МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Майкопский государственный технологический университет»

Факультет Информационных систем в экономике и юриспруденции

Кафедра Информационной безопасности и прикладной информатики

УТВЕРЖДАЮ
Проректор по учебной работе
Л.И. Задорожная
" 27 " мая 2019 г

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.Б.18 Безопасность операционных систем

по специальности 10.05.04 Информационно-аналитические системы безопасности

по специализации №2 «Информационная безопасность финансовых и экономических структур

квалификация (степень) выпускника Специалист

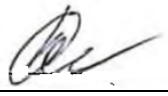
форма обучения Очная

год начала подготовки 2019

Майкоп

Рабочая программа составлена на основе ФГОС ВО и учебного плана МГТУ по направлению (специальности) 10.05.04 Информационно-аналитические системы безопасности

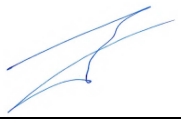
Составитель рабочей программы:

доцент, канд. пед. наук, , доцент		Паскова А.А.
(должность, ученое звание, степень)	(подпись)	(Ф.И.О.)

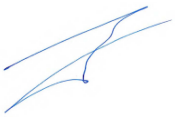
Рабочая программа утверждена на заседании кафедры

Информационной безопасности и прикладной информатики

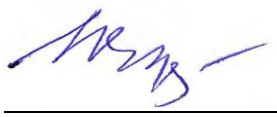
(наименование кафедры)

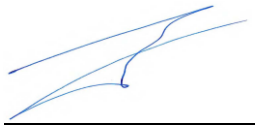
Заведующий кафедрой «27» мая 2019 г.		Чундышко В.Ю.
	(подпись)	(Ф.И.О.)

Одобрено учебно-методической комиссией факультета
(где осуществляется обучение) «27» мая 2019 г.

Председатель учебно-методического совета направления (специальности) (где осуществляется обучение)		Чундышко В.Ю.
	(подпись)	(Ф.И.О.)

Декан факультета (где осуществляется обучение) «27» мая 2019 г.		Доргушаова А.К.
	(подпись)	(Ф.И.О.)

СОГЛАСОВАНО: Начальник УМУ «27» мая 2019 г.		Чудесова Н.Н..
	(подпись)	(Ф.И.О.)

Зав. выпускающей кафедрой по направлению (специальности)		Чундышко В.Ю.
	(подпись)	(Ф.И.О.)

1. Цели и задачи освоения дисциплины

Основной целью изучения дисциплины «Безопасность операционных систем» является обучение основным механизмам защиты современных операционных систем, получение знаний о принципах построения защиты информации в операционных системах и анализе надежности защиты операционных систем

Основные задачи дисциплины:

- обучить студентов принципам построения системы защиты в операционных системах различной архитектуры;
- - дать теоретические основы устройства и функционирования современных операционных систем;
- привить студентам системный подход к проблеме защиты информации в операционных системах;
- дать студентам представление о средствах и методах несанкционированного доступа к операционной системе.

2. Место дисциплины в структуре ОП специалитета

Дисциплина входит в перечень дисциплин базовой части ОП. Она имеет параллельные логические и содержательно-методические связи с дисциплинами «Информатика», «Основы информационной безопасности», «Безопасность информационно-аналитических систем».

Стремительное развитие информационных технологий привело к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Однако с развитием информационных технологий возникают и стремительно растут риски, связанные с их использованием, появляются совершенно новые угрозы, с последствиями, от реализации которых человечество раньше не сталкивалось.

Одним из главных инструментов для реализации конкретных информационных технологий являются информационные системы, задача обеспечения безопасности которых является приоритетной, так как от сохранения конфиденциальности, целостности и доступности информационных ресурсов зависит результат деятельности информационных систем.

Операционная система является важнейшим программным компонентом любой вычислительной машины, поэтому от уровня реализации политики безопасности в каждой конкретной операционной системе во многом зависит и общая безопасность информационной системы.

В связи с этим знания в области современных методов и средств обеспечения безопасности операционных систем являются необходимым условием для формирования специалиста по информационной безопасности.

Дисциплина «Безопасность операционных систем» предназначена для формирования у выпускников теоретических знаний и практических навыков в области в области обеспечения безопасности операционных систем, выбора и применения операционных систем для задач автоматизации обработки информации и управления.

3.Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

В результате изучения курса «Безопасность операционных систем» у студентов должны быть сформированы следующие компетенции:

Способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерной системе (ПК-9).

Студенты должны:

знать: основные средства и способы обеспечения информационной безопасности; требования к защищенным операционным системам; критерии оценки эффективности и надежности средств защиты операционных систем; принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; защитные механизмы и средства обеспечения сетевой безопасности; критерии и методы оценивания механизмов защиты (ПК-9).

уметь: оценивать эффективность защиты; выявлять слабости защиты операционных систем и использовать их для вскрытия защиты; планировать политику безопасности операционных систем; пользоваться средствами защиты, предоставляемыми операционными системами; применять средства антивирусной защиты и обнаружения вторжений; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; проводить анализ и оценивание механизмов защиты (ПК-9).

владеть: навыками построения защиты в операционных системах Windows, Unix, работы в различных операционных средах; реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; методикой анализа сетевого трафика (ПК-9).

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3 **зачетные единицы (108 часов).**

4.1. Объем дисциплины и виды учебной работы по очной форме обучения.

Вид учебной работы	**Всего часов/з.е.**	**Семестры**			
		6			
Контактные часы (всего)	**72,25/2**	**72,25/2**			
В том числе:					
Лекции (Л)	18/0,5	18/0,5			
Практические занятия (ПЗ)	-	-			
Семинары (С)	-	-			
Лабораторные работы (ЛР)	54/1,5	54/1,5			
Контактная работа в период аттестации (КРАт)	-	-			
Самостоятельная работа под руководством преподавателя (СРП)	0,25/0,1	0,25/0,1			
Самостоятельная работа студентов (СРС) (всего)	**35,75/0,99**	**35,75/0,99**			
В том числе:					
Курсовой проект (работа)	-	-			
Расчетно-графические работы	-	-			
Реферат	-	-			
Другие виды СРС (если предусматриваются, приводится перечень видов СРС) 1. Составление плана-конспекта 2. Выполнение самостоятельных заданий 2. Подготовка к лабораторным работам	 14,75/0,42 14/0,39 7/0,19	 14,75/0,42 14/0,39 7/0,19			
Форма промежуточной аттестации: **зачет**	+	+			
Общая трудоемкость	**108/3**	**108/3**			

5. Структура и содержание дисциплины

5.1. Структура дисциплины для очной формы обучения

№ п/п	Раздел дисциплины	Неделя семестра	Виды учебной работы, включая самостоятельную и трудоемкость (в часах)						Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
			Л	ПР	КРАт	СРП	Контроль	СР	
6 семестр									
1.	Понятие операционных систем. Основные механизмы функционирования операционных систем.	1-4	4	10	-			6,75	Обсуждение докладов
2.	Теоретические основы защиты операционных систем. Обзор методов несанкционированного доступа к операционной системе.	5-9	4	12	-			7	Письменный опрос
3.	Основные механизмы защиты в ОС Windows.	10-11	4	12	-			7	Обсуждение докладов, тестирование
4.	Администрирование сетей передачи данных. Защита операционной системы в сети. Службы каталогов. ActiveDirectory.	12-13	2	10	-			7	Обсуждение докладов
5.	Основные механизмы защиты в ОС Linux. Системы мандатной защиты. SELinux. Защита операционной системы в сети.	14-16	4	10	-			8	Контрольная работа
6.	Промежуточная аттестация, зачет	17						+	Зачет в форме теста
Итого:			**18**	**18**	**54**	**-**	**-**	**237**	**35,75**

5.2.Содержание разделов дисциплины «Безопасность операционных систем», образовательные технологии

Лекционный курс

№ п/п	Наименование темы дисциплины	Трудоемкость (часы/зач. ед.) ОФО	Содержание	Формируемые компетенции/ трудовые функции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
Тема 1.	Понятие операционных систем. Основные механизмы функционирования операционных систем.	4/0,11	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.	ПК-9	**Знать:** основные понятия и термины в области операционных систем, основные механизмы функционирования операционных систем. **Уметь:** организовать своюсамостоятельную работу по изучению основной и дополнительной литературы. **Владеть:** навыками сбора и анализа информации	Слайд-лекции

Тема 2.	Теоретические основы защиты операционных систем. Обзор методов несанкционированного доступа к операционной системе.	4/0,11	Основные термины безопасности операционных систем. Обработка исключений, сохранение и восстановление процессов; организация управления доступом и защиты ресурсов ОС, основные механизмы безопасности. Несанкционированный доступ. Эксплоит. Руткит. Вирус. Троянский конь. Удаленный доступ. «Зеро-дэй» уязвимости. Шелл-коды. Пользователи. Дискреционное разделение доступа. Мандантная политика. Матрицы доступа. 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.	ПК-9	**Знать:**термины безопасности операционной системы, Понятие несанкционированного доступа к операционной системе, основные понятия администрирования операционных систем. **Уметь:** организовать своюсамостоятельную работу по изучению основной и дополнительной литературы. **Владеть:** навыками администрирования операционных систем.	Лекции-беседы, работа в малых группах
Тема 3.	Основные механизмы защиты в ОС Windows.	4/0,11	Основные принципы ОС Windows. Планирование развертывания ОС Windows. Эволюция технологий разграничения доступа в ОС Windows.	ПК-9	**Знать:** понятие SID, RID, файловые системы. **Уметь:** развертывать ОС Windows, организовывать разграничение доступа.	Лекция-визуализация, коллективное обучение

