Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____А.В. Бушманов
«_____»_____2018 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Модернизация локальной сети предприятия ООО «ВНК»

Исполнитель
студент группы 455 об _____ С.О. Троценко
(подпись, дата)

Руководитель
доцент, канд. техн. наук _____ А.Н. Гетман
(подпись, дата)

Консультант
по безопасности и
экологичности
доцент, канд. техн. наук _____ А.Б. Булгаков
(подпись, дата)

Нормоконтроль
инженер кафедры _____ В.В. Романико
(подпись, дата)

Благовещенск 2018

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав.кафедрой
_____ А.В. Бушманов
«_____»_____2018 г.

З А Д А Н И Е

К бакалаврской работе студента Троценко Сергея Олеговича

1. Тема бакалаврской работы: Модернизация локальной сети предприятия ООО «ВНК» (утверждена приказом от_____ № _____)

2. Срок сдачи студентом законченной работы_____

3. Исходные данные к бакалаврской работе: отчет по практике, специальная литература, нормативные документы.

4. Содержание бакалаврской работы (перечень подлежащих разработке вопросов): анализ объекта исследования, анализ организационной структуры, анализ бизнес-процессов, анализ документооборота, проектирование локальной вычислительной сети, техническое задание, анализ угроз информационной безопасности объекта исследования, разработка политики безопасности, анализ безопасности и экологичности объекта исследования.

5. Перечень материалов приложения: (наличие чертежей, таблиц, графиков, схем, программных продуктов, иллюстративного материала и т.п.) техническое задание, диаграммы DFD и IDEF0, ER-диаграммы, инструкции, положение о секторе по ТЗИ.

6. Консультанты по бакалаврской работе (с указанием относящихся к ним разделов) консультант по безопасности и экологичности доцент, канд. техн. наук Булгаков А.Б.

7. Дата выдачи задания_____

Руководитель бакалаврской работы: доцент, канд. техн. наук. Гетман А.Н.

Задание принял к исполнению:_____

РЕФЕРАТ

Бакалаврская работа содержит 74 с., 17 рисунков, 2 таблицы, 1 приложений, 14 источников.

ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ, БЕЗОПАСНОСТЬ, VPN, ЗАЩИТА, УГРОЗА, СЕТЕВОЕ ОБОРУДОВАНИЕ, РЕЗЕРВНОЕ КОПИРОВАНИЕ

Субъектом данной работы является ООО «Восточная нефтяная компания».

Целью работы является модернизация локальной вычислительной сети предприятия ООО «Восточная нефтяная компания». Для достижения цели работы были выполнены следующие задачи: исследована предметная область, изучена организационная структура и деятельность сотрудников отдела офиса компании ООО «ВНК», сформировано технического задания на модернизацию локальной сети. Также была проанализирована текущая локальная сеть компании. Локальная вычислительная сеть была проанализирована на предмет угроз информационной безопасности, на основании этих угроз была разработана политика безопасности. Была проанализирована на соответствие безопасности и экологичности.

В результате работы получена модернизированная локальная вычислительная сеть, позволяющая сократить расходы компании.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей бакалаврской работе использованы ссылки на следующие стандарты и нормативные документы:

ГОСТ 2.104-68 ЕСКД Основные надписи

ГОСТ 2.105-95 ЕСКД Общие требования к текстовым документам

ГОСТ 2.111-68 ЕСКД Нормоконтроль

ГОСТ 19.201-78 ЕСПД Техническое задание. Требования к содержанию и оформлению

ГОСТ 34.601-90 КСАС Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ 34.602-89 КСАС Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы управления

ГОСТ 19.502-78 Описание применения. Требования к содержанию и оформлению

ГОСТ 19.505-79 Руководство оператора. Требования к содержанию и оформлению

ГОСТ 7.1-2003 Библиографическое описание документа. Общие требования и правила составления

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ВНК – Восточная нефтяная компания;

ЛВС – локальная вычислительная сеть;

БП – бизнес-процесс;

ИБП – источники бесперебойного питания;

МФУ – многофункциональное устройство;

ОС – операционная система;

ПО – программное обеспечение;

ПЭВМ – персональная электронная вычислительная машина;

СБ – служба безопасности предприятия;

ЮО – юридический отдел предприятия;

ИТ-отдел (IT-отдел) – отдел информационных технологий предприятия;

ПБ – пожарная безопасность;

ЧС – чрезвычайная ситуация;

VPN – частная виртуальная сеть;

ТЗ – техническое задание.

ВВЕДЕНИЕ

Объектом бакалаврской работы является ООО «ВНК». В настоящее время эффективное управление фирмой невозможно без непрерывного отслеживания состояний коммерческого и финансового рынков, без оперативной деятельности всех филиалов и сотрудников. Реализация поставленной цели и задач требует совместного участия большого числа различных специалистов, часто территориально удаленных друг от друга. В такой ситуации для организации эффективного взаимодействия этих специалистов служат системы распределенной обработки данных.

Для развития компании применяются современные технологии, позволяющие поддерживать степень информационно-технического обеспечения на высоком уровне. Любое современное предприятие, имеющее в своем распоряжении более одного компьютера, стремится объединить их в локальную сеть.

Задачи и цели, решаемые компьютерной сетью:

– обеспечить быструю и надежную взаимосвязь между сотрудниками и клиентами;

– защитить особо важные данные от несанкционированного доступа;

– предоставить всем работникам одновременный доступ к ресурсам сети и периферийному оборудованию;

– перемещать и добавлять рабочие места существенных финансовых затрат и дополнительной прокладки кабеля.

Локальная вычислительная сеть (ЛВС) – это компьютерная сеть, покрывающая относительно небольшую территорию или небольшую группу, связанных между собой ПК, принтеры, факсы, серверы и другое оборудование.

Сеть делает возможным сотрудникам организации взаимодействовать между собой и обращаться к используемым ресурсам; позволяет получать доступ к данным, хранящимся на ПК с любого ПК устройства, имеющего доступ.

Помимо этого, требуется правильно смонтировать оборудование сети и установить системное программное обеспечение.

При выборе активного оборудования сети необходимо учитывать растущие требования к скорости передачи данных.

Создание надёжной и полнофункциональной корпоративной сети очень важно на сегодняшний день. Создание защищенного канала передачи информации необходимо в первую очередь, потому что информация сегодня достаточно дорогостоящий ресурс, а любому предприятию нужна хорошая настройка такой сети и обеспечение максимально эффективной защиты.

Существует ряд причин, для создания ЛВС:

– совместное использование ресурсов позволяет нескольким компьютерам и другим устройствам осуществлять доступ к отдельному хранилищу, принтерам, к сканерам и другому периферийному оборудованию, что снижает затраты времени и ресурсов, для всех пользователей;

– кроме совместного использования дорогих устройств, ЛВС позволяет использовать сетевое программное обеспечение, что облегчает работу пользователям;

– ЛВС облегчает взаимодействие при работе над общим проектом;

– ЛВС даёт возможность использовать средства связи между различными системами (IP-телефония, Видео связь и т.д.).

С помощью предложенной системы связи и передачи данных будет возможным удовлетворять всем возложенным на неё задачам. А именно: обеспечению безошибочного обмена данными между рабочими станциями, снижению нагрузки на сетевое оборудование, исключение ошибок возникающих при работе с БД. Наряду с этим, система связи и передачи данных будет обеспечивать должный уровень защиты информации, не допускающий ее искажения или утечки.

Целью данной бакалаврской работы является модернизация локальной сети ООО «ВНК».

В рамках сформулированной цели ВКР необходимо решить следующие задачи:

1) произвести анализ предметной области;

2) произвести анализ документооборота предприятия;

3) проанализировать аппаратно-технический комплекс, имеющийся на предприятии;

4) модернизировать локальную сеть;

5) провести анализ угроз объекта защиты и разработать политику безопасности.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Общие сведения о предприятии

Объектом исследования в рамках написания бакалаврской работы является ООО «ВНК» (Восточная нефтяная компания). В офисе ведется работа, заключаются сделки, в компанию приходят партнеры и клиенты. В услуги компании входят:

– оптовая продажа ГСМ;

– розничная продажа ГСМ;

– доставка по региону ГСМ.

Сеть функционировавшая в ООО «ВНК» имела массу недостатков, низкая отказоустойчивость, неизбежность значительных физических и финансовых затрат при добавлении новых пользователей. Это говорит о том, что необходимо разработать топологию таким образом, чтобы сеть обеспечивала быстрый доступ к информации на территории всего офиса, так же обеспечивала работу ЭВМ даже при частичном отказе оборудования.

В связи с тем, что для передачи данных в офисе используется ЛВС, на фирме действует режим коммерческой тайны и большое значение уделяется ее защите.

Большая часть информации циркулирует во внутренней сети фирмы, что предъявляет к ней высокие требования безопасности. Наиболее важная информация хранится в сейфе в документированном виде под замком. На фирме действует система разграничения доступа, у каждого работника свое рабочее место и свой рабочий стол с ЭВМ. Непосредственно сам вход в ЭВМ проходит таким образом, что работник вводит свой логин и пароль для доступа в общую базу данных.

1.2 Анализ организационной структуры предприятия

Каждое предприятие, независимо от численности рабочих, должно иметь свою организационную структуру, которая показывает распределение полномочий и обязанностей внутри организации.

Рассмотрим организационную структуру офиса компании «ВНК», которая

показана на рисунке 1.

Рисунок 1 – Организационная структура ООО «ВНК»

Организационная структура предприятия является линейной, так как во главе каждого производственного или управленческого подразделения находится руководитель, наделенный всеми полномочиями и осуществляющий единоличное руководство подчиненными ему работниками и сосредоточивающий в своих руках все функции управления. Рассмотрим организационную структуру ООО «ВНК». Начнем с самого верхнего звена – генерального директора ООО «ВНК». В его подчинении находится – директор компании.

Директор несёт ответственность за сохранность и эффективное использование имущества предприятия, за последствия принимаемых решений, финансово-хозяйственные результаты деятельности компании.

Функции директора заключаются в общем руководстве производственно-хозяйственной деятельностью компании, так же в его обязанности входит:

– общее руководство производственно-хозяйственной и финансово-экономической деятельностью предприятия.

– организация взаимодействия всех структурных подразделений, цехов и производственных единиц;

– обеспечение выполнения всех принимаемых предприятием обязательств, включая обязательства перед бюджетами разных уровней и внебюджетными фондами, а также по договорам;

– создание условий для внедрения новейшей техники и технологии, прогрессивных форм управления и организации труда;

– принятие мер по обеспечению здоровых и безопасных условий труда на предприятии;

– контроль за соблюдением законодательства Российской Федерации в деятельности всех служб;

– защита имущественных интересов предприятия в суде, органах государственной власти;

– обеспечение соблюдения законности в деятельности компании;

– осуществление руководства финансовой и хозяйственной деятельностью компании в соответствии с её уставом;

– организация работы компании с целью достижения эффективного взаимодействия всех структурных подразделений;

– выполнение поручений генерального директора.

Именно генеральный директор несет полную ответственность за все принятые решения, за результаты деятельности предприятия и сохранность его имущества.

Задачи, которые относятся к области продаж, решает менеджер. Данный руководитель является вторым человеком после директора, по степени важности в компании. Ему приходится взаимодействовать практически со всеми подразделениями компании, так как организация продаж требует большого количества информации.

Логист осуществляет руководство всеми логистическими процессами, протекающими на предприятии, и координирует деятельность подразделений предприятия, которые участвуют в реализации логистических процессов, а также поставке и сбыте продукции.

В функции системного администратора входит:

– планирование системы:

– планирование использования дискового пространства;

– подсистемы (печать, сеть и т.п.);

– присвоение имен;

– установка и конфигурация аппаратных устройств;

– установка программного обеспечения;

– архивирование (резервное копирование) информации;

– создание и управление учетными записями пользователей;

– поиск неисправностей;

– контроль защиты;

– управление системными ресурсами;

– мониторинг системы;

– планирование нагрузки;

– документирование системной конфигурации.

Одной из основных обязанностей системного администратора является предоставление пользователям необходимых им сервисов.

Главный бухгалтер занимается ведением бухгалтерского учета согласно законодательству РФ. Составляет бухгалтерский и налоговые отчеты, расчет по заработной плате и тд.

Главный бухгалтер выполняет следующие должностные обязанности:

– руководство ведением бухгалтерского учета и составлением отчетности на предприятии;

– формирование учетной политики с разработкой мероприятий по ее реализации;

– оказание методической помощи работникам подразделений предприятия по вопросам бухгалтерского учета, контроля и отчетности;

– обеспечение составления расчетов по зарплате, начислений и перечислений налогов и сборов в бюджеты разных уровней, платежей в банковские учреждения;

– выявление внутрихозяйственных резервов, осуществление мер по

устранению потерь и непроизводительных затрат;

– внедрение современных технических средств и информационных технологи;

– контроль за своевременным и правильным оформлением бухгалтерской документации;

– обеспечение здоровых и безопасных условий труда для подчиненных исполнителей, контроль за соблюдением ими требований законодательных и нормативных правовых актов по охране труда;

– согласовывает с директором направления расходования средств с рублевых счетов организации;

– осуществляет экономический анализ хозяйственно-финансовой деятельности компании по данным бухгалтерского учета и отчетности;

– участвует в подготовке мероприятий системы внутреннего контроля, предупреждающих образование недостач и незаконное расходование денежных средств и товарно-материальных ценностей;

– контролирует соблюдение порядка оформления первичных и бухгалтерский документов, расчетов и платежных обязательств предприятия.

Бухгалтера выполняют расчеты по материальным, трудовым и финансовым затратам, необходимые для производства, осуществляют прием денежных средств в кассу предприятия. Выдает наличные денежные средства подотчетным лицам на основании служебных записок, заверенных подписью генерального директора и контролирует соблюдение лимита остатка денежных средств в кассе.

Юридические функции компании ООО «ВНК» возложены на секретаря, а также отдел закупок, в связи с наличием юридического образования, в их обязанности входит:

– обеспечение контроля за деятельностью организации с точки зрения соблюдения действующего законодательства;

– мониторинг и анализ изменений в законодательстве, судебной практики;

– информирование работников компании о наиболее важных изменениях законодательства;

– консультация работников других подразделений по правовым вопросам;

– подготовка и экспертиза проектов локальных нормативных актов (инструкций, положений, регламентов, приказов, распоряжений), принимаемых в компании(обычно распределено по профильным отделам, например, договорной отдел разрабатывает положение о договорной работе, регламент выдачи кредитов разрабатывается кредитующим подразделением, а рассматривается отделом по обеспечению основной деятельности в составе юридического подразделения);

– обеспечение учета и хранения различных документов, относящихся к работе юриста (внутренние служебные записки, письма, претензии, судебные решения, исполнительные листы, иногда уставы, свидетельства о регистрации, приказы);

– участие в подготовке мер по обеспечению сохранности имущества компании;

– внесение предложений о совершенствовании законодательства в уполномоченные органы;

– подготовка отчетности о проведенной работе;

– утверждение личного плана работы у руководителя.

1.3 Анализ внешнего и внутреннего документооборота

Документооборот – это процесс движение документов с момента создания или получения до завершения пользованием, отправкой или хранением.

Организация документооборота показывает всю последовательность перемещения документов на предприятии (прием, передача, составление и оформление, отправка.).

Основной объём документооборота составляет документация, направления и характер, которых напрямую зависит от утвержденной структуры организации. В данной группе документов, не зависимо от форм

собственности и структуры организации, можно выделить основные виды документов:

– распорядительная документация (приказы, распоряжения, решения, протоколы общих собраний различных органов);

– бухгалтерского учета и отчетности;

– документы фиксирующие трудовые отношения работников с работодателем (документы по личному составу);

– планово-отчетная (бизнес-планы, совет директоров, общие собрания, акционерные и т.д.).

Рассмотрим внешний документооборот (взаимодействие предприятие с другими организациями, потоки входящих и исходящих документов) и внутренний документооборот.

Офис компании ООО «ВНК» взаимодействует со следующими внешними субъектами; головным офисом, клиентом, поставщиком (заводом), подрядными организациями и банком.

