МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учебно-методическое объединение по естественнонаучному образованию

УТВЕРЖДАЮ
Первый заместитель Министра
образования Республики Беларусь
_____И.А.Старовойтова
«_____»_____ 2018г.
Регистрационный № ТД-_____/тип.

СИСТЕМНОЕ ПРОГРАММИРОВАНИЕ

Типовая учебная программа по учебной дисциплине

для специальности

1-31 03 07 Прикладная информатика (программное обеспечение компьютерных систем)

СОГЛАСОВАНО
Председатель Учебно-
методического объединения по
естественнонаучному образованию
_____ О.А. Ивашкевич
«____» _____ 2018 г.

СОГЛАСОВАНО
Начальник Главного управления
профессионального образования
Министерства образования
Республики Беларусь
_____ А.С. Касперович
«____» _____ 2018 г.

СОГЛАСОВАНО
Проректор по научно-методической
работе Государственного
учреждения образования
«Республиканский институт высшей
школы»
_____ И.В. Титович
«____» _____ 2018 г.

Эксперт-нормоконтролер
_____ _____
«____» _____ 2018 г.

Минск 2018

СОСТАВИТЕЛИ:
А.Н.Курбацкий, заведующий кафедрой технологий программирования Белорусского государственного университета, доктор технических наук профессор;
В.М.Гошко, ассистент кафедры технологий программирования факультета прикладной математики и информатики Белорусского государственного университета

РЕЦЕНЗЕНТЫ:
Кафедра информационных радиотехнологий Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»;

И.А.Король, заместитель начальника управления стратегических проектов Министерства связи и информатизации, кандидат физико-математических наук

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:
Кафедрой технологий программирования Белорусского государственного университета
(протокол № 12 от 17 мая 2018 г.).

Научно-методическим Советом Белорусского государственного университета (протокол № 6 от 16 июня 2018 г.).

Научно-методическим Советом по прикладной математике и информатике учебно-методического объединения по естественнонаучному образованию (протокол № 16 от 29 мая 2018 г.).

Ответственный за редакцию: В.М.Гошко

Ответственный за выпуск: А.Н.Курбацкий

Пояснительная записка

Типовая учебная программа по учебной дисциплине «Системное программирование» разработана в соответствии с типовым учебным планом и образовательным стандартом высшего образования первой ступени по специальности 1-31 03 07 «Прикладная информатика (по направлениям)» (ОСВО 1-31 03 07 – 2013).

Учебная дисциплина «Системное программирование» знакомит студентов с основными принципами построения и организации работы операционных систем семейства Windows.

Подробно рассматриваются вопросы системного программирования с использованием интерфейса Win32 API. Описываются управление потоками и процессами, включая их диспетчеризацию; передача данных между процессами, с использованием анонимных и именованных каналов, а также почтовых ящиков; структурная обработка исключений; управление виртуальной памятью; управление файлами и каталогами; асинхронная обработка данных; создание динамически подключаемых библиотек; разработка сервисов.

Особое внимание уделено вопросам отладки программного обеспечения. Дается обзор существующих инструментов поиска и устранения дефектов, приводится ряд практических рекомендаций по настройке отладчиков, рассматриваются различные сценарии исследования программного обеспечения.

Рассматриваются основы взаимодействия приложений по сети с использованием библиотеки WinSock.

Отдельно рассматриваются методы перехвата вызовов функций и модификации возвращаемых значений. Главной задачей данных тем является формирование у студентов четкого представления функционирования программного обеспечения, передачи управления между функциями, использование стека потока. Предусмотрены соответствующие лабораторные задания.

Данная типовая учебная программа предусматривает поверхностное рассмотрение тем, которые позже будут детально изложены в рамках учебной дисциплины «Операционные системы». Например, управление процессами и потоками, диспетчеризация потоков.

Цель преподавания учебной дисциплины «Системное программирование»: дать студентам базу, необходимую для успешного усвоения материала дисциплин специализации, а также получить знания, необходимые им в дальнейшем для успешной работы. Приобретенные знания позволяют понять основы функционирования операционной системы, и, как следствие, создавать более эффективное программное обеспечение.

