МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет компьютерных технологий и прикладной математики

подпись

«27» мая 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1. О.01 «Теория и практика передачи и защиты информации»

Направление подготовки 09.04.02 Информационные системы и технологии

Направленность (профиль) Искусственный интеллект и машинное обучение

Форма обучения очно-заочная

Квалификация магистр

Краснодар 2022

Рабочая программа дисциплины «Теория и практика передачи и защиты информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 09.04.02 Информационные системы и технологии.

Программу составил:

Осипян В. О. проф., д. физ.-мат. наук, доцент

Рабочая программа дисциплины утверждена на заседании кафедры анализа данных и искусственного интеллекта протокол №10 от 18 мая 2022 г.
Заведующий кафедрой (разработчика)
Коваленко А.В., д. тех. н., доцент

Рабочая программа обсуждена на заседании кафедры анализа данных и искусственного интеллекта протокол №10 от 18 мая 2022 г.
Заведующий кафедрой (выпускающей)
Коваленко А.В., д. тех. н., доцент

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол №6 от 25 мая 2022 г.
Председатель УМК факультета
А. В. Коваленко

Рецензенты:
Бегларян М. Е., зав. кафедрой социально-гуманитарных и естественнонаучных дисциплин СКФ ФГБОУВО «Российский государственный университет
правосудия», канд. физ.-мат. наук, доцент

Рубцов Сергей Евгеньевич, кандидат физико-математических наук, доцент кафедры математического моделирования ФГБГОУ «КубГУ»

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Цель освоения дисциплины «Теория и практика передачи и защита информации» – формирование у студентов основ знаний об информационной безопасности, роли и внедрении информации в современном обществе; изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.2 Задачи дисциплины

Основными задачами изучения дисциплины являются:

– систематизация, формализация и расширение знаний по основным положениям защиты информации, криптографии и информационной безопасности;

– обучение студентов приемам работы с современным программным обеспечением для практического освоения принципов и методов обеспечения информационной безопасности;

– формирование комплексных знаний об основных тенденциях развития технологий, связанных с обеспечением информационной безопасности;

– формирование практических навыков применения средств защиты информации при решении профессиональных задач.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Теория и практика передачи и защита информации» относится к «Обязательная часть» Блока 1 «Дисциплины (модули)» учебного плана.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

УК-2 **Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений**

Знать

ИУК-2.1 (С/16.6 Зн.1) Языки программирования и работы с базами данных, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.2 (С/16.6 Зн.3) Инструменты и методы верификации структуры программного кода, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.16 (А/01.5 Зн.1) Цели и задачи проводимых исследований и разработок в рамках поставленной цели, методы выбира оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.18 (А/01.5 Др.1 Зн.)Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Уметь ИУК-2.19 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.20 (A/01.5 У.1) Применять нормативную документацию в соответствующей области знаний, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.21 (A/01.5 У.3) Применять методы анализа научно-технической информации, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Владеть ИУК-2.27 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта, в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ОПК-2 Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

Знать

ИОПК-2.1 (D/03.6 Зн.3) Методы и средства проектирования программного обеспечения, оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры и оценки качества программного кода

ИОПК-2.3 (C/16.6 Зн.4) Возможности ИС в различных областях человеческой деятельности

ИОПК-2.4 (C/16.6 Зн.8) Основы программирования, проектирования, разработки, реализации и оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.5 (C/16.6 Зн.14) Современный отечественный и зарубежный опыт, современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.6 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.7 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.8 (A/01.5 Зн.4) Методы проведения экспериментов и наблюдений, обобщения и обработки информации, связанной с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.9 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач на основе современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

Уметь

ИОПК-2.10 (C/16.6 У.2) Верифицировать структуру программного кода, применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.11 (A/27.6 У.1) Анализировать входные данные, применять современный математический аппарат, связанный с проектированием, разработкой и реализацией программных продуктов и программных комплексов в различных областях человеческой деятельности

