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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита персональных данных

Кафедра Информационных технологий и безопасности компьютерных систем факультета ИиИТ

Образовательная программа бакалавриата

10.03.01 Информационная безопасность

Направленность (профиль) программы:
Безопасность компьютерных систем

Уровень высшего образования:
бакалавриат

Форма обучения
Очная, очно-заочная

Статус дисциплины:
входит в часть формируемую участниками образовательных отношений ОПОП

Махачкала, 2022

Рабочая программа дисциплины «Защита персональных данных» составлена в 2022 г в соответствии с требованиями ФГОС ВО - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность» от 17 ноября 2020 г. N 1427

Составитель: Омарова М.А, преподаватель каф. ИТиБКС

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

Протокол № __8____ от ___16.03_____ 2022 г

Зав кафедрой ИТиБКС _____ Ахмедова З.Х.

Одобрена на заседании Методической комиссии факультета Информатики и информационных технологий от ____17.03_____ 2022 г протокол № __7____

Председатель _____ Бакмаев А.Ш.

Рабочая программа согласована с учебно-методическим управлением

«_31___» ____марта_____2022 г

Начальник УМУ _____ Гасангаджиева А.Г.

Аннотация рабочей программы дисциплины.

Дисциплина «Защита персональных данных» входит в часть формируемую участниками образовательных отношений образовательной программы бакалавриата по направлению 10.03.01 Информационная безопасность.

Формирование мирового информационного пространства определило высокую значимость информации, которая выступает главным продуктом современного производства. Информационные процессы затрагивают все стороны человеческой жизни. Документирование информации, ее поиск, обработка, хранение и передача являются важнейшим фактором существования современного социума, что, в свою очередь, определяет необходимость подготовки профессионально подготовленных специалистов для качественной работы с документированной информацией.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных - ОПК- 2, ОПК-10, ОПК-1.4, ПК-3, ПК-6. Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, самостоятельная работа.

Объем дисциплины 3 зачетные единицы, в том числе в академических часах по видам учебных занятий.

Объем дисциплины в очной форме

Семестр	Всего	Учебные занятия							Форма промежу-точной аттестации
		в том числе							
		Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		Всего	из них						
			Лекции	Лабораторные занятия	Практические занятия		консультации		
4	108	50	34		16			58	зачет

Объем дисциплины в очно-заочной форме

Семестр	Всего	Учебные занятия					Форма промежу-точной аттестации
		в том числе					
		Контактная работа обучающихся с преподавателем				СРС, в том числе экзамен	
		Всего	из них				
			Лекции	Лабораторные занятия	Практические занятия		
4	108	36	18		18	72	зачет

1.Цели освоения дисциплины.

Целью освоения дисциплины "Защита персональных данных" - формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

2. Место дисциплины в структуре ОПОП бакалавриата.

Дисциплина входит в часть формируемую участниками образовательных отношений ОПОП по направлению подготовки “Информационная безопасность”.

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-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИД.1 ОПК-2.1..Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. Ид2.ОПК-2.2.Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. ИД3.ОПК-2.3.Имеет навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	**Знать:** современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. **Уметь**: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. **Владеть:** навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	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 ИД 2 ОПК-10.2.Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности ИД 3 ОПК-10.3. Владеет принципами формирования политики информационной безопасности объекта информатизации	**Знать:** программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях. **Уметь:** конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности. **Владеть:** принципами формирования политики информационной безопасности объекта информатизации.	Круглый стол
ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями		**Знать:** основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных; основные виды угроз безопасности персональных данных в информационных системах персональных данных; содержание и порядок организации работ по выявлению угроз безопасности персональных данных. **Уметь:** создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных; планировать мероприятия по обеспечению безопасности персональных данных; обосновывать и задавать требования по обеспечению безопасности персональных	Устный опрос, письменный опрос

