НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ «УНИВЕРСИТЕТ СИНЕРГИЯ»

Факультет заочного обучения

ОТЧЕТ О ПРОХОЖДЕНИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ ПО СПЕЦИАЛЬНОСТИ 09.03.03 «ПРИКЛАДНАЯ ИНФОРМАТИКА»

Работу выполнил студент

группы:

ОБП-1701ВЛКк

ФИО студента:

Алилуев Роман Евгеньевич

Направление подготовки:

Прикладная информатика

Владикавказ 2019 г.

Содержание

ГЛАВА 1. ОСНОВНАЯ ЧАСТЬ.

1.1 Характеристика объекта прохождения практики.

Я проходил практику в филиале компании ООО «Высокие – Технологии» в г.Владикавказ, в отделе проектирования и разработки программного обеспечения с 25.11.19 по 09.12.19 (2 недели), данный отдел занимается созданием и размещением программ на различных сайтах, регистрацией доменных имен, настройкой почтовых, web-серверов.

Филиал компании ООО «Высокие – Технологии», находится по адресу: Россия, г.Владикавказ, улица Щорса, 27, офис 23,.

Контакты: адрес и телефоны: info@computerpilot.ru ; +7 (8672) 98-96-07.

Компания ООО «Высокие - Технологии» была создана коллективом единомышленников в 1999 году, в г.Москве. За время своей деятельности она выросла из домашней сети в одного из крупнейших операторов связи г. Москвы. На сегодняшний день компания объединяет более 300 высококлассных специалистов и 25 филиалов в различных городах.

Компания ООО «Высокие - Технологии» предоставляет полный спектр услуг в области связи: доступ к Интернет, городская телефония, защита и учет трафика внутри локальной сети, корпоративная электронная почта, виртуальное объединение офисов, цифровое телевидение и радиовещание, сервис хранения и печати фотографий, создание и размещение web-сайтов, colocation, регистрация доменных имен, настройка почтовых, web-серверов.

Вся деятельность по предоставлению услуг связи по передаче данных и телематических служб осуществляется на основании лицензий. Для оказания клиентам наиболее качественных услуг специалисты компании «Высокие - Технологии» постоянно изучают новинки индустрии и новые тенденции на рынке и работает с различными регионами России. Список дополнительных

возможностей постоянно пополняется. Все услуги сопровождаются службой технической поддержки, которая работает круглосуточно.

1.2 Анализ текущего состояния информационной системы в отделе «Проектирования и разработки программного обеспечения»

В данном отделе используется информационная система «Единый сервер статистики», в котором храниться данные о заявка, клиентах и узлах связи, а также через неё происходит оповещение новых документах и вводимых изменения. система разработана техническим отделом кампании. Смс рассылки об аварийных и профилактических работах так же происходят через информационную систему.

В системе храниться все номера которые клиенты указали для оповещения в случаях неисправности. Технический отдел производит модернизацию информационной системы, и вводит новые модули для увеличения функциональности и отказоустойчивости.

Информационная система разработана с помощью нескольких языков программирования таких как: Php, C++, Sql.

На данный момент персонал отдела технической поддержки включает в себя около 50 сотрудников, из которых 30 работают в головном офисе, остальные в регионах. Первая линия поддержки ИТ централизованная, предназначенная только для обслуживания внутренних клиентов. Она поддерживается командой из 20 сотрудников, при этом одновременно в системе работают только 15 человека. На текущий момент график работы ИТ практически круглосуточный 24x7. Суммарное число конечных пользователей ИТ-услуг составляет более 50 тысяч человек, куда входят сотрудники четырех филиалов и работники дополнительных офисов.

1.3 Инструктаж по технике безопасности и противопожарным мероприятиям.

Организационными мероприятиями, обеспечивающими безопасность работы в электроустановках, являются:

а) оформление работы нарядом-допуском (далее нарядом), распоряжением или перечнем работ, выполняемых в порядке текущей эксплуатации;

б) допуск к работе;

в) надзор во время работы;

г) оформление перерыва в работе, переводов на другое рабочее место, окончания работы.

Наряд, распоряжение, текущая эксплуатация.

Работа в электроустановках производится по наряду, распоряжению, в порядке текущей эксплуатации.

