МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Моделирование с использованием пакета прикладных программ Matlab ответных действий информационно-вычислительной системы предприятия на информационно-технические воздействия

Исполнитель Рейш Владислав Максимович
(фамилия,имя,отчество)

Руководитель кандидат технических наук, профессор
(ученая степень, ученое звание)

Рябухов Игорь Рустиславович
(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой _____
(подпись)

доктор технических наук, профессор
(ученаястепень,ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия,имя,отчество)

«17» февраля 2017 г.

Санкт–Петербург
2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение

высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ

ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему Моделирование с использованием пакета прикладных программ Matlab ответных действий информационно-вычислительной системы предприятия на информационно-технические воздействия

Исполнитель Рейш Владислав Максимович
(фамилия,имя,отчество)

Руководитель кандидат технических наук, профессор
(ученая степень, ученое звание)

Рябухов Игорь Рустиславович
(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой_____
(подпись)

доктор технических наук, профессор
(ученая степень,ученое звание)

Бурлов Вячеслав Георгиевич
(фамилия,имя,отчество)

«»20г.

Санкт–Петербург
2017

РЕФЕРАТ.

Отчет 54 с., 4 ч., 8 рис., 35 источников, 1 прил.

«Моделирование с использованием пакета прикладных программ Matlab ответных действий информационно-вычислительной системы предприятия на информационно-технические воздействия Объектом исследования являлась модель оценки защищенности речи от несанкционированного доступа»

Цель работы – уменьшение рисков на ИТВ при распределении ресурсов под задачи в нестохастической среде методами теории адаптивного управления.

Задачи для достижения поставленной цели в соответствии с ТЗ

- Формализация информационно-технических воздействий врага для лучшего описания возможностей противника по изменению структур ИВС, что дозволяет сделать модель системы конкретно в ходе управления;

-Создание пула (агрегирование ресурсов) в процессе решения измененной задачи об упаковке контейнеров.

- Сужением большого количества альтернатив и использованием принципа постепенного распространения разных задач по системе.

В работе разработаны и представлены:

- предложен метод, адаптирующий текущую структуру распределенной информационно-вычислительной системы,

- расширение пула, смежными элементами до тех пор, пока не будут исчерпаны все ресурсы системы или не будет сформирован пул с требуемыми характеристиками.

-обоснование экономической составляющей представленной программы.

Оглавление

Введение

Информационно-вычислительные системы (ИВС) помогают в решении огромного количества неоднозначных задач: от обрабатывания изображений конкретных районов и селекции до предоставления услуг быстрой и качественной связи. Общие сроки решения задач зависят от сформировавшейся обстановки и имеют все шансы поменяться скачкообразно в любой момент. Иная способность ИВС обусловлена тем, что они являются главным объектом информационно-технических воздействий (ИТВ), то есть, они могут рушиться в процессе установленных задач. Таковым образом, в ходе использования ИВС всегда появляются следующие трудности, связанные с недостатком ресурсов:

1. часть ИВС разрушена и интенсивности потоков задач значительно вырастут.
2. часть ИВС разрушена, а интенсивности потоков решаемых задач меняются слабо.
3. структура ИВС сохранена, однако интенсивности потоков задач значительно возрастают.

Интенсивности потоков решаемых задач возрастают, к примеру, при переводе войск в высшие степени боевой готовности. При конкретных ограничениях такие потоки могут быть описаны как стохастические процессы. Факторами разрушения ИВС выступают обычные естественные сбои, либо отказы частей ИВС, которые описываются стохастическими действиями, а также ИТВ, которые в общем случае показать в виде стохастических процессов нереально.

Так как ИВС как система, трудящаяся со стохастическими потоками отказов и возобновлений, а еще также со стохастическими потоками задач и сервисов, довольно изучена, заострим интересы только на работе ИВС и только при условиях ИТВ.

Цель :

Уменьшение рисков на ИТВ при распределении ресурсов под задачи в нестохастической среде методами теории адаптивного управления.

Задачи :

1. Формализация информационно-технических воздействий врага для лучшего описания возможностей противника по изменению структур ИВС, что дозволяет сделать модель системы конкретно в ходе управления;
2. Создание пула (агрегирование ресурсов) в процессе решения измененной задачи об упаковке контейнеров.
3. Сужением большого количества альтернатив и использованием принципа постепенного распространения разных задач по системе.

Актуальность:

Итоги дальнейшего исследования могут быть применены при разработке единого информационного пространства разных министерств и служб, в автоматизированных системах военного назначения и не только.

Список условных сокращений:

ИВС – информационно-вычислительная сеть

ИКТ – информационно-коммуникационные технологии

ИБ – информационная безопасность

ЭМВОС – эталонная модель взаимодействия открытых систем

ПО– программное обеспечение

ОС – операционная система

ЭВМ – электронная вычислительная машина

ТКС – телекоммуникационная система

ССОП – сеть связи общего пользования

ИТВ – информационно-техническое воздействие

1 Анализ типовой ИВС предприятия

1.1 Типовая структура ИВС предприятия

Основной эффект ИВС – доступность ресурсов сети для пользователей, в соответствие с политикой конфиденциальности. Сети могут создавать непростые информационные структуры. Информационные связи между пользователями могут решать значительно усложненные задачи.

Под ИВС обычно понимается конкретная распределенная система коллективного пользования средств связи и вычислительных ресурсов, взаимосвязанных каналами приема и передачи информации, обеспечивающая повышение эффективности функционирования линий передачи информации и вычислительных средств при решении нестандартных задач обработки информации.

Организационное предприятие ИВС должна удовлетворять следующим главным требованиям:

Открытость – возможность включения резервных абонентских пунктов, информационных ресурсов, узлов и каналов связи без изменения программных и технических средств действующих компонентов.

Эффективность – обеспечение требуемого качества обслуживания

Гибкость – сохранность работоспособности при изменении структуры в ходе выхода из строя абонентского пункта, информационных ресурсов, узлов и линий связи, допустимость изменения типа ЭВМ и линий связи пользователей при маленьких затратах.

Главными отличительными чертами ИВС являются:

Операционные возможности сети – перечень главных действий по обрабатыванию и сохранению данных.

Время полной доставки сообщений определяется как статистическое среднее время от начала передачи сообщения в сеть до момента получения сообщения адресатом.

Продуктивность сети представляет собой суммарную производительность информационных ресурсов и абонентских пунктов.

Стоимость обработки данных создается с учетом средств, используемых для ввода-вывода, передачи, сохранения и обработки данных. На основе стоимости рассчитывается цена обработки данных, которая зависит от размера используемых ресурсов вычислительной сети.

Работа ИВС представляется в терминах процессов. Процесс – это динамический объект, показывающий собой целенаправленный акт обработки данных. Процессы подразделяются на 2 класса: прикладные и системные.

Прикладной процесс – работа прикладной, и (или) обрабатывающей программы ОС компьютера, а также функционирование терминала, то есть специалиста по информационной безопасности, который работает на терминале.

Системный процесс – выполнение алгоритма, реализующей вспомогательную функцию, связанную с помощью в создании прикладных процессов. Системные процессы: активация терминала прикладного процесса, организация связи меж процессами и прочее.

Процесс создается программой или специалистом и связан с данными, поступающими извне в качестве исходных и создаваемыми процессом для внешнего пользования. Введение данных, нужных для процесса, и вывод данных производится в форме сообщений – алгоритму данных, имеющих законченное смысловое значение. Внедрение сообщений в структуру и вывод сообщений из нее делается через логические (программно-организованные) точки, называемыми портами. Порты бывают на входные и выходные. Процесс как объект представляется суммой портов, через которые он взаимодействует с иными процессами сети.

Взаимодействие процессов сводится к обмену сообщениями, которые передаются по каналам, создаваемым средствами сети. Временной промежуток, в течение которого взаимодействуют процессы, называется

сеансом. Важно выделить, что в ПК и вычислительных комплексах взаимодействие процессов обеспечивается за счет доступа к общим для них данным (общей памяти) и обмена прерывающимися сигналами. В ИВС единственная система взаимодействия процессов – обмен сообщениями.

Такое отличие связано с локальной распределенностью процессов в ИВС, а также с тем, что для физического сопряжения компонентов сети используются каналы связи, которые помогают в передаче сообщений, но не отдельных сигналов.

Сеть – это объекты, образуемые устройствами передачи и обработки данных.

Вычислительная сеть - последовательная бит-ориентированная передача информации между связанными друг с другом независимыми устройствами. Сети обычно бывают в частном ведении специалиста и занимают некую территорию и по этому признаку разделяются на: Локальные вычислительные сети, которые находятся в одном или нескольких расположенных зданиях неподалеку. ИВС по обычаю размещаются в рамках какого-то предприятия, из-за этого их называют корпоративными. Распределенные компьютерные сети, глобальные или, находящиеся в разных зданиях, городах, которые бывают локальными, смешанными и глобальными. В зависимости от этого глобальные сети существуют 4 основных видов:

-городские

-региональные

-национальные

-транснациональные.

В состав сети в общем случае включается следующие элементы:

- сетевые компьютеры с адаптером;
- каналы связи (кабельные, спутниковые, телефонные, цифровые, волоконно-оптические, радиоканалы и др.);
- разного вида преобразователи сигналов;

- сетевое оборудование.

Различают 2 понятия сети: коммуникационная сеть и информационная сеть. Коммуникационная сеть необходима для передачи данных, также она выполняет функции, связанные с преобразованием данных. Коммуникационные сети различаются по видуприменяемых физических средств соединения, и на базе коммуникационной сети создается группа информационных сетей. Информационная сеть нужна для хранения информации и создается из информационных систем. Под ней следует понимать систему, которая является поставщиком, либо потребителем информации. Компьютерная сеть создана из информационных систем и каналов связи. Под информационной системой необходимопринять объект, который способен осуществить хранение, обработку или передачу разного вида информации. В её состав входят: компьютеры, программы, специалисты и иные составляющие, нужные для процесса обработки , а также передачи данных. Далее информационная система, предназначенная для завершения задач специалиста по информационной безопасности, будет называться рабочая станция. Рабочая станция в сети отличается от домашнего ПК существующим сетевым адаптером, канала для передачи данных и сетевого ПО. Под каналом связи нужно понимать дальнейший путь или структуру, по которой передаются сигналы. Средство передачи сигналов называют абонентским, или физическим каналом. Каналы связи формируются по линиям связи при помощи сетевого оборудования, либо физических средств данной связи. Физические средства связи сформированы на основе RJ-45, коаксиальных кабелей, оптических каналов. Между работающими ИС через физические каналы коммуникационной сети и узлы коммутации инсталлируются логические каналы.

Логический канал – это способ для передачи данных к одной системеот другой. Логический канал обычно находитсяна маршруте в одном или множестве физических каналах. Логический канал можно объяснить как маршрут, лежащий через физические каналы и узлы коммутации.

Информация в сети транслируется блоками данных по процедурам передачи данных между объектами. Такие процедуры называют протоколами данных. Протокол – это совокупность правил, имеющие формат и процедуры обмена информацией меж двух или несколькими устройствами. Загрузка сети характеризуется параметром, называемым трафиком.Трафик - поток сообщений в сети для передачи. Его характеризуют как количественное измерение в нужных точках сети числа проходящих блоков данных и их длины, выраженное в битах в секунду. Сильное изменение на характеристики сети влияет метод доступа. Метод доступа – это способ определения, чтоза рабочая станция может следующей использовать канал связи, а также как управлять доступом к кабелям. В сети абсолютно все рабочие зоны физически связаны между собой каналами связи по структуре, называемой топологией. Топология – это показатель физических коннекторов в сети, указывающихна рабочие станции, которые могут связываться между собой. Особенность топологии показывает производительность, работоспособность и надежность эксплуатации рабочих зон, и еще, время обращения к файловому серверу. В зависимости от топологии,в сети применяют метод доступа. Структура главных элементов в сети зависит от архитектуры, то есть концепции, определяющей взаимосвязь, состав и функции работы рабочих станций в сети. Архитектура, такжеопределяет логическую, функциональную и физическую структуру технических и программных средств сети. Она может определять принцип строения и функционал аппаратного и ПО элементов сети. Обычно выделяют 3 вида архитектур: архитектура терминал – основной компьютер, архитектура клиент – это сервер, а также одноранговую архитектуру. Современные сети классифицируют по разным признакам: удаленностьПК, топологии, их назначения, перечень предлагаемых услуг, принцип управления в целом, метод коммуникации, метод доступности, среды передачи, скорость передачи данных.