Офис заключает договор на предоставление услуг (уборка территории, уборка офиса, доступ в Интернет, транспорт и перевозка товара, отопление, водоснабжение, сантехнические и слесарные услуги), обговариваются все условия и сумма, если все условия удовлетворили стороны и подписан договор, после выполнения заказа, выдается акт о выполненных работах, и подрядчик предоставляет счет за свои услуги.

Завод является неотъемлемой частью в работе офиса компании ООО «ВНК», он осуществляет поставки ГСМ. С заводом заключается договор на поставку. Офис ООО «ВНК» делает заявку, а завод отправляет товар и прикладывает к поставке соответствующие накладные.

Для хранения денежных средств, предприятие выбрало Публичное акционерное общество ПАО «Сбербанк России». Банк осуществляет расчетно-кассовые операции. Для поставки ГСМ в розничные торговые точки компания выбрала качестве поставщика ОАО «Нефтяная компания «Роснефть»».

Схема внешнего документооборота офиса компании ООО «ВНК» представлена на рисунке 2.

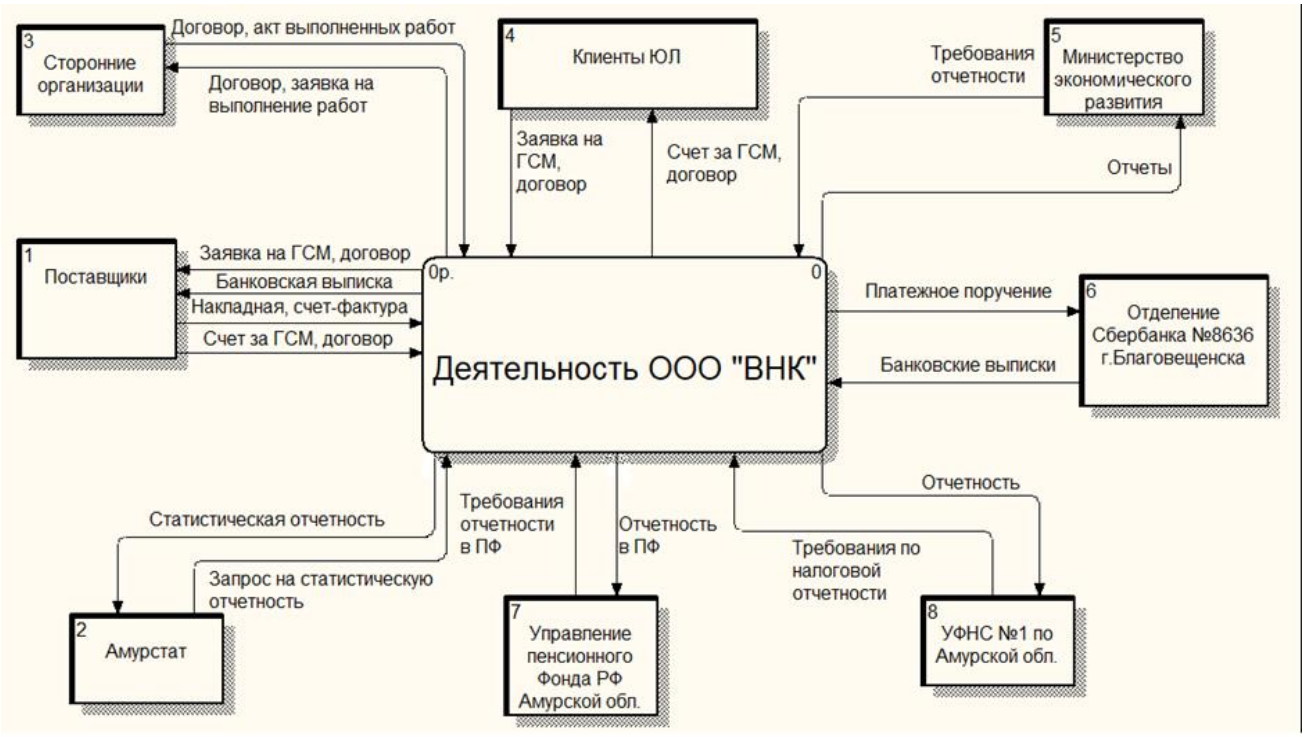

Рисунок 2 – Внешний документооборот ООО «ВНК»

Внутренний документооборот показывает документопоток между отделами офиса. Организация внутреннего документооборота должна основываться на принципах, которые обеспечивают оперативное передвижение документов, что повысило бы эффективность бизнес-процессов, сократило затраты рабочего времени. Рассмотрим внутренний документооборот на рисунке 3.

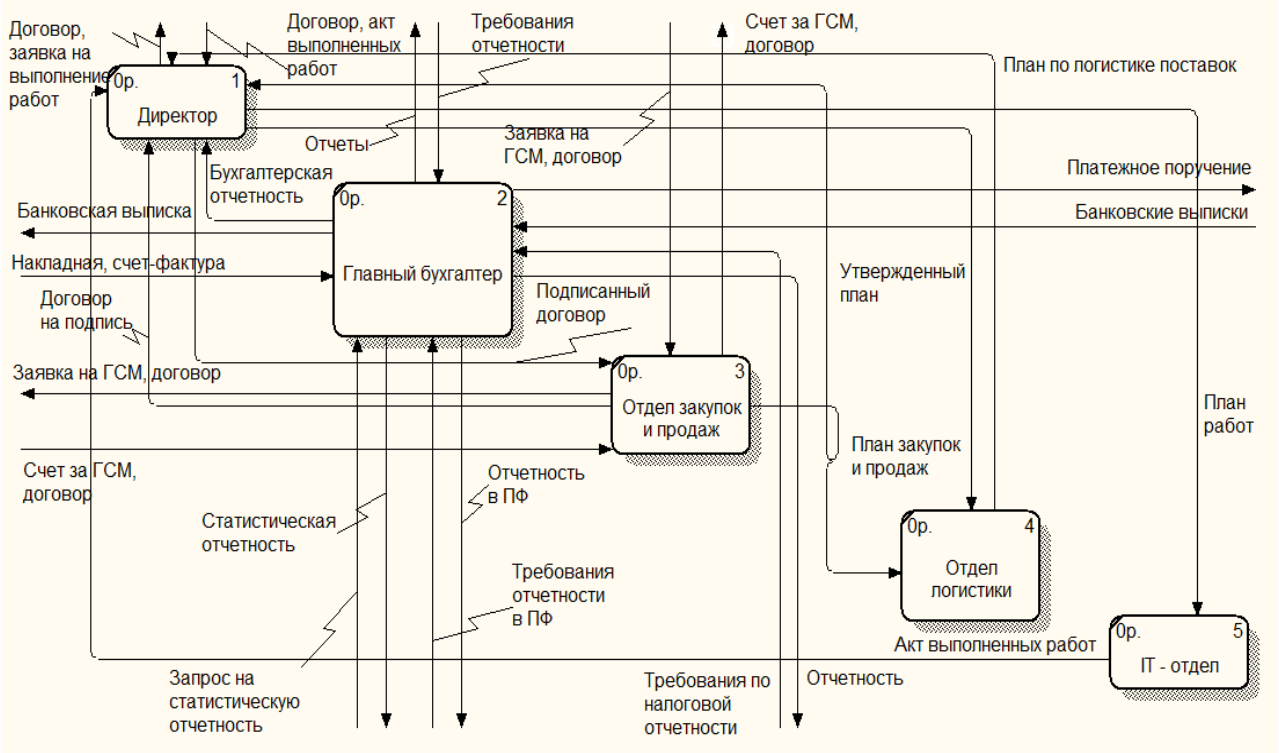

Рисунок 3 – Внутренний документооборот ООО «ВНК»

Логист принимает заявки от розничных торговых точек, формирует накладные для отправки, договор передается на подписание директору. После подписания накладной, данный отдел приступает к выполнению работ. При завершении работ с заказом, логист заносит данные в журнал отчетности в информационной системе, которые просматривает менеджер. Когда логист нанимает подрядчика (транспортную компанию), договор передается на подписание менеджеру.

Отдел закупок занимается руководством производственного процесса, издает распоряжения. Просматривает список заказов, отчетность по отправленным товарам, предоставляет бухгалтерии отчеты по расходам.

Бухгалтерия ведет бухгалтерский учет, следит за движением финансов, готовит отчеты, контролирует соблюдение лимита остатка денежных средств в кассе, ежедневно ведет кассовую книгу и оформляет первичные кассовые документы своевременно погашает дебиторскую и кредиторскую задолженность офиса, так как, от этого зависит финансовая стабильность компании.

Системный администратор занимается ремонтом и настройкой офисного

оборудования, а также настройкой и бесперебойной работы информационной системы офиса, а также оборудования, которое находится в кабинетах персонала. Системный администратор оформляет и отправляет заявки в центральный офис ООО «ВНК» о необходимости закупки нового оборудования и его обновления. Если в офисе необходима замена или совершенствование оборудования, то оформляется заявка, после чего отправляется на рассмотрение директору, затем он в электронном виде отправляет заявку в центральный офис. Существуют и ситуации, когда оборудование подлежит списанию в силу износа. В этом случае также необходима заявка на списание. После того, как заявка одобрена директором, системный администратор упаковывает пришедшее в негодность оборудование и отправляет его на центральный склад.

1.4 Анализ бизнес-процессов предприятия

Бизнес-процесс – последовательность действий (подпроцессов), направленная на получение заданного результата, ценного для организации. Рассмотрим деятельность ООО «ВНК» в нотации IDEF0.

На рисунке 4 представлена контекстная диаграмма деятельности ООО «ВНК».

Входящими потоками для ООО «ВНК» являются товары от поставщиков (нефтепродукты, сопутствующие товары, продаваемые на заправках и т.д), счета на товары от поставщиков, а также накладные и счета-фактуры, прилагаемые к поставляемым поставщиками товарам. Кроме того, от клиентов входными потоками являются денежные средства за нефтепродукты (бензин разных марок, дизтопливо). Выходными потоками являются оказанные клиентам услуги, сопровождаемые счетом за услуги и чеком, банковские выписки поставщикам (оплата счетов поставляемых товаров) и заявки на товар поставщикам. Механизмом для контекстной диаграммы являются персонал и оборудование. Управляющим воздействием является законодательство Российской Федерации и Устав предприятия.

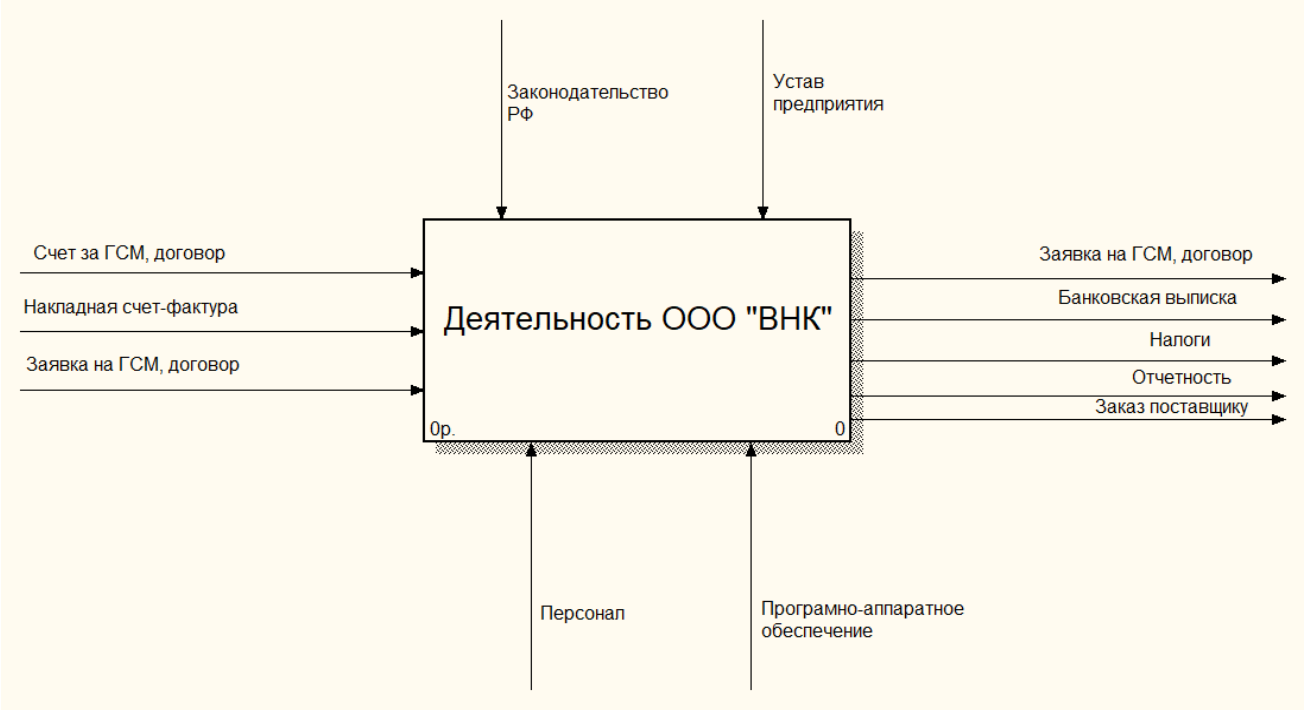

Рисунок 4 – Контекстная диаграмма деятельности предприятия

Для более подробного анализа бизнес–процессов предприятия произведем декомпозицию контекстной диаграммы (рисунок 5).

В диаграмме декомпозиции представлены следующие бизнес-процессы:

– деятельность директора ООО;

– деятельность бухгалтерии;

– деятельность отдела логистики;

– деятельность отдела закупок и продаж;

– деятельность IT-отдела.

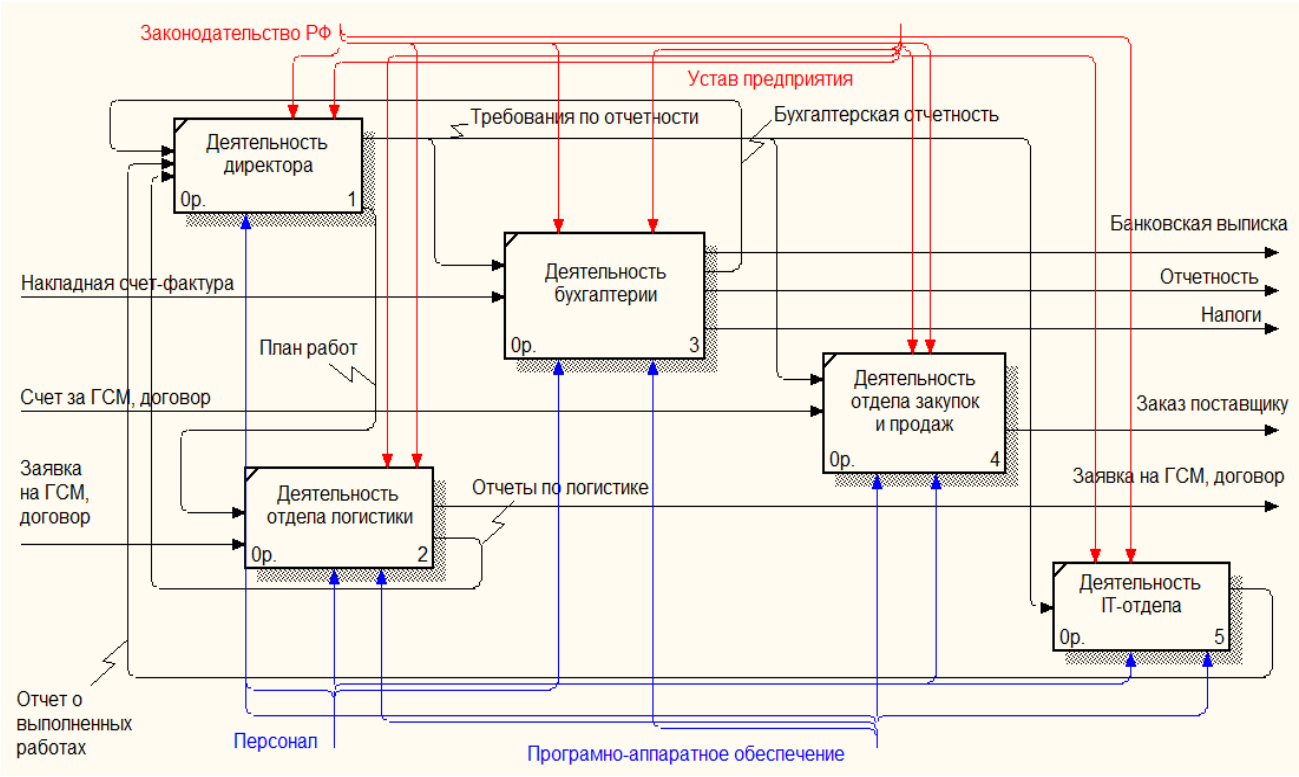

Рисунок 5 – Декомпозиция контекстной диаграммы деятельности предприятия

Отдел логистики принимает заявки от розничных торговых точек, формирует накладные для отправки. После получения накладной, данный отдел приступает к выполнению работ. При завершении работ с заказом, данные заносятся в журнал отчетности в информационной системе, которые просматривает менеджер. Когда логист нанимает подрядчика (транспортную компанию), договор передается на подписание менеджеру.

