Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное
учреждение высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор
_____/Т.Р. Змызгова/
«31» августа 2022 г.

Рабочая программа учебной дисциплины

БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ

образовательной программы высшего образования –
программы специалитета
10.05.03 — Информационная безопасность автоматизированных систем
Специальность: (специализация №5) безопасность открытых информационных систем
Формы обучения: очная

Курган 2022

Рабочая программа дисциплины «Безопасность операционных систем» составлена в соответствии с учебными планами по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным для очной формы обучения « 30 » 08 2022 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29.08 2022 года, протокол № 1.

Рабочую программу составил:
канд. тех. наук Р.С. Коротовских

Согласовано:

Заведующий кафедрой «БИАС»
канд. техн. наук, доцент Д.И. Дик

Начальник Управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 7 зачетных единиц трудоемкости (252 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр	
		5	6
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**128**	**64**	**64**
Лекции	64	32	32
Лабораторные работы	64	32	32
Самостоятельная работа, всего часов в том числе:	**124**	**80**	**44**
Подготовка к зачету	18	-	18
Подготовка к экзамену	27	27	-
Курсовая работа	36	36	-
Другие виды самостоятельной работы (подготовка к практическим, лабораторным занятиям и рубежному контролю)	43	17	26
Вид промежуточной аттестации	**зачет с оценкой, экзамен**	**экзамен**	**зачет с оценкой**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**252**	**144**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Изучение дисциплины «Безопасность операционных систем» относится к базовой части формируемой участниками образовательных отношений Блока1, сформированных при изучении следующих дисциплин:

- Основы теории защиты информации
- Основы информационной безопасности
- Организация ЭВМ и вычислительных систем.

Результаты обучения служат основой для дисциплин «Сети и системы передачи информации», «Разработка и эксплуатация защищенных автоматизированных систем», «Методы проектирования защищенных распределенных информационных систем», «Техническая защита информации», «Управление информационной безопасностью» и применяются для выполнения курсовых работ и проектов и выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины является приобретение знаний и практических навыков по эксплуатации современных операционных систем (ОС) для обеспечения их эффективного применения с учетом требований информационной безопасности.

Задачи дисциплины:

- изучение устройства и принципов функционирования ОС различной архитектуры;

- изучение принципов построения подсистем защиты в ОС различной архитектуры;

- изучение средств и методов несанкционированного доступа (НСД) к ресурсам ОС.

Компетенции, формируемые в результате освоения дисциплины:

- способность применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем (ОПК-12);

- способность организовывать и проводить диагностику и тестирование систем, защиты информационных автоматизированных систем, проводить анализ уязвимостей систем защиты информационных автоматизированных систем (ОПК-13);

- способность осуществлять администрирование и контроль функционирования средств и систем защиты информационных автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем(ОПК-15);

В результате изучения дисциплины обучающийся должен:

знать:

- принципы построения и функционирования, примеры реализации современных ОС (для ОПК-12);

- функции ОС, основные концепции управления процессом, памятью, устройствами (для ОПК-12);

уметь:

- использовать средства ОС для обеспечения эффективного и безопасного функционирования автоматизированных систем (для ОПК-12, ОПК-13, ОПК-15);

владеть навыками:

- работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев (для ОПК-13, ОПК-15);
- установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности (для ОПК-13, ОПК-12, ОПК-15);
- эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных систем с учетом требований по обеспечению информационной безопасности (для ОПК-15, ОПК-13, ОПК-12).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем	
			Лекции	Лабораторные работы
5 семестр				
Рубеж 1	1	Введение в операционные системы	6	-
	2	Управление процессами	10	16
Рубеж 2	3	Управление памятью	16	16
		Итого:	**32**	**32**
6 семестр				
Рубеж 1	4	WMI – инструментарий управления Windows	4	4
Рубеж 2	5	Основные компоненты системы безопасности и соответствующие функции программного доступа	28	28
		Итого:	**32**	**32**
		Всего за 5 и 6 семестр	**64**	**64**

4.2. Содержание лекционных занятий

5 семестр

Тема 1. Введение в операционные системы.

История развития ОС. Классификация ОС. Основные функции, возлагаемые на ОС. Поколения операционных систем. Ресурсы и управление ими. Вычислительная система как совокупность ресурсов.

