**Математическое обеспечение системы документооборота Министерства торговли Российской Федерации.**

ВВЕДЕНИЕ

Широкое внедрение информационных технологий в жизнь современного общества привело к необходимости решения ряда общих проблем информационной безопасности. Потенциальная уязвимость информационной системы (ИС) по отношению к случайным и предумышленным отрицательным воздействиям выдвинула проблемы информационной безопасности в разряд важнейших, стратегических, определяющих принципиальную возможность и эффективность применения ряда ИС в гражданских и военных отраслях.

Требования по обеспечению безопасности в различных ИС могут существенно отличаться, однако они всегда направлены на достижение трех основных свойств:

* целостность – информация, на основе которой принимаются решения, должна быть достоверной и точной, защищенной от возможных непреднамеренных и злоумышленных искажений;
* доступность (готовность) – информация и соответствующие автоматизированные службы должны быть доступны, готовы к работе всегда, когда в них возникает необходимость;
* конфиденциальность – засекреченная информация должна быть доступна только тому, кому она предназначена.

Для решения проблем информационной безопасности необходимо сочетание законодательных, организационных, программно-технологических мероприятий.

Так сложилось, что основное внимание в теории и практике обеспечения безопасности применения информационных технологий и систем сосредоточено на защите от злоумышленных разрушений, искажений и хищений программных средств и информации баз данных. Для этого разработаны и развиваются проблемно-ориентированные методы и средства защиты:

* от несанкционированного доступа;
* от различных типов вирусов;
* от утечки информации по каналам электромагнитного излучения.

Целью настоящей работы является разработка математического и программного обеспечения модуля мандатного разграничения прав доступа для системы документооборота Министерства Торговли.

Мандатный принцип контроля доступа является необходимым требованием при реализации комплекса средств защиты (КСЗ) средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) четвертого и более высокого класса в соответствие с руководящим документом Гостехкомиссии России. Надо сказать, что четвертый класс, по упомянутой классификации, является наиболее приемлемым для многопользовательских ИС, в которых содержатся данные конфиденциального порядка или же содержащие государственную тайну.

Суть мандатного принципа контроля доступа состоит в сопоставлении каждому субъекту (пользователю) и объекту системы классификационных меток, которые можно условно считать уровнями секретности, кроме того внутри каждого уровня секретности содержатся категории (их можно понимать как отделы или подразделения).

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила — читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может писать в секретные файлы, но не может — в несекретные (разумеется, должны также выполняться ограничения на набор категорий). На первый взгляд подобное ограничение может показаться странным, однако оно вполне разумно. Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен. Посторонний человек может случайно узнать секретные сведения и сообщить их куда следует, однако лицо, допущенное к работе с секретными документами, не имеет права раскрывать их содержание простому смертному.

В основном данный механизм направлен на защиту от ошибок пользователей, которые могут непреднамеренно разгласить конфиденциальные данные. Кроме того, при использовании описанной схемы разграничения прав доступа, после того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа, что позволяет проведение более жесткой и четкой сформулированной политики безопасности.

ГЛАВА 1. СИСТЕМНЫЙ АНАЛИЗ И СИНТЕЗ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

1.1. Анализ замысла, целей, направлений и этапов разработки системы

1.1.1. Замысел и цели разработки системы

Настоящая глава является частью "Технического предложения", разработанного в соответствии с "Соглашением о намерениях по взаимодействию в области создания Системы внешнеторговой информации между Министерством торговли Российской Федерации и НИИ автоматической аппаратуры им. академика В.С. Семенихина", подписанного Министром торговли и Директором НИИ АА 12 октября 1998 г. Соглашение предусматривало *инициативное* проведение информационного обследования Минторга России специалистами НИИ АА и разработку "Технического предложения" по информатизации Министерства. В результате выполнения работы необходимо было получить ответы на вопросы:

существует ли проблема информатизации Министерства торговли РФ;

если существует, то каким образом ее можно решить.

1.1.2. Направления и этапы разработки системы

Работы проводились в соответствии с государственным стандартом ГОСТ 34.601 - 90 "Автоматизированные системы. Стадии создания", который предусматривает следующую последовательность выполнения работ:

Проведение обследования объекта и формирование требований к автоматизированной системе.

Разработка концепции автоматизированной системы.

Техническое задание.

Эскизный проект.

Технический проект.

Рабочая документация.

Ввод в действие.

Сопровождение АС.

При проведении обследования, основная задача состояла в получении информации по следующим вопросам организационного построения и деятельности каждого из структурных подразделений министерства (департаментов, управлений и т.д.):

Организационно-функциональная структура Подразделения; схема информационного взаимодействия между его структурными единицами и отдельными функционерами.

Система делопроизводства, разработки и хранения документов.

Функции, задачи и процессы деятельности Подразделения.

Предложения по решению задач на ПЭВМ; краткие постановки таких задач.

Расширенные постановки нескольких наиболее проработанных и эффективных задач, для реализации их на опытном участке системы.

Информационные ресурсы Подразделения (как поставленные на ЭВМ, так и ведущиеся вручную): состав и структура баз данных (картотек), используемые словари и классификаторы.

Подразделения Минторга России, федеральные органы исполнительной власти РФ, международные организации, субъекты внешнеторговой деятельности и т.д., с которыми Подразделение должно взаимодействовать.

Характеристика каждого направления взаимодействия: регламент, структура документов, информационные потоки и вид взаимодействия (электронная почта, онлайн, офлайн); проблемы, возникающие при взаимодействии.

Характеристика обрабатываемой, хранящейся и передаваемой информации по уровню конфиденциальности (служебная, открытая).

Необходимость доступа сотрудников Подразделения к информационным ресурсам сети Интернет (если можно, конкретизировать к каким именно).

Информация Подразделения, которую целесообразно разместить на Web-сервере Минторга России в сети Интернет.

Оснащенность Подразделения средствами вычислительной техники (ВТ), используемые программные продукты.

Характеристика размещения средств ВТ в помещениях Подразделения.

Оценка степени подготовленности пользователей и актуальности автоматизации.

Следует отметить, что, по тем или иным причинам (как объективным, так и субъективным), не для всех обследованных подразделений удалось получить полную информацию по сформулированным выше вопросам.

Результаты проведенного информационно-технологического обследования, показали, что проблема информатизации Минторга России существует и заключается в несоответствии уровня информатизации министерства уровню, требуемому для его эффективного функционирования в современных условиях.

Можно утверждать, что необходимое повышение эффективности деятельности Минторга невозможно без использования в повседневной практике работы современных информационных технологий, т.е. без информатизации.

Информатизация - это организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей органов государственной власти, на основе формирования и использования информационных ресурсов.

Чтобы создать оптимальные условия для удовлетворения информационных потребностей Минторга России, т.е. решить проблему его информатизации, необходимо:

* создать инфраструктуру, поддерживающую формирование и использование информационных ресурсов, на базе современных компьютерных и телекоммуникационных технологий;
* разработать и внедрить на этой инфраструктуре программные средства автоматизации основных видов деятельности;
* наполнить информационные базы данных Министерства и обеспечить оперативный доступ сотрудников к информационным ресурсам Федеральных и региональных органов государственной власти России, общедоступным и коммерческим ресурсам сети Интернет.

1.2. Министерство торговли как объект информатизации

1.2.1. Министерство торговли как потребитель и источник информации

Министерство торговли РФ является весьма крупным потребителем и источником информации о чем свидетельствуют приводимые ниже потоки входящих и исходящих документов, а также оценки объемов хранимой информации, необходимой в повседневной работе.

Оценка общего количества документов за 1998 год, прошедших через Канцелярию УД Министерства и службы делопроизводства департаментов (управлений):

входящие - свыше 30000;

исходящие - свыше 12000.

Объемы информации, необходимой центральному аппарату Министерства в повседневной работе (статистическая и конъюнктурная информация, нормативно-правовые акты, исполняемые и разрабатываемые документы и т.п.) оцениваются следующими величинами:

* текущая (актуальная) информация - 2 - 3 миллиона условных машинописных страниц (что, при переводе в машинные форматы представления, соответствует объемам хранения примерно 200 - 300 гигабайт);
* информационная предыстория за 7 - 10 лет (в основном это статистическая информация прошлых периодов, которую необходимо хранить для получения сравнительных оценок, переписка, разрешительные документы и т.п.) - 10 - 15 миллионов условных машинописных страниц (что, при переводе в машинные форматы представления, соответствует объемам хранения примерно 1 - 1,5 терабайта).

Из-за большого объема документооборота, в Министерстве торговли имеет место отход от технологии делопроизводства, определенной государственными стандартами, инструкциями и наставлениями, в сторону комбинированной вертикально-горизонтальной технологии - правом внешней переписки обладают и начальники департаментов (управлений). Определенный объем переписки имеется также непосредственно между департаментами Министерства (минуя уровень Министра и его заместителей) и между отделами различных департаментов. Фактически система делопроизводства и документооборота Министерства представляет собой распределенную систему делопроизводства, состоящую из множества взаимодействующих между собой участков делопроизводства, причем один из них (Канцелярия Управления делами) играет по отношению к остальным координирующую и контролирующую роль. Каждый из таких участков в зоне своей ответственности использует строго вертикальную технологию движения документов. Движение документов между участками делопроизводства имеет вертикально-горизонтальный характер, определяемый как их относительным положением в организационно-штатной структуре центрального аппарата Министерства, так и рангом их внешних корреспондентов и адресатов.

В настоящее время в центральном аппарате Министерства с помощью средств вычислительной техники обрабатывается лишь ничтожная часть всей этой информации (порядка 1-2 %).

Анализ задач и функций, предписанных Министерству в соответствии с Положением о нем, показывает, что основные направления его деятельности связаны с глубоким анализом огромных объемов статистического, конъюнктурного, нормативно-правового и другого материала в контексте сложных и многомерных экономических, социальных, внутри- и внешнеполитических целей, устанавливаемых Правительством РФ.

В настоящее время в центральном аппарате Министерства не используется каких-либо средств поддержки аналитической обработки информации.

Вместе с тем в арсенале современных информационных технологий имеется ряд методов и средств аналитической обработки как структурированной, так и неструктурированной информации, а также технологий решения сложных многомерных количественно-качественных проблем, для которых характерно отсутствие аналитических зависимостей между определяющими их факторами.

В данных Технических предложениях рассматривается несколько прикладных задач аналитической обработки информации, которые, на наш взгляд, будут полезны в качестве средств поддержки аналитической работы специалистов центрального аппарата Министерства и некоторых входящих в его систему учреждений и организаций.

Основные проблемы, которые необходимо решить для развертывания полномасштабной системы аналитической обработки информации:

Получение необходимой Министерству информации от федеральных и региональных органов

Внедрение единой системы классификации и кодирования элементов данных.

Разработка единой для взаимодействующих министерств и ведомств системы представления информации об объектах учета (уровень агрегирования информации, состав представляемых элементов данных, форматы данных и т.п.).

Придание электронным документам юридической силы.

Общесистемные прикладные задачи информатизации Министерства торговли

В рамках предлагаемой системы информатизации Министерства имеется ряд системных и прикладных задач, которые необходимы каждому (или большинству) из рассматриваемых подразделений. К таким задачам относятся:

Автоматизированная система делопроизводства и документооборота.

Контроль исполнения поручений.

Разработка и согласование документов.

Справочная информация по министерству.

Справочная информация по органам государственной власти и управления РФ.

Внутриминистерская электронная почта.

Внешняя электронная почта.

Информационные ресурсы Интернет.

База нормативных и правовых документов федерального уровня.

Система внешнеторговой информации (СВТИ).

Доступ к функциям этих задач должен обеспечиваться с каждого автоматизированного рабочего места (АРМ) будущей системы (разумеется, в пределах прав и полномочий, определяемых статусом и должностными функциями пользователей АРМ).

1.2.2. Комплекс прикладных задач "Делопроизводство, документооборот и электронный архив"

Этот комплекс задач является одним из основных общесистемных прикладных комплексов. Анализ показал, что суммарный поток входящих и исходящих документов на уровне Министерства и его департаментов (управлений) превышает 40000 единиц в год. Существующая система автоматизации делопроизводства охватывает только канцелярию Управления делами, функционально не удовлетворяет потребностям морально и физически устарела.

При таком объеме документооборота можно ожидать, что эффект от реализации единой автоматизированной системы делопроизводства Министерства будет весьма значительным.

Реализация и внедрение данного комплекса задач должно постепенно перевести делопроизводство и документооборот в Министерстве торговли РФ на уровень, соответствующий современному состоянию информационных технологий.

1.2.2.1. Общие требования к комплексу задач ДДЭА

Комплекс задач "Делопроизводство, документооборот и электронный архив" (ДДЭА) должен обеспечивать соблюдение требований российских стандартов, инструкций и наставлений в области делопроизводства и документооборота. Кроме того, он должен сохранять полезные традиции и технологии делопроизводства, выработанные за долгую предысторию Министерства.

Поскольку в настоящее время действующие стандарты и инструкции определяют лишь бумажную форму документа, то на данном этапе комплекс задач должен выполнять в основном функции сопровождения бумажного документооборота, обеспечивая снижение трудоемкости рутинных операций делопроизводства за счет автоматизации процессов регистрации документов, учета резолюций руководителей на документах, отслеживания движения документов и контроля исполнения резолюций.

Вместе с тем, комплекс задач с момента ввода его в эксплуатацию должен начать выполнять функцию "мостика" для постепенного перехода от бумажных к "электронным" документам, обеспечивая разработку документов на ПЭВМ с помощью современных программных средств, ведение архивов подготовленных электронных документов, поиск документов в таких архивах, ведение внутриминистерской переписки в электронном виде (по крайней мере - частично).

В соответствии с принятой в Министерстве смешанной вертикально-горизонтальной технологией делопроизводства и документооборота, программные средства комплекса прикладных задач ДДЭА должны обеспечивать формирование в рамках центрального аппарата Министерства совокупности взаимодействующих "локальных" систем (или участков) делопроизводства и документооборота.

Такая совокупность взаимодействующих "локальных" систем делопроизводства и документооборота в рамках единой технологии должна охватывать уровни:

Министерства

Департаментов (управлений) или самостоятельных отделов

Отделов в составе департаментов (управлений)

Для системы делопроизводства и документооборота, соответствующей уровню Канцелярии Управления делами Министерства, должна обеспечиваться возможность выполнения координирующих и контролирующих функций по отношению к остальным участкам делопроизводства. Каждый из формируемых участков делопроизводства в зоне своей ответственности использует строго вертикальную технологию движения документов. Движение документов между участками делопроизводства имеет вертикально-горизонтальный характер, определяемый как их относительным положением в организационно-штатной структуре центрального аппарата Министерства, так и рангом их внешних корреспондентов и адресатов.

В пределах центрального аппарата Министерства взаимодействие между участками делопроизводства должно осуществляться через систему внутренней электронной почты (на начальном этапе информатизации - для подразделений Министерства, расположенных в одном здании). По мере развития уровня информатизации Министерства, обретения электронным документооборотом юридической силы, а также по мере готовности внешних адресатов и корреспондентов, должен обеспечиваться постепенный переход на взаимодействие участков делопроизводства через систему электронной почты и с внешними учреждениями и организациями, а также с территориально-удаленными учреждениями, входящими в систему Министерства (управления уполномоченных Минторга в субъектах Федерации и регионах РФ, торговые представительства РФ за рубежом и др.).

Программные средства комплекса задач должны обеспечивать его адаптацию к изменениям организационно-штатной структуры Министерства и его подразделений.

Программно-аппаратные средства комплекса задач должны обеспечивать функции разграничения доступа и защиты учетно-регистрационных данных делопроизводства и документов, хранимых в электронном виде, в соответствии с действующими в Министерстве инструкциями.

Комплекс задач ДДЭА должен обладать следующими функциональными возможностями, поддерживающими основные задачи и функции делопроизводства:

Учетной обработки документов

Доведения документов до должностных лиц

Рассылки документов

Контроля исполнения резолюций

Подготовки отчетных документов делопроизводства

Архивирования документов и поиска их в архивах

Ведения и использования разнообразных справочников, классификаторов и шаблонов, необходимых в делопроизводстве

К функциям делопроизводства и документооборота тесно примыкает (хотя и не относится к ним) функция поддержки разработки документов в подразделениях Министерства. Будучи важной составной частью общего процесса документационного обеспечения управления, эта функция также рассматривается в рамках комплекса задач поддержки делопроизводства и документооборота.

1.2.3. Современное состояние информатизации Минторга

*Центральный аппарат* при численности 939 человек, имеет 524 компьютера. Из них 337 компьютеров безнадежно устаревших моделей, требуют списания. 187 компьютеров могут быть использованы (с определенными ограничениями) в дальнейшем. Неплохо оснащены департаменты ВТС и ДФБУ. Компьютеры, как правило, используются автономно. Дополнительно требуется 350 современных компьютеров, объединение всех их в единую локальную вычислительную сеть (ЛВС) и использование в соответствии с системной идеологией.

*Управления и представительства уполномоченных в регионах* (79 представительств) имеют 217 маломощных устаревших компьютера. Работоспособные компьютеры могут продолжать ограниченно использоваться. Для целей информатизации требуется приобретение 200 современных компьютеров и создание ЛВС в некоторых управлениях.

*Госторгинспекции в регионах* (80 инспекций)оснащены достаточно неплохо. Имеют 45 устаревших и 121 достаточно современных компьютера. Требуется дооснащение 50 компьютерами.

*Торговые представительства в иностранных государствах* (86 ТП и АТС) имеют 161 устаревший и 94 современных компьютера. 26 ТП и АТС подключены к международным сетям передачи данных. Требуется дооснащение 100 компьютерами и развертывание ЛВС в ряде ТП.

Примечание. Оценки потребностей в оснащении компьютерами являются экспертными. Они будут уточнены на стадии технического проектирования.

*Автоматизации основных видов деятельности.*На большинстве компьютеров осуществляется набор и распечатка текстов подготавливаемых документов (интеллектуальная пишущая машинка). В некоторых отделах ведутся отраслевые базы данных, доступные, как правило, незначительному числу сотрудников отдела. Осуществляется анализ достаточно ограниченных объемов статистических данных. Ввод данных часто производится (например, в департаментах внутренней торговли) вручную с бумажных носителей. В департаменте ДФБУ используется бухгалтерская система. В УД используется морально устаревшая система ведения делопроизводства, а в УКГС - кадровая система. В ближайшее время предполагается создание комплекса средств автоматизации для обеспечения выдачи экспортных сертификатов по текстилю за счет финансирования по программе TASIS (ДГРВЭД).

Телекоммуникационные сети и каналы связи для обмена данными между подразделениями Минторга, с органами исполнительной власти и взаимодействующими организациями используются весьма ограниченных масштабах.

*Доступ к информационным ресурсам.* Внутренние информационные ресурсы Минторга доступны, в основном, сотрудникам отделов, создающих эти ресурсы.