			Пользователи в Windows. Понятие SID, RID. Алгоритм генерации SID. Делегирование полномочий. Разделение доступа. Администрирование дисковых ресурсов. Файловые системы Windows.		**Владеть:** навыками администрирования дисковых ресурсов.	
Тема 4.	Администрирование сетей передачи данных. Защита операционной системы в сети. Службы каталогов. ActiveDirectory.	2/0,055	Брандмауэр Windows. Сетевые технологии Windows. SMB. Net Bios. Контроль подключений к ОС. Технологии удаленного доступа к ОС Windows. Типы сетей. Основные принципы Active Directory. Домен. Лес. Интеграция Active Directory с DNS. Политики безопасности. Контроллеры домена. Роли мастера операций. Парольные политики. Делегирование полномочий. Наследование полномочий. Уровни доверия.	ПК-9	**Знать:** понятие и термины сетевых технологий, классификацию сетей, основные принципы ActiveDirectory. **Уметь:** осуществлять адресацию в сетях TCP/IP, работать со службой и протоколом DNS, работать с утилитами тестирования работы службы. **Владеть:** методами контроля доступности файловых ресурсов и управления безопасностью общих сетевых ресурсов, навыками администрирования сетей.	Проблемные лекции, интерактивное электронное обучение
Тема 5.	Основные механизмы защиты в ОС Linux. Системы мандатной защиты. SELinux. Защита операционной системы в сети.	4/0,11	Основные принципы ОС на базе ядра Linux. Планирование развертывания ОС на базе ядра Linux. Классические механизмы защиты. Пользователи и группы в Linux. Разделение доступа. Понятие пользователей и групп в Linux.	ПК-9	**Знать:** особенности операционных систем семейства Linux, понятие процесса, канала, файловой системы, файла аудита, мандатной защиты. **Уметь:** организовывать разграничение доступа,	Проблемные лекции, интерактивное электронное обучение

			Понятие ID. Классическая схема разделения доступа. Понятие владельца. Наследование полномочий. Системы мандатной защиты. Основные принципы SELinux. Принципы совмещения классической системы разделения доступа с мандатной защитой. Ограничения SELinux. Аналоги SELinux. Механизмы изоляции исполняемого кода в Linux. Виртуализация. Контейнеры. Зоны. Изоляция кода на уровне пользователя. Изоляция кода на уровне ядра. Механизмы защиты данных в Linux. Понятие шифрования данных. Шифрования уровня отдельных файлов. Шифрование на уровне файловой системы. Сертификаты и ключи. Резервное копирование. Снимки файловых систем. Журналирование. Защита ОС в сети. Сетевое взаимодействие с ОС. Протоколы удаленного доступа. Сетевые экраны. Принципы фильтрации сетевых пакетов. IPTables.		работать с сетевыми фильтрами. **Владеть:** навыками работы с объектами файловой системы.	
	Итого	**18/0,5**				

5.3.Практические и семинарские занятия, их наименование, содержание и объем в часах

Учебным планом не предусмотрены.

5.4. Лабораторные занятия, их наименование и объем в часах

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Объем в часах/ трудоемкость в з.е.
1	Понятие операционных систем. Основные механизмы функционирования операционных систем.	Определение основных угроз информационной безопасности в компьютерных системах.	4/0,11
		Резервное копирование образа системы и восстановление операционной системы, приложений, личных параметров и файлов на компьютере.	6/0,17
2	Теоретические основы защиты операционных систем. Обзор методов несанкционированного доступа к операционной системе.	Организация консоли администрирования в ОС Windows	4/0,11
		Архивирование и восстановление данных	4/0,11
		Защита файлов от несанкционированного доступа с помощью архиваторов и средств MS Office.	4/0,11
3	Основные механизмы защиты в ОС Windows.	Мониторинг, оптимизация и аудит ОС Windows	4/0,11
		Файловая система и права доступа	4/0,11
		Изучение команд для работы с файлами	2/0,055
		Изучение команд для работы с дисками	2/0,055
4	Администрирование сетей передачи данных. Защита операционной системы в сети. Службы каталогов. ActiveDirectory.	Определение конфигурации и тестирование работоспособности протокола TCP/IP в ОС Windows.	4/0,11
		Анализ степени защищенности серверной операционной системы.	6/0,17
5	Основные механизмы защиты в ОС Linux. Системы мандатной защиты. SELinux. Защита операционной системы в сети.	Исследование файловых объектов с правами пользователя	2/0,055
		Детальное исследование файловой системы EXT2FS	2/0,055
		Восстановление данных программными средствами ОС Linux	2/0,055
		Администрирование операционной системы Linux	2/0,055
		Исследование процессов в ОС Linux	2/0,055

	Итого		**54/1,5**

5.5. Примерная тематика курсовых проектов (работ)

Курсовой проект (работа) учебным планом не предусмотрены.

5.6. Самостоятельная работа студентов

Содержание и объем самостоятельной работы студентов

№ п/п	**Разделы и темы рабочей программы самостоятельного изучения**	**Перечень домашних заданий и других вопросов для самостоятельного изучения**	**Сроки выполнения**	**Объем в часах/трудоемкость в з.е.**
6 семестр				
1.	Задачи современных информационных систем. Понятие защищенной информационной системы. Свойства защищенной информационной системы. Методы создания защищенных информационных систем.	Составление плана-конспекта.	1-4 неделя	6,75/0,19
2.	Понятие безопасности информационных систем в нормативных документах. Классификация защищенности (международные стандарты). Обзор свойств основных классов. Политика безопасности, формальное представление политикбезопасности. Классификация изъянов защиты поразмещению в вычислительной системе. ОС как среда нарушений безопасности. Категорииизъянов защиты в ОС. Понятие доверенного ПО операционных систем, ТСВ.	Выполнение самостоятельных заданий.	5-9 неделя	7/0,19
3.	Типы субъектов и объектов защиты. Атрибутивная природа контроля доступа к объектамзащиты. Списки и записи контроля доступа. Проверка доступа. Эффективные права доступа. Организация контроля безопасности в ОС Windows. Шаблоны безопасности. Анализбезопасности с	Подготовка к лабораторным работам.	10-11 неделя	7/0,19

	помощью шаблонов. Подсистема аудита. Защита данных при хранении в ОС, EFS. Защита данных при передаче, поддержка VPN. Контроль целостности в ОС. Целостность ядра ОС. Обеспечениецелостности кода. Управление учетными записями. Мандатный контроль целостности. Изоляция привилегий пользовательского интерфейса. Защищенные процессы. Изоляциянулевой сессии.			
4.	Обеспечение безопасности серверных приложений ОС. Сервер IIS, его механизмызащиты. Защита DNS. Защита RDS (протокола удалённого рабочего стола).	Выполнение самостоятельных заданий.	12-13 неделя	7/0,19
5.	Шифрованиефайловых систем в ОС UNIX. Защищенные терминалы. Механизмы RSBAC, GR Security. Применение подключаемыхмодулей аутентификации PAM. Анализ журналов, управление ими изащита. Фильтрация трафика. Использованиепрокси-серверов. Технологии Open SSL,SSH. Задание конфигурации безопасности.Файлы конфигурации. Настройка безопасности сервера Apache, модули, создание замкнутой среды выполнения. Анализ уязвимостей на примере ОС UNIX.	Составление плана-конспекта	14-16 неделя	8/0,22
6.	Промежуточная аттестация, зачет	Подготовка к зачету	17 неделя	+
	Итого:			**35,75/0,99**

6.Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю).