Отдел закупок и продаж занимается руководством производственного процесса, издает распоряжения. Просматривает список заказов, отчетность по отправленным товарам, предоставляет бухгалтерии отчеты по расходам.

Бухгалтерия ведет бухгалтерский учет, следит за движением финансов, готовит отчеты, контролирует соблюдение лимита остатка денежных средств, в кассе и на предприятии, ежедневно ведет кассовую книгу и оформляет первичные кассовые документы, своевременно погашает дебиторскую и кредиторскую задолженность офиса, так как, от этого зависит финансовая стабильность компании.

Системный администратор оформляет и отправляет заявки в центральный

офис ООО «ВНК» о необходимости закупки нового оборудования и его обновления. Если в офисе необходима замена или совершенствование оборудования, то оформляется заявка, после чего отправляется на рассмотрение директору, затем он в электронном виде отправляет заявку в центральный офис. Существуют и ситуации, когда оборудование подлежит списанию в силу износа. В этом случае также необходима заявка на списание. После того, как заявка одобрена директором, системный администратор упаковывает пришедшее в негодность оборудование и отправляет его на центральный склад.

Организация документооборота компании основываться на принципах, которые обеспечивают оперативное передвижение документов, что повышает эффективность проходящих бизнес-процессов и сокращает затраты рабочего времени.

1.5 Анализ ЛВС на предприятии

В настоящее время аппаратно-технический комплекс ООО «ВНК» представляет собой четыре автоматизированных рабочих места, на которых установлены персональные компьютеры. Каждый ПК имеет выход в интернет с помощью беспроводного маршрутизатора. Общая схема сети представлена на рисунке 6. АЗС не связаны между собой и не имеют связи с офисом. Учет и документация продаж хранится на ПК АЗС, один раз в день менеджер осуществляет выгрузку информации на съемный носитель, а в дальнейшем вводится в общий учет на главном офисе предприятия.

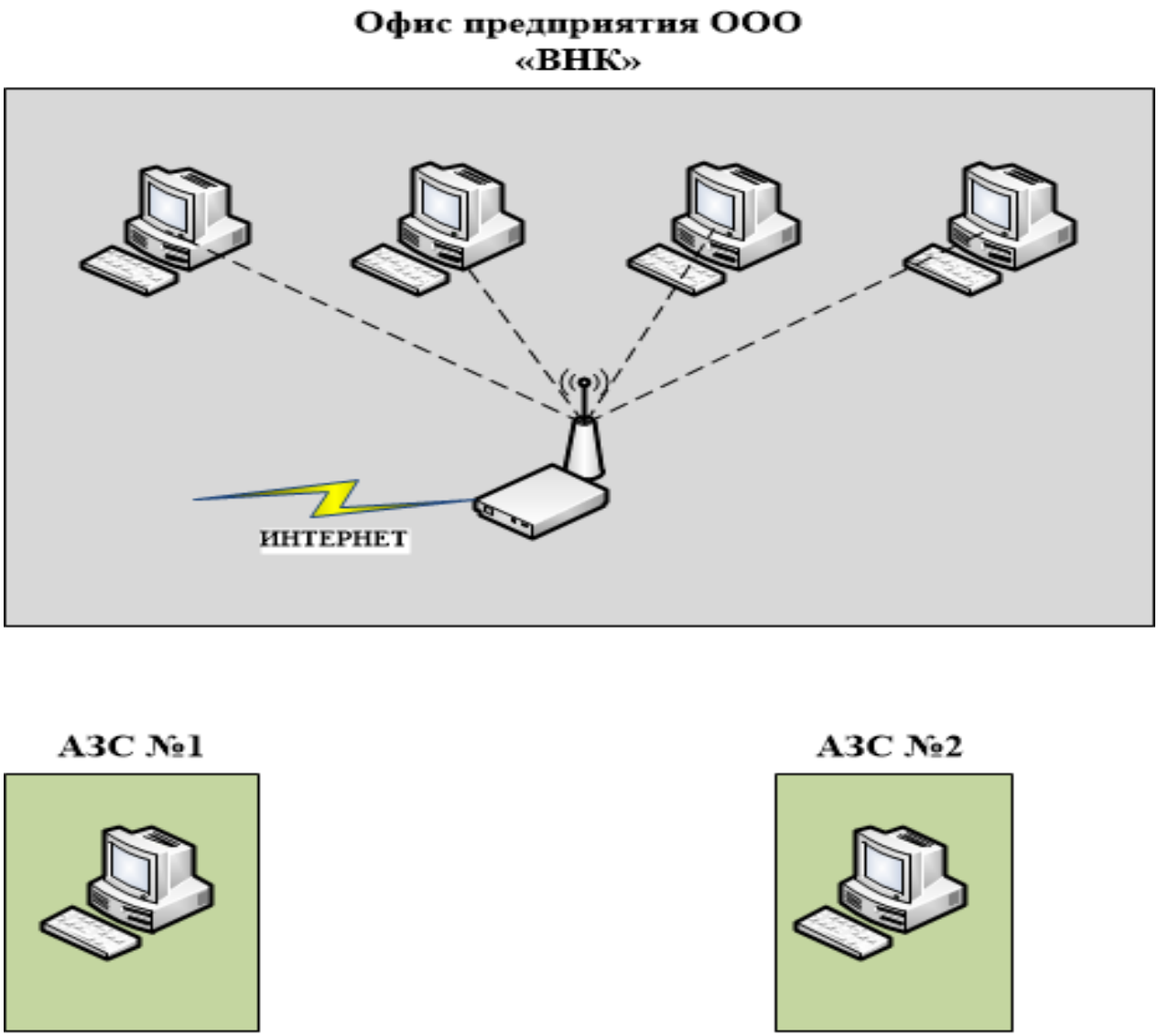

Рисунок 6 – Общая схема ЛВС предприятия ООО «ВНК» до модернизации

Связь с операторами офиса осуществляется с помощью Wi-Fi роутера. Wi-Fi роутер – сетевое устройство которое выполняет функции пересылки пакетов данных между сегментами сети, то есть помогает построить сеть между подключенными между собой компьютерами и при возможности соединиться с интернетом.

Подробный план офиса представлен на рисунке 7.

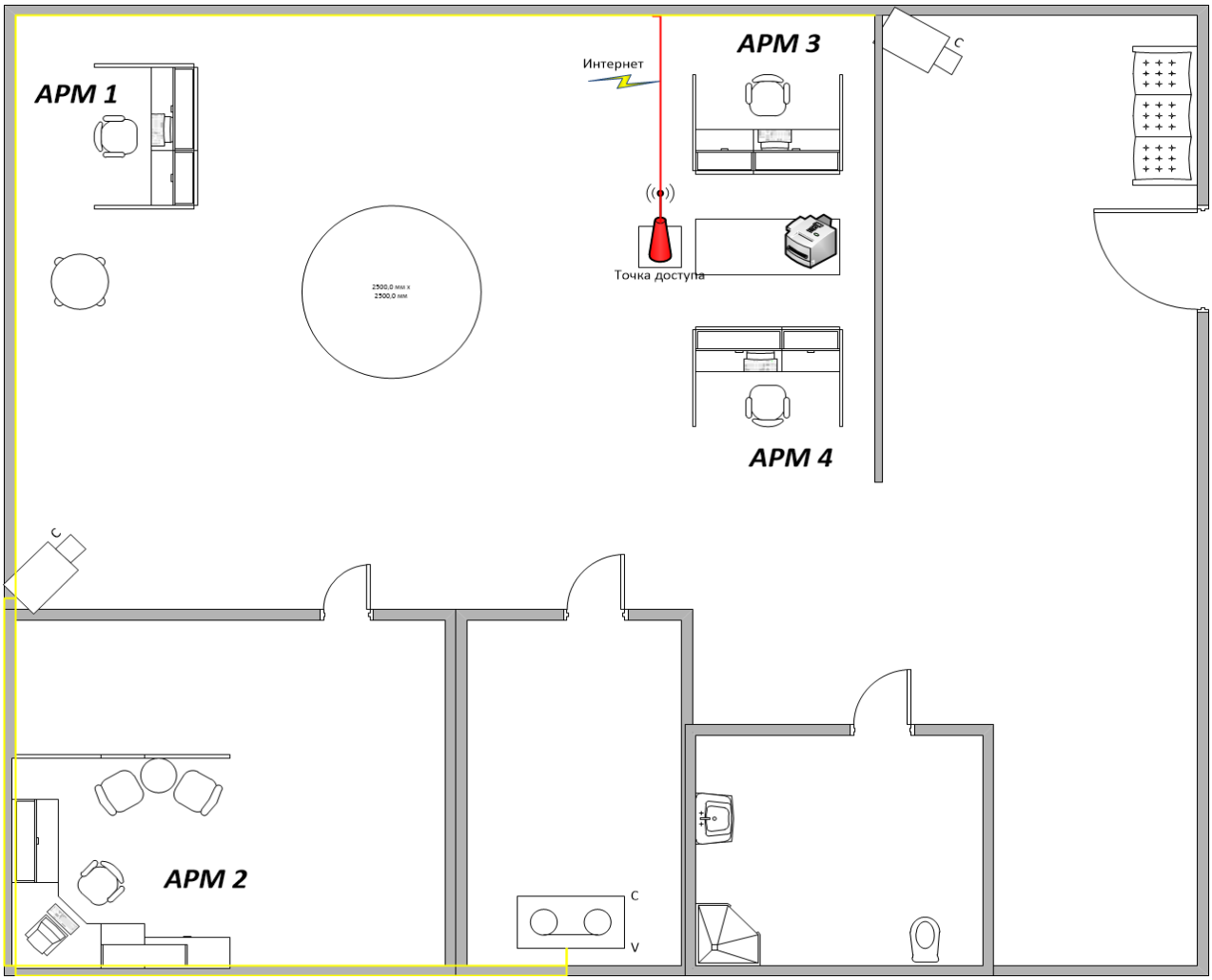

Рисунок 7 – Схема ЛВС офиса ООО «ВНК» до модернизации

Достоинства Wi-Fi:

– отсутствие проводов – это один из самых главных плюсов Wi-Fi;

– мобильность и высокая скорость передачи данных;

– сети Wi-Fi не создают помех;

– Wi-Fi безопасен для человека;

– простая настройка Wi-Fi сетей.

Недостатки Wi-Fi роутера:

– влияние окружающей среды на передачу данных;

– ограниченный радиус действия. У каждого Wi-Fi модуля он свой (может достигать до 500 метров);

– на качество связи влияет толщина стен и другие препятствия;

– слабая защита от взлома;

– высокое энергопотребление;

– из-за большого количество точек доступа Wi-Fi в офисе, передача данных ухудшается.

На предприятии ООО «ВНК» в настоящее время установлен Wi-Fi маршрутизатор D-Link DIR-300 с основными характеристиками:

– диапазон частот: 2.4 ГГц;

– скорость беспроводного соединения: 54 Мбит/с;

– мощность передатчика: 46 dBM;

– интерфейс подключения: Ethernet ;

– защита беспроводной сети: WEP, WPA,WPA2.

Автоматизированное рабочее место (АРМ) – это рабочее место специалиста оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций.

Основными функциями АРМ – работника являются:

– анализ производственной деятельность объекта управления и выявления ожидаемых отклонений от плана;

– сбор статистики по принятию управленческих решений;

– работа в диалоговом режиме;

– составление плана личной работы.

Для АРМ информационное обеспечение создается в виде информационной базы и базы данных. Вычислительные задачи являются как формализуемыми, так и не полностью формализуемыми. Формализуемые задачи решаются на базе формальных алгоритмов. Не полностью формализуемые задачи являются статическими и решаются, такие задачи возникают очень часто при управлении экономическими объектами.

АРМ обладает следующими характеристиками:

– процессор с частотой 2,5 ГГц;

– объем оперативного запоминающего устройства 6 Гб;

– операционная система Windows 8.1;

– 64-разрядная операционная система.

Существующая до начала модернизации ЛВС была организована следующим образом: ЭВМ одной конфигурации общим количеством 4 штуки были объединены wi-fi роутером, который так же обеспечивал доступ к интернет ресурсам и с его помощью осуществлялась функция беспроводной печати.

Схема локальной сети существующей до модернизации, на предприятии ООО «ВНК», представлена на рисунке 5.

На каждом компьютере в офисе стоят офисные пакеты Microsoft Office 2010 и 1С: Предприятие 8.3. При этом сервер 1С: Предприятие поднят на виртуальном сетевом диске АРМ 1. Все ПК офиса подключаются к сетевому диску 1С: Предприятие, как клиенты.

Предприятие имеет две АЗС, на которых также установлены 1С: Предприятие 8.3, вся документация заправок ведется в 1С: Предприятии, однако связи с центральным офисом и главным сервером 1С АЗС не имеют и работают в монопольном режиме. Отчеты о работе работники АЗС отправляют на съемных носителях вместе с дневной выручкой менеджеру отдела закупок и продаж, который лично объезжает АЗС. Для оперативной связи используется телефонная связь.

Недостатками существующей сети являются:

– перегруженность виртуального диска 1С:Предприятия, выполняющего функции сервера на слабом аппаратном обеспечении;

– отсутствие сетевой оперативной связи между АЗС и офисом, в результате, которой сведения об операциях на АЗС обновляется в лучшем случае один раз в день;

– невозможность оперативно контролировать процесс продаж на АЗС;

– сравнительно низкая надежность сети офиса;

– низкая устойчивость к взлому при неправильной настройке роутера;

– отсутствие выделенного сервера сети не позволяет фиксировать атаки на внутреннюю сеть офиса, так как в установленном роутере отсутствует журнализация;

– низкая скорость передачи данных через Wi-Fi роутер. Скорость передачи делится между всеми устройствами Wi-Fi в пределах обслуживания их одной и той же точкой доступа. Это значит, что если точка доступа предоставляет скорость передачи данных 54 Мбит/с и к ней будет одновременно подключено, например, 4 ЭВМ, то скорость передачи данных для каждого ноутбука составит 54 / 4 = 13,5 Мбит/с. А в реальности и того меньше, поскольку объем передаваемой служебной информации может достигать 30-40%. В итоге скорость передачи составляет около 10 Мбит/с на устройство;

– при прохождении через стены (примером наличия данной проблемы является деятельность оператора АРМ 2, который отвечает за торговлю на бирже, так как передача данных осуществляется по средствам беспроводной сети, а роутер имеет достаточно слабый принимаемый и отправляемый сигнал проходящий через стены, большая часть торгов на бирже проигрывалась).

В связи с большим количеством недостатков существующей сети было принято решение о её модернизации.

Процесс модернизации ЛВС, включает в себя выбор и обоснование сетевой архитектуры, которыми являются:

– среда передачи информации (тип кабеля);

– метод доступа к среде;

– обеспечение быстродействия между сотрудниками офиса;

– высокая скорость ЛВС;

– надежность каналов связи;

– пропускная способность;

– метод передачи и т.д.