Классификация операционных систем по особенностям алгоритмов управления ресурсами, особенностям аппаратных платформ, особенностям областей использования. Загрузка ОС на примере XP. Архитектура ОС. Основные

компоненты исполнительной подсистемы. Компоненты ОС. вынесенные на пользовательский уровень.

Структура файла boot.ini. Файлы NTI.PR и nldelecl. Загрузка драйверов и соответствующие ключи реестра. Загрузка сервисов. SMSS. CSRSS. Winlogon. Ключи реестра. Назначение и возможности систем клона UNIX, систем группы Windows. Интерфейс ОС с пользователями. Диалоговые и пакетные интерфейсы.

Тема 2. Управление процессами.

Понятие процесса. Структуры ОС процесса. Классы приоритетов. Создание процесса. Организация межпроцессорного взаимодействия.

Нити. Структуры ОС нити. Графы состояний и событий. Создание нитей. Организация очередей. Синхронизация нитей.

Эффект гонок. Тупики. Программная реализация. Атомарные инструкции процессора.

Критические секции, семафоры, события. Аппаратная реализация взаимоисключении. Управление распределением времени ЦП. Диспетчеризация нитей.

Алгоритм работы планировщика XP. Win32 Priority Separation. Структурированная обработка исключений.

Тема 3. Управление памятью.

Организация и управление виртуальной памятью. Сегментная, страничная организация памяти. Распределение памяти и выполнение программ.

Адресное пространство процесса. Memory Manager. Отображение файлов в адресное пространство и разделяемая память.

Копирование записью. Рабочие множества. Стратегия замещения страниц.

Системные функции выделения, сканирования, освобождения памяти. Куча и работа с ней.

Динамически линкуемые библиотеки. Структура исполняемых файлов РК - формата. Заголовок РК файла. Таблица объектов (секций] файла.

Страницы образов секций. Экспорт. Таблица экспорта. Таблица адресов экспорта. Таблица указателей на имена. Таблица ординалов. Таблица имен экспорта.

Импорт. Каталог импорта. Таблица просмотра импорта. Таблица адресов импорта. Каталог ресурсов.

Ускорение загрузки приложений с помощью предварительного связывания.

6 семестр

Тема 4. WMI – инструментарий управления Windows.

WM1 - инструментарий управления Windows. Компоненты WMI. Формат управляемого объекта. C1MOM.

Провайдеры ресурсов. Виды классов. Иерархия классов. Подписка на события. Удаленное управление.

Тема 5. Основные компоненты системы безопасности и соответствующие функции программного доступа.

Организация управления доступом и защиты ресурсов ОС.

Основные механизмы безопасности: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита.

Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС.

Основные стандарты ОС. Элементы классификации ОС на примере «Оранжевой книги».

Вход пользователя в локальную систему Windows XP.

Способы хранений хэшей паролей. Формирование ntlm и nt хэшей.

Типичные атаки. Недостатки RC4 механизма 3-го уровня шифрования.

Анатомия токена доступа и дескриптора безопасности.

Работа с привилегиями. SID, DACL, SACL, ACE, маска доступа.

Обобщенные, стандартные и специфические права. Принципы наследования.

Алгоритм предоставления доступа. Challenge-response алгоритм сетевого входа.

Классификация уязвимостей ОС, способы их эксплуатации и основные формы противодействия.

4.3. Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторных работ	Норматив времени, час.
		5 семестр	
2	Управление процессами	*Лабораторная работа №1.* Создать процесс notepad.exe. открывающий текстовый файл, и создать процесс calc.exe в suspended-режиме.	1
		Лабораторная работа №2. Создать процесс calc.exe на новом десктопе. Создать полноэкранный процесс.	1
		Лабораторная работа №3. Вывести pid созданного процесса. Вывести класс приоритета созданного процесса.	1
		Лабораторная работа №4. Создать нить, рекурсивно создающую себя с завершением.	1
		Лабораторная работа №5. Синхронизировать с помощью критической секции доступ к глобальному массиву.	1
		Лабораторная работа №6. Организовать вычисление факториала с помощью 2 нитей.	1
		Лабораторная работа №7. Вывести tid главной нити созданного процесса.	1
		Лабораторная работа №8. Создать нить, рекурсивно создающую себя без завершения.	1
		Лабораторная работа №9. Создать нить, выводящую через каждую секунду свой текущий приоритет.	1