С получением данных из Федеральных исполнительных органов (ГТК, Госкомстат и т.д.) связаны большие трудности, информация, как правило, не удовлетворяет сотрудников министерства ни формой представления, ни составом, ни качеством. Необходимо на правительственном уровне решить проблему получения информации из ГТК, Госкомстата, Минэкономики и ряда других министерств и ведомств. Информация должна поступать своевременно, быть достаточно детальной, точной и полной.

В департаментах внутренней торговли необходимая для анализа информация из регионов добывается часто за счет личных связей с сотрудниками региональных администраций. И это - при наличии в регионах уполномоченных Минторга и госторгинспекций. В процессе обследования у нас сложилось впечатление оторванности департаментов внутренней торговли от всех остальных подразделений министерства.

Многообразные ресурсы Интернет сотрудникам министерства практически недоступны. Исключение, видимо, составляют 26 ТП и АТС, подключенных к мировым сетям передачи данных.

1.3. Архитектура разрабатываемой системы

Рассмотрим общие требования к системе электронного документооборота.

Масштабируемость. Желательно, чтобы система документооборота могла поддерживать как пять, так и пять тысяч пользователей, и ее способность наращивать мощность определялась только мощностью аппаратного обеспечения, на котором она установлена. Выполнение этого требования может быть обеспечено с помощью поддержки индустриальных серверов баз данных, производства, например, компаний Sybase, Microsoft, Oracle, Informix, которые существуют практически на всех возможных программно-аппаратных платформах, обеспечивая тем самым максимально широкий спектр производительности.

Распределенность. Основные проблемы при работе с документами возникают в территориально-распределенных организациях, поэтому архитектура системы документооборота должна поддерживать взаимодействие распределенных площадок. Причем они могут быть объединены самыми разнообразными по скорости и качеству каналами связи. Также архитектура системы обязана обеспечивать взаимодействие с удаленными пользователями.

Модульность. Вполне возможно, что заказчику может не потребоваться сразу внедрение всех компонентов системы документооборота, а иногда круг решаемых заказчиком задач меньше всего спектра задач документооборота. Поэтому очевидно, что система должна состоять из отдельных модулей, интегрированных между собой.

Открытость. Система документооборота не может и не должна существовать в отрыве от других приложений, к примеру часто необходимо интегрировать систему с прикладной бухгалтерской программой. Следовательно, система документооборота должна иметь открытые интерфейсы для возможной доработки и интеграции.

На основании сформулированных требований группой разработчиков в составе Беляева А.И-М., Игнатова-Радохова Д.В. и Яковлева Д.В. была спроектирована архитектура системы документооборота Минторга РФ. Основой данной системы является сетевая операционная система Microsoft Windows NT и продукт той же компании – MS Exchange Server. Архитектура разрабатываемой системы приведена на рисунке 1.1. Обоснование выбора программных средств приводится в разделе 1.4.

1.4. Обоснование выбора программных средств

1.4.1. Операционная среда

Операционные среды: Windows 95 (или Windows NT Workstation 4.0) определена требованиями Заказчика, вытекающими из проектных работ.

1.4.2. Инструментальные средства разработки

В качестве средств разработки специального программного обеспечения была выбрана система Borland C++ Builder 3.0 Client/Server. Выбор обуславливается тем, что с ее помощью можно в кратчайшие сроки разработать быстрое, компактное и полноценное Windows-приложение, работающее с базами данных и приложениями электронной почты.

Для разработки программного обеспечения по курсу "Экономика" был выбран Visual Basic for Applications, так как программа должна будет работать под операционными системами Windows 95, в среде электронных таблиц Excel.

Для разработки программного обеспечения по курсу "Экология и охрана труда" был выбран пакет Borland C++ Builder 3.0 Client/Server, с помощью визуальной среды программирования которого легко создавать различные формы и пользовательские диалоги.

Для разработки программного обеспечения по курсу "Гражданская оборона" был также выбран Borland C++ Builder 3.0 Client/Server.

1.4.3. Среда реализации

Ниже приведены результаты проведенного комплексного исследования трех наиболее известные продуктов: Notes компании IBM/Lotus, Exchange Server фирмы Microsoft и GroupWise производства Novell. Были рассмотрены все достоинства и недостатки вышеприведенных систем и выбрана система, ставшая средой реализации задач данного дипломного проекта.

Все три продукта поддерживают несколько клиентских платформ - Microsoft Windows, Windows 95, Windows NT, Apple Macintosh, а в некоторых конфигурациях - IBM OS/2 и Unix. Для подключения к сети Интернет и другим системам электронной почты в каждом из пакетов предусмотрено шлюзовое ПО. Учитывая, что эти почтовые серверы поддерживают тысячи почтовых ящиков пользователей, а также включают функции администрирования и защиты данных в многодоменных системах с множеством почтовых отделений, становится ясно, почему разработкой продуктов такого класса занимаются только ведущие компании, обладающие для этого необходимыми ресурсами.

1.4.3.1. Основные особенности продуктов

Начнем с версии Notes 4.0 фирмы Lotus. Система Notes представляет собой операционную среду для создания документов и поддержки рабочих групп, организованную на основе сервера базы данных.

Независимые производители дополняют Notes все новыми и новыми приложениями, расширяющими возможности пакета, что немаловажно для продукта, претендующего на роль сетевой платформы масштаба предприятия. Система Notes давно получила признание благодаря своим средствам электронной почты и поддержки рабочих групп. Однако самой сильной стороной продукта является возможность настройки на конкретные требования заказчика, получившая развитие именно в последней версии Notes.

Как это ни парадоксально, но широкий выбор функций Notes - палка о двух концах. Например, при отсутствии в Notes нужного приложения вам нелегко будет найти опытного специалиста, способного создать программу для этой среды. Но, с другой стороны, если вы уже освоили систему Notes, то ее функции обработки документов, распределения и управления информацией, а также автоматического администрирования откроют перед вами такие возможности, которые нельзя даже сравнивать с имеющимися в любой из существующих стандартных систем электронной почты.

Основной конкурент Notes - продукт Exchange Server компании Microsoft. Это не просто расширение существующего пакета электронной почты MS Mail, а новая система, созданная в результате его коренной переработки. Exchange обладает гораздо более широкими возможностями, чем MS Mail, и включает средства подготовки форм на основе среды программирования Visual Basic (VB) 4 компании Microsoft. Exchange Server поддерживает архитектуру клиент/сервер и совместим с клиентской версией Exchange, поставляемой в составе Windows 95. Если пакет MS Mail ориентирован на рабочие группы, то Exchange Server, позволяющий управлять множеством серверов и доменов, подходит для использования в масштабе предприятия.

Пакет GroupWise компании Novell представляет собой систему передачи почтовых сообщений и календарного планирования, в которой предусмотрена возможность тесной интеграции с другими продуктами Novell. В частности, благодаря объединению GroupWise с пакетами InForms и SoftSolutions можно получить среду для создания и заполнения электронных форм, а также для управления документооборотом. В ближайшем будущем возможности GroupWise еще расширятся. Пакет получит название - GroupWise XTD и будет иметь расширенные функции совместной работы с файлами и управления почтовыми отделениями. При этом пакет XTD совместим не только с существующей версией GroupWise, но и со всеми предыдущими.

Все три продукта - Notes, Exchange и GroupWise - не только включают собственное клиентское ПО, но и совместимы с другими клиентскими приложениями электронной почты. При тестировании главное внимание мы уделяли работе серверной части продуктов. Тем не менее все изделия имеют надежную клиентскую часть, которая обеспечивает возможность обработки списков рассылки, присоединенных файлов и правил управления сообщениями.

Несмотря на то что каждому серверному продукту соответствует собственное клиентское ПО, в реальной жизни сетевым администраторам приходится объединять серверы электронной почты разных производителей, например Notes и Exchange Server. Обычно эта проблема решается с помощью шлюзового ПО, предусмотренного в этих серверах. Связь с коммерческими службами электронной почты, такими как MCI Mail, America Online и CompuServe (а также и с Интернет), тоже может быть реализована с помощью шлюзов или средств независимых поставщиков. Подключение к Интернет может потребоваться не только для использования электронной почты, но и для доступа к группам новостей и взаимодействия с системой Интернет. Например, продукт InterNotes фирмы Lotus позволяет преобразовывать документы базы данных Notes в формат HTML, применяемый в Интернет.

1.4.3.2. Расширенные функциональные возможности продуктов

Платформы, предназначенные для работы в масштабе предприятия, обычно устанавливаются на множестве серверов и узлов. Это вызывает огромное количество проблем, которые отсутствуют, когда система электронной почты работает на одном- единственном узле, так как в этом случае не нужно заботиться о защите информации, управлении документами, синхронизации передачи сообщений и тиражировании данных. Особенно важно определить дополнительные меры безопасности для защиты бизнес-приложений, такие как шифрование данных, электронная подпись и управление документами с применением цифровых кодов.

Важнейшей характеристикой серверов является степень их готовности, под которой подразумевается минимизация времени простоя оборудования. Для этого нужно предусмотреть избыточные средства связи между серверами, а также объединить почтовые серверы с системами резервного копирования. Желательно, чтобы операции резервного копирования и восстановления данных не влияли на функционирование системы в целом, однако они должны охватывать всю информацию, относящуюся к серверу, включая данные системы безопасности.

И наконец, несмотря на то что функции настройки и мониторинга редко встречаются в небольших системах электронной почты, они необходимы для более крупных сетевых продуктов. Хотя при выборе системы электронной почты вы, скорее всего, не будете исходить из числа сообщений, передаваемых в минуту, эта информация может пригодиться для определения узких мест и оптимизации производительности сервера после инсталляции.

Сравнение всех функций и возможностей Notes, Exchange Server и GroupWise - непростая задача. И хотя эти продукты во многом схожи, каждый из них обладает огромным количеством уникальных особенностей. Чтобы подобрать подходящую систему, прежде всего определите, какой из предлагаемых наборов функций для вас более важен. Так, для автоматизации деловых процедур база данных Notes подходит больше, чем средства обработки форм, реализованные в Exchange Server.

С другой стороны, если среди ваших разработчиков немало программистов на языке Visual Basic, вам лучше использовать систему подготовки форм Exchange Server, интегрированную с клиентской частью Exchange, входящей в Windows 95, чем средства для работы с формами пакета GroupWise. Но если решающим фактором является возможность интеграции с NDS (службой каталогов NetWare), присмотритесь к GroupWise.

В любом случае не следует выбирать продукт исходя только из одной его функции или производительности. Напротив, необходимо тщательно взвесить все функции и особенности вашей сети. Если вы собираетесь заменить один сервер электронной почты на другой, воспользуйтесь средствами перехода. Одни системы автоматически заменяют клиентские части системы электронной почты при смене серверной, другие же используют службу каталогов, например NDS компании Novell.

1.4.3.3. Notes фирмы Lotus

По своим возможностям Notes, несомненно, превосходит простой сервер электронной почты для сети предприятия. Этот пакет стал своего рода стандартом, в сравнении с которым определяется качество многих средств для поддержки рабочих групп. Он содержит не только сервер базы данных и сервер управления документацией, но и средства разработки программ и автоматизации деловых процедур, которые являются предметом зависти конкурентов фирмы Lotus, так как им трудно предложить изделия, соперничающие с функциями, предоставляемыми Notes. Если же к этим достоинствам приплюсовать огромное количество приложений независимых разработчиков, а также немалое число платформ (как клиентских, так и серверных), которые поддерживает этот продукт, то он будет выглядеть весьма привлекательно.

Пакет Notes благодаря широким функциональным возможностям и увеличению числа операционных сред, в которых пакет работает наиболее эффективно, медленно, но верно завоевывает признание. Мы рассмотрели только основные возможности Notes, но и они дают представление о мощи этого пакета. Применять Notes лишь в качестве сервера электронной почты нецелесообразно: это все равно что использовать авианосец для запуска бумажных самолетиков. Продукт подходит для крупных компаний, где для работы необходимо использовать несколько серверов Notes. Но один сервер Notes подходит для небольших и средних предприятий, где не более 200 пользователей. Можно даже применять Notes на автономной рабочей станции, однако эта конфигурация обычно служит для работы с мобильными или удаленными пользователями.

Пакет поддерживает архитектуру клиент/сервер, но при этом больше напоминает сервер базы данных, чем просто сервер электронной почты. Клиентская часть состоит из набора папок, обеспечивающих доступ к базам данных, управляемым сервером Notes. В системе Notes записи базы данных называются документами. Документ Notes допускает любое количество полей и присоединенных файлов, которые могут представлять собой документы, созданные другими приложениями. Кроме того, документы Notes могут включать в себя объекты OLE и ссылки на другие документы Notes. Не напоминает ли это вам документы на языке HTML, используемом в гипертекстовой системе World Wide Web? Однако Notes предлагает значительно больше, так как позволяет подключаться к Интернет. Но эти возможности мы обсудим ниже.

Notes обладает расширенными средствами программирования, которые позволяют выполнять обработку простых формул и правил, а также поддерживает собственный язык программирования LotusScript, обеспечивающий доступ к другим серверам баз данных с помощью интерфейса ODBC (Open Database Connectivity). Если вы имеете опыт в создании электронных таблиц, приложений Basic и других программ, то вам понравится LotusScript. Если же вас не удовлетворяют возможности LotusScript, обратитесь с помощью интерфейса прикладного программирования Notes к другим инструментальным средствам. Notes обеспечивает поддержку SmartButtons, а также работу с формами и программами-агентами. Последние могут применяться для реагирования на различные события, такие как заранее предусмотренные ситуации или поступление почтовых сообщений.

Поскольку Notes рассматривает сообщение электронной почты в качестве документа, реализуется главное преимущество этого продукта: все его функции в одинаковой степени применимы как для почтовых сообщений, так и для любых других записей базы данных. Например, перемещение документа электронной почты из папки входного почтового ящика в другую папку может выполнять программа-агент, которая проверяет поступление новых документов и начинает их обработку под управлением специализированного приложения Notes. Такой согласованный метод обработки документов позволяет интегрировать электронную почту с приложениями Notes.

Расписания, списки срочных дел и другие приложения рабочих групп также укладываются в схему, которая применяется в Notes для работы с документами. Все эти приложения могут создаваться на основе базы данных документов Notes. Кроме того, клиентская часть Notes поставляется с множеством таких приложений.

На различных платформах клиентская часть Notes поддерживает соответствующий графический интерфейс, который внешне несколько отличается от собственного интерфейса операционной среды. Например, при работе под управлением Windows серверу Notes требуется двойное нажатие на клавишу мыши для перехода на другой документ, хотя для большинства браузеров веб достаточно одного нажатия. Но многие пользователи Notes не обращают внимания на такие мелочи и применяют для работы с веб исключительно этот продукт.

Серверы Notes функционируют на разнообразных платформах - от IBM OS/2 до Novell NLM, серверов Windows NT и Unix. Пакет проверялся на платформе Windows NT. Ранее мы работали с Notes в среде OS/2 и NLM 4.0 для NetWare. Различий между ними оказалось гораздо меньше, чем можно было ожидать.

Интерфейс сервера Notes разделен на две части: одна поддерживает текстовый режим для клиента Notes, другая - графический. Большинство функций управления сервером исполняется через клиентскую часть Notes, которую можно установить на любой станции сети, причем один клиент способен управлять множеством серверов Notes. Для защиты средств управления применяются те же самые средства, что и для сервера базы данных Notes. Преимуществом текстового режима является то, что интерфейс не зависит от операционной платформы Notes и одинаков для NetWare, OS/2, Windows NT и Unix-систем.

Пакет Notes прославился своими возможностями тиражирования и синхронизации баз данных. Например, содержимое папки можно тиражировать во множество серверных или клиентских баз данных, что позволяет мобильным пользователям брать БД Notes с собой в дорогу. Удаленных пользователей Notes, применяющих различные платформы, особенно обрадует версия 4.0, поддерживающая режим транзитной передачи данных, при котором серверы Notes передают запрос друг другу до тех пор, пока он не достигнет нужного узла. При этом удаленный пользователь может не беспокоиться об особенностях сети, к которой он обращается, а кроме того, его изолированность от сети обеспечивает высокую степень защиты данных.

Для каждой базы данных в пакете Notes предусмотрены функции защиты, а также шифрование и поддержка цифрового ключа для каждого поля БД. Так, например, персональная карточка служащего с зашифрованным полем оклада может быть доступна многим пользователям, но только те из них, кто имеет специальное разрешение и нужный ключ, смогут увидеть содержимое этого поля.

Notes поддерживает различные сетевые шлюзы, в том числе и для подключения к Интернет. Шлюзовое ПО для доступа к другим почтовым службам работает так же, как аналогичные средства других тестируемых продуктов. При этом поддерживаются такие стандарты, как SMTP (Simple Mail Transfer Protocol) и Х.400, а также факсимильная связь. Для работы с Интернет служит дополнительный комплект InterNotes, содержащий модули InterNotes News, веб Navigator и веб Publisher. При подключении сервера Notes к Интернет модуль InterNotes News распределяет группы новостей Интернет по папкам Notes. веб Navigator обеспечивает доступ к гипертекстовой системе WWW, а веб Publisher позволяет преобразовать документы Notes в формат HTML. Чтобы распространять документы через Интернет или сеть Интранет, помимо веб Publisher следует использовать и Web-сервер.

Если у нас и есть пожелания к расширению Notes, то они касаются дополнительных средств для измерения производительности системы. Хотя в документации имеются некоторые рекомендации, а по базам данных собираются статистические сведения, процедура оптимизации сервера Notes не рассчитана на среднего пользователя. Для копирования баз данных Notes можно применять обычные программы резервного копирования, но выполнение процедур резервного копирования и восстановления данных должно быть спланировано так, чтобы в это время файлы БД не использовались.

Управление множеством серверов Notes - непростая задача. Обычно эти серверы ориентированы на выполнение определенных функций, таких как поддержка базы данных, электронной почты, удаленного доступа, шлюза и др. Кроме того, в крупных сетях Notes могут присутствовать концентраторы, а также транзитные серверы передачи информации для связи клиентов с несколькими серверами Notes. Концентраторы позволяют объединить серверы друг с другом, давая возможность осуществлять тиражирование данных и обмен документами между этими серверами.

Хотя собрать из различных продуктов систему, выполняющую функции Notes, теоретически возможно, ее внедрение наверняка превратится в кошмар. Notes предоставляет так много хорошо интегрированных друг с другом средств, что было бы трудно оправдать временные затраты на то, чтобы самостоятельно добиться такого уровня интеграции.

1.4.3.4. Exchange Server компании Microsoft

Exchange Server поддерживает только серверную ОС Windows NT Server 3.51 (или более старшую версию), что ограничивает сферу его применения. Но есть у него и существенное преимущество - возможность работы на всех аппаратных платформах, поддерживаемых системой Windows NT, включая микропроцессоры i486 и Pentium фирмы Intel и Alpha корпорации Digital Equipment. Перечень клиентских платформ более широк: в него входят DOS, все версии Windows и Macintosh. Продукт совместим с сетевыми протоколами TCP/IP, NetBEUI и NetWare SPX (Sequenced Packet Exchange).