Наряд - это задание на производство работы, оформленное на специальном бланке установленной формы и определяющее содержание, место работы, время ее начала и окончания, условия безопасного проведения, состав бригады и лиц, ответственных за безопасность выполнения работы, и пр.

По наряду могут производиться работы в электроустановках, выполняемые:

а) со снятием напряжения;

б) без снятия напряжения на токоведущих частях и вблизи них.

Распоряжение - это задание на производство работы, определяющее ее содержание, место, время, меры безопасности (если они требуются) и лиц, которым поручено ее выполнение. Распоряжение может быть передано непосредственно или с помощью средств связи с последующей записью в оперативном журнале.

Лица, ответственные за безопасность работ, их права и обязанности.

Ответственными за безопасность работ являются:

а) лицо, выдающее наряд, отдающее распоряжение;

б) допускающий - ответственное лицо из оперативного персонала;

в) ответственный руководитель работ (далее ответственный руководитель);

г) производитель работ;

д) наблюдающий;

е) члены бригады.

Лицо, выдающее наряд, отдающее распоряжение, устанавливает необходимость и объем работы, отвечает за возможность безопасного ее выполнения, достаточность квалификации ответственного руководителя, производителя работ или наблюдающего, а также членов бригады.

Лицо, выдающее наряд, обязано в случаях, предусмотренных настоящими Правилами, определить содержание строки наряда "Отдельные указания".

Право выдачи нарядов и распоряжений предоставляется лицам из электротехнического персонала предприятия, уполномоченным на это распоряжением лица, ответственного за электрохозяйство предприятия (организации).

Указанные лица должны иметь группу по электробезопасности не ниже V в электроустановках напряжением выше 1000 В и не ниже IV в установках напряжением до 1000 В.

Право давать распоряжения на производство ряда работ, перечень которых определяется лицом, ответственным за электрохозяйство предприятия, предоставляется также лицам из оперативного персонала с группой не ниже IV.

1.4 Изучение организационной структуры предприятия, должностных инструкций на рабочих местах, документооборота.

Ведущий специалист подчиняется начальнику сектора по кадровому, правовому, документационному, информационному и ресурсному обеспечению.

В своей работе ведущий специалист должен руководствоваться Уставом организации, Правилами внутреннего трудового распорядка, Правилами охраны труда и техники безопасности, обеспечения производственной санитарии и противопожарной защиты, защиты информации Центра, коллективным договором, трудовым договором и настоящей должностной инструкцией.

Осуществляет информационное взаимодействие на основе заключенных соглашений с учреждениями, организациями и ведомствами по вопросам, входящим в компетенцию организации в соответствии с установленным порядком (в том числе с использованием электронных сетей телекоммуникаций);

Изучает рынок средств вычислительной техники, программных средств и выдает рекомендаций по приобретению и внедрению системного и прикладного программного обеспечения.

В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимает меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

Информирует ответственного за обеспечение защиты персональных данных или начальника сектора о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Обеспечивает строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств

и отправке их в ремонт.

Основной задачей ведущего специалиста - является поддержание в актуальном рабочем состоянии полного объема оперативной, накапливаемой и нормативной информации по предоставлению мер социальной поддержки отдельным категориям граждан Ванинского муниципального района, а также защита информации от несанкционированного доступа.

Ведущий специалист должен знать:

- Конституцию Российской Федерации, действующие законодательство Российской Федерации, нормативные правовые акты Российской Федерации и применительно к исполнению должностных обязанностей;

1.5 Техническое оснащение отдела проектирования и разработки программного обеспечения и структура локальных сетей.

В ООО «Высокие – Технологии», имеется 40 компьютеров, из которых 15 ноутбуков, 24 персональных компьютеров и 1 сервер.

В организации ПК имеют следующие характеристики:

– CPU 2,4GHz;
– оперативная память 4 Gb;
– сетевой адаптер – 100Mb/s Network Connection.

Все компьютеры, расположенные в здании, объединены в локальную сеть и соединены с другим оборудованием, необходимым для работы. Это позволяет обеспечить быстрый обмен данными, удобство работы. Предприятие ООО «Высокие – Технологии», использует технологию WTware.

WTware – это программное обеспечение, которое позволяет с минимальными затратами времени и средств эффективно использовать

компьютер в качестве Windows – терминалов. Терминалом называется устройство ввода и отображения информации.