		Лабораторная работа №10. Создать нить в процессе explorer.exe.	1
		Лабораторная работа №11. Создать нить, ожидающую своего завершения.	1
		Лабораторная работа №12. Создать ситуацию взаимоблокировки двух нитей.	1
		Лабораторная работа №13. Создать нить, ожидающую завершения процесса explorer.exe.	1
		Лабораторная работа №14. Синхронизировать с помощью мьютекса доступ к глобальному массиву.	1
	1-ый рубежный контроль	***Тестирование***	***2***
3	Управление памятью	*Лабораторная работа №1.* Выделить 1 мб виртуальной памяти с защитой - только чтение. Выделить 2 мб виртуальной памяти по адресу 0x60000000.	1
		Лабораторная работа №2. Зарезервировать 1 мб виртуальной памяти с защитой - только запись.	1
		Лабораторная работа №3. Вывести адреса всех свободных участков памяти текущего процесса.	1
		Лабораторная работа №4. Вывести адреса всех свободных участков памяти процесса explorer.exe.	1
		Лабораторная работа №5. Вывести список адресов загруженных .dll текущею процесса на основе анализа поля Type структуры MFMORY_BASIC_INFORMATION.	1
		Лабораторная работа №6. Вывести список загруженных .dll текущего процесса на основе анализа заголовка PE-файла.	1
		Лабораторная работа №7. Выделить 3 мб виртуальной памяти с защитой, включающее исполнение, скопировать код, выполнить его.	1
		Лабораторная работа №8. Зарезервировать 1 мб виртуальной памяти с защитой - только запись.	1
		Лабораторная работа №9. Вывести полную карту памяти текущего процесса.	1
		Лабораторная работа №10 . Вывести полную карту памяти процесса explorer.exe.	1
	2-ой рубежный контроль	***Тестирование***	***2***
		Лабораторная работа №11. Вывести список адресов загруженных модулей, не являющиеся dll.	1

		Лабораторная работа №12. Загрузить собственную dll в адресное пространство процесса explorer.exe.	1
		Лабораторная работа №13. С помощью проецируемых в память файлов организовать межпроцессорное взаимодействие.	1
		Лабораторная работа №14. Оценить скорость работы функций библиотеки C runtime library и функций отображения файлов.	1
	Итого		**32**
		6 семестр	
4	WMI – инструментарий управления Windows	*Лабораторная работа №1.* Использование WM1 для полноценного контроля ОС.	4
	1-ый рубежный контроль	***Тестирование***	***1***
5	Основные компоненты системы безопасности и соответствующие функции программного доступа	***Api - функции для работы с гокеном доступа, дескриптором безопасности, ACE.*** *Лабораторная работа 2.* Запрет группе «Администраторы» права исполнения файла.	1
		Лабораторная работа 3. Запрет группе «Пользователи» права чтения файла.	1
		Лабораторная работа 4. Разрешение зарегистрированному пользователю права читать владельца файла.	1
		Лабораторная работа 5. Разрешение зарегистрированному пользователю права записи владельца файла.	1
		Лабораторная работа 6. Разрешение группе «Администраторы» получения списка файлов в каталоге.	1
		Лабораторная работа 7. Разрешение группе «Администраторы» создания нового файла в каталоге.	1
		Лабораторная работа №8. Запрет Системе права чтения файла.	1
		Лабораторная работа 9. Разрешение Системе создавать новый файл в каталоге.	1
		Лабораторная работа №10. Зарезервировать 2 мб виртуальной памяти по адресу 0x70000000.	1
		Лабораторная работа №11. Зарезервировать 1 мб виртуальной памяти в процессе explorer.exe.	1
		Лабораторная работа 12. Разрешение всем полного доступа к файлу.	1
		Лабораторная работа №13. Запрет всем права чтения атрибутов.	1

