МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
В Г. ТАГАНРОГЕ РОСТОВСКОЙ ОБЛАСТИ
ПИ (филиал) ДГТУ в г. Таганроге

ЦМК «Прикладная информатика»

Практикум

По выполнению практических работ

по профессиональному МДК:

МДК 07.02 Сертификация ИС

для специальности 09.02.07 Информационные системы и программирование,

квалификации

«Специалист по информационным системам»

Таганрог
2023

Составители: А.А. Погорелов

Практикум по выполнению практических работ по МДК:

МДК 07.02 Сертификация информационных систем. ПИ (филиала) ДГТУ в г.Таганроге, 2023г.

В практикуме кратко изложены теоретические вопросы, необходимые для успешного выполнения практических работ, рабочее задание и контрольные вопросы для самопроверки.

Предназначено для обучающихся по специальности 09.02.07 «Информационные системы и программирование». Квалификации выпускника: «Специалист по информационным системам»

Ответственный за выпуск:

Председатель ЦМК: _____ О.В. Андриян

Общие указания к составлению отчёта

Практические занятия являются одним из элементов учебной деятельности обучающегося, выполнив которую, он должен составить отчёт.

Правильно составить отчёт, значит показать:

- степень усвоения знаний не только по дисциплине МДК.07.02 Сертификация информационных систем, но и по другим дисциплинам, изучаемым обучающимися данной специальности;
- умение проявить самостоятельность;
- творческий подход к выполнению заданий;
- знание нормативных документов, ГОСТов, ЕСКД;
- наиболее лучшую организацию своей работы, чтобы с наименьшими затратами времени и труда найти оптимальное техническое, математическое и другое решение;
- умение пользоваться справочной, информационной, нормативной литературой, ресурсами Интернет.

Отчёт выполняется рукописным способом на обеих сторонах листа формата А4. Оформление отчёта выполняется в соответствии с методическими указаниями по применению стандартов при оформлении учебной документации, текст отчёта иллюстрируется при необходимости графическим материалом в виде рисунков, схем, таблиц. Текст отчёта пишется пастой синего цвета. Отчёт составляется в соответствии с методическими указаниями к работе на основе результатов выполненной работы.

Проверяя отчёт, преподаватель отмечает:

правильность оформления отчёта, т.е. соблюдение требований ГОСТ, ЕСКД и других нормативных документов;

правильность выполнения задания;
достоверность полученных результатов;

ответы на контрольные вопросы и выводы по работе.

Преподаватель отмечает ошибки и выставляет оценку. В случае неудовлетворительной оценки отчёт возвращается. Обучающийся исправляет ошибки и вновь сдаёт отчёт для проверки.

Образовательные результаты, заявленные в ФГОС по
МДК.07.02 Сертификация информационных систем

Обучающийся должен:

уметь:

- проектировать и создавать базы данных;
- выполнять запросы по обработке данных на языке SQL;
- осуществлять основные функции по администрированию баз данных;
- разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных;
- владеть технологиями проведения сертификации программного средства

знать:

- модели данных, основные операции и ограничения;
- технологию установки и настройки сервера баз данных;
- требования к безопасности сервера базы данных;
- государственные стандарты и требования к обслуживанию баз данных

иметь практический опыт:

- В участии в соадминистрировании серверов;
- разработке политики безопасности SQL сервера, базы данных и отдельных объектов базы данных;
- применении законодательства Российской Федерации в области сертификации программных средств информационных технологий

Практическое занятие 1

Тема: «Настройка политики безопасности»

Цель: приобретение необходимого объёма знаний и практических навыков в области политики безопасности.

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Главная цель мер административного уровня - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Термин "политика безопасности" является не совсем точным переводом английского словосочетания "securitypolicy", однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные "правила безопасности". Мы будем иметь в виду не отдельные правила или их наборы, а стратегию организации в области информационной безопасности. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности мы будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений на верхнем уровне детализации может включать в себя следующие элементы:

· решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;

· формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;

· обеспечение базы для соблюдения законов и правил;

· формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Ход работы

Задание.

