

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы оценки безопасности компьютерных 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:

входит в обязательную часть ОПОП

Махачкала, 2021

Рабочая программа дисциплины «Методы оценки безопасности компьютерных 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

Составитель:



Ахмедова З.Х., доцент каф. ИТиБКС

Рабочая программа одобрена на заседании кафедры «Информационных технологий безопасности компьютерных систем».

Протокол № 11 от 28.06 2021г

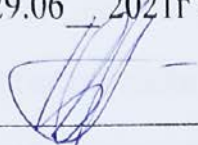
Зав кафедрой ИТиБКС



Ахмедова З.Х.

Одобрена на заседании Методической комиссии факультета Информатики и информационных технологий от 29.06 2021г протокол № 11

Председатель



Бакмаев А.Ш.

Рабочая программа согласована с учебно-методическим управлением

«___» _____ 2021г

Начальник УМУ



Гасангаджиева А.Г.

Аннотация рабочей программы дисциплины.

Дисциплина «Методы оценки безопасности компьютерных систем» входит в обязательную часть образовательной программы ОПОП бакалавриата по направлению подготовки 10.03.01 Информационная безопасность.

Содержание дисциплины охватывает круг вопросов, связанных с методами оценки безопасности компьютерных систем; проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации (ЗИ) в компьютерных системах; принципы и способы использования существующих средств ЗИ в компьютерных системах; принципы применения современных методов оценки безопасности компьютерных систем.

Дисциплина реализуется на факультете _ИиИТ_ кафедрой ____ИТиБКС____.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональные ОПК-5, ОПК-10, ОПК-1.4, профессиональные ПК-7, ПК-9.

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

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

Объем дисциплины 2 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	
		Все го	из них						
			Лекц ии	Лаборатор ные занятия	Практич еские занятия		консульт ации		
8	72	36	24	0	12			36	зачет

Объем дисциплины в очно-заочной форме

Семестр	Всего	Учебные занятия					СРС	Форма промежуточной аттестации
		в том числе						
		Контактная работа обучающихся с преподавателем						
		Все го	из них					
			Лекции	Лабораторные занятия	Практические занятия			
А	72	28	18	0	10	44	зачет	

1.Цели освоения дисциплины.

Целью дисциплины «Методы оценки безопасности компьютерных систем» является формирование у студентов знаний по оценке безопасности компьютерных систем.

Задачи дисциплины – дать основы принципов построения подсистем защиты в компьютерных системах различной архитектуры; средств и методов несанкционированного доступа к ресурсам компьютерных систем; системного подхода к проблеме защиты информации в компьютерных системах механизмов защиты информации и возможностей по их преодолению.

2.Место дисциплины в структуре ОПОП бакалавриата.

Дисциплина Б1.О.04.17 входит в обязательную часть 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.

Изучение данной дисциплины базируется на следующих дисциплинах:

1. Защита персональных данных
2. Техническая защита информации
3. Защита программ и данных
4. Программно-аппаратные средства защиты информации

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

1. 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 -5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите	ИД1.ОПК-5.1 Знает основные правовые понятия, категории, юридические конструкции	Знает основные правовые понятия, категории, юридические конструкции	Устный опрос, письменный опрос
	ИД2.ОПК-5.2. Умеет анализировать законодательство и	Умеет анализировать законодательство и правовую информацию,	Устный опрос,