Exchange Server был разработан компанией Microsoft взамен почтовой системы Mail, основанной на совместном использовании файлов. Новый продукт поддерживает более надежный интерфейс для архитектуры клиент/сервер на базе MAPI, который реализован и в последней клиентской версии Exchange, входящей в базовый комплект Windows 95. Однако вместе с Exchange Server поставляется новая клиентская версия, обеспечивающая доступ ко всем функциям сервера. Фактически любое клиентское ПО, совместимое с МАРI, может применять Exchange Server для работы с такими приложениями, поддерживающими электронную почту, как Excel и Word.

Для удаленного доступа к Exchange Server служит утилита RAS (Remote Access Server) системы Windows NT, используемая для модемной связи и подключения через Интернет. Правда, в последнем случае поддерживается только соединение машины- клиента со службами Exchange Server, а Remote Access Server дает возможность удаленной рабочей станции получить доступ к любой службе Windows NT и даже обеспечивает совместное использование дисков и принтеров. Кроме того, Exchange Server поддерживает автономные адресные книги удаленных пользователей, которые содержат подмножества адресов всех пользователей данного сервера.

В адресные книги этого пакета могут входить записи в различных форматах, например в принятых в сетях X.400 или Интернет. Для передачи почтовых сообщений по таким адресам Exchange Server использует шлюзы.

Клиентская часть Exchange поддерживает стандарт OLE 2.0 в почтовых сообщениях. Кроме того, имеются специальные объекты OLE для доступа к почтовым службам. Технология OLE Automation позволяет приложениям, написанным на языке VBA (Visual Basic for Applications) и работающим в среде Excel, пересылать диаграммы и графики Excel средствами электронной почты. Это может пригодиться и при составлении расписаний совещаний или встреч.

Общедоступные папки обеспечивают поддержку телеконференций, аналогичных тем, которые применяются во многих коммерческих информационных службах, таких как CompuServe. Хотя папки содержат только сообщения, поддержка присоединенных файлов позволяет хранить в папках документы любого типа. В папках поддерживаются связанные сообщения, что весьма удобно для отслеживания источника общедоступных аннотаций или при обмене частными сообщениями.

Несмотря на то что клиентская часть Exchange не выполняет всех функций браузера веб, она распознает адреса URL в почтовых сообщениях и может запустить браузер веб. Это, например, позволяет сначала передать адрес Web-страницы в составе сообщения, а затем с помощью браузера отобразить эту страницу на экране.

Для мобильных пользователей предусмотрен широкий набор средств для загрузки сообщений, включая фильтрацию сообщений по размеру или по адресу отправителя, возможность загрузить только краткое содержание сообщения, а полный текст считать позднее. Кроме того, Exchange Server поддерживает тиражирование и синхронизацию автономных папок, которые хранятся на локальных дисках, в частности на переносном ПК. С помощью процедуры синхронизации можно автоматически обновлять папки и приводить их в соответствие с содержимым папок, записанных на Exchange Server.

Продукт поддерживает более 22 тыс. пользователей, используя для этого несколько серверов, организованных в виде двухуровневой иерархической структуры, когда главный сервер обеспечивает управление связями с серверами нижнего уровня. Управление всеми серверами Exchange Server может осуществляться с одной рабочей станции. За счет интеграции архитектур Exchange Server и сервера Windows NT доменная система защиты системы NT позволяет управлять администрированием серверов. Интеграция Exchange Server и Windows NT распространяется и на другие средства. Регистрация событий, мониторинг и даже контроль производительности объединены с аналогичными программами NT. Особенно важно то, что все сведения об Exchange Server доступны этим средствам NT. Поэтому данные, относящиеся к Exchange Server, отображаются на экране вместе с соответствующей информацией по Windows NT Server, что значительно облегчает контроль за взаимодействием Exchange Server и Windows NT Server.

В состав Exchange Server входит программа моделирования нагрузки, которая служит для оценки производительности определенной конфигурации системы без подключения к серверу большого числа рабочих станций. Эта же утилита может применяться вместе со средствами мониторинга событий и контроля производительности. Функции резервного копирования пакета Exchange Server позволяют осуществлять эту процедуру без отключения системы. Стандартные программы резервного копирования, используемые многими средствами электронной почты предыдущего поколения, требовали отключения почтового сервера. Процедура резервного копирования Exchange Server допускает полное и частичное копирование, а также создание резервных копий только для измененных данных аналогично обычным утилитам этого класса. Кроме того, мы протестировали ряд программ резервного копирования независимых разработчиков, которые могут быть интегрированы в Exchange Server. Необходимо отметить, что многие из них обладают более широкими возможностями, чем утилита, созданная Microsoft: в частности, они позволяют осуществлять дистанционное резервное копирование и предоставляют более совершенные средства планирования этой процедуры.

Защита доступа к данным в Exchange Server обеспечивается стандартными способами, наибольший интерес из которых представляют шифрование и электронная подпись. С помощью Exchange Server можно шифровать сообщения и дополнять их цифровыми подписями. Кроме того, он дает возможность использовать специальные средства управления цифровыми ключами, обеспечивающими распределение по рабочим станциям открытых ключей шифрования и даже отмену ключей, применяемых пользователями.

"Экспертные подсказки" (wizard) значительно упрощают установку Exchange Server. Сложнее оказалось реализовать процедуры перехода с других почтовых систем или добавления почтовых ящиков пользователей, а также конфигурирование этого сервера для совместной работы с другими серверами локальной или глобальной сети. Средства перехода, входящие в базовый комплект Exchange Server, позволяют переносить из других почтовых служб типа MS Mail только списки пользователей, но они не поддерживают перенос сообщений или присоединенных файлов. Вместо полного переноса почтовых ящиков пользователей используется шлюз, который обеспечит связь существующего почтового отделения с сервером Exchange.

Средства планирования и составления расписаний также интегрированы в Exchange Server. Помимо этого, пакет совместим с другим продуктом Microsoft - Schedule+. С помощью почтовых сообщений можно проверять время совещаний, а Schedule+ будет поддерживать ваш план работы в соответствии с этими данными.

В комплект поставки Exchange Server входят средства разработки, управления и распространения форм, предназначенных для работы с автономными приложениями на базе форм или для объединения с сообщениями и папками. Поддержка стандарта MAPI дает возможность продуктам независимых разработчиков взаимодействовать с Exchange Server.

Средство разработки форм пакета Exchange Server, созданное на базе Visual Basic (VB) 4.0, использует графический интерфейс, применяемый в VB. Этот "дизайнер форм" также поддерживает код формы и диалоговые окна с закладками. Опытные программисты могут настраивать это приложение в соответствии со своими требованиями, однако можно строить сложные приложения и с минимальным количеством программных кодов или вообще без ручного программирования. Хотя Exchange Server не имеет собственной базы данных (как, например, Notes), эта система включает мощные средства для работы с папками и для передачи почтовых сообщений.

Средства поддержки множества серверов выполняют обмен сообщениями электронной почты, тиражирование и синхронизацию папок, а также распространение форм. Тиражирование папок обмена можно производить либо после каждого внесения изменений, либо в соответствии с предварительно установленным графиком. В Exchange Server предусмотрены средства разрешения конфликтов при тиражировании, которые следят за внесением изменений на различных серверах. Обычно при возникновении конфликта с какой-либо папкой в нее добавляется сообщение, указывающее тип ошибки. Для передачи этих сообщений в средства регулирования работы с папками можно использовать набор правил.

Exchange Server поддерживает работу с Интернет. Сообщения групп новостей считываются из Интернет и хранятся в папках, которые, в свою очередь, могут тиражироваться по всему домену Exchange. Пока этот продукт не поддерживает прямого доступа к Web-серверу, однако вскоре Web-сервер компании Microsoft и соответствующие средства поддержки будут интегрированы в Windows NT. Прямой доступ к Exchange Server через Интернет особенно удобен для удаленных пользователей, поскольку средства подключения к Интернет сейчас широко доступны.

1.4.3.5 Продукт GroupWise компании Novell

Этот продукт представляет собой оригинальное сочетание электронной почты на базе технологии совместного использования файлов и системы календарного планирования, поддерживающей архитектуру клиент/сервер для обмена почтовыми сообщениями между доменами. В последнюю версию GroupWise - XTD - не только включены все возможности этого продукта, они там значительно расширены, особенно поддержка интерфейсов прикладного программирования. XTD полностью совместима с предыдущими версиями и дополнительно предоставит пользователям электронную почту и функции планирования в среде клиент/сервер.

Хотя пакет GroupWise обеспечивает передачу почтовых сообщений и календарное планирование, он состоит из такого числа отдельных программ, что проверка всех возможностей продукта весьма затруднена. Например, модуль SoftSolutions, который является средством управления документами, использует для работы с Windows- приложениями стандарт ODMA (Open Document Management Architecture). Найти нужный документ можно по ключевым словам. Кроме того, SoftSolutions обеспечивает контроль версий и может использоваться при совместной работе с документами. Как и подсистема передачи сообщений пакета GroupWise, модуль SoftSolutions использует архитектуру клиент/сервер, но эти продукты абсолютно независимы друг от друга.

Модуль InForms поддерживает подготовку форм и автоматизацию деловых процедур, применяется для управления базой данных и может работать как со службой электронной почты пакета GroupWise, так и с другими почтовыми системами, например с Notes фирмы Lotus.

Стандартные средства администрирования пакета GroupWise, как и другие аналогичные изделия Novell, ориентированы только на текстовое представление информации на экране. В GroupWise также входит продукт NetWare Admin Integration Snap-in for GroupWise, который позволяет осуществлять системное администрирование для серверов NetWare 4.x и GroupWise с одной консоли. Благодаря использованию службы каталогов NDS он особенно эффективен в крупных сетях с большим количеством серверов.

Если в сети имеется одно почтовое отделение, клиентские приложения GroupWise пользуются только режимом совместного использования файлов. Если почтовых отделений в сети больше одного, целесообразно представить GroupWise в виде загружаемых модулей NLM. В этом случае применяются серверы четырех типов - сообщений, администрирования, почтового отделения и синхронизации базы данных для сетевых ресурсов.

Сервер сообщений распределяет сообщения по почтовым отделениям и доменам (домен - базовая административная единица, состоящая из почтовых отделений и шлюзов, непосредственно обслуживаемых сервером сообщений). Он применяется в сетях, содержащих множество почтовых отделений, доменов и шлюзов или поддерживающих прямое подключение удаленных почтовых служб. Сервер администрирования получает управляющие сообщения и использует эту информацию для обновления баз данных доменов и почтовых отделений, которые он обслуживает. Сервер почтового отделения распределяет сообщения по почтовым ящикам своих отделений. Клиент почтовой службы может передать сообщение только через собственное почтовое отделение. Сервер синхронизации базы данных для сетевых ресурсов обновляет перечень пользователей GroupWise, когда в БД сетевых ресурсов вносятся изменения.

Шлюзы - это тоже загружаемые модули NLM, которые взаимодействуют с серверными NLM-модулями GroupWise. Некоторые из шлюзов поддерживают доступ к другим почтовым системам, например к использующим протоколы Х.400 и SMTP, а также к системам на базе совместной работы с файлами, в частности к службе Message Handling Service компании Novell. Адресные книги могут содержать адреса, передаваемые через эти шлюзы. Удаленный доступ через модемную связь тоже обеспечивается с помощью шлюзов.

Так как базы данных GroupWise хранятся как обычные файлы, их резервное копирование выполняют соответствующие приложения NetWare. К сожалению, при восстановлении БД необходимо временно отключить связанные с ней серверы.

Пакет GroupWise, в отличие от Notes и Exchange Server, хотя и обеспечивает передачу почты и составление расписаний, но не поддерживает совместно используемой базы данных и общих папок обмена. Поэтому в продукте GroupWise не применяются службы тиражирования и синхронизации данных. Что касается автоматизации деловых процедур, то соответствующие клиентские средства отличаются более широкими функциональными возможностями, чем серверные.

Клиентская часть GroupWise обеспечивает доступ к электронной почте, составлению планов и расписаний, несмотря на то что возможности клиентских средств по оформлению текста почтовых сообщений весьма ограниченны; поддерживаются такие атрибуты, как выделенные символы и курсив. К сообщению можно присоединять любые файлы и объекты OLE. Кроме того, личные сообщения можно помечать, но система защиты не поддерживает ни шифрования, ни цифровых подписей.

GroupWise обеспечивает доступ к Интернет только через шлюзовое ПО в стандарте SNMP (Simple Network Management Protocol). Поэтому единственным средством доступа к группам новостей и системе веб являются продукты независимых производителей.

Хотя GroupWise отстает от Notes и Exchange Server по многим показателям, этот пакет обеспечивает все функции системы электронной почты, поддерживает календарное планирование и управление документами, а также позволяет работать с формами и базами данных на целом ряде платформ, и прежде всего на NetWare.

По результатам обследования Минторга РФ, как объекта автоматизации получены следующие выводы.

Номинально достаточно обширная компьютерная база министерства незначительно повышает эффективность труда сотрудников министерства по следующим причинам:

* большинство компьютеров не пригодно для работы с современными прикладными программами;
* компьютеры используются автономно;
* попытки создания подсистем (ДФБУ, ДГРВЭД, УКГС) ведутся без ориентации на единую системную идеологию (кусочно-лоскутная автоматизация);
* информационные ресурсы министерства незначительны, доступны ограниченному кругу лиц;
* современные информационные технологии, телекоммуникационные сети и мировые информационные ресурсы для обеспечения деятельности министерства, практически, не используются.

Проблема информатизации Минторга может быть решена путем создания Автоматизированной Информационной системы Министерства Торговли РФ. В качестве одной из ее подсистем может выступать система документооборота, атоматизирующая основные процессы по подготовке, обработке, хранению, поиску и обмену документами, циркулирующими в Министерстве Торговли.

В качестве программной платформы для реализации разработки автоматизированной системы документооборота Минторга РФ необходимо использовать пакет Microsoft Exchange Server, как наиболее удовлетворяющий требованиям заказчика и разработчика по своим функциональным возможностям.

В качестве средств разработки необходимо использование Borland C++ Builder 3.0 Client\Server, Microsoft Visual Basic for Applications.

ГЛАВА 2. МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СИСТЕМЫ ДОКУМЕНТООБОРОТА МИНТОРГА РФ. РЕШЕНИЕ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Постановка задачи и её спецификация

2.1.1. Понятие информационной безопасности применительно к системе документооборота Минторга РФ

Под информационной безопасностью в общем случае понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и/или пользователям информации АС и поддерживающей систему инфраструктуре.

Информационная безопасность современных автоматизированных систем согласно общепринятому подходу включает три взаимоувязанных аспекта:

* целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения;
* конфиденциальность – защита от несанкционированного ознакомления с информацией;
* доступность – возможность за приемлемое время получить требуемую информацию, информационную услугу.

Для органов государственной власти первые два аспекта контролируются соответствующими федеральными структурами: вопросы защиты от НСД (то есть обеспечение конфиденциальности и целостности информации) курирует Гостехкомиссия России, криптографические средства (а это опять же связано с обеспечением конфиденциальности и целостности) – Федеральное агентство правительственной связи и информации при президенте России ФАПСИ. Доступности, как важному аспекту информационной безопасности, должного внимания пока, к сожалению, не уделяется. Между тем, нормальная работа любой автоматизированной системы класса системы документооборота Минторга РФ (СД МТ) базируется на получении определенной информации, определенных информационных услуг (сервиса). Если по тем или иным причинам своевременное получение информации и услуг пользователями становится невозможным, то это наносит ущерб всем субъектам информационных отношений и может оказаться вообще неприемлемым. Наиболее вероятными причинами нарушения доступности информации в министерстве можно считать следующие:

* отнесение к информации ограниченного доступа информационных ресурсов, которые в соответствии с законодательством РФ являются открытыми;
* локализация информационных ресурсов внутри отдельных подразделений из-за нежелания руководства этих подразделений предоставлять информацию сотрудникам других подразделений Минторга, даже в ущерб общему делу;
* увеличение времени отклика системы в связи с недостаточной производительностью программно-технических средств или из-за ненадежности программ или технических средств.

Вопросы информационной безопасности в СД МТ следует решать на основе комплексного учета всех трех названных аспектов. При этом необходимо иметь в виду два существенных фактора:

* действие аспектов целостности и конфиденциальности, с одной стороны, и доступности, с другой стороны, обычно противоположно. Повышение уровня целостности и конфиденциальности практически всегда ведет к увеличению времени реакции системы, дополнительным задержкам информации, то есть к ухудшению доступности. Можно сделать систему, хорошо защищенную от НСД, но совершенно непригодную для работы в режиме, близком к реальному масштабу времени;
* повышение уровня целостности и конфиденциальности, как правило, сопряжено с резким ростом стоимости системы, а это может оказаться практически неприемлемым для СД.

Отсюда вытекает необходимость классифицирования информации, циркулирующей в СД МТ по критерию открытости. Задача описания информационных ресурсов (ИР) по аспекту открытости распадается на 2 части: точности и правомерности такой классификации.

Вопрос точности заключается в том, что не все категории закрытости и конфиденциальности ИР определены в действующем законодательстве. Имеется определенная ясность с секретной ин­формацией (к ней относятИР**,** содержащие сведения, отнесенные к государственной тайне), поскольку имеется соответствующее законодательство. Более или менее точно в существующих зако­нопроектах, а также в некоторых подзаконных актах определены понятия коммерческой тайны и персональных данных. Кроме того, в данном случае имеются международные нормативные акты и зарубежный опыт их применения.

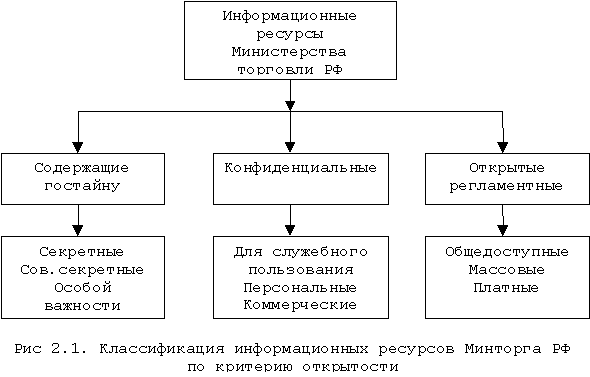
Что же касается так называемой "служебной тайны" (применяются грифы "для служебного пользования" и "не для печати"), то эта категория не имеет законодательной базы вовсе. В то же время к ней относится значительная доля ИР министерства.

Таким образом, описание ИР по аспекту открытости может во многих случаях вызвать неясности и разночтения.

