Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБЕСПЕЧЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Направление подготовки: 10.04.01 «Информационная безопасность»

Магистерская программа «Безопасность автоматизированных систем»

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2021

Смоленск

Методические материалы составил:
канд. техн. наук, доцент кафедры
«Вычислительная техника»  Я.А. Федулов

«28» _июня_ 2021 г.

Заведующий кафедрой «Вычислительная техника»:


подпись

__д-р техн. наук, профессор_А.С. Федулов__
ФИО

«02» _июля_ 2021 г.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

Лабораторные работы 8 шт. по 4 часа и 1 шт. – 2 часа:

Лабораторная работа 1. Перехват и анализ сетевых пакетов.

Задания

1. Изучить возможности библиотеки WinPcap.
2. Изучить возможности библиотеки SharpPcap.
3. Осуществить перехват и анализ сетевых пакетов на сетевом транспортном и прикладном уровнях модели OSI.
4. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Для каких целей проводится мониторинг трафика сети?
2. Основные возможности анализатора сетевого трафика Wireshark.
3. Как выполнить захват сетевого трафика рабочей станции?
4. Как можно определить принадлежность пакета узлу сети и протоколу?
5. Как получить общую статистику по захвату?
6. Как получить информацию о распределении трафика по протоколам?
7. Какой трафик потенциально опасен?
8. Как получить справку по функции printf языка программирования C?
9. Приведите практические примеры использования средств перенаправления ввода-вывода.
10. Чем отличаются команды вывода содержимого файлов на экран page, less и more?
11. Объедините два текстовых файла в один с помощью команды cat.
12. Как организовать чат между пользователями двух терминалов?
13. Что такое переменная окружения?
14. Как определить полное имя домашнего каталога текущего пользователя?
15. Приведите все способы записи пути к файлу myname.txt (текущий каталог — Dn).
16. Как скопировать файл без использования команды cp?
17. Как создать скрытый каталог?

Лабораторная работа 2. Современные симметричные криптосистемы.

Задания

программная реализация существующих симметричных криптоалгоритмов.

1. Изучить принципы работы симметричных криптосистем.
2. Изучить национальные и ведомственные стандарты управления безопасностью.
3. Изучить реализаций симметричной криптографии в среде .NET Framework.
4. Осуществить программную реализация существующих симметричных криптоалгоритмов.
5. Настроить учетные записи.
6. Оформить отчет по проделанной работе.

Контрольные вопросы

1. На какие операции с файлами оказывают влияние права доступа к файлу, а на какие — права доступа к каталогу, в котором содержится указанный файл?
2. Можно ли отредактировать файлы с правами доступа 204 и 240 и каким образом?
3. Пользователь установил права доступа к файлу только на чтение — 444, но хакеру удалось отредактировать этот файл. Какие ошибки мог совершить пользователь?
4. Как разрешить пользователю удалять из каталога только те файлы, владельцем которых он является?
5. Что такое тёмный каталог?
6. Как определить только с помощью команды ср в какие группы входит пользователь student?
7. Как суперпользователю root запретить всем пользователям самостоятельно изменять пароль?
8. Как запретить вход в систему суперпользователю root?
9. Как получить список всех пользователей системы?
10. В чем разница между командами su и sudo?

Лабораторная работа 3. Современные асимметричные криптосистемы.

Задания

1. Изучить принципы работы асимметричных криптосистем.
2. Рассмотреть реализаций асимметричной криптографии в среде .NET Framework.
3. Провести реализацию существующих асимметричных криптоалгоритмов.
4. Задать управление процессами сигналы процессам, управление стандартными потоками.
5. Рассмотреть текстовые процессоры, потоковые редакторы и регулярные выражения.
6. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Что называется жесткими ссылками?
2. Какие свойства файлов-ссылок?
3. Что представляют символические ссылоки?
4. Какие существуют способы созданияссылок?
5. Что происходит с файлами с нулевым количеством ссылок?
6. Что называется именем файла в системе?
7. Какое содержание панели и меню Midnight Commander
8. Назначение функциональных клавиш Midnight Commander?
9. Как создать структуру каталогов, файлов и ссылок.
10. Перечислите основные настройки Midnight Commander.
11. Какие способы получения справки по использованию команд.
12. Дайте определение процессу.
13. Что нужно сделать для приостановления задания, работающее в фоновом режиме?
14. Какие команды управления процессами в Linux?
15. Что делает команда yes?
16. Задания в фоновом режиме и приостановленные задания, в чем их отличие?
17. Для чего служит системный вызов kill()?