информации в сфере профессиональной деятельности;	правовую информацию, необходимую для принятия обоснованных решений в профессиональной сфере	необходимую для принятия обоснованных решений в профессиональной сфере	письменный опрос
	ИД3.ОПК-5.3 Владеет навыками поиска правовой информации для решения профессиональных задач	Владеет навыками поиска правовой информации для решения профессиональных задач	Устный опрос, письменный опрос
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ИД 1 ОПК-10.1.Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	Устный опрос, письменный опрос
	ИД 2 ОПК-10.2. Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	Устный опрос, письменный опрос
	ИД 3 ОПК-10.3. Владеет принципами формирования политики информационной безопасности объекта информатизации	Владеет принципами формирования политики информационной безопасности объекта информатизации	Устный опрос, письменный опрос
ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ИД1 ОПК-1.4. Знает принципы применения современных методов оценки безопасности компьютерных систем	Знает принципы применения современных методов оценки безопасности компьютерных систем	Устный опрос, письменный опрос
	ИД2 ОПК-1.4. Умеет выявлять угрозы и определять их актуальность для компьютерных систем	Умеет выявлять угрозы и определять их актуальность для компьютерных систем	Устный опрос, письменный опрос
	ИД3 ОПК-1.4. Владеет практическими навыками применения методов обеспечения безопасности компьютерных систем	Владеет практическими навыками применения методов обеспечения безопасности компьютерных систем	Устный опрос, письменный опрос
ПК-7 Обеспечение функционирования средств связи сетей связи	ПК 7.1. Номенклатура, функциональное назначение и основные характеристики средств	Знать: Руководящие и методические документы уполномоченных федеральных органов	Устный опрос, письменный опрос

специального назначения	связи сетей связи специального назначения, включая СКЗИ;	исполнительной власти по защите информации	
	ПК 7.2. Проводить проверку комплектности средств связи сетей связи специального назначения, включая СКЗИ	Уметь: Выполнять настройку и проверку функционирования средств связи сетей связи специального назначения, включая СКЗИ	Устный опрос, письменный опрос
	ПК 7.3. Настройкой средств связи сетей связи специального назначения, включая СКЗИ;	Владеть: Проверкой функционирования средств связи сетей связи специального назначения, включая СКЗИ	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 2 зачетных единиц,

72 академических часа.

4.2. Структура дисциплины.

4.2.1. Объем дисциплины в очной форме.

№ п/п	Названия разделов	Семестр	Неделя	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Контроль	Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Лекции	Практические занятия	Лабораторные занятия			
1	2								
1	Общие вопросы оценки безопасности компьютерных систем	8	1-2	6	3			2	устный опрос
2	Методы и средства оценки безопасности компьютерных систем	8	3-4	6	3			2	устный опрос
	Итого за модуль			12	6			18	
5	Организация оценки безопасности компьютерных систем	8	5-6	6	3			2	устный опрос
6	Оценка эффективности мер защиты информационных систем персональных данных	8	7-8	6	3			1	устный опрос
	Итого за модуль			12	6			18	
	Всего часов	72		24	12			36	

4.2.2 Объем дисциплины в очно-заочной форме.

№ п/п	Названия разделов	Семестр	Неделя	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Контроль	Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Лекции	Практические занятия	Лабораторные занятия			

1	2								
1	Общие вопросы оценки безопасности компьютерных систем	8	1-4	4	3			2	устный опрос
2	Методы и средства оценки безопасности компьютерных систем	8	5-8	6	2			2	устный опрос
	Итого за модуль			10	5			21	
5	Организация оценки безопасности компьютерных систем	8	9-13	4	2			2	устный опрос
6	Оценка эффективности мер защиты информационных систем персональных данных	8	14-17	4	3			1	устный опрос
	Итого за модуль			8	5			23	
	Всего часов	72		18	10			44	

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

4.3.1. Содержание лекционных занятий по дисциплине

Тема 1. Предметная область оценки безопасности компьютерных систем. Исторические сведения и этапы развития оценки безопасности компьютерных систем. Математические основы оценки безопасности компьютерных систем.

Тема 2. Анализ рисков в области защиты информации. Международная практика защиты информации. Национальные особенности защиты информации. Постановка задачи анализа рисков. Методы, использующие оценку рисков на качественном уровне. Методы, использующие оценку рисков на количественном уровне. Методы, использующие смешанную оценку рисков. Управление рисками и международные стандарты. Технологии анализа рисков. Инструментальные средства анализа рисков. Аудит безопасности и анализ рисков. Анализ защищенности компьютерной системы. Учет возможностей обнаружения атак и управления рисками в компьютерных системах для оценки безопасности компьютерных систем.