Проведенный анализ российского законодательства, порядка накопления и обработки документированной информации с ограниченным доступом, правил ее защиты и порядка доступа к ней вМинторге РФ**,** позволяет предложить следующую классификацию информационных ресурсов министерства по критерию открытости (рисунок 2.1.):

Документы (или их проекты), разрабатываемые в Министерстве в служебном порядке (служебные документы) могут быть:

* конфиденциальными(документы, содержащие информацию, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и или по решению лиц, уполномоченных Министром торговли)**;**
* открытыми регламентными документами(документы, не отнесенные к категории ограниченного доступа, но для распространения которых требуется разрешение соответствующего должностного лица).



В результате разрешения соответствующего должностного лица регламентные документы министерства могут стать либо общедоступными, либо платными, либо массовыми. Не обязательно получать разрешение на каждый конкретный документ, поскольку на некоторые группы документов в Минторге может быть установлен регламент, позволяющий без обращения к должностному лицу относить документы к той или иной категории открытости. Служебные документы ограниченного распространения должны иметь пометку "Для служебного пользования" или "Коммерческий". Необходимость проставления пометок на документах и изданиях, содержащих служебную информацию ограниченного распространения, определяется исполнителем и должностным лицом, подписывающим, или утверждающим документ.

Доступ к открытым информационным ресурсам законодательством РФ не ограничен. Однако часть из них (открытые платные ИР), в связи с необходимостью поддержания этих ресурсов в актуальном состоянии, затратами, связанными с их хранением и распространением и т.д. предоставляются пользователям за плату.

Таким образом, для решения поставленной задачи необходимо создать концепцию безопасности СД МТ, на основе которой будет создана система защиты информации (СЗИ), реализующая ряд программных и организационных мер по предотвращению несанкционированных действий по уничтожению, искажению, подделке, хищению или блокированию информации, сохранению коммерческой и государственной тайны, обеспечению конфиденциальности документированной информации. Степень защиты определяется требованиями заказчика по уровню конфиденциальности данных циркулирующих в системе.

Реализация СЗИ СД МТ подразумевает под собой использование как стандартных средств защиты информации, предоставляемых программным обеспечением, входящим в состав ее компонент, так и создание специального программного обеспечения, которое призвано дополнить стандартные возможности и увеличить степень защиты информации. Кроме того СЗИ может включать в себя ряд административно-организационных мер.

2.1.2. Модель нарушителя в СД МТ

Безусловно, при построении защищенного компьютерного комплекса, значительные усилия приходится направлять на создание средств защиты от НСД. Поскольку невозможно разрабатывать эти средства без определения того, от кого обеспечивается защита, вводится понятие модели нарушителя – “абстрактное (неформализованное) описание нарушителя. Перечень правил, определяющих ограничения, исходя из которых анализируются возможные действия нарушителя”.

В разрабатываемой системе угрозы разрушения информационных массивов или несанкционированного доступа к данным могут возникнуть из двух источников внешнего, то есть со стороны пользователя СД МТ, и внутреннего, то есть исходящие от злоумышленника, пытающегося проникнуть в систему из вне. Исходя из этого, представляется целесообразным рассмотрение двух типов нарушителей, обладающих различными характеристиками, которые за счет своих умышленных или неумышленных действия могут нанести урон целостности системы или получить доступ к конфиденциальным данным.

Итак предполагается, что внутренний пользователь:

* хорошо разбирается во всех документированных возможностях ОС и пользовательского ПО и обладает программистскими навыками;
* не знает об недокументированных особенностях функционирования ОС;
* не знает об возможных программных закладках, оставленных разработчиками в пользовательском и системном ПО;
* не обладает спецсредствами для фиксации электромагнитного излучения, создаваемого компьютерами других пользователей, а также не обладает возможностью встраивать физические закладки в рабочие места других пользователей;
* не может узнать пароль администратора системы.

В свою очередь считается, что внешний нарушитель:

* не обладает спецсредствами для улавливания электромагнитного излучения, создаваемого СВТ работающих в составе СД МТ, он также не обладает оптическими и звуковыми приборами, позволяющими получить несанкционированный доступ к системе;
* лишен возможности проводить активные мероприятия по установке подслушивающих устройств и камер слежения;
* является опытным программистом хорошо знакомым с сетевыми протоколами и недокументированными возможностями ОС, способен к написанию компьютерных вирусов типа “Троянский конь”, макровирусов.

Данные допущения выработаны на основе обследования объекта автоматизации, а также требований, предъявляемых заказчиком к системе СД МТ. Именно исходя из них, необходимо определять комплекс мер по защите информации, на основе которых будет создаваться СЗИ.

2.1.3. Выбор классов защищенности информации от НСД

Согласно руководящему документу “Автоматизированные системы защита от несанкционированного доступа к информации (классификация автоматизированных систем и требования по защите информации)” Гостехкомиссии России устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

* наличие в АС информации различного уровня конфиденциальности;
* уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
* режим обработки данных в АС: коллективный или индивидуальный.

Разбитие классов на группы производится следующим образом. Третья группа классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса 3Б и 3А. Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса 2Б и 2А. Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов 1Д, 1Г, 1В, 1Б и 1А.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД, условно состоящей из следующих четырех подсистем:

* управления доступом;
* регистрации и учета;
* криптографической;
* обеспечения целостности.

Состав данных подсистем приведен на рисунке 2.2.

Проведенный анализ информации, обрабатываемой в СД МТ, а также возможных угроз безопасности системы и описанная модель нарушителя, позволяют выбрать класс 1В по защите от НСД к информации, согласно РД Гостехкомиссии России, поскольку:

* СД МТ – это иерархическая, многопользовательская система, в которой одновременно обрабатывается и хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации;
* информация циркулирующая в СД МТ не относится к категории закрытой, поскольку рассматриваемая система оперирует с информацией общедоступной и конфиденциальной (для служебного пользования).

Согласно упомянутому РД Гостехкомиссии России, для разработки АС подлежащей защите от НСД по классу 1В необходимо использовать сертифицированные СВТ не ниже 4 класса.

Классификация СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований устанавливается в другом РД Гостехкомиссии России – "Средства вычислительной техники, защита от несанкционированного доступа к информации, показатели защищенности от НСД к информации". Под СВТ в данном документе понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

*Таблица. 2.1.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Наименование** | **Класс защищенности показателя** | | | | | |
| **6** | **5** | **4** | **3** | **2** | **1** |
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |
| Очистка памяти | - | + | + | + | = | = |
| Изоляция модулей | - | - | + | = | + | = |
| Маркировка документов | - | - | + | = | = | = |
| Защита ввода и вывода на отчуждаемый физический носитель информации | - | - | + | = | = | = |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Идентификация и аутентификация | + | = | + | = | = | = |
| Гарантии проектирования | - | + | + | + | + | + |
| Регистрация | - | + | + | + | = | = |
| Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |
| Надежное восстановление | - | - | - | + | = | = |
| Целостность КСЗ | - | + | + | + | = | = |
| Контроль модификации | - | - | - | - | + | = |
| Контроль дистрибуции | - | - | - | - | + | = |
| Гарантии архитектуры | - | - | - | - | - | + |
| Тестирование | + | + | + | + | + | = |
| Руководство пользователя | + | = | = | = | = | = |
| Руководство по КСЗ | + | + | = | + | + | = |
| Тестовая документация | + | + | + | + | + | = |
| Конструкторская (проектная) документация | + | + | + | + | + | + |

Данный РД предусматривает семь классов защищенности СВТ от НСД. Перечень показателей по классам защищенности СВТ приведен в таблице 2.1. Приведенные в таблице наборы требований к показателям каждого класса являются минимально необходимыми. Используемые обозначения: "-" нет требований к данному классу; "+" новые или дополнительные требования, "=" требования совпадают с требованиями к СВТ предыдущего класса.

Более подробно остановимся на показателях соответствующих четвертому классу.

*Дискреционный принцип контроля доступа.* КСЗ должен контролировать доступ наименованных субъектов к наименованным объектам. Для каждой пары субъект-объект в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ. КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД. Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов). Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов. Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности. Кроме того, КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД). Под "явными" здесь подразумеваются действия, осуществляемые с использованием системных средств системных макрокоманд, инструкций языков высокого уровня и т.д., а под "скрытыми" иные действия, в том числе с использованием собственных программ работы с устройствами. Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

*Мандатный принцип контроля доступа*. Для реализации этого принципа каждому субъекту и каждому объекту должны сопоставляться классификационные метки, отражающие место данного субъекта (объекта) в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа. КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки субъектов и объектов должны точно соответствовать внутренним меткам (внутри КСЗ). КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов: субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта; субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта. Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами. В СВТ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

*Очистка памяти.* При первоначальном назначении или при перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

*Изоляция модулей*. При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса, от программных модулей других процессов, т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.

*Маркировка документов.* При выводе защищаемой информации на документ в начале и конце проставляют штамп N 1 и заполняют его реквизиты в соответствии с Инструкцией N 0126-87.

*Защита ввода и вывода на отчуждаемый физический носитель информации.* КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные ("помеченные"). При вводе с "помеченного" устройства (вывода на "помеченное" устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с "помеченным" каналом связи. Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем КСЗ.

*Сопоставление пользователя с устройством*. КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки). Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

*Идентификация и аутентификация*. КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификатора субъекта осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать входу в СВТ неидентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась. КСЗ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

*Гарантии проектирования*. Проектирование КСЗ должно начинаться с построения модели защиты, включающей в себя: непротиворечивые ПРД; непротиворечивые правила изменения ПРД; правила работы с устройствами ввода и вывода информации и каналами связи.

*Регистрация*. КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

* использование идентификационного и аутентификационного механизма;
* запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
* создание и уничтожение объекта; действия по изменению ПРД.
* Для каждого из этих событий должна регистрироваться следующая информация:
* дата и время;
* субъект, осуществляющий регистрируемое действие;
* тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
* успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией. Кроме того должны регистрироваться все попытки доступа, все действия оператора и выделенных пользователей (администраторов защиты и т.п.).

*Целостность КСЗ*. В СВТ данного класса защищенности должен осуществляться периодический контроль за целостностью КСЗ. Программы КСЗ должны выполняться в отдельной части оперативной памяти.

*Тестирование*. В данном классе защищенности должно тестироваться:

* реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верное сопоставление меток субъектам и объектам, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД);
* невозможность присвоения субъектом себе новых прав; очистка оперативной и внешней памяти;
* работа механизма изоляции процессов в оперативной памяти; маркировка документов;
* защита вода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;
* идентификация и аутентификация, а также их средства защиты;
* запрет на доступ несанкционированного пользователя; работа механизма, осуществляющего контроль за целостностью СВТ;
* регистрация событий, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

Кроме этого выдвигается ряд требований по разработке документации на КСЗ.

Необходимо также упомянуть, что все используемые при построении СЗИ средства криптографической защиты, должны быть надлежащим образом сертифицированы уполномоченным органом – ФАПСИ.

2.1.4. Варианты обеспечения безопасности

Существует три метода решения задач, связанных с проблемами обеспечения информационной безопасности АС.

Прежде всего это – программный метод**.** В этом случае на этапе разработки комплекса необходимо предусмотреть механизмы безопасности, обеспечивающие невозможность НСД в следующих условиях:

Нарушитель знает о реализованных в комплексе механизмах безопасности.

Если в комплексе используются криптографические средства, то нарушитель владеет исходными текстами этих средств.

Нарушитель имеет полный физический доступ к комплексу.

Противоположностью этого метода является организационный метод. При организационном подходе комплекс создается на базе уже имеющихся программных средств. Применяются административные ограничения на доступ в помещение, в котором расположен комплекс, ПЭВМ комплекса тщательно охраняются. Вводятся инструкции по работе, которых четко придерживаются все пользователи. Считается, что при соблюдении инструкций невозможна утечка защищаемых данных.

Третий путь – комбинация программного и организационного методов. К стандартному программному обеспечению добавляются модули, обеспечивающие безопасность, а также вводится ряд инструкций и правил, направленных на эти же цели.

Следует отметить, что при использовании третьего метода необходимо четко скоррелировать набор дополнительных программных средств и вводимых правил.

Рассмотрим теперь достоинства и недостатки вышеперечисленных методов.

Для реализации программного метода как минимум необходимо:

Написать свою операционную систему.

Разработать средства общего управления и восстановления.

Разработать программные средства защиты.

Разработать собственную систему аналогичную Microsoft Exchange Server.

Разработать собственную систему управления базами данных аналогичную Microsoft SQL Server.

При выполнении вышеперечисленных требований этот метод обладает следующими достоинствами:

Утечка защищаемой информации из комплекса невозможна.

Обеспечивается защита хранимой информации при получении нарушителем физического доступа к комплексу.

Есть уверенность в том, что при разработке комплекса туда не было встроено закладок.

Возможность предусмотреть оптимальную настройку комплекса под нужды и специфику конкретного учреждения.

Главным недостатком является чрезвычайно высокая сложность реализации проекта. Такую задачу невозможно выполнить за приемлемое время и с приемлемыми экономическими затратами.

Основным достоинством организационного метода является, напротив, простота реализации с точки зрения программиста. Для реализации этого метода необходимо разработать правила, регламентирующие работу пользователей, и систему административных мер, ограничивающих доступ к комплексу, соблюдение которых полностью исключает утечку информации. При этом нет необходимости применять какие-либо криптографические средства, разрабатывать дополнительные программные модули. Однако, в этом случае к каждому компьютеру необходимо будет поставить круглосуточную охрану или убирать его в сейф. Также этот метод не предусматривает защиты от ошибок пользователей, которые могут повлечь за собой утечку или разрушение защищаемой информации. Кроме того, при помощи административных мер трудно обеспечить действенную защиту информации от потери в результате сбоев системы.

Применениетретьего, программно-организационнго метода, несомненно, оптимально. Комбинируя административные меры со специально разработанными программными средствами можно получить достаточно надежную защиту при разумной затрате сил и средств. Следуя этому методу, разработчик может выбирать какие механизмы защиты можно реализовать программно, а какие проще решить при помощи административных санкций. Этот метод имеет ряд достоинств. Вот основные:

Разработчик может обеспечить защиту от ошибок пользователя при помощи специально разработанных программных средств.

Достаточно просто организуется защита хранимой информации при помощи сертифицированных криптографических средств.

Защиту от модификации имеющегося ПО и от закладок можно реализовать при помощи административных ограничений и использованием контрольных сумм.

Как и любой другой метод, комбинация организационных и программных средствимеет свои недостатки. Главным из них является трудность выбора границы между этими средствами. Необходимо найти "золотую середину", которая будет отражать оптимальное использование как административных, так и программных средств. Также необходимо убедиться, что совокупность используемых средств защиты полностью обеспечивает защиту информации от утечки, потери, модификации.

Итак, проанализировав вышеперечисленные методы обеспечения безопасности информации, а также требования предъявляемые к системе защиты СД МТ, надо отметить необходимость создания некоторых специальных программных средств для обеспечения безопасности, несмотря на то, что большинство мер СЗИ от НСД можно реализовать с помощью средств, предоставляемых ПО, служащим основой для разрабатываемой СД МТ, (примером может служить дискреционное управление доступом, обеспечиваемое ОС Windows NT), или с помощью специальных программных комплексов и средств, таких как межсетевые экраны или сканеры безопасности, создаваемых компаниями специализирующимися на разработках в области информационной безопасности, а также некоторого набора организационных мер. Создаваемое СПО призвано не заменить существующие механизмы и средства защиты, а напротив, усилить их, позволяя обеспечить соответствие выбранному классу защиты.

В настоящем дипломном проекте основное внимание уделяется управлению доступом к данным, конкретно – реализации механизма мандатного управления доступом.

2.1.5. Управление доступом

Под управлением доступом понимается процесс регулирования использования ресурсов АС. Управление доступом включает решение следующих задач:

* идентификацию пользователей, персонала и ресурсов АС;
* установление подлинности субъектов и объектов, допускаемых к использованию ресурсов АС;
* проверку полномочий субъектов на доступ к защищаемым ресурсам;
* регистрацию (протоколирование) обращений к защищаемым ресурсам;
* реакцию на несанкционированные действия.

Рассмотрим подробнее общие вопросы проверки полномочий доступа, так как данному вопросу в основном и посвящен настоящий ДП.

2.1.5.1. Проверка полномочий субъектов на доступ к ресурсам

После положительного установления подлинности пользователя (и системы со стороны пользователя) система должна осуществлять постоянную проверку полномочий поступающих от субъектов запросов. Проверка полномочий заключается в определении соответствия запроса субъекта предоставленным ему правам доступа к ресурсам. Такую процедуру часто называют "контроль полномочий" или "контроль доступа".

При создании механизмов контроля доступа необходимо, прежде всего, определить множества субъектов доступа, активных ресурсов, осуществляющих какие-либо действия над другими ресурсами, и объектов доступа, пассивных ресурсов, используемых субъектом доступа для выполнения операций. Субъектами могут быть, например, пользователи, задания, процессы и процедуры. Объектами - файлы, программы, семафоры, директории, терминалы, каналы связи, устройства, блоки ОП и т.д. Субъекты могут одновременно рассматриваться и как объекты, поэтому у субъекта могут быть права на доступ к другому субъекту. В конкретном процессе в данный момент времени субъекты являются активными элементами, а объекты - пассивными. Для осуществления доступа к объекту субъект должен обладать соответствующими полномочиями. Полномочие есть некий символ, обладание которым дает субъекту определенные права доступа по отношению к объекту, область защиты определяет права доступа некоторого субъекта ко множеству защищаемых объектов и представляет собой совокупность всех полномочий данного субъекта. При функционировании системы необходимо иметь возможность создавать новые субъекты и объекты. При создании объекта одновременно создается и полномочие субъектов по использованию этого объекта. Субъект, создавший такое полномочие, может воспользоваться им для осуществления доступа к объекту или же может создать несколько копий полномочия для передачи их другим субъектам. Непосредственная реализация контроля прав доступа обычно выполняется с помощью матриц доступа.

При использовании матричной модели доступа условия доступа каждого субъекта s к каждому объекту o определяются содержимым элемента матрицы доступа или матрицы установления полномочий M. Каждый элемент Mij матрицы доступа M определяет права доступа i-го субъекта к j-му объекту (читать, писать, выполнять, нельзя использовать и т.п.). Пример матрицы доступа приведен на рисунке 2.3. Элементы в матрице доступа имеют следующие значения: r - чтение, w - запись, е - выполнение, 0 - нельзя использовать.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | o1 | o2 | … | on |
| s1 | r | w |  | w |
| s2 | rw | rw |  | 0 |
| … |  |  |  |  |
| sn | e | rwe |  | we |

Рисунок 2.3. Пример матрицы доступа.

Элементы матрицы доступа могут содержать указатели на специальные процедуры, которые должны выполняться при обращении субъекта к объекту. Решение о доступе в этом случае осуществляется на основании результатов выполнения процедур, например:

* решение о доступе в данный момент времени основывается на анализе предыдущих доступов к другим объектам;
* решение о доступе основывается на динамике состояния системы (права доступа субъекта зависят от текущих прав доступа других субъектов);
* решение о доступе основывается на значении определенных переменных, например, на значении таймера.