18. Что осуществляет планировщик cron?
19. Какие основные команды для работы с планировщиком заданий в Linux?
20. Что происходит с выводимой отложенным процессом информацией?
21. Для чего нужна команда at? Какой у ней формат?
22. С помощью каких команд осуществляется управление приоритетами процессов в Linux?
23. Каково влияние приоритета на производительность процесса?

Лабораторная работа 4. Хэширование и электронная цифровая подпись.

Задания

1. Изучить работу методы формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП).
2. Рассмотреть реализации хэш-функций и ЭЦП в среде .NET Framework.
3. Провести реализацию существующих хэш-функций и алгоритмов ЭЦП..
4. Внести изменения в структуру и состав пакета.
5. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Для считывания аргументов командной строки используются?
2. Как скомпилировать проект?
3. Какие функции стандартной библиотеки для работы с файловой системой?
4. Как выводить список файлов в два столбца: имя файла, размер файла?
5. Из каких составных элементов состоит пакет?
6. Какие основные пакетныен менеджеры применяются в операционных системах?
7. Какие основные команды нужны для установки и удаления пакетов?

Лабораторная работа 5. Работа с системными журналами в операционной системе.

Задания

1. Разработать методы работы с системными журналами.
2. Составить диаграмму отслеживания событий записи в системные журналы.
3. Реализовать перехват системных событий.
4. Провести анализ записей системных журналов.
5. Разработать автоматизированную систему с использованием объектного подхода.
6. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Дайте определение технологичности программного обеспечения.
2. Что понимают под связностью модуля, типы связности.
3. Что понимают под сцеплением модуля, типы сцепления.
4. Нисходящая и восходящая разработка программного обеспечения. Перечислите достоинства и недостатки данных методов.
5. Постройте диаграмму Насси-Шнейдермана для программы перевода числа из десятичной формы в шестнадцатеричную.
6. Перечислите формы описания структурных алгоритмов, опишите особенности данных форм, их достоинства и недостатки.
7. Постройте flow-форму для программы определения типа треугольника по трем его сторонам.

Лабораторная работа 6. Работа с системными журналами в операционной системе. Файловая система.

Задания

1. Разработать методы отслеживания событий изменения файловой системы (создание, удаление, переименование и изменение выбранных файлов и папок).
2. Реализовать отслеживание событий изменения аппаратной конфигурации компьютера.
3. Провести анализ записей системных журналов.
4. Внести изменения в автоматизированную систему с использованием объектного подхода.
5. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Какие элементы определяются в составе класса?
2. Приведите синтаксис описания класса в общем виде. Проиллюстрируйте его фрагментом программы на языке высокого уровня.
3. Какие модификаторы типа доступа Вам известны?
4. В чем заключаются особенности доступа членов класса с модификатором public, private, protected, internal?
5. Приведите синтаксис создания объекта в общем виде. Проиллюстрируйте его фрагментом программы на языке высокого уровня.
6. Что понимается под термином «конструктор», В чем состоит назначение конструктора, Каждый ли класс имеет конструктор, Какие умолчания для конструкторов приняты? Приведите синтаксис конструктора класса в общем виде.
7. Что понимается под термином «деструктор», В чем состоит назначение деструктора? Приведите синтаксис деструктора класса в общем виде. Проиллюстрируйте его фрагментом программы на языке высокого уровня.
8. Что понимается под термином «наследование»? Какая классификация объектов соответствует наследованию? Что общего имеет дочерний класс с родительским? В чем состоит раз-личие между дочерним и родительским классами? Приведите синтаксис описания наследования классов в общем виде.
9. Приведите классификацию диалогов и общие принципы их работы.
10. Укажите составные элементы графа диалога с пользователем.

Лабораторная работа 7. Удаленный доступ и управление операционной системой.