1.2 Типовые приложения ИВС предприятия

Выделим характерные индивидуальности ИВС:

— интенсивности поступления потока и обработки задач почти не прогнозируемы, что впоследствии тянет за собой неопределенность в применении ресурсов ИВС;

— конструкция ИВС является недетерминированной и динамично измененной. Главными факторами изменения структуры выступают:

1. Перемещение мобильных ИВС, таких как космические аппараты на околоземных орбитах, самолеты на маршрутах патрулирования и

тому подобные (они могут характеризоваться закономерностями детерминированных или стохастических процессов); переносных комплексов управления, маневрирующих летательных аппаратов и так далее (являются предвиденными процессами).

2. Сбойили отказ элементов ИВС по естественным причинам или в случаях информационно-технических воздействий противника.

Подобные факторы могут быть приняты при адаптивном изменении всей структуры ИВС. Пример, который я рассмотрелв данной работе - динамическое объединениересурсов в пулы.

Пул — объединение ресурсов на некоторый промежуток времени, предназначенное для решения некой задачи (группы задач). Он необходим в период достижения цели, после решения задачи пулы расформировываются. Вообще, с точки зрения динамического создания пулов трудности, названные в начале и связанные с недостатком ресурса, идентичны. Примером статичного пула из вычислителей служит кластер, а пула из каналов связи — транк. Пул создается на уровне логической структуры ИВС. Требования к немувносят на уровне программного обеспечения. Подробно модель ИВС как главной системы с обратными связями между уровнями представлена в работе. Рассмотрим типовые методы формирования пулов сделаны в следующих технологиях:

— кластерах на базе Windows Server 2012.

Кластер протекает постоянно , что обычно не соответствует особенностям информационно-вычислительным сетям.

— Dynamic Trunking Protocol, разработанном компанией Cisco для формирования транков. Они могут делаться в реальном времени.
— пуле ресурсов Sun Solaris 11.x, более-менее подходящем для достижения задач ИВС, так как он формируется динамически. Хоть и каждый ресурс привязывается к какому-то конкретному приложению за некоторое время, фактически в Sun Solaris нужно сделать выбор нужной конфигурации пула, но сами они задаются администратором раньше всех.

Рассмотрим метод формирования пулов, без указанных выше недостатков. Предположим, что мы знаем состояния и особенности всех элементов ИВС. Зная, что семантическое наполнение решаемых в ИВС задач при создании пула крайне мало, что для ИВС основополагающие характеристики, как представление данных задачи (плавающая или фиксированная точка, количество разрядов), количество и скорость ввода/вывода данных, вероятность допустимых потерь, необходимое время реакции информационно-вычислительной системы

Основное назначение информационно-вычислительной системы— достичь цели выполняемой задачи по производительности. Значит, любая задача может быть предоставлена в информационно-вычислительной системе в виде набора нужных для ее решения производительностей, и первоначальное назначение пула — сделатьнеобходимую производительность. У нас есть производительность как количество задач, взятое в единицу времени.

Любая информационно-вычислительная система имеет в своей структуре вычислители, каналы связи, устройства ввода-вывода и память. Главное назначение вычислителей - выполнять вычисления (то есть команды/операции), назначение каналов связи - передавать данные, устройств ввода, либо вывода, то есть вводить, либо выводить данные,

накопителей - сохранять данные. Производительностью вычислителей, чаще всего называют количество исполняемых операций за секунду, производительностью каналов — пропускную способность. Исходной производительностью представим производительность, доступную для решения целей, то есть производительность, выделяемая в задаче.

1.3 Типовые информационно-технические воздействия на ИВС предприятия

Под ИТВ будем воспринимать целенаправленные разрушающие действия на процесс генерации, обработки, сохранения и передачи данных в ИВС. Данное определение охватывает довольно обширный класс воздействий — от только компьютерных (внедрение вирусов, атаки DDoS, IP Spoofing) до физических воздействий на элементы инфраструктуры информационно-вычислительной системы (уничтожение канала связи, уничтожение серверов, воздействие электромагнитными импульсами).

В итоге ИТВ может быть разрушен некий узел информационно-вычислительной системы, канал связи, изменено количество связей, которое может образовать узел, а объектами ИТВ в информационно-вычислительной системепоказаны следующие ресурсы: вычислители (наземные вычислительные комплексы), каналы связи (спутниковые, проводные, оптические), накопители данных (накопители на борту космических аппаратов и в вычислительных центрах), устройства ввода или вывода данных (стандартные: монитор, принтер, клавиатура, компьютерная мышь; расширенные: оптико-электронные, радиоэлектронные системы и т. д.).

Бывают случаи, когда злоумышленник только смотрит за сообщениями, передаваемыми по линиям связи, не мешая их передаче. Именно такое вторжение называется “наблюдением за сообщениями”. Даже если данные зашифрованы, нарушитель может видеть управляющую

информацию, которая сопровождает сообщения, и так выявить локацию и идентификаторы объекта информационно-вычислительной системы. Также, он может понять длину сообщения, время, когда оно было отправлено, частоту обратной связи. Последние 2 вида пассивных вторжений связывают либо с анализом трафиков, или с нарушением защиты связи.

Специальный вид защиты разных каналов передачи является защиты двухуровневой линий связи, при которых реализуются следующие уровни защиты: защита процесса передачи сообщения и шифрование текста данного сообщения.

Другое требование, используемое для защиты передаваемых сообщений, состоит в том, что настоящие идентификаторы сети (зарегистрированные и используемые в процессе аутентификации защищенных объектов) должны быть спрятаны не только от таких вторжений со стороны несанкционированных пользователей, но также и друг от друга. Подобное средство защиты называется “цифровым псевдонимом”. В этом случае специалист получает различные идентификаторы для различных соединений, тем самым, скрывая настоящие идентификаторы не только от преступников, но и от союзников.

Подобные средства охраны ИВС, необходимые для противодействия пассивным вторжениям в системах связи, состоят в следующем:

1. Защита содержания сообщения.

2. Предотвращение возможности анализа трафика.

3. Числовой псевдоним.

Противник может организовать активное вторжения, исполняя разные манипуляции над сообщениями во время соединения. Сообщения могут быть скрыто модифицированы, полностью уничтожены, задержаны, скопированы, изменен распорядок их следования, введены в сеть через линию связи в наиболее позднее время. Могут быть также синтезированы фиктивные сообщения и введены в сеть через канал передачи данных.

Целенаправленно можно подчеркнуть следующие категории активных

вторжений:

- воздействие на поток сообщений: трансформация, удаление, задержка, переупорядочение дублирование регулярных и посылка ложных сообщений.

- блокировке передаче сообщений.

- осуществление ложных соединений.

Действие на поток сообщений включает опасности процедурам подтверждения подлинности, единства и распорядку следования сообщений во время соединения. В контексте коммуникационных функций информационно-вычислительной системы доказательство подлинности сообщения означает, что источник сообщения можно надежно определить, то есть указать, что приобретенное сообщение передано этому объекту некоторым иным объектом в течение времени соединения. Целостность сообщения показывает, что сообщение не изменялось во время передачи, а понятие «порядок следования» показывает, что расположение сообщения в потоках сообщений может быть просканировано.

Вторжение в процедуры установления подлинности существовать методом усовершенствования основной информации, сопровождающей сообщения, и таковым образом сообщения будут отосланы в неверном направлении, либо включать ложные сообщения (специально сформированные либо сохраненные из прошлых соединений). Повреждение целостности может быть вызвано улучшением частиц данных в сообщении, а нарушение порядка следования – удалением сообщения или изменением информации, управляющей передачей сообщения. Хотя охрана от воздействия на поток сообщений поддерживается коммуникационными протоколами, в данном контексте защита направлена на то, чтобы пресечь умышленные вторжения, а не просто защититься от случайных непреднамеренных ошибок элементов сети.

В связи с этим, структура защиты, обеспечивающая любые сопротивления опасностям целостности, распорядку следования и

подлинности отдельных сообщений, может быть определена как снабжение целостности потока сообщений.

Блокирование передачи сообщения – 2-ая категория активных вторжений в подсистемах связи. Она сводит вместе вторжения, в которых противник либо удаляет все сообщения во время присоединения, или просто увеличивает время отправки сообщения, идущие в том или ином направлении. Подобное нападение может быть организовано злоумышленником, который, генерируя интенсивный трафик ложных и подставных сообщений, не дает возможности постоянным сообщениям проходить по линиям связи.

Трудноуловимое отличие между атаками на ряд сообщений и препятствованием их передачи напрямую зависит от интенсивности атак и целостностью соединения. К примеру, механизмы защиты, обеспечивают целостность ряда сообщений, которые смогут найти возможные вторжения, мешающие передаче сообщений. Хотя, если соединение оказалось пассивным, в смысле, что все сообщения разрешаются в любом направлении, то данный протокол функционирования такого объекта на одном из окончании соединения может не определить, когда следующее сообщение должно прибыть от соответствующего абонента . В такой ситуации нереально понять угрозу с целью оградить передачу сообщения, которая полностью оборвала бы поток поступающих сообщений. Дабы защититься от подобных вторжений, необходимы и иные способы защиты. Соответствующий метод защиты сети мог бы быть назван процедурой поддержки потокового процесса передачи. Он гарантирует взаимодействующим в ИВС объектам невозможность несанкционированного удаления всех сообщений в процессе соединения без обрыва самого соединения. Осуществление фиктивных соединений – 3-я категория активных вторжений в линии связи. Она объединяет все вторжения, в которых вредитель либо повторяет запись предыдущих соединений, либо делает попытки установить соединение под неверным идентификатором.

Чтобы предупредить подобные вторжения, метод инициализации соединения должен включать некие охраняемые механизмы, которые верифицируют соединения в целое.

Абстрактно ИВС можно представить как системы, связанные вместе некой передающей структурой. В качестве систем бывают абонентские пункты и узлы связи. В каждой системе сети существует некая совокупность разных процессов. Процессы, определенные по абсолютно разным системам, действуют чрез передающую структуру обменом сообщениями.

Для обеспечения гибкости и открытости , либо эффективности сети управление процессами организуется по многоуровневой схеме, описывающей ЭМВОС.

ЭМВОС – эталонная модель взаимодействия открытых систем

В каждой из систем указаны программные и аппаратные модули, создающие определенный функционал работы передачи данных. Модули распределены по 7 уровням:

Первый уровень – физический – создает управление каналом связи, для подключения и отключения канала связи и формировании сигналов, показывающих передаваемые данные.

Второй уровень – канальный – помощник в создании безопасной передачи данных через канал, сделанный на первом уровне.

Третий уровень – сетевой – обеспечивает передачу, базовую сеть передачи данных. Управление сетью, созданное на этом уровне, состоит в выборочном маршруте передачи данных на линиях, соединяющих узлы сети.

Первые 3 уровня создают базовую сеть передачи данных между разными абонентами сети.

Четвертый уровень – транспортный – формирует процедуру соединения абонентов сети с базовой сетью передачи данных. На 4-ом уровне вероятно стандартное формирование различных систем с сетью передачи данных, а также организуется транспортная служба для обмена данными между сетью и системами сети.

Пятый уровень – сеансовый – организует сеансы связи на время взаимодействия процессов. На данном уровне по запросам процессов формируются порты приема и передачи сообщений, выстраиваются соединения – логические каналы.

Шестой уровень – представления – формирует трансляцию разных языков, форматов данных, кодов для взаимодействия разных видов компьютеров, с нестандартными операционными системами.

Седьмой уровень – прикладной – проходит передача всеобщих данных прикладному процессу.

1.4 Формализация исходных данных

В информационно-вычислительной системе выделяют две взаимосвязанные подсети: транспортную сеть и абонентскую сеть.

Транспортная сеть, как правило, включает в себя: узлы связи и каналы связи.

Узел связи –средства коммутации и передачи данных в назначенном пункте назначения – принимает данные, проходящие по каналам связи, и передает информацию в каналы, ведущие к абонентам.

Канал связи – формируется на основе линии связи. В него входят аппаратура передачи данных и физиологическую среду передачи данных.

