МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет Информатики и Информационных Технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность операционных систем

Кафедра Информационных технологий и БКС

Образовательная программа

10.03.01 Информационная безопасность

Профиль подготовки:
Безопасность компьютерных систем

Уровень высшего образования:
бакалавриат

Форма обучения
Очная, очно-заочная

Статус дисциплины:
по выбору

Махачкала, 2022

Рабочая программа дисциплины «Безопасность операционных систем» составлена в 2021г в соответствии с требованиями ФГОС ВО - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность» от 17 ноября 2020 г. N 1427

Разработчик(и): кафедра ИТиБКС, Ахмедова З.Х, доцент, кандидат ф-м.наук

Рабочая программа дисциплины одобрена:
на заседании кафедры __ИТиБКС_____ от «__13_» __04__2022г., протокол № _9_

Зав. кафедрой _____ Ахмедова З.Х..

на заседании Методической комиссии факультета_ИиИТ_от «15»_04_2022г., протокол №_9_.

Председатель _____ Бакмаев А.Ш

Рабочая программа дисциплины согласована с учебно-методическим управлением
«31» 03 2022г.

Начальник УМУ _____ Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины.

Дисциплина «Безопасность операционных систем» входит в часть формируемую участникам образовательных отношений образовательной программы ОПОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность.

Содержание дисциплины охватывает круг вопросов, связанных с построением защищенных автоматизированных систем на основе современных операционных систем, а также администрирования подсистем информационной безопасности операционных систем.

Дисциплина реализуется на факультете _ИиИТ_ кафедрой ____ИТиБКС____.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональные ОПК-6, ОПК-9, ОПК-1.2, профессиональные ПК-5, ПК-9.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, лабораторные занятия, практические занятия и самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме коллоквиум, устный опрос и промежуточный контроль в форме экзамена.

Объем дисциплины 4 зачетные единицы, в том числе в академических часах по видам учебных занятий

Объем дисциплины в очной форме

Семестр	Всего	Учебные занятия							Форма промежуточной аттестации
		в том числе							
		Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		Всего	из них						
			Лекции	Лабораторные занятия	Практические занятия		консультации		
7	144	90	36	36	18			54	экзамен

Объем дисциплины в очно-заочной форме

Семестр	Всего	Учебные занятия				Форма промежуточной аттестации
		в том числе				
		Контактная работа обучающихся с преподавателем			СРС, в том числе экзамен	
		Всего	из них			
			Лекции	Лабораторные занятия	Практические занятия	
8	144	54	22	22	10	90	экзамен

1.Цели освоения дисциплины.

Цель дисциплины – сформировать компетенции обучающегося в области построения защищенных автоматизированных систем на основе современных операционных систем, а также администрирования подсистем информационной безопасности операционных систем.

Задачи дисциплины:

- Рассмотреть основные принципы устройства и принципов функционирования операционных систем различной архитектуры;
- Раскрыть принципы построения подсистем защиты в операционных системах различной архитектуры;
- Показать особенности средств и методов несанкционированного доступа к различным ресурсам операционных систем.

2.Место дисциплины в структуре ОПОП бакалавриата.

Дисциплина Б1.В.01.08 входит в часть формируемую участникам образовательных отношений образовательной программы бакалавриата направлению подготовки 10.03.01 Информационная безопасность и является одной из дисциплин, в рамках которой изучаются методы и средства обеспечения информационной безопасности. Курс занимает важное место в профессиональной подготовке специалиста по защите информации. Он является одним из основных специализированных курсов. Знания, полученные в результате изучения предмета также необходимы для выполнения курсовых и дипломных работ.

Изучение данной дисциплины базируется на следующих дисциплинах:

1. Защита персональных данных
2. Техническая защита информации
3. Защита программ и данных

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

1. Методы оценки безопасности компьютерных систем
2. Знания, умения и навыки, полученные студентами в рамках данной дисциплины, пригодятся им при написании выпускной квалификационной работы, а также необходимы при прохождении производственной практики

3.Компетенции обучающего, формируемые в результате освоения дисциплины.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Код и наименование компетенции из ОПОП	Код и наименование индикатора достижения	Планируемые результаты обучения	Процедура освоения
ОПК -6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД1.ОПК-6.1. Знать: нормативно-правовые основы и документы по проблеме организационного обеспечения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации	Знать: нормативно-правовые основы и документы по проблеме организационного обеспечения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации	Устный опрос, письменный опрос
	ИД2.ОПК-6.2. Уметь: использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации	Уметь: использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации	Устный опрос, письменный опрос
	ИД3.ОПК-6.3. Владеть: навыками работы с нормативно-правовыми и организационно-	Должен владеть: навыками работы с нормативно-правовыми и организационно-	Устный опрос, письменный опрос

	распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутри объектового режима.	распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутри объектового режима.	
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД 1 ОПК-9.1.Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Устный опрос, письменный опрос
	Ид 2 ОПК-9.2. Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации	Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации	Устный опрос, письменный опрос
	ИД 3 ОПК-9.3. Владеет методами и средствами криптографической и технической защиты информации	Владеет методами и средствами криптографической и технической защиты информации	Устный опрос, письменный опрос
ОПК-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ИД 1 ОПК-1.2 Понимает угрозы безопасности, режимы противодействия	Понимает угрозы безопасности, режимы противодействия	Устный опрос, письменный опрос
	ИД 2 ОПК-1.2 Понимает угрозы безопасности, режимы противодействия	Понимает угрозы безопасности, режимы противодействия	Устный опрос, письменный опрос

	ИД 3 ОПК-1.2 Обладает навыками мониторинга функционирования подсистемы ИБ	Обладает навыками мониторинга функционирования подсистемы ИБ	Устный опрос, письменный опрос
ПК-5 Способность выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций	ПК-5.1. Знает методы обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций	Знает: методы обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций	Устный опрос, письменный опрос
	ПК-5.2. Умеет обслуживать программно-аппаратными средствами сети и инфокоммуникации	Умеет: обслуживать программно-аппаратными средствами сети и инфокоммуникации	Устный опрос, письменный опрос
	ПК-5.3. Имеет навыки по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций	Имеет: навыки по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций	Устный опрос, письменный опрос
ПК-9 Разработка и внедрение прикладное программное обеспечение с учетом требований информационной безопасности	ПК 9.1 Методы и инструментальные средства проектирования систем искусственного интеллекта: методы реализации формальных моделей и реализацию вывода на знаниях;	Знает: методы реализации формальных моделей и реализацию вывода на знаниях; основы программирования интеллектуальных задач с использованием классических языков символьной обработки	Устный опрос, письменный опрос
	ПК 9.2 Применять методы и инструментальные средства проектирования систем искусственного интеллекта: методы реализации формальных моделей и реализацию вывода на знаниях;	Умеет: Применять основы программирования интеллектуальных задач с использованием классических языков символьной обработки	Устный опрос, письменный опрос
	ПК 9.3 Методами и инструментальными средствами проектирования систем искусственного интеллекта:	Владеет: методами реализации формальных моделей и реализациями вывода на знаниях;	Устный опрос, письменный опрос

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 4 зачетных единиц, 144 академических часа.

4.2. Структура дисциплины.

4.2.1. Структура дисциплины в очной форме.

№ п/п	Названия разделов	Семестр	Неделя	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Лекции	Практические	Лабораторные	Контроль самост работы	Самостоятельная работа	
1	2								
1	Понятие защищенной операционной системы.	7	1-2	2	2	4		2	устный опрос
2	Управление доступом	7	3	2	2	2		2	устный опрос
3	Аутентификация	7	4-5	4		2		1	устный опрос
4	Аудит и обнаружение вторжений	7	6	4	2	4		1	устный и письменный опросы
	Итого за модуль			12	6	12		6	
5	Обеспечение целостности данных и систем	7	7	2	2	3		2	устный опрос
6	Сетевая безопасность ОС	7	8-9	2		2		1	устный опрос
7	Доверенная загрузка ОС	7	10-11	4	2	3		1	устный опрос
8	Основные понятия операционных систем специального назначения	7	12-13	4		2		2	устный и письменный опросы
	Итого за модуль			12	6	12		6	
9	Управление доступом и безопасностью в ОССН	7	14	4	2	4		10	устный опрос

10	Виртуализация операционных систем	7	15-16	4	2	4		10	устный опрос
11	Безопасность операционных систем мобильных устройств	7	17	4	2	4			устный и письменный опросы
	Итого за модуль:			12	6	12		6	
								36	**экзамен**
	Всего часов	**144**		**36**	**18**	**36**		**54**	

4.2.2 Структура дисциплины в очно-заочной форме.