Необходимо отметить, что строка M[s,\*] содержит список разрешенных операций субъекта s по отношению ко всем объектам (список возможностей), а столбец M[\*,o] - определяет, какие субъекты имеют права доступа к объекту o и какие именно права доступа (список доступа).

Размерность матрицы доступа зависит от количества субъектов и объектов в системе и может быть достаточно большой. Для уменьшения размерности матрицы доступа могут применяться различные методы:

* установление групп субъектов, называемых кликами, каждая из которых представляет собой группу субъектов с одинаковыми правами;
* установление групп терминалов по классам полномочий (клики терминалов);
* группировка объектов по уровням категорий (например, по уровням секретности);
* хранение списка пар вида (o, f), где о - защищаемый объект, а f - разрешение на использование его субъектом.

Перечисленные методы и другие, им подобные, могут применяться как по отдельности, так и в совокупности.

В процессе функционирования системы множества субъектов и объектов могут динамически изменяться. Такие изменения могут происходить, например, в результате появления новых субъектов и объектов, уничтожения субъектов и объектов и изменения прав доступа субъектов к объектам. Соответственно, в процессе функционирования системы должна изменяться и матрица доступа. Динамика изменения множеств субъектов и объектов, а также матрицы доступа при выполнении некоторых операций представлена в таблице 2.2.

В таблице 2.2: S – множество субъектов; O – множество объектов, причем S принадлежит O; M[s,o] – матрица доступа. Элементами матрицы M являются права доступа g, принадлежащие G. Изменившиеся множества помечены штрихом.

Таким образом, при создании субъекта s' этот субъект вводится в состав элементов множеств S и О. В матрице доступа появляется новая строка, соответствующая новому субъекту: М'[s,о] = M[s,о]. M'[s',о] = 0; M'[s',s] = 0, так как субъект создан, но его права по отношению к существующим субъектам и объектам не определены. Матрицы доступа в той или иной степени используются во многих защищенных системах.

*Таблица 2.2.*

|  |  |  |
| --- | --- | --- |
| Исходное состояние | Операция | Результирующее состояние |
| S, O, M  s'  O | Создание субъекта s' | S'= S  {s'}, O' = O  {s'} M'[s,o] = M[s,o], s  S, o  O M'[s',o] = 0, o  O' M'[s',s] = 0, s  S' |
| S, O, M  o'  O | Создание объекта o' | S'=S, O' = O  {o'} M'[s,o] = M[s,o], s  S, o  O M'[s,o'] = 0, s  S' |
| S, O, M  s'  S | Уничтожение субъекта s' | S'= S  {s'}, O'= O  {s'} M'[s,o] = M[s,o], s  S', o  O' |
| S, O, M  o'  O  o'  S | Уничтожение объекта o' | S' = S, O' = O  {o'} M'[s,o] = M[s,o], s  S', o  O' |
| S, O, M  s  S  o  O | Введение права g в М[s,o] | S'=S, O' = O M'[s,o] = M[s,o]  {g}  M'[s',o'] = M[s',o'], если (s',o')  (s',o') |
| S, O, M  s  S  o  O | Удаление права g из М[s,o] | S'=S, O' = O M'[s,o] = M[s,o]  {g}  M'[s',o'] = M[s',o'], если (s',o')  (s',o') |

Расширением матричной модели доступа является многоуровневая модель доступа. Объекты в многоуровневой модели имеют различные уровни доступа (например, уровни секретности), а субъекты – степени допуска. Разрешение допуска субъекта к объекту является функцией от степени допуска конкретного субъекта и уровня допуска конкретного объекта. Многоуровневая модель доступа создана на основе теории алгебраических решеток. Данные могут передаваться между субъектами, если выполняются следующие правила (здесь буквами а, b и с обозначим идентификаторы субъектов, а буквами х, у и z, соответственно, их уровни доступа).

Данные могут передаваться субъектом самому себе:

x <= x (2.1. а)

Данные могут передаваться от субъекта а к субъекту с, если они могут передаваться от субъекта a к субъекту b и от субъекта bк субъекту с:

если x <= у и y <= z, то x <= z (2.1. б)

Если х <= у и у <= х, то x = y (2.1. с)

Отметим, что рассмотренные правила представляют, соответственно, свойства рефлективности, транзитивности и антисимметричности.

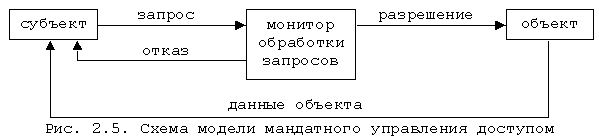
Примером использования многоуровневой модели доступа является система контроля доступа, принятая в военном ведомстве США (рисунок 2.4). Уровнями доступа выступают уровни секретности: НЕСЕКРЕТНО, КОНФИДЕНЦИАЛЬНО, СЕКРЕТНО, СОВЕРШЕННО СЕКРЕТНО. Внутри отдельных уровней секретности для выделения разделов данных, требующих специального разрешения на доступ к ним, определены категории: АТОМНЫЙ, НАТО и ДРУГИЕ. Для получения доступа к данным определенной категории субъект должен иметь не только доступ к данным соответствующего уровня (по секретности), но и разрешение на доступ по категории. Например, субъект, имеющий доступ к данным с уровнем СОВЕРШЕННО СЕКРЕТНО и категории НАТО, не может получить доступ к данным с категориями АТОМНЫЙ и ДРУГИЕ уровня СОВЕРШЕННО СЕКРЕТНО.

2.2. Обоснование проектных решений

2.2.1. Математическая модель мандатного управления доступом

Рассмотрим модель доступа используемую в данном ДП, схема которой приведена на рисунке 2.5. Она состоит из следующих элементов:

* множества субъектов S;
* множества объектов О;
* множества уровней защиты L;
* множества прав доступа G;
* списка текущего доступа b;
* списка запросов Z.



Каждому субъекту s  S сопоставляются два уровня защиты: базовый Is(Si)  L, задаваемый в начале работы и остающийся неизменным, и текущий It(Si)  L, зависящий от уровней защиты тех объектов, к которым субъект Si имеет доступ в настоящий момент времени.

Множество объектов О наделяется структурой дерева таким образом, что каждому объекту Oj соответствует список объектов, непосредственно следующих за ним (объектов-сыновей) и, если Oj отличен от корня дерева, то существует единственный объект O(j),непосредственно предшествующий ему (отец объекта Oj). Каждому объекту Oj приписывается уровень защиты I(Oj)  L.

Множество L, является конечным частично упорядоченным множеством, обладавшим свойством алгебраической решетки. Возможно представление каждого уровня защиты Lr  L, в виде вектора из двух компонент: классификации и множества категорий. Будем говорить, что уровень защиты I1 больше уровня защиты I2, если классификация I1 больше или равна классификации I2, и множество категорий I1 содержит множество категорий I2 ( в формализованном виде: I1  I2).

Множество прав доступа G имеет вид:

G = {r, а, w, e}, (2.2)

где r – чтение объектом субъекта (получение субъектом данных, содержащихся в объекте ) ;

а – модификация данных объекта субъектом без их предварительного прочтения;

w – запись-модификация данных объекта после их предварительного прочтения субъектом;

е – исполнение субъектом объекта (действие, не связанное ни с чтением, ни с модификацией данных).

Расширения модели допускают использование права С-управления, при котором субъект Si может передать права доступа, которыми он владеет по отношению к объекту Oj, другому субъекту Sk.

При описании модели будем рассматривать следующую схему управления передачей прав доступа: передача прав доступа к объекту Oj субъектом Si субъекту Sk связана с наличием у субъекта Si права w к "отцу" объекта Oj. Матрица доступа M = ||Mij|| не содержит пустых столбцов. Однако, наличие элемента Mij  0 является необходимым, но недостаточным условием разрешения доступа. Список текущего доступа b содержит записи вида (Si, Oj, X), если субъекту Si разрешен доступ x  G к объекту Oj и это разрешение к настоящему моменту времени не отменено. Разрешение доступа действительно до тех пор, пока субъект не обратился с запросом на отказ от доступа к монитору. Список запросов Z описывает возможности доступа субъекта к объекту, передачи прав доступа другим субъектам, создания или уничтожения объекта. В настоящей модели рассматриваются 11 следующих запросов:

1) запрос на чтение (r) объекта;

2) запрос на запись (w) в объект;

3) запрос на модификацию (a) объекта;

4) запрос на исполнение (е) объекта;

5) запрос на отказ от доступа;

6) запрос на передачу доступа к другому объекту ;

7) запрос на лишение права доступа другого субъекта;

8) запрос на создание объекта без сохранения согласованности;

9) запрос на создание объекта с сохранением согласованности;

10) запрос на уничтожение объекта;

11) запрос на изменение своего текущего уровня защиты.

Можно сформулировать два условия защиты для модели:

1) простое условие защиты;

2) \* - условие.

Простое условие защиты предложено для исключения прямой утечки секретных данных и состоит в следующем. Если субъекту Sj запрещен доступ:

а) по чтению r объекта Oj, тогда Is(Si)  I(Oj);

б) по записи w в объект Oj, тогда Is(Si)  I(Oj).

Простое условие защиты накладывает ограничения на базовые уровни защищенных объектов.

\*-условие защиты (\*-свойство) предназначено для предотвращения косвенной утечки данных. Это условие накладывает ограничения на уровни защиты тех объектов, к которым субъект может иметь доступ одновременно. Если субъект S имеет доступ X1 к объекту O1 и доступ X2 к объекту O2, то, в зависимости от вида доступа, должны выполняться соотношения между уровнями защиты, приведенные в таблице 2.3.

*Таблица 2.3*

|  |  |  |
| --- | --- | --- |
| Доступ к О1 | Доступ к О2 | Соотношение |
| Чтение - r | Дополнение - а | I(S1)  I(O2) |
| Чтение - r | Запись - w | I(S1)  I(O2) |
| Запись - w | Дополнение - а | I(S1)  I(O2) |
| Запись - w | Запись - w | I(S1)  I(O2) |

Введение \*-условия предназначено для предотвращения потока данных вида "чтение объекта для переписи данных в объект с меньшим либо несравнимым уровнем защиты" (напомним, что доступ w предполагает предварительное чтение).

Состояние системы считается безопасным, если соотношения между уровнями защиты объектов и субъектов удовлетворяют как простому условию защиты, так и \*-условию.

Система защиты должна обеспечивать безопасность данных, если она не допускает перехода из безопасного состояния в состояние, не являвшееся безопасным.

Для обеспечения безопасности данных необходимо и достаточно, чтобы изменение состояний системы приводило только к безопасным состояниям, если исходное состояние было безопасным.

В рассматриваемой модели описываются правила разрешения каждого из 11 возможных запросов. Эти правила используют понятие текущего уровня защиты субъекта, которое определяется следующим образом.

Пусть Or, Ow, Oa – множества тех объектов, к которым субъект S имеет доступ r, w и а соответственно. Если Ow  0, то

It(s) = max I(Oj) = min I(Oj) (2.3)

(Oj  Ow) (Oj  Ow)

Если Ow = 0, то It(s) может иметь уровень защиты в пределах:

max I(Oj)  It (s)  min I(Oj) (2.4)

(Oj  Or) (Oj  Oa)

В случае, если нижняя граница в этом неравенстве берется по пустому множеству, она полагается равной

min I(Oj), (2.5 а)

(Oj  Ow)

а верхняя – Ib(s) (2.5 б)

Рассмотрим правила выполнения каждого из 11 возможных запросов модели.

1. Запрос на чтение субъектом Si объекта Oj разрешается, если выполняется условие:

r Mij ^ Is(Si)  I(Oj) ^ It(Si)  I(Oj) (2.6 а)

При невыполнении условия (2.6 а) запрос отвергается.

2. Запрос на запись субъектом Si в объект Oj разрешается, если выполняется условие:

w  Mij ^ Is(Si)  I(Oj) ^ It(Si)  I(Oj) (2.6 б)

При невыполнении условия (2.6 б) запрос отвергается.

3. Запрос на дополнение субъектом Si объекта Oj разрешается, если выполняется условие:

a  Mij ^ It(Si)  I(Oj) (2.6 в)

При невыполнении условия (2.6 в) запрос отвергается.

4. Запрос на исполнение субъектом Si объекта Oj разрешается, если e  Mij, и отвергается - в противном случае.

5. Отказ субъекта Si от доступа x  G к объекту разрешается безусловно. При этом происходит изменение состояния системы :

b' = b  {Si,Oi,x} (2.6 г)

6. Передача субъекту Sk субъектом Si права на доступ x к объекту Oj разрешается, если субъект Sk имеет доступ w к "отцу" Os(j) объекта Oj, то есть если

{Sk,Os(j),w}  b, (2.6 д)

и отвергается - в противном случае. При этом происходит изменение состояния системы:

M'ij = Mij  {x}, x  G (2.6 е)

7. Лишение субъекта Sk субъектом Si права на доступ x к объекту Oj разрешается, если субъект Sk имеет доступ w к "отцу" Os(j) объекта Oj, то есть если

{Sk,Os(j),w}  b, (2.6 ж)

и отвергается - в противном случае. При этом происходит изменение состояния системы:

M'ij = Mij  {x}, x  G (2.6 з)

8. Создание субъектом Si объекта Ot(j) с уровнем защиты I, являющегося "сыном" объекта Oj, разрешается, если список текущего доступа b содержит записи:

{Si,Oj,w} ^ {Si,Oj,a} (2.6 и)

и отвергается - в противном случае. При этом происходит изменение состояния системы:

O' = O  {Ot(j)}; M' = M  Mt(j) (2.6 к)

где столбец Mt(j) содержит один ненулевой элемент Mit(j), значение которого зависит от дополнительного параметра, указываемого при запросе. Оно может принимать значения либо {r,а,w}, либо {r,а,w,е).

9. Создание субъектом Si объекта Ot(j) с уровнем защиты I, являющегося "сыном" объекта Oj, с сохранением согласованности разрешается, если список текущего доступа b содержит записи:

{Si,Oj,w} ^ {Si,Oj,a} ^ I > I(Oj) (2.6 л)

и отвергается - в противном случае. Изменение состояния системы происходит аналогично восьмому запросу.

10. Уничтожение субъектом Si объекта Oj (и всех объектов Oj1,Oj2,… Ojk, являющихся "последователями" по структуре дерева) разрешается, если субъект Si имеет доступ w к "отцу" Oi(j) объекта Oj, и отвергается - в противном случае. Изменение состояния системы происходит следующим образом: из списка текущего доступа b удаляются все записи, содержащие объекты Oj1,Oj2,… Ojk; из матрицы M удаляются столбцы с номерами j1,j2,… jk.

11. Изменение субъектом Si своего текущего уровня защиты It(Si) на It' разрешается, если выполняются условия:

а) Is(Si)  It' и

б) It'  I(Oj), если субъект Si имеет доступ а к какому-либо объекту Oj

в) It' = I(Oj), если субъект Si имеет доступ w к какому-либо объекту Oj

г) It'  I(Oj), если субъект Si имеет доступ r к какому-либо объекту Oj.

В противном случае запрос отвергается.

2.3. Программная реализация

В данном разделе описывается программный модуль, реализующий изложенные выше алгоритмы разграничения прав доступа.

2.3.1. Выбор средств программирования

Для написания программы была выбрана интегрированная система программирования Borland C++ Builder 3.0 и объектно‑ориентированный язык C++, так же использовался компилятор С++ 5.02 фирмы Borland. Эти средства позволяют создавать прикладные программы, предназначенные для работы на ПЭВМ IBM PC AT под управлением оболочки Windows 95 и более поздних версий, а так же операционной системы Windows NT и использующие общепринятые для Windows элементы пользовательского интерфейса, а также позволяющие с легкостью реализовывать работу с базами данных и создавать клиент/серверные приложения.

Предпочтение было отдано системе Borland C++ Builder благодаря широкому набору стандартных средств программирования, называемых компонентами, позволяющих экономить время на создание различных программных интерфейсов и реализации многих общих для широкого спектра программных продуктов функций. Кроме того визуальная среда проектирования, который обладает Borland C++ Builder, существенно ускоряющая и упрощающая разработку, является практически стандартом среди разработчиков ПО. Еще одним преимуществом выбранной системы является высокая (по сравнению со многими другими средствами программирования) эффективность генерируемого компилятором кода, что весьма существенно для данного ДП, т.к. в нем применяется метод, требующий большого количества вычислений.

2.3.2. Описание программного продукта

Программный модуль мандатного разграничения доступа имеет следующие функциональные возможности:

* контроль прав доступа субъектов системы на чтение (r) объекта;
* контроль прав доступа субъектов системы на запись (w) в объект;
* контроль прав доступа субъектов системы на модификацию (a) объекта;
* контроль прав доступа субъектов системы на исполнение (е) объекта;
* контроль прав доступа субъектов системы на отказ от доступа;
* контроль прав доступа субъектов системы на передачу доступа к другому объекту ;
* контроль прав доступа субъектов системы на лишение права доступа другого субъекта;
* контроль прав доступа субъектов системы на создание объекта без сохранения согласованности;
* контроль прав доступа субъектов системы на создание объекта с сохранением согласованности;
* контроль прав доступа субъектов системы на уничтожение объекта;
* контроль прав доступа субъектов системы на изменение своего текущего уровня защиты.

2.3.3. Разработка программной документации

В документацию к ПП на КЗ "Система документооборота Минторга РФ" должны входить тексты исходных модулей программы. Программная документация на КЗ "Система документооборота Минторга РФ" должна разрабатываться в соответствии с требованиями ГОСТ 19.301-76, ГОСТ 19.503-79 и ГОСТ 19.504-79.

2.3.4. Результаты опытной эксплуатации КЗ "Система документооборота Минторга РФ" и технические предложения по ее развитию

Опытная эксплуатация разработанного МО КЗ и ПП показала, что он соответствует требованиям ТЗ на данный комплекс и решает поставленную перед ним задачу. Программный модуль корректно справляется с контролем полномочий и соблюдением прав доступа на основе меток безопасности (мандатным принципом управления доступом). В рамках поставленной задачи заложенная функциональность реализована полностью.

Были проведены испытания, с целью выявить влияние созданного модуля на общее свойство доступности системы.

Испытания проводились в следующей конфигурации.

Сервер Compaq Proliant 800, процессор Intel Pentium II 450 МГц, RAM 256 Мб, жесткий диск 9,1 Гб Wide-Ultra SCSI 3, под управлением MS Windows NT Server 4.0 с установленной СД МТ.

Рабочая станция: процессор Intel Pentium 166MMX, RAM 64 Мб, жесткий диск Quantum Fireball TM 2,1 Гб, операционная системой MS Windows 95 OSR 2.

Сетевое оборудование 3Com.

