальном приросте переменной x. Поскольку минимальное значение прироста переменной x обеспечивается малой скоростью точки x, то можно сделать вывод, что минимальный прирост функции прямо пропорционален минимальному значению градиента функции в данной точке, т.е. минимальной скорости нарастания функции. Лемма доказана.

В предлагаемом методе шаг направления выбирается как градиент от Лагранжиана $(L(\alpha,\beta))$, т.е.

$$\varphi^{m+1} = \varphi^{m} + \gamma \nabla_{\varphi} L(.,\varphi),$$

где φ^{m}-множитель на m-ом шаге итерации; γ - шаговый множитель; $\nabla_{\varphi} L(.,\varphi)$-градиент функции L по φ.

Для обеспечения наилучшей сходимости следует применить шаговый множитель, вычисляемый по следующим соображениям.

В соответствии с основами геометрии в малой окрестности точки x приращение функционала определяется как

$$\nabla_x L(x) = \mathrm{tg}(\alpha) = \frac{dL(x)}{dx}.$$

Отсюда можно определить

$$dx = dL(x)/\nabla_x L(x).$$

Данное выражение позволяет получить прирост функции, или другими словами, шаговый множитель:

$$\gamma = \frac{L_f - L(.,\varphi)}{\sum \nabla_{\varphi_k} L(.,\varphi)},$$

где $L(.,\varphi)$-численное значение Лагранжиана на данном шаге итерации, L_f-наперед заданное числовое значение оптимизационного функционала, а k-индекс элементов вектора множителей Лагранжиана.

Разработанный комбинированный метод синтеза топологии корпоративных компьютерных сетей, сочетающий в себе достоинства методов релаксации и градиента Лагранжа, позволяет находить решение, максимально приближаемое к оптимальному при большом количестве оптимизационных параметров.

Для сравнительной оценки предложенного метода синтеза с широкораспространенным при структурном синтезе методом насыщенного сечения проектирование велось параллельно по обоим методам.

При реализации комбинированного метода (КМ) количество вычислительных операций определяется по формуле:

$$C_{КМ}=I\cdot D\ (M\cdot J),$$

где D – количество допустимых уровней концентраторного перекрытия; I – количество точек размещения терминалов; J – количество точек расположения концентраторов; M – количество итераций.

При реализации метода насыщенного сечения (НС), где необходимо учитывать количество допустимых удалений связи между терминалом и концентратором γ, количество вычислительных операций определяется по формуле

$$C_{НС}=I\cdot J\cdot D\ (1+\gamma\cdot I).$$

В связи с тем, что количество итераций в сравниваемых методах имеют различные значения, а количество допустимых удалений связи между терминалом и концентратором учитывается только в методе насыщенного сечения, были использованы их усредненные значения.

Результаты сравнительной оценки приведены на рис.1 в виде графика, где T – количество вычислительных операций, N – количество элементов сети.

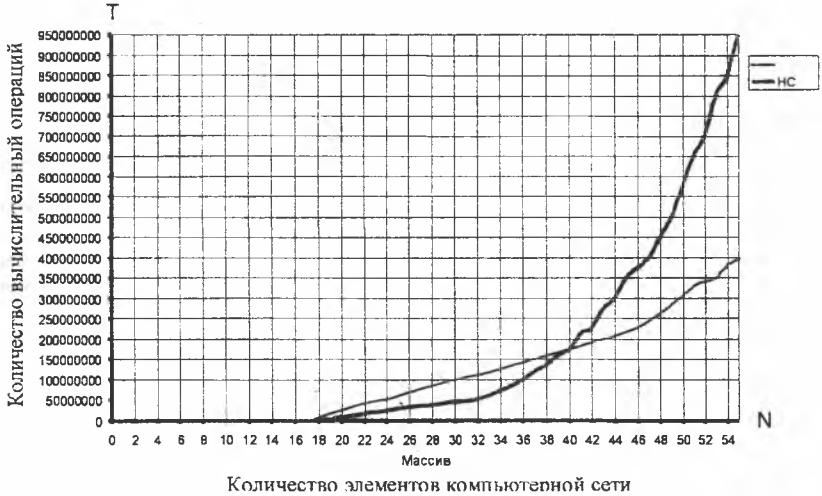

Рис.1. Сравнительная оценка комбинированного метода и метода насыщенного сечения.

Как видно из графика, количество вычислительных операций в комбинированном методе при небольших размерностях задачи в 1.8 раза больше,

нежели количество вычислительных операций в методе насыщенного сечения. Однако при больших размерностях задачи (что свойственно корпоративным компьютерным сетям), комбинированный метод требует в 2.3-2.5 раза меньше вычислительных операций.

Предложенный комбинированный метод подразумевает следующую последовательность процедур синтеза топологии терминальной сети:

1. Выбор варианта подключения терминальных компьютеров к концентратору с минимальной стоимостью или определение функции выгоды

$$P(x) = \sum_{i \in I} f_i \sum_{j \in J} \lambda_i x_{ij} .$$

2. Определение затрат на передающую среду для выбранного варианта подключения компьютеров к концентратору

$$C_1(x) = \sum_{i \in I} \sum_{j \in J} c_{ij} x_{ij} .$$

3. Определение затрат на возможные дополнительные порты

$$C_2(x) = \sum_{j \in J} c_j \sum_{i \in I} x_{ij} .$$

4. Определение затрат на подключение концентратора к сети:

$$C_3(y) = \sum_{j \in J} u_j y_j .$$

5. Определение итоговой выгоды:

$$Z(x, y) = \sum_{i \in I} f_i \sum_{j \in J} \lambda_i x_{ij} - \sum_{i \in I} \sum_{j \in J} c_{ij} x_{ij} - \sum_{j \in J} c_j \sum_{i \in I} x_{ij} - \sum_{j \in J} u_j y_j .$$

На данный функционал, как обычно, накладываются следующие ограничения:

$$\sum_{i \in I} x_{ij} \geq y_j, \forall j \in J; \qquad (1)$$

$x_{ij} \in \{0,1\}, \quad \forall j \in J, \quad \forall i \in I; \qquad (2)$

$y_j \in \{0,1\}, \quad \forall j \in J. \qquad (3)$

Ограничение (1) необходимо для исключения ситуации, когда терминал i установлен к j-му концентратору, но еще не подключен. В связи с тем, что к одному концентратору может подключаться несколько терминалов, данное ограничение нестрогое. Ограничения (2) и (3) объясняются начальными предположениями, поскольку переменные x_{ij} и y_{ij} принадлежат целочисленной области значений и представляют собой наличие либо отсутствие терминала или концентратора.

