**ООО «ИНФОУРОК»**

**ОТЧЕТ ПО ПРАКТИКУМУ**

слушателя дополнительной профессиональной программы профессиональной переподготовки

**УПРАВЛЕНИЕ И АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫМИ СЛУЖБАМИ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ**

Разработал: \_\_\_\_\_\_\_\_\_\_\_\_\_

ФИО слушателя

Город, 20\_\_\_

**СОДЕРЖАНИЕ**

Введение……………………………………………………………...……………3

1. Анализ состояния системного администрирование ООО ПК «Венткомплекс»……………………………………………………………5
   1. Системное администрирование. Изучение технических и программных средств компьютерного обеспечения………………….5
   2. Изучения уровня администрирования инфокоммуникационных систем организации……………………………………………………..8
   3. Оценка эффективности использования технических и программных средств.…………………………………………………………………11
2. Анализ администрирования и эксплуатации аппаратно-программных средств инфокоммуникационных систем организации; анализ обеспечения защищенности компьютерных систем от вредоносных воздействий ООО ПК «Венткомплекс»………………………………….12
   1. Правила, регламенты и стратегия администрирования в ИС……….12
   2. Выполнение работ по проектированию сетевой инфраструктуры…13
   3. Функциональные области системного администрирования………..14
   4. Состав служб администратора системы и их функции. Требования к специалистам служб администрирования ИС……………………….15
   5. Управление доступом к программно-аппаратным средствам администрируемой сети……………………………………………….16
   6. Организация инвентаризации технических средств………………...17
   7. Правила маркировки устройств и элементов инфокоммуникационной системы……………….……………….……………….………………18
   8. Основы проектирования инфокоммуникационных систем…………19
   9. Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе……………...20
   10. Операционные системы. Службы управления доступом………..22
   11. Кабельные и сетевые анализаторы………………………………...23
   12. Диагностика отказов и ошибок сетевых устройств и программного обеспечения……………………………………………………………24
   13. Методы и технологии повышения производительности сети…..25
   14. Основные средства криптографии………………………………...27
   15. Классификация операционных систем согласно классам безопасности. Профиль защиты………………………………………29
   16. Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных……….31
3. Разработка предложений по автоматизации администрирования инфокоммуникационной системы и эксплуатации аппаратно-программных средств, улучшения использования ресурсов обеспечению защищенности компьютерных систем от вредоносных воздействий и повышения производительности………………………………………...34

Заключение……………………………..………………………………………...39

Список использованных источников и литературы……………………………40

**Введение**

Производственная практика является важным этапом подготовки квалифицированных специалистов.

Основной целью производственной практики является закрепление теоретических знаний по курсу и смежных с ним дисциплин, приобретение практических навыков в области разработки программного обеспечения, внедрение специализированного программного обеспечения на предприятии, администрирование корпоративной базы данных, а также администрирование локальной вычислительной сети.

Основные задачи прохождения производственной практики можно сформулировать так:

- закрепление теоретических знаний, полученных в высшем учебном заведении;

- изучение технологии и организации деятельности предприятия;

- ознакомление с технической оснащённостью предприятия;

- изучение аппаратных и программных компонент локальной вычислительной сети и приобретение практических навыков их применения;

- приобретение опыта работы с технологической документацией;

В изучение также входит:

- общее знакомство с предприятием;

- изучение основных технико-экономических показателей;

- изучение основных проектных решений по автоматизации управления предприятием;

- изучение передовых технологий сбора, передачи, обработки, хранения и выдачи информации;

- изучение структуры и особенностей работы информационного отдела на конкретном предприятии.

Объект исследования: ООО ПК «Венткомплекс».

1. Анализ состояния системного администрирование ООО ПК «Венткомплекс»
   1. Системное администрирование. Изучение технических и программных средств компьютерного обеспечения

Юридический адрес: город 427629, республика Удмуртская, город Глазов, улица Куйбышева, дом 77 строение 1, кабинет 111.

**Миссия компании** — это комплексное оснащение вентиляционно-отопительным оборудованием строящихся зданий и сооружений, промышленных, социальных, спортивных, сельскохозяйственных объектов на территории Российской Федерации и стран СНГ.

**ООО** ПК **«ВентКомплекс»** имеет огромный опыт работы в области вентиляции и выполняет весь комплекс работ по проектированию, поставке, монтажу и гарантийному обслуживанию систем вентиляции и кондиционирования воздуха в бытовых, офисных и промышленных помещениях.

ООО ПК **«ВентКомплекс»** осуществляет прямые поставки климатического оборудования от ведущих европейских и российских производителей, а также имеет собственное производство вентиляционного оборудования из импортных комплектующих, что позволяет вести гибкую ценовую политику.

Программное обеспечение (ПО), применяемое на предприятии, классифицируется по назначению и виду. По назначению ПО подразделяется на прикладное, системное и специализированное. Программы по виду подразделяются на комплексы и компоненты

Главной задачей сервисной службы ООО **«ПК ВентКомплекс»** является программное и техническое обеспечение деятельности основных и вспомогательных подразделений компании.

Область деятельности сервисной службы включает:

- программное и техническое обеспечение работы серверов (файловые хранилища, СУБД, почтовые системы, контроллеры домена, информационные и справочные ресурсы, системы контроля и ограничения доступа) и рабочих станций пользователей;

- обеспечение доступа компании к глобальной сети Интернет;

- организация и обеспечение работы информационно-технологических Интернет-ресурсов;

- обеспечение информационной безопасности (в том числе, персональных данных);

- техническое обслуживание и организация ремонта вычислительной и орг. техники;

- обеспечение компьютерной и оргтехникой ООО **«ПК ВентКомплекс»;**

- организация функциональных рабочих мест сотрудников;

- контроль за лицензированием используемого программного обеспечения.

Рассмотрим техническую архитектуру на предприятии (рисунок 1).

Видно, что данные предприятия хранятся на группе серверов (серверная ферма). На этих серверах организована работа почтового сервера, прокси-сервера, веб-сервера, а также файлового сервера.



Рисунок 1 – Техническая архитектура предприятия ООО **«ПК ВентКомплекс»**

Программная архитектура предприятия ООО **«ПК ВентКомплекс»** представлена на рисунке 2.

Рисунок 2 - Программная архитектура предприятия ООО **«ПК ВентКомплекс»**

Среди облачных технологий, организация отдает предпочтение разработке российской компании «Mail.Ru Group» под названием «Облако Mail.Ru» - почтовый сервис и набор офисных приложений для редактирования документов и хранения файлов в облаке.

Для организации видеоконференций используется программный продукт «Skype». Он обеспечивает высокое качество связи при организации интернет-видеоконференций на персональных компьютерах и обычных интернет-каналах.