По результатам испытания время отклика системы с использованием дискретного (обеспечиваемого Windows NT) разграничения доступа составило 0,51 секунды, с использованием модуля мандатного разграничения прав доступа – 0,63 секунды, что является более чем приемлемым результатом.

Кроме того было проведено тестирование с целью обнаружения "дырок" в разработанном программном модуле. В соответствие с квалификацией разработчика в данной области критичных ошибок обнаружено не было.

Проведенное исследование не претендует на абсолютную объективность. Кроме того согласно существующему законодательству разработанный программный модуль должен пройти сертификацию Гостехкомиссии Росси, однако, в рамках разрабатываемого ДП он полностью удовлетворяет требованиям заказчика.

Выявлены следующие недостатки разработки (большинство из которых предполагалось заранее):

необходимо более углубленное тестирование модуля на предмет обнаружения возможных ошибок, могущих повлечь за собой возникновения несанкционированного доступа к СД МТ и нарушения прав доступа, это, в основном, следует из необходимости сертификации данного СЗИ;

для адаптации к универсальному использованию данного модулю (не только в рамках СД МТ) необходима некоторая доработка программ и алгоритмов, однако, этот недостаток не является критичным, так как небольшая переработка модуля для каждый конкретной задачи обеспечения защиты от НСД, не только не ослабит разрабатываемый КСЗ, но наоборот позволит проводить более согласованную политику безопасности и гарантировать надежную защиту.

Подведем итоги. В данной главе решены следующие задачи:

1. Выполнена постановка задачи на разработку КЗ "Решение задач информационной безопасности". В рамках разрабатываемой тематики было принято решение о создание СПО, реализующего мандатный принцип управления доступом к системе документооборота Минторга РФ.

2. Рассмотрены общие вопросы информационной безопасности автоматизированных систем и методы их решения.

3. Разработано математическое и программное обеспечение КЗ "Решение задач информационной безопасности", создан модуль мандатного управления доступом к СД МТ. Программная документация содержит 1037 строк исходного кода C++.

4. Разработанный математический аппарат признан пригодным для автоматизации проводимых в министерстве работ по повышению эффективности функционирования данной организации.

В перспективе возможно применение разработанных методов и построенных моделей в других учреждениях Российской Федерации.

ГЛАВА 3. МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРИКЛАДНЫХ ЗАДАЧ

3.1. Деловая игра по курсу “Гражданская оборона”

3.1.1. Постановка задачи и ее спецификация

Гражданская оборона (ГО) Российской Федерации – это составная часть системы общегосударственных мероприятий, проводимых в целях защиты населения и обеспечения устойчивой работы отраслей и хозяйственных объектов государства в условиях применения противником в военное время оружия массового поражения, а так же для спасательных и неотложно-восстановительных работ в очагах поражения и зонах катастрофических разрушений в результате стихийных бедствий.

Сильнодействующие ядовитые вещества широко применяются в современном производстве. На химически опасных объектах экономики используются, производятся, складируются и транспортируются огромные количества СДЯВ. Большое число людей работающих на подобных предприятиях могут подвергнутся значительному риску при возникновении аварий и различных чрезвычайных ситуаций (ЧС).

Прогнозирование возможных последствий ЧС позволяет своевременно принять необходимые меры по повышению устойчивости работы объекта, способствует предотвращению человеческих жертв и уменьшению экономического ущерба.

Заблаговременное прогнозирование позволяет вывить критичные элементы объекта экономики, определить возможные последствия ЧС, в том числе и последствия вторичных поражающих факторов и на их основе подготовить рекомендации по защите гражданского населения от этих последствий.

Представляемая часть дипломного проекта посвящена выработке рекомендаций по защите персонала предприятий объекта экономики от аварии со СДЯВ. Кроме того, рассматривается способ прогнозирования последствий подобных аварий и возможных потерь среди гражданского населения.

Основная задача обучения в высших учебных заведениях по курсу ГО – дать студентам теоретическую основу для осуществления мероприятий ГО на объектах экономики. Компьютеризация всех сфер экономики предоставляет широкие возможности по использованию средств вычислительной техники в сфере обучения . Возникает потребность в разработке АРС (Автоматизированной расчетной системы), одним из возможных применений которой является использование ее студентами при выполнении лабораторных работ по курсу “Гражданская оборона”. Предполагается, что студент предварительно знакомится со справочной информацией по работе, получая необходимые сведения о цели работы, составе входных и выходных параметров, а также о методике расчета. После этого студент производит необходимые измерения и вводит данные в систему, которая выдает рассчитанные значения параметров.

Другим важным применением АРС является ее использование сотрудниками отделов ГО предприятий, которые получают возможность делать необходимые расчеты по предложенным методикам. Выполняемые ранее человеком сложные расчеты берет на себя АРС. Это не только облегчает работу сотрудников отделов ГО, но и предотвращает возможное появление ошибок. Кроме того, при расчетах часто используется информация, получаемая из справочных таблиц, которые можно заранее занести в АРС, что устраняет необходимость искать необходимые данные в многотомных справочниках. При разработке такой АРС важное значение приобретает тот факт, что система ориентирована на пользователей, имеющих в большинстве своем чрезвычайно небольшой опыт обращения с ПК. Это приводит к необходимости создания программ с простым, интуитивно понятным пользовательским интерфейсом. Кроме того, должна быть обеспечена проверка введенных пользователем данных, чтобы не возникло сбоев системы. Вообще, система должна корректно реагировать на любое действие пользователя, например, выполнять требуемое действие или выдавать сообщение об ошибке, в противном случае пользователь перестанет понимать, что он должен делать, что в конечном итоге приведет к отказу от использования системы.

Состав и содержание расчетов, составляющих АРС “Гражданская оборона: оценка химической обстановки при аварии со СДЯВ”, определялись в соответствии с консультациями, получаемыми на кафедре “Безопасность жизнедеятельности”.

АРС представляет собой прикладную программу для ЭВМ IBM PC с процессором класса Pentium 60 или выше под управление ОС Windows 9x или Windows NT 3.0 или выше.

Программа обеспечивает расчет и моделирование зависимостей выходных параметров от входных.

Работа с системой предполагает выполнение студентами лабораторных работ по указанной теме, с использованием результатов работы программы.

3.1.2. Методика оценки химической обстановки случае разрушения емкостей со СДЯВ

Угроза поражения людей СДЯВ требует быстрого и точного выявления и оценки химической обстановки. Под химической обстановкой понимают масштабы и степень химического заражения местности, оказывающие влияние на действия формирований ГО, работу объекта экономики и жизнедеятельность населения.

Под оценкой химической обстановки понимается определение масштаба и характера заражения СДЯВ, анализ их влияния на деятельность объекта экономики, сил ГО и населения.

Исходными данными для оценки химической обстановки являются: тип СДЯВ, район, время и количество СДЯВ, разлившееся в результате аварии (при заблаговременном прогнозировании для сейсмических районов за величину выброса принимают общее количество СДЯВ). Кроме того, на химическую обстановку влияют метеорологические условия: температура воздуха и почвы, направление и скорость приземного ветра, состояние вертикальной устойчивости приземного слоя атмосферы.

В основу метода заблаговременной оценки химической обстановки положено численное решение уравнения турбулентной диффузии. Для упрощения расчетов ряд условий оценивается с помощью коэффициентов.

3.1.3. Глубина, ширина и площадь заражения СДЯВ, время подхода зараженного воздуха к объекту и время действия поражающих концентраций

Глубина зоны химического поражения рассчитывается следующим образом:

, м, (3.1)



где *G* – количество СДЯВ, кг;

*D* – токсодоза, мг . мин/л (D = C . T, здесь С – поражающая концентрация, мг/л, а Т – время экспозиции, мин);

*V* – скорость ветра в приземном слое воздуха, м/с.

Ширина зоны поражения:

, м, (3.2)



Площадь зоны поражения:

, м2, (3.3)



Время подхода зараженного воздуха к объекту рассчитывается из следующего соотношения:

, мин, (3.4)



где *L* – расстояние от места аварии до объекта экономики, м;

– скорость переноса облака, зараженного СДЯВ.



Время действия поражающих концентраций считается следующим образом:

, час, (3.5)



где – время испарения СДЯВ в зависимости от оборудования хранилища, час.



В приведенных уравнениях:

*K*1, *K*2, *K*6, – коэффициенты, учитывающие состояние атмосферы.

*K*3, *K*4 – учитывают условия хранения и топографические условия местности.

*K*5 – учитывает влияние скорости ветра на продолжительность поражающего действия СДЯВ.

Значения коэффициентов *K*1, *K*2, *K*6 в зависимости от вертикальной устойчивости атмосферы определяются из таблицы 3.1., значение коэффициента *K*5 в зависимости от скорости ветра определяется из таблицы 3.2., значение коэффициента *K*3 в зависимости от типа хранилища СДЯВ определяется из таблицы 3.3., значение коэффициента *K*4 в зависимости от типа местности определяется из таблицы 3.4., время испарения СДЯВ при скорости ветра 1 м/с определяется из таблицы 3.5., токсические свойства СДЯВ определяются из таблицы 3.6.

*Таблица 3.1.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Вертикальная устойчивость атмосферы** | | | |
|  | | Инверсия | Изотермия | Конвекция |
| *K*1 | | 0,03 | 0,15 | 0,8 |
| *K*2 | | 1 | 1/3 | 1/9 |
| *K*6 | | 2 | 1,5 | 1,5 |

*Таблица 3.2.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **V м/с** | **1** | **2** | **3** | **4** | **5** | **6** |
| *K*5 | 1 | 0,7 | 0,55 | 0,43 | 0,37 | 0,32 |

*Таблица 3.3.*

|  |  |  |
| --- | --- | --- |
| **Тип хранилища СДЯВ** | | |
|  | открытое | обвалованное | |
| *K*3 | 1 | 2/3 | |

*Таблица 3.4.*

|  |  |  |
| --- | --- | --- |
|  | **Тип местности** | |
|  | открытая | закрытая |
| *K*4 | 1 | 1/3 |

*Таблица 3.5.*

|  |  |  |
| --- | --- | --- |
| **Наименование СДЯВ** | **Тип хранилища** | |
| открытое | обвалованное |
| Аммиак | 1,3 | 22 |
| Хлор | 1,2 | 20 |
| Сернистый ангидрид | 1,3 | 20 |
| Фосген | 1,4 | 23 |

*Таблица 3.6.*

|  |  |  |
| --- | --- | --- |
| **Наименование СДЯВ** | **Токсические свойства** | |
| Поражающая концентрация, мг/л | Экспозиция, мин |
| Аммиак | 0,2 | 360 |
| Хлор | 0,01 | 60 |
| Сернистый ангидрид | 0,05 | 10 |
| Фосген | 0,4 | 50 |

3.1.4. Рекомендации по защите

В первую очередь необходимо определить границу возможного очага химического поражения. Для этого на карту или план объекта экономики наносят зону возможного заражения, а затем выделяют объекты или их части, которые попадают в зону химического заражения.

Исходя из полученной картины, необходимо определить места расположения аптечек первой помощи, количества и места складирования средств индивидуальной защиты (респираторов, противогазов, защитных костюмов). Кроме того, учитывая, что большинство СДЯВ являются еще и горючими, необходимо предусмотреть наличие средств пожаротушения.

Основным видом защиты от воздействия СДЯВ являются: промышленные противогазы марки “В”, “К”, и “М”, гражданский противогаз ГП-5 и фильтрующие противогазы типа КД, также при объемной дохе кислорода не менее 18% и суммарной дозе ядовитых паров и газов не более 0,5% возможно применение респиратора РПГ-67 КД. При высоких концентрациях необходимо применять изолирующие противогазы и защитный костюм от токсичных аэрозолей, резиновые сапоги, перчатки.

При этом необходимо помнить, что время пребывания в средствах индивидуальной защиты существенно зависит от температуры окружающей среды (при работе в пасмурную погоду сроки работы могут быть увеличены в 1,5 – 2 раза). Ориентировочные сроки пребывания людей в изолирующих средствах в зависимости от температуры воздуха приведены в таблице 3.7.

*Таблица 3.7.*

|  |  |  |
| --- | --- | --- |
| **Температура наружного воздуха** | **Продолжительность работы в изолирующей одежде** | |
| без влажного экранирующего комбинезона | с влажным экранирующим комбинезоном |
| +30 и выше  +25 до +29  +20 до +24  ниже +15 | до 20 мин  до 30 мин  до 45 мин  более 3 часов | 1 – 1,5 часа  1,5 – 2 часа  2 – 2,5 часа  более 3 часов |

При серьезных авариях, а также в случае возможности возникновения пожара, необходима эвакуация персонала. Также, силами медперсонала объекта, службы ГО и сотрудников объекта экономики должна быть оказана первая помощь пострадавшим.

Для возможности применения всех этих средств защиты и мер безопасности, необходимо, чтобы весь персонал объекта экономики, на котором возможна авария со СДЯВ, был ознакомлен с правилами техники безопасности, а также с правилами применения средств индивидуальной защиты и оказания первой медицинской помощи при отравлении ядовитыми газами. Службе ГО объекта необходимо проводить периодические учения и/или методические занятия, способствующие получению описанных навыков служащими объекта экономики, и моделирующие возможные ситуации при возникновении аварии со СДЯВ и эвакуации людей.

3.1.5. Разработка программной документации

На АРС “Гражданская оборона: оценка химической обстановки при аварии со СДЯВ” должен быть разработан документ “Руководства оператора” (Р. МИРЭА.00003-01 34 01).

Документ оформляется в соответствии с ГОСТ 19.505-79 и должен содержать следующие разделы:

* назначение программы;
* условия выполнения программы;
* выполнение программы;
* сообщения оператору.

Руководство должно содержать сведения, необходимые для обеспечения процесса интерактивного взаимодействия пользователя с АРС, и позволять облегчение процесса освоения разработанной АРС.

3.1.6. Результаты опытной эксплуатации системы и технические предложения по её развитию

В ходе опытной эксплуатации был сделан вывод, что система удовлетворяет требованиям заказчика.

В целом разработанная система вполне может быть использована как кафедрой “Безопасность жизнедеятельности” в качестве дополнительного обучающего средства при выполнении студентами лабораторных работ, так и сотрудниками отделов ГО на предприятиях.

АРС “Гражданская оборона: оценка химической обстановки при аварии со СДЯВ” на следующих этапах разработки может быть расширена за счет дополнительных расчетных и информационных модулей, охватывающих другие направления ГО производства, или за счет предоставления возможности выбора методик для существующих расчетов. Кроме того, АРС может быть дополнена развернутой диагностикой ошибок пользователя при вводе данных, а также модулем пояснения пользователю того, как был получен каждый конкретный результат, при желании с выдачей промежуточных результатов.

3.2. Автоматизированная система по курсу “Экология и охрана труда”

3.2.1. Постановка задачи и ее спецификация

В процессе труда человек подвергается воздействию большого числа факторов, различных по своей природе и характеру воздействия, которые влияют на его здоровье и работоспособность. Обязательным условием для сохранения здоровья работающих и обеспечения высокой производительности труда является соответствие трудовой деятельности свойствам и возможностям человека, исключение воздействия опасных и вредных производственных факторов. Это достигается при помощи систем законодательных актов, социально – экономических, организационных, технических и профилактических мероприятий и средств охраны труда (ОТ).

ОТ – это система законодательных актов, мероприятий и средств, обеспечивающих безопасность, сохранение здоровья и работоспособности человека в процессе труда.

Основная задача обучения в высших учебных заведениях по курсу ОТ – дать студентам теоретическую основу для осуществления мероприятий ОТ на объектах народного хозяйства. Компьютеризация всех сфер народного хозяйства предоставляет широкие возможности по использованию средств вычислительной техники в сфере обучения и, в частности, на кафедре “Охрана труда”. Возникает потребность в разработке АРС, одним из возможных применений которой является использование ее студентами при выполнении лабораторных работ по курсу “Охрана труда”. Предполагается, что студент предварительно знакомиться со справочной информацией по работе, получая необходимые сведения о цели работы, составе входных и выходных параметров, а также о методике расчета. После этого студент производит необходимые измерения и вводит данные в систему, которая выдает рассчитанные значения параметров.

Другим важным применением АРС является ее использование сотрудниками отделов ОТ предприятий, которые получают возможность делать необходимые расчеты по предложенным методикам, с которыми они могут ознакомиться, используя справочную информацию, предлагаемую АРС. Выполняемые ранее человеком сложные расчеты, часто включающие в себя вычисление интегралов, логарифмов, использование метода наименьших квадратов, берет на себя АРС. Это не только облегчает работу сотрудников отделов ОТ, но и предотвращает возможное появление ошибок. Кроме того, при расчетах часто используется информация, получаемая из справочных таблиц, которые могут быть заранее включены в АРС, что устраняет необходимость искать необходимые данные в многотомных справочниках. При разработке такой АРС важное значение приобретает тот факт, что система ориентирована на пользователей, имеющих в большинстве своем чрезвычайно небольшой опыт обращения с ПК. Это приводит к необходимости создания программ с простым, интуитивно понятным пользовательским интерфейсом. Кроме того, должна быть обеспечена проверка введенных пользователем данных, чтобы не возникло сбоев системы. Вообще, система должна корректно реагировать на любое действие пользователя, например, выполнять требуемое действие или выдавать сообщение об ошибке, в противном случае пользователь перестанет понимать, что он должен делать, что в конечном итоге приведет к отказу от использования системы.

Состав и содержание расчетов, составляющих АРС “Охрана труда: компьютерное моделирование местной вентиляции”, определялись в соответствии с консультациями, получаемыми на кафедре “Охрана труда”.

АРС представляет собой прикладную программу для ЭВМ IBM PC с процессном класса Pentium 60 или выше под управление ОС Windows 9x или Windows NT 3.0 или выше.

Программа обеспечивает расчет и моделирование зависимостей выходных параметров от входных.

Работа с системой предполагает выполнение студентами лабораторных работ по указанной теме, с использованием результатов работы программы.

3.2.2. Постановка задачи по исследованию местной вентиляции

Приступая к проектированию вентиляции, необходимо прежде всего дать характеристику производственного помещения и проводимых в нем технологических процессов. Следует указать все виды выделений (влаги, вредных веществ, избытка тепла), характер их воздействий на человека, нормируемые предельно допустимые концентрации вредных веществ и параметры микроклимата в помещении, где осуществляется производственный процесс.

3.2.2.1 Влаговыделение

Влага выделяется в результате испарения со свободной поверхности воды и влажных поверхностей материалов и кожи, в результате дыхания людей, а также химических реакций, работы оборудования и т.д. Количество влаги, выделяемое людьми (см. табл. 1), г/ч, определяется по формуле:

W **=** n / w**,** г/чел., (3.6)

где n – число людей; w – количество влаги, выделенное одним человеком, г/чел.

Количество тепла и влаги, выделяемое человеком приведено в таблице 3.8.