6.1. Методические указания (собственные разработки)

1. Чефранов, С.Г. Идентификация и управление сложными объектами: математические модели, информационные технологии и комплексы программ [Электронный ресурс]: учебное пособие / Чефранов С.Г., Сапиев А.З.; – Майкоп: МГТУ, 2015. – 123 с. – Режим доступа: http://lib.mkgtu.ru:8002/libdata.php?id=2100023696

6.2 Литература для самостоятельной работы

1. Васильков, А. В. Безопасность и управление доступом в информационных системах [Электронный ресурс]: учеб. пособие / А.В. Васильков, И.А. Васильков. — М.: ФОРУМ: ИНФРА-М, 2017. – 368 с. ЭБС «Znanium.com» – Режим доступа: http://znanium.com/catalog.php?bookinfo=537054
2. Власов, Ю.В. Администрирование сетей на платформе MS WindowsServer [Электронный ресурс]/ Ю.В. Власов, Рицкова Т.И. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 622 с. – ЭБС «IPRbooks» — Режим доступа: http://www.iprbookshop.ru/52219
3. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]: учебное пособие / Е.В. Глинская, Н.В. Чичварин. – М.: ИНФРА-М, 2018. – 118 с. – ЭБС «Znanium.com» – Режим доступа:http://znanium.com/catalog.php?bookinfo=925825
4. Гончарук, С.В. Администрирование ОС Linux [Электронный ресурс]/ С.В.Гончарук – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 164 с. – ЭБС «IPRbooks» – Режим доступа: http://www.iprbookshop.ru/52142
5. Култыгин, О.П. Администрирование баз данных. СУБД MS SQL Server [Электронный ресурс]: учебное пособие/ О.П. Култыгин – М.: Московский финансово-промышленный университет «Синергия», 2012.– 232 с.– ЭБС «IPRbooks»– Режим доступа: http://www.iprbookshop.ru/17009
6. Назаров, С.В. Современные операционные системы [Электронный ресурс]: учебное пособие/ С.В. Назаров, А.И. Широков. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 351 с. – ЭБС «IPRbooks» – Режим доступа: http://www.iprbookshop.ru/52176.html.
7. Федотов, Е.А. Администрирование программных и информационных систем [Электронный ресурс]: учебное пособие/ Е.А.Федотов – Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2012.– 136 с.– ЭБС «IPRbooks» – Режим доступа: http://www.iprbookshop.ru/27280
8. Филиппов, М.В. Операционные системы [Электронный ресурс]: учебно-методическое пособие/ М.В. Филиппов, Д.В. Завьялов. - Волгоград: Волгоградский институт бизнеса, 2014. – 163 с. – ЭБС «IPRbooks» – Режим доступа: http://www.iprbookshop.ru/56020.html
9. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей[Электронный ресурс]: учебное пособие/ В.Ф. Шаньгин. – М.: ФОРУМ: ИНФРА-М, 2017. – 416 с. – ЭБС «Znanium.com» – Режим доступа: http://znanium.com/catalog.php?bookinfo=775200

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Безопасность операционных систем»

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Этапы формирования компетенции (номер семестра	**Наименование учебных дисциплин, формирующих компетенции в процессе освоения образовательной программы**

согласно учебному плану)	
ПК-9Способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	
3	Основы информационной безопасности
6	***Безопасность операционных систем***
9	Безопасность информационно-аналитических систем
6-8	Производственная (организационно-технологическая) практика
11	Преддипломная практика
11	Государственная итоговая аттестация

7.2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**	
ПК-9Способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах					
знать: основные средства и способы обеспечения информационной безопасности;требования к защищенным операционным системам;критерии оценки эффективности и надежности средств защиты операционных систем;принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows; защитные механизмы и средства обеспечения сетевой безопасности;критерии и методы оценивания механизмов защиты.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	контрольная работа, тесты, письменный опрос, доклады, зачет
уметь: оценивать эффективность защиты; выявлять слабости защиты операционных систем и использовать их для вскрытия защиты; планировать политику безопасности операционных систем; пользоваться средствами защиты, предоставляемыми операционными системами; применять средства антивирусной защиты и обнаружения вторжений; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; проводить анализ и оценивание механизмов защиты.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
владеть: навыками построения защиты в операционных системахWindows, Unix, работы в различных операционных средах; реализации сетевых протоколов с помощью программных средств; навыками настройки	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков	Успешное и систематическое применение навыков	

межсетевых экранов; методикой анализа сетевого трафика.			допускаются пробелы		

7.3. Типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Перечень докладов по теме «Понятие операционных систем»

1. Основные задачи и принципы администрирования ОС.
2. Создание домашней сети.
3. История создания и развития операционных систем.
4. Разновидности операционных систем.
5. Основные возможности современных операционных систем.
6. Основные производители операционных систем.
7. Основные механизмы функционирования ОС.
8. Установка операционных систем Linuxи Windowsна виртуальную машину.
9. Основные термины безопасности ОС.
10. Базовая настройка основных систем безопасности ОС.

Вопросы по теме «Теоретические основы защиты ОС»

1. Охарактеризуйте информацию и ее свойства.
2. Что является предметом и объектом защиты информации?
3. Чем определяется ценность информации? Приведите классификацию конфиденциальной информации.
4. Охарактеризуйте свойства достоверности и своевременности информации.
5. Дайте определения информационной безопасности АСОИ и политики информационной безопасности.
6. Что понимается под угрозой информации? Назовите разновидности угроз информации.
7. Приведите классификацию угроз информации.
8. Какие основные направления и методы реализации угроз вам известны?
9. Поясните классификацию злоумышленников.
10. Охарактеризуйте причины и виды утечки информации.
11. Назовите и приведите примеры каналов утечки информации.
12. Охарактеризуйте подходы к обеспечению компьютерной безопасности.
13. Перечислите основные и вспомогательные сервисы безопасности, дайте их классификацию.
14. Дайте характеристику групп требований к системе защиты.
15. Перечислите основные требования к защите конфиденциальной информации.
16. Перечислите основные требования к защите секретной информации.
17. Опишите основные различия требований и механизмов защиты от НСД для конфиденциальной и секретной информации.
18. Сформулируйте список функциональных дефектов с точки зрения защиты в используемой ОС.
19. Какие элементы безопасности содержит ОС Windows NT?
20. Назовите элементы безопасности ОС UNIX?
21. Охарактеризуйте элементы безопасности ОС Novell NetWare? Приведите определение понятий "протоколирование" и "аудит".
22. Назовите задачи, реализуемые протоколированием и аудитом.
23. Дайте характеристику задачи активного аудита.
24. Дайте характеристику сигнатурного метода активного аудита.
25. Охарактеризуйте функциональные компоненты активного аудита.

Перечень докладов по теме «Механизмы защиты в ОС Windows».

1. Основные функции и задачи администратора ОС.
2. Основные инструментальные средства применяемые для администрирования ОС.
3. Основные задачи по управлению учетными записями пользователей и их реализация.
4. Виды резервного копирования.
5. Основные этап сборки ядра Windows.
6. Методы дополнительной защиты ОС.
7. Инструменты администрирования пользователей в доменах Microsoft(графические утилиты, утилиты командной строки).
8. Группы безопасностей в сетях Microsoft. Типы групп безопасностей, их назначение. Встроенные группы безопасности, их назначение.
9. Инструменты администрирования группами безопасности (графические утилиты, утилиты командной строки, программный интерфейс).
10. Обеспечение информационной безопасности в сетях Microsoft: аутентификация, разграничение доступа, групповые политики. Инструменты анализа и управления безопасностью в сетях Microsoft.
11. Аутентификация в распределенных системах. Схема Kerberos, применение схемы Kerberosв доменах Windows.
12. Управление доступом к данным. Списки прав доступа к объектам операционной системы, управление доступом к файлам и каталогам (графические утилиты, утилиты командной строки).
13. Групповые политики, функции и назначения. Объекты групповой политики. Использование групповых политик для задач администрирования.
14. Создание и редактирование объектов групповой политики. Инструменты управления групповыми политиками.

Пример тестового задания по теме «Службы каталогов. Active Directory»

1. Укажите функцию, которая не выполняется службой каталогов?

a) централизация;
b) виртуализация;
c) масштабируемость.
d) стандартизация.

2. Сколько объектов поддерживается в одном домене каталога ActiveDirectory?

a) число не зависит от производительности сервера, хранящего учетные записи;
b) десять;
c) пятьдесят;
d) ограничен типом применяемого микропроцессора сервера.

3. Какой протокол позволяет обеспечивать механизм связи каталога Windows с другими каталогами на предприятии?

a) ARP;
b) MCYR;
c) LDAP;
d) TWES.

4. Укажите отсутствующее ключевое преимущество службы Active Directory Windows Server 2003:

a) единая регистрация;
b) децентрализованный каталог;
c) делегированное администрирование;
d) интегрированная безопасность.

5. Как называется единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows?

a) область;

b) раздел;
c) фрагмент;
d) домен.

6. В Active Directoryкаждый сервер всегда содержит не менее контекстов имен?

a) двух;
b) трех;
c) четырех;
d) пяти.

7. Как называется способ создания прямых доверительных отношений между двумя доменами, которые могут быть уже связаны цепочкой транзитивных доверий, но нуждаются в более оперативном реагировании на запросы друг от друга?

a) доверие к сокращению;
b) доверие к сфере;
c) доверие к лесу;
d) доверие к внешнему домену.

8. Как называется одно или несколько деревьев, которые не образуют непрерывного пространства имен?

a) сайт;
b) контейнер
c) ;домен;
d) лес.

9. Какие сегменты содержит раздел Active Directory, называемый контекстом именования?

a) раздел домена каталога;
b) раздел конфигурации каталога;
c) раздел дерева каталога;
d) раздел глобального каталога;
e) разделы удаленных каталогов.

10. Как называется область сети, где все контроллеры домена связаны быстрым, недорогим и надежным сетевым подключением?

a) сайт;
b) контейнер
c) ;домен;
d) лес.