* 1. Изучения уровня администрирования инфокоммуникационных систем организации

Объектами защиты информации на **ООО «ПК ВентКомплекс»** являются:

- жесткие диски серверов;

- финансовые отчеты, прогнозы, положение;

- условия оказания услуг;

- характеристика производимой и перспективной продукции;

- партнеры, клиенты и содержание договоров с ними;

- SAN;

- NAS;

- диски CD/DVD/Blue-ray;

- персональные компьютеры (в том числе ноутбуки);

- внешние устройства;

- система безопасности и, первую очередь, средства защиты конфиденциальной информации и т.д.

На **ООО «ПК ВентКомплекс»** применяют следующие средства защиты информации:

1. Средства защиты от несанкционированного доступа (НСД):

- Средства авторизации;

- Мандатное управление доступом;

- Избирательное управление доступом.

2. Системы анализа и моделирования информационных потоков (CASE-системы).

3. Системы мониторинга сетей:

- Системы обнаружения и предотвращения вторжений (IDS/IPS);

- Системы предотвращения утечек конфиденциальной информации (DLP-системы).

4. Антивирусные средства.

5. Криптографические средства:

- Шифрование;

- Цифровая подпись.

6. Системы резервного копирования.

7. Системы бесперебойного питания:

- Источники бесперебойного питания;

- Резервирование нагрузки.

8. Системы аутентификации:

- Пароль;

- Ключ доступа (физический или электронный);

Сертификат;

9. Средства предотвращения взлома корпусов и краж оборудования.

**ООО «ПК ВентКомплекс»** работает с 8:30 по 18:00.

**ООО «ПК ВентКомплекс»** использует на ПК антивирусные средства.

«Антивирус Касперского» — это программное решение для защиты компьютера от всех видов интернет-угроз. Характерный компонент антивирусной программы Касперского — так называемый «Безопасный браузер», обеспечивающий безопасность публичных сетей Wi-Fi, контроль интернет-трафика и защиту от несанкционированного подключения к веб-камере.

Антивирусом предусмотрено бесплатное автоматическое обновление и моментальный переход на новую версию.

На главном компьютере стоит система защиты информации от несанкционированного доступа - Dallas Lock, что позволяет обеспечивать защиту конфиденциальной информации на ПЭВМ путем разграничения полномочий пользователей по доступу к файловой системе и другим ресурсам.

Система резервного копирования и восстановления данных на предприятии реализована в виде программно – аппаратного комплекса «PBBA integrated systems». Такая система имеет большую интеграцию между аппаратурой и программным обеспечением, и могут включать дополнительные инструменты для работы с сетью.

В организации присутствуют средства архивации информации. На компьютерах используют архиватор ZIP, для операционных систем DOS и Windows. Очень важно установить постоянный график проведения работ по архивации данных или выполнять их после большого обновления данных.

Так же, на ПК каждого сотрудника стоит система парольной защиты.

Эффективным средством защиты, используемым для управления входом в систему по учетным записям пользователей, а также организации доступа к компьютерам и ресурсам является пароль.

* 1. Оценка эффективности использования технических и программных средств

Анализ уровня технической и программной оснащенности компании позволяет сделать вывод, что ООО «ПК Венткомплекс» является предприятием современного уровня, которое использует высококачественное серверное оборудование и средства, обеспечивающие контроль безопасности хранимых данных. Такое уровень информатизации предприятия способствует внедрению новых программных решений для улучшения бизнес-процессов компании.

1. Анализ администрирования и эксплуатации аппаратно-программных средств инфокоммуникационных систем организации; анализ обеспечения защищенности компьютерных систем от вредоносных воздействий ООО ПК «Венткомплекс»
   1. Правила, регламенты и стратегия администрирования в ИС

Вся стратегия администрирования должна быть первоначально построена на основе правил и регламентов.

Документально оформленные, доведенные до сведения всех сотрудников правила и регламенты необходимы для нормального функционирования любой организации.

В организации ООО ПК «Венткомплекс» следующие документы:

- правила административного обслуживания;

- регламенты прав и обязанностей пользователей;

- правила для администраторов (пользователей с особыми привилегиями);

- правила создания «гостевых» учетных записей.

В современных системах почти все стандартные задачи документированы в форме контрольных списков и инструкций. Написанием и поддержкой этих инструкций занимается дополнительная группа системных администраторов (не входящая в состав основного штата системных администраторов, обслуживающих технику и использующих эти инструкции). Тем не менее такая организация и стандартизация в конечном счете окупаются. В перечень таких регламентов входят:

- подключения компьютера;

- подключения пользователя;

- настройки и конфигурирования компьютера;

- установки библиотеки TCP-оболочек на компьютер;

- настройки резервного копирования для нового компьютера;

- защита нового компьютера;

- перезапуск сложного программного обеспечения;

- восстановления Web-серверов, которые не отвечают на запросы или не предоставляют данных;

- разгрузки очереди и перезагрузки принтера;

- модернизации операционной системы;

- инсталляции пакета прикладных программ;

- инсталляции программного обеспечения по сети;

- модернизации наиболее важных программ;

- резервные копирования и восстановления файлов;

- выполнение аварийной остановки системы (всех компьютеров; всех, кроме наиболее важных, компьютеров и т. д.).

Некоторые положения инструкций диктуются особенностями ПО, с которым вы работаете, либо правилами, принятыми в тех или иных сторонних группах, например у поставщиков услуг Интернета. Соблюдение некоторых положений является обязательным, особенно если вы должны обеспечить секретность данных пользователей. В частности, управление интернет-адресами, именами компьютеров, идентификаторами пользователей и групп, регистрационными именами должно осуществляться единообразно для всех компьютеров организации.

* 1. Выполнение работ по проектированию сетевой инфраструктуры

Сетевой инфраструктуре требуются соответствующие программные приложения или службы, которые должны быть установлены на компьютерах и регулировать трафик данных.

В большинстве случаев службы системы доменных имен (DNS) также являются протоколом обмена динамической конфигурации хоста (DHCP) и службы Windows (WINS), которые являются частью базового пакета услуг. Эти приложения должны быть настроены соответствующим образом и постоянно быть доступными.

В компании установлены три физических сервера, на которых, соответственно, работают три программных сервера.

Почтовый сервер работает под управлением ОС Debian 8. В качестве ПО почтового сервера применяется iRedMail.

iRedMail  – бесплатное «open source» решение для создания почтовых серверов. В отличие от ручной конфигурации и сборки из необходимых пакетов, требующей достаточно глубоких знаний linux-дистрибутивов, iRedMail позволяет сэкономить время при создании почтовых серверов.

Прокси и веб сервер работает также под управлением Debian 8. Также на сервере установлено ПО Apache 2.2, СУБД MySql 5.3 и поддержка языка php 5.0.4.