Тема 3. Организация службы информационной безопасности. Формирование экспертных систем оценки безопасности компьютерных систем. Жизненный цикл компьютерных систем. Модель угроз и принципы обеспечения безопасности компьютерных систем. Политика безопасности. Оценка рисков и ущербов безопасности компьютерных систем.

Тема 4. Оценка обстановки и формирование замысла защиты персональных данных. Классификация ИСПД. Обязательные требования по обеспечению безопасности ПД от НСД

Темы практических занятий.

1. Критерии оценки безопасности информационных технологий
2. Управление рисками безопасности
3. Стандарты и системы качества в области информационной безопасности
4. Технологии и инструментарий для управления рисками
5. Инфраструктура службы информационной безопасности предприятия

Примерный перечень вопросов к зачету.

- 1 Законодательная и нормативно-правовая база в области оценки безопасности компьютерных систем
- 2 Основные методы оценки безопасности компьютерных систем

- 3 Основные средства оценки безопасности компьютерных систем
- 4 Современные подходы к управлению рисками в компьютерных системах
- 5 Риск-модель компьютерной системы
- 6 Алгоритм вычисления комплексного риска
- 7 Алгоритм управления информационными рисками
- 8 Критерии оценки безопасности информационных технологий
- 9 Политика безопасности
- 10 Организационные меры по обеспечению безопасности в компьютерных системах
- 11 Аудит безопасности, оценка действующего уровня защищенности в компьютерных системах
- 12 Средства защиты в компьютерных системах
- 13 Технология оценки рисков в компьютерных системах
- 14 Оценка потенциального ущерба при осуществлении угроз в компьютерных системах
- 15 Теоретико-вероятностный метод оценки рисков в компьютерных системах
- 16 Экспертный метод оценки рисков в компьютерных системах
- 17 Статистический метод оценки рисков в компьютерных системах
- 10 Вероятностно-статистический метод оценки рисков в компьютерных системах
- 19 Взаимосвязь угроз, уязвимостей и рисков
- 20 Оценки защищенности на основе модели комплекса механизмов защиты
- 21 Семантические показатели защищенности компьютерных систем
- 22 Нечеткие оценки защищенности компьютерных систем
- 23 Комплексные оценки защищенности компьютерных систем
- 24 Типовая архитектура системы выявления атак
- 25 Методы тестирования системы защиты
- 26 Система обнаружения вторжений
- 27 Парольная защита
- 28 Жизненный цикл компьютерных систем
- 29 Защита информации от несанкционированного доступа
- 30 Защита от копирования
- 31 Защита от вирусов
- 32 Руководство по разработке профилей защиты и заданий по информационной безопасности компьютерных систем
- 33 Биометрическая защита компьютерных систем
- 34 Порядок организации оценки безопасности компьютерных систем
- 35 Технические меры обеспечения безопасности компьютерных систем.

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 проведении 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

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

Форма контроля и критерий оценок

В соответствии с учебным планом предусмотрен зачет в восьмом 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	4	4	ОПК-5, ПК-7
опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	4	4	ОПК-10, ПК-9
самостоятельное изучение разделов дисциплины	2	4	ОПК-1.4
выполнение домашних заданий, домашних контрольных работ	2	2	ПК-7, ОПК-1.4
подготовка к практическим занятиям	2	6	ОПК-5, ПК-9
подготовка к контрольным работам, коллоквиумам	2	4	ПК-5, ОПК-1.4
подготовка к зачету	6	6	ОПК-10, ОПК-1.4, ПК-7, ПК-9
Творческая проблемно-ориентированная СРС			
поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	4	4	ОПК-1.4
исследовательская работа, участие в конференциях, семинарах, олимпиадах	2	2	ОПК-5
анализ данных по заданной теме, написание программ, составление моделей на основе исходных данных	2	2	ПК-7
ИТОГО:	36 ч	44 ч	

Рекомендуемая литература.