Перечень докладов по теме «Администрирование операционных систем семействаWindows».

1. Основные функции и задачи администратора ОС.
2. Основные инструментальные средства, применяемые для администрирования ОС.
3. Основные задачи по управлению учетными записями пользователей и их реализация.
4. Виды резервного копирования.
5. Основные этап сборки ядра Windows.
6. Методы дополнительной защиты ОС.
7. Инструменты администрирования пользователей в доменах Microsoft(графические утилиты, утилиты командной строки).
8. Группы безопасностей в сетях Microsoft. Типы групп безопасностей, их назначение. Встроенные группы безопасности, их назначение.
9. Инструменты администрирования группами безопасности (графические утилиты, утилиты командной строки, программный интерфейс).
10. Обеспечение информационной безопасности в сетях Microsoft: аутентификация, разграничение доступа, групповые политики. Инструменты анализа и управления безопасностью в сетях Microsoft.
11. Аутентификация в распределенных системах. Схема Kerberos, применение схемы

Kerberosв доменах Windows.

12. Управление доступом к данным. Списки прав доступа к объектам операционной системы, управление доступом к файлам и каталогам (графические утилиты, утилиты командной строки).
13. Групповые политики, функции и назначения. Объекты групповой политики. Использование групповых политик для задач администрирования.
14. Создание и редактирование объектов групповой политики. Инструменты управления групповыми политиками.

Контрольная работа по теме «Механизмы защиты в ОС LINUX»
«Права доступа к файлам и управление ими в Linux».

Целью проведения контрольной работы является выявление уровня знаний по теме «права доступа к файлам и управление ими». Студенты выполняют задание, содержащее ряд вопросов, связанных с управлением правами доступа.

Пример контрольного задания.

1. Укажите объект операционной системы Linux, в котором хранится информация о правах доступа к файлу.
2. Укажите команду и необходимые ключи для получения сведений о правах доступа к файлу в операционной системе Linux.
3. Опишите правила назначения прав доступа к файлам и каталогам в UNIX-подобных ОС.
4. Что означает право на чтение применительно к каталогу в UNIX-подобных ОС.
5. Что означает право на выполнение применительно к каталогу в UNIX-подобных ОС.
6. Пользователь **kurs3**, для которого первичной группой является группа **kurs3**, создал файл **test_3_kurs.** Укажите, как должны быть заданы права доступа к файлу **test_3_kurs,** если читать содержимое файла могут только участники группы **kurs3,** вносить изменения в файл может только его создатель, а все остальные пользователи системы не имеют никаких прав в отношении файла **test_3_kurs.**
7. Укажите команду, с помощью которой пользователь **kurs3** сможет передать права владельца в отношении файла **test_3_kurs** пользователю **laborant**.
8. Укажите, как записать команды, реализующие два действия:

а) добавить право на изменение файла **test_3_kurs** всем членам группы **kurs3**;

б) установить право на изменение файла **test_3_kurs** всем членам группы **kurs3.**

Есть ли разница в результатах выполнения этих команд.

Первые 6 вопросов оцениваются 1 баллом, вопросы 7 и 8 оцениваются двумя баллами каждый. Итоговая отметка за контрольную работу рассчитывается в соответствии с представленной ниже шкалой.

Шкала итоговых отметок за контрольную работу

№ п/п	Сумма баллов	Отметка
1	10	Отлично
2	7-9	Хорошо
3	4-6	Удовлетворительно
4	Менее 4	Неудовлетворительно

Контрольные вопросы и задания для проведения текущего контроля

1. Понятие операционной системы.
2. Основные принципы построения операционной системы.
3. Классификация операционных систем.
4. Пользовательский интерфейс.

5. Пакетную технологию как интерфейс.
6. Интерфейс командной строки.
7. Графический интерфейс.
8. Речевая технология как интерфейс.
9. Семантический интерфейс.
10. Многопользовательские операционные системы.
11. Многозадачные операционные системы.
12. Операционные системы реального времени.
13. Операционные системы с разделением времени.
14. Понятие процесса.
15. Потоковая обработка.
16. Прерывания.
17. Понятие ресурса.
18. Организация управления в операционной системе.
19. Организация памяти.
20. Дать определение и характеристику основных режимов работы, дисциплин и режимов обслуживания заявок в вычислительных системах.
21. Перечислить дисциплины обслуживания.
22. Перечислить режимы обслуживания.
23. Пояснить понятия "нить" и "процесс".
24. Охарактеризовать алгоритмы выбора очередности обработки.

Примерный вариант тестового задания для проведения текущей аттестации

1. Выберите из предложенного списка, что может являться критерием эффективности вычислительной системы (выберите несколько вариантов ответа):

1. пропускная способность
2. занятость оперативной памяти
3. загруженность центрального процессора
4. реактивность системы.

2. В каких системах гарантируется выполнение задания за определенный промежуток времени:

1. пакетной обработки
2. разделения времени
3. системах реального времени

3. В каком из алгоритмов планирования решение о переключении процессора на выполнение другого процесса принимает операционная система:

1. вытесняющий
2. невытесняющий

4. Процессорное время распределяется между:

1. процессами
2. задачами
3. потоками

5. Hardware Interrupt – это:

1. отказ в работоспособности аппаратной части компьютера
2. аппаратное прерывание
3. программа перезагрузки операционной системы
4. программный способ очистки ядра процессора

6. Для согласованного управления работой всех устройств и программ компьютера используется ...

1. менеджер файлов

2. библиотека подпрограмм
3. программа-резидент
4. операционная система

7. Укажите главное отличие многопользовательских систем от однопользовательских:

1. поддержка смены сеанса работы одного пользователя на сеанс работы другого пользователя без завершения сеанса первого пользователя
2. решение о переключении процессора с одного процесса на другой принимается операционной системой, а не самим активным процессом
3. поддержка одновременного исполнения (в режиме квантования времени) задач, запущенных разными пользователями
4. наличие средств защиты информации каждого пользователя от несанкционированного доступа других пользователей

8. Выберите верное высказывание.

1. **во многих операционных системах алгоритмы планирования построены с использованием как концепции квантования, так и приоритетов**
2. концепция квантования и концепция приоритетов не могут одновременно использоваться для построения алгоритмов планирования
3. концепция квантования и концепция приоритетов не имеют отношения к вопросу планирования процессов
4. нет правильного ответа

9. Стандарт пользовательского интерфейса – это

1. унифицированные действия пользователя;
2. единые правила взаимодействия пользователя с любыми приложениями;
3. единые правила обработки данных в разных приложениях;
4. навигация по приложению;
5. реализация технологии OLE

10. Минимальной адресуемой ячейкой оперативной памяти является …

1. файл
2. сектор
3. программа
4. байт

Перечень вопросов к зачету по дисциплине «Безопасность операционных систем»

1. Понятие операционных систем.
2. Понятие ОС. Архитектура современных ОС.
3. Общая характеристика операционных систем; назначение и возможности систем клона UNIX, систем группы Windows.
4. Виды пользовательских интерфейсов.
5. Управление ресурсами.
6. Управление процессорами.
7. Управление памятью, управление устройствами.
8. Основные механизмы функционирования ОС.
9. Взаимодействие ОС с программами и отладчиками.
10. Управление процессами: состояния процессов, синхронизация процессов, обмен сообщениями.
11. Стратегии и дисциплины планирования, наследование ресурсов, тупиковые ситуации.
12. Основные понятия безопасности ОС.

13. Классификация методов несанкционированного доступа.
14. Обработка исключений, сохранение и восстановление процессов.
15. Организация управления доступом и защиты ресурсов ОС.
16. Основные механизмы безопасности.
17. Обзор методов несанкционированного доступа.
18. Разграничение доступа в ОС.
19. Дискреционное разделение доступа.
20. Мандантная политика.
21. Матрицы доступа.
22. Средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита.
23. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения, генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС.
24. Основные принципы ОС на базе ядра Linux. Планирование развертывания ОС на базе ядра Linux. Классические механизмы защиты.
25. Пользователи и группы в Linux. Разделение доступа.
26. Понятие ID. Классическая схема разделения доступа. Понятие владельца. Наследование полномочий.
27. Системы мандатной защиты.
28. SELInux. Основные термины и определения,
29. SELinux. Правила построения политики.
30. Принципы совмещения классической системы разделения доступа с мандатной защитой. Ограничения SELinux. Аналоги SELinux.
31. Механизмы изоляции исполняемого кода в Linux. Виртуализация. Контейнеры. Зоны.
32. Изоляция кода на уровне пользователя.
33. Изоляция кода на уровне ядра.
34. Механизмы защиты данных в Linux.
35. Понятие шифрования данных. Шифрования уровня отдельных файлов. Шифрование на уровне файловой системы.
36. Сертификаты и ключи. Резервное копирование. Снимки файловых систем. Журналирование.
37. Сетевые экраны. IPTables. Протоколы удаленного доступа. Принципы фильтрации сетевых пакетов.
38. Планирование развертывания ОС Windows.
39. Эволюция технологий разграничения доступа в ОС Windows.
40. Пользователи и группы в Windows. Разделение доступа.
41. Понятие SID, RID. Алгоритм генерации SID. Делегирование полномочий.
42. Брандмауэр Windows. Защита ОС в сети. SMB. Net Bios. Контроль подключений к ОС. Технологии удаленного доступа к ОС Windows. Типы сетей.
43. Основные принципы Active Directory. Домен. Лес. Интеграция Active Directory с DNS. Политики безопасности. Контроллеры домена. Роли мастера операций. Парольные политики. Делегирование полномочий. Наследование полномочий. Уровни доверия.
44. Службы каталогов. Терминология, назначения и роль в структуре безопасности.