Файловый сервер работает под управлением Windows Server 2008, на котором установлено СУБД MS SQL 2008 R2, а также сервер 1С бухгалтерии.

Персональные компьютеры сотрудников работают под управлением Windows 10.

В качестве офисного пакета установлен MS Office 2013, который включает в себя весь набор необходимого офисного ПО для работы с документами.

Просмотр страниц глобальной сети интернет, а также подключение к серверу 1С происходят через веб интерфейс, который предоставляет браузер Google Chrome.

* 1. Функциональные области системного администрирования

Основной целью системного администрирования является приведение сети в соответствие с целями и задачами, для которых эта сеть предназначена. Достигается эта цель путём управления сетью, позволяющего минимизировать затраты времени и ресурсов, направляемых на управление системой, и в тоже время максимизировать доступность, производительность и продуктивность системы.

Функциональные области управления, относящиеся к системному администрированию, определены в спецификациях ISO, и ориентированы на:

- решение проблемных ситуаций (диагностика, локализация и устранение неисправностей, регистрация ошибок, тестирование);

- управление ресурсами (учёт, контроль использования ресурсов, выставление счетов за использованные ресурсы и ограничение доступа к ним);

- управление конфигурацией, направленное на обеспечение надёжного и эффективного функционирования всех компонентов информационной системы;

- контроль производительности (сбор и анализ информации о работе отдельных ресурсов, прогнозирование степени удовлетворения потребностей пользователей/приложений, меры по увеличению производительности);

- защита данных (управление доступом пользователей к ресурсам, обеспечение целостности данных и управление их шифрованием).

* 1. Состав служб администратора системы и их функции.Требования к специалистам служб администрирования ИС

IT отдел выполняет множество функций, для обеспечения комфортной работы сотрудников предприятия.

В штате IT сотрудников предприятия состоят специалисты разного профиля. Каждый специалист занят выполнением только своей задачи.

В составе отдела IT 4 человек:

1. Главный системный администратор;

2. Специалист по поддержке пользователей;

3. Разработчик базы данных;

4. Web – программист.

На системного администратора возлагается максимальная ответственность в информационной работе предприятия. Он следит за состоянием сервера, за нагрузкой на сервер. Так же в его обязанности входит регулярное архивирование данных, хранимых на серверах, архивация баз данных, так как вся документация и все операции предприятия хранятся на сервере.

Системный администратор является управляющим звеном в IT отделе, удаленно он может диагностировать проблему у пользователя на месте и уже послать туда специалиста по поддержке пользователей, дав ему конкретное задание для выполнения. Системный администратор организует антивирусную и информационную безопасность.

Специалист по поддержке пользователей – связующее звено между системным администратором и рядовым сотрудниками предприятия.

Специалист технической поддержки должен обладать коммуникабельностью, целеустремлённостью, быстрой обучаемостью, ответственностью, внимательностью. Часто в работе приходится осваивать новые программы и оборудование.

* 1. Управление доступом к программно-аппаратным средствам администрируемой сети

На предприятии существует как удаленная техническая поддержка – helpdesk, так и локальная техническая поддержка. Специалист по поддержке пользователей регистрирует обращения сотрудников, о проблемах возникающих у них в работе с компьютерами, офисным оборудованием и т.д. Ведет документацию, статистику по возникающим проблемам, для дальнейшего анализа и улучшения качества работы сотрудников. Так же специалист технической поддержки занимается установкой и обновлением программного обеспечения, ремонт и обслуживание компьютерной техники, наличие расходных материалов.

Web-программист разрабатывает и администрирует web-сайт предприятия, осуществляет SEO продвижение сайта предприятия в поисковых системах таких, как Google и Яндекс. Следит за тем, чтобы на сайте в новостном разделе присутствовала только самая свежая информация.

Определяет вместе с непосредственным руководителем цели и задачи проекта, разрабатывает удобный, с точки зрения навигации, интерфейс web-сервера, осуществляет администрирование web-сервера и операционной системы, под управлением которой работает web-сервер. Так же web-программист подготавливает предложения клиентам и партнерам для размещения рекламы на сайте. Обеспечивает защиту web сайта от угроз.

* 1. Организация инвентаризации технических средств

Инвентаризация — это сверка фактического наличия имущества с данными бухгалтерского учета.

Инвентаризация - сети — это учет всей компьютерной техники и программного обеспечения сети. Эта процедура просто необходима при планировании апгрейдов аппаратного обеспечения, добавлении новых рабочих мест или закупки дополнительных аппаратных или программных ресурсов.

Участвовала в инвентаризации рабочих станций и сетевого оборудования своего отдела.

Инвентаризация проводиться в компании раз в год.

Документооборот — это движение документов в организации с момента их создания или получения до завершения исполнения или отправки. В то же время, документация является неотъемлемой частью успешного бизнеса. При этом должны быть учтены юридический и коммуникативный аспекты.

Внутренние документы составляются, оформляются, исполняются и хранятся в рамках самого предприятия, не выходя за его пределы. На этапах подготовки и оформления порядок работы с ними такой же, как и с исходящими документами.

Разработка внутренней документации предприятия предусматривает создание должностных инструкций, приказов и решений. Кроме юридической безупречности, они должны быть четко сформулированы и однозначно истолковываться.

Принимал участие по формированию документации по проведенной инвентаризации. В ходе инвентаризации было выявлено:

- 11 единиц оборудования без инвентарных номеров;

- 5 единиц оборудования не хватает: 1 монитор, 1 принтер, 2 коммутатора, 1ситемный блок.

* 1. Правила маркировки устройств и элементов инфокоммуникационной системы

Маркировку выполняют любым способом. Способ и качество выполнения маркировки должны обеспечивать четкое и ясное изображение ее в течение срока службы СВТ в режимах и условиях, установленных в настоящем стандарте.

 На СВТ должна быть нанесена маркировка, содержащая:

- наименование или товарный знак предприятия-изготовителя (кроме СВТ, предназначенных на экспорт);

- шифр или условное наименование СВТ;

- порядковый номер СВТ по системе нумерации предприятия-изготовителя;

- дату изготовления (год и месяц);

- надпись «Страна-изготовитель» на русском или иностранном языке, установленном в договоре (контракте) внешнеторговой организации (для СВТ, предназначенных на экспорт).

Маркировка, информирующая о напряжении электропитания, частоте и потребляемом токе, - по ГОСТ 25861.

Маркировку вычислительных систем, комплексов и ЭВМ следует наносить на центральном процессоре или пульте управления в соответствии с ТУ на конкретные СВТ.