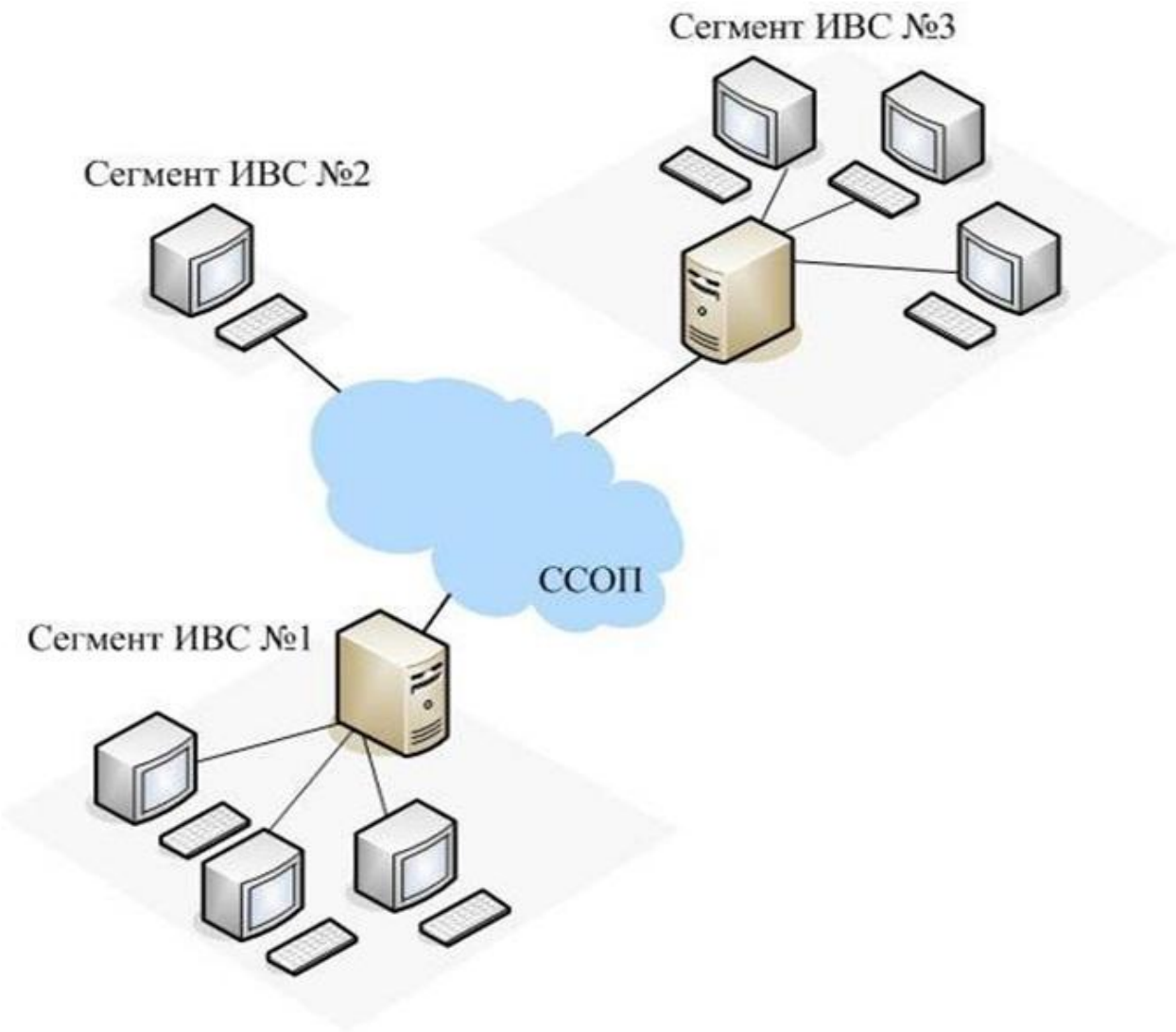

Рисунок 1 - Структурная модель ИВС

ССОП – сеть связи общего пользования

Абонентская сеть - это комплекс аппаратурно-программных средств, реализующих функции объемной обработки информации, а также функции взаимодействия пользователей информации. Абонентский пункт создается из взаимосвязанных устройств ввода-вывода, обеспечивающих ввод и вывод данных в разной форме.

Информационные ресурсы – необходимы для хранения и обработки информации

2 Макет программного комплекса моделирования ответных действий информационно-вычислительной системы предприятия на информационно-технические воздействия

2.1 Требования к ИВС

При организации и эксплуатации информационно-вычислительной системы основополагающими требованиями при работе являются следующие:

- производительность;
- надежность и безопасность;
- расширяемость, масштабируемость;
- прозрачность;
- поддержка разных видов трафика;
- управляемость;
- совместимость.

Производительность – характеристика сети, помогающая понять, насколько скоро информация передающей рабочей станции придет до принимающей рабочей станции. На производительность ИВС сети воздействуют следующие характеристики: конфигурация; скорость передачи информации; метод доступов к каналам передачи данных; топология сети; технология. Так как производительность сети может прекратить отвечать необходимым от нее требованиям, то администратор сети может предпринять следующие действия: поменять конфигурацию сети так, что бы структура самой сети больше была похожа на структуру информационных потоков; поменять на другую модель построения распределенных приложений, которая помогла бы снизить сетевой трафик; сменить мосты на более скоростные коммутаторы. Обычно лучший способ в данной ситуации будет перейти на более скоростную модель. При росте масштаба сетей

появилась необходимость в улучшения их общей производительности. Так, зародился новый способ называемый – микросегментация, которая помогает снизить количество пользователей на один сегмент и уменьшить объем трафика, то есть, увеличить производительность сети. Изначально, для микросегментации применялись маршрутизаторы, не предназначенные для таких целей. Решения на их основе были очень дорогими и были приметны высокой временной задержкой и низкой пропускной способностью. Лучшими в этом деле, и наиболее подходящими устройствами для микросегментации стали коммутаторы. Благодаря относительно невысокой цене, большой производительности и легкость в применении они стремительно стали популярны в ИВС. Следовательно, сети начали строить на базе коммутаторов и маршрутизаторов. Теперь первые дают высокоскоростную пересылку трафика меж сегментами, входящие в одну подсеть, а вторые передают данные между подсетями, ограничивая утечку широковещательного трафика, исполняя задачи безопасности ИВС.

Наиболее важной характеристикой информационно-вычислительной системы сетей - надежность. Улучшение надежности построено по принципу предотвращения отказов и сбоевспособомуменьшения интенсивности неполадок за счет использования электронных схем и компонентов с высокой и сверхвысокой степенью интеграции, повышения уровня помехоустойчивости, упрощённых режимов задач схем, обеспечение тепловых режимов их работы, иулучшения методов сборки аппаратуры.

Отказоустойчивость – свойство вычислительной системы, которое помогает ИВС, как машине вероятность продолжения деяний, заданных программными модулями, после возникновения неполадок. Введение отказоустойчивости необходимо для избыточного АО и ПО. Направления, связанные с предотвращением неисправностей и отказоустойчивостью, основные в проблеме надежности. На параллельных вычислительных системах получается как самая высокая производительность, так и, во многих случаях, достаточно высокая надежность. Имеющиеся ресурсы избыточности

в параллельных системах могут гибко применятся для повышения производительности, а также для улучшения надежности. Однако, в понятие надежности входит не только аппаратные средства, но и ПО. Основной задачей улучшения надежности систем будет целостность хранимых в них данных. Безопасность – главная задача, исполняемая абсолютно любой компьютерной сетью. Недостаток безопасности можно рассматривать с различных углов – намеренная порча данных, конфиденциальность информации, несанкционированный доступ, воровство информации и тому подобные. Помочь в защите информации при условиях ИВС сети всегда проще, чем при имении на предприятии множества автономно работающих компьютеров. Фактически у нас есть только один инструмент – резервное копирование. Для упрощения его еще называют резервированием. Нужен он для того чтобы создавать в безопасном месте полную копию данных, обновляемой постоянно и по возможности очень часто. Для ПК в последнее время более безопасным стало резервное «облако». Конечно, возможны применения стримера, но это уже будут излишние затраты на аппаратуру.

Прозрачность – это состояние сети, когда специалист, находясь в сети, не может в нее зайти. Коммуникационная сеть будет прозрачной относительно проходящей насквозь нее информации, если выходной поток битов, один в один дублирует входной поток. Однако, сеть возможна быть непрозрачной во времени, если из-за измененных размеров очередей объема данных меняется и время прохождения разных блоков через узлы коммутации. Прозрачность сети, говоря о скорости передачи данных показывает, что данные возможно перекидывать с разной необходимой скоростью. Если в сети по тому же маршруту передастся информационные и управляющие сигналы, то называют, что сеть прозрачна по отношению к видам сигналов. А если передаваемые данные могут кодироваться абсолютно разным способом, то это значит, что сеть прозрачна для разных методов кодировок. Прозрачная сеть является легким решением, в котором для взаимодействия сетей, расположенных на приличном большом расстоянии

между собой, применяется принцип Plug-and-play.

Поддержка разновидных трафиков - трафик в сети получается рандомным образом, но в нем показаны и некие закономерности. Обычно, некоторые специалисты ИБ, занимающиесярешением общей задачи, частоспрашивают друг у друга, иди же у общего сервера, и в самых редких случаяхспециалисты испытывают необходимость доступа к ресурсам компьютеров иного отдела. Идеально, чтобы структура сети была схожа с структурой информационных потоков. В зависимости от сетевого трафика Компьютеры в сети могут быть распределены на группы, будет ли так или нет зависит от сетевого трафика. Компьютеры формируются в группу, если большая часть создаваемых ими сообщений, передана компьютерам той же группы. Для разделения сети на отдельные части применяются мосты и коммутаторы. Они показывают локальный трафик внутри нужного сегмента, не передавая за его грани никаких кадров, помимо тех, которые посланы компьютерам, которые находятся в иных сегментах. Следовательно, сеть расформировывается на отдельные подсети. Это помогает более правильно выбрать пропускную способность сохраненных линий связи, тем более зная интенсивность трафика внутри любой группы, а также активность обмена информацией между ними. Хотя, локализация трафика средствами мостов и коммутаторов обладает существенными ограничениями. Если посмотреть по-другому, применение механизма виртуальных сегментов, сделанного в коммутаторах ИВС сетей, приводит к полной локализации трафика, а такие сегменты безоговорочно изолированы друг от друга, в случае широковещательных кадров тоже происходит изоляция. В связи с этим, в сетях, сделанных только на мостах и коммутаторах, компьютеры, принадлежащие различным виртуальным сегментам, не формируютобщей сети.

Цель управления защитой данных – это контролируемый доступ к сетевым ресурсам в соответствии с локальными руководящими правилами, для создания антисаботажа сети и доступа к уязвимой информации лицам, не

обладающим соответствующим разрешением. К примеру, главная из подсистем управления защитой информации может контролировать регистрацию специалистов ресурса сети, отказывая в доступе, если вводящий код доступане соответствует правилам установки. Подсистемы управления защитой информации работают путем распределения источников на санкционированные и несанкционированные области. Для некоторых специалистов доступ к некоторым источникам сети будет закрыт. Подсистемы управления защитой данных используют следующие функции: идентифицируют чувствительные ресурсы сети; определяют отображения в виде карт между чувствительными источниками сети и набором пользователей; контролируют точки доступа к чувствительным ресурсам сети; регистрируют несоответствующий доступ к чувствительным ресурсам сети. Концепция программной совместимости была впервые использована в широких масштабах разработчиками самой системы. Огромныеплюсы такого подхода, дозволяющего сохранять существующую работуПО при переходе на новые модели, были моментально оценены производителями компьютеров, а также пользователями. Начиная с того времени фактически все фирмы-поставщики компьютерного оборудования существовали согласно этим принципам, предоставляя серии совместимых компьютеров. Следует подметить, что с течением времени даже самая актуальное оборудование постоянно устаревает и появляетсянадобностьвнедрения радикальных переменне только в архитектуру, но и в способы организации ИВС. В настоящее время самый важный фактор, определяющий современные тенденции в развитии информационных технологий, является ориентирование компаний-поставщиков оборудования для компьютеров на рынок прикладных программных средств. Данный переход выдвинул ряд новых требований. Начнем с того, что вычислительная среда может позволять менять объем и состав аппаратных средств и ПО в соответствии с изменяющимися требованиями решаемых и поставленных задач. Помимо этого, она обязана обеспечивать запускодинаковых программных систем на

различных аппаратных платформах, то есть обеспечивать мобильность программного обеспечения. Также, эта среда обязана гарантировать возможность использования одних и тех же машинных интерфейсов на всех ПК, входящих в неоднородную сеть. При условии жесткой конкуренции производителей аппаратных платформ и программного обеспечения получилась концепция открытых систем, показывающая совокупность стандартов на разные компоненты вычислительной среды, предназначенных для обеспечения мобильности программных средств в рамках неоднородной, распределенной вычислительной системы.