В результате изучения учебной дисциплины обучаемый должен

знать:

– основные функции операционной системы;
– основные компоненты операционной системы
– методы взаимодействия процессов;
– методы синхронизации потоков;
– модель памяти в защищенном режиме;
– методы управления виртуальной памятью;
– методы управления файлами;
– принципы построения клиент-серверных приложений с использованием библиотеки WinSock;
– принципы обработки исключительных ситуаций в ОС Windows;
– методы перехвата вызовов функций;
– основные виды уязвимостей программного обеспечения;
– механизмы защиты программ, предоставляемые операционной системой;
– методы отладки и поиска дефектов в программном обеспечении;

уметь:

– программировать многопоточные приложения;
– организовать обмен данными между двумя процессами;
– создавать приложения, взаимодействующие по сети;
– создавать и использовать динамически подключаемые библиотеки;
– пользоваться отладчиком, исследовать аварийные дампы памяти, проблемы утечки памяти;

владеть:

– методами и инструментами отладки и поиска дефектов в системном и прикладном программном обеспечении;
– языком программирования низкого уровня С.

В соответствии с типовым учебным планом и образовательным стандартом для направления специальности: 1-31 03 07-01 «Прикладная информатика» (программное обеспечение компьютерных систем) учебная программа предусматривает для изучения дисциплины 104 учебных часа, из них аудиторных – 68 часов. Примерное распределение аудиторных часов по видам занятий: лекций – 34 часа, лабораторных занятий – 34 часа.

Примерный тематический план

Название раздела	Количество аудиторных часов		
	Всего	В том числе	
		Лекции	Лабораторные занятия
Раздел I. Язык программирования C.	2	2	-
Раздел II. Операционные системы	4	2	2
Раздел III. Управление процессами и потоками	4	2	2
Раздел IV. Управление памятью	6	2	4
Раздел V. Управление файлами	6	2	4
Раздел VI. Динамически подключаемые библиотеки	6	2	4
Раздел VII. Сервисы и драйверы Windows	6	4	2
Раздел VIII. Программирование сети	2	2	-
Раздел IX. Перехват API вызовов	4	2	2
Раздел X. Уязвимости ПО. Безопасное программирование	6	2	4
Раздел XI. Структурная обработка исключений	4	2	2
Раздел XII. Отладка ПО	8	4	4
Раздел XIII. Утилиты SysInternals	4	2	2
Раздел XIV. Инструменты статического анализа кода	6	4	2
Итого	68	34	34

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Язык программирования С

Тема 1.1. Особенности языка языка программирования С

Особенности языка. Отличия от С++. Массивы, строки, адресная арифметика, указатели на функции, функции с переменным числом аргументов. Построение программы (исходные коды -> исполняемый модуль). Построение основных структур данных. Стандартная библиотека языка С. Безопасные аналоги стандартных функций языка С.

Раздел 2. Операционная система Windows.

Тема 2.1. Операционные системы

Операционные системы. Функции. Архитектура. Выполнение задач. Процессы, потоки. Многозадачность. Windows API. UNICODE. etc.

Тема 2.2. Управление процессами и потоками

Понятие процесса. Ресурсы, принадлежащие процессу. Создание и завершение процессов. Дескрипторы процесса. Взаимодействие процессов (файлы, командная строка, разделяемая память). Безопасность. Маркер доступа. Понятие потока. Контекст потока.

Тема 2.3. Управление памятью

Модель памяти в защищенном режиме. Виды памяти (стек, куча, пулы памяти режима ядра, тегирование пула)

Тема 2.4. Управление файлами

Обзор средств управления файлами. Представление файлов на жестком диске. Открытие, закрытие, чтение, запись, управление курсором. Чтение и изменение атрибутов. Создание и удаление каталогов, наблюдение за изменениями. Копирование и перемещение файлов.

Тема 2.5. Динамически подключаемые библиотеки

Назначение динамически подключаемых библиотек. Варианты использования библиотек. Зависимости библиотек. Формат файла PE. Таблицы импорта и экспорта.Загрузка библиотек. Внедрение кода в другой процесс.

Тема 2.6. Сервисы и драйверы Windows

Сервисы Windows. Создание сервиса. Регистрация сервиса в системе. Менеджер сервисов. Запуск и остановка сервисов. Драйверы, точки входа в драйвер. Объект, описывающий драйвер. Объект, описывающий файл. Взаимосвязь объектов. Запрос ввода-вывода. Менеджер ввода-вывода. Стек драйверов. Прерывания, уровни прерываний. Подпрограммы обработки прерываний. Отложенные вызовы процедур. Асинхронные вызовы процедур. Типы асинхронных процедур.

Тема 2.7. Программирование сети

Обзор модели OSI. Обзор сетевых API Windows. Использование Windows Sockets.

Тема 2.8. Перехват API вызовов

Выполнение кода. Стек потока. Соглашения о вызовах. Перехват функций путем модификации исходного кода. Перехват функций путем модификации таблиц импорта/экспорта. Перехват функций путем модификации системных таблиц. Использование драйверов-фильтров.