Владеть ИОПК-2.13 (С/16.6 Тд.2) Верификация структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС, оценка качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.15 (А/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта при разработке программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.16 (А/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в соответствующей области знаний, использование современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ПК-1 Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий

Знать ИПК-1.1 (D/03.6 Зн.2) Типовые решения, математические модели, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения

ИПК-1.3 (С/16.6 Зн.2) Инструменты и методы проектирования и дизайна ИС

ИПК-1.4 (С/16.6 Зн.5) Предметная область автоматизации

ИПК-1.5 (С/16.6 Зн.8) Основы программирования и информационных технологий

ИПК-1.8 (А/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.9 (А/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.10 (А/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач в области знания математических и естественных наук, программирования и информационных технологий

Уметь ИПК-1.11 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения на основе знаний и моделей математических и естественных наук

ИПК-1.13 (А/27.6 У.1) Анализировать входные данные

ИПК-1.14 (А/01.5 У.3) Применять методы анализа научно-технической информации с использованием базовых знаний математических и естественных наук, программирования и информационных технологий

Владеть ИПК-1.15 (D/03.6 Тд.2) Проектирование структур данных, построение математических моделей

ИПК-1.16 (А/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в области знаний математических и естественных наук, программирования и информационных технологий

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72часов), их распределение по видам работ представлено в таблице

Вид учебной работы		Всего часов	Семестры (часы)					
			1					
Контактная работа, в том числе:		**30,2**	**30,2**					
Аудиторные занятия (всего):		**36**	**36**					
Занятия лекционного типа		**36**	**36**					
Лабораторные занятия								
Занятия семинарского типа (семинары, практические занятия)								
Иная контактная работа:		**2,2**	**2,2**					
Контроль самостоятельной работы (КСР)		**2**	2					
Промежуточная аттестация (ИКР)		**0,2**	0,2					
Самостоятельная работа, в том числе:		**35,8**	**35,8**					
Курсовая работа								
Проработка учебного (теоретического) материала		**5**	5					
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		**10**	10					
Реферат		**10**	10					
Подготовка к текущему контролю		**8**	8					
Контроль:								
Подготовка к экзамену								
Общая трудоемкость	**час.**	**72**	**72**					
	в том числе контактная работа	**30,2**	**30,2**					
	зач. ед	**2**	**2**					

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые в 8 семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Информация и неопределённость. Численная мера неопределённости	2	2			

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7

2.	Алгебраическая система **<A, F, R>** с заданными отношениями	3	3			
3.	Общая схема передачи, хранения и защиты информации. Кодирование информации.	2	2			
4.	Линейное кодирование. Свойства и способы задания линейных кодов	3	3			
5.	Основные решаемые проблемы криптографией и криптологией. Криптостойкость шифра. Принцип Керкхоффса	3	3			
6.	Математическое моделирование систем защиты информации (ВОО_СЗИ)	2	2			
7.	Методы моноалфавитных (многоалфавитных) подстановок и перестановок Применение логических функций в криптографии. Хеш-функции	3	2			
8.	Современные методы решения проблемы передачи ключей. Алгоритм генерации ключа для цифровой подписи	3	3			
9.	Аддитивная группа точек эллиптической кривой	4	2			
10.	Рюкзачная криптосистема на основе кода Варшамова	3	3			
11.	Системы ЭЦП. Установление подлинности и целостности данных	3	3			
12.	Диофантовы уравнения. Десятая проблема Гильберта. ДБК	4	3			
13.						
14.						

ИТОГО по разделам дисциплины	**32**				
Контроль самостоятельной работы (КСР)	4				
Промежуточная аттестация (ИКР)	0,2				
Подготовка к текущему контролю	12				
Общая трудоемкость по дисциплине	**72**				

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
1.	Информация и неопределённость.	Количественная мера неопределённости. Условная неопределённость. Количество	К, Т

