МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Утверждаю:
Зав. кафедрой компьютерных интеллектуальных технологий проектирования

_____ М.И. Чижов
«21» декабря 2021 г.

УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

«Специальные методы информационной безопасности»

Направление подготовки: 09.04.01 Информатика и вычислительная техника

Направленность (профиль): Искусственный интеллект

Квалификация выпускника магистр

Нормативный период обучения 2 года / 2 года и 5 м.

Форма обучения очная / заочная

Год начала подготовки 2022

Составитель:
ДОВГАЛЮК П.М., СТАРШИЙ ПРЕПОДАВАТЕЛЬ
КАФ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ (НГУ)
МАКАРОВ В.А., ДОЦЕНТ
КАФ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ (НГУ)
Ершов Евгений Валентинович, д.т.н., профессор, директор института информационных технологий, зав. кафедрой МПО ЭВМ ЧГУ

г. Воронеж - 2021

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1. Защита информации техническими средствами [Электронный ресурс] : учебное пособие / А.И. Спивак; А.В. Разумовский; Ю.Ф. Каторин; ред. Ю.Ф. Каторин. - Санкт-Петербург : Университет ИТМО, 2012. - 417 с.URL: http://www.iprbookshop.ru/66445.html

2. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. URL: http://biblioclub.ru/index.php?page=book&id=480637

3. Защита информации : лабораторный практикум / В.И. Смирнов. - Йошкар-Ола : ПГТУ, 2017. - 67 с. - ISBN 978-5-8158-1866-8. URL: http://biblioclub.ru/index.php?page=book&id=476512

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Ресурсы информационно-телекоммуникационной сети «Интернет»:
- http://www.edu.ru/
- Образовательный портал ВГТУ

Информационные справочные системы:
- http://window.edu.ru
- https://wiki.cchgeu.ru/

Учебно-методические указания и рекомендации к изучению тем лекционных и практических занятий, самостоятельной работе студентов

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основы информационной безопасности	Концептуальная модель информационной безопасности. Понятие политики безопасности. Основные информационные угрозы	4	4	18	26
2	Причины нарушения безопасности	Исследование причин нарушений безопасности. Анализ опасности. Методики противодействия. Реализация и гарантирование политики безопасности.	4	4	18	26
3	Защищенные сети	Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей. Создание механизмов безопасности в распределенной компьютерной системе.	2	4	18	24
4	Методы криптографии	Анализ существующий подходов. Типы шифрования. Симметричные и несимметричные шифры. Анализ криптостойкости. Цифровая электронная подпись.	2	4	18	24
5	Разработка криптографических систем	Разработка программных продуктов, использующих основные алгоритмы шифрования. Использование типовых библиотек. Алгоритмизация. Протоколы шифрования	2	2	18	22
6	Реализация защищенных информационных систем	Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов.	2	2	18	22

		Использование программных средств собственной разработки для защиты информации				
		Итого	**16**	**20**	**108**	**144**

заочная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Основы информационной безопасности	Концептуальная модель информационной безопасности. Понятие политики безопасности. Основные информационные угрозы	2	2	20	24
2	Причины нарушения безопасности	Исследование причин нарушений безопасности. Анализ опасности. Методики противодействия. Реализация и гарантирование политики безопасности.	2	2	20	24
3	Защищенные сети	Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. Современные средства построения защищенных виртуальных сетей. Создание механизмов безопасности в распределенной компьютерной системе.	-	2	22	24
4	Методы криптографии	Анализ существующий подходов. Типы шифрования. Симметричные и несимметричные шифры. Анализ криптостойкости. Цифровая электронная подпись.	-	2	22	24
5	Разработка криптографических систем	Разработка программных продуктов, использующих основные алгоритмы шифрования. Использование типовых библиотек. Алгоритмизация. Протоколы шифрования	-	-	22	22
6	Реализация защищенных информационных систем	Модели безопасного субъектного взаимодействия в компьютерной системе. Аутентификация пользователей. Сопряжение защитных механизмов. Использование программных средств	-	-	22	22

		собственной разработки для защиты информации				
		Итого	4	8	128	140

Темы лабораторных работ Лабораторная работа № 1.