Применение метода релаксации для оптимизации полученного функционала требует предварительного анализа на наличие локальной выпуклости. При наличии последней граничные условия (2) и (3) имеют вид:

$x_{ij} \in \{0,1\}, \quad \forall j \in J, \quad \forall i \in I;$

$y_j \in \{0,1\}, \quad \forall j \in J.$

Поскольку стоимость подключения концентратора к терминальной сети представляет собой дискретную зависимость от количества портов, что приводит к увеличению числа переменных, и применение метода множителей Лагранжа требует перехода от двухмерной к трехмерной плоскости.

Лемма. При большом количество переменных, для решения задачи оптимизации единственным приемлемым решением является перенос функционала в трехмерную плоскость.

Доказательство. Пусть $f(x)$- некоторая функция, где x является вектором двух переменных (рис.2).

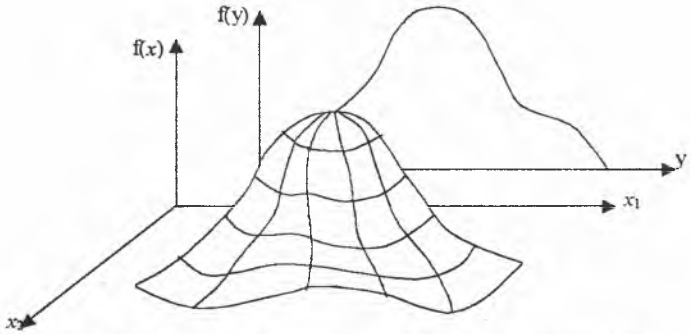

Рис. 2. Перенос функционала в трехмерную плоскость.

Тогда

$$y = Ax_1 + Bx_2 , \qquad (4)$$

где A и B числовые коэффициенты.

Наличие точек экстремума можно определить с помощью неравенства

$$\nabla^2_{x_1 x_2} f(x_1, x_2) > 0 \quad . \qquad (5)$$

Условием наличия точек экстремума для функции $f(x)$ является

$$\nabla^2_y f(y) > 0 \quad . \qquad (6)$$

Для функции $f(y)$ второй градиент после соответствующих преобразований будет вычисляться по следующему выражению:

$$\nabla^2_y f(y) = \frac{\partial^2 f(Ax_1 + Bx_2)}{A\,\partial x_1^2} + \frac{\partial^2 f(Ax_1 + Bx_2)}{B\,\partial x_2^2} + \frac{1}{2AB} \cdot \frac{\partial^2 f(Ax_1 + Bx_2)}{\partial x_1 \partial x_2}$$

или

$$\nabla^2_y f(y) = \frac{\partial^2 f(x_1)}{\partial x_1^2} + \frac{B}{A} \cdot \frac{\partial^2 f(x_2)}{x_2^2} + \frac{A}{B} \cdot \frac{\partial^2 f(x_1)}{x_2^2} + \frac{\partial^2 f(x_2)}{x_2^2} + \frac{1}{2AB} \cdot \frac{\partial^2 f(Ax_1 + Bx_2)}{\partial x_1 \partial x_2} .$$

Поскольку

$$\frac{\partial f(x_2)}{\partial x_1^2} = \frac{\partial f(x_1)}{\partial x_2^2} = 0,$$

в итоге получим

$$\nabla_y^2 f(y) = \frac{1}{2AB} \cdot \frac{\partial^2 f(Ax_1 + Bx_2)}{\partial x_1 \partial x_2} = \frac{1}{2AB} \cdot \nabla_{x_1 x_2}^2 f(Ax_1 + Bx_2)$$

или

$$\nabla_y^2 f(y) = \frac{C}{2AB} \cdot \nabla_{x_1 x_2}^2 f(x_1, x_2) > 0,$$

где C – постоянный коэффициент.

Лемма доказана.

Аналогичные математические выкладки можно выполнить и для n-мерного вектора:

$$\nabla_y^2 f(y) = \sum_{i,j=1}^{n} \frac{1}{2A_i A_j} \cdot \frac{\partial^2 f(y)}{\partial x_i \partial x_j} = \sum_{i,j=1}^{n} \frac{1}{2A_i A_j} \cdot \nabla_{x_i x_j}^2 f(x).$$

Учитывая приведенную лемму, можно перейти в трехмерную плоскость. В качестве весовых коэффициентов используются градиенты функционала в данной точке. Тогда функционал будет выглядеть следующим образом:

$$Z^1(x, y) = P(x, y) - Ax - By,$$

где x и y – переменные, вычисляемые как

$$x = \sum_{i \in I} \sum_{j \in J} \nabla_{x_{ij}} Z(x, y) x_{ij},$$

$$y = \sum_{j \in J} \nabla_{y_j} Z(x, y) \cdot y_j.$$

Здесь $P(x, y)$ – функция выгоды от подключения терминала.

Так как на функционал наложено ограничение (1), функция выгоды должна зависеть от обеих переменных. По характеру эта функция, скорее всего, похожа на функцию стоимости.

Коэффициенты A и B определяются следующим образом:

$$A = \sum_{i \in I} \sum_{j \in J} (c_{ij} + c_j),$$

$$B = \sum_{j \in J} u_j.$$

Согласно признаку выпуклости

$$\nabla_{xy} Z^1(x,y) > 0.$$

Тогда условием выпуклости функции будет неравенство

$$\nabla_{xy} P(x,y) - A - B > 0.$$

Таким образом, можно заключить, что при условии

$$\nabla_{xy} P(x,y) > A + B$$

мы имеем выпуклую функцию, при условии

$$\nabla_{xy} P(x,y) < A + B$$

имеет место вогнутая функция, а при условии

$$\nabla_{xy} P(x,y) = A + B$$

мы не имеем точек экстремума.