*Таблица 3.8.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Характер Выполняемой Работы** | **Тепло, Вт** | | | | | **Влага, г/ч** | |
| полное | | явное | | |
| при 10 °С | при 35 °С | при 10 °С | при 35 °С | | при 10 °С | при 35 °С |
| Умственная | 160 | 93 | 140 | 16 | | 30 | 115 |
| Физическая | | | | | | | |
| Легкая | 180 | 145 | 150 | 8 | 40 | | 200 |
| Средняя | 215 | 195 | 165 | 8 | 70 | | 280 |
| Тяжелая | 290 | 290 | 195 | 16 | 135 | | 415 |

Количество влаги, испаряющейся с открытой поверхности не кипящей воды, определяется по формуле:

, кг/ч, (3.7 а)



где - коэффициент, зависящий от температуры поверхности испарения, его значение определяется по таблице 3.9.; - скорость движения воздуха над поверхностью испарения, м/с.; , - давление водяного пара, соответственно, при температуре поверхности испарения и полном насыщении и в окружающем воздухе, кПа; - площадь поверхности испарения, ; - барометрическое давление, кПа.



*Таблица 3.9.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **tисп, °С** | 30 | 40 | 50 | 60 | 70 | 80 | 90 |
| **** | 0,02 | 0,028 | 0,033 | 0,037 | 0,041 | 0,046 | 0,051 |

Для не кипящей воды температура поверхности испарения находиться из таблицы 3.10. по средней температуре воды



*Таблица 3.10.*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **tисп, °С** | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 |
| **tе, °С** | 18 | 28 | 37 | 45 | 51 | 58 | 69 | 82 |

Количество влаги, испарившейся при кипении воды, , кг/ч, зависит от количества подводимого к воде тепла и вида укрытия воды и может быть определено по формуле:



, кг/ч, (3.7 б)



где - опытный коэффициент, учитывающий вид укрытия:



для плотных укрытий без отсоса воздуха – , при отсосе воздуха – ; - мощность теплового источника испарения, Вт; - скрытая теплота испарения, кДж/кг.



Ориентировочно интенсивность испарения может быть принята равной кг в 1 час с 1 поверхности.



Количество водяных паров, образующихся при химических реакция, в том числе и при горении веществ, определяется по опытным данным. При сжигании 1 кг горючего количество образовавшейся влаги может быть определено по таблице 3.11.

*Таблица 3.11.*

|  |  |
| --- | --- |
| **Горючей вещество** | **Wгор, кг/кг** |
| Водный генераторный газ | 0,61 |
| Ацетилен | 0,7 |
| Бензин | 1,4 |

Количество испаряющейся влаги (кг/ч) при применении охлаждающих эмульсий при охлаждении металлорежущих станков определяется по формуле , где - мощность станков, кВт.



Влаговыделения от технологического оборудования обычно принимаются по справочным данным.

3.2.2.2. Газо- и пылевыделение

В помещении могут находится различные источники выделений газов и пыли. Необходимо учитывать газовыделения со свободной поверхности жидкостей, при сгорании топлива, через неплотности аппаратуры и трубопроводов, при различных технологических операциях (окраске, сварке, гальванизации, пайке, травлении, нанесении фоторезисторов и т.д.). Пылевыделения имеют место при механической обработке материалов, их очистке, полировке, дроблении, транспортировке, сварочных работах и других операциях. Места пылеобразования, как правило, оборудуются местной вентиляцией.

Количество двуокиси углерода, содержащийся в выдыхаемом человеком воздухе, определяется по таблице 3.12.

При наличии в помещении источников других вредных выделений количество этих выделений в воздухе (газы, пары, пыль и др.) подсчитываются исходя из особенностей технологического процесса и оборудования.

*Таблица 3.12.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Характер выполняемой работы** | | **Расход CO2** | |
| объемный, л/ч | массовый, г/ч |
| Умственная | | 23 | 45 |
| Физическая | |  |  |
|  | легкая | 25 | 50 |
|  | средняя | 35 | 70 |
|  | тяжелая | 45 | 90 |

3.2.3. Расчеты выделений тепла

3.2.3.1. Тепловыделения от людей

Тепловыделения человека зависят от тяжести работы, температуры и скорости движения окружающего воздуха. Количество тепла, выделяемого одним человеком, приведено в таблице 3.2.2.1.1 Считается, что женщина выделяет 85%, а ребенок 75% тепловыделения взрослого мужчины.

В расчетах используется явное тепло, т.е. тепло, воздействующее на изменение температуры в помещении.

3.2.3.2. Тепловыделения от солнечной радиации

Расчет тепла, поступающего в помещение от солнечной радиации и , производиться по следующим формулам:



для остекленных поверхностей

, Дж, (3.8 а)



для покрытий

, Дж, (3.8 б)



где , - площади поверхности остекления и покрытия, ; , – тепловыделения от солнечной радиации, , через поверхности остекления (с учетом ориентации по сторонам света) и через покрытия (таблицы 3.13. и 3.14.); - коэффициент учета характера остекления (таблица 3.15.).



*Таблица 3.13.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Характер остекления** | **При ориентации остекления по географической широте** | | | | | | | | | | | | | | | | | | |
| Ю | | | | | ЮВ и ЮЗ | | | | | В и З | | | | | СВ и СЗ | | | |
| 35 | 45 | 55 | 65 | 35 | | 45 | 55 | 65 | 35 | | 45 | 55 | 65 | 35 | | 45 | 55 | 65 |
| Окна с двойным остеклением с переплетами: | | | | | | | | | | | | | | | | | | | |
| деревянными | 128 | 145 | 145 | 170 | 100 | | 128 | 145 | 170 | 145 | | 145 | 170 | 170 | 75 | | 75 | 75 | 75 |
| металлическими | 165 | 185 | 185 | 120 | 128 | | 165 | 185 | 210 | 185 | | 185 | 200 | 210 | 95 | | 95 | 95 | 95 |
| Фонари с двойным вертикальным остеклением с переплетами: | | | | | | | | | | | | | | | | | | | |
| деревянными | 140 | 170 | 170 | 175 | 115 | | 145 | 175 | 175 | 170 | | 170 | 185 | 185 | 87 | | 87 | 87 | 80 |
| металлическими | 150 | 185 | 185 | 200 | 128 | | 165 | 200 | 200 | 185 | | 185 | 210 | 210 | 100 | | 100 | 100 | 95 |

Для остекленных поверхностей, ориентированных на север,

= 0



*Таблица 3.14.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Характер покрытия** | **При географической широте** | | | | |
| 35 | 45 | 55 | 65 |
| Плоское безчердачное | 24 | 21 | 17 | 14 |
| с чердаком | 6 | 6 | 6 | 6 |

Солнечную радиацию следует учитывать при наружной температуре от 10 °С и выше.

*Таблица 3.15.*

|  |  |
| --- | --- |
| **Характер остекления, его состояние** | **Aост** |
| Двойное остекление в одной раме | 1,15 |
| Одинарное остекление | 1,45 |
| Обычное загрязнение | 0,8 |
| Сильное загрязнение | 0,7 |
| Забелка окон | 0,6 |
| Остекление с матовыми стеклами | 0,7 |
| Внешнее зашторивание окон | 0,25 |

За величину остекления принимается большая величина, полученная при расчете двух вариантов:

тепловыделение через остекление в одной стене в сумме с тепловыделением через покрытие и фонари;

тепловыделение через остекление в двух взаимно перпендикулярных стенах с коэффициентом 0,7 в сумме с тепловыделением через покрытие и фонари.

3.2.3.3. Тепловыделение от электродвигателей

Расчет тепловыделения от электродвигателей , Вт, производиться по формуле:



, Дж, (3.9)



где - суммарная номинальная мощность электродвигателей, кВт; - коэффициент, учитывающий использование установочной мощности двигателей, их загрузку по мощности, одновременность их работы, долю перехода механической энергии в тепловою.



Приближенно для электродвигателей, работающих с устройствами без принудительного жидкостного охлаждения ; для приводов станков с использованием эмульсии ; для двигателей, приводящих устройства с местными отсосами, .



3.2.3.4. Тепловыделение от печей

Расчет тепловыделения от печей , Вт, производиться по следующим формулам:



для печей, работающих на топливе:

, Дж, (3.10 а)



для электрических печей

, Дж, (3.10 б)



где - расход топлива, кг/ч;, - коэффициенты, учитывающие долю тепла, поступающую в помещение (см. таблицу 3. 16.); - теплотворная способность топлива, кДж/кг (таблица 3.17.); - коэффициент неполноты сгорания топлива, принимаемый равным ; - суммарная мощность электропечей, кВт.



*Таблица 3.16.*

|  |  |  |
| --- | --- | --- |
| **Вид оборудования, технологических процессов** | **Доля тепла, поступающего в помещение** | |
| при обогреве оборудования топливом, | при обогреве оборудования электричеством, |
| Индукционные печи плавки емкостью кг | - |  |
| Электродуговые печи плавки емкостью кг | - |  |
| Тигельные газовые печи |  | - |

*Таблица 3.17.*

|  |  |  |
| --- | --- | --- |
| **Топливо** | **Qтопл** | |
|  |  |
| Бутан | 12250 |  |
| Пропан | 91340 |  |
| Ацетилен | 47770 |  |
| Природный газ | 35620 |  |
| Мазут |  | 38970 |
| Условное твердое топливо |  | 29330 |
| Каменный уголь |  | 29330 |
| Кокс |  | 21780 |

3.2.3.5. Тепловыделения от источников искусственного освещения

Расчет тепловыделения от источников искусственного освещения , Вт, производиться по формуле:



, Дж, (3.11)



где - суммарная мощность источников освещения, кВт; - коэффициент тепловых потерь (для ламп накаливания, для люминесцентных ламп).



Для расчета тепловыделений от радиотехнических установок и устройств вычислительной техники используется аналогичная формула, в которой для радиотехнических устройств и для устройств вычислительной техники.



3.2.4. Определение потребного воздухообмена

Необходимый расход воздуха определяется вредными факторами, вызывающими отклонения параметров воздушной среды в рабочей зоне от нормируемых (поступление вредных веществ, влаги, избытков тепла).

3.2.4.1. Потребный воздухообмен при поступлении вредных веществ в воздух рабочей зоны

В помещения, загрязненных вредными парами, газами или пылью, количество воздуха , необходимого для разбавления концентрации вредных веществ до допустимых, рассчитывают по формуле:



, /ч**,** (3.12)



где - количество вредных веществ, выделяющихся в помещении за 1 час, мг/ч; , - концентрация вредных веществ в приточном и удаляемом воздухе, .



Концентрация принимается равной предельно допустимой для рассматриваемого вредного вещества.



При одновременном выделении в воздух рабочей зоны нескольких вредных веществ, не обладающих однонаправленным действием, потребный воздухообмен следует принимать по тому вредному веществу, для которого требуется подача чистого воздуха в наибольшем количестве.

В тех случаях, когда происходит одновременное выделение нескольких вредных веществ однонаправленного действия, расчет общеобменной вентиляции выполняется путем суммирования количеств воздуха, необходимого для разбавления каждого вещества до его предельно допустимой концентрации .



3.2.4.2. Воздухообмен, обеспечивающий удаление избытков тепла

В помещения со значительными тепловыделениями объем приточного воздуха, необходимого для поглощения избытков тепла, , ч**,** рассчитывают по формуле:



, /ч**,** (3.13)



где - теплоизбытки, Вт; - массовая удельная теплоемкость воздуха (); - плотность приточного воздуха (); , - температура удаляемого и приточного воздуха °С.



Температуры приточного воздуха принимаются по СНиП-П-33-75 для холодного и теплого времени года. Температура удаляемого воздуха определяется по формуле:

, (3.14)



где - температура в рабочей зоне по ГОСТ 12.1.005-76; - нарастание температуры на каждый 1 м высоты, °С / м; - высота помещения, м.



Величина в зависимости от тепловыделения °С/м.



3.2.4.3. Определение потребного воздухообмена при наличие избытков влаги

Расчет расхода воздуха , /ч, ведется по формуле:



, /ч**,** (3.15)



где - количество водного пара, выделяющегося в помещении, г/ч; , - влагосодержание вытяжного (принимается равным предельно допустимому) и приточного воздуха, г/кг, определяется по температуре и относительной влажности воздуха из диаграммы; - плотность приточного воздуха, .



При одновременном выделении вредных веществ, тепла и влаги сравниваются соответствующий воздухообмены, потребные для их удаления, и выбирается из них наибольший.

3.2.5. Расчет устройств местной вентиляции, устанавливаемых на рабочих местах

3.2.5.1. Воздушное душирование

Воздушное душирование следует применять, когда на работающего воздействует лучистая теплота с интенсивностью 350 Вт/ и более.



Нормы температуры °С, и скоростей , м/с, воздушного душирования для работ средней тяжести приведены в таблице 3.18., полученные данные для всех категорий работ даны в Санитарных нормах проектирования промышленных предприятий СН 245-71 и ГОСТ 121.005-76 “Воздух рабочей зоны”.



*Таблица 3.18.*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Тепловое**  **облучение** | **Период года** | | | | | | | |
| Теплый (температура наружного воздуха +10°С и выше) | | | Холодный и переходный (температура наружного воздуха ниже +10°С) | | | |
| , °С | , м/с | | , °С | | , м/с |
| 350...700 | 21...23 | | 0,7...1,5 | 21...22 | 0,7...1,0 | | |
| 700...1400 | 20...23 | | 1,5...2,0 | 20...21 | 1,0...1,5 | | |
| 1400...2100 | 19...21 | | 1,5...2,5 | 19...20 | 1,5...2,0 | | |
| 2100...2800 | 18...21 | | 2,0...3,5 | 19...21 | 2,0...2,5 | | |
| более 28000 | 18...190 | | 3,0...3,5 | 19...21 | 2,0...25 | | |

Душирующий воздух подается на рабочее место приточными патрубками. Патрубки необходимо устанавливать на такой высоте, чтобы они создавали хорошее обдувание приточным воздухом верхней части туловища человека и не затрудняли нормальную эксплуатацию оборудования.

На рабочее место воздух может подаваться или горизонтально, или сверху по углом 45°. Расстояние от выходного патрубка до рабочего, обслуживающего установку, должно быть не менее 1 метра. Расчет душирующего патрубка ведется но следующей схеме:

Первоначально определяется отношение разности температур :



,(3.16)



где , и – температура в рабочей зоне, нормируемая температура воздуха на рабочем месте и температура воздуха на выходе из душирующего патрубка.



При для достижения достаточно адиабатного охлаждения воздуха, при требуется искусственное охлаждение.



В задачу расчета воздушного душа входит определение необходимой скорости воздуха на выходе из патрубка и площади выходного сечения патрубка .



При значение определяется по формуле:



, м2**,** (3.17 а)



где - расстояние от душирующего патрубка до рабочего места, м; - опытный коэффициент, характеризирующий изменение температуры по осу струн (для патрубков типа ППД )



При в пределах от до расчет ведет по формуле:



, м2**,** (3.17 б)



Скорость воздуха на выходе из патрубка , определяется как:



, м/с(3.18)



где - скорость ветра на рабочем месте (нормируемая) м/с. По значениям и определяется расход воздуха через патрубок:



, (3.19)



3.2.5.2. Воздушный зонт

Воздушный зонт представляет собой металлический колпак, расположенный над источником вредных выделений. Сечение всасывающего отверстия колпака должно иметь форму, геометрически подобную горизонтальной проекции зеркала вредных выделений.

Размер каждой из сторон всасывающего сечения колпака определяется по формуле:



, м2**,** (3.20)



где - размер стороны (или диаметра) зеркала выделений вредностей, м; - расстояние от поверхности источника выделения до приемного отверстия колпака, м. Минимальное значение определяется удобством работы при конкретном технологическом процессе.



Для равномерности всасывания угол раскрытия колпака следует принимать не менее 60°.

Объем удаляемого воздуха , ч, определяется по формуле:



, ч, (3.21)



где - площадь приемного отверстия колпака;



- средняя скорость ветра в приемном отверстии зонта, м/с (данные о значениях приведены в таблице 3.19.).



*Таблица 3.19.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Число открытых сторон зонта** | **4** | **3** | **2** | **1** |
| Скорость воздуха , м/с |  |  |  |  |

Часто зонты устанавливают у загрузочных отверстий печей. В этом случае размер зонта у загрузочного отверстия печи должен соответствовать размерам вырывающейся свободной струи с учетом ее искривления под действием гравитационных сил.

Вылет зонта рассчитывают по формуле:



, м, (3.22)



где - высота загрузочного отверстия печи м.



Ширину зонта необходимо принимать на м больше ширины загрузочного отверстия. Зонт необходимо устанавливать на уровне верхней кромки окна. Для зонтов, расположенных над нагретыми поверхностями, объем воздуха в теплой струе, поднимающейся над источником, равен:



, ч, (3.23)



где - количество тепла, удаляющегося за счет конвекции, Вт; -горизонтальная проекция источника тепловыделения, ; - расстояние от плоскости тепловыделения до приемного отверстия зонта, м.



3.2.5.3 Вытяжные шкафы

Вытяжные шкафы создают укрытия источника вредных выделений со всех сторон. Для наблюдения за работой в шкафу имеется рабочие проемы, закрываемые подвижными шторками. Вытяжные шкафы с механической тягой устраивают с верхним отсосом, с нижним отсосом и комбинированные.

Объем отсасываемого из шкафа воздуха рассчитывается по формуле:

, ч, (3.24)



где - площадь рабочих проемов шкафа ; - средняя скорость воздуха в рабочих проемах шкафа, м/с.



Рекомендуемые значения в зависимости от характера работ приведены в таблице 3.20.



*Таблица 3.20.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Характер технологического процесса** | | | **Средняя скорость движения воздуха в рабочем проеме вытяжного шкафа, м/с** | |
| Обезжиривание мелких деталей | | |  | |
| Лужение | | |  | |
| Растворение кислот, щелочей, солей: | | |  | |
|  | холодные растворы |  | |
|  | нагретые растворы |  | |
| Кадмирование цианистое или серебрение | |  | |
| Свинцование | |  | |
| Травление | |  | |
|  | азотной кислотой |  | |
|  | соляной кислотой |  | |
| Хромирование | |  | |
| Цинкование цианистое | |  | |
| Пайка свинцом или третником | |  | |
| Лабораторные работы | |  | |

При наличие в шкафу теплового источника (печи, горелки), объем удаляемого воздуха, ч, определяется по формуле:



, ч, (3.25)



где - высота рабочих проемов шкафа, ч; - количество тепла, выделяемое внутри шкафа, Вт.



3.2.5.4 Отсасывающие панели

Отсасывающие панели применяются для удаления вредных выделений, увлекаемых конвективными потоками, в том числе, когда зона вредных выделений относительно велика и более полное укрытие организовать трудно. Отсасывающие панели следует применять при сварке, пайке, выдувке стекла, при удалении нагретых газов и пыли.