Изучить теоретический материал

Контрольные вопросы

1. Какие события безопасности должны фиксироваться в журнале аудита?
2. Какие параметры определяют политику аудита?
3. Целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
4. Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
5. Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
6. Нужно ли ограничивать права пользователей по запуску прикладных программ и почему?
7. Какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?
8. Из каких этапов состоит построение политики безопасности для компьютерной системы?
9. К чему может привести ошибочное определение политики безопасности (приведите примеры)?
10. Почему, на Ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 2

Тема: «Создание резервных копий базы данных»
«Восстановление базы данных»

Цель: Получение практических навыков администрирования и сопровождения логической и физической структур базы данных.

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Для небольшой базы данных достаточно создать одно табличное пространство SYSTEM; однако, Oracle рекомендует создавать дополнительные табличные пространства для хранения данных и индексов пользователя, сегментов отмены, временных сегментов отдельно от словаря данных. Это обеспечивает вам большую гибкость в выполнении различных задач администрирования и уменьшает конкуренцию при обращении к объектам словаря и схемы.

Администратор может создавать новые табличные пространства, изменять размер файлов данных, добавлять файлы к табличным пространствам, устанавливать и изменять параметры хранения по

умолчанию сегментов в табличном пространстве, переводить табличное пространство в состояние «только чтение» или «чтение-запись», делать табличное пространство временным или постоянным или удалить его.

Ход работы

Задание.

1. необходимо создать резервные копии базы данных «МММ» с использованием полного резервного копирования, разностного резервного копирования и резервного копирования журнала транзакций.
2. необходимо провести восстановление базы данных «МММ» из сделанных в задании

№1 резервных копий.

Контрольные вопросы

1. Зачем выполнять резервное копирование?
2. Стратегии резервного копирования и восстановления?

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 3

Тема: «Восстановление носителей информации» «Восстановление удаленных файлов»

Цель: Получение теоритических и практических навыков программного восстановления данных.

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

TestDisk — свободная программа для восстановления данных, предназначенная прежде всего для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора, после программных или человеческих ошибок (например, потеря MBR).

- Установка **<sudo apt-get install testdisk>**.
- Запускаем TestDisk **<sudotestdisk>**.
- Появляется окошко приветствия TestDisk, нам предлагается вести лог работы (для выполнения данной работы лог не требуется).
- Выбираем нужный диск и нажимаем **Enter**.
- Предлагается выбрать тип таблицы разделов, обычно TestDisk определяет все правильно, так что нажимаем **Enter**.
- Выбираем **Analise**.
- Выбираем **QuickSearch**.
- Нам выводят таблицу разделов. Выбираем раздел и нажимаем **P**, чтобы вывести список файлов.
- Выбираем файлы для восстановления и нажимаем **C**.

- Выбираем папку, куда будут сохранены файлы и нажимаем **C**.

PhotoRec - это утилита, входящая в состав пакета TestDisk. Предназначена для восстановления испорченных файлов с карт памяти цифровых фотоаппаратов (CompactFlash, SecureDigital, SmartMedia, MemoryStick, Microdrive, MMC), USB flash-дисков, жестких дисков и CD/DVD. Восстанавливает файлы большинства распространенных графических форматов, включая JPEG, аудио-файлы, включая MP3, файлы документов в форматах MicrosoftOffice, PDF и HTML, а также архивы, включая ZIP. Может работать с файловыми системами ext2, ext3, ext4 FAT, NTFS и HFS+, причем способна восстановить графические файлы даже в том случае, когда файловая система повреждена или отформатирована.

- Установка **<sudo apt-get install testdisk>**.
- Запускаем PhotoRec **<sudophotorec>**.
- Выбираем нужный диск и нажимаем **Enter**.
- В нижнем меню можно выбрать **FileOpt**, чтобы выбрать типы файлов для восстановления (по умолчанию выбраны все).
- Чтобы начать восстановление нажмите **Enter**, выбрав **Search**.
- У нас выбрана система ext4, поэтому выбираем первый вариант [ext2/ext3].
- Если выбрать пункт **FREE**, то поиск будет произведен в пустом пространстве и в этом случае будут восстановлены только удаленные файлы, а если выбрать **WHOLE**, то поиск будет произведен на всем диске.
- Теперь нужно указать директорию, куда будем сохранять нужные нам файлы. Выбираем нужную папку и нажимаем **C**.
- Выбираем файлы для восстановления и нажимаем **C**.

Extundelete – утилита, позволяющая восстанавливать файлы, которые были удалены с разделов ext3/ext4.