		данных в информационных системах персональных данных; проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. **Владеть:** навыками работы с правовыми базами данных; навыки определения уровней защищённости персональных данных; навыки выявления угроз безопасности персональных данных в информационных системах персональных данных; навыки разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных; навыки применения сертифицированных средств защиты информации.	
ПК-3. Способность готовить презентации, оформлять научно-технические отчеты по результатам выполненной работы, публиковать результаты исследований в виде статей и докладов на научно-технических конференциях.	ПК-3.1. Знает современные программные продукты по подготовке презентаций и оформлению научно-технических отчетов. ПК-3.2. Умеет готовить презентации и оформлять научные отчеты. ПК-3.3. Имеет навыки по подготовке статей и докладов на научно-технических конференциях.	**Знать:** современные программные продукты по подготовке презентаций и оформлению научно-технических отчетов. **Уметь:** готовить презентации и оформлять научные отчеты . **Владеть:** навыками по подготовки статей и докладов на научно-технических конференциях.	Устный опрос, письменный опрос
ПК-6. Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных	ПК-6.1. Знает архитектуру и принцип работы операционных систем семейства UNIX и Linux. ПК 6.2.Умеет выполнять работы по установке, настройке, отладке и обслуживанию операционных систем. ПК 6.3. Владеет навыками	**Знать:** архитектуру и принцип работы операционных систем семейства UNIX и Linux. **Уметь:** выполнять работы по установке, настройке, отладке и обслуживанию операционных систем. **Владеть:** навыками	Устный опрос, письменный опрос

спецификаций, систем управления базами данных	эффективного управления серверными операционными системами, конфигурирования корпоративных сервисов.	эффективного управления серверными операционными системами, конфигурирования корпоративных сервисов	

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 3 зачетные единицы, 108 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)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост.работы		
1	2								
Модуль I. Основы обработки и защиты персональных данных в информационных системах персональных данных									
1	Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации	4		2				8	Устный опрос
2	Принципы обработки персональных данных	4		2				8	Устный опрос
3	Трансграничная передача персональных данных	4		4	2			10	Устный опрос
	Итого за модуль:			8	2			26	
	Модуль II. Методы защиты информационных систем персональных данных.								
4	Требования к обеспечению безопасности	4		4	2			8	Устный опрос

	персональных данных при их обработке в информационных системах персональных данных								
5	Нормативно-методическое обеспечение безопасности информационных систем персональных данных	4		4				2	Устный опрос
6	Классификация информационных систем персональных данных	4		4	4			8	Письменный опрос
	Итого за модуль:			12	6			18	
	Модуль III. Обеспечение и оценка эффективности системы защиты информационных систем персональных данных.								
7	Модель угроз для информационных систем персональных данных	4		4	4			6	Устный опрос
8	Организация и обеспечение режимов защиты персональных данных	4		4	4			6	Устный опрос
9	Оценка эффективности системы защиты информационных систем персональных данных	4		4				4	Письменный опрос
	Итого за модуль:			12	8			16	
	Всего часов			**34**	**16**			**58**	**зачет**

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)		Самостоятельна	Формы текущего контроля успеваемости (по неделям семестра) Форма

				Лекции	Практические занятия	Лабораторные занятия	Контроль самост.работы		промежуточной аттестации
1	2								
Модуль I. Основы обработки и защиты персональных данных в информационных системах персональных данных									
1	Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации	4		2				8	Устный опрос
2	Принципы обработки персональных данных	4		2	2			8	Устный опрос
3	Трансграничная передача персональных данных	4		2	2			10	Устный опрос
	Итого за модуль:			6	4			26	
	Модуль II. Методы защиты информационных систем персональных данных.								
4	Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	4		2	2			16	Устный опрос
5	Нормативно-методическое обеспечение безопасности информационных систем персональных данных	4		2	2			12	Письменный опрос
	Итого за модуль:			4	4			28	
	Модуль III. Обеспечение и оценка эффективности системы защиты информационных систем персональных данных.								
6	Модель угроз для информационных систем персональных данных	4		2	2			10	Устный опрос
7	Организация и обеспечение режимов защиты персональных данных	4		2	2			10	Устный опрос

8	Оценка эффективности системы защиты информационных систем персональных данных	4		4	4				Письменный опрос
	Итого за модуль:			8	8			20	
	Всего часов			**18**	**18**			**72**	**зачет**

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

Модуль 1. Основы обработки и защиты персональных данных в информационных системах персональных данных.