Предложенная последовательность процедур синтеза топологии терминальной сети удовлетворяет условиям сходимости для метода релаксации Лагранжа. Следует отметить, что при задании входных параметров необходимо учитывать выгоду от подключения терминала к концентратору. Это объясняется тем, что в зависимости от разницы между выгодой и затратами получим либо выпуклую, либо вогнутую поверхность.

В работе разработан алгоритм формирования топологии коммутационной сети на основе алгоритма формирования топологии терминальной сети. Он ориентирован на структуру сети с минимальной стоимостью подключения. Если выгоду от подключения концентраторов равномерно распределить между всеми концентраторами, то получим топологию коммутационной сети с минимальными затратами.

Для эффективного управления и организации взаимодействия компонентов корпоративной компьютерной сети необходимо выделить некоторое множество управляющих компьютеров, связанных в единую управляющую структуру.

Показано, что естественным вариантом объединения управляющих компьютеров в единую структуру является некоторая их иерархия, представленная дерево – кубической структурой. Оценены возможности использования различных базовых структур топологии сетей для построения иерархических дерево – гиперкубов и определены значения их метрических характеристик (табл.1).

В четвёртой главе освещены вопросы организации интегрированной системы защиты информации в корпоративных компьютерных сетях. Предлагается базовая структура интегрированной системы защиты информации, сочетающая в себе все информационные характеристики систем защиты и позволяющая унифицировать задачи обеспечения сетевой безопасности под эгидой единого управления. Приведены структуры специализированных программно-аппаратных средств интегрированных систем защиты информации, в которых с целью

повышения уровня безопасности интегрированной системы рекомендовано использование модифицированных алгоритмов шифрования данных и процедуры оперативного мониторинга топологии сети.

Таблица 1.

Метрические характеристики различных базовых структур компьютерных систем

Вид топологии	Диаметр	Степень	Средний диаметр	Связанный	Связанность	Стоимость	Плотность трафика
Шинная (Линейная)	N-1	2	(N+1)/3	1	1	N-1	2/3*(N+1)
Кольцо	[N/2]	2	(N+1)/4	2	2	N	(N+1)/4
Петля	$2(\sqrt{N}-1)$	4	$(2\sqrt{N})/3$	$\sqrt{N}$	2	$2(N-\sqrt{N})$	$1/3*\sqrt{N}$
Завернутая петля	$2[\sqrt{N/2}]$	4	$\sqrt{N/2}$	$2\sqrt{N}$	4	2*N	$1/4*\sqrt{N}$
Звезда	2	N-1	2	1	1	N-1	4/(N-1)
Дерево	2log((N+1)/2)	3	2log((N+1)/2)	1	1	N-1	2/3 log((N+1)/2)
Гиперкуб	$\log_2 N$	$\text{Log}_2 N$	$(\log_2 N)/2$	$\log_2 N$	N/2	$N/2 \log_2 N$	1
Гиперкуб с большим радиусом	R	$3(N^{1/r}-1)$	r/2	$\frac{N*N^{1/r}}{4}$	$3(N^{1/r}-1)$	$\frac{3N(N^{1/r}-1)}{2}$	$\frac{R}{3(N^{1/r}-1)}$
Комплекс-ный граф	1	N-1	1	N-1		N(N-1)/2	2/(N-1)

Предложена базовая структура интегрированной системы защиты информации, состоящая из следующих компонентов: межсетевого экрана, средств обнаружения несанкционированных воздействий, средств анализа защищенности, специализированных программно – аппаратных средств защиты и устройства управления.

Межсетевые экраны устанавливаются в точке соприкосновения корпоративных компьютерных сетей передачи данных с сетями общего пользования. Они ограничивают поток информации, поступающей к сети передачи данных общего пользования – во внутреннюю сеть передачи данных. Такое ограничение имеет место в результате функционирования механизмов фильтрации сетевого трафика и аутентификации субъектов сети передачи данных, претендующих на доступ к информационной сфере.

Средства обнаружения несанкционированных воздействий позволяют проводить мониторинг и анализ работы сети передачи данных, а также фиксировать попытки нарушения информационной безопасности сети. Определив факт атаки, система обнаружения пытается локализовать источник и сообщает администратору о необходимости принятия соответствующих мер.

Средства анализа защищенности предназначены для определения степени защищенности компьютерной сети. Они проводят осмотр сети на наличие мест уязвимости и на базе полученной информации предлагают возможные решения, направленные на их устранение.

Специализированные программно-аппаратные средства защиты предназначены для реализации специальных методов защиты информации (биометрическая аутентификация, оперативный мониторинг топологии сети и т.д.) и позволяют агрегировать данные, обрабатывать тривиальные ситуации и уведомлять администраторов об исключительных событиях, требующих незамедлительного внимания к себе.

Устройство управления отвечает за контроль и управление процессами функционирования компонентов системы защиты.

Эксплуатация интегрированной системы защиты информации должна выполняться под контролем администратора. Перед установкой на конкретный хост должен быть оценен уровень его защищенности с помощью средств безопасности. Только убедившись в том, что хост не имеет точек уязвимости, администратор вправе выполнить процедуру установки.

Рассмотрены функции, выполняемые интегрированной системой защиты информации. Приведены конкретные примеры совместного использования различных компонентов интегрированной системы. Сформулированы требования, выполнение которых обеспечивает эффективное функционирование интегрированной системы.

Разработаны модифицированные алгоритмы шифрования, использующие различные методы шифрования и обеспечивающие более высокую криптостойкость системы. В частности, разработана трехключевая система шифрования данных на базе одно- и двухключевого алгоритмов шифрования. При этом использованы стандартные методы шифрования DES с секретным ключом и шифратор RSA с открытым ключом.

Система состоит из трех ключей: сеансовый, открытый и секретный. Система с секретным ключом состоит из сеансового ключа, шифратора DES и DES дешифратора. Система же с открытым ключом образуется из открытого ключа, секретного ключа, шифратора RSA и дешифратора RSA. Сеансовый ключ для одноключевой системы является секретным и одновременно выступает источником входной информации для системы с открытым ключом. Эта информация должна храниться в какой-нибудь области памяти или непосредственно отправляться по каналу связи к получателю информацию. Если сеансовый ключ передается по отдельному каналу связи, шифрование ключа и открытого текста не имеет смысла. В связи с этим разработаны различные методы передачи секретного ключа, одним из которых является размещение секретного

ключа в составе шифрованной информации в рассеянном виде, что производится по заранее выбранному закону.