№ п/п	Названия разделов	Семестр	Неделя	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Лекции	Практические	Лабораторные	Контроль самост работы	Самостоятельная работа	
1	2								
1	Понятие защищенной операционной системы.	8	1-2	2	1	2		4	устный опрос
2	Управление доступом	8	3	2	1	2		4	устный опрос
3	Аутентификация	8	4-5	2	1	2		4	устный опрос
4	Аудит и обнаружение вторжений	8	6	2	1	2		4	устный и письменный опросы
	Итого за модуль			8	4	8		16	
5	Обеспечение целостности данных и систем	8	7	2	1	2		4	устный опрос
6	Сетевая безопасность ОС	8	8-9	2	1	2		4	устный опрос

7	Доверенная загрузка ОС	8	10-11	2	1	2		4	устный опрос
8	Основные понятия операционных систем специального назначения	8	12-13	2	1	2		4	устный и письменный опросы
	Итого за модуль			8	4	8		16	
9	Управление доступом и безопасностью в ОССН	8	14	2	1	2		8	устный опрос
10	Виртуализация операционных систем	8	15-16	2	1	2		6	устный опрос
11	Безопасность операционных систем мобильных устройств	8	17	2		2		8	устный и письменный опросы
	Итого за модуль:			6	2	6		22	
								36	**экзамен**
	Всего часов	**144**		**22**	**10**	**22**		**54**	

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине

Тема 1. Понятие ОС, история, классификация, основные функции. Понятие операционной системы, история развития системного программного обеспечения, принципы функционирования операционных систем

Тема 2. Процессы, модель, состояния. Понятие процесса, контекст процесса, диспетчеризация процессов.

Тема 3. Диспетчеризация и синхронизация процессов. Понятие нити или потока управления. Алгоритмы диспетчеризации потоков управления

Тема 4. Проблемы межпроцессного взаимодействия. Гонки процессов. Понятие критической секции. Алгоритмы предотвращения гонок процессов. Семафоры

Тема 5. Взаимоблокировки процессов Понятие взаимоблокировки. Причины взаимоблокировок. Методы борьбы с взаимоблокировками. Алгоритмы обхода взаимоблокировок

Тема 6. Основные принципы организации подсистем управления памяти виртуальная память, подкачка на диск, методы организации виртуальной памяти. Кольцевая защита процессора

Тема 7. Файловые системы. Механизмы защиты Назначение, классификация, принципы организации файловых систем. Учёт сводного дискового пространства, методы повышения надежности и быстродействия файловых систем

Тема 8. Управление вводом – выводом в ОС. Использование архитектур, отличных от фоннеймановской. Системы перлюстрации запросов на обращения к данным. Защита от считывания со сменных носителей.

Тема 9. Механизмы разграничения доступа в ОС Организация, функции, компоненты, защитные механизмы современных операционных систем

Тема 10. Механизмы безопасной работы в ОС Принципы реализации политик безопасности в ОС. Мандатная, дискреционная и групповые политики

Тема 11. Администрирование ОС Принципы администрирования операционных систем семейства Linux и Windows. Команды управления полномочиями

4.3.2. Содержание лабораторных занятий.

- Лабораторная работа 1. Безопасность клиентских операционных систем.
- Лабораторная работа 2. Проверка безопасности операционных систем.
- Лабораторная работа 3. Настройка политик и паролей и учетных записей в операционной системе Windows.
- Лабораторная работа 4. Планирование и описание области проверки безопасности операционных систем
- Лабораторная работа 5. Анализ программно-технических средств, используемых для протоколирования и аудита информационной безопасности операционных систем.
- Лабораторная работа 6. Настройка протокола безопасных соединений – SSH в операционной системе семейства Unix - Ubuntu server
- Лабораторная работа 7. Настройка аудита доменных служб Active Directory в операционной системе семейства Windows

4.3.3. Содержание практических занятий по дисциплине

1. Организация управления доступом и защиты ресурсов ОС.
2. Основные механизмы безопасности: средства и методы аутентификации в ОС.
3. Модели разграничения доступа.
4. Организация и использование средств аудита.
5. Администрирование ОС: задачи и принципы сопровождения системного программного обеспечения.
6. Генерация, настройка, измерение производительности и модификация систем.
7. Управление безопасностью ОС.
8. Основные стандарты ОС.
9. Механизмы аудита в ОС.
10. Журналирование служб и приложений.
11. Механизмы контроля доступа к ресурсам.
12. Аутентификация в операционных системах.
13. Службы доменных имен.
14. Распределение адресов и DHCP.
15. Установка и настройки серверных операционных систем.
16. Серверные операционные системы. Добавление ролей. Доменные службы.
17. Создание и управление инфраструктурой на основе виртуальных машин.
18. Платформы для виртуализации на основе Windows HyperV. 33
19. KVM.
20. VmWare vCenter и vSphere.