2.2 Алгоритм работы ПК

Количество возможных комбинаций элементов в пуле нестабильно увеличивается с удалением от точки входа задачи (элемента информационно-вычислительной системы, на котором начинается достижение цели задачи). Вместе с тем информационно-вычислительная системаможет создавать пулы в реальном или близком к реальному времени, в связи с этим есть необходимость понижения объема возможных комбинаций, которые должна проанализировать система управления пулами.

Снижение количества возможных комбинаций может быть реализовано посредством применения принципа постепенного распространения задач по информационно-вычислительной системе, предполагающего формирование пула из элементов ИВС, которые:

1) имеют минимально допустимую производительность;

2) располагаются на минимальном расстоянии от точки входа задачи. В качестве расстояния могут быть разные величины: количество связей, созданных элементом; количество путей, проходящих через элемент.

Принцип постепенного распространения задач по информационно-вычислительной системе главныйв методе динамического формирования

пулов.

Введем следующие обозначения:

Wmin > 0 - минимальная производительность в i-м пуле;

r - радиус элемента в i-м пуле

V - множество элементов ИВС;

Vr - множество элементов кандидатов расположенных по порядку, которые могут участвовать в формировании пулов;

Ux - множество команд на образование физических связей. Физическая связь — связь на физическом уровне или MAC-подуровне канального уровня модели.

Ui - множество команд на образование логических связей. Логическая связь — связь, созданная на LLC-подуровне канального уровня, сетевом или транспортном уровнях модели.

Uk - множество команд на физическое перемещение элементов.

Входными данными для предлагаемого метода динамического создания пула являются:

- количество пулов N;
- размеры пулов,
- минимально допустимая производительность элемента в i-м пуле меньше 0, текущая производительность j-го элемента j > 0.

Схема метода приведена ниже на рисунке 2. В начале производится сокращениемножества возможных комбинаций выбором и упорядочивания элементов-кандидатов, подходящих для создания пула.[7, с.15]

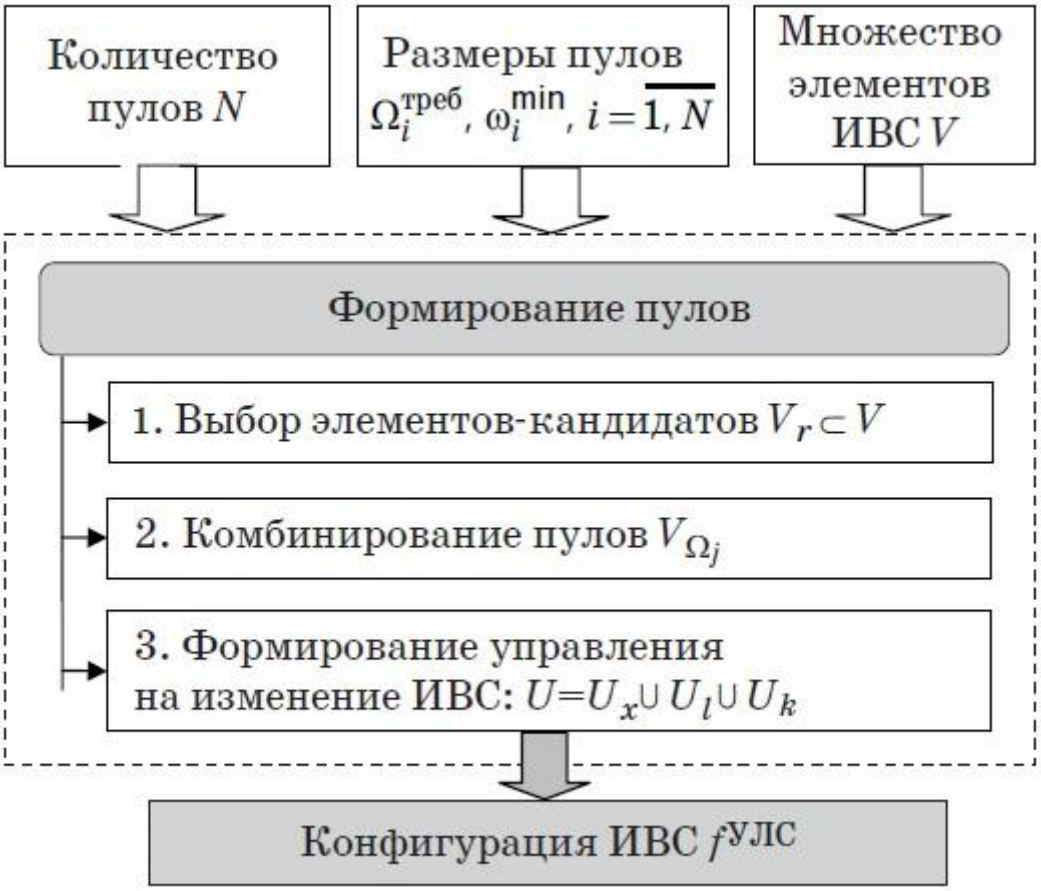

Рисунок 2 - Схема метода динамического формирования пулов

2.3Интерпретация работы

1. Выбор элементов-кандидатов.

Подбор подходящих элементов будет основываться от значения радиуса элемента r .Если r < 1 значит элемент обладает необходимой минимальной производительностью и может использоваться в пуле. Элементы, для которых

r < 1 составляют множество Vr. Далее, после отбора элементов производится их упорядочивание.

Правило упорядочивания может быть разным, например, по увеличению текущей производительности элемента j.

По итогам работы шага № 1 данного метода получаем упорядоченное множество кандидатов Vr, которые могут принять участие в создании пула. Такое множество служит исходными данными для шага № 2 такого метода.

Рисунок 3 - Метод формирования пулов

2. Комбинирование пула

На 2-ом шаге производится еще одно сокращение количествавозможных

комбинаций, выбираются элементы информационно-вычислительной системы, смежные с точкой входа задачи, которую нужно решить (расстояние до точки входа 1).Точка входа v* — это элемент, с которого начинается выполнение цели, то есть точка входа может быть нам неизвестна. После отбора смежных элементов выполняется улучшенная задача по комбинированию контейнеров. Если пул с нужной производительностью не может быть сформирован на элементах, смежных с точкой входа задачи, которую необходимо решить, то осуществляется попытка сформировать пул с применением элементов информационно-вычислительной системы, смежных с теми, которые уже входят в комбинирование (расстояние до точки входа 2). Дальше делается тестирование на соответствие скомбинированного пула, который требовался изначально. Если сформирован пул с требуемой производительностью, то можно следовать к шагу № 3, или повторяются работы по комбинированию пула с применением элементов, входящих в пул (расстояние до точки входа 3). Делаем так, пока не будет сформирован пул с нужной производительностью, либо не будут закончены все элементы, имеющие физическую связь. Если пул не удалось скомбинировать, то делается попытка создать комбинации с применением элементов, меж которыми возможна установлена физическая связь, к примеру, с переносными устройствами (беспилотными летательными аппаратами, подвижными центрами обработки данных). Далее исполняются работы по комбинированию пула по инструкциям и правилам шага 2. Ответ комбинирования пула передаётся системе управления целями, запросившей ресурс, то есть где принимается решение о целесообразности применении скомбинированного пула. Если пул целесообразно применить, появляются команды на его создание, то есть на физическое перемещение, либо коммутацию элементов информационно-вычислительной системы (шаг №3), образование физических, или жедругих логических связей в ИВС.

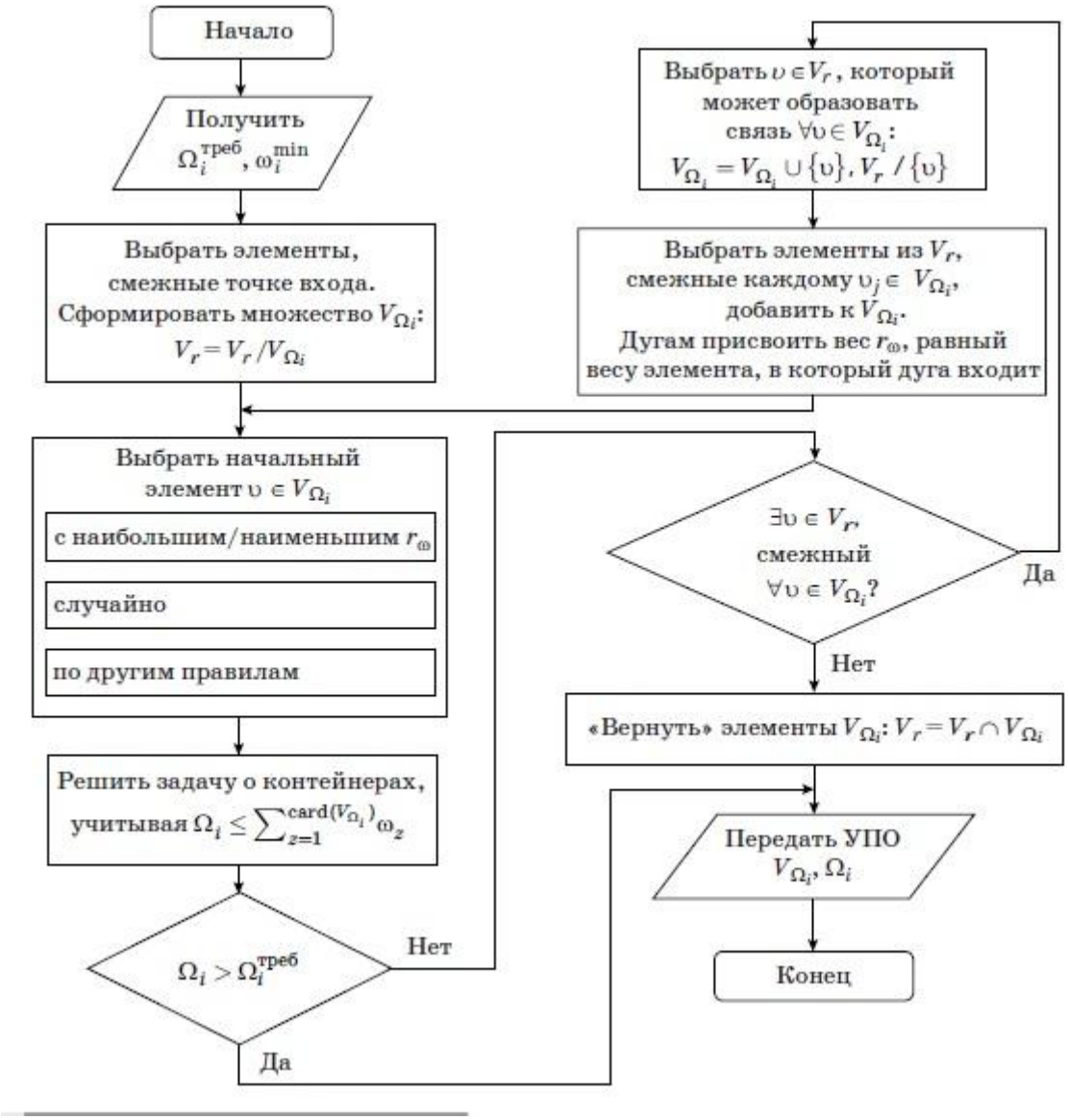

Рисунок 4 - Метод формирования пулов (Шаг 2)

Шаг 3. Формирование управления на изменение.

На этом этапе исполняется проверка на физическую связность комбинаций, сделанных на шаге 2. Если между каждыми элементами информационно-вычислительную системы, входящими в комбинацию, существует физическая связь, то появляется формирование пула, реализуются требуемые логические связи или же, по специальному алгоритму создаются новые связные сегменты.

В случае некоторых возможных вариантов создания пула могут появиться дополнительные требования к структуре, к примеру, по живучести на максимальном уровне. После создания i-го пула пройденные до этого шаги

метода повторяются для i+1 пула.