Отличительными особенностями разработанной системы шифрования являются:

– расширение секретного DES ключа на 128 бит;

– шифрование секретного DES ключа с помощью открытого ключа;

– размещение секретного DES ключа в передаваемой информации путем ее рассеивания.

В упомянутых модифицированных методах длина ключей увеличена в два раза от 64 до 128, при этом количество циклов шифрования сокращено от 16 до 12. Если учесть, что между длиной ключа, количеством циклов шифрования и криптостойкостью существует прямая пропорциональная зависимость, то увеличение длины ключа на 64 и уменьшение количества циклов на 8, в конечном итоге, приводит к увеличению криптостойкости в 1,4 раза.

За счет совмещения во времени процессов преобразования ключа шифрования исходных данных и логических операций над ключом, а также сокращения числа циклов шифрования затраты времени на шифрование данных, как показали результаты расчета, сокращаются в 1,3 раза.

Разработан специальный алгоритм оперативного мониторинга топологии сети, позволяющий определять место несанкционированного подключения станции к сети. Основной принцип мониторинга топологии сети заключается в том, что программа мониторинга посылает пакет с запросом о конфигурации одновременно всем станциям данной сети, на сокет 0456h, указав в качестве номера сети путь; в качестве адреса станции –значение *FF....Fh*. В ответ на данный запрос все подключенные к сети станции посылают сведения о своей конфигурации станции, которая отправила пакет с запросом.

Проанализировав пришедшую от станций диагностическую информацию, программа мониторинга может определить конфигурацию подключенных станций. Программа оперативного мониторинга топологии сети посылает запросы только тем станциям, которые подключены нелегально и исключает из запроса станции, которые имеют право на подключение. Получив информацию от станций, программа оперативного мониторинга формирует информацию о несанкционированных подключенных станциях.

В пятой главе рассмотрены вопросы разработки специализированных программно-аппаратных средств интегрированной системы защиты. Предлагаются специальные методы шифрования данных, предназначенные для совместного использования с типовыми методами шифрования данных и отличающиеся простотой аппаратной реализации, а также высокой оперативностью. Освещены также вопросы теории и практики синтеза структур аппаратных средств защиты

информации и приведен алгоритм синтеза с учетом сформулированной задачи оптимизации их структур..

Предложен специальный метод шифрования информации, в соответствии с которым осуществляются: первичная перестановка; первичная подстановка; вторичная перестановка; вторичная подстановка; сложение по модулю 2. Для выполнения перестановок и подстановок составляются специальные таблицы, в которых сообщения записываются по строкам, а считываются по столбцам. После перестановок и подстановок сообщения складываются с ключами по модулю 2, и первый цикл шифрования заканчивается.

Разработан также специальный алгоритм шифрования с перестановкой и логическим преобразованием, реализующийся в пяти тактах. Криптостойкость данного метода шифрования зависит от таблицы перестановки элементов и от ключа. При этом таблицы перестановок элементов и ключ должны быть известны только отправителю и получателю.

Предложен специальный метод шифрования данных, основанный на операциях над матрицами (операциях умножения вектора на матрицу $\overline{D} \cdot M = \overline{B}$ при шифровании и $\overline{B} \cdot M^{-1} = \overline{D}$ при дешифровании).

Вектор шифрованных данных для четырёхмерного случая определяется следующим образом:

$$\begin{vmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{vmatrix} = \begin{vmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{vmatrix} \cdot \begin{vmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \\ m_{41} & m_{42} & m_{43} & m_{44} \end{vmatrix}.$$

Откуда:

$$b_1 = d_1 m_{11} + d_2 m_{12} + d_3 m_{13} + d_4 m_{14}, \quad b_2 = d_1 m_{21} + d_2 m_{22} + d_3 m_{23} + d_4 m_{24},$$
$$b_3 = d_1 m_{31} + d_2 m_{32} + d_3 m_{33} + d_4 m_{34}, \quad b_4 = d_1 m_{41} + d_2 m_{42} + d_3 m_{43} + d_4 m_{44}.$$

Для реализации дешифрования, т.е. восстановления, необходимо, предварительно определив обратную матрицу $\|M\|^{-1}$, реализовать следующие выражение:

$$\overline{B} \cdot \|M\|^{-1} = \overline{D},$$

где

$$\begin{vmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{vmatrix} \cdot \begin{vmatrix} \overline{m}_{11} & \overline{m}_{12} & \overline{m}_{13} & \overline{m}_{14} \\ \overline{m}_{21} & \overline{m}_{22} & \overline{m}_{23} & \overline{m}_{24} \\ \overline{m}_{31} & \overline{m}_{32} & \overline{m}_{33} & \overline{m}_{34} \\ \overline{m}_{41} & \overline{m}_{42} & \overline{m}_{43} & \overline{m}_{44} \end{vmatrix} = \begin{vmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{vmatrix}.$$

Отсюда

$$d_1 = b_1\overline{m}_{11} + b_2\overline{m}_{12} + b_3\overline{m}_{13} + b_4\overline{m}_{14}, \qquad d_2 = b_1\overline{m}_{21} + b_2\overline{m}_{22} + b_3\overline{m}_{23} + b_4\overline{m}_{24},$$

$$d_3 = b_1\overline{m}_{31} + b_2\overline{m}_{32} + b_3\overline{m}_{33} + b_4\overline{m}_{34}, \qquad d_4 = b_1\overline{m}_{41} + b_2\overline{m}_{42} + b_3\overline{m}_{43} + b_4\overline{m}_{44}.$$

Процесс шифрования по этому методу реализуется в два такта. На первом такте выполняется только операция умножения, затраты времени на которую можно приравнивать четырем сложениям $\left(t_1 = t_{умн} = 4t_{сл}\right)$. Второй такт требует в среднем затраты времени, равные 1,5 сложениям $\left(t_2 = t_{сум/выч} = 1{,}5t_{сл}\right)$. Таким образом, для реализации как процесса шифрования, так и процесса дешифрования потребуется время, равное $T_{шиф} = T_{дешиф.} = 5{,}5\ t_{сл.}$, что свидетельствует о высокой оперативности реализации процесса шифрования предлагаемым методом.