1. Персональные данные в Федеральном законе и Трудовом кодексе Российской Федерации. Основные понятия и определения. Содержание категории «персональные данные». Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение.

2. Принципы обработки персональных данных. Принципы обработки персональных данных. Условия обработки персональных данных. Согласие субъекта. Обработка биометрических данных. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными. Специальные категории персональных данных и особенности их обработки. Права субъектов персональных данных и их соблюдение при обработке.

3. Трансграничная передача персональных данных. Обработка персональных данных третьим лицом в интересах оператора. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. Ответственность за нарушение требований по обращению с персональными данными.

Модуль 2. Методы защиты информационных систем персональных данных.

4. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Мероприятия по защите сведений конфиденциального характера, основные внутренние нормативные документы, меры по охране конфиденциальности; формирование перечня персональных данных. Ограничение доступа к персональным данным, учет лиц, допущенных к персональным данным, определение порядка обращения с такими сведениями, контроля над его соблюдением, организация доступа к персональным данным, внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие, контроль над соблюдением режима конфиденциальности.

5. Нормативно-методическое обеспечение безопасности информационных систем персональных данных. Руководящие документы ФСТЭК и ФСБ России по защите персональных данных. Нормативно-методическое обеспечение безопасности информационных систем персональных данных в органах власти, учреждениях (предприятиях). Порядок лицензирования операторов информационных систем персональных данных.

6. Классификация информационных систем персональных данных. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении

требований к защите персональных данных при их обработке в информационных системах персональных данных». Порядок проведения классификации информационных систем персональных данных.

Модуль 3. Обеспечение и оценка эффективности системы защиты информационных систем персональных данных.

7. Модель угроз для информационных систем персональных данных. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Модель злоумышленника информационных систем персональных данных. Разработка частных моделей угроз безопасности персональных данных в конкретных информационных системах персональных данных с учетом их назначения, условий и особенностей функционирования.

8. Организация и обеспечение режимов защиты персональных данных. Организационные и технические мероприятия, направленные на минимизацию ущерба от возможной реализации угроз безопасности персональных данных. Защита персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.

9. Оценка эффективности систем защиты информационных систем персональных данных. Мероприятия по оценке соответствия принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных требованиям безопасности информации. Мероприятия по контролю обеспечения безопасности персональных данных. Механизмы и средства

10 контроля. Периодичность и содержание работ. Ответственность оператора за нарушение правил обращения с персональными данными. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

4.3.2. План практических занятий

Темы семинарских занятий.

Модуль 1. Основы обработки и защиты персональных данных в информационных системах персональных данных.

1. Категории персональных данных. Определение категории персональных данных. Принципы и правила определения персональных данных к категории биометрических, специальных, общедоступных или иных.

2. Защищённая обработка персональных данных. Реализация защищённой автоматизированной обработки персональных данных в информационных системах персональных данных.

3. Распределённые информационные системы персональных данных. Организация системы защиты распределённой информационной системы персональных данных.

Модуль 2. Методы защиты информационных систем персональных данных.

4. Разграничение прав доступа в информационных системах персональных данных. Реализация механизмов разграничения доступа в информационной системе персональных данных.

5. Нормативно-правовой подход к защите информационной системы персональных данных. Подготовка пакета документов, необходимого для аттестации информационной системы персональных данных в соответствии с законодательством и нормативно-правовой базой Российской Федерации.

6. Классификация информационных систем персональных данных. Определение уровня защищённости информационных систем персональных данных в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 г. Москва «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Модуль 3. Обеспечение и оценка эффективности системы защиты информационных систем персональных данных.