21. Наложенные средства защиты операционных систем и интеграция их в инфраструктуру ОС.
22. Файловые системы ОС Windows и Linux восстановление удаленных файлов.

5.Образовательные технологии.

В учебном процессе помимо традиционных форм проведения занятий используются лекции – визуализации, лекции – диалоги. Лабораторные занятия проводятся в компьютерном классе с использованием Интернет среды. При проведение практических занятий используются деловые игры с разбором конкретных ситуаций.

- Лекционные занятия
- Традиционные технологии
- Иллюстрация работы алгоритмов с использованием видео и элементов анимации в презентациях.
- Демонстрация элементов современных методов разработки программ с использованием видеопроектора
- Практические занятия
- Традиционные технологии
- Коллективное выполнение заданий с использованием видеопроектора, среды разработчика и системы контроля версий исходного кода SVN или Git
- Лабораторные занятия
- Традиционные технологии

6.Учебно-методическое обеспечение самостоятельной работы студентов обучающихся по дисциплине «Безопасность операционных систем».

Форма контроля и критерий оценок

В соответствии с учебным планом предусмотрен экзамен в четвертом семестре.
Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине предполагают следующее распределение баллов.
Текущий контроль

- Выполнение 1 домашней работы 10 баллов
- Активность в системе Moodle 60 баллов

Примерное распределение времени самостоятельной работы студентов

Вид самостоятельной работы	Примерная трудоёмкость, а.ч.	Примерная трудоёмкость, а.ч.	Формируемые компетенции
	Очная	Очно-заочная	
Текущая СРС			
работа с лекционным материалом, с учебной литературой	10	***10***	ОПК-6, ПК-5
опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	10	10	ОПК-9, ПК-9
самостоятельное изучение разделов дисциплины	12	10	ОПК-1.2
выполнение домашних заданий, домашних контрольных работ	10	10	ПК-5, ОПК-1.2
подготовка к лабораторным работам, к практическим и семинарским занятиям	2		ОПК-6, ПК-9
подготовка к контрольным работам, коллоквиумам, зачётам	10	10	ПК-5, ОПК-9

подготовка к экзамену (экзаменам)	36	36	ОПК-6, оПК-9, ОПК-1.2, ПК-1, ПК-9
Творческая проблемно-ориентированная СРС			
поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	10	20	ОПК-1.2
исследовательская работа, участие в конференциях, семинарах, олимпиадах	10	14	ОПК-6
анализ данных по заданной теме, написание программ, составление моделей на основе исходных данных	2	10	ПК-5
ИТОГО:	102ч	130ч	

Рекомендуемая литература.

а) основная литература:

1. Гончарук, С.В. Администрирование ОС Linux 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 165 с. Режим доступа: http://www.iprbookshop.ru/33054.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]

2. Ложников П.С. Средства безопасности операционной системы ROSA Linux // Омск: Издательство ОмГТУ, 2017. - 94 с. Режим доступа: http://www.iprbookshop.ru/48034.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]

б) дополнительная литература:

1. Молочков В. П. Операционная система ROSA // Омск: Издательство ОмГТУ, 2017. - 226 с. Режим доступа: http://www.iprbookshop.ru/42123.html.— ЭБС «IPRbooks»[Дата обращения 20 июня 2021]

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

7.1. Типовые контрольные задания или иные материалы

ПРИМЕРЫ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ

№Текст тестовых материалов

1. Информационная безопасность характеризует защищённость:
А) Пользователя и информационной системы
Б) Информации и поддерживающей еѐ инфраструктуры
В) Источника информации
Г) Носителя информации

2. Что из перечисленного является составляющей информационной безопасности?
А) Нарушение целостности информации
Б) Проверка прав доступа к информации
В) Доступность информации
Г) Выявление нарушителей

3. Получение требуемой информации информационной услуги пользователем за определѐнное время, это:
А) Целостность информации
Б) Конфиденциальность информации
В) Доступность информации
Г) Защищенность информации

4. Конфиденциальность информации гарантирует:
А) Доступность информации кругу лиц, для кого она предназначена
Б) Защищѐнность информации от потери
В) Защищѐнность информации от фальсификации
Г) Доступность информации только автору