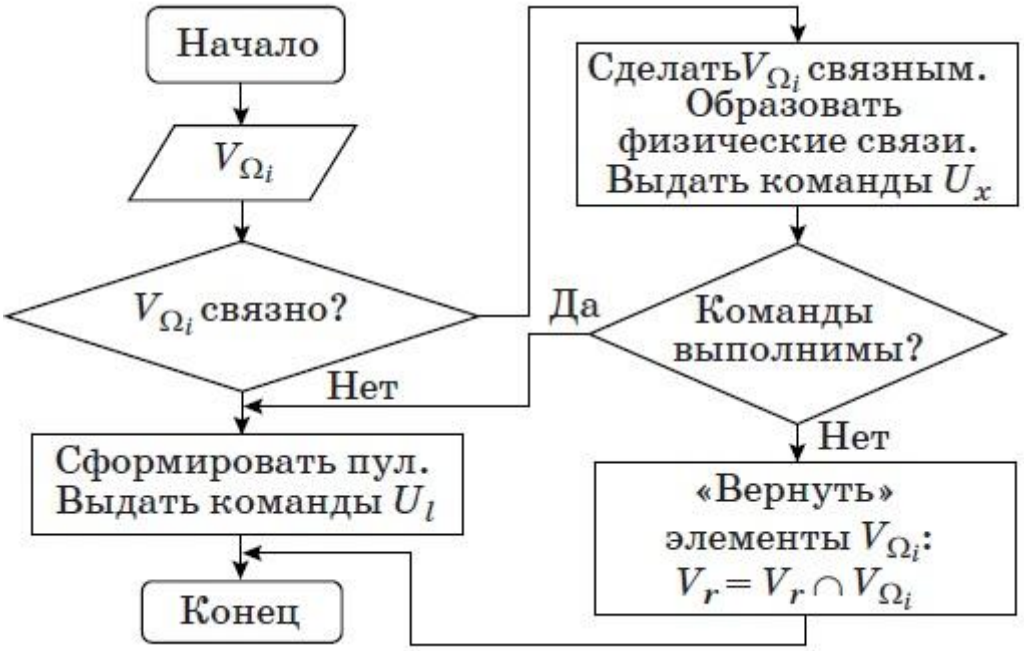

Рисунок 5 - Метод формирования пулов (Шаг 3).

Возможен вариант, что в ходе выполнения метода была изменена линия задач, вызвавшая изменение требований к пулам, или же былиинформационно-технические воздействия, поменявшие состав информационно-вычислительную систему, то на уровне ПО может решиться выполнять процедуру сначала. Понятно, что метод целесообразно применять для распараллеливаемых задач. Цель, которая изначально не была распараллелена, показывается в виде одного пула с минимально возможной производительностью. Элементы информационно-вычислительной системы, на базе которых создаются пулы, обладают z > 0, а это значит, на каждом шаге предлагаемого метода (при каждом действии элемента с производительностью z) происходит положительное монотонное возрастание i. То есть, метод сходится, а i стремится к максимуму.

2.4 Математическая постановка задачи на исследование

Метод для формирования пулов P={ Pi,Wmin }={ 18,3 , 16,3 , 3,3 , 4,3 } в произвольной ИВС, обладающей структурой.

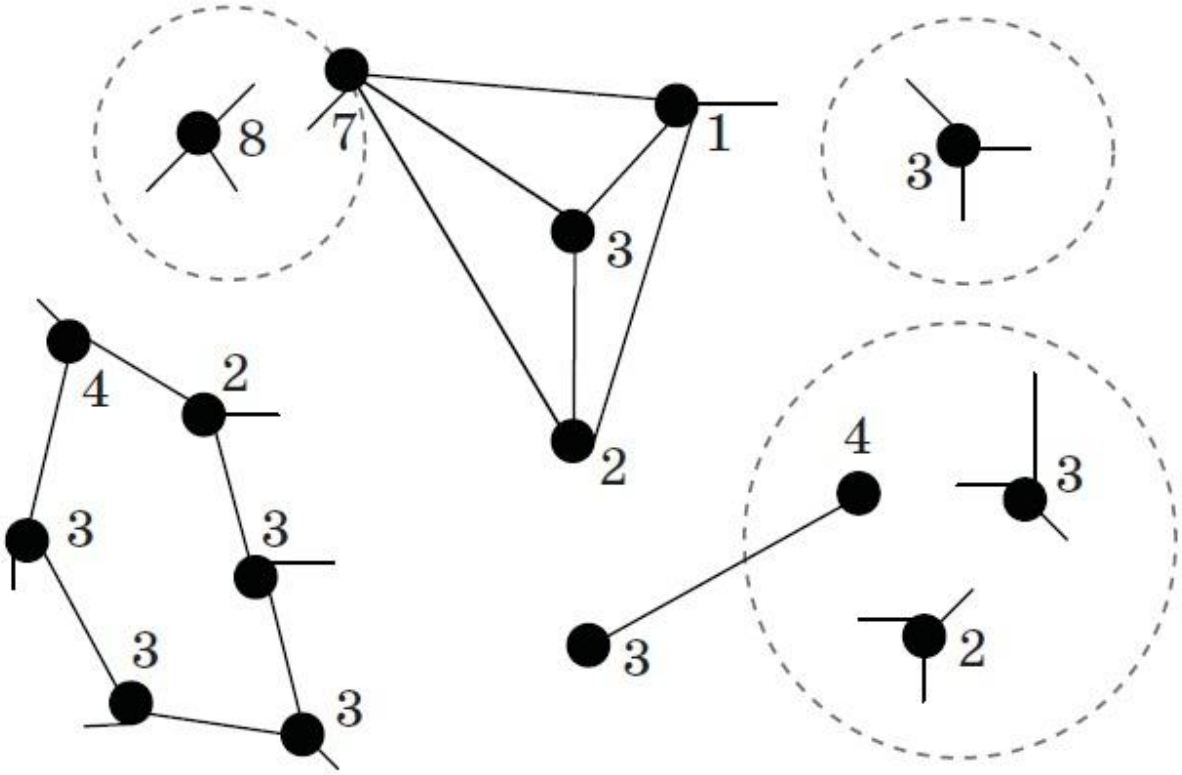

Рисунок 6 - Структура ИВС и производительности элементов

Цифрами на рисунке 6 отмечены производительности элементов i, измеряемые в условных единицах. Штрихпунктом обозначены видимые элементы ИВС. Если элементы находятся внутри пунктирной линии,то между нимиможет быть произведена физическая связь. Создаем первый пул с характеристиками, рассчитываем радиусы элементов r и формируем множество Vr.

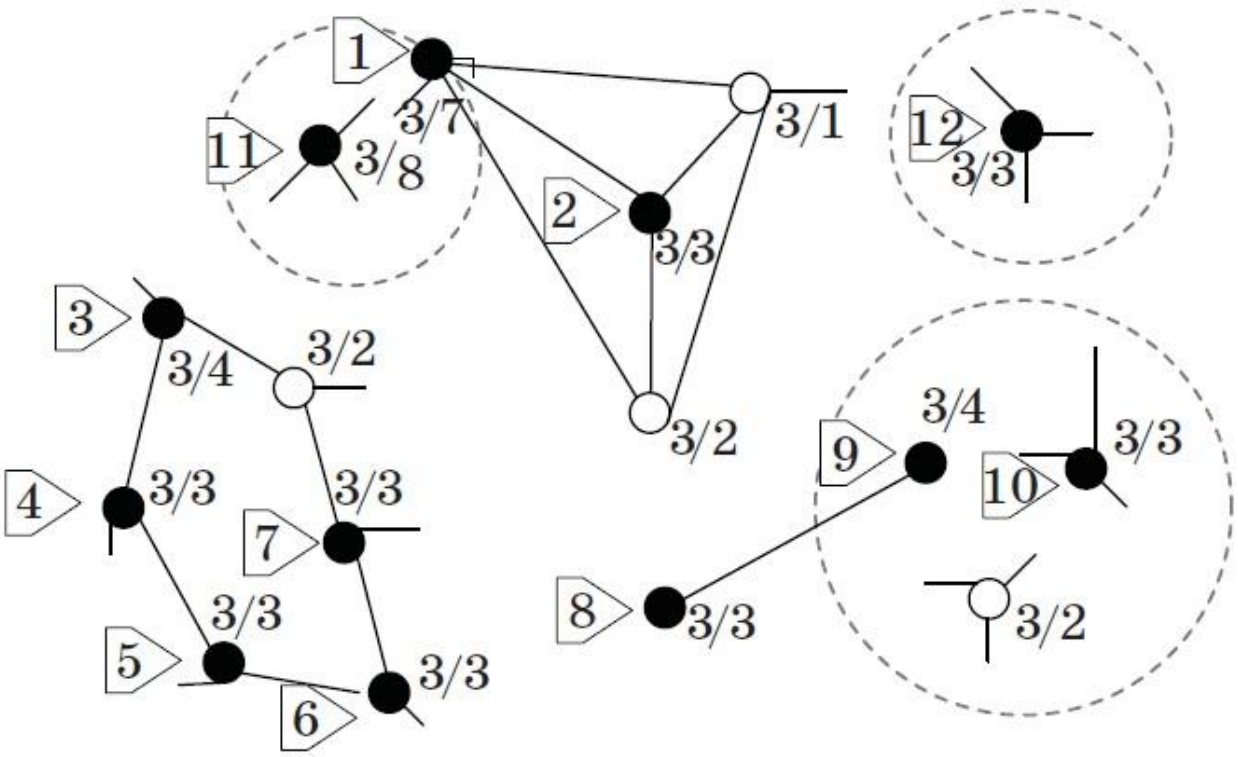

Рисунок 7 - Формирование множества Vr.

Множество сформировано элементами, обозначенными закрашенными кругами. Далее производим упорядочивание элементов Vr по числу существующих физических связей. Порядковые номера элементов множества Vr отмечены цифрами в указателях.

Множество Vr = {1,2,3,4,5,6,7,8,9,10,11,12}.

Предположим, что производительность каналов связи (пропускная способность) и производительность любого элемента достаточны для передачи данных (элемент способен выполнять транзит данных).

На втором шаге производим комбинирование пула.

1. Предположим, что точка входа для задачи v1 — элемент с номером 5, поэтому сразу включаем его в V1 :

Vr={1,2,3,4,6,7,8,9,10,11,12}

2. Добавляем в V1 ближайший элемент с наименьшим номером, физически связанный с элементом 1:

Vr={1,2,3,4,6,7,8,9,10,11,12}

V = {5,6} < 7+3=10<16

3. Так как не осталось элементов из Vr, физически связанных с элементами 1 и 2, берем элемент, ближайший к элементу 1, имеющий наименьший номер:

Vr={3, 4, 5, 6, 7, 8, 9, 10, 12}

V = {1,2,11} < 10+8=18>16

4. Пул P,Wmin = {16,3} скомбинирован.

Аналогично повторяем для остальных пулов.

Комбинируем пул i=2, точка входа — вершина 3.

а). V ={4,5,6,7,8,9,10,11}

б). V ={5,6,7,8,9,10,11}

в). Элементы 5 и 7 имеют одинаковое расстояние до точки входа, равное 2.

Мы берем элемент с меньшим номером — 5,

Vr ={6,7,8,9,10,12}.

5. Vr ={6,8,10,12}.

6. Максимальная производительности второго пула 2 максимально меньше требуемой на 2. Поскольку элементов нет, с которыми смогут образоваться физические связи, комбинирование пула заканчивается выдачей сообщения на степень программного обеспечения, что пул с нужными характеристиками не может быть скомбинирован. Возможно из-за того, что на уровне программного обеспечения принято решение о целесообразности пользования данного пула. Удаляем созданную комбинацию и возвращаем элементы в Vr.

Далее комбинируем пул i = 3, то есть {3,3}, здесь точкой входа будет вершина номер 8:

Vr = {4,5,6,7,9,10,11}.

После выполнения шага 3 и выдачи соответствующих управляющих воздействий ИВС приобретет структуру, показанную на рисунке 8.