Сетевая архитектура – это совокупность стандартов, топологий, а также протоколов, необходимых для создания работоспособной сети.

Выбор топологии определяется, в частности, планировкой помещения, в котором разворачивается ЛВС. На сегодняшний день сформировались и устоялись несколько основных топологий. Из них можно отметить «шину», «кольцо» и «звезду». Топология типа «звезда» представляет собой более производительную структуру. Каждый компьютер, в том числе и сервер, соединяется отдельным сегментом кабеля с центральным коммутатором. Данную топологию будем использовать в дальнейшем.

Таким образом, проанализировав локальную вычислительную сеть ООО «ВНК», можно прийти к выводу о том, что дальнейшее развитие предприятия невозможно без существенной модернизации ЛВС. На основе выделенных проблем было составлено техническое задание, которое описывается в приложении А.

2 ОПИСАНИЕ ПРИНЦИПОВ ПРОЕКТИРОВАНИЯ СЕТИ И ТЕХНОЛОГИИ ЕЕ ПОСТРОЕНИЯ

2.1 Назначение и цели модернизации локально-вычислительной сети

Локальная вычислительная сеть (Local Area Network), именуемая в дальнейшем LAN, – это совокупность компьютеров и других средств вычислительной техники (активного сетевого оборудования, принтеров, факсов, модемов и т. п.), объединенных в вычислительную сеть с помощью кабелей и сетевых адаптеров и работающих под управлением сетевой операционной системы.

Модернизируемая локально – вычислительная сеть предназначена для:

– обмена информацией между абонентами сети, что позволяет сократить бумажный документооборот и перейти к электронному документообороту;

– обеспечить распределение обработки данных, связанное с АРМ всех специалистов данной организации в сеть. Несмотря на существенные различия в характере и объеме расчетов, проводимых на АРМ специалистами различного профиля, используемая при этом информация в рамках одной организации находится в единой базе данных, поэтому объединение таких АРМ в сеть является целесообразным и эффективным решением;

– поддержка принятия управленческих решений, предоставляющая руководителям и управленческому персоналу организации достоверную и оперативную информацию необходимую для оценки ситуации и принятия правильных решений;

– организация собственных информационных систем, содержащих АРМ;

– коллективное использование ресурсов, таких как сетевые принтеры, запоминающие устройства большой емкости, мощные средства обработки информации, прикладные программные системы, базы данных базы знаний.

Эффективно эксплуатировать мощности сети позволяет применение технологии «клиент-сервер». В таком случае приложения будут делиться на две части: клиентскую и серверную. Один наиболее мощный компьютер сети конфигурируется как сервер приложений: на нем выполняются серверные части

приложений. Клиентские части выполняются на рабочих станциях; именно на этих рабочих станциях формируются запросы к серверам приложений, а так же отображаются полученные результаты. Для взаимодействия определяется некоторый протокол.

Зачастую каждая сторона модели «клиент-сервер» способна выполнять функции, как сервера, так и клиента. При создании компьютерной сети необходимо выбрать различные компоненты, определяющие, какое программное обеспечение и оборудование будет использоваться, формируя свою корпоративную сеть.

Различия в реализации технологии «клиент-сервер» определяются следующим образом:

– виды программного обеспечения;

– механизмы программного обеспечения;

– способы распределения логических компонентов между компьютерами в сети.

Выделяются четыре подхода, реализованные в следующих технологиях:

– файловый сервер;

– доступ к удаленным данным;

– сервер баз данных;

– сервер приложений.

Компьютерная сеть является неотъемлемой частью современной деловой инфраструктуры, локальная сеть – это лишь одно из используемых в ней приложений и не должна быть единственным фактором, определяющим выбор компонентов сети.

2.2 Выбор топологии для модернизации локально-вычислительной сети

АРМ и другие компоненты локальной сети могут соединяться между собой различными способами. Используемая схема физического расположения сетевых компонентов называется топологией.

Наиболее удобной и практичной является топология «звезда». Достоинства звездоподобной топологии заключаются в том что:

– нарушение соединения в одном месте, кроме центрального узла, не прерывает работы локальной сети;

– при подключении большого количества компьютеров не происходит снижения производительности ;

– безопасность информации обеспечивается на высоком уровне так как, компьютеры не получают чужих данных;

Так же у данной топологии имеются недостатки:

– большой расход соединительного кабеля;

– поломка центрального узла приводит к неработоспособности всей сети;

– наращивание сети сопряжено с большими финансовыми затратами.

Топология «звезда», является на сегодняшний день наиболее надежной и быстродействующей из всех топологий, так как передача данных между АРМами происходит через сервер по отдельным линиям, используемым только этими компьютерами.

В качестве топологии сети выбрана сеть типа «звезда», подобная схема имеет высокую отказоустойчивость. Выход из строя одного или нескольких АРМ не приведет к отказу всей системы.

2.3 Протоколы

Протокол – это набор соглашений интерфейса логического уровня, которые определяют обмен данными между двумя и более, включенными в сеть компьютерами.

Протокол RDP – удобное, эффективное и практичное средство удаленного доступа как для целей администрирования, так и для повседневной работы, на сегодняшний день данный протокол является достаточно защищенным, а так же позволяет скрыть факт туннелирования, то есть для SOCKS-прокси пользователь выглядит так, словно он работает напрямую с арендуемого сервера, а для конечного узла напрямую с SOCKS-прокси.

RDP – использует преимущества сетевой нагрузки (NLB), если таковые имеются. Кроме того, RDP содержит следующие функции:

– поддержка 24-битного кода:

– улучшенную производительность по коммутируемым низкоскоростным соединениям за счет уменьшения пропускной способности;

– Smart Card аутентификацию с помощью служб удаленных рабочих столов;

– перенаправление звука, портов, дисков и сетевого принтера. Звуки, которые воспроизводятся на удаленном компьютере можно услышать на клиентском компьютере под управлением RDC клиента, а так же локальные диски клиента видны удаленному рабочему столу.

От протокола VPN зависит то, как строятся туннели, безопасность созданного туннеля, скорость передачи данных и надежность сети в общем.

Рассмотрим самые популярные VPN протоколы.

PPTP - Этот протокол разработан ассоциацией, возглавляемой Microsoft, и представляет собой туннелирование «точка-точка», то есть создается виртуальная частная сеть внутри общей сети, этот протокол был, есть и остается стандартом VPN с момента создания. Это первый VPN-протокол, поддерживаемый Windows, безопасность обеспечивается различными методами аутентификации, например, самый распространенный из них MS_CHAP v2. Это также самый быстрый протокол, так как для его реализации требуется меньше всего вычислений.

Однако, хотя по умолчанию используется 128-битное шифрование, присутствуют определенные уязвимости безопасности, одна из самых серьезных — не инкапсулированная аутентификация MS-CHAP v2. Из-за этого PPTP можно взломать в течение двух дней. И хотя эта проблема была исправлена Microsoft, все же рекомендуется использовать протоколы SSTP или L2TP для повышенной безопасности.

Достоинства:

– высокая скорость;

– встроенный клиент практически на всех платформах;

– простая настройка.

L2TP и L2TP/IPsec - протокол туннелирования уровня 2, в отличие от других протоколов VPN, не шифрует и не защищает данные. Из-за этого часто используются дополнительные протоколы, в частности IPSec, с помощью которого данные шифруются еще до передачи. Все современные устройства и системы, совместимые с VPN, имеют встроенный протокол L2TP/IPSec. Установка и настройка совершаются легко и не занимают много времени, однако может возникнуть проблема с использованием порта UDP 500, который блокируется файрволлами NAT. Так что, если протокол используется с брандмауэром, может потребоваться переадресация портов.

Неизвестно о каких-либо крупных уязвимостях IPSec, и при правильном применении, этот протокол обеспечивает полную защиту конфиденциальных данных. Но, двукратное капсулирование данных делает протокол не столь эффективным, как, например, решения на основе SSL, но при этом он работает медленнее других протоколов.

Достоинства:

– считаются относительно безопасными протоколами;

– доступны в большинстве систем и почти на всех устройствах;

– простая настройка.

Недостатки:

– медленнее, чем OpenVPN;

– защита протокола нарушена Агентством национальной безопасности США;

– сложно использовать при наличии блокировки со стороны брандмауэра.

2.4 Сетевые технические средства

Каждый сервер, соединяется отдельным сегментом кабеля, подключенным к коммутатору. При необходимости сервер может иметь несколько сетевых карт.

2.4.1 Коммутатор

Коммутатор (Switch) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов. Коммутатор работает на канальном уровне модели OSI, они были

разработаны с использованием мостовых технологий, которые часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат – маршрутизаторы.

В отличие от концентратора, который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю, исключение составляет широковещательный трафик всем узлам сети, а так же трафик для устройств, для которых неизвестен исходящий порт коммутатора. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости обрабатывать данные, которые им не предназначались.

2.4.2 Маршрутизатор

Маршрутизатор (Router) – специализированный сетевой компьютер, имеющий два или более сетевых интерфейса, пересылающий пакеты данных между различными сегментами сети. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором.

Маршрутизаторы работают на более высоком сетевом уровне сетевой модели OSI, нежели коммутатор и концентратор.

2.4.3 Логическая локальная компьютерная сеть

VLAN (Virtual Local Area Network) – логическая локальная компьютерная сеть, которая представляет собой группу хостов с общим набором требований, взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения, вместо физического перемещения устройств.

2.4.4 Спецификация Ethernet

Спецификацию Ethernet в конце семидесятых годов предложила компания

Xerox Corporation. Позднее к этому проекту присоединились компании Digital Equipment Corporation (DEC) и Intel Corporation. В 1982 году была опубликована спецификация на Ethernet версии 2.0. На базе Ethernet институтом IEEE был разработан стандарт IEEE 802.3.

Сети со звездообразной топологией поддерживают технологию Ethernet, это позволяет увеличивать пропускную способность сети в десятки раз, при использовании соответствующих сетевых кабелей и адаптеров.

Метод обнаружения коллизий используется стандартом Ethernet. Адаптеры непрерывно находятся в состоянии прослушивания сети.

Передача сообщений в сети Ethernet производится пакетами со скоростью 10, 100 и 1000 Мбит/с.

2.4.5 Кабель «витая пара»

В настоящее время технология, применяющая кабель на основе витой пары, является наиболее популярной. Такой кабель не вызывает трудностей при прокладке.

Правила сети Ethernet на витой паре:

– максимальное количество расположенных подряд концентраторов не должно превышать четырёх;

– использование кабеля 3 или 5 категории;

– максимальная длина кабельного сегмента – 100 м.

Сеть на основе «витой пары», в отличие от тонкого и толстого коаксиального кабеля, строится по топологии «звезда».

Существуют два вида кабеля «витая пара»:

1) STP (Shielded Twisted Pair) экранированная витая пара;

2) UTP (Unshielded Twisted Pair) неэкранированная витая пара.

Оба эти типа кабеля состоят из пар скрученных проводов. UTP стал наиболее популярным, благодаря своей низкой стоимости. Единственным недостатком данного кабеля является уязвимость к помехам.

Кабели этого типа бывают 3-х категорий:

– 3-я категория – 16 Мбит/с;

– 4-я категория – 25 Мбит/с;

– 5-я категория – 100 Мбит/с.

Для монтажа кабеля используются коннекторы RJ-45.

2.4.6 Волоконно-оптический кабель

Волоконно-оптический кабель (optic fiber cable) – кабель на основе волоконных световодов, который предназначен для передачи оптических сигналов в линиях связи.

Достоинства:

– высокая скорость передачи информации (от 1 до 10 Гбит/с на расстоянии 1 км);

– малые потери;

– высокая помехозащищённость (невосприимчивость к различного рода помехам);

– небольшие габаритные размеры и масса;

– возможность доводить расстояния между передающим и приёмным устройствами до 400–800 км.

Недостатки:

– уменьшение полосы пропускания при воздействии ионизирующих излучений вследствие увеличения поглощения оптического излучения световедущей жилой;

– трудоёмкость сварки и ослабление сигнала в месте сварного шва;

– риск поражения сетчатки глаза световым излучением.

2.5 Сетевые программные средства

Существует множество программных средств, которые предоставляют возможность управления сетью. Для управления сетью используются такие программные продукты, как Friendly Pinger, а так же подключаемый модуль noVNC.

2.5.1 Friendly Pinger

Friendly Pinger – это бесплатное приложение для администрирования, мониторинга и инвентаризации компьютерных сетей. Данное программное

обеспечение обладает следующими функциональными возможностями:

– визуализация компьютерной сети в анимационной форме;

– отображение, какие компьютеры включены, а какие нет;

– пингование всех устройств за один раз;

– оповещение в случае остановки или запуска серверов;

– инвентаризация программного, аппаратного обеспечения всех ЭВМ в сети;

– назначение внешних команд (например, telnet, tracert, net.exe) устройствам;

– поиск HTTP, FTP, e-mail и других сетевых служб;

– отображение состояния сети на рабочем столе или Web-странице;

– графический TraceRoute;

– функция «Создать дистрибутив» позволяет создать облегченную версию с вашими картами и настройками.

2.5.2 Windows Server 2012

Windows Server 2012 – серверная операционная система, которая может выполнять роли файлового сервера, сервиса службы web-приложений, сервера терминалов, службы DNS (доменных имен), службы каталогов, сервера потоков, мультимедиа и другие.

Windows Server является достаточно быстрой и надежной ОС. Надежность обеспечивает платформа приложений, в которую встроены функции сервера приложений, а также интегрированная среда обеспечивающая доступность и безопасность информации.

Эту ОС достаточно просто развернуть и проводить ее администрирование. Она дает возможность управлять сетью с помощью политик и автоматизации выполнения каких-либо задач.

Для организаций, работающих с важными сетевыми бизнес-приложениями очень важна служба кластеров, позволяющая объединить несколько серверов. Узлы в кластере взаимно заменяемы. То есть, если один из серверов становится недоступным, обслуживание переходит на другой сервер.

Очень многие особенности Windows Server дают возможность

сотрудникам организации работать более производительно. Файловые службы и службы печати позволяют управлять файловыми ресурсами, в то же время сохраняется безопасность и доступ для пользователей. Служба каталогов в Windows Server называется Active Directory. Благодаря этой службе сохраняются сведения о сетевых объектах, кроме того Active Directory позволяет администратору быстро найти данную информацию, также упрощает работу по проектированию, развертыванию и управлению каталогами сети.

Для управления доступом к файлам и папкам, на выделенных серверах используется система Access Control List, которая позволяет давать доступ только на основании учетных записей пользователей или членства пользователя в группе.

Модель управления доступом выглядит так: существует общая папка на уровне NTFS. Для доступа к ней составлялся список групп или пользователей, имеющих право доступа.

У такой модели присутствуют некоторые недостатки:

– если есть достаточно много общих ресурсов, то требуется создать много групп;

– нельзя проконтролировать доступ с учетом каких-либо атрибутов пользователя либо характеристик устройства, с которого осуществляется подключение, достаточно членства пользователя в определенной группе;

– достаточно проблематично осуществить сложные сценарии доступа. Пользователь может случайно выложить закрытую информацию в общую папку, где каждый из членов группы может ее прочитать.

Так же Windows Server 2012 обеспечивает ряд основных преимуществ:

– Windows Server 2012 позволяет лучше контролировать инфраструктуру серверов и сети и сконцентрироваться на решении задач первоочередной важности благодаря следующему:

– упрощенное управление ИТ-инфраструктурой с помощью новых средств, обеспечивающих единый интерфейс для настройки и мониторинга серверов и возможность автоматизации рутинных операций;

– оптимизация процессов установки Windows Server 2012 и управления ими за счет развертывания только нужных ролей и функций. Настройка конфигурации серверов уменьшает количество уязвимых мест и снижает потребность в обновлении программного обеспечения, что приводит к упрощению текущего обслуживания;

– эффективное обнаружение и устранение неполадок с помощью мощных средств диагностики, дающих наглядное представление об актуальном состоянии серверной среды, как физической, так и виртуальной;

– улучшенный контроль над удаленными серверами, например серверами филиалов. Благодаря оптимизации процессов администрирования серверов и репликации данных вы сможете лучше обслуживать своих пользователей и избавитесь от некоторых управленческих проблем;

– облегченное управление веб-серверами с помощью Internet Information Services 7.0 – мощной веб-платформы для приложений и служб.