* 1. Основы проектирования инфокоммуникационных систем

Язык UML практически не зависим от организации процесса разработки, и его можно применять, например, при создании систем в рамках технологии, ориентированной на использовании главным образом каскадной модели жизненного цикла. Стадии и этапы работы согласно этой технологии описаны в действующем стандарте ГОСТ 34.601-90 (переиздание 01.09.2009).

Отметим те стадии, при реализации которых полезно бы использование тех или иных диаграмм UML (более подробно о диаграммах будет говориться в последующих лекциях). UML как язык специфицирования позволяет построить точные, недвусмысленные и полные модели. UML позволяет специфицировать все существенные решения, касающиеся анализа, проектирования и реализации, которые должны приниматься в процессе разработки и развертывания систем.

Стадия 1. Формирование требований к системе.

На этой стадии проектирования выделяют следующие этапы работ:

- обследование объекта и обоснование необходимости создания системы;

- формирование требований пользователей к системе;

- оформление отчета о выполненной работе и тактико-технического задания на разработку.

Стадия 2. Разработка концепции.

- изучение объекта автоматизации;

- проведение необходимых научно-исследовательских работ;

- разработка вариантов концепции системы, удовлетворяющих требованиям пользователей;

- оформление отчета и утверждение концепции.

Стадия 3. Техническое задание.

- разработка и утверждение технического задания на создание систем.

Стадия 4. Эскизный проект.

- разработка предварительных проектных решений по системе и ее частям;

- разработка эскизной документации на систему в целом и ее части.

Стадия 5. Технический проект.

- разработка проектных решений по системе и ее частям;

- разработка документации на систему и ее части;

- разработка и оформление документации на поставку комплектующих изделий;

- разработка заданий на проектирование в смежных частях проекта.

Для достижения сформулированных целей на первом этапе полезно построить модель в форме диаграммы вариантов использования (use case diagram), которая описывает функциональное назначение системы или, другими словами, то, что система будет делать в процессе своего функционирования. Диаграмма вариантов использования является исходным концептуальным представлением или концептуальной моделью системы в процессе ее проектирования и разработки.

При выборе объектно-ориентированного подхода к проектированию обязательной является диаграмма классов (class diagram), которая служит для представления статической структуры модели системы в терминологии классов объектно-ориентированного программирования. Диаграмма классов может отражать, в частности, различные взаимосвязи между отдельными сущностями предметной области, такими как объекты и подсистемы, а также описывает их внутреннюю структуру и типы отношений.

Следующей диаграммной, которая может быть построена, является диаграмма последовательности (sequence diagram). С помощью этой диаграммы описывают поведение взаимодействующих групп объектов. Как правило, для каждого случая (прецедента) составляется своя диаграмма последовательности. На диаграмме отображаются объекты, сообщения, которыми они обмениваются, и временная шкала обмена этими сообщениями. По горизонтали можно проследить последовательность возникновения сообщений. По вертикали для каждого объекта отображается набор входящих и исходящих сообщений в порядке их возникновения.

На заключительных этапах разработки могут быть реализованы диаграммы компонентов и развертывания. На диаграмме компонентов представляется организация совокупности компонентов и существующие между ними зависимости.

* 1. Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе:

- Основы обеспечения информационной безопасности;

- Нормативные правовые акты в области информационной безопасности;

- Инструкции по настройке устанавливаемого системного программного обеспечения, включая знания о типовых уязвимостях;

- Инструкции по эксплуатации устанавливаемого системного программного обеспечения, включая знания о типовых уязвимостях;

- Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе;

- Регламенты обеспечения информационной безопасности;

- Локальные правовые акты, действующие в организации;

- Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы.

* 1. Операционные системы. Службы управления доступом

Система управления доступом распределяет полномочия пользователей в сети, устанавливает права доступа к приложениям и файлам на основе шаблонов и правил. Основными компонентами системы являются:

- Разрешение на доступ;

- Таблица фактического доступа;

- Контроль удаленного доступа.

В компании установлены три физических сервера, на которых, соответственно, работают три программных сервера.

Почтовый сервер работает под управлением ОС Debian 8. В качестве ПО почтового сервера применяется iRedMail.

iRedMail  – бесплатное «open source» решение для создания почтовых серверов. В отличие от ручной конфигурации и сборки из необходимых пакетов, требующей достаточно глубоких знаний linux-дистрибутивов, iRedMail позволяет сэкономить время при создании почтовых серверов.

Прокси и веб сервер работает также под управлением Debian 8. Также на сервере установлено ПО Apache 2.2, СУБД MySql 5.3 и поддержка языка php 5.0.4.

Файловый сервер работает под управлением Windows Server 2008, на котором установлено СУБД MS SQL 2008 R2, а также сервер 1С бухгалтерии.

Минимальные требования:

Процессор: i486 или выше

Оперативная память: от 128 MB

Место на жёстком диске: от 2.5 GB

Сильные и слабые стороны Linux:

Сильные стороны:

– Некоммерческое распространение;

– Некоммерческое распространение большинства прикладного ПО;

– Низкие требования к аппаратным ресурсам;

– Высокое быстродействие системы;

– Высокая стабильность системы (система может работать годами без выключения и вмешательства человека);

– Высокая безопасность;

– Низкая подверженность заражению компьютерными вирусами;

– Открытый код системы и прикладного программного обеспечения;

Слабые стороны:

– Частичное отсутствие русской локализации;

– Отсутствие технической поддержки, компенсируемое огромным количеством различных форумов и тематических сообществ;  
Корпоративный сервер является частью общей IT инфраструктуры организации, такой же частью, как и вычислительная сеть организации. Именно ЛВС предприятия осуществляет передачу информации внутри организации.

Прокси-сервер осуществляет:

– Кэширование и обеспечение доступа к запрашиваемым сайтам;

– Блокирование доступа к нежелательным сайтам;

– Ведение журналов (логов) посещённых пользователями сайтов;

– Возможность просматривать логии (журналы) прокси-сервера для получения информации о посещённых пользователями сайтах и количестве использованного трафика.

* 1. Кабельные и сетевые анализаторы

Сетевые анализаторы представляют собой эталонные измерительные приборы для диагностики и сертификации кабелей и кабельных систем. Они могут с высокой точностью измерить все электрические параметры кабельных систем, а также работают на более высоких уровнях стека протоколов.

Сетевые анализаторы генерируют синусоидальные сигналы в широком диапазоне частот, что позволяет измерять на приемной паре амплитудно-частотную характеристику и перекрестные наводки, затухание и суммарное затухание. Сетевой анализатор представляет собой лабораторный прибор больших размеров, достаточно сложный в обращении.

**Кабельные сканеры** - это портативные приборы, которые обслуживающий пер­сонал может постоянно носить с собой.

**Кабельные тестеры** - наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить непрерывность кабеля, однако, в отличие от кабельных сканеров, не дают ответа на вопрос о том, в каком месте произошел сбой.