Пример зачетного задания
для проведения промежуточной аттестации
по дисциплине «Безопасность операционных систем»

1. Какие интерфейсы поддерживают ОС семейства UNIX?

1. интерфейс системных вызовов, интерфейс библиотечных функций, интерфейс пользователя
2. интерфейс прикладного программирования (API), интерфейс командной строки, графический пользовательский интерфейс
3. интерфейс аппаратных абстракций, интерфейс библиотечных функций, пользовательский интерфейс
4. интерфейс аппаратных абстракций, интерфейс прикладного программирования (API), пользовательский интерфейс

2. Как реализованы небольшие каталоги в файловой системе NTFS?

1. небольшой каталог реализуется в виде записи в главной файловой таблице с атрибутом Index Allocation, который содержит список файлов, входящих в каталог, организованный в виде бинарного дерева
2. небольшой каталог реализуется в виде записи в главной файловой таблице с атрибутом Index Allocation, который содержит список файлов, входящих в каталог; каждый элемент списка содержит все атрибуты файла
3. небольшой каталог реализуется в виде записи в главной файловой таблице с атрибутом Index Root, который содержит список указателей на начальные записи файлов, входящих в каталог
4. небольшой каталог реализуется в виде записи в главной файловой таблице с атрибутом Index Root, который содержит список файлов, входящих в каталог; каждый элемент списка состоит из имени файла и номера записи MFT, содержащего начальную запись файла

3. Что является основным методом выявления вторжений?

1. ведение аудита
2. антивирусное программное обеспечение
3. пороговое обнаружение
4. профильное обнаружение

4. Выберите правильное определение контроллера домена:

1. контроллер домена – это компьютер в составе домена, на котором хранится Глобальный каталог
2. контроллер домена – это компьютер в составе домена, отвечающий за функционирование службы имен доменов (DNS)
3. контроллер домена – это компьютер в составе домена, отвечающий за репликацию данных в каталоге
4. контроллер домена – это компьютер в составе домена, отвечающий за аутентификацию пользователей и содержащий полную копию базы данных Active Directory этого домена

5. Выберите правильное определение службы каталогов:

1. служба каталогов – это средство именования, хранения и выборки информации в распределенной среде, доступное клиентам этой среды
2. служба каталогов – это часть операционной системы, управляющая организацией файлов в каталоги
3. служба каталогов – это логическая группировка объединенных в сеть компьютеров
4. служба каталогов – это средство хранения учетных записей пользователей в сети

6. Выберите принципиальное различие между клиентом и сервером в сети:

1. инициатором выполнения работы сетевой службой всегда выступает сервер, а клиент всегда находится в режиме пассивного ожидания для формирования запросов
2. инициатором выполнения работы сетевой службой всегда выступает клиент, а сервер всегда находится в режиме пассивного ожидания запросов

3. инициатором выполнения работы сетевой службой всегда выступает клиент, а сервер всегда находится в режиме активного ожидания запросов
4. нет правильного ответа

7. На каком уровне модели OSI работают протоколы TCP и UDP?

1. на прикладном
2. TCPна представительном, aUDPна канальном
3. TCP на транспортном, а UDP на сеансовом
4. на транспортном

8. Выберите верное утверждение, касающееся DLL-библиотек, из приведенных ниже:

1. функции DLL-библиотек выполняются только в привилегированном режиме
2. DLL-библиотека загружается в адресное пространство использующего её процесса, поэтому в оперативной памяти присутствует столько её экземпляров сколько процессов её загрузило
3. все создаваемые DLL-библиотекой окна и открываемые файлы принадлежат самой библиотеке, а не использующему её процессу
4. память, запрашиваемая DLL-библиотекой, выделяется в адресном пространстве процесса

9. Что такое список управления доступом (в ОС Windows)?

1. специальный файл операционной системы, хранящий пароли пользователей системы
2. структура данных, содержащая список прав на выполнение операций пользователей и групп пользователей над данным файловым объектом и хранящаяся вместе с ним
3. структура данных, находящаяся на пересечении строки и столбца матрицы, хранящейся в базе данных операционной системы, в которой столбцы соответствуют всем файловым объектам, а строки – всем пользователям системы, и содержащая перечень разрешенных операций
4. структура данных, содержащая список прав на выполнение операций пользователей и групп пользователей над данным файловым объектом и хранящаяся в специальной базе данных ОС

10. Выберите верное высказывание.

1. поток может содержать несколько процессов
2. поток и процесс являются равноправными единицами работы
3. процесс может содержать несколько потоков
4. поток является разновидностью процесса, запускаемого другим процессом в качестве дочернего

11. Укажите главное отличие многопользовательских систем от однопользовательских:

1. поддержка смены сеанса работы одного пользователя на сеанс работы другого пользователя без завершения сеанса первого пользователя
2. решение о переключении процессора с одного процесса на другой принимается операционной системой, а не самим активным процессом
3. поддержка одновременного исполнения (в режиме квантования времени) задач, запущенных разными пользователями
4. наличие средств защиты информации каждого пользователя от несанкционированного доступа других пользователей

12. Что такое невытесняющая многозадачность?

1. активный процесс выполняется до тех пор, пока он сам, по собственной инициативе, не отдаст управление операционной системе для того, чтобы та выбрала из очереди другой готовый к выполнению процесс
2. решение о переключении процессора с одного процесса на другой принимается операционной системой, а не самим активным процессом

3. нет правильного ответа
4. выполнение процесса с использованием сразу нескольких процессоров

13. Выберите ответ, в котором наиболее полно отражены функции операционной системы:

1. загрузка в оперативную память программ, выполнение запросов программ на операции ввода-вывода
2. организация упрощенного доступа пользователя к ресурсам вычислительной системы, выполнение программ
3. загрузка в оперативную память программ, распределение ресурсов между программами, прием и исполнение запросов от выполняющихся программ, организация упрощенного доступа пользователя к ресурсам вычислительной системы

14. Для согласованного управления работой всех устройств и программ компьютера используется ...

1. менеджер файлов
2. библиотека подпрограмм
3. программа-резидент
4. операционная система

15. Минимальной адресуемой ячейкой оперативной памяти является …

1. файл
2. сектор
3. программа
4. байт

16. Память компьютера с минимальным временем доступа – это …

1. жесткий диск
2. лазерный диск
3. оперативная память (ОЗУ)
4. кэш-память

17. Состояние процесса, когда он ожидает завершения некоторого события?

1. готовый
2. завершенный
3. ожидающий

18. Какая файловая система из перечисленных ниже является журналируемой:

1. FAT-16
2. FAT-32
3. NTFS
4. Ext2

19. Минимальный фактический размер файла на диске равен:

1. 1 биту
2. 1 байту
3. 1 сектору
4. 1 кластеру

20. Файловая система является частью:

1. дисковых систем
2. драйверов дисков
3. операционной системы

21. Каких классов прерываний нет?

1. аппаратных
2. асинхронных
3. внутренних
4. программных

22. В Linux для переключения консолей используется следующее сочетаний клавиш:

1. Ctrl+Alt+Delete
2. Ctrl+N , где N - цифра от 0 до 9
3. Alt+FN, где N - цифра от 0 до 9.

23. От выбора типа файловой системы будет зависеть (выберите несколько вариантов ответа):

1. вид графической оболочки ОС,
2. правильность работы ПК,
3. правильность установки ОС,
4. скорость работы ПК.

24. ОС Linux принадлежит к семейству:

1. Unix - подобных операционных систем,
2. Windows - подобных операционных систем,
3. MacOS- подобных операционных систем,
4. OS/2 - подобных операционных систем.

25. Входит ли имя каталога, в котором находится файл, в полное имя файла на диске?

1. не входит.
2. входит.
3. это зависит от того, является ли данный каталог рабочим.

26. Приложение выгружается из оперативной памяти и прекращает свою работу, если:

1. запустить другое приложение
2. свернуть окно приложения
3. закрыть окно приложения
4. переключиться в другое окно

Тестовые задания для контроля остаточных знаний
По дисциплине «Безопасность операционных систем»

1. В каких системах гарантируется выполнение задания за определенный промежуток времени:

1. пакетной обработки
2. разделения времени
3. реального времени

2. В каком из алгоритмов планирования решение о переключении процессора на выполнение другого процесса принимает операционная система:

1. вытесняющий
2. невытесняющий

3. Hardware Interrupt – это:

1. отказ в работоспособности аппаратной части компьютера
2. аппаратное прерывание
3. программа перезагрузки операционной системы
4. программный способ очистки ядра процессора

4. Для согласованного управления работой всех устройств и программ компьютера используется ...