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
	Численная мера неопределённости	информации. Формулы Р. Хартли и К. Шеннона. Передача информации	
2.	Алгебраическая система **<A, F, R>** с заданными отношениями	Алгебраические операции и системы. Классификация алгебраических систем в современной алгебре в соответствии с усложнением их математической структуры: группа, кольцо, поле.	К, Т
3.	Общая схема передачи, хранения и защиты информации. Кодирование информации.	Общая схема передачи, хранения и защиты информации. Построение функций шифрования. Односторонние функции. Кодирование информации.	К, Т
4.	Линейное кодирование. Свойства и способы задания линейных кодов	Линейное кодирование. Свойства и способы задания линейных кодов. Примеры кодов. Коды Хэмминга, БЧХ. Нелинейные коды. Коды Адамара. Границы мощности кодов	К, Т
5.	Основные решаемые проблемы криптографией и криптологией. Криптостойкость шифра. Принцип Керкхоффса	Основные решаемые проблемы криптографией и криптологией. Криптостойкость шифра. Примеры криптосистем. Принцип Керкхоффса	К, Т
6.	Математическое моделирование систем защиты информации (ВОО_СЗИ)	Математическое моделирование систем защиты информации (ВОО_СЗИ).	К, Т

7.	Методы моноалфавитных (многоалфавитных) подстановок и перестановок. Применение логических функций в криптографии. Хеш-функции	Методы моноалфавитных (многоалфавитных) подстановок и перестановок. Метод гаммирования. . Метод блочных шифр. Применение логических функций в криптографии. Хеш-функции	К, Т
8.	Современные методы решения проблемы передачи ключей. Алгоритм генерации ключа для цифровой подписи	Современные методы решения проблемы передачи ключей. Протокол ДиффиХеллмана. Алгоритм генерации ключа для цифровой подписи	К, Т
9.	Аддитивная группа точек эллиптической кривой	Аддитивная группа точек эллиптической кривой. Количество точек эллиптической кривой. Примеры.	К, Т
10.	Рюкзачная криптосистема на основе кода Варшамова	Рюкзачная криптосистема на основе кода Варшамова. Система защиты информации на основе заданного рюкзака. Рюкзачные асимметричные и симметричные системы	К, Т
11.	Системы ЭЦП. Установление подлинности и целостности данных	Вопросы установления подлинности. Системы электронной подписи. Аутентикация данных Реализация цифровой подписи на основе криптосистемы Эль-Гамаля.	К, Т
№	**Наименование раздела (темы)**	**Содержание раздела (темы)**	**Форма текущего контроля**
1	**2**	**3**	**4**
		Установление подлинности и целостности данных.	
12.	уравнения. проблема Диофантовы Десятая Гильберта. ДБК	Диофантовы уравнения. Десятая проблема Гильберта. ДБК 3. Математические модели алфавитных криптосистем, содержащих диофантовы трудности. Модель криптосистемы на основе теоремы Эйлера–Ферма. Математическое моделирование криптосистем методом гаммирования, содержащих диофантовы трудности. Математическая модель криптосистемы на основе диофантова уравнения первой степени. Метод параметризации однородных многостепенных систем диофантовых уравнений второй степени и математическое моделирование СЗИ на их основе. Разработка математических моделей систем защиты информации на основе многостепенных систем	К, Т

		диофантовых уравнений	
			К, Т
			К, Т

Примечание: ЛР – отчет/защита лабораторной работы, КП - выполнение курсового проекта, КР - курсовой работы, РГЗ - расчетно-графического задания, Р - написание реферата, Э - эссе, К - коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.2 Занятия семинарского типа

Примечание: ЛР – отчет/защита лабораторной работы, КП - выполнение курсового проекта, КР - курсовой работы, РГЗ - расчетно-графического задания, Р - написание реферата, Э - эссе, К - коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.3 Лабораторные занятия

№	Наименование раздела (темы)	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

9.			
10.			
11.			
№	**Наименование раздела (темы)**	**Наименование лабораторных работ**	**Форма текущего контроля**
1	**2**	**3**	**4**
12.			
13.			
14.			

Примечание: ЛР – отчет/защита лабораторной работы, КП - выполнение курсового проекта, КР - курсовой работы, РГЗ - расчетно-графического задания, Р - написание реферата, Э - эссе, К - коллоквиум, Т – тестирование, РЗ – решение задач.