Персональные компьютеры сотрудников работают под управлением Windows 10.

Кроме того, широко используются периферийные устройства: принтеры, сканеры, ксероксы, а также средства мультимедиа - проекторы, Web - камеры, звуковые колонки.

* 1. Диагностика отказов и ошибок сетевых устройств и программного обеспечения

Выделяют два вида диагностики персонального компьютера: программная диагностика и аппаратная диагностика.

Программная диагностика:

Данная диагностика неисправностей компьютера или ноутбука выявит причины некорректной работы устройства. Она поможет выяснить, почему операционная система перестала правильно работать:

- пострадала от атаки вируса

- произошел сбой в работе жесткого диска

- отсутствие в папке Windows файлов

В зависимости от задачи, диагностика системы компьютера включает:

- диагностика компьютера на вирусы;

- автоматический поиск неисправностей в системе;

- проверка системных файлов;

- проверка жесткого диска на системные ошибки.

Программное обеспечение для диагностики состояния компьютера поможет выявить неполадки, если:

- работа ПК прерывается;

- ОС тормозит;

- сбились настройки программ;

- некорректно работают отдельные приложения;

- нет изображения или звука - диагностика устройств компьютера;

- данные не сохраняются.

Аппаратная диагностика компьютера:

Если программная ошибка исключена, проводится диагностика оборудования компьютера или ноутбука. Процедура требует применения специального оборудования. Так называемая диагностика железа компьютера помогает определить локализацию неисправности: в блоке питания или другом узле.

Аппаратная диагностика работы компьютера включает проведение различных тестов (диагностика памяти компьютера, материнской платы, диагностика температуры компьютера, расшифровка сигналов, подаваемых системой BIOS).

* 1. Методы и технологии повышения производительности сети

Используется три основных способа повышения производительности сети:

- высокоскоростные технологии передачи данных;

- сегментация структуры сети;

- использование технологии коммутации кадров.

Первые классические варианты сетей использовали базовую технологию передачи данных Ethernet IDBase со скоростью передачи 10 Мбит/с.

В настоящее время появилось много новых высокоскоростных технологий, в частности Fast Ethernet 100 Base и Gigabit Ethernet 1000 Base, позволяющие увеличить скорость переда­чи соответственно в 10 и 100 раз (при условии наличия хороших каналов связи).

Интенсивность обмена данными между пользователями сети не является одно­родной. Часто в сети можно выделить группы пользователей, информационно более интенсивно связанных друг с другом, — рабочие группы, выполняющие решение схожих или тождественных задач. Тогда можно увеличить производи­тельность сети, разместив разные рабочие группы в отдельных сегментах сети.

Сегментация сети может быть выполнена установкой в сети мостов, коммута­торов, маршрутизаторов. В этом случае интенсивный информационный обмен, в том числе и широковещательный трафик, чаще выполняется внутри одного сегмента, интенсивность межсегментного трафика уменьшается и количество коллизий в сети существенно снижается.

Применение в сегментированной сети коммутаторов и маршрутизаторов совмест­но с технологией коммутации кадров (пакетов) может уменьшить интенсивность внутрисегментного трафика.

Интеллектуальные коммутаторы и маршрутизаторы определяют порт назначения кадра на основании адреса, содержащегося в кадре, и посылают последний, не дублируя его по всем направлениям, а лишь в нужный сегмент. Снижение интенсивности трафика за счет удаления из него ненужных состав­ляющих создает более благоприятные условия для передачи действительно нуж­ной информации, и производительность сети увеличивается.

* 1. Основные средства криптографии

Многие службы информационной безопасности, такие как контроль входа в систему, разграничение доступа к ресурсам, обеспечение безопасного хранения данных и ряд других, опираются на использование криптографических алгоритмов.

Шифрование – процесс преобразования сообщения из открытого текста (plaintext) в шифротекст (ciphertext) таким образом, чтобы его могли прочитать только те стороны, для которых оно предназначено, проверить подлинность отправителя (аутентификация), гарантировать, что отправитель действительно послал данное сообщение.

В алгоритмах шифрования предусматривается наличие ключа. Ключ – это некий параметр, не зависящий от открытого текста. Результат применения алгоритма шифрования зависит от используемого ключа. В криптографии принято правило Кирхгофа: «Стойкость шифра должна определяться только секретностью ключа». Правило Кирхгофа подразумевает, что алгоритмы шифрования должны быть открыты.

В методе шифрования с секретным или симметричным ключом имеется один ключ, который используется как для шифрования, так и для расшифровки сообщения. Такой ключ нужно хранить в секрете. Это затрудняет использование системы шифрования, поскольку ключи должны регулярно меняться, для чего требуется их секретное распространение. Наиболее популярные алгоритмы шифрования с секретным ключом: DES, TripleDES, ГОСТ и ряд других.

Часто используется шифрование с помощью односторонней функции, называемой также хеш- или дайджест-функцией. Применение этой функции к шифруемым данным позволяет сформировать небольшой дайджест из нескольких байтов, по которому невозможно восстановить исходный текст. Получатель сообщения может проверить целостность данных, сравнивая полученный вместе с сообщением дайджест с вычисленным вновь при помощи той же односторонней функции. Эта техника активно используется для контроля входа в систему. Например, пароли пользователей хранятся на диске в зашифрованном односторонней функцией виде. Наиболее популярные хеш-функции: MD4, MD5 и др.

В системах шифрования с открытым или асимметричным ключом (public/ assymmetric key) используется два ключа. Один из ключей, называемый открытым, несекретным, используется для шифрования сообщений, которые могут быть расшифрованы только с помощью секретного ключа, имеющегося у получателя, для которого предназначено сообщение. Иногда поступают по-другому. Для шифрования сообщения используется секретный ключ, и, если сообщение можно расшифровать с помощью открытого ключа, подлинность отправителя будет гарантирована (система электронной подписи). Этот принцип изобретен Уитфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом (Martin Hellman) в 1976 г.

Среди несимметричных алгоритмов наиболее известен RSA, предложенный Роном Ривестом (Ron Rivest), Ади Шамиром (Adi Shamir) и Леонардом Эдлманом (Leonard Adleman). Идея, положенная в основу метода, состоит в том, чтобы найти такую функцию y=Φ(x), для которой получение обратной функци иx=f-1(y)было бы в общем случае очень сложной задачей (NP-полной задачей). Например, получить произведение двух чисел n=p×q просто, а разложить n на множители, еслиpиqдостаточно большие простые числа, – NP-полная задача с вычислительной сложностью~ n10. Однако если знать некую секретную информацию, то найти обратную функцию x=f-1(y) существенно проще. Такие функции также называют односторонними функциями с лазейкой или потайным ходом.