- Установка: **<sudo apt-get install extundelete>**.
- Как только вы поняли, что удалили нужные файлы, необходимо отмонтировать раздел: **<umount /dev/<partition>>**
- Зайдите в каталог, в который будут восстанавливаться удаленные данные. Он должен быть расположен на разделе отличном от того, на котором хранились восстанавливаемые данные: **cd /<путь_к_каталогу_куда_восстанавливать_данные>**
- Запустите **extundelete**, указав раздел, с которого будет происходить восстановление и файл, который необходимо восстановить: **sudoextundelete /dev/<partition> –restore-file /<путь к файлу>/<имя_файла>**
- Можно так же восстанавливать содержимое каталогов: **sudoextundelete /dev/<partition> –restore-directory /<путь_к_директории>**

Foremost - консольная программа, позволяющая искать файлы на дисках или их образах по hex-данным, характерным заголовкам и

окончаниям. Программа проверяет файлы на предмет совпадения заранее определённых hex-кодов (сигнатур), соответствующих наиболее распространённым форматам файлов. После чего экстрагирует их из диска/образа и складывает в каталог, вместе с подробным отчётом о том, чего, сколько и откуда было восстановлено. Типы файлов, которые foremost может сразу восстановить: jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, cpp. Есть возможность добавлять свои форматы (в конфигурационном файле /etc/foremost.conf), о которых программа не знает.

- Установка: **<sudo apt-get install foremost>**
- Примериспользованиядлявосстановленияизображенийсдиска **/dev/sdb** вкаталог **~/out_dir**
  : **<sudo foremost -t jpg,gif,png,bmp -i /dev/sdb -o ~/out_dir>**

Ход работы

Задание.

Добавьте в виртуальную машину виртуальный жесткий диск. Запустите виртуальную машину с Linux.

Запустите fdisk (gdisk или parted) и создайте таблицу разделов MBR с разделами. Отформатируйте созданные разделы в файловую систему ext4.

Установите TestDisk.

Удалите MBR (или таблицу разделов) с помощью команды DD. Восстановите MBR (или таблицу разделов) с помощью TestDisk. Смонтируйте восстановленные разделы и создайте там произвольные файлы. Удалите созданные файлы.

С помощью TestDisk восстановите данные.

Создайте произвольный каталог и запишите туда данные каталога /var/log/ .

Удалите данные с созданного каталога.

С помощью PhotoRec восстановите данные.

Создайте произвольный каталог и запишите туда данные каталога /etc/ .

С помощью Extundelete или Foremost восстановите данные.

Контрольные вопросы

1. С помощью какой из программ, используемых в этой лабораторной работе, можно восстановить таблицу разделов?
2. Какие файловые системы поддерживает PhotoRec?
3. Какие форматы поддерживает PhotoRec?
4. Как Foremost восстанавливает файлы?
5. Можно ли восстановить данные с файловой системы NTFS, используя

extundelete?

6. Все ли данные скопированные с каталога /var/log/ восстановились?
7. Все ли данные скопированные с каталога /etc/ восстановились?

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 4

Тема: «Мониторинг активности портов»

Цель: Получение практических навыков мониториинга активности портов

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

На этапе ***мониторинга*** выполняется процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п.

Далее выполняется этап ***анализа***, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Ход работы

Задание.

1. Опишите процедуру активности портов.

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 5

Тема: «Блокирование портов»

Цель: Получение практических навыков мониториинга активности портов

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Понятие порта в компьютере многозначно.

Самое общее определение: порт - это соединение (физическое или логическое), через которое принимаются и отправляются данные. Обмен данными между любыми устройствами возможен только при наличии

утвержденного стандарта на интерфейс.

В состав аппаратного обеспечения порта входит специализированный разъём, предназначенный для подключения оборудования определённого типа. Часто этот специализированный разъем и называют портом, например USB-порт, но есть разъемы, которые портами называть не принято, например, RJ11. Как правило, каждый порт имеет обозначение, которое размещается рядом с разъемом.

Основные порты, используемые в компьютерах, ноутбуках:

- USB-порт;
- IEEE 1394 (FireWire) ;
- Порт eSATA и комбинированный порт USB/eSATA;
- Сетевой порт Ethernet;
- Порт SCSI;
- Последовательный порт RS-232;
- Порты для подключения внешних мониторов VGA, DVI, S-Video, HDMI, DisplayPort;
- Порт для док-станции и порт репликатор;
- Порты для модулей расширения PCMCIA, ExpressCard. USB - UniversalSerialBus -

универсальная последовательная шина.