Разработаны структурные, функциональные и принципиальные схемы специализированных устройств шифрования данных специальными методами.

Для обеспечения высокой оперативности процесса шифрования блоки и узлы специализированных устройств реализованы на матричных схемах, где используется принцип временного перекрытия выполнения операций. С целью повышения криптостойкости методов в составе специализированных устройств использованы ускоренные сумматоры с управляемыми ключами. При этом тип выполняемой операции над данными определяется в зависимости от значения ключа и наличия или отсутствия межразрядного переноса.

Предложен формализованный метод синтеза структур специализированных устройств защиты информации на базе алгебраической модели. Последняя задается в виде четверки

$$m_{суз} = <k, 0_{(.)}, A, P>,$$

где $0_{(.)}$- непустое множество входных, внутренних и выходных переменных;
A – множество типовых алгоритмов или операторов; P – множество отложений, заданных $\theta_{(.)} \cup A$; k – параметр, учитывающий особенности синтезируемых устройств.

В качестве критерия оценки оптимальности структуры специализированных устройств шифрования использована функция, характеризующая относительную простоту информационно-аппаратурных связей между их блоками.

Шестая глава посвящена вопросам организации корпоративной сети с интегрированной системой защиты информации Республиканского информационно-аналитического центра (РИАЦ). Кроме того, здесь же приведено описание функционирования корпоративной сети высших учебных заведений города Ташкента на организационно-функциональном уровне.

В результате применения предложенного метода комбинированного синтеза топологии сети получена структура корпоративной сети РИАЦ, сочетающая в себе древовидную, радиальную и шинную структуры. Применение алгоритма

сегментирования структуры сети к проектируемой сети позволило получить 12 подсетей (сегментов) с максимальной внутренней интенсивностью потоков. Построено дерево концентраторов проектируемой корпоративной сети. Разработана структура и определён состав центрального офиса корпоративной сети РИАЦ и оптимальный вариант структуры для его филиалов.

Интегрированная система защиты корпоративной сети РИАЦ организована на базе мостов, установленных в выходных точках сегментов, программного комплекса «ФПСУ», специальных программных модулей шифрования и средств оперативного мониторинга топологии сети.

Установка мостов в выходных точках сегментов приводит к локализации трафика, что способствует повышению производительности за счет изоляции трафика одной подсети от трафика другой, а также к уменьшению возможности несанкционированного доступа к данным, благодаря фильтрации, то есть анализа их в соответствии с совокупностью критериев.

Программный комплекс «ФПСУ» позволяет создавать в общей транспортной сети виртуальную реальность с повышенной степенью защиты от несанкционированного доступа, осуществлять контроль и управление входящими и исходящими межсетевыми потоками информации, обеспечивая при этом повышение в 2,4 раза пропускной способности виртуальной системы сети при безопасном взаимодействии подсетей.

Интегрированная система защиты сети РИАЦ не имеет собственного сетевого адреса и к нему не может быть осуществлено обращение по сети. Компьютер с установленной подсистемой удаленного администрирования комплекса имеет сетевой адрес. Однако соединение с ним по сети могут осуществлять только взаимно зарегистрированные межсетевые экраны.

Разработана организационно-функциональная структура корпоративной сети ВУЗов Ташкента. Сеть состоит из «сегментов» -комплексов технических и программных средств, создаваемых в ВУЗах, которые через Internet взаимодействуют между собой и с другими учебными заведениями и научно-исследовательскими учреждениями (колледжи, лицеи, НИИ АН РУз и.т.д), а также с их персоналом, выполняющим как традиционные, так и дополнительные функции, определяемые участием ВУЗов в работе корпоративной сети.

Построена схема инфраструктуры корпоративной сети, при этом задействованы все каналы, уже имеющиеся в ВУЗах и использующие протокол TCP/IP. При отсутствии же таковых предусмотрена их организация с учетом минимизации необходимых расходов.

Определен общий состав программно-аппаратного комплекса телекоммуникационной инфраструктуры сети. Выделены функциональные подсистемы комплекса.

Значимость полученных результатов заключается в том, что при проектировании сложных корпоративных сетей с большим количеством узлов одним из наиболее эффективных методов синтеза является предложенный нами комбинированный метод. Кроме того, необходимо отметить, что предложенный метод построения древовидных концентраторов может найти применение и при оптимизации структур корпоративных сетей.

Наличие в составе интегрированной системы устройства управления адаптивной системы шифрования данных и других специализированных средств позволяет предлагаемой системе приблизиться к уровню интеллектуальных систем.

Разработанные методы и алгоритмы способствуют реализации параллельного синтеза интегрированной системы защиты и собственно корпоративной сети.

Промышленные испытания разработанных методов, алгоритмов и программных модулей проводились в условиях корпоративной сети РИАЦ. Испытания показали:

- малые затраты времени на проектирование и оптимизацию топологии корпоративной сети;
- повышение надежности и гибкости системы защиты информации вследствие применения специальных программных модулей шифрования данных и оперативного мониторинга топологии сети;
- предложенные алгоритмы концентраторного перекрытия оказались также конструктивными и при решении задач оптимального подключения как терминалов к концентратору, так и концентраторов к центральному концентратору;
- разработанные экономичные специализированные устройства шифрования данных позволяют повысить криптостойкость системы защиты, сохраняя при этом те же временные показатели передачи данных;
- предложенный в работе формализованный метод синтеза специализированных устройств защиты может найти приложение и для аналогичных и близких к нему компонентов компьютерных сетей и устройств управления.

ЗАКЛЮЧЕНИЕ

Рассмотренные в данной диссертационной работе вопросы ставили своей целью показать перспективность корпоративных компьютерных сетей с интегрированной системой защиты информации, сформулировать на основе теоретических и экспериментальных исследований рекомендации по их эффективной разработке, а также определить оптимальную структуру интегрированной системы защиты информации, позволяющую представить общую картину сети с точки зрения ее безопасности.

В соответствии с этой целью в работе поставлены, решены и доведены до практической реализации задачи синтеза корпоративных сетей с интегрированной системой защиты информации, позволяющие совместить процесс разработки системы защиты информации с процессом синтеза самой корпоративной сети.