Применяемые в RSA прямая и обратная функции просты. Они базируются на применении теоремы Эйлера из теории чисел.

* 1. Классификация операционных систем согласно классам безопасности. Профиль защиты

ОС называется защищенной, если она предусматривает средства защиты от основных классов угроз. ОС частично-защищенная, если предусматриваются не все средства защиты.

Политика безопасности – это набор норм, правил и практических приемов, регулирующих порядок хранения и обработки ценной информации.

Адекватная политика безопасности – это такая политика безопасности, которая обеспечивает доста­точный уровень безопасности ОС.

Адекватная политика безопасности – это необязательно та политика безопасности, при которой достигается максимальный уровень защищенности ОС.

Два подхода к созданию защищенной ОС: комплексный (механизм защиты внедряется на стадии разработки ОС; на момент создания сис­темы должна быть продумана линия зашиты), фрагментальный (простота, но система не гарантирует защиты от комплексных угроз). Пре­имущества: защиты организуется одним модулей, относительная дешевизна.Если ОС сертифицирована по некоторому классу защищенности, то это не означает, что информа­ция хранится и обрабатывается в этой системе согласно классу защищенности.

Безопасность определяется не только архитектурой ОС, но и политикой безопасности. Сертификация ОС по некоторому классу защиты, как правило, сопровождается составлением требо­ваний к адекватной политике безопасности, при неукоснительном выполнении которой защищенность ОС будет соответствовать требованиям защищенности класса защиты. Все АС делятся на 3 группы. В каждой существует своя иерархия.

Группа 3 – однопользовательские системы. Делятся на 2 класса. Класс 3Б – осуществляется проверка подлинности доступа при входе в систему, регистрация входа и выхода, учет используемых носителей (диски и т.д.). Класс 3А – выполняются все требования класса 3Б + регистрация распечатки документов и физиче­ская очистка очищаемой аппаратной области и внешней памяти.

Группа 2: Класс 2В – многопользовательские системы, в которых пользователи имеют равные права. Класс 2Б – проверка подлинности пользователей, регистрация и т.д. (как в 3Б). Класс 2А – выполняются все требования 2Б, избирательные разграничения доступа, регистрация со­бытий, потенциально опасных для поддержания защищенности системы, физическая очистка внешней и оперативной памяти, наличие подсистемы шифрования конфиденциальной информации, использование сертифицированных алгоритмов. Группа 1 – многопользовательские системы, в которых пользователи имеют различные полномочия доступа информации. Класс 1Д – должна проверяться подлинность пользователя, регистрация входа и выхода, учет внеш­них носителей информации.

Класс 1Г – предыдущие + избирательные разграничения доступа, регистрация событий, потенци­ально опасных для поддержания безопасности, и физическая очистка очищаемой аппаратной области и внешней памяти. Класс 1В – предыдущие + полномочные разграничения доступа, усилены требования для поддержа­ния опасных для поддержания защищенности системы, интерактивное оповещение администратора системы о попытках несанкционированного доступа.

Класс 1Б – предыдущие + наличие подсистемы шифрования конфиденциальной информации и ис­пользование сертифицированных алгоритмов. Класс 1А – предыдущие + различные субъекты доступа используют различные ключи.

Классификация угроз безопасности ОС:

по цели реализации: несанкционированное чтение информации; несанкционированное изменение информации; несанкционированное удаление информации; полное или частичное разрушение ОС (разрушение – это комплекс воздействий от кратковре­менного вывода отдельных модулей из строя до физических стираний системных файлов).

по принципу воздействия: использование известных каналов получения информации (несанкционированное чтение фай­лов, доступ к которым запрещен); использование скрытых каналов получение информации (использование недокументирован­ных функций); создание новых каналов получения информации (при разработке системы (какие-либо за­кладки)).

по характеру воздействия на ОС: активное воздействие; пассивное воздействие (наблюдение за процессами);

по типу использования слабой защиты: использование неадекватной политики безопасности, в том числе ошибки администратора; использование ошибок и недокументированных возможностей программного обеспечения (служебные закладки).

по способу воздействия на объект атаки: непосредственное воздействие; превышение пользователя своих полномочий; работа от имени другого пользователя; использование результатов работы другого пользователя.

по способу действия злоумышленника: можно работать в интерактивном режиме (пошагово, вручную); либо в пакетном режиме.

по объекту атаки: ОС в целом; Объект ОС (пользователи, процессы, запущенные от их имени); Каналы передачи данных.

по использованным средствам атаки: штатные средства ОС без использования дополнительного программного обеспечения; программное обеспечение третьих фирм; специально разработанное программное обеспечение; по состоянию атакуемого объекта на момент состояния (хранение, передача, обработка инфор­мации).

* 1. Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных

К основным программным средствам защиты информации относятся:

- программы идентификации и аутентификации пользователей КС;

- программы разграничения доступа пользователей к ресурсам КС;

- программы шифрования информации;

- программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Также к программным средствам защиты информации относятся:

- программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);

- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;

- программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);

- программы тестового контроля защищенности КС и др.

К преимуществам программных средств защиты информации относятся:

- простота тиражирования;

- гибкость (возможность настройки на различные условия применения, учитывающие специфику угроз информационной безопасности конкретных КС);

- простота применения -- одни программные средства, например шифрования, работают в «прозрачном» (незаметном для пользователя) режиме, а другие не требуют от пользователя ни каких новых (по сравнению с другими программами) навыков;

- практически неограниченные возможности их развития путем внесения изменений для учета новых угроз безопасности информации.

К недостаткам программных средств защиты информации относятся:

- снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирования программ защиты;

- более низкая производительность (по сравнению с выполняющими аналогичные функции аппаратными средствами защиты, например шифрования);

- пристыкованность многих программных средств защиты (а не их встроенность в программное обеспечение КС, рис. 4 и 5), что создает для нарушителя принципиальную возможность их обхода;

- возможность злоумышленного изменения программных средств защиты в процессе эксплуатации КС.

Основные компоненты:

Локальный администратор безопасности - несет ответственность за несанкционированный доступ, проверяет полномочия пользователя на вход в систему, поддерживает:

Аудит - проверка правильности выполнения действий пользователя

Диспетчер учетных записей - поддержка БД пользователей их действий и взаимодействия с системой.

Монитор безопасности - проверяет имеет ли пользователь достаточные права доступа на объект

Журнал аудита - содержит информацию о входах пользователей, фиксирует работы с файлами, папками.

Пакет проверки подлинности - анализирует системные файлы, на предмет того, что они не заменены. MSV10 - пакет по умолчанию.

Windows XP дополнена:

- можно назначать пароли для архивных копий

- средства защиты от замены файлов

- система разграничения путем ввода пароля и создания учета записей пользователя. Архивацию может проводить пользователь, у которого есть такие права.