а) основная литература:

1. Технологии защиты информации в компьютерных сетях [Электронный ресурс]/ Н.А. Руденков [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 368 с.— Режим доступа: <http://www.iprbookshop.ru/73732.html>.— ЭБС «IPRbooks»
2. Глотина И.М. Средства безопасности операционной системы Windows Server 2008 [Электронный ресурс]: учебно-методическое пособие/ Глотина И.М.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 141 с.— Режим доступа: <http://www.iprbookshop.ru/72538.html>.— ЭБС «IPRbooks»

б) дополнительная литература:

1. Никифоров С.Н. Защита информации. Защита от внешних вторжений [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 84 с.— Режим доступа: <http://www.iprbookshop.ru/74381.html>.— ЭБС «IPRbooks»

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. Кто является основным ответственным за определение уровня классификации информации?
 - A. Руководитель среднего звена
 - B. Высшее руководство
 - C. Владелец
 - D. Пользователь
2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
 - A. Сотрудники
 - B. Хакеры
 - C. Атакующие
 - D. Контрагенты (лица, работающие по договору)
3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
 - A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
 - B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
 - C. Улучшить контроль за безопасностью этой информации
 - D. Снизить уровень классификации этой информации
4. Что самое главное должно продумать руководство при классификации данных?
 - A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
 - B. Необходимый уровень доступности, целостности и конфиденциальности
 - C. Оценить уровень риска и отменить контрмеры
 - D. Управление доступом, которое должно защищать данные
5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
 - A. Владельцы данных
 - B. Пользователи
 - C. Администраторы
 - D. Руководство
6. Что такое процедура?

- A. Правила использования программного и аппаратного обеспечения в компании
- B. Пошаговая инструкция по выполнению задачи
- C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
- D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

- A. Поддержка высшего руководства
- B. Эффективные защитные меры и методы их внедрения
- C. Актуальные и адекватные политики и процедуры безопасности
- D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

- A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- B. Когда риски не могут быть приняты во внимание по политическим соображениям
- C. Когда необходимые защитные меры слишком сложны
- D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

- A. Пошаговые инструкции по выполнению задач безопасности
- B. Общие руководящие требования по достижению определенного уровня безопасности
- C. Широкие, высокоуровневые заявления руководства
- D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- A. Анализ рисков
- B. Анализ затрат / выгоды
- C. Результаты ALE
- D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что является наилучшим описанием количественного анализа рисков?

- A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
- B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
- C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
- D. Метод, основанный на суждениях и интуиции

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	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	5		15	25	0	5	40	100

Программа оценивания учебной деятельности студента. Семестр 7

Лекции. Посещаемость, опрос, активность за семестр — от 0 до 5 баллов.

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 защиты доклада 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 **Зачет**. Зачет проводится в форме тестирования. При соответствии ответа учащегося на зачете более чем 55 % критериев из этого списка выставляется оценка «зачет».

8.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

1. Технологии защиты информации в компьютерных сетях [Электронный ресурс]/ Н.А. Руденков [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 368 с.— Режим доступа: <http://www.iprbookshop.ru/73732.html>.— ЭБС «IPRbooks»
2. Глотина И.М. Средства безопасности операционной системы Windows Server 2008 [Электронный ресурс]: учебно-методическое пособие/ Глотина И.М.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 141 с.— Режим доступа: <http://www.iprbookshop.ru/72538.html>.— ЭБС «IPRbooks»

б) дополнительная литература:

2. Никифоров С.Н. Защита информации. Защита от внешних вторжений [Электронный ресурс]: учебное пособие/ Никифоров С.Н.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017.— 84 с.— Режим доступа: <http://www.iprbookshop.ru/74381.html>.— ЭБС «IPRbooks»

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