1. менеджер файлов
2. библиотека подпрограмм
3. программа-резидент
4. операционная система

5. Стандарт пользовательского интерфейса – это

1. унифицированные действия пользователя
2. единые правила взаимодействия пользователя с любыми приложениями

3. единые правила обработки данных в разных приложениях
4. навигация по приложению
5. реализация технологии OLE

6. Каких классов прерываний нет?

1. аппаратных
2. асинхронных
3. внутренних
4. программных

7. Кэш-память используется для …

1. хранения файлов
2. хранения программы начальной загрузки
3. хранения часто используемых команд и данных
4. копирования дисков

8 Правила разграничения доступа не должны позволять:

1. присутствия ничейных объектов в системе
2. присутствия объектов, недоступных для администраторов системы
3. присутствия всем доступных объектов

9. Многопользовательские операционные системы используют

1. сетевой режим работы
2. только пакетный режим работы
3. режим разделения времени
4. режим работы в реальном времени

10. Выберите правильное определение службы каталогов:

1. служба каталогов – это средство именования, хранения и выборки информации в распределенной среде, доступное клиентам этой среды
2. служба каталогов – это часть операционной системы, управляющая организацией файлов в каталоги
3. служба каталогов – это логическая группировка объединенных в сеть компьютеров
4. служба каталогов – это средство хранения учетных записей пользователей в сети

11. Укажите главное отличие многопользовательских систем от однопользовательских:

1. поддержка смены сеанса работы одного пользователя на сеанс работы другого пользователя без завершения сеанса первого пользователя
2. решение о переключении процессора с одного процесса на другой принимается операционной системой, а не самим активным процессом
3. поддержка одновременного исполнения (в режиме квантования времени) задач, запущенных разными пользователями
4. наличие средств защиты информации каждого пользователя от несанкционированного доступа других пользователей

12. Какая файловая система из перечисленных ниже является журналируемой:

1. FAT-16
2. FAT-32
3. NTFS
4. Ext2

Ключи к тестовому заданию

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
3	1	2	4	2	2	3	2	3	1	4	3

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений и навыков, и опыта деятельности, характеризующих этапы формирования компетенций

Требования к контрольной работе

Контрольная работа – средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.

Контрольная работа представляет собой один из видов самостоятельной работы обучающихся. По сути – это изложение ответов на определенные теоретические вопросы по учебной дисциплине, а также решение практических задач. Контрольные проводятся для того, чтобы развить у обучающихся способности к анализу научной и учебной литературы, умение обобщать, систематизировать и оценивать практический и научный материал, укреплять навыки овладения понятиями определенной науки и т.д.

При оценке контрольной работы преподаватель руководствуется следующими критериями:

- работа была выполнена автором самостоятельно;
- обучающийся подобрал достаточный список литературы, который необходим для осмысления темы контрольной работы;
- автор сумел составить логически обоснованный план, который соответствует поставленным задачам и сформулированной цели;
- обучающийся проанализировал материал;
- обучающийся сумел обосновать свою точку зрения;
- контрольная работа оформлена в соответствие с требованиями;
- автор защитил контрольную работу и успешно ответил на все вопросы преподавателя.

Контрольная работа, выполненная небрежно, без соблюдения правил, предъявляемых к ее оформлению, возвращается без проверки с указанием причин. В этом случае контрольная работа выполняется повторно.

Вариант контрольной работы выдается в соответствии с порядковым номером в списке студентов.

Критерии оценки знаний при написании контрольной работы

Оценка «отлично» выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания вопросов контрольной работы и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка «удовлетворительно» выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными понятиями выносимых на контрольную работу тем, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает большей части основного содержания выносимых на контрольную работу вопросов тем дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания.

Требования к проведению письменных блиц-опросов

Письменные блиц-опросы позволяют проверить уровень подготовки к практическому занятию всех обучающихся в группе, при этом оставляя достаточно учебного времени для иных форм педагогической деятельности в рамках данного занятия. Письменный блиц-опрос проводится без предупреждения, что стимулирует обучающихся к систематической подготовке к занятиям. Вопросы для опроса готовятся заранее, формулируются узко, дабы обучающийся имел объективную возможность полноценно его осветить за отведенное время

Письменные опросы целесообразно применять в целях проверки усвояемости значительного объема учебного материала, например, во время проведения зачета (экзамена), когда необходимо проверить знания студентов по всему курсу.

При оценке опросов анализу подлежит точность формулировок, связность изложения материала, обоснованность суждений.

Критерии оценивания результатов письменного блиц-опроса

Каждому студенту выдается свой собственный, узко сформулированный вопрос. Ответ должен быть четким и кратким, содержащим все основные характеристики описываемого понятия, института, категории.

«Отлично» – вопрос раскрыт полностью, точно обозначены основные понятия и характеристики по теме.

«Хорошо» – вопрос раскрыт, однако нет полного описания всех необходимых элементов.

«Удовлетворительно» – вопрос раскрыт не полно, присутствуют грубые ошибки, однако есть некоторое понимание раскрываемых понятий.

«Неудовлетворительно» – ответ на вопрос отсутствует или в целом не верен.

Требования к написанию доклада

Доклад – продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Критерии оценивания доклада:

Оценка «отлично» выполнены все требования к написанию и защите доклада: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо» – основные требования к докладу и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, не выдержан объём доклада, имеются упущения в оформлении, не допускает существенных неточностей в ответе на дополнительный вопрос.

Оценка «удовлетворительно» – имеются существенные отступления от требований к докладу. В частности, тема освещена лишь частично, допущены фактические ошибки в содержании доклада или при ответе на дополнительные вопросы, во время защиты отсутствует вывод.

Оценка «неудовлетворительно» – тема доклада не раскрыта, обнаруживается существенное непонимание проблемы.

Требования к выполнению тестового задания

Тестирование является одним из основных средств формального контроля качества обучения. Это метод, основанный на стандартизированных заданиях, которые позволяют измерить психофизиологические и личностные характеристики, а также знания, умения и навыки испытуемого.

Основные принципы тестирования, следующие:

− связь с целями обучения – цели тестирования должны отвечать критериям социальной полезности и значимости, научной корректности и общественной поддержки;

− объективность – использование в педагогических измерениях этого принципа призвано не допустить субъективизма и предвзятости в процессе этих измерений;

− справедливость и гласность – одинаково доброжелательное отношение ко всем обучающимся, открытость всех этапов процесса измерений, своевременность ознакомления обучающихся с результатами измерений;

− систематичность – систематичность тестирований и самопроверок каждого учебного модуля, раздела и каждой темы; важным аспектом данного принципа является требование репрезентативного представления содержания учебного курса в содержании теста;

– гуманность и этичность – тестовые задания и процедура тестирования должны исключать нанесение какого-либо вреда обучающимся, не допускать ущемления их по национальному, этническому, материальному, расовому, территориальному, культурному и другим признакам;

Важнейшим является принцип, в соответствии с которым тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

− закрытая форма – является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Например, обучающемуся задается вопрос, требующий альтернативного ответа «да» или «нет», «является» или «не является», «относится» или «не относится» и т.п. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя один или несколько правильных ответов и иногда называется выборочным заданием. Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде. Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

− открытая форма – вопрос в открытой форме представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие – части слова или буквы, условные обозначения, линии или изображения элементов схемы и графика. Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

− установление соответствия – в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

− установление последовательности – предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

Критерии оценки знаний при проведении тестирования

Оценка «Отлично» выставляется при условии правильных ответов не менее, чем на 85% тестовых заданий;

Оценка «Хорошо» выставляется при условии правильных ответов не менее, чем на 70% тестовых заданий;

Оценка «Удовлетворительно» выставляется при условии правильных ответов не менее, чем на 50% тестовых заданий;

Оценка «Неудовлетворительно» выставляется при условии правильных ответов менее, чем на 50% тестовых заданий.

Требования к проведению текущей аттестации

Текущий контроль по дисциплине «Безопасность операционных систем» проводится в форме контрольного среза по оцениванию фактических результатов освоения материала пройденных тем дисциплины, и осуществляется ведущим преподавателем.

Текущая аттестация проводится в форме теста.

Оценивание достижений обучающегося проводится по итогам контрольного среза за текущий период с выставлением оценок в ведомости. Прохождение процедуры текущего контроля является обязательным для обучающихся по очной форме обучения. Условием допуска к промежуточной аттестации по дисциплине обучающихся по очной форме является успешное прохождение процедуры текущего контроля (оценка не ниже, чем «удовлетворительно»).

Критерии оценки знаний при проведении текущей аттестации

Оценка «Отлично» выставляется при условии правильных ответов не менее, чем на 85% тестовых заданий;

Оценка «Хорошо» выставляется при условии правильных ответов не менее, чем на 70% тестовых заданий;

Оценка «Удовлетворительно» выставляется при условии правильных ответов не менее, чем на 50% тестовых заданий;

Оценка «Неудовлетворительно» выставляется при условии правильных ответов менее, чем на 50% тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации.