1. Разработка предложений по автоматизации администрирования инфокоммуникационной системы и эксплуатации аппаратно-программных средств, улучшения использования ресурсов обеспечению защищенности компьютерных систем от вредоносных воздействий и повышения производительности

Для описания существующей технологии складского учета на предприятии ООО «ПК Венткомплекс», построим структурно-функциональную диаграмму изучаемого процесса по методологии SADT[[1]](#footnote-1). Среди множества CASE средств, пригодных для реализации таких диаграмм, предпочтение было отдано продукту компании «Computer Associates» - «BPwin». Проектирование функциональных моделей будет производиться на основе стандарта IDEF0.

Контекстная диаграмма процесса «Складской учет» в ООО «ПК Венткомплекс» представлена на рисунке 3. На диаграмме дается общее представление об изучаемом процессе.

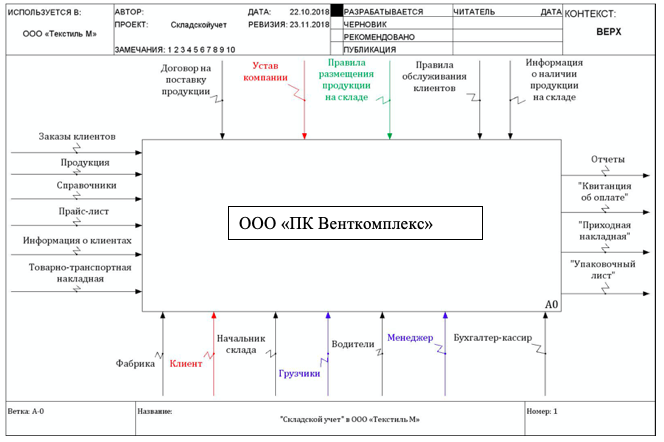


Рисунок 3 - Контекстная диаграмма процесса «Складской учет» в ООО «ПК Венткомплекс». Модель AS-IS

ООО «ПК Венткомплекс»

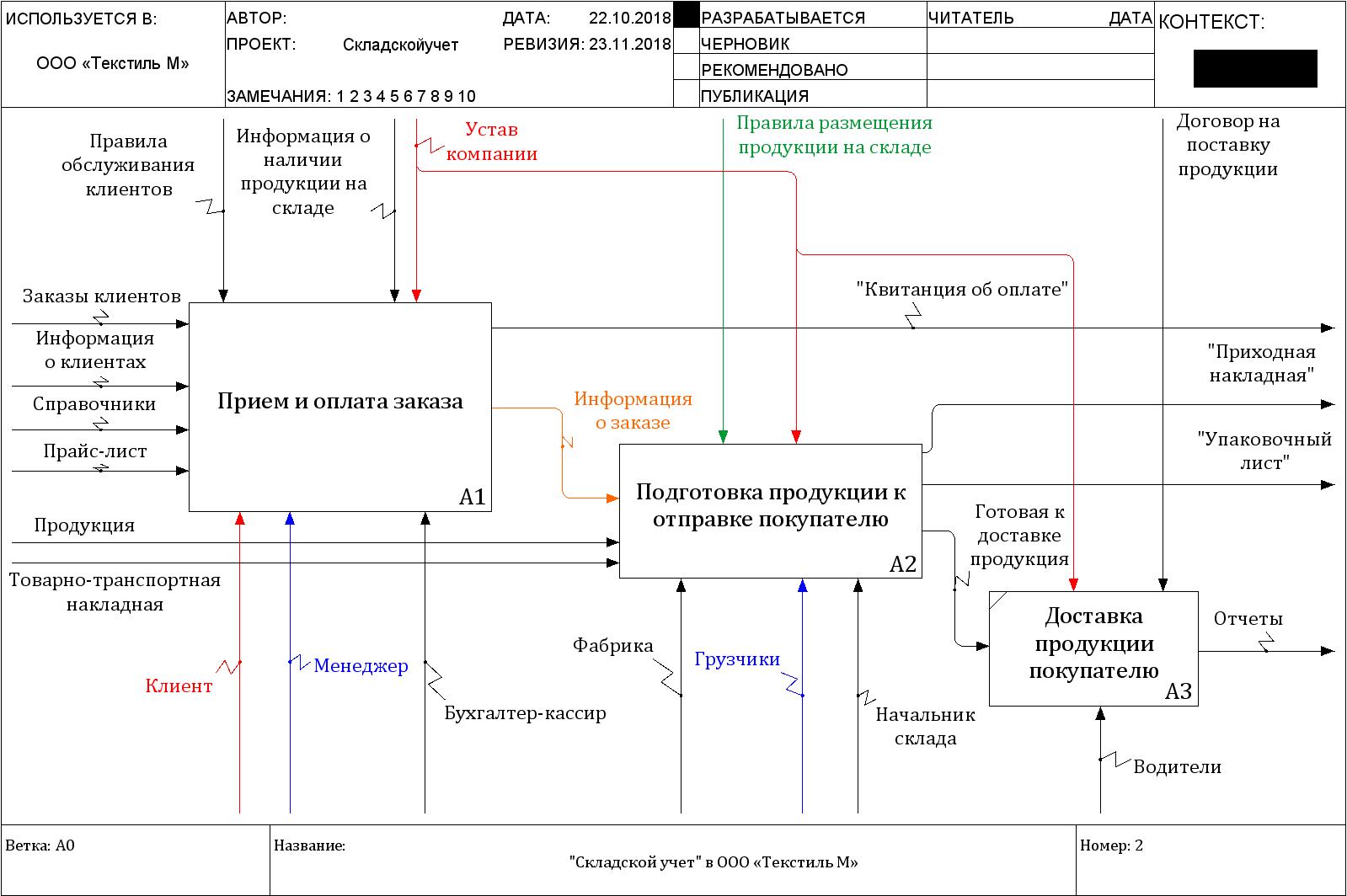


Рисунок 4 - Декомпозиция процесса «Складской учет». Модель AS-IS

В результате проведенного анализа на основе моделирования бизнес-процессов исследуемой компании, были выявлены следующие недостатки складского учета:

- нет доступа к актуальной информации о состоянии склада и свободных ячейках;

- длительные процедуры поиска интересующей информации;

- отсутствие контроля сроков исполнения заказов;

- длительные процедуры размещения товаров на складе, связанные с поиском свободных мест и ячеек;

- высокая трудоемкость и низкая оперативность обработки информации;

- отсутствие единых стандартов сбора и регистрации информации, приводящих к дублированию или потере данных о заказах или же товарах;

- низкий уровень безопасности хранимых данных, доступ к модификации и уничтожению которых может получить любой сотрудник компании;

- большой объем бумажных носителей информации, занимающих немалую долю офисного пространства.