Эта модульная платформа имеет более простой интерфейс управления на основе задач и интегрированные средства управления состоянием веб-служб, обеспечивает строгий контроль над взаимодействием узлов, а также содержит ряд усовершенствований по части безопасности:

– улучшенный контроль параметров пользователей с помощью расширенной групповой политики;

– встроенные технологии для виртуализации на одном сервере нескольких операционных систем (Windows, Linux и т. д.). Благодаря этим технологиям, а также более простым и гибким политикам лицензирования сегодня можно без труда воспользоваться преимуществами виртуализации, в том числе экономическими;

– централизованный доступ к приложениям и беспрепятственная интеграция удаленно опубликованных приложений. Кроме того, нужно отметить возможность подключения к удаленным приложениям через межсетевой экран без использования VPN – это позволяет быстро реагировать на потребности пользователей, независимо от их местонахождения;

– широкий выбор новых вариантов развертывания;

– гибкие и функциональные приложения связывают работников друг с другом и с данными, обеспечивая таким образом наглядное представление, совместное использование и обработку информации;

– взаимодействие с существующей средой;

– развитое и активное сообщество для поддержки на всем протяжении жизненного цикла.

Windows Server 2012 усиливает безопасность операционной системы и среды в целом, формируя надежный фундамент, на котором вы сможете развивать свой бизнес. Защита серверов, сетей, данных и учетных записей пользователей от сбоев и вторжений обеспечивается Windows Server за счет следующего:

– усовершенствованные функции безопасности уменьшают уязвимость ядра сервера, благодаря чему повышается надежность и защищенность серверной среды;

– технология защиты сетевого доступа позволяет изолировать компьютеры, которые не отвечают требованиям действующих политик безопасности. Возможность принудительно обеспечивать соблюдение требований безопасности является мощным средством защиты сети;

– усовершенствованные решения по составлению интеллектуальных правил и политик, улучшающих управляемость и защищенность сетевых функций, позволяют создавать регулируемые политиками сети;

– защита данных, которая разрешает доступ к ним только пользователям с надлежащим контекстом безопасности и исключает потерю в случае поломки оборудования;

– защита от вредоносных программ с помощью функции контроля учетных записей с новой архитектурой проверки подлинности;

– повышенная устойчивость системы, уменьшающая вероятность потери доступа, результатов работы, времени, данных и контроля.

3 МОДЕРНИЗАЦИЯ ЛОКАЛЬНОЙ СЕТИ ОБМЕНА ДАННЫМИ ООО «ВНК»

3.1 Обоснование выбора используемого оборудования локальной сети

В основе проектировании ЛВС предприятия выбрана архитектура клиент – сервер. Топология сети – звезда. Данная конфигурация позволит рационально развернуть сеть без больших затрат, архитектура клиент – сервер позволит снизить системные требования с АРМ-ов сотрудников, так как все необходимые процессы буду проходить на сервере.

Стабильность работы локальной сети обмена данными ООО «ВНК» зависит в большей части от правильного выбора оборудования, организующего сеть. Оборудование должно поддерживать протоколы RDP.

Lenovo System x3250 M5 Rack будет выступать в качестве сервера. Данное оборудование, будет обеспечивать многопользовательский режим работы сотрудников компании, так же работу в системе программ 1С: предприятие и хранение базы данных, в таком случае сервер должен обеспечивать максимальную защищенность и безопасность выполняемых задач, а так же их сохранность. Выбранный сервер обладает следующими параметрами:

– 64 – разрядная операционная система Windows server 2012;

– четырехъядерный процессор с частотой 3.5 ГГц;

– объем оперативного запоминающего устройства 16 Гб.

Рисунок 8 – Сервер Lenovo System x3250 M5 Rack

В локальную сеть также встраивается маршрутизотор - MikroTik RouterBoard RB2011UiAS-RM. Данный маршрутизатор кроме 5 гигабитных и пяти 100 мегабитных портов имеет RJ45 serial порт и порт microUSB 2.0, также имеется порт SFP для установки модулей (не прилагаются). Также для удобства конфигурирования на лицевой стороне находится сенсорный LCD экран. Маршрутизатор MikroTik RB2011UiAS-RM использует RouterOS L5, открывающую такие возможности как динамические маршруты, хотспот, firewall, MPLS, VPN, конфигурирование и мониторинг в реальном времени, а также многое другое. Для работы с провайдерами и магистральными сетями предусмотрены 5 гигабитных портов, а для устройств, не требующих большой ширины канала есть 5 портов по 100 МБит. Данный маршрутизатор будет обеспечивать хорошую пропускную способность на предприятии и полностью обеспечит связь между АРМ-ми работников.

Рисунок 9 – Маршрутизатор MikroTik RouterBoard RB2011UiAS-RM

3.1.1 Обоснование выбора используемого программного обеспечения, для защиты локальной сети

В настоящее время существует большое количество вирусов, основная часть которых попадает в компьютеры из-за наличия «дыр» в сетевой безопасности, поэтому необходима качественная защита от киберугроз во всех рабочих средах.

В погоне за соотношением цены и качества безусловным лидером на рынке антивирусных программ является Kaspersky, а разнообразие предлагаемых пакетов антивирусного обеспечения с разнообразным набором функций, позволяет подобрать подходящий вариант программного обеспечения.

В качестве антивирусного ПО на предприятии, ООО «ВНК» будет установлен – Kaspersky Small Office Security, в его функции входит:

– защита от вредоносного ПО;

– сочетание сигнатурных и облачных технологий;

– защита от спама;

– блокирование нежелательных сообщений;

– менеджер паролей ;

– создание и хранение надежных паролей;

– антифишинг;

– блокирование мошеннических ссылок;

– безопасные платежи;

– защита финансовых операций онлайн;

– резервное копирование;

– гарантия сохранности ваших данных;

– веб-контроль;

– контроль использования интернет-ресурсов;

– шифрование на уровне файлов.

Каждое предприятие нуждается в сохранности и целостности данных, для этого существует термин, как резервное копирование. Резервное копирование - процесс создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения. В качестве программного обеспечения для резервного копирования мы будем использовать Acronis backup. Acronis обеспечивает непрерывную работу путем предотвращения простоев или аварийного восстановления за считанные секунды. Acronis также защищает любую информацию вне зависимости от используемых технологий и объемов создаваемых данных. Данный продукт имеет большой диапазон настроек данного ПО, выбор периодичности резервного копирования, выбор источника резервных копий. Быстрая скорость восстановления данных за счет хорошей оптимизации приложения.

3.2 Модернизация локальной сети обмена данными ООО «ВНК»

Исходя из существующих данных, произведено построение плана локальной сети обмена данными ООО «ВНК» в составе следующих объектов:

– АРМ – работника 1и 2 персональный компьютер;

– АРМ – бухгалтера.

План локальной сети обмена данными ООО «ВНК» показан на рисунке

14.

На данной схеме отражено подключение сервера к рабочим АРМам. К каждому АРМ подведен UTP, который обеспечивает улучшенные характеристики передачи данных и большую пропускную способность канала. Так же изображен маршрутизатор, с помощью которого происходит объединение нескольких сетевых устройств. Доступ к сетевому принтеру осуществляется с помощью локальной сети, так же все АРМ имеют общее сетевое пространство, которое позволяет существенно облегчить взаимосвязь между сотрудниками компании.

К общему серверу подсоединены камеры видеонаблюдения, сигнал с которого передается в свою очередь на монитор работника, что позволяет отображать «картинку» в реальном времени. Запись с камер так же резервируется через локальную сеть и записывается с помощью видеорегистратора.

Для лучшего обзора устанавливаются панорамные IP – камеры Cobell HD 960 P, позволяющие обеспечить угол обзора в 180 градусов по горизонтали. Данная модель камеры может работать с двумя видеоформатами: традиционным для камер MJPEG и H.264.

IP-видеорегистратор HIWATCH DS-N316/2 подключается через коммутатор к IP-камерам видеонаблюдения, что позволяет вести видеонаблюдение в режиме реального времен, но и сохранять запись с камер видеонаблюдения. У данной модели видеорегистратора, имеется возможность расширения памяти с помощью дополнительных жестких дисков.

Рисунок 11 – IP-видеорегистратор HIWATCH DS-N316/2

Соединение IP-камеры видеонаблюдения и IP-видеорегистратора с

сервером осуществляется с помощью UTP кабеля, так же каждой камере присваивается свой IP – адрес, необходимый для передачи изображения на соответствующий компьютер, а также для централизованного сбора и обработки информации, которая поступает от сетевых камер. Основными функциональными возможностями IP-видеорегистратора являются:

– возможность расширения системы видеонаблюдения. (Пользователи могут увеличивать количество камер, а также объем хранения данных.);

– возможность работы с большим количеством объектов. Если необходимо осуществлять контроль большого количества объектов, сетевой IP видеорегистратор просто незаменим;

– качество изображения. Формат MPEG-4 позволяет обеспечить высокое качество видеофайлов.

АЗС подключаем к интернет соединению посредством USB модема от провайдера МТС, данный провайдер обеспечивает высокую скорость соединения посредством беспроводной высокоскоростной передачи данных, так называемой LTE. Спецификация LTE позволяет обеспечить скорость загрузки до 326,4 Мбит/с, скорость отдачи до 172,8 Мбит/с, а задержка в передаче данных может быть снижена до 5 миллисекунд. LTE поддерживает полосы пропускания частот от 1,4 МГц до 20 МГц и поддерживает как частотное разделение каналов (FDD), так и временное разделение (TDD). В нашем случае мы будем использовать модем МТС 827F он же Huawei E3372. Его технические характеристики:

– поддерживаемые стандарты и частоты: 2G - GSM / GPRS / EDGE - 850 /900 / 1800 / 1900 МГц, 3G - UMTS / DC-HSPA+ / WCDMA - 900 / 2100 МГц, 4G - LTE 800/1800/2600;

– скорость приёма данных модемом до 100 Мбит/с;

– скорость передачи данных - до 50 Мбит/с.

С помощью сервиса Open VPN мы объединяем сеть. Она позволит нам установить соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек.

Схема представлена на рисунке 12.

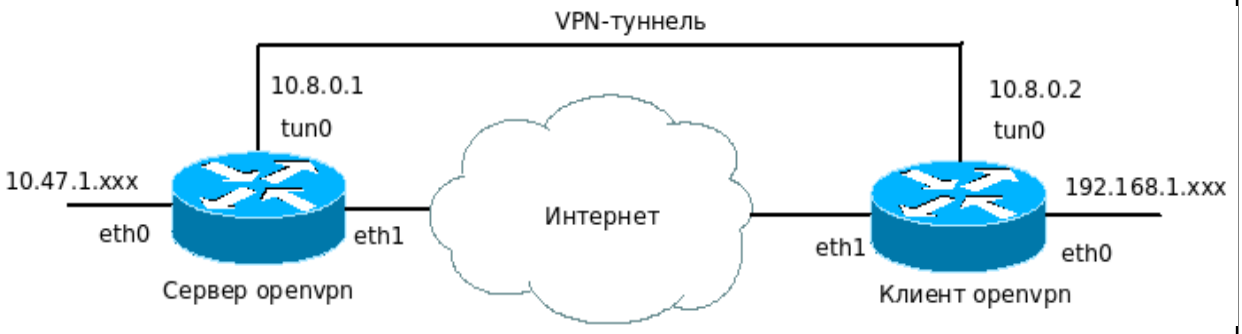

Рисунок 12 – Схема объединения с помощью VPN-туннеля

Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку OpenSSL. Это позволит нам задействовать весь набор алгоритмов шифрования, доступных в данной библиотеке. Также может использоваться пакетная аутентификация HMAC, для обеспечения большей безопасности, и аппаратное ускорение для улучшения производительности шифрования. Эта библиотека использует OpenSSL, а точнее протоколы SSLv3/TLSv1.2. Важно, чтобы на сервере был статический адрес.

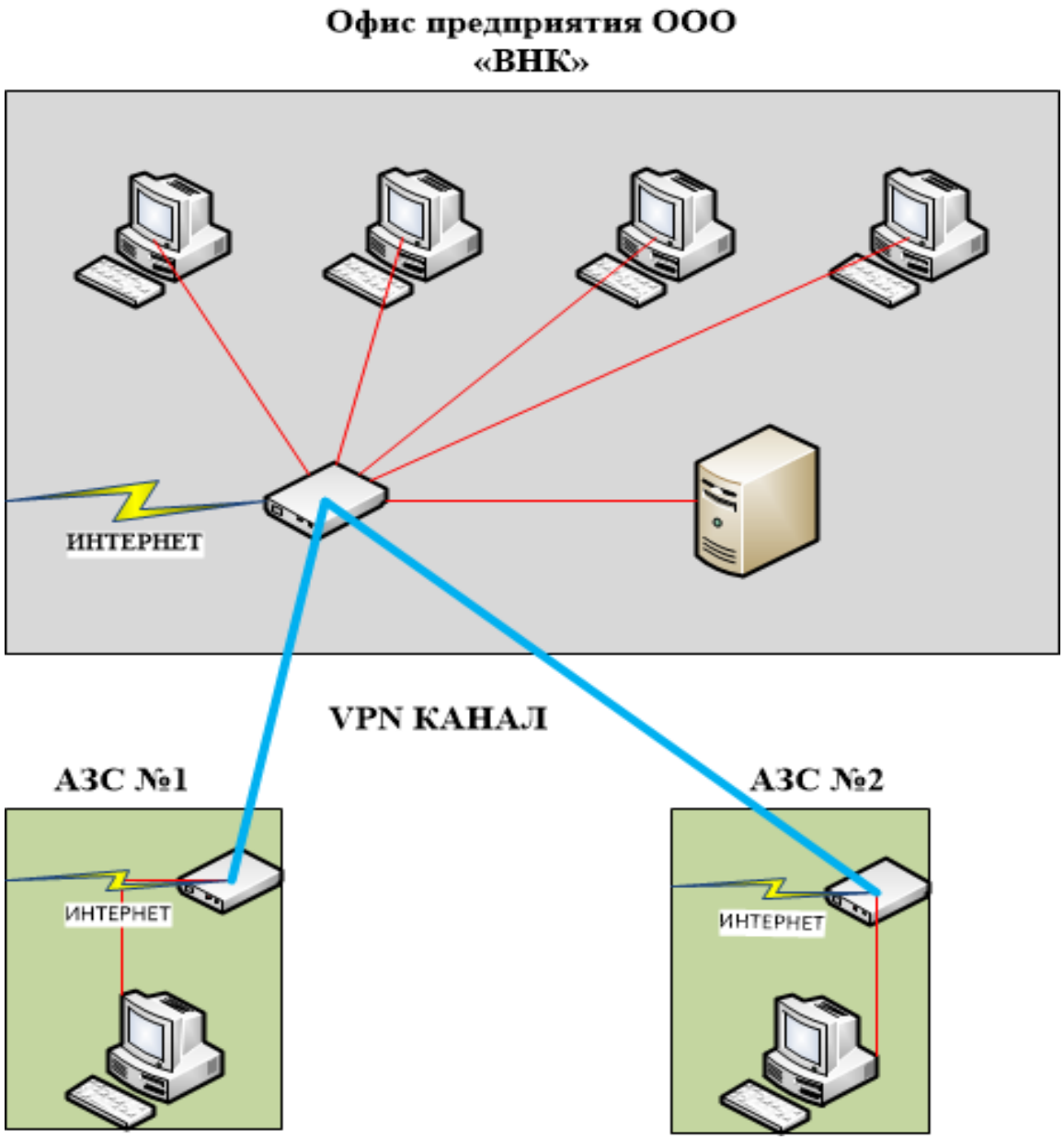

Рисунок 13 – Общая схема ЛВС предприятия ООО «ВНК» после модернизации

Данная схема показывает связь между АЗС и офисом ООО «ВНК». С помощью данной модернизации мы добились связи между АЗС и офисом, отчеты с АЗС будут идти в электронном виде на сервер, тем самым можно будет просматривать продажи в реальном времени и сократить расходы на разъезд менеджера по точкам.