Основные результаты, полученные в ходе выполнения диссертационной работы сводятся к следующему:

1. Обоснована перспективность проблемно-ориентированного подхода к созданию системы защиты информации корпоративных компьютерных сетей, заключающегося в объединении этапов синтеза топологии компьютерной сети и систем ее защиты.

2. Для корпоративных компьютерных сетей с большим числом оптимизируемых параметров обоснована необходимость разработки нового метода синтеза их топологии, поскольку существующие методы обладают высокой чувствительностью к дополнительным параметрам оптимизации.

3. Обоснована целесообразность решения проблемы сегментирования структуры слабосвязанного графа топологии корпоративной компьютерной сети как задачи формирования минимального подмножества сочленения и определены необходимые и достаточные условия существования сети. Доказано, что для подграфов размерности m и k в матрице инцидентности исходного графа может быть выделена нулевая подматрица размером m×k и две подматрицы сочленения размером (m×l) и (l×k), где l=n-(m+k). При l=0 граф распадается на два несвязных подграфа.

4. Разработан комбинаторный метод декомпозиции исходного графа топологии корпоративной компьютерной сети, отличающийся от известных высокой скоростью сходимости, а алгоритм, реализованный на его основе, позволяет представить граф корпоративной компьютерной сети в виде двух слабосвязных графов.

5. На основе методов релаксации и градиента Лагранжа разработан комбинированный метод синтеза топологии корпоративных компьютерных сетей, отличающийся высокой скоростью сходимости процесса оптимизации структур. Применение метода к задачам формирования топологии терминальной и коммутационной сетей привело к сокращению вычислительных процедур и ускорению процесса сходимости.

6. Доказано, что синтез эффективных структур управляющих компьютеров корпоративной сети необходимо осуществлять на базе дерево-гиперкубической топологии ТН (b,d), обладающей преимуществами наиболее распространенных базовых топологий.

7. Установлено, что для создания интегрированных систем защиты информации в корпоративных компьютерных сетях со всеми функциональными

характеристиками безопасности целесообразно включать в структуру системы защиты межсетевой экран, средство обнаружения несанкционированных воздействий, средства анализа защищенности, специализированные программно-аппаратные средства и устройство управления, обеспечивающие гибкость системы защиты, заключающаяся в возможности перехода от одной платформы защиты к другой.

8. Разработаны модифицированные методы шифрования данных на базе стандартных DES и RSA методов, отличающиеся длиной ключа и количеством циклов шифрования и позволяющие шифровать в 1.3 раза быстрее, чем стандартные методы – при одновременном простоте программно-аппаратной реализации.

9. Разработан метод оперативного мониторинга топологии корпоративной компьютерной сети, основанный на реализации функции опроса стандартным протоколом IPX узлов топологии сети и обеспечивающий высокую оперативность обнаружения несанкционированных подключений к сети при минимальных вычислительных затратах.

10. Разработаны специальные методы шифрования данных на базе операций подстановок, перестановок, логических преобразований и операций над матрицами, отличающиеся простотой аппаратно-программной реализации и высокой оперативностью шифрования. Специализированные устройства шифрования данных на базе вышеперечисленных модифицированных и специальных методов обеспечивают шифрование данных на два порядка быстрее, нежели при программной реализации.

11. Разработан принцип формализации алгоритмического описания и синтеза структур специализированных устройств шифрования данных с использованием алгебраического подхода. Получена алгебраическая модель функционирования специализированных устройств шифрования и сформулирована задача синтеза оптимальной (в смысле относительной простоты информационно-аппаратурных связей), структуры специализированных устройств шифрования данных. Показано, что предложенная модель позволяет формализовать процесс синтеза на этапе проектирования и дает возможность объективно обосновать и выбрать оптимальную структуру устройства.

12. Экспериментально-прикладные результаты внедрения алгоритмов и программ структурного синтеза и оптимизации мониторинга топологии корпоративной компьютерной сети, специальных методов шифрования данных в интегрированных системах защиты информации в Республиканском информационно-аналитическом центре и в Государственной акционерной железнодорожной компании «Узбекистон темир йуллари» подтвердили их эффективность.

Исследованные в реферируемой работе теоретические и прикладные вопросы, естественно, не исчерпывают всю проблематику разработки полной теории создания корпоративных компьютерных сетей с интегрированной системой защиты информации. Полученные результаты дают основание для постановки новых задач, решение которых обусловит разработку более эффективных методов синтеза корпоративных сетей с интегрированной системой защиты информации.

Одной из интересных задач в этом свете является разработка эффективного метода синтеза структур корпоративных компьютерных сетей, основанного на выполнении минимального количества операций и обеспечивающего высокую сходимость процесса, что обеспечивает резкое сокращение времени синтеза структур корпоративных компьютерных сетей. Решение данной задачи связано с дальнейшим исследованием и совершенствованием методов структурного описания и синтеза корпоративных компьютерных сетей.

Перспективным представляется исследование вопросов разработки комбинированных методов шифрования в плане строгого доказательства их криптостойкости.

Решение указанных, а также многих других задач, несомненно, будет способствовать развитию и широкому внедрению корпоративных сетей с интегрированной системой защиты информации.

Исследования по некоторым аспектам вышеперечисленных задач проводятся на кафедре «Компьютерные системы и сети» ТашГТУ им. Абу Райхана Беруни.

Основные результаты диссертации опубликованы в следующих работах:

Статьи:

1. Каримов М.М. Описание модели корпоративной компьютерной сети. // ТДТУ. Хабарлар. № 4/2001. С. 29 – 32.
2. Каримов М.М. Об одном подходе к защите информации в локальных вычислительных сетях. / В кн. «Сборник научных трудов ИПМЭ НАН Украины». Киев, 2001. С.145-151.
3. Каримов М.М., Ирмухамедова Р.М. Особенности топологии вычислительных сетей, построенных на основе транспьютеров. // Вестник ТГТУ. 2001. №1. С.3-5.
4. Каримов М.М., Сагатов М.В., Руденко А.Б. Защита информации в беспроводных локальных вычислительных сетях. / «Моделирование и информационные технологии»: Сб. научных трудов. Киев, 1999. С.175-182.
5. Karimov M.M., Sagatov M.V. Digital processing of signals in systems with network topology. / World Conference on Intelligent Systems for Industrial Automation (WCIS 2000). Tashkent, 2000. P.101-104.
6. Ганиев С.К., Каримов М.М., Акбарходжаев Ш.Н., Убайдуллаев Ф. Некоторые аспекты аппаратной защиты информации в локальных вычислительных сетях. // Вестник ТГТУ. №2. 2000. С.131-134.

