

# БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

**УТВЕРЖДАЮ**

Проректор по учебной работе и  
образовательным инновациям



О.И. Чуприс  
2018 г.

Регистрационный № УД- 5216 / уч.

## СИСТЕМНОЕ ПРОГРАММИРОВАНИЕ

Учебная программа учреждения высшего образования  
по учебной дисциплине для специальности первой ступени высшего об-  
разования:

1-31 03 07 «Прикладная информатика» (по направлениям)  
направление специальности

1-31 03 07-01 «Прикладная информатика» (программное обеспечение  
компьютерных систем)

2018 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-31 03 07-2013, учебного плана УВО G31-167/уч. от 30.05.2013, G31и-194/уч. от 30.05.2013

**СОСТАВИТЕЛИ:**

В.М. Гошко, ассистент кафедры технологий программирования Белорусского государственного университета, магистр физико-математических наук

**РЕЦЕНЗЕНТЫ:**

Рафеенко Е.Д., доцент кафедры многопроцессорных систем и сетей, кандидат физико-математических наук

Дравица В.И., директор ГП «Центр систем идентификации», кандидат физико-математических наук.

**РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:**

Кафедрой технологий программирования (протокол № 11 от 20 апреля 2018 г.).

Научно-методическим Советом Белорусского государственного университета (протокол № 5 от 04 мая 2018 г.).



## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа по дисциплине «Системное программирование» разработана в соответствии с учебным планом и образовательными стандартами первой ступени высшего образования по специальности 1- 31 03 07 Прикладная информатика.

Дисциплина «Системное программирование» относится к циклу специальных дисциплин государственного компонента.

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

Основой для изучения дисциплины «Системное программирование» являются следующие учебные дисциплины: «Программирование», «Операционные системы».

Основные **задачи**, решаемые при изучении учебной дисциплины «Системное программирование»:

- дать студентам базу, необходимую для успешного усвоения материала дисциплин специализации;
- 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 результате изучения учебной дисциплины специалист должен владеть следующими академическими компетенциями (АК) и профессиональными компетенциями (ПК):

**академических компетенций**

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Иметь навыки, связанные с использованием технических устройств, управления информацией и работой с компьютером.

**профессиональных компетенций**

ПК-1. Проектировать, разрабатывать и тестировать программное обеспечение различных видов.

ПК-7. Применять профессиональные знания и навыки для проведения научных исследований в области прикладной информатики.

ПК-9. Работать с научно-технической информацией с использованием современных информационных технологий.

**Социально-личностные компетенции:**

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-5. Быть способным к критике и самокритике.

В соответствии с учебным планом 1-31 03 07 Прикладная информатика для студентов дневной формы получения образования учебная программа предусматривает для изучения дисциплины 104 учебных часа, в том числе 68 аудиторных часа: лекции – 34 часа, лабораторные занятия – 30 часов, управляемая самостоятельная работа – 4 часа. Форма текущей аттестации студентов в рамках данной дисциплины – зачет на втором курсе в 3-ем семестре.

## **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 прерыва-

ний. 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

## УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	Язык программирования С.							
1.1	Особенности языка языка программирования С	4			4			Устный опрос. Отчет по лабораторной работе
2	Операционная система Windows.							
2.1	Операционные системы	2			4			Устный опрос. Отчет по лабораторной работе
2.2	Управление процессами и потоками	2			4			Устный опрос. Отчет по лабораторной работе
2.3	Управление памятью	4			4			Устный опрос. Отчет по лабораторной работе
2.4	Управление файлами	2						Устный опрос
2.5	Динамически подключаемые библиотеки	4			4			Устный опрос. Отчет по ла-



								бора- торной работе
2.6	Сервисы и драйверы Windows	2						Устный опрос
2.7	Программирование сети	2						Устный опрос
2.8	Перехват API-вызовов	2						Устный опрос
3	Безопасное программирование							Кон- троль- ная ра- бота. Колло- квиум
3.1	Уязвимости ПО. Безо- пасное программирова- ние	2			4		2	Устный опрос. Отчет по ла- бора- торной работе
3.2	Структурная обработка исключений	2			2			Устный опрос. Отчет по ла- бора- торной работе
3.3	Отладка ПО	2			2		2	Устный опрос. Отчет по ла- бора- торной работе
3.4	Утилиты Sysinternals	2			2			Устный опрос. Отчет по ла- бора- торной работе
3.5	Инструменты статиче- ского анализа кода	2						Устный опрос
<b>ИТОГО</b>		<b>34</b>			<b>30</b>		<b>4</b>	

## ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

### Рекомендуемая 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.

### **Рекомендации по контролю качества усвоения знаний**

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.

### **Примерный перечень заданий управляемой самостоятельной работы**

Изучение и демонстрация эксплуатации ошибок переполнения буфера, переполнения переменных, форматирования строк.

### **Перечни используемых средств диагностики результатов учебной деятельности**

Для аттестации обучающихся на соответствие их персональных достижений конечным требованиям образовательной программы создаются фонды оценочных средств, включающие типовые задания, контрольные и лабораторные работы.

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

1. Устная форма: опросы, устная защита лабораторных работ, коллоквиум.
2. Письменная форма: отчеты по лабораторным работам.

### **Итоговая оценка формируется на основе:**

1. Правил проведения аттестации студентов (Постановление Министерства образования Республики Беларусь № 53 от 29 мая.2012г.);
2. Положения о рейтинговой системе оценки знаний по дисциплине в БГУ (Приказ ректора БГУ от 18.08.2015 № 382-ОД);
3. Критериев оценки студентов (Письмо Министерства образования от 22.12.2003г.)

## ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Операционные системы	Технологий программирования	Нет	Оставить содержание учебной дисциплины без изменения, протокол № 11 от 20.04.2018 г.

**ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ**

на \_\_\_\_/\_\_\_\_ учебный год

№№ Пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры технологий программирования (протокол № \_\_\_\_ от \_\_\_\_\_ 201\_ г.)

Заведующий кафедрой

\_\_\_\_\_  
(ученая степень, звание)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(И.О. Фамилия)

УТВЕРЖДАЮ

Декан факультета

\_\_\_\_\_  
(ученая степень, звание)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(И.О.Фамилия)