Критерии оценки знаний на зачете

Промежуточная аттестация по дисциплине «Безопасность операционных систем» проводится в соответствии с учебным планом в 6-м семестре в виде зачета в соответствии с графиком проведения зачетов.

Обучающиеся допускаются к зачету по дисциплине в случае выполнения всех заданий и мероприятий, предусмотренных программой дисциплины (для обучающихся по очной форме – успешного прохождения текущего контроля).

Зачетное задание представляет собой тест в электронном виде или с использованием специальных бланков. Каждый вопрос предполагает только один правильный ответ. При указании студентом двух и более ответов на один вопрос ответ считается неверным.

Тестовые задания для зачета утверждаются на заседании кафедры и подписываются заведующим кафедрой.

При оценке знаний обучающегося на зачете преподаватель может принимать во внимание его учебные достижения в семестровый период, результаты текущего контроля знаний. Экзаменатор может выставить оценку без тестирования тем студентам, которые досрочно выполнили все лабораторные работы и самостоятельные задания к ним.

Оценка знаний в соответствии с установленными критериями реализуется следующим образом:

Оценка «Зачтено» выставляется при условии правильных ответов не менее, чем на 50% тестовых заданий;

Оценка «Не зачтено» выставляется при условии правильных ответов менее, чем на 50% тестовых заданий.

8.Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

1. Васильков, А. В. Безопасность и управление доступом в информационных системах [Электронный ресурс]: учебное пособие / А.В. Васильков, И.А. Васильков. — М.:

ФОРУМ: ИНФРА-М, 2017. – 368 с. ЭБС «Znanium.com» – Режим доступа: http://znanium.com/catalog.php?bookinfo=537054
2. Власов, Ю.В. Администрирование сетей на платформе MS WindowsServer [Электронный ресурс]/ Ю.В. Власов, Рицкова Т.И. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 622 с. – ЭБС «IPRbooks» — Режим доступа: http://www.iprbookshop.ru/52219
3. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]: учебное пособие / Е.В. Глинская, Н.В. Чичварин. – М.: ИНФРА-М, 2018. – 118 с. – ЭБС «Znanium.com» – Режим доступа:http://znanium.com/catalog.php?bookinfo=925825
4. Гончарук, С.В. Администрирование ОС Linux [Электронный ресурс]/ С.В. Гончарук– М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 164 с. – ЭБС «IPRbooks» – Режим доступа: http://www.iprbookshop.ru/52142
5. Назаров, С.В. Современные операционные системы [Электронный ресурс]: учебное пособие/ С.В. Назаров, А.И. Широков. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 351 с. – ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/52176.html.
6. Филиппов, М.В. Операционные системы [Электронный ресурс]: учебно-методическое пособие/ М.В. Филиппов, Д.В. Завьялов. - Волгоград: Волгоградский институт бизнеса, 2014. – 163 с. – ЭБС «IPRbooks» – Режим доступа: http://www.iprbookshop.ru/56020.html
7. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. – М.: ФОРУМ: ИНФРА-М, 2017. – 416 с. – ЭБС «Znanium.com» – Режим доступа: http://znanium.com/catalog.php?bookinfo=775200

8.2. Дополнительная литература

1. Чефранов, С.Г. Идентификация и управление сложными объектами: математические модели, информационные технологии и комплексы программ [Электронный ресурс]: учебное пособие / Чефранов С.Г., Сапиев А.З.; – Майкоп: МГТУ, 2015. – 123 с. – Режим доступа: http://lib.mkgtu.ru:8002/libdata.php?id=2100023696
2. Култыгин, О.П. Администрирование баз данных. СУБД MS SQL Server [Электронный ресурс]: учебное пособие/ О.П. Култыгин– М.: Московский финансово-промышленный университет «Синергия», 2012. – 232 с. – ЭБС «IPRbooks» – Режим доступа: http://www.iprbookshop.ru/17009
3. Федотов, Е.А. Администрирование программных и информационных систем [Электронный ресурс]: учебное пособие/ Е.А.Федотов– Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2012. – 136 с. – ЭБС «IPRbooks» – Режим доступа: http://www.iprbookshop.ru/27280

8.3.Информационно-телекоммуникационные ресурсы сети «Интернет»

- Образовательный портал ФГБОУ ВО «МГТУ» [Электронный ресурс]: Режим доступа: https://mkgtu.ru/
- Информационно-правовой портал «Гарант» [Электронный ресурс]: Режим доступа: http://www.garant.ru/
- Научная электронная библиотека www.eLIBRARY.RU – Режим доступа: http://elibrary.ru/
- Электронный каталог библиотеки – Режим доступа: //http://lib.mkgtu.ru:8004/catalog/fol2;
- Единое окно доступа к образовательным ресурсам: Режим доступа: http://window.edu.ru/
- Сетевые компьютерные практикумы: Режим доступа:http://webpractice.cm.ru

- Единая коллекция цифровых образовательных ресурсов: Режим доступа:http://scool-collection.edu
- Федеральный портал «Российское образование»:Режимдоступа:http://edu.ru
- Портал с материалами по изучению информационных технологий:Режим доступа: www.ict.edu.ru.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Комплексное изучение предлагаемой студентам учебной дисциплины «Безопасность операционных систем» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе выполнения лабораторных работ, а также систематическое выполнение заданий для самостоятельной работы студентов. Основными видами занятий при изучении дисциплины являются лекции, лабораторные работы и самостоятельная работа. Изучение дисциплины «Безопасность операционных систем» осуществляется в учебных аудиториях, компьютерных классах согласно расписанию занятий, а также в свободное от плановых занятий время на факультете или дома.

Раздел / Тема с указанием основных учебных элементов	**Формируемые компетенции**	**Методы обучения**	**Способы (формы) обучения**	**Средства обучения**
Понятие операционных систем. Основные механизмы функционирования операционных систем.	ПК-9	Работа с рекомендованной литературой, работа с электронными ресурсами, метод лабораторных работ.	Индивидуальная работа, самостоятельная работа.	Конспект лекций, информация электронных источников, учебники и учебные пособия; методические разработки (рекомендации) по предмету, технические средства доступа к электронным ресурсам.
Теоретические основы защиты операционных систем. Обзор методов несанкционированного доступа к операционной системе.	ПК-9	Ознакомление с нормативными документами, работа с рекомендованной литературой, работа с электронными ресурсами.	Индивидуальная работа, самостоятельная работа.	Нормативные документы, Конспект лекций, информация электронных источников, учебники и учебные пособия; методические разработки (рекомендации) по предмету, технические средства доступа к электронным ресурсам.
Основные механизмы защиты в ОС Windows.	ПК-9	Работа с рекомендованной литературой, работа с электронными ресурсами, метод лабораторных работ.	Индивидуальная работа, самостоятельная работа.	Конспект лекций, информация электронных источников, учебники и учебные пособия; методические разработки (рекомендации) по предмету, технические средства доступа к электронным ресурсам.
Администрирование сетей передачи данных. Защита операционной системы в сети. Службы каталогов. ActiveDirectory.	ПК-9	Работа с рекомендованной литературой, работа с электронными ресурсами, метод	Индивидуальная работа, самостоятельная работа.	Конспект лекций, информация электронных источников, учебники и учебные пособия; методические разработки (рекомендации) по

		лабораторных работ.		предмету, технические средства доступа к электронным ресурсам.
Основные механизмы защиты в ОС Linux. Системы мандатной защиты. SELinux. Защита операционной системы в сети.	ПК-9	Работа с рекомендованной литературой, работа с электронными ресурсами, метод лабораторных работ.	Индивидуальная работа, самостоятельная работа.	Конспект лекций, информация электронных источников, учебники и учебные пособия; методические разработки (рекомендации) по предмету, технические средства доступа к электронным ресурсам.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям и контрольным мероприятиям. Лекции проводятся в лекционных аудиториях по расписанию занятий для нескольких академических групп, объединенных в лекционный поток.

На лекции студент должен вести конспект, который в сочетании с рекомендованной литературой используется для подготовки к лабораторным занятиям, контрольным работам, экзаменам и зачетам.

На первом лабораторном занятии студенты получают инструктаж по технике безопасности при работе в классе и знакомятся с особенностями работы на конкретной вычислительной машине.

Индивидуальные задания и методические указания к выполнению каждой последующей работы студент получает, как правило, на предыдущем занятии. Подготовка к выполнению лабораторных работ осуществляется в часы самостоятельной работы. Студенты, не подготовившиеся к занятиям, к работе на компьютере не допускаются. Для подготовки к лабораторным занятиям нужно изучить предлагаемую литературу и ответить на контрольные вопросы.

По каждой выполненной лабораторной работе студент оформляет отчет по установленной форме.