Прикладные программы (Word, Excel, 1С или любая другая программа для Windows) выполняются на сервере, а для пользователя терминала все выглядит так, как если бы компьютер, равный по мощности серверу, стоял у него на столе. Специфика современных программ такова, что можно подключить десятки терминалов к одному серверу и при этом ни один из пользователей не заметит, что сервер используется кем-то еще. Основная цель использования терминалов – снижение TCO (total cost of ownership, совокупная стоимость владения). Снижение достигается за счет снижения расходов при развертывании решения и затем за счет упрощения администрирования системы, повышения надежности комплекса в целом. Windows – терминалы применимы там, где большое количество пользователей используют компьютеры для решения однотипных офисных или специализированных задач. Это залы операторов, рабочие места в офисах, учебные классы и многое другое.

1.6 Технические характеристики программных и аппаратных средств с использованием литературы и сети Интернет

Программные средства – это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения.

Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Ниже перечислены программные средства защиты информации, имеющиеся на предприятии.

1. Антивирусные программы:

1.1. Средство антивирусной защиты для компьютеров и серверов SystemCenterEndpointProtection

MicrosoftSystemCenter 2012 EndpointProtection обеспечивает универсальную защиту от вредоносных программ конечных устройств: бизнес компьютеров, ноутбуков и серверных операционных систем.

Основные особенности Microsoft System Center 2012 Endpoint Protection:

1) простой в использовании:

– создает единый опыт работы администратора для управления и обеспечения устройств;

– улучшает видимость для выявления и ликвидации последствий уязвимых конечных устройств.

2) интеграция средств защиты:

– развертывание более тысячи конечных устройств, используя совместимость с системой SystemCenterConfigurationManager;

– снижает стоимость владения, используя общую инфраструктуру для управления конечными устройствами и безопасности.

3) защита от угроз:

– обновленный антивирусный движок гарантирует более эффективное обнаружение угроз и обеспечивает надежную защиту от новых версий вредоносных программ;

– новые механизмы поведенческого анализа и мониторинга помогут справиться с малоизученными угрозами;

– встроенные средства управления межсетевым экраном WindowsFirewall позволят специалистам убедиться в правильной настройке этого защитного механизма и его корректном функционировании на всех конечных точках сети;

– механизм DynamicCloudUpdate обеспечит своевременное обновление сигнатур для успешной идентификации подозрительных файлов и

ранее неизвестных вредоносных программ.

1.2. Антивирус Касперского, сертифицированный ФСТЭК; WindowsDefender – антивирусная программа, разработанная компанией Microsoft самостоятельно, присутствует в последних версиях операционных систем Windows;

Программы идентификации и аутентификации пользователей:

- CryptoProCSP версии 3.6.

- Криптопровайдер

КриптоПро CSP предназначен для:

– авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001;

– обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования в соответствии с ГОСТ 28147-89;

– контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;

– управления ключевыми элементами системы в соответствии с регламентом средств защиты.

Реализуемые алгоритмы:

– алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ Р 34.11 94 "Информационная технология. Криптографическая защита информации. Функция хэширования";

– алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи";

– алгоритм зашифрования/расшифрования данных и вычисление

имитовставки реализованы в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая".

Программы разграничения доступа пользователей к ресурсам:

1.2. ActiveDirectory;

1.3. Контроллер доступа С2000-2

Контроллер доступа «С2000-2» предназначен для управления доступом через одну или две точки доступа путем считывания кодов предъявляемых идентификаторов (карт Proximity, ключей TouchMemory и PIN-кодов), проверки прав доступа и замыкания (размыкания) контактов, управляющих запорными устройствами (электромеханическими и электромагнитными замками и защелками, турникетом, шлагбаумом).

Особенности:

- настраиваемый контроль взлома и блокировки двери;
- программируемый временной график доступа;
- встроенные энергонезависимые часы с календарем;
- встроенный звуковой сигнализатор.

Программы шифрования информации:

CryptoPro IPsec

IPsec — это набор протоколов по защите информации в сети, который позволяет подтверждать подлинность участников сетевого обмена, контролировать конфиденциальность и целостность сетевых пакетов.

Данный продукт разрабатывается по техническому заданию, согласованному с ФСБ России.

