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

Методы оценки безопасности компьютерных систем

Кафедра Информатики и Информационных технологий

Образовательная программа

10.03.01 Информационная безопасность

Профиль подготовки:
Безопасность компьютерных систем

Уровень высшего образования:
бакалавриат

Форма обучения
очная

Статус дисциплины:
вариативная

Махачкала 2018

Рабочая программа по дисциплине «Методы оценки безопасности компьютерных систем» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 –_«Информационная безопасность» (уровень: бакалавриата) от 1 декабря 2016 г. №1515.

Составитель: Мустафаев А.Г., профессор каф. ИИиТ

Рабочая программа одобрена на заседании кафедры «Информатики и информационных технологии».

Протокол № 12 от 2.07 2018г

Зав кафедрой ИиИТ _____ С.А. Ахмедов

Одобрена на заседании Методической комиссии факультета Информатики и информационных технологий

Протокол № 10 от 3.07 2018г

Председатель _____ Камилов К.Б.

Рабочая программа согласована с учебно-методическим управлением

3.07 2018г _____

Аннотация рабочей программы дисциплины.

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

Дисциплина призвана способствовать формированию у студентов навыков современных научных исследований в области проектирования и эксплуатации ИС.

В результате изучения дисциплины студент должен знать:

- суть системного подхода к построению высоконадежных ИС;
- углубить знания в области теории надёжности;
- изучить инженерные методы решения задач оценки надежности, точности, качества функционирования ИС.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных- ОПК-7, профессиональных – ПК-5, ПК-6, ПК-7, ПК-8, ПК-13, ПК-15. Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, самостоятельная работа.

Объем дисциплины 2 зачетных единиц, в том числе в академических часах по видам учебных занятий

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе							
	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
	Всего	из них						
		Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
8	72	14		28			30	зачет

1.Цели освоения дисциплины.

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

Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач программной защиты информации с учетом требований системного подхода.

Дисциплина «Методы оценки безопасности компьютерных систем» имеет целью обучить студентов принципам построения защиты информации в ОС и анализа надежности, защиты компьютерных системах.

Задачами дисциплины являются:

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 принадлежит вариативной части ОПОП по направлению подготовки “Информационная безопасность”. для успешного освоения дисциплины необходимы входные знания в области физики, построения и функционирования компьютерных систем, распространения сигналов, теории вероятностей и математической статистики, теории цифровой обработки сигналов, информатики.

В результате изучения дисциплины студент должен:

знать: базовые понятия современных методов 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;

уметь: выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать(моделировать) объекты защиты и угрозы безопасности компьютерных систем; применять наиболее эффективные методы обеспечения безопасности компьютерных систем; применять современные методы оценки безопасности компьютерных систем;

владеть: практическими навыками применения методов обеспечения безопасности компьютерных систем; навыками применения современных методов оценки безопасности компьютерных систем.

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 компетенций из ФГОС ВО	Наименование компетенций из ФГОС ВО	Перечень планируемых результатов обучения
ПК-5	способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности	Знать: методы формализации процессов функционирования систем Уметь: выбрать из освоенного арсенала необходимый математический аппарат и применить соответствующую методику его

	информации	использования при решении задач моделирования технических систем Владеть: культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения
ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений	Знать: понятия и определения, используемые в рамках направления, общие законы и правила измерений, обеспеченность их единства, требуемой точности и достоверности, основы Государственной системы стандартизации, основные метрологические методы и средства измерения линейных и угловых величин, показатели качества продукции и методы ее оценки; Уметь: обоснованно выбирать и применять соответствующие конкретной ситуации положения законодательных актов и основополагающих документов по метрологии, стандартизации, сертификации, применять действующие стандарты, положения и инструкции по оформлению технической документации; Владеть: основными понятиями и определениями, используемые в рамках направления подготовки, навыками выбора универсального измерительного средства в зависимости от требуемой точности параметра, навыками проведения измерений и оценки погрешности измерений, оценки качества изделий
ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать:** основные подходы к описанию моделей сложных систем и соответствующие формальные модели (клеточные автоматы, графы событий, агрегированные системы, DEVS формализм и т.д.); **Уметь:** обосновывать выбор способа представления модели и программных средств её реализации;
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать:** методы организации управления, планирования, диспетчеризации и синхронизации процессов **Уметь:** использовать полученные знания при работе с ВС, использующими современные ОС; **Владеть:** методами восстановления работоспособности ОС при устранения последствий сбоев в работе ОС.
ПК-13	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать:** понятия и определения, используемые в рамках направления, физические основы и принципы работы вычислительных, устройств, основные характеристики процессоров и устройств памяти, принципы обмена данными