USB-порты являются своего рода стандартом для подключения внешних устройств, к которому стремятся все производители этих устройств. К портам USB подключаются: мыши, клавиатуры, принтеры, сканеры, модемы, кардридеры, флэш-накопители, фотоаппараты, сотовые телефоны, плееры, жёсткие диски, оптические дисководы и др. IEEE 1394 - высокоскоростной последовательный порт для цифровых видеоустройств.

Компания Apple продвигает стандарт IEEE 1394 под маркой FireWire, компания Sony – под маркой i.LINK. IEEE 1394 применяется для подключения видеокамер, цифровых фотоаппаратов и других мультимедийных устройств, а также принтеров, сканеров, внешних жестких дисков. Основные преимущества по сравнению с USB 2.0 - более высокая скорость передачи, большая стабильность, большая длина кабеля до оконечного устройства.

eSATA - ExternalSerial ATA (AdvancedTechnologyAttachment - присоединение по передовой технологии) – последовательный интерфейс для подключения внешних устройств, поддерживающий режим «горячей замены». Стандарт eSATA предусматривает подключение внешних жестких дисков, оптических дисков, RAID-массивов. Скорость передачи данных гораздо выше, чем у USB 2.0 или IEEE 1394.

Недостатки eSATA:

- максимальная длина кабеля не превышает 2 метров;
- жёсткие диски, подключаемые через eSATA, потребуют дополнительного источника питания - это могут быть как разъёмы USB или 1394, так и розетка.

Порт Ethernet предназначен для подключения ноутбука к

компьютерной сети с помощью сетевого кабеля через разъем RJ45 (RJ-45). Технология Ethernet описывается стандартами IEEE группы 802.3. Существует несколько стандартов технологии Ethernet. Стандарты различаются скоростью передачи данных и передающей средой. В ноутбуках обычно устанавливают порт Ethernet 10/100/1000, который поддерживает стандарты 10BASE-T, 100BASE-TX и 1000BASE-T для расстояний до 100 м.

Стандарт 10BASE-T позволяет передавать данные со скоростью 10 Мбит/с. Для передачи используется 4 провода кабеля витой пары категории 3 или категории 5. По стандарту 100BASE-TX скорость передачи данных составляет 100 Мбит/с. Стандарт применяется для построения сетей топологии «звезда». Задействована витая пара категории 5, поддерживается дуплексная передача данных. Стандарт 1000BASE-T - гигабитный (Gigabit, Geth) Ethernet позволяет передавать данные со скоростью до 1 Гбит/с. Стандарт предусматривает использование витой пары категорий 5e. RS-232 (англ. RecommendedStandard) - стандарт последовательной асинхронной передачи двоичных данных между двумя устройствами на расстоянии до 15 метров.

Порт RS-232 в последнее время не часто встречается в бизнес-ноутбуках, но может быть полезен в промышленных ноутбуках. Он используется для реализации систем сбора данных в реальном времени, подключения научного оборудования, управления другими устройствами. Для подключения оборудования, работающего по стандарту RS-232, ноутбуки оснащаются 9- штырьковым разъёмом DB-9 (D-sub).

VGA (англ. VideoGraphicsArray) - аналоговый интерфейс, предназначенный для подключения внешнего дисплея или проектора через 15-контактный разъём DB-15F (D-sub). DVI (англ. DigitalVisualInterface - цифровой видеоинтерфейс) - стандарт на интерфейс и соответствующий разъём, предназначенный для передачи видеоизображения на цифровые устройства отображения, такие как жидкокристаллические мониторы и проекторы. Имеются три версии DVI:

- DVI-A - только аналоговая передача.
- DVI-I - аналоговая и цифровая передача.
- DVID - только цифровая передача. Аналоговый порт S-Video служит для подключения ноутбука к телевизору.

HDMI (англ. High-DefinitionMultimediaInterface - мультимедиа интерфейс высокой чёткости) - интерфейс, позволяющий передавать цифровые видеоданные высокого разрешения и многоканальные цифровые аудиосигналы с защитой от копирования. Разъем HDMI в ноутбуке используется для подключения к жидкокристаллическому телевизору или проектору. Основное различие между HDMI и DVI состоит в том, что разъём HDMI меньше по размеру, а также поддерживает передачу многоканальных цифровых аудиосигналов. DisplayPort – современный интерфейс, предназначенный для подключения к компьютеру аудио и видеоаппаратуры.