КриптоПро IPsec применяется для:

- защиты подключений удалённых пользователей или малых офисов (VPN);
- защиты соединений между шлюзами корпоративной

вычислительной сети (Site-to-Site VPN);

– защиты передачи конфиденциальной информации в ЛВС от нарушителей, не являющихся пользователями автоматизированных систем, но имеющим физический доступ к ЛВС и нарушителей, являющихся пользователями ЛВС, но не имеющих необходимых полномочий.

1.4. CryptoProArm

КриптоАРМ – программа, предназначенная для шифрования и расшифрования данных, создания и проверки электронной цифровой подписи (ЭЦП) с использованием сертификатов открытых ключей, для работы с сертификатами и криптопровайдерами. «КриптоАРМ», наряду со стандартными криптопровайдерами (входящими в поставку Windows), использует реализацию криптоалгоритмов в сертифицированных ФСБ РФ криптопровайдерах компании «КРИПТО-ПРО».

Функциональные возможности программы:

– шифрование и расшифрование файлов произвольного формата (преобразования файлов функциями СКЗИ);

– создание и проверка корректности одной или нескольких ЭЦП;

– выполнение операций подписи и шифрования за одно действие;

– управление цифровыми сертификатами и ключами пользователя, списками отозванных и доверенных сертификатов;

– управление криптопровайдерами;

– совместимость с ключевыми носителями Рутокен, eToken;

– отправка подписанных и зашифрованных файлов по e-mail.

1.5. Средство шифрации и аутентификации РУТОКЕН

Электронный идентификатор (токен) Рутокен S — это компактное USB-устройство, предназначенное для безопасной двухфакторной аутентификации пользователей, защищенного хранения ключей шифрования и ключей электронной подписи, а также цифровых сертификатов и иной информации.

Рутокен S обеспечивает двухфакторную аутентификацию в

компьютерных системах. Для успешной аутентификации требуется выполнение двух условий: физическое наличие самого USB-токенаРутокен и знание PIN-кода к нему. Это обеспечивает гораздо более высокий уровень безопасности по сравнению с традиционным доступом по паролю. Основу Рутокен S составляют микроконтроллер, который выполняет криптографическое преобразование данных, и защищенная память, в которой в зашифрованном виде хранятся данные пользователя: пароли, сертификаты, ключи шифрования и т.д.

Назначение:

Аутентификация	– Двухфакторная аутентификация при доступе к операционным системам, почтовым серверам, серверам баз данных, Web-серверам и файл-серверам.
Безопасное хранение ключевой информации	– Использование ключевой информации для выполнения криптографических операций на самом устройстве, без возможности выдачи наружу закрытой ключевой информации. – Сгенерированные на токене ключи не могут быть скопированы. – При утере или краже токена безопасность не нарушается: для доступа к информации требуется PIN-код.
Защита персональных данных	– Защита электронной переписки: шифрование почты, электронная подпись почтовых отправлений. – Защита доступа к компьютеру и в домен локальной сети. – Возможность шифрования данных на дисках.
Корпоративное использование	– Используется в корпоративных системах для хранения служебной информации, персональной информации пользователей, паролей, ключей шифрования, цифровых сертификатов и любой другой конфиденциальной информации. – Может выступать как единое идентификационное устройство для доступа пользователя к разным элементам корпоративной системы и обеспечивать, например, необходимое разграничение доступа, цифровую подпись

	создаваемых документов, аутентификацию при доступе к компьютерам и приложениям системы.
Дополнительные возможности	– Поддержка национального стандарта шифрования ГОСТ 28147-89.
Аутентификация и конфиденциальность	– Двухфакторная аутентификация: предъявление самого идентификатора и уникального PIN-кода. – 3 уровня доступа к токену: Гость, Пользователь, Администратор. – Разграничение доступа к файловым объектам в соответствии с уровнем доступа. – Ограничение числа попыток ввода PIN-кода.

Программы защиты ресурсов от несанкционированного копирования, изменения и использования:

1.6. MicrosoftRMS (RightsManagementServices - технология защиты документов MicrosoftActiveDirectory путем шифрования с применением ограничений доступа и лицензий доступа позволяющая сохранять ограничения даже после загрузки и открытия файла пользователем).

Вспомогательные средства:

– программы уничтожения остаточной информации: деформация носителей, сжигание;

– программы аудита событий: встроенные в рабочие станции локальные программы на базе домена.