Передача управления: условные и безусловные переходы.

Составить программу решения задачи:

1. Даны три битовые переменные без знака a, b, c, d. Записать в d наибольшее из значений этих переменных.

2. Пусть a, b, c – числа размером в слово. Вычислить значение функции f при следующих условиях:

f=4*a+b/c-6, если a>=b

f=6-c*(a+b), если b>=c f=3/a-

(7+b)*5, если c>=a

3. Пусть k – байтовая переменная со значением от 1 до 18. Записать в регистр AL количество двухзначных десятичных чисел (от 10 до 99), сумма цифр которых равна k.

Проверить работу программы на 4-5 наборах тестовых данных.

Контрольные вопросы:

1. Сколько операндов имеют команды условного и безусловного переходов?
2. Опишите результат выполнения команды CMP?
3. Что такое дальний переход?
4. Влияют ли команды перехода на значения регистра флагов?
5. Для чего используется оператор SHORT?

Лабораторная работа № 2. Вызовы функций. Аппаратная поддержка стека.

Подпрограмма должна выполняться через вызов пользовательского прерывания (например, INT 60h). Адрес подпрограммы должен быть занесен в таблицу векторов прерываний при помощи функций DOS 25h и 35h. Подпрограмма должна выполнять действия, указанные в конкретном задании, при этом подпрограмме должны передаваться параметры N и j. Подпрограмма также должна возвращать результаты работы в регистрах общего назначения. После вызова подпрограммы программа должна восстановить адрес старого обработчика прерывания при помощи тех же функций DOS.

Параметры N и j могут передаваться в подпрограмму обработки прерывания через регистры общего назначения или через ячейки памяти. Значения параметров N и j не

должны быть тривиальными (например, 1 или 0). Значение параметра N должно быть больше 1.

При вычислении произведений значения параметров N и j следует выбирать так, чтобы не происходило переполнения разрядной сетки для факториальных выражений. В процессе проверки работы программы в отладчике для выполнения в пошаговом режиме подпрограммы обработки прерывания необходимо команду INT выполнить в режиме пошагового выполнения команды (нажать комбинацию клавиш Alt+F7).

Работу программы в отладчике проверить для нескольких пар значений параметров N и j.

Варианты заданий на лабораторную работу

$$N2\underline{i}$$

1. Вычислить значение суммы: $\sum_{i=1}^{j}$

$$Ni^{+}\ \underline{3}$$

2. Вычислить значение произведения: $\prod_{i=1}^{j}$

$$N$$

3. Вычислить значение суммы: $\sum^{i2} + j\ i=1$

$$N\ \underline{i}$$

4. Вычислить значение произведения: $\prod_{i=1}^{2-j}$

$$N$$

5. Вычислить значение суммы: $\sum i^{\cdot}\ j^{-}\ 1\ i=1$

Контрольные вопросы

1. Объясните работу механизма вызова и обработки программных прерываний для МП 8086?

2. Объясните работу механизма вызова и обработки аппаратных прерываний для МП 8086?
3. Какова структура стека сразу после входа в процедуру обработки программного прерывания?
4. Какими способами можно установить значение вектора прерывания?
5. Какие действия выполняет команда INT?
6. Поясните использование функций DOS 25H и 35H.

Лабораторная работа № 3. Техническая реализация средств процедурного программирования в языке C++

Разработайте алгоритм и программу, реализующую структурированный тип данных (СТД), согласно варианту. Определите функции инициализации, присваивания, вывода содержимого и обработки (сортировка, поиск, сравнение, арифметические действия и т.д.).