Описание работ и методические указания к ним содержатся в учебно-методических пособиях. Работы выполняются в той последовательности, в которой они изложены в пособиях, т.к. выполнение каждой следующей работы требует освоения материала предыдущей. Каждая работа выполняется в соответствии с заданиями, содержащимися в ней, отчетом о выполнении лабораторной работы являются файлы, созданные в процессе работы и сохраненные на диске. Защита лабораторной работы представляет собой выполнение самостоятельного задания и ответы на вопросы. Самостоятельное задание представляет собой реализацию творческого проекта по конкретной теме. Перед выполнением работы необходимо изучить теоретическую часть, содержащуюся в описании работы и соответствующие разделы учебной литературы, затем ответить на контрольные вопросы.

Каждому студенту во время лабораторной работы предоставляется полная возможность быть индивидуальным пользователем компьютера, самостоятельно отрабатывать учебные вопросы и выполнять индивидуальные учебные задания преподавателя.

Основными видами самостоятельной работы студентов являются составление плана-конспекта, выполнение самостоятельных заданий, подготовка к лабораторным работам, подготовка к экзамену.

Самостоятельная работа студентов при изучении курса «Безопасность операционных систем» предполагает, в первую очередь, работу с основной и дополнительной литературой.

В силу особенностей индивидуального режима подготовки каждого студента, представляется, что планирование должно осуществляться студентом самостоятельно, с учетом индивидуальных рекомендаций и советов преподавателей дисциплины в соответствии с вопросами и обращениями студентов при встречающихся сложностях в подготовке и освоении

Самостоятельную работу по изучению дисциплины целесообразно начинать с изучения рабочей программы, которая содержит основные требования к знаниям, умениям, навыкам обучающихся, ознакомления с разделами и темами.

Получив представление об основном содержании раздела, темы, необходимо изучить данную тему, представленную в учебнике, придерживаясь рекомендаций преподавателя, данных в ходе установочных занятий по методике работы над учебным материалом.

Рекомендуется дополнить конспект лекций по результатам работы с источниками.

При изучении курса нужно иметь в виду, что список рекомендуемой литературы не исчерпывает все имеющиеся сегодня пособия по дисциплине. Поэтому допускается использование любой доступной литературы, в которой освещены вопросы, содержащиеся в программе курса.

В ходе самостоятельной работы рекомендуется дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

Записи имеют первостепенное значение для самостоятельной работы студентов. Они помогают понять построение изучаемого материала, выделить основные положения, проследить их логику.

Ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память. Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд подсобных материалов для быстрого повторения прочитанного, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе.

При самостоятельной подготовке к лабораторным занятиям необходимо вдумчиво прочитать описание работы, после прочтения следует продумать содержание, определить последовательность и порядок выполнения заданий. Затем изучить соответствующие разделы основной и дополнительной литературы и ответить на контрольные вопросы. Кроме того, для более качественной подготовки к занятию нужно ответить на дополнительные вопросы для самостоятельной подготовки.

Самостоятельная работа также включает в себя подготовку к контрольным мероприятиям. Контрольные работы могут проводиться, как правило, по основным темам на любом виде занятий. О проведении контрольной работы и ее содержании студенты оповещаются заранее. Текущая аттестация и зачет проводятся в виде тестов.

Решение ситуационных задач осуществляется с целью проверки уровня навыков (владений) студента по решению практической ситуационной задачи.

В первую очередь следует внимательно ознакомиться с условиями задачи, затем необходимо определить основные вопросы задачи. Определив основные вопросы, студентам следует обозначить пути решения вопросов и приступить к решению задачи. В процессе решения задачи следует использовать конспекты лекций и специальную литературу. Решение задачи представляется на проверку в письменном (электронном) виде.

При оценке решения задач анализируется понимание студентом конкретной ситуации, способность обоснования выбранной точки зрения, глубина проработки материала.

Для студентов, обучающихся по заочной форме обучения, самостоятельная работа является основным видом работы по изучению дисциплины. Она включает

- изучение лекционного материала;

– работу с рекомендованной литературой и дополнительными источниками информации;

– подготовку к сдаче зачета.

При подготовке к зачету необходимо ориентироваться на конспекты лекций и рекомендуемую литературу.

Подготовка обучающегося к зачету включает в себя самостоятельную работу в течение семестра, непосредственную подготовку в дни, предшествующие зачету по темам курса.

Особое внимание следует уделить практической составляющей дисциплины. Если при подготовке к зачету обучающийся сталкивается с затруднениями по некоторым вопросам, он имеет возможность получить разъяснений преподавателя на групповой консультации перед зачетом, четко обозначив суть затруднений.

Зачет проводится в виде теста.

Для успешной сдачи зачетаобучающиеся должны принимать во внимание, что все основные вопросы, указанные в перечне вопросов к зачету, нужно знать и понимать их смысл.

Методические рекомендации по работе студентов в системе дистанционного обучения.

Портал online обучения находится по адресу http://learn-mkgtu.ru. Он специально разработан для облегчения дистанционного обучения, дает возможность удобно и оперативно контролировать процесс обучения.

В первую очередь следует создать аккаунт. Для этого необходимо указать логин (имя для входа) и пароль, а также фамилию, имя, отчество, город и адрес электронной почты. На указанный адрес электронной почты будут приходить все уведомления, а также письма при восстановлении пароля. Именно к этому контактному лицу будут обращаться сотрудники Университета при общении.

Дальнейшая работа с системой предполагает использование логина и пароля.

Для перехода к нужному учебному курсу используйте соответствующее меню.

Основное содержание курса расположено в разделах, которые организованы по тематическому принципу.

Дистанционный курс – это набор тематических (или календарных) разделов, в которых размещены ресурсы и активные элементы курса.

Система позволяет изучать материалы курса в любом порядке, но следует придерживаться заданной преподавателем последовательности, т.к. изучение некоторых материалов предполагает знание уже пройденных.

Активные элементы курса – это интерактивные средства, с помощью которых преподаватель либо проверяет уровень знаний студентов, либо вовлекает их во взаимодействие как друг с другом, так и с собой. К активным элементам курса относятся: форумы, задания, тесты и пр.

Активные элементы могут предполагать как одностороннюю активность участников курса, так и обоюдную: между студентом и преподавателем.

Активные элементы требуют коммуникационной активности студента, как правило, в режиме online.

Студентам следует обращать внимание на все задания курса.

Вы можете обращаться к преподавателям курса по всем возникающим у Вас в ходе обучения вопросам.

В некоторых случаях может быть удобнее или целесообразнее не просматривать, а скачать с сайта материалы курса.

Ряд элементов курсапредусматривает прикрепление ответов студентов в виде файлов непосредственно в элементе курса.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Для осуществления учебного процесса используется свободно распространяемое (бесплатное не требующее лицензирования) программное обеспечение:

1. Операционная система;
2. Офисный пакет Open Office;
3. Графический пакет Gimp;
4. Векторный редактор Inkscape;
5. Тестовая система на базе Moodle
6. Тестовая система собственной разработки, правообладатель ФГБОУ ВО «МГТУ», свидетельство №2013617338.

11. Описание материально-технической базы необходимой для осуществления образовательного процесса по дисциплине (модулю)

Наименования специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Специальные помещения		
Учебные аудитории для проведения занятий лекционного типа: № 13 ауд., корпус 3 Аудитория для занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: №13 ауд., корпус 3 Компьютерный класс: № 01 ауд., корпус 3	Переносное мультимедийное оборудование, доска, мебель для аудиторий, компьютерный класс на 15 посадочных мест, оснащенный компьютерами Pentium с выходом в Интернет	свободно распространяемое (бесплатное не требующее лицензирования) программное обеспечение: 1. Операционная система на базе Linux; 2. Офисный пакет Open Office; 3. Графический пакет Gimp; 4. Векторный редактор Inkscape; Антивирусные программы: Kaspersky Endpoint Security - № лицензии 17E0160128-13174640772. Количество: 400 рабочих мест. Срок действия 1 год.
Помещения для самостоятельной работы		
Учебные аудитории для самостоятельной работы: №13 ауд., корпус 3 В качестве помещений для самостоятельной работы могут быть: компьютерный класс, читальный зал: ул. Первомайская, 191, 3 этаж.	Переносное мультимедийное оборудование, доска, мебель для аудиторий, компьютерный класс на 15 посадочных мест, оснащенный компьютерами Pentium с выходом в Интернет	свободно распространяемое (бесплатное не требующее лицензирования) программное обеспечение: 1. Операционная система на базе Linux; 2. Офисный пакет Open Office; 3. Графический пакет Gimp;

		4. Векторный редактор Inkscape; Антивирусные программы: Kaspersky Endpoint Security - № лицензии 17E0160128-13174640772. Количество: 400 рабочих мест. Срок действия 1 год.

Дополнения и изменения в рабочей программе
за _____/_____ учебный год

В рабочую программу_____
(наименование дисциплины)

для направления (специальности) _____
(номер направления (специальности)

вносятся следующие дополнения и изменения:

Дополнения и изменения внес _____
(должность, Ф.И.О., подпись)

Рабочая программа пересмотрена и одобрена на заседании кафедры
_____
(наименование кафедры)

«____»_____201_г.

Заведующий кафедрой_____ _____