1. Криптографические методы и средства защиты информации

Криптографические методы защиты информации — это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например,

зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ.

Методы защиты, применяемые на предприятии:

– запрет на хранение конфиденциальной информации на открытых носителях;

– обеспечение целостности информации при передаче при помощи единого центра обработки данных.

2. Методы и средства инженерно-технической защиты информации

Инженерно-техническая защита информации включает комплекс организационных и технических мер по обеспечению безопасности информации техническими средствами. Она решает следующие задачи:

– предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения;

– защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении;

– предотвращение утечки информации по различным техническим каналам.

Методы и средства инженерно-технической защиты информации, применяемые на предприятии:

1. Защита от проникновения нарушителей: проход строго по пропускам/документам, удостоверяющим личность; контроллер доступа VIZIT в комплекте со считывателем; железная дверь; датчик движения.

2. Защита аппаратных средств и носителей от хищения производится путем опечатывания всех ПК и носителей.

3. Предотвращение возможности удаленного видеонаблюдения/подслушивания за работой персонала и ТС: системы защиты «Гром» и «Шорох».

Система защиты «Гром»

Назначение:

Система защиты «Гром» предназначена для маскировки побочных электромагнитных излучений и наводок (ПЭМИН) средств вычислительной техники.

Особенности:

«Гром» формирует шумовую помеху в широком диапазоне частот и полностью соответствует СМД ФСТЭК по контролю защищенности информации, обрабатываемой СВТ от утечки за счет ПЭМИН.

Система является двухканальной. Первый канал системы формирует магнитную составляющую электромагнитного поля помех в диапазоне частот от 0,01 МГц до 30 МГц. Второй канал формирует электрическую составляющую электромагнитного поля в диапазоне от 0,01 МГц до 2000 МГц.

Система состоит из генератора шумовой помехи «Гром», дисконусной антенны «SI-5002.1» и трёх рамочных антенн.

Система защиты «Шорох»

Назначение**:**

Система «Шорох» предназначена для защиты акустической речевой информации в выделенных помещениях (до второй категории включительно) от утечки по акустическому и вибрационному каналам.

Минимизация ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий на предприятии происходит при помощи следующих средств и выполнения нижеприведенных действий: конфиденциальная информация находится в сейфах; источники бесперебойного питания АРС; также присутствуют ТС охраны;

Доступ сотрудников в защищенное помещение (9 человек) осуществляется только в присутствии ответственных за эксплуатацию УЦ.

1.7 Изучение стандартов присоединения периферийных устройств ПК и их особенностей

Большинство периферийных устройств подключаются через промежуточные периферийные интерфейсы, находящиеся на нижних уровнях иерархии подключений (на верхнем уровне -- системная шина). Периферийные интерфейсы -- самые разнообразные из всех аппаратных интерфейсов. К периферии, подключаемой через промежуточные интерфейсы, относятся большинство устройств хранения (дисковые, ленточные), устройств ввода-вывода (дисплеи, клавиатуры, мыши, принтеры, плоттеры), ряд коммуникационных устройств (внешние модемы). По назначению периферийные интерфейсы можно разделить на специализированные и универсальные, выделенные и разделяемые:

Специализированные интерфейсы ориентированы на подключение устройств определенного узкого класса, и в них используются сугубо специфические протоколы передачи информации. Примеры - популярнейший интерфейс мониторов VGA, интерфейс накопителя на гибких дисках, традиционные интерфейсы клавиатуры и мыши, IDE/ATA и ряд других.

Универсальные интерфейсы имеют более широкое назначение, их протоколы обеспечивают доставку данных, не привязываясь к специфике передаваемой информации. Примеры -- коммуникационные порты (COM), интерфейс SCSI, шины USB и FireWire.

Выделенные интерфейсы позволяют подключить к одному порту (точке подключения) адаптера (контроллера) лишь одно устройство; число подключаемых устройств ограничено числом портов. Примеры -- COM-порт, интерфейс VGA-монитора, порт AGP, интерфейс Serial SCSI.

Разделяемые интерфейсы позволяют подключить к одному порту адаптера множество устройств. Варианты физического подключения разнообразны: шина (жесткая, как ISA или PCI; кабельная шина SCSI и IDE/ATA), цепочка (daisy chain) устройств (SCSI, IEEE 1284.3), логическая шина на хабах (USB) или встроенных повторителях (IEEE 1394 FireWire).