Подробная схема ЛВС офиса данного предприятия представлена на рисунке 14.

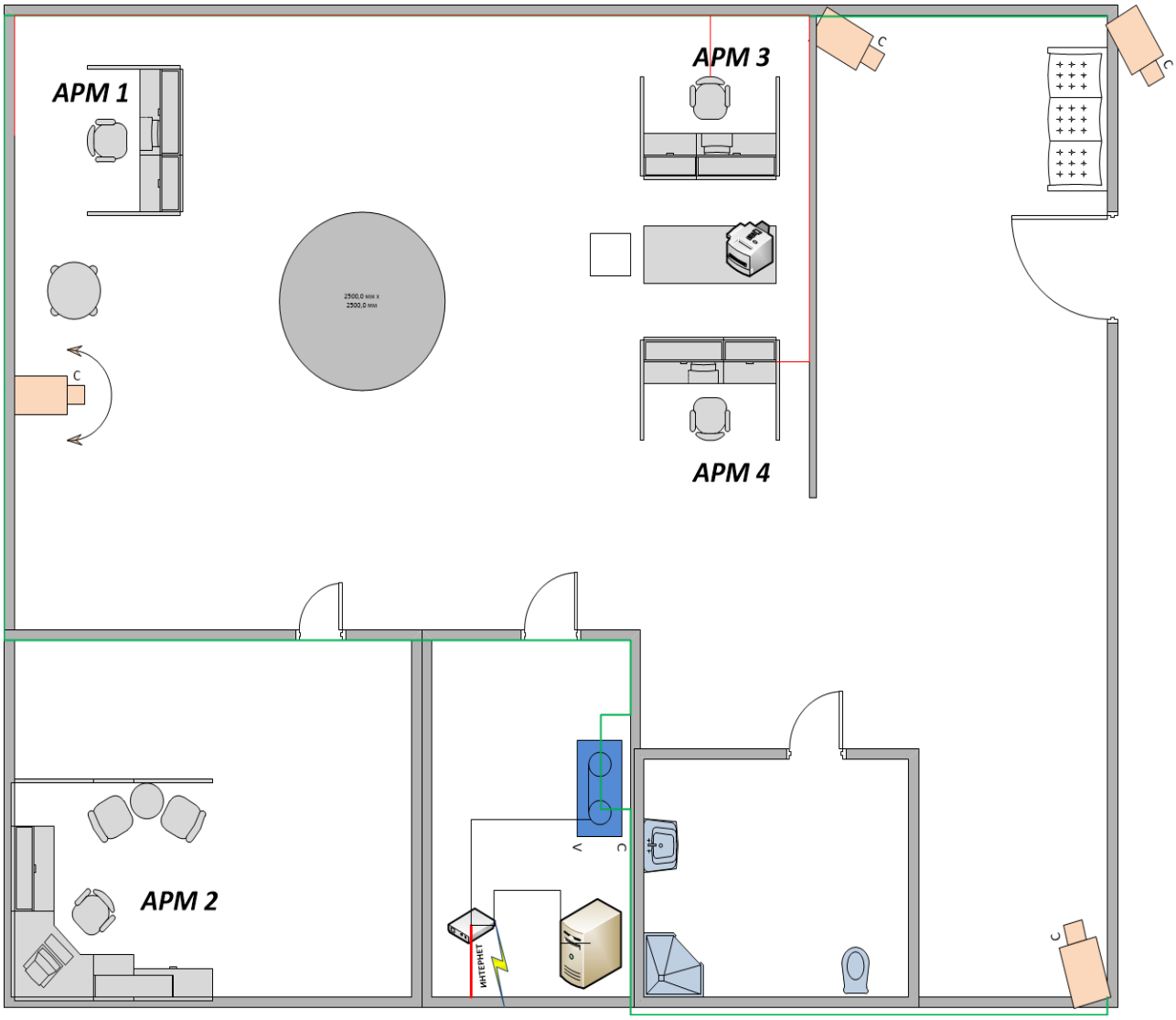

Рисунок 14 – Схема ЛВС офиса ООО «ВНК» после модернизации

После проведения модернизации локальной сети предприятия, улучшилось не только взаимодействие между сотрудниками, которое осуществляется с помощью доступа к единым информационным ресурсам, а также периферийным устройствам и сети интернет, но и безопасность офиса компании. Взаимосвязь между АЗС и офисом обеспечена, тем самым уменьшили расходы предприятия.

3.2.1 Расчет стоимости оборудования.

Примерный расчет стоимости оборудования для модернизации ЛВС ООО «ВНК» представлен в таблице 1. Стоимость оборудования может отличаться в зависимости от политики цен в магазинах.

Таблица 1 – Расчет стоимости оборудования для модернизации ЛВС предприятия ООО «ВНК»

Смета на материалы и оборудование	Кол-во	Ед.	Цена (руб.)	Сумма (руб.)
Маршрутизатор Mikrotik RB2011UiAS-RM	1	шт.	7200	7200
Сервер Lenovo System x3250 M5 Rack	1	шт.	48000	48000
Видеорегистратор HIWATCH DS-N316/2	1	шт.	4490	4490
Камера Cobell HD 960 P	2	шт.	2570	5140
USB – модем Huawei E3372	2	шт.	2430	4860
Кабель UTP 5e 0.50 CU (100м бухта)	1	шт.	1490	1490
Камера Cobell HD 960	2	шт.	1490	2980
Расходные материалы	1	шт.	700	700
ИТОГО:		***74860*** (руб.)		

После проведения расчета можно сделать вывод, о том что стоимость модернизации довольно не маленькая, но при этом ПК операторов разгрузятся, тем самым работа с программой 1С: Предприятие станет более эффективной.

3.3 Защита информации

Под информационной безопасностью систем понимается поддержание физической сохранности, целостности, доступности, конфиденциальности, достоверности и своевременности информации, а также гарантированной работоспособности средств, используемых для ввода, хранения, обработки и передачи данных.

Целями защиты информации предприятия являются:

– предупреждение хищения, утечки, утраты, искажения, подделки конфиденциальной информации (персональных данных);

– предотвращение угроз безопасности личности и предприятия;

– предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение, конфиденциальности документированной информации в соответствии с законодательством.

3.3.1 Основные угрозы информационной безопасности.

Угрозой является потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации. Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Такие угрозы, воздействуя на ресурсы, могут привести к искажению данных, копированию, несанкционированному распространению, ограничению или блокированию к ним доступа. В настоящее время известно достаточно большое количество угроз, которые классифицируют в соответствии с рисунком 16:

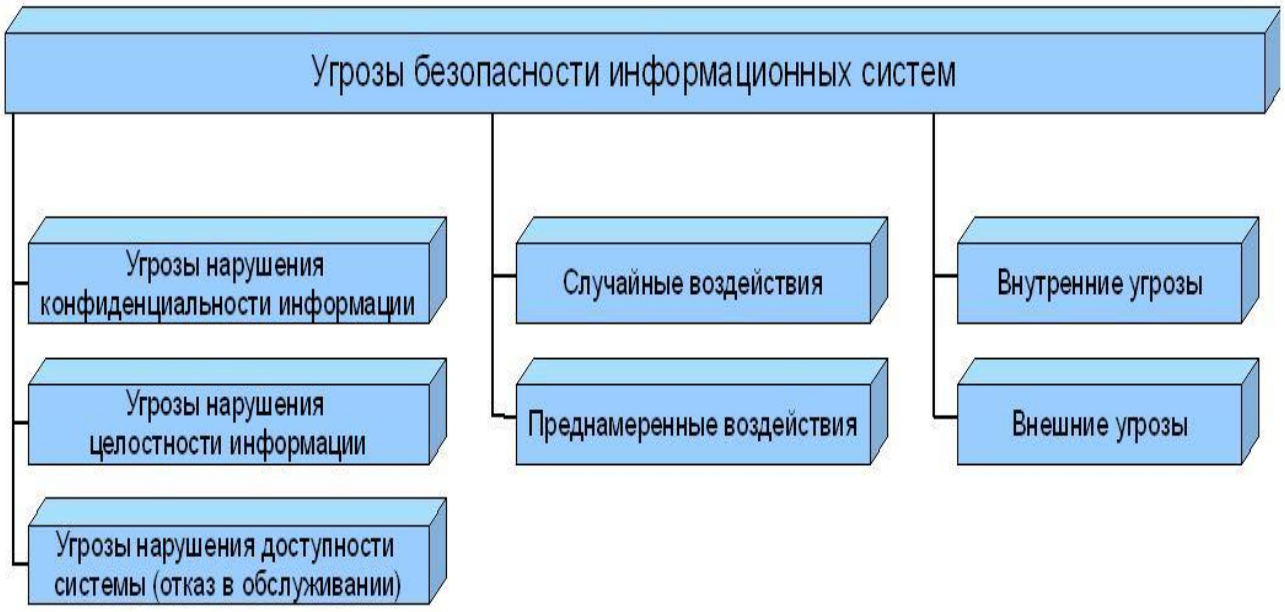

Рисунок 16 – Схема угроз информационной безопасности

3.3.2 Типы угроз информационной безопасности

Основные типы угроз информационной безопасности:

– угрозы конфиденциальности;

– угрозы целостности;

– угрозы доступности.

Угрозы нарушения конфиденциальности направлены на получение (хищение) конфиденциальной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. Несанкционированный доступ к информации, хранящейся в информационной системе или передаваемой по каналам (сетям) передачи данных, копирование этой информации является нарушением конфиденциальности информации.

Угрозы нарушения целостности информации, хранящейся в информационной системе или передаваемой посредством сети передачи данных, направлены на изменение или искажение данных, приводящее к нарушению качества или полному уничтожению информации. Целостность информации может быть нарушена намеренно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему (помехи). Эта угроза особенно актуальна для систем передачи информации – компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется авторизованными пользователями с обоснованной целью.

Угрозы нарушения доступности системы (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым её ресурсам.

3.3.3 Угрозы по характеру возникновения

Угрозы по характеру возникновения разделяют на:

– случайные;

– преднамеренные.

Причины случайных воздействий:

– аварийные ситуации из-за стихийных бедствий и отключения электроэнергии;

– ошибки в программном обеспечении;

– ошибки в работе обслуживающего персонала и пользователей;

– помехи в линии связи из-за воздействия внешней среды, а также вследствие плотного трафика в системе (характерно для беспроводных решений).

Примерами случайных угроз могут быть:

– неосторожные действия, приводящие к разглашению информации ограниченного доступа или делающие ее общедоступной;

– передача сторонним лицам сведений, документов и носителей, составляющих или содержащих конфиденциальную информацию, обрабатываемую в информационной системе;

– подмена существующей информации (ввод ошибочных данных, удаление данных и т.п.).

Преднамеренные воздействия связаны с целенаправленными действиями злоумышленника, в качестве которого может выступить любое заинтересованное лицо (конкурент, посетитель, персонал и т.д.). Действия злоумышленника могут быть обусловлены разными мотивами: недовольством сотрудника своей карьерой, материальным интересом, любопытством, конкуренцией, стремлением самоутвердиться любой ценой и т.п.

Для проникновения в компьютерную систему с целью дальнейшего хищения или уничтожения информации используются такие методы и средства шпионажа, как прослушивание, хищение программ, атрибутов защиты, документов и носителей информации, визуальное наблюдение, заражение ПК вредоносными программами и другие.

3.3.4 Внутренние и внешние угрозы

Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию. Причинами возникновения таких угроз может послужить нездоровый климат в

коллективе или неудовлетворенность от выполняемой работы некоторых сотрудников, которые могут предпринять действия по выдаче информации лицам, заинтересованным в её получении.

Также имеет место так называемый "человеческий фактор", когда человек не умышленно, по ошибке, совершает действия, приводящие к разглашению конфиденциальной информации или к нарушению доступности информационной системы. Большую долю конфиденциальной информации злоумышленник (конкурент) может получить при несоблюдении работниками-пользователями компьютерных сетей элементарных правил защиты информации. Это может проявиться, например, в примитивности паролей или в том, что сложный пароль пользователь хранит на бумажном носителе на видном месте или же записывает в текстовый файл на жестком диске и пр. Утечка конфиденциальной информации может происходить при использовании незащищенных каналов связи, например, по телефонному соединению.

Под внешними угрозами безопасности понимаются угрозы, созданные сторонними лицами и исходящие из внешней среды, такие как:

– атаки из внешней сети (например, Интернет), направленные на искажение, уничтожение, хищение информации или приводящие к отказу в обслуживании информационных систем предприятия;

– распространение вредоносного программного обеспечения;

– нежелательные рассылки (спам);

– перехват информации с использованием радиоприемных устройств;

– воздействие на персонал предприятия с целью получения конфиденциальной информации.

В современном мире, когда стало возможным применять сервисы и службы с использованием информационной коммуникационной среды (электронные платежи, Интернет-магазины, электронные очереди и т.п.), многократно увеличивается риск именно внешних угроз.

3.3.5 Перечень информации подлежащей защите

Защищаемая информация делится на следующие виды:

– информация, составляющая коммерческую тайну (научно-техническая, производственная, финансово-экономическая или иная информация, которая имеет коммерческую ценность;

– персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

– иная информация, не относящаяся ни к одному из указанных выше видов, которая определена как защищаемая в соответствии с нормативно-правовыми актами РФ.

К сведениям, составляющим коммерческую тайну, хранящимся и обрабатываемым на предприятии можно отнести:

– сведения, содержащиеся в бухгалтерских книгах предприятия;

– сведения о заработной плате сотрудников;

– сведения о готовящихся, принятых и исполняемых решениях руководства организации и ее подразделений по различным вопросам ведения коммерческой деятельности;

– сведения, связанные с финансовым кругооборотом, платежными расчетами, состоянием банковских счетов, различными кредитными операциями, уровнем доходов и расходов, а так же циркуляцией денежных средств;

– сведения, содержащиеся в контрактах и других документах, определяющих порядок соглашения и обязательства организации перед партнерами;

– бухгалтерские и финансовые отчеты.

К сведениям, являющимися персональными данными, хранящимся и обрабатываемым в информационной системе можно отнести:

– сведения, составляющие контактную и личную информацию граждан;

– сведения, составляющие контактную и личную информацию сотрудников организации.

3.3.6 Требования безопасности

Политика безопасности должна быть реалистичной и выполнимой, краткой и понятной, а также не приводить к существенному снижению общей производительности бизнес-подразделений компании и оправдывать вложения, потраченные на ее создание.

Политика безопасности должна:

– указывать на причины и цели создания политики безопасности;

– должна быть написана понятным языком для конечных пользователей и руководства компании и быть по возможности краткой;

– должна определять цели ИБ, способы их достижения и ответственность;

– политика безопасности должна быть реальной и осуществимой;

– определить ответственных по политике безопасности.

Для информации, циркулирующей в системе, в соответствие с ее разделением по степени важности должны быть сформулированы правила доступа для объектов.

Сформируем минимальные требования безопасности к защищаемой системе.

Минимальные требования безопасности охватывают административный, процедурный и программно-технический уровни ИБ.

Организация должна разработать, документировать и обнародовать официальную политику безопасности и формальные процедуры, периодически производить оценку рисков, включая оценку угроз миссии, функционированию, имиджу и репутации организации, ее активам и персоналу направленные на выполнение приведенных ниже требований, и обеспечить эффективную реализацию политики и процедур.

Минимальные требования безопасности:

– протоколирование и аудит;

– аутентификация, авторизация;

– регулярная смена паролей;

– обеспечение целостности;

– защита носителей;

– информирование и обучение персонала;

– оценка рисков;

– кадровая безопасность;

– физическая защита;

– управление конфигурацией;

– политика ИБ;

– защита систем и телекоммуникаций;

– реагирование на нарушение ИБ.

Для обеспечения безопасности информации необходимо ввести разграничение прав доступа. Так, например, при необходимости внесения изменений, добавления новой информации или полного пересмотра состава сведений отнесенных к персональным данным доступ будет разрешен только лицам, имеющим соответствующие права, которые займутся данной работой. Обеспечить управление доступом, предоставив доступ к активам ИС только авторизованным пользователям, процессам, действующим от имени этих пользователей, а также устройствам (включая другие ИС) для выполнения разрешенных пользователям транзакций и функций.