		в вычислительных машинах, назначение интерфейсов, структуру персонального компьютера, принципы построения вычислительных систем, принципы построения вычислительных сетей, тенденции использования вычислительной техники в управлении **Уметь:** применять вычислительную технику при решении задач управления;
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации Уметь: пользоваться нормативными документами; оценивать качество готового программного обеспечения; Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 2 зачетные единицы, 72 академических часа.

4.2. Структура дисциплины.

Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся.

№ п/п	Названия разделов	Семестр	Неделя	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост.работы		
1	2								
Модуль I.									
1	Общие вопросы оценки безопасности компьютерных систем	8		4	6			6	Устный опрос

2	Методы и средства оценки безопасности компьютерных систем			4	8			8	Устный опрос
	Итого за модуль:			8	14			14	
	Модуль II.								
4	Организация оценки безопасности компьютерных систем			6	14			16	Устный опрос
	Итого за модуль:			6	14			16	
	Всего часов			**14**	**28**			**30**	**зачет**

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

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.

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.

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
- Компьютерное тестирование программ, разрабатываемых студентами

6. Учебно-методическое обеспечение самостоятельной работы студентов обучающихся по дисциплине.

Форма контроля и критерий оценок

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

Текущий контроль

- Посещаемость занятий 5 баллов
- Выполнение 1 домашней работы 10 баллов

Промежуточный контроль

По завершении модуля проводить письменный опрос 60 баллов

Темы для самостоятельного изучения.

№	Содержание дисциплины, самостоятельно изучаемой студентами	Формы контроля (контр. работа, лаб. занятия и т.д.)
1	Основные понятия и положения защиты информации в информационно-вычислительных системах	опрос
2	Угрозы безопасности компьютерных систем	опрос
3	Анализ защищенности современных операционных систем. Встроенные средства защиты Windows, Unix	опрос
4	Анализ параметров безопасности и конфигурирование безопасности систем под управлением Windows, Unix	опрос
5	Идентификация и аутентификация пользователей в компьютерных системах	опрос

Рекомендуемая литература.

а) основная литература:

1. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие/ Спицын В.Г.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 с.— Режим доступа: http://www.iprbookshop.ru/13936.html.— ЭБС «IPRbooks»

2. 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»

3. 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. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»/ В.Ю. Рогозин [и др.].— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2017.— 287 с.— Режим доступа: http://www.iprbookshop.ru/72444.html.— ЭБС «IPRbooks»

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»

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

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

В результате освоения дисциплины «Методы оценки безопасности компьютерных систем» ОПОП по направлению 10.03.01 Информационная безопасность обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код и компетенция из ФГОС ВО	Планируемые результаты обучения	Процедура освоения
ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	**Знать**: методы использования основных законов естественнонаучных дисциплин в профессиональной деятельности, способы применения методов математического анализа и моделирования, теоретического и экспериментального исследования **Уметь**: работать в коллективе в кооперации с коллегами Владеть: культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения	Устный опрос, Контр. работа
ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать и проведении технико-экономического обоснования соответствующих проектных решений	**Знать**: этапы имитационного моделирования и их задачи; методы генерации псевдослучайных объектов (величин, процессов, структур); Уметь: проводить системный анализ моделируемой системы; **Владеть**: навыками работы с отечественным и зарубежным информационно-справочным материалом	Устный опрос, Контр. работа
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать:** основные подходы к описанию моделей сложных систем и соответствующие формальные модели (клеточные автоматы, графы событий, агрегированные системы, DEVS формализм и т.д.); **Уметь:** обосновывать выбор способа представления модели и программных средств её реализации;	Устный опрос, Контр. работа
ПК-6 способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать:** методы планирования имитационных экспериментов и анализа их результатов; способы создания и использования программных средств имитации **Уметь:** использовать приобретённые знания при самостоятельном проведении имитационного моделирования сложных систем **Владеть:** проводить имитационный эксперимент и анализировать его результаты.	Устный опрос, Контр. работа