Учитывая выявленные недостатки учета, необходимо разработать программный продукт, который позволит:

- автоматизировать процесс учета поставки товаров на склад;

- автоматизировать процесс размещения товаров на складе с учетом информации о количестве свободных мест в ячейках;

- автоматизировать процесс расчета свободных и занятых мест в ячейках на складе компании;

- автоматизировать процесс комплектования заказов;

- автоматизировать формирование документа «Упаковочный лист»;

- автоматизировать расчет остатка товаров каждого вида на складе;

- автоматизировать процесс списания недоброкачественных товаров.

Современный рынок программных продуктов предлагает множество решений для автоматизации работы склада. Наибольшей популярностью среди них пользуются системы «Автоматизация склада» от компании «Abmcloud», «1С-Логистика: Управление складом 3.0» и «Мой склад» от компании «Логнекс». Данные системы находятся в свободном доступе и обладают минимальным набором функций.

В продукте компании «1С» - «1С-Логистика: Управление складом 3.0» отсутствуют базовый набор функций, необходимых для работы современного склада. Интерфейс программы имеет сложную и непонятную структуру.

Итоги анализа существующих на отечественном рынке программных продуктов для автоматизации учета продаж ООО «Венткомплекс» доказывают, что наиболее рациональным решением для является разработка собственной системы, специально ориентированной под ее бизнес-процессы.

Для разработки информационной системы может быть успешно использована среда разработки «Delphi 7».

«Delphi 7» является мощной и быстрой средой разработки приложений для Windows с использованием объектно-ориентированного подхода к программированию.

Основными преимуществами «Delphi» можно назвать:

- надежность, стабильность и простота изучения;

- отсутствие необходимости в установке дополнительных библиотек;

- встроенный инструмент визуального моделирования;

- мощный генератор отчетов «Rave Designer»;

- совместимость с различными СУБД;

- огромное количество встраиваемых компонентов.

В главном меню выберите «Delphi 7», чтобы запустить мастера установки (рисунок 5).

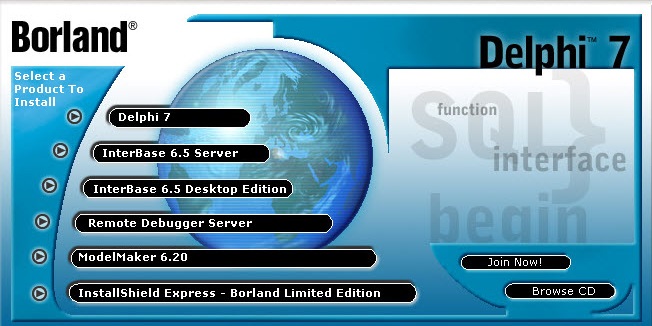


Рисунок 5 – Интерфейс установки «Delphi 7»

Дальше нужно лишь дождаться окончания инсталляции и попытаться запустить Delphi 7 на Windows 7.

Согласно уровню программно-технического оснащения ООО «Венткомплекс», компания открыта для внедрения новых решений, способных автоматизировать существующие бизнес-процессы, требующие оптимизации.

Заключение

В ходе прохождения практики в ООО «ПК Венткомплекс» были изучены организационные и юридические документы компании, в целях ознакомления с задачами, решаемыми организацией в процессе осуществления своей деятельности. Была изучена организационная структура предприятия, в частности, был выявлен перечень подразделений компании и список решаемых ими задач.

В целях анализа программно-технической архитектуры компании, были изучены особенности используемых в компании технических средств (компьютеров, серверов, сканеров, принтеров, АТС и т.д.) и программного обеспечения (описаны их возможности и функциональное назначение).

Исследование деятельности склада позволило выявить бизнес-процессы, нуждающиеся в автоматизации и информатизации.

В рамках данной задачи была описана существующая технология ввода, обработки, хранения, передачи и выхода данных, выявлены ее недостатки и внесены предложения по решению выявленных проблем.

В целях поиска решения был проведен анализ существующих программных продуктов от известных разработчиков, который показал, что наиболее рациональным решением для автоматизации складского учета в ООО «Венткомплекс» является разработка ИС собственными силами.

Для выбора средств разработки ИС был проведен анализ сред разработки и СУБД, в соответствии с которым для создания системы будут использоваться «Delphi 7» и «My SQL».

Список использованных источников и литературы

1. Гугуева, Т.А. Конфиденциальное делопроизводство: Учебное пособие / Т.А. Гугуева. [Текст]: - М.: Альфа-М, НИЦ ИНФРА-М, 2012. - 192 c.
2. Кирсанова, М.В. Современное делопроизводство: Учебное пособие / М.В. Кирсанова. [Текст]: - М.: НИЦ ИНФРА-М, 2012. - 312 c.
3. Кузнецов, Д.Л. Кадровое делопроизводство (правовые основы): Практическое пособие / Ю.П. Орловский, Д.Л. Кузнецов, И.Я. Белицкая, Ю.С. Корякина. [Текст]: - М.: ИНФРА-М, Контракт, 2012. - 239 c.
4. Кузнецов, Д.Л. Кадровое делопроизводство (правовые основы): Практическое пособие / Ю.П. Орловский, Д.Л. Кузнецов, И.Я. Белицкая, Ю.С. Корякина. [Текст]: - М.: ИНФРА-М, Контракт, 2013. - 239 c.
5. Кузнецов, И.Н. Документационное обеспечение управления. Документооборот и делопроизводство: Учебник и практикум / И.Н. Кузнецов. [Текст]: - Люберцы: Юрайт, 2016. - 477 c.
6. Кузнецов, И.Н. Делопроизводство: Учебно-справочное пособие / И.Н. Кузнецов. [Текст]: - М.: Дашков и К, 2013. - 520 c.
7. Кузнецов, И.Н. Делопроизводство: Учебно-справочное пособие / И.Н. Кузнецов. [Текст]: - М.: Дашков и К, 2016. - 520 c.
8. Кузнецов, И.Н. Документационное обеспечение управления и делопроизводство: Учебник для бакалавров / И.Н. Кузнецов. [Текст]: - М.: Юрайт, ИД Юрайт, 2012. - 576 c.
9. Кузнецов, И.Н. Документационное обеспечение управления и делопроизводство: Учебник для бакалавров / И.Н. Кузнецов. [Текст]: - М.: Юрайт, ИД Юрайт, 2013. - 576 c.
10. Куняев, Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: Учебник / Н.Н. Куняев. [Текст]: - М.: Логос, 2015. - 500 c.

1. SADT (StructuredAnalysisandDesignTechnique) - методология структурного анализа и проектирования. [↑](#footnote-ref-1)