7. Модель угроз для информационных систем персональных данных. Разработка модели угроз для информационных систем персональных данных. Разработка частной модели угроз информационной системы персональных данных.

8. Организация и обеспечение режимов защиты персональных данных. Обеспечение защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.

9. Оценка эффективности систем защиты информационных систем персональных данных. Определение и оценка эффективности систем защиты информационных систем персональных данных в соответствии с законодательством и нормативно-правовой базой Российской Федерации.

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 видов документов и реквизитов в презентациях.

Практические занятия

- Традиционные технологии

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	Особенности защиты персональных данных при их обработке в государственных информационных системах	доклад

2	Подготовка объекта к аттестации. Типовые формы документов. Изучение методов обезличивания персональных данных.	опрос
3	Особенности организации обработки персональных данных в государственных информационных системах. Постановление Правительства РФ от 21.03.2012 г. №211 (с изм.). Обезличивание персональных данных при их обработке в ГИС. Аттестация ГИС.	опрос доклад
4	Регуляторы в области защиты персональных данных. Проверки Роскомнадзора. Проверки ФСБ. Проверка ФСТЭК.	опрос доклад
5	Этап внедрения. Обучение персонала. Установка, настройка, учет и контроль СЗИ. Описание системы защиты персональных данных. Проверка эффективности СЗПДн.	опрос доклад

Рекомендуемая литература				
. Основная литература				
	Авторы	**Заглавие**	**Издательство, год**	**Эл. адрес**
1	Петренко В. И.	Защита персональных данных в информационных системах: Учебники и учебные пособия для ВУЗов	СКФУ, 2016 // ЭБС "Университетская библиотека online"	http://biblioclub.ru/index.php?page=book_red&id=459205
6.1.2. Дополнительная литература				
	Авторы	**Заглавие**	**Издательство, год**	**Эл. адрес**
2	Ахрамеева О.В., Дедюхина И.Ф., Жданова О.В. и др.	Правовое регулирование информационных отношений в области государственной и коммерческой тайны, персональных данных: Учебники и учебные пособия для ВУЗов	Ставропольский государственный аграрный университет, 2015 // ЭБС "Университетская библиотека online"	http://biblioclub.ru/index.php?page=book_red&id=438603

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

7.1. Типовые контрольные задания или иные материалы

Примерные темы докладов:

1. Биометрические системы аутентификации. Статические и динамические методы. Дактилоскопия по фотографиям рук; распознавание по сетчатке глаза и (или) по радужной оболочке по фотографиям глаз; распознавание по геометрии лица по фотографиям лиц.
2. Хранение и обработка персональных медицинских данных. Особенности защиты персональных данных в медицинской отрасли. Защита врачебной тайны.

3. Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.
4. Стандарт OpenId. Аутентификация и авторизация через открытый протокол OAuth. Безопасность при аутентификации и авторизации на сайтах по OpenID.
5. Государственные информационные системы (ГИС). Проблемы классификации ГИС. Аспекты классификации государственных информационных систем с точки зрения Федеральных законов №149 и №242.
6. Трансграничная передача ПДн. Ответственность за нарушение правил трансграничной передачи. "Адекватная" защита прав субъектов персональных данных.
7. Законность видеосъемки, фотосъемки и звукозаписи в общественных местах. Охрана изображения гражданина. Нарушение неприкосновенности частной жизни. Статья 137 УК РФ, статьи 151, 152, 152.1 Гражданского Кодекса РФ.
8. Уничтожение электронных данных. Уровни уничтожения электронных данных (очистка, очищение, разрушение). Стандартизация уничтожения электронных данных.
9. Хранение ПДн в «облаке». Необходимые свойства «облака» для построения «облачной» ИСПДн. Требования регулирующих органов по защите ИСПДн в «облаке».
10. Защита персональных данных в мобильных устройствах. Проблемы приватности данных, хранящихся на мобильных устройствах. Защитные механизмы мобильных операционных систем и приложений.