2.3.4 Примерная тематика курсовых работ (проектов) - не предусмотрены

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Изученние теоретического материала	Методические указания по организации самостоятельной работы студентов, утвержденные кафедрой информационных технологий, протокол №1 от 30.08.2019
2	Решение задач	Методические указания по организации самостоятельной работы студентов, утвержденные кафедрой информационных технологий, протокол №1 от 30.08.2019

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

– в форме аудиофайла,

– в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа, – в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В соответствии с требованиями ФГОС в программа дисциплины предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; метод малых групп, разбор практических задач и кейсов.

При обучении используются следующие образовательные технологии:

- Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.
- Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал. Создание и использование диагностических тестов является неотъемлемой частью данной технологии.
- Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.
- Информационно-коммуникационные технологии (ИКТ) - расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы учащихся и повышению познавательной активности. В рамках ИКТ выделяются 2 вида технологий:
- Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения языку на всех уровнях.
- Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.
- Технология индивидуализации обучения – помогает реализовывать личностноориентированный подход, учитывая индивидуальные особенности и потребности учащихся.
- Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.
- Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.
- Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого учащегося.
- Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеназванных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные

процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Основные виды интерактивных образовательных технологий включают в себя:

− работа в малых группах (команде) - совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путём творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности;

− проектная технология - индивидуальная или коллективная деятельность по отбору, распределению и систематизации материала по определенной теме, в результате которой составляется проект;

− анализ конкретных ситуаций - анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений;

− развитие критического мышления – образовательная деятельность, направленная на развитие у студентов разумного, рефлексивного мышления, способного выдвинуть новые идеи и увидеть новые возможности.

Подход разбора конкретных задач и ситуаций широко используется как преподавателем, так и студентами во время лекций, лабораторных занятий и анализа результатов самостоятельной работы. Это обусловлено тем, что при исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Семестр	**Вид занятия**	**Используемые интерактивные образовательные технологии**	**количество интерактивных часов**
8	ЛР	Практические занятия в режимах взаимодействия «преподаватель – студент» и «студент – студент»	8
Итого			**8**

Примечание: Л – лекции, ПЗ – практические занятия/семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и практических занятий.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом, – в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные и методические материалы

4.1 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «название дисциплины».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме тестовых заданий, доклада-презентации по проблемным вопросам, разноуровневых заданий, ролевой игры, ситуационных задач и **промежуточной аттестации** в форме вопросов и заданий к зачету.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом, – в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Контролируемые разделы (темы) дисциплины*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	Информация и неопределённость. Численная мера неопределённости	**УК-1** ИУК-1.3 (D/03.6 Тд.5) **ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.2 (D/03.6 Зн.3) ИПК-4.5 (C/16.6 Зн.2) ИПК-4.9 (C/16.6 Зн.10) ИПК-4.10 (C/16.6 Зн.11) ИПК-4.19 (A/01.5 Зн.3) ИПК-4.24 (C/16.6 У.1) ИПК-4.30 (A/01.5 Тд.2) **ПК-6** ИПК-6.1 (D/03.6 Зн.2) ИПК-6.5 (C/16.6 Зн.4) ИПК-6.7 (C/16.6 Зн.8) ИПК-6.8 (C/16.6 Зн.9) ИПК-6.9 (C/16.6 Зн.10) ИПК-6.14 (C/16.6 Тд.1)	Типовые контрольные вопросы 1 Типовые контрольные задания 1-12	Вопрос на зачете1-2 Задание для самостоятельной работы
2	Алгебраическая система **<A, F, R>** с заданными отношениями	**УК-1** ИУК-4.11 (D/03.6 Тд.1) ИУК-4.13 (C/16.6 Тд.2) **ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.2 (D/03.6 Зн.3) ИПК-4.5 (C/16.6 Зн.2) ИПК-4.6 (C/16.6 Зн.3) ИПК-4.17 (A/01.5 Зн.1) ИПК-4.19 (A/01.5 Зн.3) **ПК-6** ИПК-6.1 (D/03.6 Зн.2)	Типовые контрольные вопросы 2-3 Типовые контрольные задания 1-12	Вопрос на зачете2-3 Задание для самостоятельной работы
		ИПК-6.9 (C/16.6 Зн.10) ИПК-6.14 (C/16.6 Тд.1)		