Расход воздуха через панель, , ч, вычисляется по формуле:



,, ч, (3.26)



где - коэффициент, зависящий от конструкции панели и ее расположения относительно источников тепла; – конвективная составляющая источника тепла, Вт.; - расстояние от верха плоскости до центра всасывающих отверстий панели, м.; - ширина источника тепла, м.



Коэффициент принимается равным для панелей:



тип 1 (односторонняя панель)



тип 2 (панель с экраном)



3.2.5.5. Бортовые отсосы

Бортовой отсос является основным местным отсосом от ванн в гальванических и травильных цехах и участках. В настоящее время распространение получили бортовые отсосы обычные и опрокинутые, каждый из которых может быть активирован поддувом воздуха (отсос с передувкой). Бортовые отсосы располагают с одной стороны ванны (однобортные отсосы) или с двух ее сторон (двубортные отсосы).

3.2.6. Разработка программной документации

На АРС “Охрана труда: компьютерное моделирование местной вентиляции” должен быть разработан документ “Руководства оператора” (Р. МИРЭА.00003-01 34 01).

Документ оформляется в соответствии с ГОСТ 19.505-79 и должен содержать следующие разделы:

назначение программы;

условия выполнения программы;

выполнение программы;

сообщения оператору.

Руководство должно содержать сведения, необходимые для обеспечения процесса интерактивного взаимодействия пользователя с АРС, и позволять облегчение процесса освоения разработанной АРС.

3.2.7. Результаты опытной эксплуатации системы и технические предложения по её развитию

В ходе опытной эксплуатации по методике представленной в Приложении 5 был сделан вывод, что система удовлетворяет требованиям заказчика.

В целом разработанная система вполне может быть использована как кафедрой “Охрана труда” в качестве дополнительного обучающего средства при выполнении студентами лабораторных работ, так и сотрудниками отделов ОТ на предприятиях.

АРС “Охрана труда” на следующих этапах разработки может быть расширена за счет дополнительных расчетных и информационных модулей, охватывающих другие направления ОТ производства, или за счет предоставления возможности выбора методик для существующих расчетов. Кроме того, АРС может быть дополнена развернутой диагностикой ошибок пользователя при вводе данных, а также модулем пояснения пользователю того, как был получен каждый конкретный результат, при желании с выдачей промежуточных результатов.

3.3. Автоматизированная обучающая система по курсу экономики

3.3.1. Постановка задачи и ее спецификация

Разрабатываемый модуль должен обеспечивать расчет одной из следующих неизвестных величин:

1) Приведенная стоимость;

2) Наращенная стоимость;

3) Длина интервала наращения;

4) Эффективная годовая ставка;

5) Интенсивность роста;

6) Коэффициента дисконтирования;

7) Коэффициента наращения.

Необходимо обеспечить удобство работы с программой пользователю, не являющемуся программистом. Модуль также должен удовлетворять требованиям, предъявленным при интегрировании его в состав целостного продукта.

Обучение пользователя желательно проводить на рабочих местах, что позволяет снизить затраты и повысить эффективность обучения и контроля. Наиболее удобным в этом случае является использование ПЭВМ, установленных на рабочих местах обучаемых. В настоящее время ПЭВМ все шире используется в самых различных областях человеческой деятельности. Это привело к тому, что большинство государственных предприятий и частных фирм имеют в своем распоряжении рабочие места с установленными на них ПЭВМ. За использование ПЭВМ также говорит и то, что малые ЭВМ серии СМ, которые также можно рассматривать в качестве технического средства для реализации, не удовлетворяют пользователя по скорости работы и отсутствию удобства в интерфейсе. С другой стороны, использование больших супер-ЭВМ, обладающих высокой скоростью обработки данных, также является нецелесообразным из-за дефицита машинного времени и вычислительных ресурсов, разделяемых между задачами большой важности и срочности.

Кроме того, следует принять во внимание психологический аспект использования персональных ЭВМ, находящихся в подразделениях, особенно человеком, по роду профессиональных занятий не связанному с вычислительной техникой, гораздо проще, чем посещение занятий на специализированном стенде, где техника отделена от пользователя и общение с ней происходит через операторов и системных программистов.

По мнению разработчиков, сказанное выше является достаточным основанием для выбора профессиональной ПЭВМ в качества аппаратных средств. Это позволяет реализовать диалоговый режим реального времени, работу с цветными панелями и меню, использование звуковых эффектов и тому подобное.

Также в соответствии с требованиями к системе, изложенными выше, были выбраны и программные средства для разработки системы. Было решено проводить разработку в системе MSM Workstation 2.0 Пользовательский диалог в стиле Windows знаком многим пользователям ПЭВМ, удобен в работе , требует распространенной среды MS Windows, не требует для своей работы мощных аппаратных средств.

Более подробно требования к аппаратным средствам сформулированы ниже:

* персональная ЭВМ, совместимая с IBM PC AT с тактовой частотой процессора не ниже 40 МГц;
* наличие цветного графического адаптера VGA;
* оперативная память не менее 16 МБайт;
* наличие операционной системы MS Windows 95 и выше.
* наличие жесткого диска и дисководов для 3.5” флоппи-дисков.

3.3.2. Обоснование проектных решений

3.3.2.1. Анализ при постоянной интенсивности наращения

Модель непрерывного начисления процентов

В банковской практике — особенно при электронных методах производства и регистрации финансовых операций - проценты могут начисляться за 1 сутки или даже за несколько часов. Например, коммерческий банк, находящийся в Москве, может одолжить определенную сумму денег банку, находящемуся во Владивостоке, на 12 часов — с 20 часов сегодняшнего дня до 8 часов следующего дня по московскому времени. За счет разницы во времени Владивостокский банк может добавить эти деньги к своему фонду краткосрочных ссуд, а затем вернуть долг с определенным процентом (или долями процента) к началу работы московского банка. Очевидно, что в этом и другом аналогичных случаях возникает задача начисления процентов за очень малые промежутки времени, т.е. по существу речь идет о непрерывном начислении процентов и их непрерывной капитализации.

При анализе инвестиций также возникает аналогичная задача, поскольку многие производственные и экономические процессы непрерывны по своей природе и такой же должна быть соответствующая им финансовая модель. В главах 1 и 2 мы построили несколько моделей начисления процентов при различной длине периода начисления (конверсионного периода) — от 1 дня до 1 года. Устремляя длину периода начисления к 0, построим теперь математическую модель непрерывного начисления процентов, рассмотрим способы практического применения непрерывной модели, а также сравним результаты дискретного и непрерывного начисления процентов. Для краткости иногда говорят "непрерывные проценты" , имея в виду непрерывное начисление и капитализацию процентов, т.е. бесконечно малый период начисления.

Постоянная интенсивность наращения

Примем за базовый период 1 год и обозначим целое число периодов начисления за год через т, а длину периода начисления через h = 1/т лет, m = 1,2,3,... . Тогда соответствующая положительная годовая ставка, и в силу формулы она связана с эффективной годовой ставкой.

Для простоты обозначим i — номинальная процентная ставка за один период начисления длиной h лет. Тогда из при h = m = 1 получаем

Для практики эффективную годовую ставку удобнее обозначать просто i.

Сделаем небольшое математическое пояснение. Для этого запишем коэффициент А(h) наращения эа любой период

(t, t + h) длиной h = 1/m на рассматриваемом интервале (О, T) в виде

Поскольку h мало, то различие между простыми и сложными процентами пренебрежимо мало. Так как A(0)=1, то— приращение 1 ден. ед. за малое время h (рис. 9.1, где h и т измеряются в годах).

Если А(т) дифференцируема в точке 0 справа, то

где g — угол наклона касательной к А(т) в точке т = 0.Из определения рассматриваемых ставок и результатов п. 2 § 8 следует, что если эффективная ставка i фиксирована, то номинальная ставка, при т —>  и h = 1/т —> О монотонно убывает, оставаясь положительной. Поэтому существует положительное предельное значение, которое мы обозначим через: W.

ОПРЕДЕЛЕНИЕ. Предел 6 номинальной ставки W при т —> называется силой роста или интенсивностью наращения за год при непрерывном начислении процентов. Величину 8 можно назвать также номинальной годовой ставкой при непрерывном начислении процентов.

ТЕОРЕМА 3.1. Эффективная годовая ставка i и номинальная годовая ставка связаны соотношением

Доказательство. В курсе "Алгебра и начала анализа" доказывается, что

е = 2,718282 ... — замечательное число Эйлера (основание натуральных логарифмов). Поэтому в нашем случае

СЛЕДСТВИЕ.Справедлива и следующая двойственная к теореме 3.1

ТЕОРЕМА 9.2. Эффективная годовая ставка d дисконтирования и номинальная годовая ставка связаны соотношением

Для доказательства достаточно перейти к пределу в (3.7) при, использовав при этом вышеприведенные формулы.Формула (3.6) и соотношение и (3.2) позволяют составить таблицу 3.21, иллюстрирующую связь для нескольких значений i от 0,01 до 2) и при малых 1 до 0,10 достаточно близки. Однако с ростом 1" различие между тремя эквивалентными ставками быстро растет.

*Таблица 3.21.*

|  |  |  |
| --- | --- | --- |
| D | G | I |
| 0,00990 | 0,00995 | 0,01 |
| 0,04761 | 0,04879 | 0,05 |
| 0,09091 | 0,09531 | 0,10 |
| 0,16667 | 0,18232 | 0,20 |
| 0,20000 | 0,22314 | 0,25 |
| 0,33333 | 0,40547 | 0,50 |
| 0,42857 | 0,55962 | 0,75 |
| 0,50000 | 0,69315 | 1,00 |

Пример 3.1. Найдем наращенное за 5 лет значение суммы S(0)=10 руб., если оно реинвестируется по постоянной ставке = 25% при следующих значениях m:

а) 1 раз в год,

б) 2 раза в год,в) непрерывно.г) Вычислим g для непрерывного начисления процентов.

Пример 3.2. Найдем коэффициент наращения A(т) за т = 1 год при реинвестировании по постоянной ставке = 1 ежегодно, ежеквартально, ежемесячно, ежечасно ежеминутно и непрерывно. Вычислим для каждого из случаев.

*Таблица 3.22.*

|  |  |  |  |
| --- | --- | --- | --- |
| Период начисления | m | A(1)=(1+1/m)m | iэф = A(1)-1 |
| Ежегодное  Ежеквартальное  Ежемесячное  Ежедневное  Ежечасное  Ежеминутное  Непрерывное | 1  4  12  360  8640  518400 | (1+1/1)1 =2  (1+1/4)4 =2,441406  (1+1/12)12 =2,613035  (1+1/360)360 =2,714516  (1+1/8640)8640 =2,718125  (1+1/518400)51840=2,718276  e=2,718282 | 1  1,441406  1,613035  1,714516  1,718125  1,718276  1,718282 |

Функциональная связь между любыми парами из основных параметров

В зависимости от условий задачи может оказаться удобным принять один из четырех основных параметров i, v и d за исходный и выразить через него значения трех остальных. В табл. 3.3 объединены ранее полученные соотношения.

Каждая строка этой таблицы показывает, как параметр, стоящий в обозначении этой строки, выражается через три остальные. Каждый столбец таблицы показывает, как через параметр, стоящий в обозначении этого столбца, выражаются три остальные.

Приближенная связь между основными параметрами

Из теории рядов известно, что при малых х с точностью до членов третьего порядка малости включительно

Подставляя первую из этих формул в (3.4), а вторую — в (3.6) и пренебрегая членами третьего порядка, получим, что при i или не более 0,10-0,20 можно пользоваться приближенными соотношениями: Аналогичным образом из формулы для суммы бесконечного числа членов сходящейся прогрессии следует, что при малых i

Этими приближенными формулами можно пользоваться для ориентировочных расчетов. Однако в финансовой практике надо пользоваться калькулятором или таблицами даже при малых i и

Коэффициенты наращения и дисконтирования при непрерывном наращении процентов

Предположим, что в настоящий момент tо производится инвестиция в сумме S(tо) по постоянной эффективной годовой ставке i. Тогда в силу формулы (3.5) для сложных процентов наращенная к моменту t = tо + т сумма АV1 составит

где время измеряется в годах, а i и g = ln(1+i) — десятичные дроби.

Если же нам предстоит в будущий момент t > tо уплатить или получить сумму S(t), то ее современная приведенная стоимость РV в настоящий момент tо составит

Итак, нами доказана следующая важная

ТЕОРЕМА 3.3. При постоянной эффективной годовой ставке i к номинальной годовой ставке ln(1 + i) коэффициент наращения зависит лишь от длины т интервала наращения, измеренной в годах, и составляет

Коэффициент дисконтирования за т лет равен

Заметим теперь, что А(т) — коэффициент наращения 1 ден. ед. на интервале (tо, tо + т} при движении по этому интервалу слева направо, т.е. в положительном направлении.

Равенство можно интерпретировать как отрицательное наращение, совпадающее с дисконтированием, поскольку движение по интервалу (t, t + т) происходит справа налево, т.е. в отрицательном направлении. Аналогичным образом интерпретируется равенство

Следовательно, в рассматриваемом случае коэффициенты наращения и дисконтирования взаимозаменяемы и с математической точки зрения можно было бы пользоваться только одним из них. Однако для наглядности удобнее пользоваться двумя коэффициентами в соответствии с прямым содержательным смыслом каждого из них.

Таким образом, как при дискретном, так и при непрерывном начислении сложных процентов справедливо фундаментальное соотношение

В частности, при т = 1 получаем из ранее установленных соотношений

Заметим теперь, что если функцию е задать на интервале то [-;+] при т > 0 она совпадает с А(т), а при т < 0 — с v(т):

При этом А'{0) — интенсивность наращения за базовую единицу времени.

Пример 3.3. Сумма 2000 долл. положена в банк под схему непрерывного начисления процентов с постоянной интенсивностью роста 10% за год. Найдем наращенную в конце года t сумму S(t) при t= 1, 2, 3, 5 и 10.

Решение. Здесь S(t) = 2000е, и ответ содержится в таблице 3.23.

*Таблица 3.23.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| t, лет | 0 | 1 | 2 | 3 | 5 | 10 |
| S(t), $ | 2000 | 2210,34 | 2442,81 | 2699,72 | 3297,44 | 5436,56 |

Пример 3.5. Заемщик В должен уплатить кредитору А по векселю1000 долл. на 01.01.96, 2500 долл. на 01.01.97, 3000 долл. на 01.07.97.Найдем современную стоимость долга С(t) на моменты:а) 01.01.94 и б) 01.04.95 при = 0,06 за год.

3.3.2.2. Анализ при переменной интенсивности наращения

Описание модели и основная теорема

В настоящее время в мире действует много электронных бирж, связанных в единую мирону ю систему с несколькими центрами — в Нью-Иорке, Лондоне, Франкфурте и Токио. По существу, финансовые операции производятся круглые сутки, много раз за одну секунду. Поэтому даже за минуту на электронной бирже происходят колебания взаимных курсов основных валют, акций, облигаций и т.д. Эти колебания обычно небольшие, но наряду с интервалами относительной стабильности могут появляться и интервалы с устойчивой тенденцией к понижению (отрицательный тренд) или повышению (положительный трена) курса тех или иных денежных инструментов, а иногда происходят скачки курса. Возникает много сложных и интересных проблем, связанных с анализом и прогнозированием курса валют и связанных с ним курсов ценных бумаг. Все это оказывает влияние и на процентные ставки по обыкновенным вкладам и депозитам, которые также изменяются, хотя и не так часто, как валютный курс.

В качестве примера на рис. 10.1 приводится график среднемесячного дохода в процентах по вкладам в облагаемые налогами взаимные фонды денежного рынка США за 1975-1986 гг., заимствованный из [7]. Взаимные фонды денежного рынка (рис. 10.2) распределяют доходы от своих активов среди акционеров. Поэтому доходы акционеров увеличиваются или уменьшаются в зависимости от изменения годовых процентных ставок на краткосрочные ценные бумаги, в которые взаимные фонды вкладывают свои средства.

Период бурного роста активов взаимных фондов (от менее 10 млрд. долл. в 1974 г. до более 200 млрд. долл. в 1981 г., см. рис. 10.2) связан с резким подъемом до 12-16% ставок годового дохода в конце 70-х — начале 80-х годов.

Поэтому необходимо иметь аналитическую модель, в которой 6 и, следовательно, все другие процентные ставки зависят от времени. С этой целью рассмотрим коэффициент А(t, t + h) наращения на интервале (t, t + h) и примем

Здесь ih(t) — мгновенное значение в момент t годовой номинальной процентной ставки, которая зависит не только от длины Д интервала наращения, но и от момента t его начала. Поэтому коэффициент наращения А(t, t + h) также зависит теперь не только от hг, но и от t. Примем, что при всех t в рассматриваемом интервале существует предел

где (t) — мгновенное значение интенсивности роста за базовую единицу времени (обычно 1 год) в момент t. Из (3.12), (3.12) следует, что

Здесь означает производную по второму аргументу функции A(t, w) в точке w = t при произвольном, но фиксированном t.

Можно доказать, что справедлива следующая фундаментальная теорема.

ТЕОРЕМА 3.11. Примем, что (t) и А(tо,t) — непрерывные функция времени при и что в этом интервале выполняется принцип стабильности рынка. (4.7).

3.3.3 Разработка программной документации

Анализ непрерывного начисления процентов и непрерывного дисконтирования включает следующие блоки:

Расчет параметров непрерывного начисления процентов и непрерывного дисконтирования;

3.3.4. Результаты опытной эксплуатации игры и технические предложения по ее развитию

Модуль анализа непрерывного начисления процентов и непрерывного дисконтирования был разработан в полном объеме и отлажен по тестовым примерам расчетов.

Также по итогам опытной эксплуатации модуля разработчиками были сформулированы технические предложения по развитию системы, представленные ниже.

Программный комплекс должен в будущем создаваться совместными усилиями всех студентов, что объясняется схожими потребностями будь то предприятие, общественная организация, медицинское учреждение или учебное заведение, а также пожеланиями консультанта.

Структура программного комплекса должна определяться требованиями Заказчика, спецификой предметной области и задачами, которые должен решать этот программный комплекс, в том числе:

* представлять теоретические сведения;
* в интерактивном режиме запрашивать необходимые исходные данные, производить расчеты и немедленно выводить результаты, что позволит изменяя значения параметров, определять зависимости;
* создать "дружественную" среду работающему пользователю, оставляя возможность в любой момент прекратить сеанс диалога с программой, предлагая производить необходимые действия в удобной для того форме, блокируя неразрешенные манипуляции, сопровождая работу постоянной помощью в виде подсказок и меню.

Одни из выше перечисленных функций должны быть реализованы отдельными программными модулями, другие реализуются параллельно другими модулями.

С учетом вышесказанного структура предполагает наличие следующих компонент:

* модуль главного меню;
* модуль ввода параметров системы;
* модуль расчета непрерывного начисления процентов и непрерывного дисконтирования;
* модуль вывода расчетных значений;
* модуль работы с выходными данными в аналитическом виде;