DisplayPort имеет пропускную способность вдвое большую, чем DVI, низкое напряжение питания и низкие посторонние наводки. В настоящее время существуют два типа разъёмов: полноразмерный DisplayPort и уменьшенный MiniDisplayPort, разработанный компанией Apple. Размеры разъёма MiniDisplayPort в 10 раз меньше, чем у стандартного разъёма DVI. Технология, реализованная в DisplayPort, позволяет передавать одновременно как графические, так и аудио сигналы. Основное отличие от HDMI — более широкий канал для передачи и большая скорость передачи данных.

Док-станция (dockstation) - это специальная "подставка под ноутбук", предназначенная для подключения к ноутбуку набора различных портов, разъемов и интерфейсов. Док-станция обычно устанавливается на стационарном рабочем месте, к ней можно подключить монитор, мышь, клавиатуру, сетевой кабель, принтер. В ней может находиться встроенный блок питания, дисковод CD/DVD. Ноутбук устанавливается на док-станцию, и через специальный разъем все его интерфейсы соединяются с интерфейсами док-станции, облегчая тем самым подключение ноутбука к внешним устройствам. Док-станция не только существенно расширяет набор интерфейсов, но и делает более удобным переход из офисного режима использования ноутбука в мобильный. При использовании док-станции нет необходимости каждый день, уходя домой, терять время на то, чтобы отсоединить ноутбук от сети и периферии. Всё, что нужно сделать, – извлечь его из док-станции. Сам же разъём для подключения док-станции, как обычно, находится на днище ноутбука и в тех случаях, когда необходимости в нём нет, закрывается небольшой шторкой, предохраняющей от засорения. Док станции выпускаются, как фирмами изготовителями ноутбуков, так и сторонними разработчиками. Как правило, у каждого производителя есть собственный вариант разъёма для подключения докстанции.

Порт-репликатор (Portreplicator), как и док-станция, служит для подключения к ноутбуку различных портов, разъемов и интерфейсов, но возможности его меньше. Порт-репликатор позволяет иметь всегда готовое подключение к большому монитору, клавиатуре, принтеру, внешнему факс-модему, мыши, мощным стерео-колонкам и др. что сохраняет разъемы этих подключений на более длительный срок от возможных поломок и сокращает время подключения. Порт-репликаторы выпускаются, как фирмами производителями ноутбуков (некоторые даже идут в комплекте с ноутбуком) или же сторонними производителями – универсальные порт-репликаторы. Производители обычно имеют собственные варианты разъёмов для подключения порт-репликатора.

PCMCIA (PersonalComputerMemoryCardInternationalAssociation)-спецификация на модули расширения, разработанная ассоциацией PCMCIA. Карты расширения, изготовленные в соответствии с этой спецификацией обычно называются PC-карты (PC Card). Основные типы карт расширения: Type I, Type II и Type III. Все карты расширения имеют

размер 85,6 мм в длину и 54 мм в ширину. Карты Type I имеют 16-разрядный интерфейс и используются для расширения памяти. Толщина карты Type I- 3,3 мм. Разъем имеет один ряд контактов. Карты Type II оснащаются либо 16- , либо 32-разрядным интерфейсом. Толщина карты- 5 мм. Они поддерживают устройства вводавывода, что позволяет использовать их для подключения периферийных устройств. Разъём имеет два ряда контактов. Карты Type III поддерживают 16- или 32-разрядный интерфейс. Они имеют толщину 10,5 мм, что позволяет устанавливать на карту стандартные разъёмы внешних интерфейсов и избавиться таким образом от дополнительных кабелей. Разъем имеет четыре ряда контактов. Разъем PCMCIA представляет собой щель шириной 54 мм, которая закрыта либо откидной шторкой, либо пластиковой заглушкой. Разъем (слот) PCMCIA (вверху) и заглушка, внизу - кардридер Большинство ноутбуков оснащается лишь одним разъемом PCMCIA типа II. А современные ноутбуки уже обходятся и вовсе без этих разъемов.