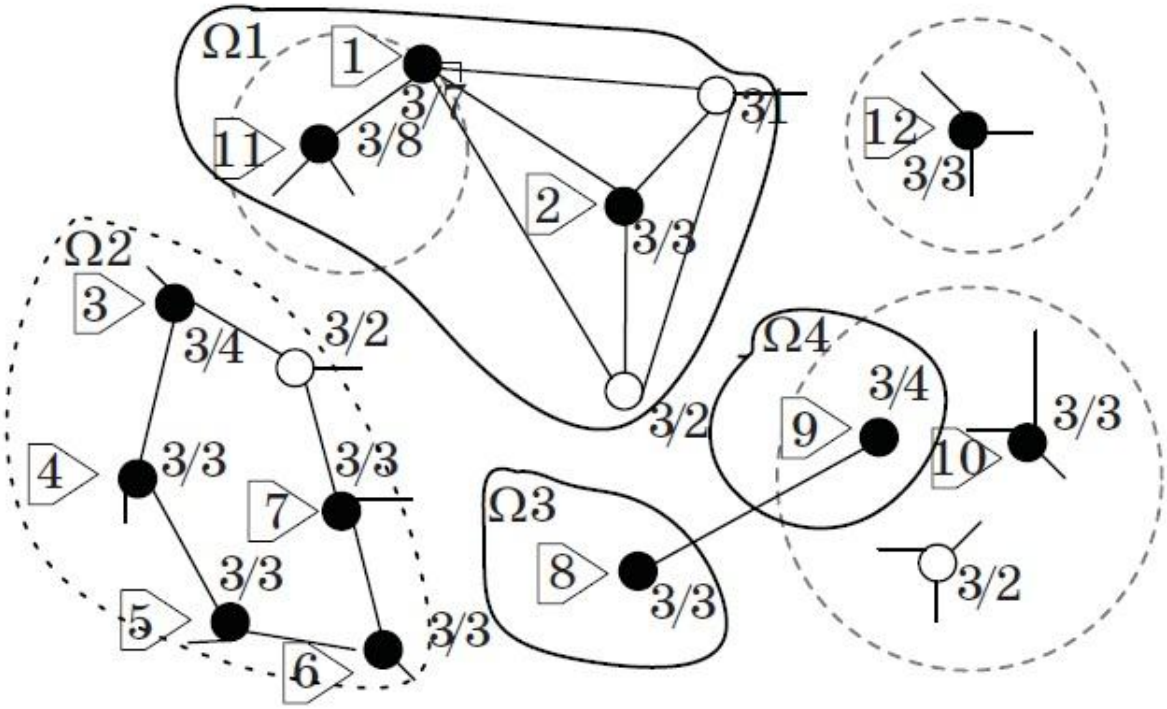

Рисунок 8 - Измененная структура ИВС.

Не получившийся пул выделен толстой пунктирной линией. Элементу 11 были даны команды на изменение локации, что бы появилась вероятность восполнить физическую связь с элементом 1. Физическим воплощением предложенного в дипломной работе метода (выделением ресурсов информационно-вычислительной системы) обязан заниматься определенный гипервизор, частицы которого возможны и есть на любом элементе информационно-вычислительной системы. Это поможет создать описанный в моей работе структуру постепенного расположения целей по информационно-вычислительной системе, уменьшить расходы на управление, а основное - продолжать решениялюбых задач в случае, когда информационно-вычислительная система будет расформирована на разные, не связанные сегменты.

3 Анализ общих требований

3.1 Эксплуатационные требования к программно-аппаратному обеспечению

Для реализации данного метода был выбран язык MatLab, рассмотрим его подробнее. Средой разработки является Matlab R2016.

MatLab — это высокоуровневый язык с интерактивной средой для программирования, различных расчетов с числами и наглядной визуализации результатов. С помощью MatLaB можно анализировать практически любые данные, разрабатывать алгоритмы, создавать приложения, а также модели.

Язык, инструментарий и встроенные функции позволяют пользователям исследовать различные методы и получать ответы намного быстрее, чем с использованием электронных таблиц или иных языков программирования, таких как C/C++ , Java.

MatLab часто используют в таких отраслях:

- обработка сигналов и связь,
- визуализации изображений
- системы управления,
- автоматизация тестирования и измерений

MatLab по сравнению с другими языками программирования (C/C++, Java, Pascal) позволяет намного сократить время решения задач и ощутимо упрощает разработку новых алгоритмов.

Ядро MatLab может очень быстро работать с матрицами реальных, комплексных и аналитических типов данных и со структурами данных и таблицами поисковых запросов.

Так как MatLab многофункциональная программа, то и требования к программно-аппаратному обеспечению и устройствам будут повышены.

Рассмотрим минимальные требования программы MatLab:

Операционные системы :

Windows 10

Windows 8.1

Windows 8

Windows 7

Windows Server 2012 SP1

Windows Server 2008 SP1

Windows Server 2008 SP2

Процессоры:

IntelилиAMDx86-x64

Свободное место на диске:

2 Гб на MatLab, 4-6 Гб для дополнительного ПО

RAM:

2 Гб или более

С Simulink 4 гб или более

С Polyspace 4 гб или более

Видеоадаптер:

Не требуется специальных графических карт

Рекомендуется аппаратное ускорение графической карты с поддержкой OpenGL 3.3 с памятью 1 Гб.

3.2 Эксплуатационные требования к персоналу

Должностные требования к специалисту по информационной безопасности:

- участие в разрабатывании перспективных и годовых графиков, планов работы, техобслуживания и ремонта оборудования, мероприятий по улучшению его эксплуатации, предупреждению простоев в работе, повышению качества работы, наилучшему использованию вычислительной техники;
- выполнять задания по обеспечению механизированной и автоматизированной обработки поступающей на предприятие информации;
- разрабатывать программы, обеспечивающие помощь в выполнении алгоритма, и поставленной задачи средствами ИТВ.
- периодически делать тестирование и отладку ИТВ;
- определять информацию, которая необходима в обработке средствами вычислительной техники, ее размеры, структуру, свойства, схемы ввода, обработки, хранения, а также методы ее контроля;
- разрабатывать инструкции по работе с ПО, оформлять нужную техническую документацию;
- выполнять работу по подготовке технических носителей информации, помогающих в получении автоматического ввода данных в ЭВМ по заполненности и систематизации показателей справочного, либо нормативного фонда, разработке форм входящих документов, внедрению необходимых изменений и своевременному исправлению рабочего ПО;
- вести расчеты применения времени работы машины, объемов законченных работ;
- организовывать работу вместе с руководством по созданию электронных учебных пособий в разрабатываемой области.

Специалист по информационной безопасности должен знать:

- способы создания механизированной и автоматизированной обработки

информации;

- вычислительную технику для сбора, переноса и обработки данных и общие правила эксплуатации;
- техническую составляющую механизированной и автоматизированной обработки данных;
- рабочие программы, все виды инструкции к ним, макеты, различные инструктивные материалы, помогающие в определении последовательности и технологию получения расчетных операций;
- виды технических носителей информации, правила их хранения и эксплуатации;
- рабочие системы вычислений, криптографии и кодов;
- основные используемые в работе языки программирования;
- способы проведения расчетов, а также вычислительных работ;
- способы расчета успешных законченных работ;
- основы экономики, трудовые обязанности предприятий и производств;
- основополагающие правила к нормам охраны труда.

3.3 Оценка экономической эффективности применения ПК

В дипломной работе было осуществлено компьютерное моделирование в пакете MatLAB. Эти данные могут быть использованы для оценки постепенного распространения задач по ИВС.

Цель экономической подглавы: расчет себестоимости представленной в работе программы. Чтобы осуществить данный расчет нужно учесть:

1).сложность разработки программы

2).зарплату программиста

3). покупка программного обеспечения

4).траты на электроэнергию

5). накладные расходы

б). налоги.

В работе использовались:

а). ноутбук HP Pavilion 6002er

б). ОС Windows 7 Ultimate

в). MatLab r2016

Цк - 24000 рублей

Цо - 9500 рублей

Цп - 11500 рублей, где

Цк - цена компьютера,

Цо - цена операционной системы,

Цп - программного обеспечения.

Суммарная стоимость технических средств, вместе с программно-технического обеспечением составляет:

Ц = Цк + Цо + Цп = 24000 + 9500 + 11500 = 45000 рублей.

Расчет затрат на электроэнергию, потребляемую компьютером.

Компьютер, потребляет электрическую энергию. Опираясь на знания, полученные из технической документации, общая мощность, которую потребляют ПК

Мс= 250 Вт·ч.

Произвести расчет трат энергопотребления :

Р= R·В·М·Цэ,

R= 30 дней (месяц);

В – длительность рабочей смены, ч.,

В - 8 часов;

М – мощность, которую потребляют технические средства, кВт·ч;

Цэ – стоимость электроэнергии по действующим тарифам, р./кВт·ч;

Цэ=1,5 рубля за кВт·ч.

Из этого получаем, что

Р = 30*8*1.5*0.25=90,

столько рублей будет уходить в месяц на специалиста для оплаты энергопотребления.

Далее рассчитаем заработную плату специалиста по информационной безопасности:

T = K * B,

где T - рабочее время программиста,

K - количество рабочих дней,

B - продолжительность рабочего дня.

T = 30*8=240,

Если взять по настоящим данным ставку специалиста, то она будет равна 220 рублей/час.

Z = T * R,

где Z - зарплата специалиста,

R - рабочая ставка.

Z = 220 * 240= 52800.

То есть суммарная стоимость одного специалиста будет составлять:

O = Z + P = 52890 рублей.

4 Безопасность жизнедеятельности

4.1 Условия эксплуатации проектируемой среды и ее описание

Безопасность жизнедеятельности - это мероприятия, нацеленные на обеспечение безопасной жизни и работы человека в окружающей среде, сохранение его самочувствия, разработку методов и средств защиты путем уменьшения воздействий вредных и опасных особенностей жизнедеятельности до минимальных значений, применение мер по снижению ущерба чрезвычайных ситуаций и стихийных бедствий.

С развитием науки и техники довольно важную роль играет возможность безопасного выполнения людьми своих жизненных обязанностей. Вопросам безопасности жизнедеятельности уделяется все больше внимания от года в год, так как забота о физическом и моральном состоянии человека является не только делом государственной важности, но и элементом соперничества организаций в вопросе привлечения новых кадров. В связи с этим вопросами в качестве варианта обеспечения защищенности человека была разработана наука о безопасности жизни человека.

Обеспечение условий сохранения здоровья работников, безопасность условий труда, ликвидация профессиональных заболеваний и производственного травматизма является одной из главных забот человеческого общества. Следует обратить внимание на необходимость глобальное применения новейших форм научной организации труда, минимизации по эксплуатации неквалифицированной сотрудников, создание условий для исключения профессиональные заболевания и производственный травматизм.

Рабочее место должно быть обеспечено всеми возможными средствами защиты человека от вредоносных воздействия производства. Уровни этих факторов не должны превышать пределы, установленных санитарно-

техническими, техническими и правовыми нормами. Эти правила требуют создания приемлемых условий труда на местах организации производства, при которых влияние опасных и вредных факторов на работающих либо полностью исключено, либо находится в допустимых диапазонах.

Выбор главных практических задач БЖД прежде всего обусловлен выбором вариантов реализации защиты, развития и подходящем использованием средств защиты человека и природной среды от воздействия техногенных источников и стихийных бедствий, а также средств, обеспечивающих комфортное состояние среды обитания.

4.2 Выявление потенциально опасных и вредных факторов и их анализ

Специалист по информационной безопасности подвергается вредному воздействию, как со стороны технических средств, так и из-за неправильно организованного рабочего места.

Опасности рабочего места :

а). Воздействие электромагнитного и электростатических полей (от онитора, системного блока, устройств ввода/вывода) на внутренние органы и на деформацию живых клеток;

б). Излучение (рентгеновский, ультрафиолетовый и инфракрасный спектры);

в). Нервно-эмоциональные нагрузки;

г). Воздействие эргономики рабочего места и дизайна внешних устройств компьютера (клавиатура, компьютерная мышь) на опорно-двигательную систему и мышечный тонус;

д). Ухудшение зрения из-за освещения;

ж). Опасность поражения электрическим током;

з). Шумы и вибрации, воздействующие на организм.

Все вышеперечисленные негативные факторы приводят к нарушениям центральной нервной, сердечно-сосудистой и эндокринной систем и

нейротрофических расстройств и патологических изменений, включая изменения в составе крови, раздражительность, головные боли, потеря слуха, головокружение, потеря памяти. У человека снижается внимательность, стремительно наступает усталость в связи с завышенными энергетическими затратами и нервно-психическим напряжением. Это может привести к снижению работоспособности, производительности, качества и безопасности труда, таким образом, долгосрочное присутствие человека в зоне комбинированного воздействия различных неблагоприятных факторов может привести к профессиональному заболеванию.