		Лабораторная работа 14. Разрешение субъектам сетевого входа права чтения атрибутов.	1
		Лабораторная работа 15. Запрет субъектам интерактивного входа права исполнения файла.	1
		Api - функции для работы с привилегиями: *Лабораторная работа №16.* Получить привилегии процесса exlporer.exe.	1
		Лабораторная работа №17. Получить привилегии процесса winlogon.exe.	1
		Лабораторная работа № 18. Получить привилегии процесса svchost.exe - к LocalService.	1
		Лабораторная работа №19. Проверить наличие привилегии SB_TCB_NAME процесса exlporer.exe.	1
		Лабораторная работа №20. Проверить наличие привилегии SB_TCB_NAME процесса winlogon.exe.	1
		Лабораторная работа №21. Проверить наличие привилегии SB_TCB_NAME процесса winlogon.exe к LocalService.	1
		Лабораторная работа №22. Проверить состояние привилегии SeRemoteShutdownPrivilege процесса exlporer.exe.	1
		Лабораторная работа №23. Проверить состояние привилегии SeRemote-ShutdownPrivilege процесса winlogon.exe.	1
		Лабораторная работа №24. Проверить состояние привилегии SeRemote-ShutdownPrivilege svchost.exe к LocalService.	1
		Лабораторная работа №25. Включить в текущем процессе привилегию SeRemoteShutdown Privi1ege.	1
		Лабораторная работа №26. Включить в текущем процессе привилегию SeTakeOwnershipPrivilege.	1
		Лабораторная работа №27. Вклю-чить в текущем процессе привилегию SeLoadDriverPrivilege	1
	2-ой рубежный контроль	***Тестирование***	***1***
	Итого		**32**
	Всего за 5 и 6 семестры		***64***

4.4 Курсовая работа

С целью углубления и укрепления знаний по характеристикам и функциям операционных систем студенты решают прикладные задачи администрирования операционных систем. Студент осуществляем выбор темы исследования самостоятельно по согласованию с преподавателем.

Курсовая работа выполняется в соответствии с индивидуальным заданием.

Объем курсового проекта 20-25 страниц. К защите работы должны быть представлены:

- действующая программа, реализующая все основные функции, указанные в задании:

- комплект программной и эксплуатационной документации.

Основным документом курсовой работы является «Пояснительная записка». Рекомендуемая структура пояснительной записки:

1) Титульный лист.
2) Оглавление (содержание) курсовой работы.
3) Введение.
4) Постановка задачи:
   а) исходные данные;
   б) цель курсовой работы;
   в) задачи, подлежащие рассмотрению (решению) в курсовой работе.
5) Содержательная часть (может быть в виде глав, разделов, параграфов, привязанных к задачам курсовой работы).
6) Заключение и выводы:
   а) перечень полученных результатов (согласно цели и задачам курсовой работы) и их новизна;
   б) выводы, полученные по итогам курсовой работы.

ТЕМАТИКА КУРСОВЫХ РАБОТ

1. Анализ PEB для получения списка загруженных dll и прямой разбор их таблиц экспорта.
2. Анализ эксплойтов для предыдущих версий Windows
3. Виды атак на операционные системы
4. Вирусы-шифровальщики: механизм работы и защита
5. Внедрение dll для перехвата оконных сообщений
6. Вспомогательный сервис для запуска программ с системными привилегиями.
7. Защита процессов с помощью модификации специфических прав.
8. Изменение MANDATORY_LABEL в системных ACE(Windows 7).
9. Изменение MANDATORY_POLICY в токенах доступа (Windows 7).
10. Изменения в списке привилегий с помощью прямой манипуляций с hive-ами.
11. Использование виртуальной машины в качестве песочницы: оптимизация производительности
12. Использование виртуальной машины для повышения безопасности web-серфинга
13. Использование консоли восстановления для удаления вредоносных

файлов
14. Использование консоли восстановления для управления запуском служб
15. Использование механизма хуков для внедрения dll.
16. Использование нотификаторов обращений к реестру.
17. Использование нотификаторов файловой системы.
18. Исследование механизма ASLR в Windows 7
19. Исследование новых аккаунтов при запуске Svchost в Windows 7.
20. Контроль исходящего трафика в Windows
21. Логгер клавиатуры.
22. Перехват API посредством модификации секции импорта.
23. Перехват API посредством сплайсинга секции экспорта.
24. Поиск stream-ов файловой системы.
25. Поиск руткитов 3 кольца с помощью прямого вызова ядра.
26. Поиск файлов с явно установленными дескрипторами безопасности.
27. Поиск файлов с явно установленными уровнями целостности (Windows 7).
28. Программпый комплекс для работы с привилегиями.
29. Процесс аутентификации в операционной системе с точки зрения безопасности
30. Реестр Windows 7 с точки зрения безопасности
31. Сравнение файловых систем с точки зрения настроек безопасности

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работы.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано на лабораторных работах коллективное взаимодействие и разбор конкретных ситуаций, а также обсуждение неясных моментов и ситуаций по лекционному курсу.