Вопросы к зачёту:

1) Определение персональных данных (ПДн) и информационной системы персональных данных.
2) Нормативно-правовая база в сфере защиты и обработки ПДн (№ 149-ФЗ, № 152-ФЗ).
3) Категории персональных данных.
4) Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5) Уровни защищённости информационных систем персональных данных.
6) Процесс подготовки пакета документов к аккредитации ИСПДн: обязательство о неразглашении информации, содержащей ПДн; согласие на обработку ПДн; перечень ИСПДн.
7) Процесс подготовки пакета документов к аккредитации ИСПДн: перечень ПДн, обрабатываемых и хранящихся в ИСПДн; положение об обработки ПДн работников; акт определения уровня защищённости ИСПДн.
8) Принципы обеспечения безопасности ПДн.
9) Обезличивание ПДн. Абсолютное обезличивание и относительное обезличивание.
10) Нормативно-правовая база в области обезличивания ПДн (Приказ Роскомнадзора от 5 сентября 2013 г. №996 «Об утверждении требований и методов по обезличиванию ПДн»).
11) Свойства обезличенных данных.
12) Свойства методов обезличивания.
13) Методы обезличивания персональных данных. Сравнительный анализ методов обезличивания.
14) Алгоритм перемешивания данных в общем виде.
15) Формальное описание алгоритма обезличивания ПДн методом перемешивания с помощью циклических перестановок.

16) Анализ эффективности алгоритма перемешивания ПДн с помощью циклических перестановок.
17) Определение политик безопасности (ПБ). Представление ПБ.
18) Закрытые, открытые, гибридные политики информационной безопасности.
19) Методы описания ПБ. Сравнительный анализ методов описания ПБ.
20) Аналитический метод описания ПБ.
21) Графовый метод описания ПБ.
22) Объектный метод описания ПБ.
23) Логический метод описания ПБ.
24) Пример графового метода описания ПБ: визуальный язык объектных ограничений «Language on Objects for Security Constraints» (LaSCO).
25) Определение графа атак. Формальное описание построения модели графа атак.
26) Анализ графа атак. Модель злоумышленника.
27) Определение гарантированной (верифицируемой) защиты.
28) Методы обеспечения гарантированности защиты.
29) Каналы несанкционированного доступа, утечки информации и деструктивных воздействий на информационную среду (НСДУВ).
30) Вероятностная оценка реализации канала НСДУВ.

7.2. 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 зачет.

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

а) основная литература:

Основная литература: 1. Башлы, П.Н. Информационная безопасность и защита информации: Учебник [Электронный ресурс] / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – М.: РИОР, 2013. – 222 с. – Режим доступа: http://znanium.com/bookread.php?book=405000 (дата обращения 01.09.2022); 2. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие [электронный ресурс] / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ 23 ИНФРА-М, 2013. – 592 с. – Режим доступа: http://znanium.com/bookread.php?book=402686 (дата обращения 01.09.2022). 12.2. Дополнительная литература: 3. Бабаш, А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. – 2-е изд. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 216 с. – Режим доступа: http://znanium.com/bookread.php?book=432654 (дата обращения 01.09.2022); 4. Дубинин, Е.А. Оценка относительного ущерба безопасности информационной системы: Монография [электронный ресурс] / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 192 с. – Режим доступа: http://znanium.com/bookread.php?book=471787 (дата обращения 01.09.2022);

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

1.ФСБ России [Электронный ресурс]. – Режим доступа: http://fsb.ru (дата обращения 01.09.2022);

2. ФСТЭК России [Электронный ресурс]. – Режим доступа: http://fstec.ru (дата обращения 01.09.2022). 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 зачету. 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. Лекционная мультимедийная аудитория для чтения лекций с использованием мультимедийных материалов.

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

Для проведения лекционных занятий, необходима

- Свободно распространяемая система виртуализации Virtual Box;
- Операционная система Linux;
- Операционная система Windows;
- Среда разработки MS Visual Studio;
- СУБД MS SQL Server.