3	Общая схема передачи, хранения и защиты информации. Кодирование информации.	**УК-1** ИУК-4.1 (С/16.6 Зн.11) ИУК-4.8 (D/03.6 У.3) ИУК-4.11 (D/03.6 Тд.1) ИУК-4.13 (С/16.6 Тд.2) **ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.4 (D/03.6 Зн.5) ИПК-4.5 (С/16.6 Зн.2) ИПК-4.21 (А/01.5 Др.1 Зн.) ИПК-4.22 (D/03.6 У.1) ИПК-4.24 (С/16.6 У.1) ИПК-4.27 (D/03.6 Тд.2) ИПК-4.28 (D/03.6 Тд.4) **ПК-6** ИПК-6.2 (D/03.6 Зн.5) ИПК-6.4 (С/16.6 Зн.2) ИПК-6.6 (С/16.6 Зн.5) ИПК-6.10 (D/03.6 У.1) **ИПК-6.13 (D/03.6 Тд.4)**	Типовые контрольные вопросы 4-6 Типовые контрольные задания 1-12	Вопрос на зачете5-7 Задание для самостоятельной работы
4	Линейное кодирование. Свойства и способы задания линейных кодов	**УК-1** ИУК-4.1 (С/16.6 Зн.11) ИУК-4.8 (D/03.6 У.3) **ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.4 (D/03.6 Зн.5) ИПК-4.5 (С/16.6 Зн.2) ИПК-4.21 (А/01.5 Др.1 Зн.) ИПК-4.28 (D/03.6 Тд.4) **ПК-6** ИПК-6.2 (D/03.6 Зн.5) ИПК-6.10 (D/03.6 У.1) **ИПК-6.13 (D/03.6 Тд.4)**	Типовые контрольные вопросы 7-11 Типовые контрольные задания 1-12	Вопрос на зачете8-10 Задание для самостоятельной работы
5	Основные решаемые проблемы криптографией и криптологией. Криптостойкость шифра. Принцип Керкхоффса	**ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.4 (D/03.6 Зн.5) ИПК-4.5 (С/16.6 Зн.2) ИПК-4.21 (А/01.5 Др.1 Зн.) ИПК-4.27 (D/03.6 Тд.2) ИПК-4.28 (D/03.6 Тд.4) **ПК-6** ИПК-6.2 (D/03.6 Зн.5) ИПК-6.4 (С/16.6 Зн.2) ИПК-6.6 (С/16.6 Зн.5) ИПК-6.10 (D/03.6 У.1) ИПК-6.12 (D/03.6 Тд.2) **ИПК-6.13 (D/03.6 Тд.4)**	Типовые контрольные вопросы 1220 Типовые контрольные задания 1-12	Вопрос на зачете11-14 Задание для самостоятельной работы

6	Математическое моделирование систем защиты информации (ВОО_СЗИ)	**ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.4 (D/03.6 Зн.5) ИПК-4.5 (C/16.6 Зн.2) ИПК-4.21 (A/01.5 Др.1 Зн.) ИПК-4.22 (D/03.6 У.1) ИПК-4.28 (D/03.6 Тд.4) **ПК-6**	Типовые контрольные вопросы 21 Типовые контрольные задания 1-12	Вопрос на зачете15-16 Задание для самостоятельной работы