9. Основной источник внутренних отказов?
А) Невозможность пользователя работать с системой в силу отсутствия соответствующей подготовки
Б) Нежелание пользователя работать с информационной системой
В) Отступление от установленных правил эксплуатации
Г) Нарушение работы систем связи, электропитания, водо-и/или теплоснабжения, кондиционирования

10. Уровни не относящиеся к уровням формирования режима информационной безопасности?
А) Законодательно-правовой
Б) Информационный
В) Административный (организационный)
Г) Программно-технический

11. На сколько классов подразделяют угрозы информационной безопасности?
А) 4
Б) 3
В) 2
Г) 5

12. Что является самым эффективным при борьбе с непреднамеренными случайными ошибками?
А) Резервирование аппаратуры
Б) Определение степени ответственности за ошибки
В) Максимальная автоматизация и строгий контроль
Г) Контроль действий пользователя

13. Средства защиты информации какого из уровней формирования режима информационной безопасности связаны непосредственно с защищаемой информацией
А) Законодательно-правовой
Б) Информационный
В) Административный (организационный)
Г) Программно-технический

20. Что из перечисленного является задачей информационной безопасности?
А) Устранение неисправностей аппаратных средств
Б) Устранение последствий стихийных бедствий

В) Защита технических и программных средств информатизации от ошибочных действий персонала
Г) Восстановление линий связи

21. Выберите правильную иерархию пространства требований в «Общих критериях»:
А) Класс –семейство –компонент –элемент
Б) Элемент –класс –семейство –компонент
В) Компонент –семейство – класс –элемент
Г) Семейство –компонент –класс –элемент

22. Сколько классов СВТ по уровню защищенности от НСД к информации определено в руководящем документе Гостехкомиссии «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?
А) Три
Б) Семь
В) Пять
Г)Четыре

23. Комплекс предупредительных мер по обеспечению информационной безопасности организации –это:
А) Информационная политика
Б) Политика безопасности
В) Информационная безопасность
Г) Защита информации

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Фонд оценочных средств дисциплины включает в себя контрольные вопросы, задания контрольных работ, вопросы для промежуточной аттестации. Виды самостоятельной работы обучающихся. Изучение основной и дополнительной литературы по материалам курса. Выполнение заданий самостоятельной работы по курсу.

Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабора-торные занятия	Практические занятия	Само-стоя-тельная работа	Автоматизированное тести-рование	Другие виды учебной дея-тельности	Промежуточная аттестация	Итого
7	5	10	15	25	0	5	40	100

Программа оценивания учебной деятельности студента. Семестр 7
Лекции. Посещаемость, опрос, активность за семестр — от 0 до 5 баллов.
Лабораторные занятия. Выполнение одной лабораторной работы – 10б.
Практические занятия. Посещаемость, опрос, активность за семестр — от 0 до 15 баллов.
Самостоятельная работа. Контроль выполнения заданий самостоятельной работы в течение одного семестра — от 0 до 25 баллов;
Контрольная работа (от 0 до 10 баллов);

Автоматизированное тестирование. Не предусмотрено.

Другие виды учебной деятельности.

Написание реферата является одной из форм обучения студентов. Данная форма обучения направлена на организацию и повышение уровня самостоятельной работы студентов. Реферат, как форма обучения студентов - это краткий обзор максимального количества доступных публикаций по заданной теме, подготовка самого реферативного обзора и презентации по нему. При проведении обзора должна проводиться и исследовательская работа, но объем ее ограничен, так как анализируется уже сделанные выводы и в связи с небольшим объемом данной формы работы. Преподавателю предоставляется сам реферат в письменной форме (электронная версия в формате Microsoft Word) и презентация к нему (электронная версия в формате PowerPoint). Сдача реферата происходит в форме защитыдоклада с использованием подготовленной презентации.

Критерии оценки рефератов:

Оценки на "отлично":

10 - тема раскрыта блестяще, презентация является целостным новым независимым дополнением высокого уровня к лекционному курсу

9 - тема раскрыта отлично, есть отдельные фрагменты, которые являются новыми независимыми смысловыми дополнениями к лекциям

8 - тема в основном раскрыта, качество материала высокое, но не является уникальным

Оценки на "хорошо"

7 - тема раскрыта не полностью, не хватает некоторой части. Качество материала хорошее.

6 - тема раскрыта не полностью, не хватает некоторой значимой части.

Удовлетворительно:

5 - раскрыта хотя бы примерно половина темы. Качество материала удовлетворительное.