Для компьютеров и связанных с ними устройств наиболее распространенной является задача передачи дискретных данных, и, как правило, в значительных объемах (не один бит). Самый распространенный способ представления данных сигналами - двоичный: например, условно высокому (выше порога) уровню напряжения соответствует логическая единица, низкому - логический ноль (возможно и обратное представление). Один двоичный сигнал за один квант времени передает один бит информации. Как говорилось ранее, процессор с периферийными устройствами обменивается байтами (8 бит), словами (в мире x86 - 16 бит), двойными словами (32 бита) данных. Для того чтобы передавать группу битов, существует два подхода к организации интерфейса:

1) Параллельный интерфейс - для каждого бита передаваемой группы имеется своя сигнальная линия (обычно с двоичным представлением), и все биты группы передаются одновременно за один квант времени, то есть продвигаются по интерфейсным линиям параллельно. Примеры: параллельный порт подключения принтера (LPT-порт, 8 бит), интерфейс ATA/ATAPI (16 бит), SCSI (8 или 16 бит), шина PCI (32 или 64 бита).

2) Последовательный интерфейс - используется лишь одна сигнальная линия, и биты группы передаются друг за другом по очереди; на каждый из них отводится свой квант времени (битовый интервал). Примеры: последовательный коммуникационный порт (COM-порт), последовательные шины USB и FireWire, интерфейсы локальных и глобальных сетей.

USB (Universal Serial Bus) - универсальная последовательная шина, предназначенная для подключения периферийных устройств. Шина USB представляет собой последовательный интерфейс передачи данных для среднескоростных и низкоскоростных периферийных устройств.

Является промышленным стандартом расширения архитектуры PC, ориентированным на интеграцию с телефонией и устройствами бытовой электроники.

С точки зрения пользователя привлекательны такие черты USB:

- Простота кабельной системы подключений.

- Изоляция подробностей электрических подключений от пользователя.

- Самоидентифицирующаяся периферия, автоматическая связь устройств с драйверами и конфигурирование.

- Возможность динамического подключения и реконфигурирования периферии.

USB обеспечивает обмен данными между хост-компьютером (сервером, установленном в узлах сети, решающий вопросы коммуникации и доступа к сетевым ресурсам) и множеством одновременно доступных периферийных устройств. Устройство USB должно иметь интерфейс USB, обеспечивающий поддержку протокола USB, выполнение стандартных операций (конфигурирование и сброс) и стандартное представление информации, описывающей устройство. Многие устройства, подключаемые к USB, имеют в своем составе и "функции" и хабы (или концентратор - многопортовой репитер - устройство, физически расположенное в сети, с двумя или более портами).

Параллельный интерфейс: LPT-порт.

Порт параллельного интерфейса был введен в PC для подключения принтера - LP'T-порт (Line PrinTer - построчный принтер).

Адаптер параллельного интерфейса представляет собой набор регистров, расположенных в пространстве ввода / вывода. Регистры порта адресуются относительно базового адреса порта, стандартными значениями которого являются 386h, 378h и 278h. Порт имеет внешнюю 8-битную шину данных, 5-битную шину сигналов состояния и 4-битную шину управляющих сигналов.

BIOS поддерживает до четырех LPT-портов (LPT1-LPT4) своим сервисом - прерыванием INT 17h, обеспечивающим через них связь с принтерами по интерфейсу Centronics. Этим сервисом BIOS осуществляет вывод символа, инициализацию интерфейса и принтера, а также опрос состояния принтера.

1.8 Инсталляция, отладка программных и технических средств.

Откладка программного обеспечения, инсталляция - процесс установки программного обеспечения на компьютер конечного пользователя.

В отделе, где я проходил практику инсталляция выполняется особой программой, присутствующей в операционной системе, или же входящим в состав самого программного обеспечения средством установки.

Инсталлятор — это компьютерная программа, которая устанавливает файлы, такие как приложения, драйверы, или другое ПО, на компьютер. Она запускается из файла SETUP.EXE или INSTALL.EXE

Каждый программный продукт — это, прежде всего, исполняемый модуль с расширением *.EXE (например, ARJ.EXE) или *.COM (например, WIN.COM), и этот модуль может работать либо автономно (например, ARJ.EXE), либо в сопровождении множества служебных файлов и других программ (например, WIN.COM).