Задания

1. Изучить удаленный доступ к ресурсам операционной системы с использованием технологии WMI.
2. Рассмотреть возможности утилиты командной строки wmic.
3. Реализовать работу с протоколом удаленного доступа SSH.
4. Построить архитектуры системы и описать особенности ее внедрения.
5. Оформить отчет о проделанной работе.

Контрольные вопросы

1. Что такое CASE-средства?

2. Зачем необходимы CASE-средства?
3. В чем заключается сущность визуального моделирования?
4. Что отображают диаграммы вариантов использования?
5. Что отображают диаграммы последовательности?
6. Что отображают кооперативные диаграммы?
7. Что отображают диаграммы классов?
8. Что отображают диаграммы состояний?
9. Что отображают диаграммы компонент?
10. Что отображают диаграммы размещения?
11. В чем состоит суть модели разработки программного обеспечения "водопад", ее особенности и недостатки?
12. Изложите шаги методики разработки приложений с использованием Rational Rose.

Лабораторная работа 8. Управление политиками безопасности.

Задания

1. Провести исследование методов контроля доступа к ресурсам операционной системы.
2. Осуществить обеспечение безопасности доступа кода (утверждение и отклонение полномочий).
3. Управление политиками безопасности и оценку качества труда при разработке автоматизированных систем.
4. Оценить качество программного обеспечения и разработки системы.
5. Оформить отчет о проделанной работе.

Контрольные вопросы

1. Каковы особенности операционных систем в защищенном исполнении?
2. В чем состоят достоинства и недостатки статистических и динамических способов исследования ПО?
3. Какие существуют способы проведения испытаний ПО, оценки качества и сертификации программных средств?
4. Каков состав методического обеспечения проведения испытаний программ?
5. Охарактеризуйте показатели качества ПО разных уровней.
6. Приведите последовательность операций при выборе номенклатуры показателей качества ПО.
7. Дайте оценку значений показателей качества ПО.
8. Какие основные этапы включают испытания ПО?
9. Приведите последовательность действий при этих испытаниях.
10. Какова технология создания сложных программных комплексов?
11. Охарактеризуйте действия разработчиков при обеспечении технологической безопасности ПО.
12. Приведите структурно-функциональную схему инструментальных средств поддержки создания безопасного программного обеспечения.
13. Каковы этапы контроля безопасности общего и специального ПО на этапе исследования и испытаний ПО?
14. Приведите требования к контрольно-испытательному стенду испытания технологической безопасности ПО.

Лабораторная работа 9. Практическая реализация распределения ключей.

Задания

1. Провести анализ методов безопасного распределение ключей.
2. Реализовать алгоритм Диффи-Хеллмана в клиент-серверной архитектуре приложения для вычислительных сетей.
3. Обеспечить санкционированный доступ, настроить авторизацию пользователей.
4. Применить методы шифрования информации.
5. Оформить отчет по проделанной работе.

Контрольные вопросы

1. Какие средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность известны?
2. Охарактеризуйте обобщенные способы анализа программных средств на предмет наличия (отсутствия) недекларированных возможностей.
3. Приведите основные этапы построения программно-аппаратных комплексов для контроля технологической безопасности программ.
4. Какие существуют средства и комплексы защиты программ от компьютерных вирусов?
6. Какие используются средства защиты программ от несанкционированного копирования?
7. Каковы этапы контроля безопасности общего и специального программного обеспечения на этапе исследования и испытаний?
8. Что является количественной мерой опасности?
9. Что аналитически выражает риск?
10. Какие существуют виды риска?
11. Что выявляют при анализе методом «деревьев отказов»?
12. В чем заключается качественный анализ «дерева отказов»?
13. Для решения каких поставленных задач используют «дерево событий»?
14. В чем состоит отличие «дерева событий» от «дерева отказов»?
15. Какие основные виды стратегий безопасности проектирования программного обеспечения существуют?

Полный комплект методического обеспечения лабораторных работ по дисциплине «Технологии обеспечения информационной безопасности» в формате pdf-файлов расположен на кафедральных ресурсах. Преподаватель, ведущий лабораторные работы, выдает раздаточный материал в начале семестра.