4 - что-то по существу реферата сказано, но мало и фрагментарно. Качество материала на грани удовлетворительного.

Неудовлетворительно:

3 - понял, о чем надо рассказывать, но практически ничего не рассказал по теме реферата. Качество материала неудовлетворительное.

2 - понял название темы, ничего не рассказал либо рассказывал не о том. Материал фактически отсутствует.

1 - не понял название темы, не рассказывал. Материал фактически отсутствует и не по теме.

0 - реферат не сдавался.

Промежуточная аттестация. Методика оценивания знаний, обучающихся по дисциплине «Облачные технологии» в ходе промежуточной аттестации:

25-40 баллов:

Ответ студента содержит:

глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;

знание концептуально-понятийного аппарата всего курса;

знание монографической литературы по курсу,

также свидетельствует о способности:

самостоятельно критически оценивать основные положения курса;

увязывать теорию с практикой.

15-24 баллов:

Ответ студента свидетельствует:

о полном знании материала по программе;

о знании рекомендованной литературы,

а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

1-14 баллов:

Ответ студента содержит:

поверхностные знания важнейших разделов программы и содержания лекционного курса;
затруднения с использованием научно-понятийного аппарата и терминологии курса;
стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.
Студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала ставится оценка 0 баллов.
Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за один семестр по дисциплине «Облачные технологии» составляет 100 баллов.

Итоговой формой контроля знаний, умений и навыков по дисциплине является **Экзамен**. Экзамен проводится в форме тестирования. При соответствии ответа учащегося на зачете более чем 51 % критериев из этого списка выставляется оценка «удовлетворительно», 66% – 85% оценка «хорошо», 86% и выше оценка «отлично».

8. Учебно-методическое обеспечение дисциплины

а) основная литература:

1. Гончарук, С.В. Администрирование ОС Linux 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 165 с. Режим доступа: http://www.iprbookshop.ru/33054.html. — ЭБС «IPRbooks»[Дата обращения 20 июня 2022]
2. Ложников П.С. Средства безопасности операционной системы ROSA Linux // Омск: Издательство ОмГТУ, 2017. - 94 с. Режим доступа: http://www.iprbookshop.ru/48034.html. — ЭБС «IPRbooks»[Дата обращения 20 июня 2022]

б) дополнительная литература:

1. Молочков В. П. Операционная система ROSA // Омск: Издательство ОмГТУ, 2017. - 226 с. Режим доступа: http://www.iprbookshop.ru/42123.html. — ЭБС «IPRbooks»[Дата обращения 20 июня 2022]

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. eLIBRARY.Ru [Электронный ресурс]: электронная библиотека / Науч. электр. б-ка.- МОСКВА.1999. – Режим доступа: http//elibrary.ru (дата обращения 15.04.2018). – Яз. рус., англ.
2. Электронный каталог НБ ДГУ Ru [Электронный ресурс]: база данных содержит сведения о всех видах лит., поступающих в фонд НБ ДГУ / Дагестанский гос.унив. – Махачкала. – 2010. – Режим доступа: http//elib.dgu.ru. свободный (дата обращения 11.03.2018)
3. Национальный Открытый Университете «ИНТУИТ»[Электронный ресурс]: электронно-библиотечная система, издательство «Лань» - www.intuit.ru(дата обращения 12.03.2018)

10. Методические указания для обучающихся по освоению дисциплины.

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умения самостоятельно добывать знания из различных источников,

систематизировать полученную информацию, давать оценку конкретной финансовой ситуации. Формирование такого умения происходит в течение всего периода обучения через участие студентов в практических занятиях, выполнение контрольных заданий и тестов, написание курсовых и выпускных квалификационных работ. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

11.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

1. Компьютерные классы с набором лицензионного базового программного обеспечения для проведения лабораторных занятий;

2. MicrosoftVisualStudio (или CodeBloc) для выполнения лабораторных заданий

3. Лекционная мультимедийная аудитория для чтения лекций с использованием мультимедийных материалов.

4. Тестовая программа Test2000 для компьютерного тестирования.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

При освоении дисциплины для выполнения лабораторных работ необходимы классы персональных компьютеров с приложениями программирования на языках C/C++. Для проведения лекционных занятий, необходима мультимедийная аудитория с набором лицензионного базового программного обеспечения.

Лекционные занятия

- Видеопроектор, ноутбук, презентатор
- Подключение к сети Интернет

Практические занятия

- Видеопроектор, ноутбук
- Подключение к сети Интернет