ПК-13 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать:** основные подходы к описанию моделей сложных систем и соответствующие формальные модели (клеточные автоматы, графы событий, агрегированные системы, DEVS формализм и т.д.); **Уметь:** обосновывать выбор способа представления модели и программных средств её реализации;	Устный опрос, Контр. работа
ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знать: этапы имитационного моделирования и их задачи; методы генерации псевдослучайных объектов (величин, процессов, структур); Уметь: проводить системный анализ моделируемой системы; Владеть: навыками работы с отечественным и зарубежным информационно-справочным материалом.	Устный опрос, Контр. работа

7.2. 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
21. 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
22. Почему количественный анализ рисков в чистом виде не достижим?
A. Он достижим и используется
B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
C. Это связано с точностью количественных элементов
D. Количественные измерения должны применяться к качественным элементам
23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
A. Много информации нужно собрать и ввести в программу
B. Руководство должно одобрить создание группы
C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
D. Множество людей должно одобрить данные
24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

A. Стандарты
B. Должный процесс (Due process)
C. Должная забота (Due care)
D. Снижение обязательств
25. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
A. Список стандартов, процедур и политик для разработки программы безопасности
B. Текущая версия ISO 17799
C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
D. Открытый стандарт, определяющий цели контроля
26. Из каких четырех доменов состоит CobiT?
A. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
B. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
C. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
D. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
27. Что представляет собой стандарт ISO/IEC 27799?
A. Стандарт по защите персональных данных о здоровье
B. Новая версия BS 17799
C. Определения для новой серии ISO 27000
D. Новая версия NIST 800-60
28. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
A. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
B. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
C. COSO учитывает корпоративную культуру и разработку политик
D. COSO – это система отказоустойчивости
29. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
A. NIST и OCTAVE являются корпоративными
B. NIST и OCTAVE ориентирован на ИТ
C. AS/NZS ориентирован на ИТ
D. NIST и AS/NZS являются корпоративными
30. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
A. Анализ связующего дерева
B. AS/NZS
C. NIST
D. Анализ сбоев и дефектов

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

а) **Критерии оценивания компетенций (результатов).**

Программой дисциплины в целях проверки прочности усвоения материала предусматривается проведение различных форм контроля:
1. «Входной» контроль определяет степень сформированности знаний, умений и навыков обучающегося, необходимым для освоения дисциплины и приобретенным в результате освоения предшествующих дисциплин.
2. Тематический контроль определяет степень усвоения обучающимися каждого раздела (темы в целом), их способности связать учебный материал с уже усвоенными знаниями, проследить развитие, усложнение явлений, понятий, основных идей.
3. Межсессионная аттестация– рейтинговый контроль знаний студентов, проводимый в середине семестра.
4. Рубежной формой контроля является зачет. Изучение дисциплины завершается зачетом, проводимым в виде письменного опроса с учетом текущего рейтинга.

Рейтинговая оценка знаний студентов проводится по следующим критериям:

Вид оцениваемой учебной работы студента	Баллы за единицу работы	Максимальное значение
Посещение всех лекции	макс. 5 баллов	5
Присутствие на всех практических занятиях	макс. 5 баллов	5
Оценивание работы на семинарских, практических, лабораторных занятиях	макс. 10 баллов	10
Самостоятельная работа	макс. 40 баллов	40
Итого		60

Неявка студента на промежуточный контроль в установленный срок без уважительной причины оценивается нулевым баллом. Повторная сдача в течение семестра не разрешается.
Дополнительные дни отчетности для студентов, пропустивших контрольную работу по уважительной причине, подтвержденной документально, устанавливаются преподавателем дополнительно.