Для текущего контроля успеваемости преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, выполнение курсовой работы, подготовку к лабораторным занятиям, к рубежным контролям, подготовку к зачету и экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела Введение в операционные системы Управление процессами Управление памятью WMI- инструментарий управления Windows Основные компоненты системы безопасности и соответствующие функции программного доступа	**6** 1 1 1 2 1
Подготовка к лабораторным работам (по 1 часа)	29
Подготовка к рубежным контролям (по 2часа)	8
Подготовка к зачету	18
Курсовая работа	36
Подготовка к экзамену	27
Всего:	**124**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ (для очной формы обучения)
2. Отчеты студентов по лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2, №3 и №4.
4. Курсовая работа.
5. Перечень вопросов к зачету и экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="6">Содержание</td></tr>
<tr><td rowspan="6">1</td><td rowspan="6">Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="6">Распределение баллов</td></tr>
<tr><td colspan="6">5 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение лабораторной работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>зачет</td></tr>
<tr><td>Балльная оценка:</td><td>1_б х 16= 16_б</td><td>2_б х 14 = 28_б
1_б х 14= 14_б</td><td>6</td><td>6</td><td>30</td></tr>
<tr><td colspan="6">6 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение лабораторной работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>1_б х 15 =15_б</td><td>л/р №1=14_б
л/р №№2-27
1_б х 26= 26_б</td><td>7</td><td>7</td><td>30</td></tr>
</table>

		Курсовая работа, 5 семестр				
		Качество пояснительной записки	Качество программной части	Ритмичность выполнения	Качество защиты	Всего
		до 20	до 30	до 20	до 30	100
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета (экзамена)	60 и менее баллов – неудовлетворительно; незачет; 61…73 – удовлетворительно; зачет; 74… 90 – хорошо; 91…100 – отлично				
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (зачету, экзамену) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные работы, а также курсовую работу в 5 семестре. Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов: - 61 баллов для получения «автоматически» зачета - 68 баллов для получения «автоматически» оценки удовлетворительно». По согласованию с преподавателем студенту, набравшему 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен «автоматически» оценка «хорошо» или «отлично».				
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету или экзамену) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение пропущенных лабораторных работ – до 2 баллов. Прохождение рубежных контролей в зависимости от рубежа. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.				

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования. Зачет и экзамен проводится в традиционной форме.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

На тестирование в 5-ом семестре при рубежном контроле студенту отводится 2 часа, а в 6-ом семестре – 1 час. Варианты тестовых заданий для рубежных контролей №1 и №2 состоят из 20 вопросов, а тестовые задания для рубежных контролей №3 и №4 состоят из 10 вопросов.

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%
«удовлетворительно» – 50% - 70%
«хорошо» – 70% - 90%
«отлично» – 90% - 100% .

Зачет и экзамен проводится в традиционной форме. Зачет и экзамен проводится в форме ответов на 2 вопроса преподавателя, каждый их которых оценивается в 15 баллов. Вопросы для зачета и экзамена доводятся до студентов на последней лекции в семестре. Время, отводимое студенту на подготовку к ответу на вопросы составляет 1 астрономический час.

Результаты текущего контроля успеваемости, зачета, курсовой работы и экзамена, зачета заносятся преподавателем в зачетную или экзаменационную ведомости, которая сдается в организационный отдел института, защиты курсовой работы и экзамена, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей, зачета и экзамена

5 СЕМЕСТР

1-ый рубежный контроль

1. К основным функциям ОС относятся:

а) Предоставление пользователю расширенной или виртуальной машины

б) Защита пользовательских данных и программ от злонамеренных действий пользователей

в) Управление ресурсами

2. Нижним уровнем вычислительной системы как совокупности ресурсов является

а) Аппаратный уровень вычислительной системы

б) Уровень систем программирования

в) Уровень управления логическими/виртуальными ресурсами вычислительной системы

3. К модулям, выполняющим основные функции ОС, относится

а) Библиотека ввода-вывода

б) Ядро

в) Компилятор

4. Возможность защиты кода и данных операционной системы за счет выполнения функций ядра реализуется с помощью

а) Привилегированного режима
б) Пользовательского режима
в) Режима отладки

2-ой рубежный контроль

1. Существует три типа систем реального времени. Какой вариант к ним не относится?