4.3 Факторы, обеспечивающие и повышающие безопасность

Соответствие требований к организации рабочего места, комплектующим деталям и особенностям работы, наилучшим образом снижает вредные факторы, оказывающие воздействие на пользователя:
Поскольку имеется множество вариантов вредоносных воздействий на здоровье человека, существует несколько способов, чтобы предотвратить их.
Для защиты от электромагнитных и электростатических полей, вы можете использовать экранные фильтры, специальные мониторы и другие средства личной защиты, которые прошли испытания в соответствии с сертификатом здоровья.

При наличии защитных фильтров, внешних или встроенных в корпус монитора, они обязательно должны быть подключены к общему заземлению
Чтобы уменьшить шанс заболеваний операторов из-за воздействием радиации во время работы на компьютере, рекомендуется использовать мониторы с минимальным уровнем излучения, разработанные по международным соглашениям, и следить за соблюдением режимов работы и отдыха.
Для уменьшения шума в комнате с компьютером, как правило, используется способ обработки акустического пространства с использованием

противостоящих поверхностей, ограждающих абсорбирующий материал с высокими коэффициентами поглощения звука в диапазоне частот 63 - 8000 Гц. С этой целью, на потолке и стенах размещены перфорированные плитки с звукопоглощающим наполнителем (минеральная вата). Усиленные панели размещают либо сразу на поверхность или в корпусе, на расстоянии от него не менее 20 см. В данном случае, более эффективно применение звукопоглощающей облицовки.

Дополнительным звукопоглощением могут служить простые занавеси из плотной ткани, в гармонии с цветом стен и подвешенные в складку на расстоянии 15 – 20 см от оконного стекла. Ширина занавеси должна быть в 2 раза больше ширины окна. Снизить уровень шума возможно также за счет использования для печати лазерных принтеров с низким уровнем шума.

Данные меры, позволяют устранить вредные факторы, оказывающие влияние на мышцы и суставы пользователя ПК:

- Обеспечение свободной площади и удобной формы рабочей поверхности.
- Комфортное расположение клавиатуры с возможностью изменения угла наклона рабочей плоскости.
- Соответствие формы спинки кресла форме спины работающего программиста.
- Перерыв в течение 15 минут после 45 минут работы.
- Занятие специальной гимнастикой, уменьшающей напряжение в фалангах пальцев, кистях, областях плеч, шеи и спины.

Меры предотвращения вредных воздействий на глазные мышцы:

- Наличие комфортного и удобного рабочего места
- Применение специализированных очков с линзами-фильтрами для людей, у которых уже наблюдается нарушение зрения;
- Использование защитных фильтров, уменьшающих вредное воздействие отраженных лучей от экрана.

- Монитор должен обладать затемненным экраном, либо покрыт слоем материала, снижающим бликовый коэффициент.
- Экран не должен находится напротив отражающих поверхностей и зеркал.
- Обеспечение правильной световой обстановки в помещении
- Зерно на экране монитора не должно быть размером до 0,28 мм.

Меры безопасности, предотвращающие возможности поражения электричеством:

- Обязательное заземление всех технических средств.
- Ограничение по подключению и ремонту средств информационной техники самим персоналом.
- Запрещение использования сломанной и неисправной аппаратуры
- Соблюдение правил техники безопасности.

Электронное оборудование, подключенное к сети переменного тока, подвергается различным негативным воздействиям со стороны питающей сети.

- радиочастотные шумы от воздействия мощных радиопередающих и иных устройств и помехи от импульсных блоков питания;
- скачок напряжения выше 110% от номинала, кратковременные (на несколько периодов сети) или длительные, связанные с техническими неполадками в сети.
- кратковременные провалы (в течение нескольких периодов), вызванные подключением мощной нагрузки, и длительные понижения уровня напряжения ниже 85% от номинального значения;
- потеря напряжения более чем на два полупериода частоты;
- отклонение частоты питающей сети от номинала 50 Гц;
- гармонические искажения питающего напряжения.

Меры, ведущие к устранению нервно-эмоциональных перегрузок:

- Использование удобного и усовершенствованного интерфейса. Необходимо соблюдать контрастную политику и не использовать

очень яркие элементы интерфейсов, негативно воздействующие на восприятие.

- Исключение присутствия на экране неспециализированной информации, которая может отвлекать внимание и снижать работоспособность.
- Специалистам по информационной безопасности необходимо обеспечить адекватное время реакции вычислительной техники. Среднее время ответа технических средств около 5-10 секунд.

Пожарной профилактикой называют комплекс организационных и технических мер, направленных на обеспечение безопасности людей, на предотвращение возгораний, ограничения его локального распространения, а также на создание условий для непосредственного тушения возгораний

Пожаром называют неконтролируемое горение во времени и пространстве, наносящее материальный ущерб и создающее угрозу жизни и здоровью людей. Опасными факторами пожара являются:

1.открытый огонь и искры;

2.повышенная температура воздуха и окружающих среды;

3.обрушение и повреждение зданий, сооружений, установок.

4.пониженная концентрация кислорода в воздухе;

5.токсичные продукты горения;

6.дым около рабочего места.

В современных ЭВМ элементы печатных плат расположены вблизи друг друга, что приводит к нагреванию этих элементов. В такой близости друг от друга располагаются и соединительные провода, кабели связи. При напряжении по ним электрического тока выделяется большое количество теплоты, что может привести к повышению температуры элементов. Возникает опасность потери изоляции соединительных проводов, их оголение и, как следствие, короткое замыкание, которое сопровождается дымообразованием и нагреванием соседних элементов. Последние, перегреваясь, сгорают и наносят вред техники.

Эффективным средством защиты от короткого замыкания и его причин является использование тугоплавких и негорючих материалов в изоляции приборов. Необходимо соблюдать требования пожарной безопасности, которые предусматриваются в ГОСТ 12.1.004-76 ССБТ «Пожарная безопасность. Общие требования.»:

- Безопасность от пожара должна проектироваться системами предотвращения пожара и защиты от пожара. Система предотвращения пожара складывается из регламентов и общими правилами эксплуатации технических средств, таких как освещения, кондиционирования и вентиляции в помещениях. Система защиты от пожара складывается из мероприятий, в состав которых входят применение специальных средств коллективной и индивидуальной защиты человека или группы людей в случае возникновения пожара, обеспечение рабочей и реагирующей пожарной сигнализации и также других средств извещения о пожаре и организация пожарной охраны объекта.
- Помещения должны соответствовать требованиям СН 512-78 и СНиП 2-2-80, которые предназначены для проектирования зданий и других построек. Все помещения должны быть спроектированы с соблюдением всех технических особенностей и сооружаются из кирпича, бетона, металла, стекла и отделяются от других соседних комнат огнеупорными стенами. Опорные конструкции над помещениями защищаются огнестойкой защитной краской. Перекрытия и потолки должны содержать изоляцию по всему контуру помещения.
- В соответствии с СНиП 2-90-81 «Проектирование зданий промышленных предприятий» устанавливается категория безопасности «В» и системы противопожарной защиты (для твердых горючих веществ и материалов). Стены должны быть огнеупорные с уровнем огнестойкости не менее 0.75. Для технологических перекрытий

устанавливаются тугоплавкие плиты. Подпольное помещение должно разделяться огнеупорными перегородками на отсеки с площадью не более 250 квадратных метров. При установке электрический линий используются минераловатные плиты для обеспечения максимальной безопасности.

- Согласно ГОСТ 12.4.009-75 «Первичные средства тушения пожара» должны присутствовать: сухой песок в железном ящике, огнетушитель, гидрант, асбестовые одеяла. По приведенному ГОСТу пожарный кран должен находится на высоте 1.35 метров от пола в доступном для пользователей месте и оснащается рукавами диаметром 50 мм и длиной от 10 до 20 метров. В зале с техническими средствами применение воды для тушения возгораний возможно только в случае отключения энергоприборов от электросети.
- Для ориентирования местонахождения пожарной техники и огнетушащих средств используются указательные знаки по ГОСТ 12.4.026-76 «Знаки указательные». Знаки размещаются на высоте от 2 до 2.5 метров. На месте расположения гидрантов устанавливается указатель (обязательно цветной) в виде букв «ПГ». Огнетушитель размещается на высоте не более 1.5 метров от пола со специальным оформлением, для того, чтобы можно было определить тип огнетушителя.

Заключение

В данной дипломной работе было разработано программное обеспечения для уменьшение рисков на ИТВ при распределении ресурсов под задачи в нестохастической среде методами теории адаптивного управления для специалистов по информационной безопасности. Таким образом, использование такого способа динамического формирования пулов сможет решать разные задачи в случаях, когда потребности задач завышают доступные ресурсы конкретных элементов ИВС, путем адаптирования структуры ИВС, существующей во время решения задачи.

Список используемой литературы:

1). Дубовцев В.А. Безопасность жизнедеятельности. / Учеб. пособие для дипломни-ков. - Киров: изд. КирПИ, 1992.+

2). Мотузко Ф.Я. Охрана труда. – М.: Высшая школа, 1989. – 336с.

3). Безопасность жизнедеятельности. /Под ред. Н.А. Белова - М.: Знание, 2000 - 364с.
4). Самгин Э.Б. Освещение рабочих мест. – М.: МИРЭА, 1989. – 186с.
5). Справочная книга для проектирования электрического освещения. / Под ред. Г.Б. Кнорринга. – Л.: Энергия, 1976.
6). Борьба с шумом на производстве: Справочник / Е.Я. Юдин, Л.А. Борисов; Под общ. ред. Е.Я. Юдина – М.: Машиностроение, 1985. – 400с., ил.
7). Метод динамического формирования пулов в информационно-вычислительных системах военного назначения / В. В. Грызунов // Информационно-управляющие системы .— 2015 .— №1 – 7с.
8). Дьяконов В. П. MATLAB. Полный самоучитель; ДМК Пресс - Москва, 2010. - 768 с.
9). Ахо А. и др. Компиляторы: принципы, технологии и инструментарий, 2-е изд.: Пер. с англ. - М.: ООО "И.Д. Вильямс", 2008. -
10). Таненбаум Э. Архитектура компьютера. – СПб.: Питер, 2007. – 844 с.
11). Мартынов Н.Н., Иванов А.П. MATLAB 5.x Вычисление, визуализация, программирование – М.: КУДИЦ-ОБРАЗ, 2000. – 336 с.
12). Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.: ил.
13). Блахнов Л.Л., Игнатенков В.Г. Инфокоммуникационные сети: архитектура, технологии, стандартизация. – М.: Радио и связь, 2004. – 56 с.: ил.
14). Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2001. –544 с.: ил.
15). Калинин В. Н. Теоретические основы системных исследований: краткий авторский курс лекций для адъюнктов академии. — СПб.: ВКА им. А. Ф. Можайского, 2011. — 278 с.
16). Грызунов В. В. Аналитическая модель целостной информационной системы // Доклады ТУСУР. № 1(19). Ч. 1. с. 226–230.

17). Грызунов В. В. Оценивание живучести неоднородных структур // Вестник СибГУТИ. 2011. № 1.с. 28–35.
18). Хорошевский В. Г. Архитектура вычислительных систем. — М.: МГТУ им. Н. Э. Баумана, 2008. — 520 с.
19). Гуров А. И. Инфосервис. // Системы безопасности. – 1995. №1. - 168 с.
20). Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через «Internet»/ Под научной редакцией проф. Зегжды П.Д. – М.: ДМК, 1999. – 336с.
21). Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.
22). Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
23). Соломин, В.П. Безопасность жизнедеятельности: Учебник для вузов / Л.А. Михайлов, В.П. Соломин, Т.А. Беспамятных; Под ред. Л.А. Михайлов. - СПб.: Питер, 2013. - 461 с.
24). Куправа, Т.А. Управление торговлей 1С: 8.3. Редакция 11. 1. Функционал развития / Т.А. Куправа. - М.: ДМК, 2015. - 316 с.
25). Никитин, А.В. Управление предприятием (фирмой) с использованием информационных систем: Учебное пособие / А.В. Никитин, И.А. Рачковская, И.В. Савченко. - М.: ИНФРА-М, 2009. - 188 с.
26). Ширяев, В.И. Управление предприятием: Моделирование, анализ, управление / В.И. Ширяев, И.А. Баев, Е.В. Ширяев. - М.: КД Либроком, 2015. - 272 с.
27). Миленина, С.А. Электротехника, электроника и схемотехника: Учебник и практикум для СПО / С.А. Миленина, Н.К. Миленин. - Люберцы: Юрайт, 2016. - 399 с.
28). Ермуратский, П. Электротехника и электроника / П. Ермуратский, Г. Лычкина. - М.: ДМК, 2015. - 416 с.