Для обеспечения протоколирования и аудита необходимо:

– создавать, защищать и поддерживать регистрационные журналы, позволяющие отслеживать, анализировать, расследовать и готовить отчеты о незаконной, несанкционированной или ненадлежащей активности;

– обеспечить прослеживаемость действий в ИС с точностью до пользователя (подотчетность пользователей).

В области идентификации и аутентификации необходимо обеспечить идентификацию и аутентификацию пользователей ИС, процессов, действующих от имени пользователей, а также устройств как необходимое условие предоставления доступа к ИС.

Для защиты носителей:

– защищать носители данных как цифровые, так и бумажные;

– предоставлять доступ к данным на носителях только авторизованным пользователям;

– сканировать или уничтожать носители перед выводом из эксплуатации или перед передачей для повторного использования.

Для обеспечения целостности систем и данных:

– своевременно идентифицировать дефекты ИС и данных, докладывать о них и исправлять;

– защищать ИС от вредоносного программного обеспечения;

– отслеживать сигналы о нарушениях безопасности и сообщения о новых угрозах для информационной системы и должным образом реагировать на них.

Для информации, являющейся персональными данными сотрудников предприятия, правила должны выполняться в следующем виде.

К информации допущено высшее руководство предприятия, сотрудники службы безопасности, сотрудники кадрового отдела, представители государственных органов по официальному запросу, а так же лица-собственники информации.

Внесение изменений в данные сведения осуществляется с письменного разрешения собственника.

Данные в системе должны храниться в закрытых каталогах. Доступ к закрытым каталогам могут иметь руководители, сотрудники кадрового отдела и администратор информационной системы. Доступ осуществляется только авторизированными пользователями.

Система должна иметь свой файерволл от несанкционированного доступа и утечки информации, для каждого пользователя так же должен быть присвоен пароль (не менее 6 символов с использованием заглавных букв, а также цифр и пробелов).

Обработка данной информации может осуществляться свободно, сотрудниками кадрового отдела и администратором информационной системы. Копирование или перенос информации из защищенных каталогов запрещено.

Данные сведения не должны копироваться на отчуждаемые носители.

Передача информации за пределы информационной системы лицам, участвующим в коммерческом взаимодействии, или органам государственной власти может осуществляться свободно, сотрудниками кадрового отдела.

Поскольку компания несет ответственность за сохранность персональных данных своих сотрудников, то она должна обеспечить их защищенность. Так же должны выполняться требования определенные Федеральным законом «О персональных данных» от 27.07.2006 N 152-ФЗ.

3.4 Политика безопасности, предъявляемая к локальной сети

Политика безопасности устанавливает правила которые определяют конфигурацию систем действия служащих организации в обычных условиях и в случае непредвиденной ситуации. Формируя политику обеспечения безопасности, администратор прежде всего проводит инвентаризацию ресурсов, защита которых планируется, идентифицирует пользователей, которым требуется доступ к каждому из этих ресурсов, и выясняет наиболее вероятные источники опасности для каждого из этих ресурсов.

Политика обеспечения безопасности включает несколько элементов:

– оценка риска. Нужно идентифицировать ценности, находящиеся в сети, и возможные источники проблем;

– ответственность. Необходимо указать ответственных за принятие тех или иных мер по обеспечению безопасности, начиная от утверждения новых учетных записей и заканчивая расследованием нарушений;

– правила использования сетевых ресурсов. В политике должно быть прямо сказано, что пользователи не имеют права употреблять информацию не по назначению, использовать сеть в личных целях, а также намеренно причинять ущерб сети или размещенной в ней информации;

– юридические аспекты. Необходимо проконсультироваться с юристом и выяснить все вопросы, которые могут иметь отношение к хранящейся или генерируемой в сети информации, и включить эти сведения в документы по обеспечению безопасности;

– процедуры по восстановлению системы защиты. Следует указать, что должно быть сделано в случае нарушения системы защиты и какие действия будут предприняты против тех, кто стал причиной такого нарушения.

В качестве правил использования сетевых ресурсов, можно использовать разграничение прав доступа. Права доступа — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы (информации, её носителям, процессам и другим ресурсам) установленных правовыми документами или собственником, владельцем информации.

Каждый сотрудник получает возможность работать только с теми ресурсами, которые ему необходимы, при этом все документы защищены от случайного или намеренного просмотра или изменения. Разграничение прав доступа в офисе компании ООО «ВНК», производится посредством, определения персонального логина и пароля для каждого сотрудника.

Один из вариантов построения локальной сети – это сеть на основе сервера. Контроллер домена – это решение для администрирования групп, предоставляющее каждому пользователю учетную запись в конкретном домене. Создание контроллера домена влечет за собой установку такого системного механизма, как Active Directory – основного средства создания, настройки и управления учетными записями пользователей и компьютеров локальной сети. Одним из безусловных плюсов доменной системы является возможность гибкой настройки групповых политик, с помощью которых можно ограничивать доступ не только к программной, но и к аппаратной части компьютера. Например, легко можно запретить использование DVD-привода, флеш-накопителей и т.д.

Active Directory – это службы каталогов корпорации Microsoft для операционных систем семейства Windows Server. Позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager, устанавливать обновления операционной

системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя Службу обновления Windows Server.

Установив политику безопасности в одном месте, администраторы могут контролировать безопасность всех серверов и рабочих станций домена. Политики безопасности в Windows Server 2012 реализуются с помощью средств групповых политик.

Также на предприятии должна быть организована регулярная смена паролей. Один раз в 2 месяца системный администратор меняет пароли. Пароли должны соответствовать современным требованиям составления паролей.

Законодательные и административные меры для регулирования вопросов защиты информации на государственном уровне применяются в большинстве развитых стран мира. Политика информационной безопасности предприятия определяет:

– какую информацию и от кого (чего) следует защищать;

– кому и какая информация требуется для выполнения служебных обязанностей;

– какая степень защиты требуется для каждого вида информации;

– чем грозит потеря того или иного вида информации;

– как организовать работу по защите информации.

Решения по этим вопросам принимают руководитель организации, а также сотрудники, имеющие право решать, какой риск должен быть исключен, а на какой можно пойти, а также определять объем и порядок финансирования работ по обеспечению выбранного уровня информационной безопасности.

4 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

Автоматизация процессов позволила решить множество проблем, но в свою очередь привнесло большое количество осложнений, связанных с профессиональными заболеваниями. В связи с этим была сформирована и развита дисциплина о безопасности труда и жизнедеятельности человека.

Безопасность жизнедеятельности (БЖД) – совокупность мероприятий, направленных на обеспечение безопасности человека в среде обитания, сохранение его здоровья, разработку методов и средств защиты, посредством уменьшения вредоносных воздействий до допустимых значений, выработку мер по ограничению ущерба в ликвидации последствий чрезвычайных ситуаций мирного и военного времени.

Охрана здоровья трудящихся, обеспечение безопасности условий труда, ликвидация профессиональных заболеваний и производственного травматизма составляет одну из главных забот человеческого общества. Формирование и обеспечение условий, не наносящих вред здоровью человека – это главная задача предприятия.

В ООО «ВНК» имеется три отдела. Общая численность сотрудников данных отделов составляет 6 человек и 6 ПЭВМ, соответственно, на каждого сотрудника организации.

Основным документом, на основе которого будет проведен анализ аспектов БЖД, является СанПиН 2.2.2/2.4.1340-03.

Внедрение вычислительной техники на производстве даёт положительный социально-экономический эффект, который выражается в росте производительности, снижении доли рутинного, монотонного труда, повышения скорости расчетов, скорости обмена информацией. Отрицательное воздействие на человека вычислительной техники менее выражено, сглажено многими положительными моментами.

4.1 Безопасность

Цели БЖД в организации «ВНК»:

– выявление и исследование факторов окружающей среды, негативно

оказывающих большое влияние на состояние здоровья человека;

– ослабление воздействия данных факторов до безопасных пределов или исключение их, в случае если это допустимо;

– обеспечение благоприятных условий для трудовой деятельности работников предприятия.

Рабочее место – это зона нахождения работника и средств приложения его труда, которая определяется на основе технических и эргономических нормативов и оснащается техническими и прочими средствами, необходимыми для исполнения работником поставленной перед ним конкретной задачи. Рабочее место представляет собой совокупность факторов окружающей среды, в том числе вредных. Вредный производственный фактор – фактор, воздействие которого на человека в определенных условиях, может привести к заболеваниям, снижениям работоспособности и/или отрицательному влиянию на здоровье потомства.

Основными вредными факторами, оказывающие негативное влияние на работника являются:

- недостаточная освещенность рабочего места;
- шум;
- микроклимат;
- электромагнитное излучение;
- тяжесть и напряженность.

4.1.1 Освещение

Производственное освещение классифицируется на:

- естественное – освещение помещений светом, исходящим от неба (прямым или отраженным), проникающим через световые проемы в наружных ограждающих конструкциях;
- искусственное освещение – создается искусственными источниками света;
- совмещенное – освещение, при котором недостаточное по нормам естественное освещение дополняется искусственным.

Существует искусственное освещение двух систем: общее (равномерное и

локализованное) и комбинированное. Помещения оборудуют системами общего искусственного освещения – когда светильники располагаются в верхней (потолочной) зоне. Если расстояние между светильниками принимается одинаковым, то освещение считают равномерным, если светильники располагают ближе к производственному оборудованию, то освещение называют локализованным. Комбинированным называют такое искусственное освещение, когда к общему добавляется местное.

В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами, следует применять системы комбинированного освещения (к общему освещению дополнительно устанавливаются светильники местного освещения, предназначенные для освещения зоны расположения документов). Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300 – 500 лк. Освещенность поверхности экрана не должна быть более 300 лк.

4.1.2. Шум

Уровень шума на рабочих местах не должен превышать предельно допустимых значений, установленных для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормами.

На рабочем месте оператора источниками шума являются технические средства (компьютер, принтер, вентиляционное оборудование), а также внешний шум. Уровни акустических шумов на рабочих местах операторов при работе аппаратуры удовлетворяет требованиям СанПиН 2.2.2/2.4.1340-03.

4.1.3 Организация рабочего места

В помещении четыре рабочих места. Расстояние между боковыми поверхностями мониторов 2 м. Рабочие столы отвечают требованиям эргономики и позволяют удобно разместить на рабочей поверхности необходимое оборудование и скрыть провода под столешницей.

Все рабочие места должны быть укомплектованы эргономическим креслом и компьютерным столом, обеспечивающим встроенное размещение

системного блока и периферийных устройств, скрытую подводку коммуникационных и силовых кабелей, иметь места крепления электророзеток, телефонных и сетевых розеток, подвижную панель устройства ввода (клавиатуры и манипулятора «мышь»), а также локальный осветительный прибор.

Подготовленные рабочие места операторов для размещения на них технических средств должны иметь площадь не менее 1,5 $м^2$, высоту рабочей поверхности стола 655 мм, высоту сидения кресла 420 мм (желательно регулируемого), расстояние от сидения до нижнего края рабочей поверхности 150 мм, размеры пространства для ног 650х500х600 мм.

Экран монитора должен размещаться на столе или на подставке так, чтобы расстояние наблюдения информации на его экране не превышало 700 мм, оптимальное расстояние от 450 до 500 мм.

Клавиатуру, манипулятор «мышь» следует располагать в оптимальной зоне – части пространства рабочего места, ограниченного дугами, описываемыми предплечьями при движении в локтевых суставах с опорой в точке локтя и с относительно неподвижным плечом. Эта зона составляет от 300 до 400 мм от точки опоры локтя оператора не более.

В офисе рабочие места сотрудников, работающих с программным продуктом, располагают так, чтобы оконные проемы находились сбоку.

Для исключения засветки экранов мониторов прямыми световыми потоками светильники общего освещения располагают сбоку от рабочего места, параллельно линии зрения оператора и стене с окнами. Также размещение светильников позволяет производить их последовательное включение в зависимости от величины естественной освещенности и исключает раздражение глаз чередующимися полосами света и тени, возникающее при поперечном расположении светильников.

4.2 Требования по охране труда при работе на компьютере

Основные требования к персоналу, эксплуатирующему средства вычислительной техники и периферийное оборудование:

– к самостоятельной эксплуатации электроаппаратуры допускается

только специально обученный персонал не моложе 18 лет, пригодный по состоянию здоровья и квалификации к выполнению указанных работ;

– перед допуском к работе персонал должен пройти вводный и первичный инструктаж по технике безопасности с показом безопасных и рациональных примеров работы. Затем не реже одного раза в 6 месяцев проводится повторный инструктаж. Внеплановый инструктаж проводится при изменении правил по охране труда, либо при обнаружении нарушений персоналом инструкции по технике безопасности, изменении характера работы персонала;

– в помещениях, в которых постоянно эксплуатируется электрооборудование, должны быть вывешены в доступном для персонала месте, инструкции по технике безопасности, в которых также должны быть определены действия персонала в случае возникновения аварий, пожаров, электротравм.

4.3 Экологичность

Для работы системы используются ПЭВМ, которые состоят из компонентов, содержащих в себе токсичные вещества и представляющие угрозу для сотрудников, а также для окружающей среды. Токсичные вещества в составе ПЭВМ представляют собой: ртуть, кадмий, мышьяк, свинец, цинк, никель, и др. ПЭВМ должны соответствовать СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к ПЭВМ и организации работы», а именно концентрация вредных веществ, выделяемых ПЭВМ в воздух помещений, не должны превышать допустимых концентраций.

В случае устаревания или выхода из строя ПЭВМ необходимо произвести его списание и процедуру утилизации техники. Для проведения утилизации задействуются сторонние организации. Вся ненужная техника, подвергающаяся процессу утилизации, проходит специальную процедуру:

- непосредственный процесс переработки, включающий в себя удаление вредных компонентов вручную, сортировка и измельчение пластика, измельчение остальных составляющих компьютера;

- аффинаж, представляющий собой металлургический процесс изъятия

высокочистых благородных металлов при отделении от них загрязняющих примесей;

- уничтожение компонентов, не допускающих повторного использования.

Согласно требованиям СанПиН 2.1.7.1322-03 сбор и временное хранение ртутьсодержащих отходов должны осуществляться следующим образом:

- специализированном контейнере с чехлом, расположенном в отдельном помещении с ограниченным доступом персонала. Помещение должно быть сухим и светлым, иметь естественную и принудительную вентиляцию. Допускается хранение отработанных ртутьсодержащих ламп в неповрежденной таре из-под новых ламп или в другой таре, обеспечивающей их сохранность при хранении, погрузочно-разгрузочных работах и транспортировании;

- место временного хранения должно быть промаркировано и оборудовано средствами локализации и удаления загрязнения ртутью при разрушении ламп или других приборов (демеркуризационным набором);

- хранение поврежденных ртутьсодержащих ламп должно осуществляться в специальной таре, не допускается совместное их хранение с неповрежденными лампами.

За использование, функционирование и утилизацию приборов освещения несет ответственность организация, предоставляющее помещение для проведения соревнований.

Также деятельность компании связана с документами, поэтому необходимо утилизировать бумажные документы при помощи шредера.

4.4 Чрезвычайные ситуации

4.4.1 Пожарная безопасность при работе с ЭВМ

Пожар в помещении

Пожаром называют неконтролируемое горение, причиняющее материальный ущерб, вред жизни и здоровью граждан, интересам общества и государства.

Горение – это химическая реакция соединения горючего вещества с кислородом воздуха. Поэтому, чтобы протекал процесс горения, необходимы следующие условия:

– наличие горючего вещества (кроме горючих веществ, применяемых в производственных процессах, и горючих материалов, используемых в интерьере жилых и общественных зданий);

– наличие окислители (обычно окислителем при горении веществ бывает кислород воздуха; кроме него окислителями могут быть химические соединения, содержащие кислород в составе молекул: селитры, перхлораты, азотная кислота);

– наличие источника воспламенения (открытий огонь свечи, спички, зажигалки, костра или искры).