7. Ганиев С.К., Каримов М.М., Ганиев А.А., Лим В.Г. К вопросу организации беспроводной локальной вычислительной сети. // Вестник ТГТУ. №1-2. 1999 . С. 37-40.

8. Ганиев С.К., Каримов М.М. Комбинированный метод криптования в системе защиты информации. // Вестник ТГТУ, 2001. №2. С.24-28.

9. Ганиев С.К., Каримов М.М. Вопросы оптимального сегментирования топологии локальных компьютерных сетей. // Проблемы информатики и энергетики. 2001. № 2. С.20-25.

10. Каримов М.М., Эшонкулов Т.Н. Криптографик баркарор алгоритмлар ишлаб чикишда бир калитли системалардан фойдаланиш. // Техника юлдузлари, 2001. №2. С.37-41.

11. Karimov M.M., Komilov R.N. Algorithm of support of robustness of network topology. / Second World Conference on Intelligent Systems for Industrial Automation (WCIS 2002). –Tashkent, 2002. P.214-216.

12. Каримов М.М., Матъякубова П.М. Оптимизация структуры компьютерной сети с помощью алгоритма насыщенного сечения и сравнение его с алгоритмом релаксации Лагранжиана. // Вестник Каракалпакского Отделения АН РУз, №1-2, Нукус. 2002. С.63-65.

13. Гулямов Ш.М., Каримов М.М., Комилов Р.Н. Формализация структурного синтеза специализированных вычислительных устройств и компонентов компьютерных сетей. // Промышленные АСУ и контроллеры.- М. , №5, 2002. С.31-33.

14. Гулямов Ш.М., Камилов Р.Н., Каримов М.М. Анализ маршрутизации сообщений в дерево-гиперкубических сетевых топологических структурах. / XV Международная научная конференция «Математические методы в технике и технологиях» (ММТТ – 15), Сб. трудов, том 8, секция 8. Тамбов, 2002. С. 77 – 80.

15. Abdusatarov B.B., Karimov M.M., Irmuhamedova R.M. Synthes of signal system processing and computing networks. / World Conference on Intelligent Systems for Industrial Automation (WCIS 2000). Tashkent, 2000. P.14-16.

16. Верлань А.Ф., Абдусатаров Б.Б., Каримов М.М., Максимович Н.А. Применение микропроцессоров для реализации интегральных моделей динамических объектов. Препринт №99, Институт проблем моделирования в энергетике АН УССР. Киев,1987. 56 с.

17. Каримов М.М. Микропроцессорная система для решения задачи восстановления сигналов: Сборник научных трудов ТашГИ «Информационные модели и робототехнические системы»..Ташкент, 1988. С.76-82.

18. Верлань А.Ф., Абдусатаров Б.Б., Каримов М.М. Применение микропроцессорных средств, для реализации интегральных моделей динамических систем. // Гибридные вычислительные машины и комплексы. №11, 1988 . С.42-49.

19. Ганиев С.К., Сангинов Р.С., Каримов М.М. Использование алгебраической модели для синтеза структур специализированных вычислительных устройств. Деп. в УзНИИНТИ за № 1109 – Уз89 от 18.09.1989 г. Библиогр. Указатель ВИНИТИ «Депонированные научные работы», 1990. № 1. С. 768 .

20. Гулямов Ш.М., Каримов М.М. Системы сетевой топологии для реализации алгоритмов цифровой обработки сигналов. // Датчики и системы. – М.: 2002, №2. С.42-44.

21. Каримов М.М. Применение аппаратных средств защиты информации в компьютерных сетях: Сб. науч. трудов ИПМЭ. НАН Украины. – Киев. 2001. Вып.7. - С.8-14.

22. Ганиев С.К., Каримов М.М., Эшанкулов Т.Н. Об одном подходе к улучшению криптостойкости криптографических систем. // Вестник ТГТУ. 2002, №2. С. 17-19.

23. Ганиев С.К., Каримов М.М., Валиев Р.Н. Адаптивная система защиты информации для компьютерных сетей. // Проблемы информатики и энергетики. 2002, №3.- С. 3-7.

24. Гулямов Ш.М., Каримов М.М., Комилов Р.Н. Определение минимального подмножества сочленения графа связности информационных потоков в компьютерных сетях.// Научно-технический журнал ФерПИ. N1,2002.- С.18-22.

25. Ганиев С.К., Каримов М.М., Ганиев А.А. Оценка эффективности методов в локальных сетях. Вестник ТГТУ, 2003 г., №1. – С. 22-24.

Авторские свидетельство и патенты:

26. Верлань А.Ф., АбдусатаровБ.Б., Каримов М.М. и др. Устройства для решения интегрального уравнения измерительного преобразователя скорости потока. Авторское свидетельство СССР № 1651283 Б.И. №44, 1991. 12 с.

27. Верлань А.Ф., Нишанова Ш.М., Гулямов Ш.М., Ахмеров И.С., Каримов М.М. Устройство для решения интегрального уравнения, описывающего задачи динамики вязкоупругой тонкостенной конструкции. Патент Республики Узбекистан № 2199, Узбекистон Республикаси Патент идораси расмий ахбороти, 1994 й. № 4. С. 55.

28. Верлань А.Ф., Абдусатаров Б.Б., Нишанова Ш.М., Гулямов Ш.М., Каримов М.М. Устройство для решения интегрального уравнения, описывающего задачи динамики вязкоупругой тонкостенной конструкции». Патент Республики Узбекистан № 2652. Узбекистон Республикаси патент идораси расмий ахбороти, 1995. № 2. -С. 81.

29. Верлань А.Ф. Абдусатаров Б.Б., Каримов М.М. и др. Устройства для решения систем интегральных уравнений. А.С N1621745 СССР G 06F 7/64 ДСП.

30. Ганиев С.К., Каримов М.М., Абдурахмонов Ш.И., Эшанкулов Т.Н., Куртаджиев Ш.С. Программный модуль шифрации данных модифицированным DES методом. Патент РУз. Программы для ЭВМ. DGU 2002 0034. Официальный вестник №5, 2002.