а) Жёсткие системы реального времени
б) Твёрдые системы реального времени
в) Чёткие системы реального времени

2. Для последовательного вычисления нескольких больших задач без промежуточных переключений между ними наиболее эффективно использовать…

а) Системы пакетной обработки
б) Системы разделения времени
в) Системы реального времени

3. Вытесняющие алгоритмы динамического планирования характерны для ОС…

а) Систем пакетной обработки
б) Систем разделения времени
в) Систем реального времени

4. Какие типы операционных систем используются наиболее часто в настоящее время?

а) системы семейства Windows
б) системы семейства MS DOS
в) системы семейства IBM OS 360/370

6 СЕМЕСТР

1-ый рубежный контроль

1. Поток - наименьшая единица обработки, исполнение которой может быть назначено ядром ОС. Общим для потоков одного процесса является…

а) Стек
б) Счётчик выполнения команд
в) Адресное пространство

2. Что в многозадачной ОС можно создать быстрее?

а) Поток
б) Процесс
в) Поток и процесс создаются с одинаковой скоростью

3. Сколько потоков может находиться в состоянии выполнения в однопроцессорной многозадачной операционной системе?

а) Не меньше двух

б) Один

в) До пяти – по количеству активных сеансов пользователей

4. В семействе ОС Windows NT при завершении процесса родителя, процесс-ребёнок…

а) Завершается

б) Переходит в состояние ожидания

в) Не завершается

2-ой рубежный контроль

1. Ситуация, когда два или более процесса обрабатывают разделяемые данные и конечный результат зависит от соотношения скоростей процессов, называется …

а) Гонкой

б) Тупиком

в) Коллизией

2. Нить (поток) в системе с тремя состояниями (готовность, выполнение, ожидание) и абсолютными приоритетами не может совершить переход…

а) из состояния готовности в состояние выполнения

б) из состояния ожидания в состояние выполнения

в) из состояния ожидания в состояние готовности

3. Какие типы операционных систем используются наиболее часто в настоящее время?

а) системы семейства Windows

б) системы семейства MS DOS

в) системы семейства IBM OS 360/370

4. Какое условие необходимо выполнить для избежания гонок

а) Два процесса должны одновременно находиться в критических областях

б) Наблюдается ситуация, в которой процесс бесконечно ждёт попадания в критическую область

в) В программе не должно быть предположений о скорости или количестве процессоров

Примерный перечень вопросов к зачету

1. История развития ОС. Классификация ОС. Основные функции возлагаемые на ОС.
2. Поколения операционных систем. Ресурсы и управление ими.
3. Вычислительная система как совокупность ресурсов.
4. Классификация операционных систем по особенностям алгоритмов

управления ресурсами, особенностям аппаратных платформ, особенно стям областей использования.
5. Загрузка ОС на примере XP.
6. Архитектура ОС. Основные компоненты исполнительной подсистемы.
7. Компоненты ОС, вынесенные на пользовательский уровень.
8. Структура файла boot.ini. Файлы NTLDR и ntdetect.
9. Загрузка драйверов и соответствующие ключи реестра.
10. Загрузка сервисов. SMSS, CSRSS, Winlogon.
11. Ключи реестра.
12. Назначение и возможности систем клона UNIX, систем группы Windows.
13. Интерфейс ОС с пользователями.
14. Диалоговые и пакетные интерфейсы.
15. Понятие процесса. Структуры ОС процесса. Классы приоритетов.
16. Создание процесса. Организация межпроцессорного взаимодействия.
17. Нити. Структуры ОС нити. Графы состояний и событий.
18. Создание нитей. Организация очередей. Синхронизация нитей.
19. Эффект гонок. Тупики. Программная реализация.
20. Атомарные инструкции процессора.
21. Критические секции, семафоры, события.
22. Аппаратная реализация взаимоисключений.
23. Управление распределением времени ЦП. Диспетчеризация нитей.
24. Алгоритм работы планировщика XP. Win32 Priority Separation.
25. Структурированная обработка исключений.
26. Организация и управление виртуальной памятью.
27. Сегментная, страничная организация памяти.
28. Распределение памяти и выполнение программ.
29. Адресное пространство процесса. Memory Manager.
30. Отображение файлов в адресное пространство и разделяемая память.
31. Копирование записью. Рабочие множества.
32. Стратегия замещения страниц.
33. Системные функции выделения, сканирования, освобождения памяти.
34. Куча и работа с ней.
35. Динамически линкуемые библиотеки. Структура исполняемых файлов PE - формата.
36. Заголовок PE файла. Таблица объектов (секций) файла.
37. Страницы образов секций. Экспорт.
38. Таблица экспорта. Таблица адресов экспорта. Таблица указателей на имена.
39. Таблица ординалов. Таблица имен экспорта.
40. Импорт. Каталог импорта. Таблица просмотра импорта.
41. Таблица адресов импорта. Каталог ресурсов.
42. Ускорение загрузки приложений с помощью предварительного связывания.
43. Внедрение dll в адресное пространство другого процесса.
44. Перехват API - функций.