1.9 Предложения по оптимизации затрат организации на ИТ инфраструктуру.

Составим некоторые предложения, по оптимизации на затраты по организации ИТ инфраструктуры:

В первую очередь, необходимо оптимизировать ИТ-инфраструктуру за счет гибкого масштабирования вычислительных ресурсов по мере увеличения потребности в них. Этот подход особенно актуален на фоне роста потребности заказчиков в вычислительных ресурсах из-за постоянно увеличивающихся объемов данных.

Во вторых, нужно создать определенные условия, которыми являются:

- более эффективное управление данными, ориентированное на совместное использование разных форм информации внутри предприятия и за его пределами, включая глобальный доступ к корпоративным данным;
- интегрированная и консолидированная инфраструктура, предназначенная для оптимизации использования ресурсов ИТ и простого перехода на новые технологии при поддержании уровня сервиса и операций;
- глобальная координация управления ИТ за счет перестроенных усовершенствованных систем и сервисов, повышающая общую эффективность и стабильность предоставления сервисов;
- фундаментальное сокращение затрат на ИТ по всей компании, включая критический анализ соотношения затрат на ИТ и отдачи от них, а также всего бюджета на закупки и эксплуатацию ИТ;

- упрощение технической инфраструктуры или набора поставщиков за счет сокращения или стандартизации фирменных интерфейсов и связанных с ними архитектур;
- стабильное предоставление сервисов за счет повышения общей производительности системы, включая конфигурации серверов и площадки, производительность сети, системное управление, планирование ресурсов, производительность и проектирование, а также навыки и организационные структуры.

2.Краткий отчет по практике

Практика проходила в соответствии с индивидуальным планом практики, мною были освоены компетенции: ОК-3, ОК-5, ОПК-1, ОПК-2, ОПК-4, ПК-21, ПК-24. В ходе прохождения учебной практики в отделе Проектирования и разработки программного обеспечения в компании ООО «Высокие – Технологии» в г.Владикавказ, я усвоил основные правила оформления документации в отделе, правила взаимодействия в коллективе, и допустимые рамки кооперации при выполнении самостоятельных заданий, которые мне рассказал мой наставник, руководитель Гордиенко А.С., а также правила обращения с конфиденциальной информацией.

Ознакомился с выбранным мною отделом, изучил организационную структуру. В ходе ознакомления я узнал, что отдел находится в непосредственном подчинении начальника отдела программ и проектов ООО «Высокие Технологии».

Отдел в своей деятельности руководствуется Конституцией Российской Федерации, законодательством Российской Федерации, Уставом, иными муниципальными правовыми актами города Москвы.

Изучил техническое оснащение подразделения и структуру локальных сетей.

Были изучены стандарты присоединения периферийных устройств ПК и их особенности.

Инсталляция программ в отделе, где я проходил практику инсталляция выполняется особой программой, присутствующей в операционной системе, или же входящим в состав самого программного обеспечения средством установки.

В целом, практика прошла хорошо, если в ходе прохождения практики, у меня возникали вопросы, я задавал их руководителю практики Гордиенко А.С.

Студент: Алилуев Роман Евгеньевич _____

ФИО подпись студента

Список использованной литературы

1Таненбаум Э. С. Компьютерные сети [Текст] / Э. С. Таненбаум — СПб.: Питер, 2018. — 848с.

2Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А. Олифер. — СПб.: Питер, 2016. — 672 с.

3Олифер В.Г. Новые технологии и оборудование IP-сетей. / В.Г. Олифер, Н.А. Олифер. — СПб.: БХВ Санкт-Петербург, 2017. — 512 с.

4Хелд Г. Технологии передачи данных. 7-е изд. — СПб.: Питер, 2013. — 720 с.

5Теренин А. А. Создание защищенного канала в сети. Материалы семинара «Информационная безопасность», Таганрог, 28–30 июня 2016 г. / А.А. Теренин, Ю.Н. Мельников.

6Электронный замок «Соболь» [Электронный ресурс] / ООО «Код Безопасности». — http://www.securitycode.ru/company/contacts (дата обращения: 11.12.2019).