31. Ганиев С.К., Каримов М.М., Абдурахмонов Ш.И., Эшанкулов Т.Н. Программный модуль шифрации данных комбинированным методом ARJ/VIGINER. Патент РУз. Программы для ЭВМ. DGU 2002 0035. Официальный вестник, №5, 2002.

Тезисы докладов, материалов конференций:

32. Ganiev S.K., Khamdamov R.Kh., Karimov M.M. The encryption device of the protocol in Local Networks. / Intergovernmental informatics program of UNESCO. National seminar and trading course on System and Network security. Tashkent, 1999. P.51-53.

33. Ganiev S. K., Khamdamov R. Kh., Karimov M.M. The analysis of protection means of the information in Local Computer Network. / Intergovernmental informatics program of UNESCO. National seminar and trading course on System and Network security. Tashkent, 1999. P.50-51.

34. Ganiev S.K., Khamdamov R.Kh., Karimov M.M. Generators of pseudo random numbers for device coding. / Intergovernmental informatics program of UNESCO. National seminar and trading course on System and Network security. Tashkent, 1999. P. 53-54.

35. Верлань А.Ф., Чмырь И.А., Сагатов М.В., Каримов М.М. Компьютерные обучающие системы со встроенным интеллектом. / Тезисы докладов Республиканской конференции «Информационные и коммуникационные технологии в учебном процессе». Сборник научных трудов ТГТУ, Ташкент, 2000 . С.12-20.

36. Ганиев С.К., Каримов М.М. Интегрированная система защиты информации в корпоративных сетях. / Тезисы докладов Международной НТК «Innovation - 2001».-Ташкент, 2001. С.97-98.

Т.ф.н. М.М.Каримовнинг "Ахборотларни ҳимоялашнинг интеграцияланган тизимли корпоратив компьютер тармоғини ташкил этиш" мавзуидаги докторлик диссертациясининг

АННОТАЦИЯСИ

Диссертация информация ҳимоясининг интеграллашган тизимли корпоратив компьютер тармоқларининг назарияси ва уларни яратиш муаммоларига бағишланган.

Қуйилган мақсад доирасида қуйидаги тадқиқот масалалари ечилган: интеграллашган системали корпоратив компьютер тармокларини ташкил қилиш тамойилларини ифодалаш; тармоқ топологиясини оптимал сегментлаш методларини яратиш; корпоратив компьютер тармоқлари топологиясини кўп параметрли оптималлаштириш усулини яратиш; концентраторларнинг оптимал дарахтини ва корпоратив компьютер тармоқларининг концентраторли қоплаш тамойилларини яратиш; тармоқ топологиясини мониторингловчи махсус алгоритмни яратиш; маълумотларни шифрлашнинг махсус усулларини яратиш ва намунавий усулларини такомиллаштириш ҳамда уларни амалга оширувчи аппарат-программ воситаларни яратиш; маълумотларни шифрловчи ихтисослаштирилган қурилмаларнинг оптимал тузилмасини синтезлаш методини яратиш.

Олинган янги илмий натижалар сифатида қуйидагиларни кўрсатиш мумкин: турли намунавий топологияларни бирлаштириш асосида тармоқ тузилмасини ташкил этиш тамойили ифодаланди; трафикни бошқаришни соддалаштиришга имкон берувчи тармоқ топологиясини оптимал сегментлаш методи яратилди; релаксация методлари ва терминал тармоқ топологиясини шакллантирувчи алгоритм асосида корпоратив компьютер тармоқ тузилмасини кўп параметрли оптималлаштириш усули яратилди; коммутацион тармоқ топологиясини шакллантирувчи ва концентраторли қоплаш ёрдамида дарахтсимон тармоқни синтезлаш алгоритмлари яратилди; информацияни интеграллашган ҳимояловчи тизимнинг базавий тузилмаси таклиф этилди; аппарат-программ амалга оширилишининг соддалигини таъминловчи маълумотларни шифрлашнинг махсус методлари яратилди; маълумотларни шифрловчи ихтисослаштирилган ҳисоблаш қурилмаларининг алгебраик модели ва синтезлаш методи тавсия этилди.

Диссертацияда яратилган методлар ва алгоритмлар информацияни мосланувчан ҳимояловчи корпоратив компьютер тармоқ топологиясини объектив асослашга ва ташкил этишга имкон беради.

THE ANNOTATION

of the thesis for a doctor's degree, Cand. Tech. Sci. M.M.Karimov on a theme "Organization of corporate computer networks with the integrated system of information protection"

The dissertation work is devoted to issues of development of the theory and creation the corporate networks with the integrated system of information protection.

Within of this purpose the following research problems have been solved : formulation of a principle corporate network organization with the integrated protection system; development of the method for optimum segmentation of network topology; development of combinatorial method and decomposition algorithm of the computer network structure; development of the way of multiparametrical optimization corporate network topology; development of construction principles of and optimum tree of concentrators and concentrator overlapping of corporate networks; development of special monitoring algorithms of network topology; development of special and improvement of typical methods for data enciphering and creation hardware-software means for their realization; development of the synthesis method of optimum structures of the specialized devices for data enciphering.

It is possible to attribute to new scientific results receive: formulating the networks structures organization principles on the basis of association of various typical organization in uniform; development of the methods of segmentation optimum of network topology allowing to simplify process of traffic management; development of the way of multiparametrical optimization of corporate networks structure on the basis of relax methods and formation topology algorithms of the terminal networks allowing to find the decision as much as possible approached to optimum; development of formation algorithm of switching network topology and treelike network synthesis using the concentrated overlapping; development of base structure of the integrated system of information protection; the development data enciphering of special methods distinguished by simplicity of hardware-software realization; the offer of algebraic model and method optimum structures synthesis of the specialized computing devices for enciphering.

The methods and algorithms developed in the dissertation work enable objectively to prove and to organize the optimum corporate network topology with flexible information protection system.

Подписано к печати 27.08.2003 г. Формат бумаги 60X84 1/16.
Объем 2 п.л. Тираж 100. Заказ № 522.
Отпечатано в типографии Таш ГТУ г.Ташкент, ул. Талабалар, 54.