29). Бочкарёв, А.И. Макроэкономика.Учебное пособие для ВУЗов / А.И. Бочкарёв, Т.С. Бочкарёва и др. - М.: КноРус, 2010. - 390 с.
30).Комарницкий, Ю.А. Экономика для инженера. В 2 ч. Ч. 1 Введение в экономическую теорию. Макроэкономика / Ю.А. Комарницкий. - М.: Высшая школа, 2001. - 359 с.
31). Ануфриев И. Самоучитель MatLab 5.3/6.x; БХВ-Петербург - Москва, 2004. - 736 с.
32). Sergey N. Makarov Antenna and EM Modeling with Matlab; Мир - Москва, 2004. - 923 с.
33). Блиновская, Я.Ю. Введение в геоинформационные системы: Учебное пособие / Я.Ю. Блиновская, Д.С. Задоя. - М.: Форум, НИЦ ИНФРА-М, 2013. - 112 с.
34).Теоретические основы информатики. Р. Б. Куликов. – Пенза, 2008.
35).Теория информации. Д. М. Михайлов. – М.: КМ-Сервис, 2009.

ПриложениеА

```
function [w12, w21] = present(P, w12, w21, rho, psi, i)
[s2,s1] = size(w12);
ind_x = [];
res_flag = 0;
while(res_flag==0)
% Шаг 1.Поочередно присваивается переменной a1.
p=P(:,i);
a1 =p;
% Шаг 2. Отклик 2-го шара
n1 = w12*a1;
n1(ind_x) = -inf*ones(size(ind_x));
[mxn1,k] = max(n1); %Максимальное значение n1 и его номер
a2 = zeros(s2,1); %Заполнение нулями a1
a2(k) = 1; %
% Шаг 3. Выбираются веса выигравшего нейрона
expect=w21(:,k);
% Шаг 4. Настройка выхода 1-го шара с учетом ожидания
a1 =p&expect;
% Шаг 5.
if ((sum(a1)/sum(p))<rho)
a0 = 1;
else
a0 = 0;
end
% Шаг 6. Проверка на резонанс, подавляя текущий отклик если нету
if (a0)
```

```
ind_x = [ind_x; k];
% Если все прототипы использованы, добавить еще один
if(length(ind_x)==s2)
if (s2==10)
error('More than four prototypes needed')
else
w21 = [w21 ones(s1,1)];
w12 = [w12; psi*ones(1,s1)/(psi+s1-1)];
s2 = s2+1;
else
% Резонанс
res_flag= 1;
% Шаг 7, Обновить строку k матрицы w12
w12(k,:) = psi*a1'/(psi+sum(a1)-1);
% Шаг 8, Обновить колонку k матрицы w21
w21(:,k) = a1;
end % if a0
end % while res_flag
%Discrete Hopfield net
clc; clear;
x=[1 1 1 0];
tx=[0 0 1 0];
w=(2*x'–1)*(2*x–1);
for i=1:4
w(i,i)=0;
end
con=1;
y=[0 0 1 0];
```

```
while con
up=[4 2 1 3];
for i=1:4
yin(up(i))=tx(up(i))+y*w(1:4,up(i));
if yin(up(i))>0
y(up(i))=1;
end
end
if y==x
disp('Convergence has been obtained');
disp('The Converged Ouput');
disp(y);
con=0;
end
function lab6
clear all; close all; clc;
s2 = 5; % 10 digits
imSize = 50;
%% Read images
for i=0:s2-1
p = imread(strcat(int2str(i),'.jpg'));
p = fixImage(p, imSize);
%p = im2bw(p);
P(:,i+1) = p(:);
end
%% Initialization
Pat = P;
P= 1-P;
```

```
W = [];
%% Training
for i = 1:s2
W = present(P(:, i), W);
end
%% Recognition
P = []; R = [];
files = ['2def.jpg'; '0def.jpg'];
for i=1:size(files,1)
[p, r] = recognition(files(i,:), W, imSize, Pat);
P = [P, p];
R = [R, r];
end;
figure('Name', 'Digits recognition', 'NumberTitle', 'off');
subplot(2, 1, 1);imshow(P); title('Pattern image')
subplot(2, 1, 2);imshow(R); title('Recognized image')
function [im, r] = recognition(file, W, imSize, P)
im = imread(file);
im = fixImage(im, imSize);
[rows cols] = size(im);
N = rows;
mat = repmat(im,N,N);
mat = mat.*W;
mat = im2col(mat,[N,N],'distinct');
networkResult = sum(mat);
networkResult = reshape(networkResult,N,N);
r = fixImage(networkResult,N);
p = double(r(:));
```

```
size(P)

size(p)

n1 = P'*p;

[mxn1,k] = max(n1);

r = imread(strcat(int2str(k-1),'.jpg'));

function W = present(im, W)

N = length(im(:));

N = sqrt(N);

im = reshape(im, N, N);

avg = mean(im(:)); %removing the cross talk part

if ~isempty(W)

W = W + ( kron(im-avg,im-avg))/(N^2)/avg/(1-avg);

else

W = ( kron(im-avg,im-avg))/(N^2)/avg/(1-avg);

end

% Erasing self weight

ind = 1:N^2;

f = find(mod(ind,N+1)==1);

W(ind(f),ind(f)) = 0;

function im = fixImage(im, N)

if length( size(im) ) == 3

im = rgb2gray(im);

end

im = double(im);

m = min(im(:));

M = max(im(:));

im = (im-m)/(M-m); %normelizing the image

im = imresize(im,[N N],'bilinear');
```

```
im = (im > 0.5); %changing image values to 0 & 1

function varargout = hopfieldNetwork(varargin)

gui_Singleton = 1;

gui_State = struct('gui_Name', mfilename, ...

'gui_Singleton', gui_Singleton, ...

'gui_OpeningFcn', @hopfieldNetwork_OpeningFcn, ...

'gui_OutputFcn', @hopfieldNetwork_OutputFcn, ...

'gui_LayoutFcn', [] , ...

'gui_Callback', []);

if nargin && ischar(varargin{1})

gui_State.gui_Callback = str2func(varargin{1});

end

if nargout

[varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});

else

gui_mainfcn(gui_State, varargin{:});

end

function hopfieldNetwork_OpeningFcn(hObject, eventdata, handles, varargin)

handles.output = hObject;

N = str2num(get(handles.imageSize,'string'));

handles.W = [];

handles.hPatternsDisplay = [];

guidata(hObject, handles);

function varargout = hopfieldNetwork_OutputFcn(hObject, eventdata, handles)

varargout{1} = handles.output;

function reset_Callback(hObject, eventdata, handles)

for n=1 : length(handles.hPatternsDisplay)

delete(handles.hPatternsDisplay(n));
```

```
end

handles.hPatternsDisplay = [];

set(handles.imageSize,'enable','on');

handles.W = [];

guidata(hObject, handles);

function imageSize_Callback(hObject, eventdata, handles)

num = get(hObject,'string');

n = str2num(num);

if isempty(n)

num = '32';

set(hObject,'string',num);

end

if n > 32

warndlg('It is strongly recomended NOT to work with networks with more then 32^2 neurons!','!! Warning !!')

end

function imageSize_CreateFcn(hObject, eventdata, handles)

if ispc

set(hObject,'BackgroundColor','white');

else

set(hObject,'BackgroundColor',get(0,'defaultUicontrolBackgroundColor'));

end

function loadIm_Callback(hObject, eventdata, handles)

[fName dirName] = uigetfile('*.bmp;*.tif;*.jpg;*.tiff');

if fName

set(handles.imageSize,'enable','off');

cd(dirName);

im = imread(fName);
```

```
N = str2num(get(handles.imageSize,'string'));
im = fixImage(im,N);
imagesc(im,'Parent',handles.neurons);
colormap('gray');
end
function train_Callback(hObject, eventdata, handles)
Npattern = length(handles.hPatternsDisplay);
if Npattern > 9
msgbox('more then 10 paterns isn''t supported!','error');
return
end
im = getimage(handles.neurons);
N = get(handles.imageSize,'string');
N = str2num(N);
W = handles.W; %weights vector
avg = mean(im(:));
if ~isempty(W)
W = W + ( kron(im-avg,im-avg))/(N^2)/avg/(1-avg);
else
W = ( kron(im-avg,im-avg))/(N^2)/avg/(1-avg);
end
% Erasing self weight
ind = 1:N^2;
f = find(mod(ind,N+1)==1);
W(ind(f),ind(f)) = 0;
handles.W = W;
% Placing the new pattern in the figure...
xStart = 0.01;
```

```
xEnd = 0.99;
height = 0.65;
width = 0.09;
xLength = xEnd-xStart;
xStep = xLength/10;
offset = 4-ceil(Npattern/2);
offset = max(offset,0);
y = 0.1;
if Npattern > 0
for n=1 : Npattern
x = xStart+(n+offset-1)*xStep;
h = handles.hPatternsDisplay(n);
set(h,'units','normalized');
set(h,'position',[x y width height]);
end
x = xStart+(n+offset)*xStep;
h = axes('units','normalized','position',[x y width height]);
handles.hPatternsDisplay(n+1) = h;
imagesc(im,'Parent',h);
else
x = xStart+(offset)*xStep;
h = axes('units','normalized','position',[x y width height]);
handles.hPatternsDisplay = h;
end
imagesc(im,'Parent',h);
set(h, 'YTick',[],'XTick',[],'XTickMode','manual','Parent',handles.learnedPaterns);
guidata(hObject, handles);
function addNoise_Callback(hObject, eventdata, handles)
```

```
im = getimage(handles.neurons);
noisePercent = get( handles.noiseAmount, 'value' );
N = round( length(im(:))* noisePercent );
N = max(N,1); %minimum change one neuron
ind = ceil(rand(N,1)*length(im(:)));
im(ind) = ~im(ind);
imagesc(im,'Parent',handles.neurons);
colormap('gray');
function run_Callback(hObject, eventdata, handles)
im = getimage(handles.neurons);
[rows cols] = size(im);
if rows ~= cols
msgbox('I don''t support non square images','error');
return;
end
N = rows;
W = handles.W;
if isempty(W)
msgbox('No train data - doing nothing!','error');
return;
end
%figure; imagesc(W)
mat = repmat(im,N,N);
mat = mat.*W;
mat = im2col(mat,[N,N],'distinct');
networkResult = sum(mat);
networkResult = reshape(networkResult,N,N);
im = fixImage(networkResult,N);
```

```
imagesc(im,'Parent',handles.neurons);

function im = fixImage(im,N)

if length( size(im) ) == 3

im = rgb2gray(im);

end

im = double(im);

m = min(im(:));

M = max(im(:));

im = (im-m)/(M-m); %normelizing the image

im = imresize(im,[N N],'bilinear');

%im = (im > 0.5)*2-1; %changing image values to -1 & 1

im = (im > 0.5); %changing image values to 0 & 1

function noiseAmount_Callback(hObject, eventdata, handles)

percent = get(hObject,'value');

percent = round(percent*100);

set(handles.noisePercent,'string',num2str(percent));

function noiseAmount_CreateFcn(hObject, eventdata, handles)

usewhitebg = 1;

if usewhitebg

set(hObject,'BackgroundColor',[.9 .9 .9]);

else

set(hObject,'BackgroundColor',get(0,'defaultUicontrolBackgroundColor'));

end

%Discrete Hopfield net

clc; clear;

x=[1 1 1 0];

tx=[0 0 1 0];

w=(2*x'–1)*(2*x–1);
```

```
for i=1:4
w(i,i)=0;
end
con=1;
y=[0 0 1 0];
while con
up=[4 2 1 3];
for i=1:4
yin(up(i))=tx(up(i))+y*w(1:4,up(i));
if yin(up(i))>0
y(up(i))=1;
end
end
if y==x
disp('Convergence has been obtained');
disp('The Converged Ouput');
disp(y);
con=0;
end
```