Итоговой формой контроля знаний, умений и навыков по дисциплине является **(экзамен)**.

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

а) основная литература:

4. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие/ Спицын В.Г.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 с.— Режим доступа: http://www.iprbookshop.ru/13936.html.— ЭБС «IPRbooks»

5. 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»

6. 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

3. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности»/ В.Ю. Рогозин [и др.].— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2017.— 287 c.— Режим доступа: http://www.iprbookshop.ru/72444.html.— ЭБС «IPRbooks»

4. 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 c.— 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. Moodl [Электронный ресурс]: система виртуального обучения:[база данных] / Даг.гос.универ. – Махачкала, - Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http: //moodl.dgu.ru. (дата обращения 22.05.18).
3. 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)
4. Национальный Открытый Университете «ИНТУИТ» [Электронный ресурс]:
   - 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.

Советы по планированию и организации времени, необходимого для изучения дисциплины.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.

Изучение конспекта лекции за день перед следующей лекцией – 10-15 минут.

Изучение теоретического материала по учебнику и конспекту – 1 час в неделю.

Подготовка к практическому занятию – 2 часа.

Всего в неделю – 3 часа 25 минут.

Описание последовательности действий студента («сценарий изучения дисциплины»).

При изучении дисциплины необходимо не только выполнять практические задания по предмету, но и регулярно изучать теоретический материал.
1. После прослушивания лекции и окончания учебных занятий, при подготовке к практическим занятиям, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2. При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).
3. Для выполнения лабораторной работы необходимо: Изучить учебные материалы, представленные в презентациях, выполнить предложенные преподавателем задания.
При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, выбрать алгоритм решения задачи. Далее необходимо написать программу, провести ее отладку. Для исправления синтаксических ошибок необходимо обратиться к теоретическому материалу в лекциях, учебниках. При дальнейшей отладке программы необходимо пользоваться либо встроенными средствами, либо вставлять в программу дополнительные операторы вывода для возможности отслеживания полученных значений и локализации возможной ошибки. Для проверки правильности работы программы необходимо составить достаточное количество тестовых заданий.

Рекомендации по использованию материалов учебно-методического комплекса.
Рекомендуется использовать методические указания по курсу программирования, текст лекций преподавателя (если он имеется), презентации лекций. Рекомендуется использовать электронные учебно-методические пособия по программированию, имеющиеся на факультетском сервере.

Рекомендации по работе с литературой. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и учебники по программированию. Необходимая литература имеется как в библиотеке, так и в кабинете математики. Также по данному курсу имеется достаточно много учебных материалов в электронном виде. При работе с литературой полезно одновременно читать учебники нескольких авторов, после прочтения необходимо выполнить несколько заданий и
упражнений самостоятельно, чтобы оценить степень усвоения материала.

Советы по подготовке к экзамену. Дополнительно к изучению конспектов лекции необходимо пользоваться любым рекомендованным учебником по программированию. Необходимо повторить методы решения различных задач, самостоятельно решить часть из них. Внимательно ознакомиться с примерами тестовых заданий.

Указания по организации работы с контрольно-измерительными материалами, по выполнению домашних заданий.
При выполнении домашних заданий необходимо сначала прочитать основные понятия и теоремы по теме задания. При выполнении задания нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, выбрать алгоритм решения задачи, попытаться запрограммировать. Если это не дало результатов, и необходимо рассмотреть решение подобных задач, и после этого попробовать решить предложенную задачу самостоятельно.

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. Microsoft Visual Studio (или CodeBloc) для выполнения лабораторных заданий
3. Лекционная мультимедийная аудитория для чтения лекций с использованием мультимедийных материалов.

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

При освоении дисциплины для выполнения лабораторных работ необходимы классы персональных компьютеров со средами программирования. Для проведения лекционных занятий, необходима мультимедийная аудитория с набором лицензионного базового программного обеспечения.

Лекционные занятия

- Видеопроектор, ноутбук, презентатор
- Подключение к сети Интернет