Порт ExpressCard Стандарт ExpressCard для карт расширения был разработан ассоциацией PCMCIA на смену стандарту PC Card. Новый стандарт был создан на базе новой скоростной последовательной шины PCI Express. Стандарт ExpressCard не только более производительный, чем PC Card, но и более универсальный. Через ExpressCard можно подключаться к шине USB. Карты ExpressCard бывают двух типов, отличающихся по ширине: 34 мм и 54 мм. Соответственно и разъемы бывают двух типов ExpressCard/34 и ExpressCard/54. При этом карты 34 мм можно устанавливать как в разъем ExpressCard/34, так и в разъем ExpressCard/54. Через разъемы ExpressCard подключают ТВ-тюнеры, звуковые карты, карты Wi-Fi, флеш-накопители (они часто подключаются через USB-составляющую интерфейса ExpressCard), модемы для работы в сотовых сетях и др. Разъем RJ11(RJ-11 Registeredjack) – разъем модема ноутбука. Используется для подключения к Интернету через модем по телефонной линии.

Ход работы

Задание.Организовать запрет доступа к USB сменным носителям при помощи групповых политик (GPO).

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 6

Тема: «Проверка наличия и сроков действия сертификатов»

Цель: знакомство с использованием сертификатов в автономном компьютере, работа с централизованной инфраструктурой открытого ключа (PubicKeyInfrastucture – PKI). Получение навыка в управлении сертификатами.

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Цифровой сертификат – электронный документ, выданный и заверенный Удостоверяющим центром.

Цифровой сертификат - это небольшой файл, содержащий в себе следующую информацию:

1. имя и идентификатор владельца сертификата;
2. открытый ключ подписи (шифрования);
3. имя, идентификатор и цифровую подпись Удостоверяющего центра;
4. серийный номер, версию и срок действия сертификата.

Инфраструктура открытых ключей (англ. ***PKI*** - *Public Key Infrastructure*) — набор средств (технических, материальных, людских и т. д.), распределенных служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей.

В основе PKI лежат несколько основных принципов:

1. закрытый ключ известен только его владельцу;
2. удостоверяющий центр создает сертификат открытого ключа,таким образом удостоверяя этот ключ;
3. никто не доверяет друг другу, но все доверяют удостоверяющему центру;
4. удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

Ход работы

Задание.С помощью консоли работы с личными сертификатами пользователя ознакомтесьс возможностями манипулирования уже полученными сертификатами.

Познакомтесь с возможностями получения сертификатов через Web от автономного центра сертификации, а также с методами работы с корпоративным центром выдачи сертификатов.

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и

практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 7

Тема: «Разработка политики безопасности корпоративной сети»

Цель: Получение навыка разработки безопасности корпоративной сети.

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Политика информационной безопасности — набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области защиты информации.

На основе политики информационной безопасности строится управление, защита и распределение критичной информации в системе. Она должна охват ывать все особенности процесса обработки информации, определяя поведение информационных систем в различных ситуациях. Для конкретной информационной системы политика безопасности должна быть индивидуальной. Она зависит от технологии обработки инфор мации, используемых программных и технических средств, структуры организации и т. д.

Политика информационной безопасности компании должна быть утверждена руководством, издана и доведена до сведения всех сотрудников в доступной и понятной форме.

Для того, чтобы политика информационной безопасности была эффективно реализована на практике, необходимо, чтобы она была:

- непротиворечивой – разные документы не должны по разному описывать подходы к одному и тому же процессу обработки информации
- не запрещала необходимые действия – в таком случае неизбежные массовые нарушения приведут к дискредитации политики информационной безопасности среди пользователей
- не налагала невыполнимых обязанностей и требований.

В организации должно быть назначено лицо, ответственное за политику безопасности, отвечающее за её эффективную реализацию и регулярный пересмотр.

Ход работы

Задание.1. Выбрать вариант (вид организации, для которой будет разрабатываться политика ИБ)

2. Скачать образец политики ИБ.

3. На основе образца разработать политику ИБ, учитывая

специфику деятельности выбранной организации.

4. Разработанную политику ИБ вложить в качестве ответа на данное задание. Варианты

1. Образовательная организация
2. Агентство недвижимости
3. Администрация города
4. Городская поликлиника
5. Компания по разработке ПО
6. Интернет-провайдер
7. Отделение налоговой службы
8. Городской архив
9. Центр оказания государственных услуг
10. Страховая компания

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 8

Тема: «Получение сертификата»

Цель: знакомство с процедурой получения сертификата
Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Компьютер – это устройство, которое используется во всех сферах жизнедеятельности человека. Передача и хранение информации, ведение бухгалтерии, диагностика в сфере медицины – далеко не полный перечень функций, выполняемых данным оборудованием. Однако успешное функционирование компьютера зависит от качества программного обеспечения. Системой стандартизации к информационным продуктам предъявляется ряд требований.