Раздел 3. Безопасное программирование

Тема 3.1. Уязвимости ПО. Безопасное программирование

Классификация уязвимостей ПО. Ошибка переполнения буфера. Ошибка переполнения переменных. Ошибки форматирования строк. Механизмы защиты программ, предоставляемые операционной системой (ASLR, DEP). Безопасное программирование (переполнение чисел, буфера, неправильное использование памяти, проверка возвращаемых значений). Проверка входных данных

Тема 3.2. Структурная обработка исключений

Обработчики завершения. Фильтры и обработчики исключений. Необработанные исключения и исключения C++.

Тема 3.3. Отладка ПО

Обзор отладчиков. Обзор пакета Debugging Tools for Windows.Отладочные символы. Отладка ПО: исследование аварийных завершений приложений. Отладка ПО: исследование ошибок синхронизации. Отладка ПО: исследование утечки памяти. Отладка ПО: настройка отладки драйверов в режиме ядра. Отладка ПО: настройка аварийного дампа памяти операционной системы.

Тема 3.4. Утилиты Sysinternals

Processmonitor. Processexplorer. autoruns. Handle.

Тема 3.5. Инструменты статического анализа кода

Использование аннотации исходного кода (SAL). PREFast. Codeanalysis для VisualStudio

Информационно-методическая часть

ЛИТЕРАТУРА

Основная

1. Mark E. Russinovich David A. Solomon, Alex Ionescu Windows Internals [Book]. - Portland : Microsoft Press, 2008. - 5th edition. - ISBN 0-7356-2530-1.
2. Рихтер Дж. Windows для профессионалов. Создание эффективных WIN32-приложений с учетом специфики 64-разрядной версии Windows. [Книга]. - СПб : Питер, 2001. - стр. 752 стр.. - ISBN 5-272-00384-5.
3. Побегайло А. П. Системное программирование в Windows. — СПб.: БХВ-Петербург, 2006. - 1056 с: ил. ISBN 5-94157-792-3
4. Mario Hewardt, Daniel Pravat Advanced Windows Debugging [Книга]. - Boston : Addison-Wesley Professional, 2007. - стр. 840. - ISBN-10 / ASIN: 0321374460 ISBN-13 / EAN: 9780321374462.

5. Шилдт, Герберт. Полный справочник по C++, 4-е издание. : Пер. с англ. – М. Издательский дом «Вильямс», 2006. – 800 с. : ил. – Парал. тит. англ.

Дополнительная

6. Алексей Беляев Централизованная обработка исключений [Журнал]. - [б.м.] : RSDN Magazine, 25.09.2004 г.. - 1.
7. Пименаускас Лохас Debugging: Развертывание сервера отладочной информации [В Интернете] // Habrahabr. - http://habrahabr.ru/blogs/development/89094/.
8. Пименаускас Лохас Введение в postmortem debugging [В Интернете] // Habrahabr. - http://habrahabr.ru/blogs/development/89220/.
9. Харт, Джонсон, М Системное программирование в среде Windows, 3-ее издание. : Пер. с англ. – М. : Издательский дом «Вильямс», 2005. – 592 с. : ил. – Парал. тит. англ.

Диагностика компетенций студента

На лекционных занятиях по учебной дисциплине «Системное программирование» рекомендуется особое внимание обратить на общие концепции организации операционных систем.

Необходимо учитывать отсутствие у студентов опыта программирования на языке ассемблера. Это требует дополнительных пояснений, особенно при рассмотрении тем безопасного программирования и перехвата API вызовов.

В силу различного уровня готовности студентов к восприятию новых понятий на практических занятиях по дисциплине рекомендуется проводить регулярные самостоятельные работы и, при необходимости, дополнительные консультации для объяснения и закрепления сложного материала.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и бумажных) вариантов лекций, учебно-методических пособий и сборников задач по основным разделам дисциплины.

Текущий контроль усвоения знаний в течение семестра по учебной дисциплине «Системное программирование» (теоретическая часть учебной дисциплины) рекомендуется осуществлять в виде проведения коллоквиума и двух-трех письменных контрольных работ. В начале лекций рекомендуется делать краткий обзор предыдущей. Для закрепления и проверки знаний и умений студентов (практическая часть) рекомендуется выполнение всех предусмотренных лабораторных работ, совместное рассмотрение наиболее удачных решений и типовых ошибок.

Перечень рекомендуемых средств диагностики

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и

бумажных) учебно-методических пособий по основным разделам учебной дисциплины.

Методические рекомендации по организации и выполнению самостоятельной работы

Текущий контроль по дисциплине «Системное программирование» рекомендуется осуществлять в течение процесса обучения в виде вопросов для самоконтроля и проведения коллоквиумов (лекционная часть).

Рекомендуемая форма текущей аттестации – зачет.