Отсюда следует, что пожар можно прекратить, если из зоны горения исключить одно из перечисленных условий.

Пожары в офисном помещении представляют особую опасность, так как сопряжены с большими материальными потерями. Как известно, пожар может возникнуть при взаимодействии горючих веществ, окислителя и источников зажигания. В офисных помещениях присутствуют все три основные фактора, необходимые для возникновения пожара.

Горючими компонентами являются: строительные материалы для акустической и эстетической отделки помещений, перегородки, двери, полы, перфокарты и перфоленты, изоляция кабелей и др.

Источниками зажигания могут быть электрические схемы от ЭВМ, приборы, применяемые для технического обслуживания, устройства электропитания, кондиционирования воздуха, где в результате различных нарушений образуются перегретые элементы, электрические искры и дуги, способные вызвать загорания горючих материалов.

4.4.1.1 Требования по обеспечению пожарной безопасности

На рабочем месте запрещается иметь огнеопасные вещества, а также в помещениях запрещается:

– зажигать огонь;

– включать электрооборудование, если в помещении пахнет газом;

– курить;

– сушить что-либо на отопительных приборах;

– закрывать вентиляционные отверстия в электроаппаратуре.

При расстановке технологического и другого оборудования должно быть обеспечено наличие проходов к путям эвакуации и эвакуационным выходам.

Коробки вводов электродвигателей и аппаратов управления должны быть уплотнены и закрыты крышкой. Рубильники должны быть установлены так, чтобы они не смогли замкнуть цепь самопроизвольно под действием силы тяжести.

Для дополнительного освещения следует пользоваться переносными светильниками напряжением не более 50 В.

Использованные материалы должны собираться в контейнеры из негорючего материала с закрывающейся крышкой и удаляться по окончании рабочей смены.

По окончании рабочего дня (смены) все электрооборудование и инструмент должны быть отключены от сети.

Ответственность за пожарную безопасность рабочих мест возлагается на должностных лиц в соответствии с приказом «О закреплении рабочих мест за ответственными должностными лицами и их единой нумерации».

При возникновении пожароопасной ситуации или пожара персонал должен немедленно принять необходимые меры для его ликвидации, одновременно оповестить о пожаре администрацию.

Помещения с электрооборудованием должны быть оснащены огнетушителями типа ОУ-2 или ОУБ-3.

4.5 Комплексы физических упражнений для сохранения и укрепления индивидуального здоровья и обеспечения полноценной профессиональной деятельности

Для предупреждения преждевременной утомляемости пользователей ПЭВМ рекомендуется организовывать рабочую смену путем чередования работ с использованием ПЭВМ и без него. В качестве рекомендации предлагается:

– проведение упражнений для глаз через каждые 20 – 25 мин. работы за ПЭВМ;

– проведение упражнений физкультминутки в течение 1 - 2 мин. для снятия локального утомления, которые выполняются индивидуально при появлении начальных признаков усталости [16].

4.5.1 Упражнения для глаз

Упражнения для глаз необходимо выполнять сидя или стоя, отвернувшись от экрана монитора при ритмичном дыхании, с максимальной амплитудой движения глаз. Комплекс упражнений для глаз при работе с компьютером помогает уменьшить нагрузку на глаза и укрепляет глазные мышцы. Каждое упражнение повторяется 10 – 12 раз. Для гимнастики глаз рекомендуется выполнить следующие упражнения:

– закрыть рукой один глаз, затем посмотреть вдаль прямо перед собой 2-3 секунды;

– поставить карандаш на расстояние 15-20 см от глаз, смотреть на его кончик 3-5 секунд; затем перевести взгляд вдаль;

– перемещать карандаш от расстояния вытянутой руки к кончику носа и обратно, следя за его движением;

– открытыми глазами медленно, в такт дыханию, плавно рисовать глазами «восьмерку» в пространстве: по горизонтали, по вертикали, по диагонали;

– поставить карандаш на расстоянии 20-30 см от глаз, смотреть двумя глазами на конец карандаша 3-5 секунд, закрыть один глаз на 3-5 секунд, затем снова смотреть двумя глазами, закрыть другой глаз;

– смотреть 5-6 секунд на карандаш, расположив его на уровне глаз на расстоянии вытянутой руки, медленно отводить руку вправо, следить взглядом за карандашом, не поворачивая головы, повторить влево;

– сделать движения глазами в соответствии с рисунком 51:

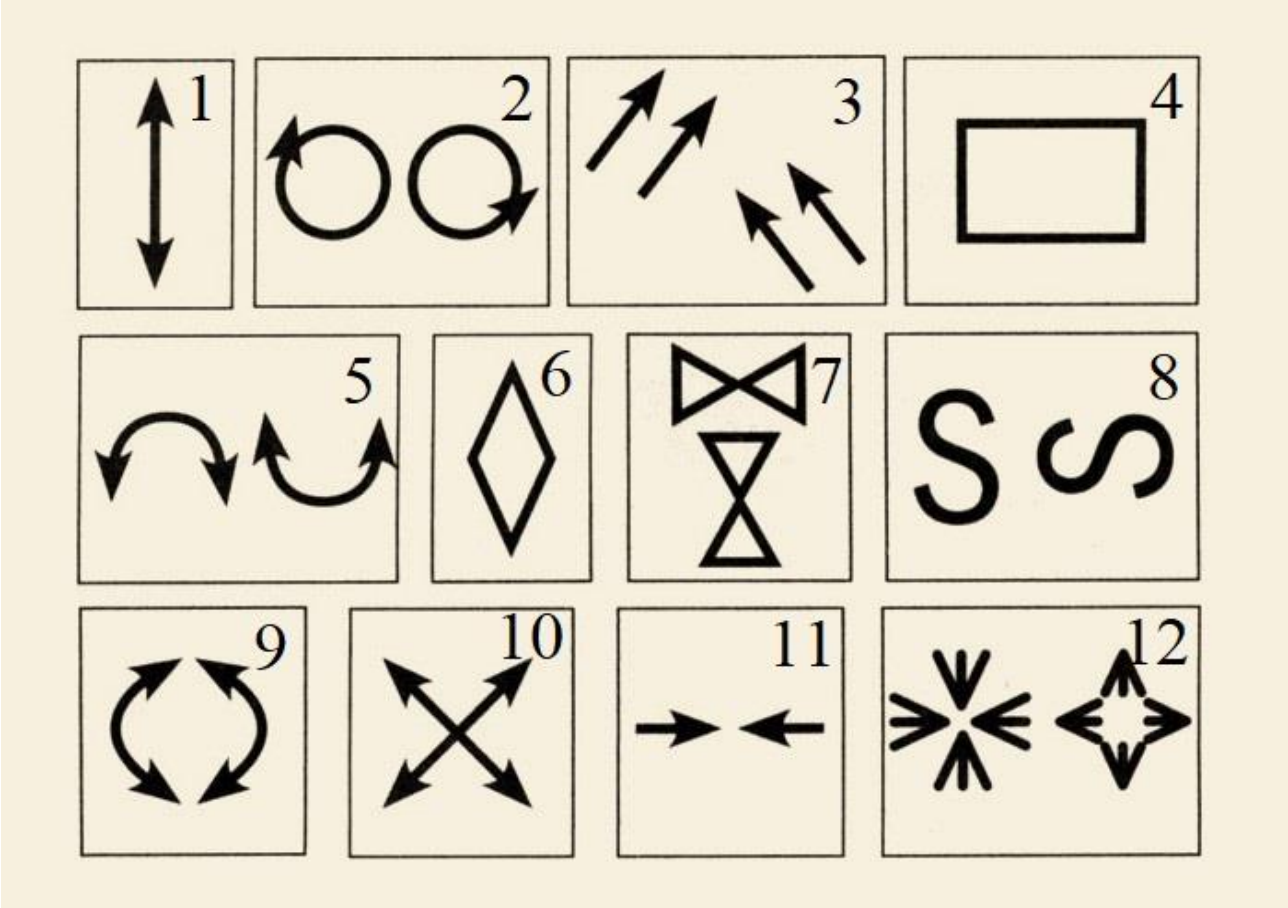

Рисунок 17 – Комплекс упражнений для глаз (1 – вверх-вниз, 2 – круг по часовой стрелке и обратно, 3 – диагонали, 4 – квадрат, 5 – выпуклая и вогнутая дуга, 6 – ромб, 7 – бантики, 8 – буква S в горизонтальном и в вертикальном положении, 9 – вертикальные дуги, по часовой и против часовой стрелки, 10 – из одного угла в другой по диагоналям квадрата, 11 – свести зрачки к переносице, приблизив палец к носу, 12 – часто-часто поморгать веками)

ЗАКЛЮЧЕНИЕ

Объектом данной работы являлся Общество с ограниченной ответственностью «Восточная нефтяная компания».

Предметом работы являлась локальная вычислительная сеть данного предприятия.

Проведён анализ предметной области, а также организационной структуры предприятия. Организационная структура предприятия является линейной, так как во главе каждого производственного или управленческого подразделения находится руководитель, наделенный всеми полномочиями и осуществляющий единоличное руководство подчиненными ему работниками и сосредоточивающий в своих руках все функции управления.

Проведен анализ документооборота предприятия. Показано, что в целом документооборот (внешний и внутренний) сбалансирован, перегруженные документацией сотрудники отсутствуют. Проведен анализ бизнес- процессов предприятия. Показано, что бизнес-процессы полностью отвечают целям и миссии предприятия, закреплёнными в уставе ООО «ВНК».

Анализ существующей ЛВС показал многочисленные недостатки существующей сети, в результате чего было принято решение о модернизации существующей локальной вычислительной сети.

Модернизация коснулась не только схемы сети (вместо Wi-Fi роутера был установлен обычный сетевой роутер, что позволило повысить скорость передачи данных по сети и исключить перехват данных), но также аппаратного комплекса (установлен выделенный сервер, вместо аналоговых видеокамер и видеорегистратора предложены к установке IP-камеры и IP-регистратор), а также программных средств (сервер 1С: Предприятия, установленный на серверную ОС Windows Server 2012).

Таким образом, цель и задачи бакалаврской работы полностью достигнуты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Таненбаум, Э. Компьютерные сети: моногр. / Э. Таненбаум, Д. Уэзеролл. – СПб: Изд-во «Питер», 2012. – 960 с.

2 Олифер, В. Компьютерные сети. Принципы, технологии, протоколы. Учебник: моногр. / В. Олифер, Н. Олифер. – СПб: изд-во «Питер» 2016. – 992 с.

3 Галатенко, В.А. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности / В.А. Галатенко, Г.Ю. Громов. – СПб: БХВ-Петербург, 2008. – 450 с.

4 ГОСТ Р 53246-2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования»; введ. 01–01–2010. – Москва: Федеральное агентство по техническому регулированию и метрологии; М.: Стандартинформ, 2009. – 71 с.

5 ГОСТ Р ИСО/МЭК 15408-2002 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий» – введ. 2004–01–01. – М. : Изд-во стандартов, 2002. – 28 с.

6 Блинов, А.М. Информационная безопасность: Учебное пособие. Часть 1 / А.М. Блинов. – СПб.: Изд-во СПбГУЭФ, 2010. – 99с.

7 Браун, С. Виртуальные частные сети VPN / С. Браун. – М : ООО «Инкобук», 2001. – 221 с.

8 Галатенко, В.А. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности / В.А. Галатенко, Г.Ю. Громов. – СПб: БХВ-Петербург, 2008. – 450 с.

9 Герасименко, А.А. Основы защиты информации / А.А. Герасименко, А.А. Малюк. – М : ООО «Инкобук», 2008. – 537 с.

10 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий – введ. 2006–07–01. – М. : Изд-во стандартов, 2006. – 23 с.

11 Платонов, В.В. – Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие для студ.

высш. учебн. заведений / В. В. Платонов. – М.: Издательский центр «Академия», 2006. – 240 с.

12 Олифер, В.Г. Новые технологии и оборудование IP-сетей / В.Г.Олифер, Н.А.Олифер. – СПб.: Питер, 2000. – 372 с

13 Винсенс, Т. Firebird. Библиотека профессионала / Т. Винсенс. — М.: Символ-плюс, 2010. – 267 с.

14 Кулаков, Ю.А. Компьютерные сети. Выбор, установка, использование и администрирование. / Ю.А. Кулаков, С.В. Омелянский – К.: Юниор, 2007. – 544 с.

ПРИЛОЖЕНИЕ А

Техническое задание

1 ОБЩИЕ ДАННЫЕ

1.1 Основание для выполнения работ

Приказ руководства ООО «ВНК» о модернизации ЛВС.

1.2 Источник финансирования

Средства компании ООО «ВНК»

1.3 Назначение системы

ЛВС предназначена для объединения компьютерных ресурсов компании (сервер, автоматизированные рабочие места, периферийное оборудование) с целью организации защищенного информационного взаимодействия пользователей информационной системы, организации их доступа к файловому хранилищу и терминальному серверу.

1.4 Рекомендации, в соответствии с которыми выполняется модернизация ЛВС

Проектирование ЛВС необходимо осуществлять с учетом возможности использования современных протоколов связи, возможного развития технологий, а так же при определении количества автоматизированных рабочих мест возможность их увеличения в связи с развитием предприятия или изменения назначения помещения (например, пересадка другого подразделения).

1.5 Нормативные документы, в соответствии с которыми выполняются работы:

Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ;

ГОСТ 21.101-97 СПДС «Основные требования к проектной и рабочей документации»;

ГОСТ Р 53246 2008 «Информационные технологии. Системы кабельные структурированные. Проектирование основных узлов системы. Общие требования»;

ГОСТ Р 53245-2008 «Информационные технологии. Системы кабельные структурированные. Монтаж основных узлов системы. Методы испытания» Международный стандарт ISO/IEC 11801:2002. «Телекоммуникационные кабельные системам в коммерческих зданиях»;

Инструкция СН 512-78 «Инструкция по проектированию зданий и помещений для электронно-вычислительных машин», в редакции 2001г.;

ПУЭ «Правила устройства электроустановок», издание 7 с изменениями и дополнениями;

ГОСТ Р 50571.22-2000. «Электроустановки зданий. Заземление оборудования обработки информации».

1.6 Состав выполняемых работ

- поставка оборудования;
- пусконаладочные работы.

2 ОБЩИЕ ТРЕБОВАНИЯ К ЛВС

2.1 ЛВС должна обеспечить 7 и более сетевое подключение. Географию подключений к сети принять в соответствии с таблицей 1.

Таблица А.1 – Размещения рабочих мест в ООО «ВНК»

Наименование	Количество подключений
Центральный офис	5
АЗС №1	1
АЗС №2	1

2.2 ЛВС должна обеспечивать максимально возможную пропускную способность передачи данных

2.3 ЛВС должна обеспечивать защищенный доступ к сети Интернет, а так же к сетевым ресурсам компании

2.4 Модернизации подлежат

- активное сетевое оборудование;

- серверное оборудование.

3 ТРЕБОВАНИЯ К ПОДСИСТЕМАМ ЛВС

3.1 Требования к ЛВС

- стандарт сети должен соответствовать 1000Base-T (GigabitEthernet)

- PDV и PVV не должны превышать 576 и 49 битовых последовательностей соответственно для офиса

- топологии в офисах должны соответствовать типу звезда

3.2 Требования к активному сетевому оборудованию ЛВС

- активное сетевое оборудование должно поддерживать технологии OpenVPN;

- число портов активного сетевого оборудования должно обеспечить функционирование 100% рабочих мест ЛВС и иметь дополнительный запас по портам не менее 20%;

- в составе поставки сетевого оборудования должны входить все необходимые сервисы производителя для обеспечения гарантии не менее 1 года на ремонт и замену неисправного оборудования, техническую поддержку производителя, обновление программного обеспечения.

4 СОСТАВ И ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ РАБОТ

4.1 Пусконаладочные работы.

- пусконаладка оборудования должна обеспечить коммутацию оборудования и первичную настройку WAN-маршрутизаторов и коммутаторов;

- при пусконаладке необходимо проверить возможность доступа из сети ЛВС в сеть Интернет, в закрытую сеть ООО «ВНК».