Варианты СТД:

1. Динамический вектор;
2. Динамическая матрица;
3. Динамический куб;
4. Динамический стек;
5. Динамическая очередь;
6. Линейный связанный список;
7. Динамический массив комплексных чисел;
8. Мультивектор, содержащий три вектора;
9. Персонал;
10. Библиотека. Проверьте работоспособность СТД на тестовом наборе данных.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Сформулируйте назначение функций, необходимость использования, синтаксис и семантику определения, объявления и вызова функций.
2. Что такое прототип функции? Какие преимущества имеют прототипы функций?
3. С какой целью применяются аргументы по умолчанию? В чем заключается синтаксис и семантика их использования?
4. Объясните механизм передачи параметров, в чем преимущества и недостатки передачи параметров по значению и по ссылке?
5. Каким образом функции возвращают значения?
6. Что означает понятие «встроенная функция»?
7. Сформулируйте алгоритм выбора перегруженной функции.
8. Что такое массив? Сформулируйте правила индексирования и инициализации массива.

9. Каким образом создается динамический массив? В чем различия между указателями массивов?
10. Опишите механизм передачи массива функциям.
11. Покажите взаимосвязь между массивами, указателями и ссылками.
12. Что означает «выход за границы массива», к чему это может привести?
13. В чем заключаются особенности работы со строками?
14. Каким образом осуществляется управление свободной памятью?
15. Что такое структуры и объединения? Сформулируйте правила инициализации.
16. Опишите механизм передачи структур функциям.
17. По какому принципу создаются динамические структуры данных?
18. Объясните, что представляет собой массив структур?
19. В каких случаях возникает необходимость использовать вложенные структуры и объединения?

Лабораторная работа № 4. Техническая реализация средств объектноориентированного программирования в языке С++

Разработайте алгоритм и программу, реализующую абстрактный тип данных (АТД) – класс, согласно варианту задания (см. лабораторную работу № 3). Предусмотрите закрытую реализацию и открытый интерфейс. Интерфейс должен содержать псевдоконструкторы и псевдодеструктор, функции присваивания, вывода содержимого и обработки (сортировка, поиск, сравнение, арифметические действия и т.д.). Проверьте работоспособность АТД на тестовом наборе данных.

Контрольные вопросы

1. Дайте определение понятия «класс». Сформулируйте правила доступа к его элементам.
2. С какой целью в классе объединены компонентные данные и компонентные функции?
3. Каким образом осуществляется доступ к открытым и закрытым элементам?
4. Опишите назначение дружественных функций, назовите их разновидности.
5. Что понимается под указателем this?
6. Каковы особенности использования статических компонентных данных?
7. В чем заключается синтаксис и семантика компонентных функций static и const?
8. Каким образом могут изменяться компонентные данные объектов, объявленных константами?
9. Каковы особенности создания вложенных классов?

Лабораторная работа № 5. Статический и динамический анализ программного обеспечения

Разработать план статического и динамического анализа программного кода. Выполнить контроль полноты планирования. Средствами интегрированной среды разработки выполнить статический анализ программного кода. Устранить выявленные несоответствия и провести динамический анализ программного обеспечения. Дополнить код необходимыми для оптимизации работы командами.

Контрольные вопросы:

1. Основные особенности статического анализа программного кода.
2. Основные особенности динамического анализа программного кода.
3. Назначение методов конфигурационного управления.
4. Оценка эффективности вносимых изменений. 5. Способы поиска критических несоответствий.

Средства контроля качества обучения

Вопросы к зачету

1. Предмет дисциплины, ее объем, содержание и связь с другими дисциплинами учебного плана. Цели и задачи дисциплины
2. Архитектура IA32. История развития архитектуры IA32. Основные регистры, форматы команд. Представление машинной команды
3. Организация программы для ОС Windows на языке ассемблера
4. Передача управления: условные и безусловные переходы
5. Вызовы функций. Аппаратная поддержка стека
6. Постановка задачи анализа программного обеспечения
7. Инструментарий для анализа программного обеспечения
8. Техническая реализация средств процедурного программирования в языке C++
9. Техническая реализация средств объектно-ориентированного программирования в языке C++
10. Техника создания защищенных программ и типичные ошибки, приводящие к появлению уязвимостей
11. Виды вредоносного программного обеспечения
12. Статический и динамический анализ программного обеспечения