Примерная тематика вопросов, выносимых на экзамен

1. WMI - инструментарий управления Windows.
2. Компоненты WMI.
3. Формат управляемого объекта.
4. CIMOM.
5. Провайдеры ресурсов.
6. Виды классов.
7. Иерархия классов.
8. Подписка на события.
9. Удаленное управление.
10. Организация управления доступом и защиты ресурсов ОС.
11. Основные механизмы безопасности: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита.
12. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС.
13. Основные стандарты ОС.
14. Элементы классификации ОС на примере "Оранжевой книги".
15. Вход пользователя в локальную систему Windows XP.
16. Способы хранений хэшей паролей.
17. Формирование ntlm и nt хэшей.
18. Типичные атаки.
19. Недостатки RC4 - механизма 3-го уровня шифрования.
20. Анатомия токена доступа и дескриптора безопасности.
21. Работа с привилегиями.
22. SID, DACL, SACL, ACE, маска доступа.
23. Обобщенные, стандартные и специфические права.
24. Принципы наследования.
25. Алгоритм предоставления доступа.
26. Challenge-response алгоритм сетевого входа.
27. Классификация уязвимостей ОС, способы их эксплуатации и основные формы противодействия.
28. Переполнение стека.
29. Format-string уязвимости.
30. Механизм DEP.
31. Рандомизация адресного пространства.
32. Усовершенствование алгоритмов управления кучей.
33. Стековые cookie.
34. Новые опции компилятора и линкера.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания об-

разовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть1. Основы и принципы [Электронный ресурс]: Бином-Пресс - Москва, 2011. - 489 с. – Доступ из ЭБС «Консультант студент».

2. Дейтел, Х.М.; Чофнес, Д.Р.; Дейтел, П.Дж. Операционные системы. Часть 2. Распределенные системы, сети, безопасность [Электронный ресурс]: М.: Бином - Москва, 2011. - 704 с. – Доступ из ЭБС «Консультант студент».

3. Дейтел, Г. Введение в операционные системы UNIX, VAX, CP/M, MVS, VM; М. [Электронный ресурс]: Мир - Москва, 2013. - 758 с. – Доступ из ЭБС «Консультант студент».

4. Киселев С. В., Алексахин С. В., Остроух А. В. Операционные системы. Учебное пособие; Академия - Москва, 2013. - 355 с. – Доступ из ЭБС «Консультант студент».

5. Олифер, В.Г. Сетевые операционные системы. 2-е изд. / В.Г. Олифер, Н.А. Олифер [Электронный ресурс]: СПб. : Питер, 2009. — 544 с. – Доступ из ЭБС «Консультант студент».

6. Таненбаум, Э. Современные операционные системы [Электронный ресурс]: СПб: Питер; Издание 2-е - Москва, 2013. - 910 с. – Доступ из ЭБС «Консультант студент».

7.2. Дополнительная учебная литература

1. Бэкон, Джин; Харрис, Тим Операционные системы. Параллельные и распределенные системы [Электронный ресурс]: СПб: Питер - Москва, 2012. - 800 с. – Доступ из ЭБС «Консультант студент».

2. Девис, У. Операционные системы. Функциональный подход [Электронный ресурс]: М.: Мир - Москва, 2013. - 437 с. URL: https://studfiles.net/preview/6149569/ (дата обращения: 18.10.2017)

3. Касперски, Крис. Фундаментальные основы хакерства [Электронный ресурс]: Искусство дизассемблирования / Крис Касперски. – М.: СОЛОН-Р, 2002. – 448 с. URL: http://forcoder.ru/security/fundamentalnye-osnovy-hakerstva-343

4. Фодор, Ж.; Бонифас, Д.; Танги, Ж. Операционные системы для IBM PC: DOS 1.1, 2.0, 2.1, 3.0, 3.1/PC-IX, XENIX; М. [Электронный ресурс]: Мир - Москва, 2013. - 244 с. – Доступ из ЭБС «znanium.com».