Сертификация программного обеспечения – это процедура, направленная на подтверждение соответствия данного компонента нормам и стандартам, действующим на территории России.

Поскольку основной контролирующей системой в нашей стране является Госстандарт, процедура проверки для такой продукции проводится именно в этой структуре. В соответствии с положениями правительственного Постановления № 982 от 1 декабря 2009 года, сертификат на данный продукт не является обязательным. Несмотря на это, многие изготовители и продавцы такой продукции считают необходимым получить документальное подтверждение соответствия в Госстандарте на основе добровольного желания.

Сертификация проводится на основе требований ГОСТ 19781-90.

Добровольная процедура контроля повышает конкурентоспособность товаров, поскольку вызывает доверие со стороны потребителей. Она осуществляется в органах по сертификации, имеющих аккредитацию Госстандарта. С целью получения разрешительного документа производителю или продавцу необходимо подать заявку, предоставить документы и саму программу для исследования. После детального изучения материалов специалисты принимают решение об их соответствии нормативам данной системы.политику безопасности, отвечающее за её эффективную реализацию и регулярный пересмотр.

Ход работы

Задание.Опишите процедуру получения сертификата на программное обеспечение

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 9

Тема: «Жизненный цикл программного средства. Качество программного средства»

Цель: Выбрать модель жизненного цикла программного обеспечения для своего проекта. Определить стадии жизненного цикла программного обеспечения

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Под моделью ЖЦ ПО понимается структура, определяющая последовательность выполнения и взаимосвязи процессов, действий, задач на протяжении ЖЦ. Модель ЖЦ зависит от специфики, масштаба исложности проекта и специфики условий, в которых система создается и функционирует. Международныйстандарт ISO/IEC 12207: 1995 описывает структуру процессов ЖЦ ПО.

Наибольшее распространение получили следующие две модели ЖЦ ПО: каскадная и спиральная.

Ход работы

Задание.

Разработайте проект своего программного обеспечения (для чего предназначено ПО, какими средствами разработано, на кого направлено, какие функции и операции выполняет, егоназвание и т.д.).

Выберите модель жизненного цикла программного обеспечения для своего проекта. Определите процессы для первой стадии (формирование требований к ПО).

Сделайте выводы по проделанной работе.

Контрольные вопросы

1. Что такое модель жизненного цикла программного обеспечения?
2. Типы моделей жизненного цикла ПО.
3. Преимущества каскадного подхода.
4. Особенности спиральной модели.
5. Стадии программного обеспечения.

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.

Практическое занятие 10

Тема: «ГОСТы ЕСПД и их применение»

Цель: Выбрать модель жизненного цикла программного обеспечения для своего проекта. Определить стадии жизненного цикла программного обеспечения

Оснащение: ПК, учебная и справочная литература.

Теоретические сведения

Единая система программной документации (ЕСПД) — комплекс государственных стандартов Российской Федерации, устанавливающих взаимосвязанные правила разработки, оформления и обращения программ и программной документации.

В стандартах ЕСПД устанавливают требования, регламентирующие разработку, сопровождение, изготовление и эксплуатацию программ, что обеспечивает возможность:

унификации программных изделий для взаимного обмена программами и применения ранее разработанных программ в новых разработках;

снижения трудоемкости и повышения эффективности разработки, сопровождения, изготовления и эксплуатации программных изделий;

автоматизации изготовления и хранения программной документации.

Сопровождение программы включает анализ функционирования, развитие и совершенствование программы, а также внесение изменений в неё с целью устранения ошибок.

Поскольку ЕСПД представляет собой набор ГОСТов, в настоящее время её применение на территории РФ носит только рекомендательный характер, то есть ЕСПД применяется на добровольной основе (если иное не предусмотрено договором, контрактом, отдельными законами, решением суда и т. п.)

Ход работы

Задание 1.Прочитайте документ ЕСПД, выделите цель введения данных стандартов.

Выпишите
основные разделы.

Задание 2. Определите области применения ЕСПД, пользователей ЕСПД.

Задание 3. Прочитайте ГОСТ 19.504-79, определите его область применения, цели введения данного стандарта.

.

Список используемой литературы

1. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для СПО М: изд-во Юрайт 2020 г.