7.3 Методическая литература:

1. Рабушко А.Г. Механизмы виртуальной памяти. [Электронный ресурс]: Методические указания к выполнению лабораторной работы по дисциплине «Безопасность операционных систем» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. КГУ, 2013. – Доступ из ЭБС КГУ.

2. Рабушко А.Г. Создание процессов и нитей. Синхронизация нитей. [Электронный ресурс]: Методические указания к выполнению лабораторной работы по дисциплине «Безопасность операционных систем» для студентов оч-

ной формы обучения для направлений 10.05.03 и 10.03.01. КГУ, 2016. – Доступ из ЭБС КГУ.

3. Рабушко А.Г. WMI - инструментарий управления Windows [Электронный ресурс]: Методические указания к выполнению лабораторной работы по дисциплине «Безопасность операционных систем» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. КГУ, 2016. – Доступ из ЭБС КГУ.

4. Рабушко А.Г. Api - функции для работы с привилегиями [Электронный ресурс]: Методические указания к выполнению лабораторной работы по дисциплине «Безопасность операционных систем» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. КГУ, 2016. – Доступ из ЭБС КГУ.

5. Рабушко А.Г. Api - функции для работы с токеном доступа, дескриптором безопасности, ACE [Электронный ресурс]: Методические указания к выполнению лабораторной работы по дисциплине «Безопасность операционных систем» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. КГУ, 2016. – Доступ из ЭБС КГУ.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

1. Ревняков Е.Н. Методические указания к выполнению курсовой работы по дисциплине «Безопасность операционных систем» для студентов очной формы обучения для направлений 10.05.03 и 10.03.01. КГУ, кафедра «Безопасность информационных и автоматизированных систем», 2017. – 13 с.

9. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронно-библиотечная система издательства «Лань». – Режим доступа: http://e.lanbook.com/. – загл. с экрана.
2. Единое окно доступа к образовательным ресурсам. – Режим доступа: http://window.edu.ru/. – загл. с экрана.
3. Научная электронная библиотека. – Режим доступа: http://elibrary.ru/. – загл. с экрана.
4. Электронно-библиотечная система научно-издательского центра «ИНФРА-М». – Режим доступа: http://znanium.com/. – загл. с экрана.
5. http://intuit.ru;
6. http://infotecs.ru;
7. http://www.itsec.ru.
8. ЭБС htt://www.znanium.com/
9. ЭБС htt://www.studentlibrary.ru
10. http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел
11. http://window.edu.ru/. Единое окно доступа к образовательным ресурсам
12. http://elibrary.ru/. Научная электронная библиотека
13. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

1. Графический сетевой эмулятор GNS3
2. Эмулятор рабочей станции Virtual PC Simulator
3. Виртуальная машина VMware Player
3. Telnet терминал Putty или TeraTerm
4. Сетевой анализатор WireShark
5. Среда программирования Visual C++
4. Пакет Open Office

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран) – 1 комплект. Для проведения практических и лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого: локальная сеть компьютеров на базе ПК Pentium с установленным программным обеспечением MS Windows XP и с возможностью выхода в Интернет. Для эффективной работы в рамках дисциплины рекомендуется иметь возможность работать с исходными текстами программ, сохраненными на съемных накопителях информации.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Безопасность операционных систем»

образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Специальность: (специализация №5) **Безопасность открытых информационных систем**

Трудоемкость дисциплины: 7 з.е. (252 академических часа)
Семестр: 5 и 6 (очная форма обучения)
Форма промежуточной аттестации: экзамен, зачет с оценкой

Содержание дисциплины

Общая характеристика операционных систем; назначение и возможности систем клона UNIX, систем группы Windows; интерфейс ОС с пользователями; диалоговые и пакетные интерфейсы; управление ресурсами; управление процессорами; управление памятью; управление устройствами; драйверы внешних устройств; файловые системы; управление программами: понятие программы, организация динамических и статических вызовов, взаимодействие ОС с программами и отладчиками; виртуальные программы; управление процессами: состояния процессов, синхронизация процессов, обмен сообщениями, стратегии и дисциплины планирования, наследование ресурсов, тупиковые ситуации, обработка исключений, сохранение и восстановление процессов; организация управления доступом и защиты ресурсов ОС; основные механизмы безопасности: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита; администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС; основные стандарты ОС.