		ИПК-6.1 (D/03.6 Зн.2) ИПК-6.2 (D/03.6 Зн.5) ИПК-6.6 (C/16.6 Зн.5) ИПК-6.10 (D/03.6 У.1) **ИПК-6.14 (C/16.6 Тд.1)**		
7	Методы моноалфавитных (многоалфавитных) подстановок и перестановок. Применение логических функций в криптографии. Хеш-функции	**УК-1** ИУК-4.11 (D/03.6 Тд.1) **ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.2 (D/03.6 Зн.3) ИПК-4.17 (A/01.5 Зн.1) ИПК-4.18 (A/01.5 Зн.2) ИПК-4.24 (C/16.6 У.1) **ПК-6** ИПК-6.8 (C/16.6 Зн.9) ИПК-6.10 (D/03.6 У.1) **ИПК-6.11 (D/03.6 У.2)**	Типовые контрольные вопросы 2224 Типовые контрольные задания 13-14	Вопрос на зачете17-18 Задание для самостоятельной работы
8	Современные методы решения проблемы передачи ключей. Алгоритм генерации ключа для цифровой подписи	УК-1 ИУК-4.11 (D/03.6 Тд.1) ПК-4 ИПК-4.1 (D/03.6 Зн.2) ИПК-4.2 (D/03.6 Зн.3) ИПК-4.7 (C/16.6 Зн.5) ИПК-4.17 (A/01.5 Зн.1) ИПК-4.18 (A/01.5 Зн.2) ИПК-4.23 (D/03.6 У.2) ИПК-4.27 (D/03.6 Тд.2) ИПК-4.32 (A/01.5 Тд.5) ПК-6 ИПК-6.3 (C/16.6 Зн.1) ИПК-6.11 (D/03.6 У.2) **ИПК-6.12 (D/03.6 Тд.2)**	Типовые контрольные вопросы 2526 Типовые контрольные задания 15-18	Вопрос на зачете19-20 Задание для самостоятельной работы

9	Аддитивная группа точек эллиптической кривой	**ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.2 (D/03.6 Зн.3) ИПК-4.6 (C/16.6 Зн.3) ИПК-4.9 (C/16.6 Зн.10) ИПК-4.17 (A/01.5 Зн.1) ИПК-4.19 (A/01.5 Зн.3) ИПК-4.20 (A/01.5 Зн.4) ИПК-4.24 (C/16.6 У.1) ИПК-4.25 (C/16.6 У.2) ИПК-4.26 (A/01.5 У.3) ИПК-4.30 (A/01.5 Тд.2) **ПК-6** ИПК-6.8 (C/16.6 Зн.9) ИПК-6.11 (D/03.6 У.2) **ИПК-6.14 (C/16.6 Тд.1)**	Типовые контрольные вопросы 2728 Типовые контрольные задания 15-18	Вопрос на зачете21-22 Задание для самостоятельной работы
10	Рюкзачная криптосистема на основе кода Варшамова	**ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.2 (D/03.6 Зн.3) ИПК-4.6 (C/16.6 Зн.3) ИПК-4.17 (A/01.5 Зн.1) ИПК-4.20 (A/01.5 Зн.4) ИПК-4.24 (C/16.6 У.1) ИПК-4.32 (A/01.5 Тд.5) **ПК-6** ИПК-6.8 (C/16.6 Зн.9) **ИПК-6.11 (D/03.6 У.2)**	Типовые контрольные вопросы 2930 Типовые контрольные задания 19-23	Вопрос на зачете23-25 Задание для самостоятельной работы
11	Системы ЭЦП. Установление подлинности и целостности данных	**ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.2 (D/03.6 Зн.3) ИПК-4.17 (A/01.5 Зн.1)	Типовые контрольные вопросы 31	Вопрос на зачете26-30 Задание для самостоятельной работы
		ИПК-4.32 (A/01.5 Тд.5)	Типовые контрольные задания 19-23	
12	Диофантовы уравнения. Десятая проблема Гильберта. ДБК	**УК-1** ИУК-4.1 (C/16.6 Зн.11) ИУК-4.11 (D/03.6 Тд.1) **ПК-3** ИПК-4.1 (D/03.6 Зн.2) ИПК-4.2 (D/03.6 Зн.3) ИПК-4.5 (C/16.6 Зн.2) ИПК-4.6 (C/16.6 Зн.3) ИПК-4.17 (A/01.5 Зн.1) ИПК-4.26 (A/01.5 У.3) **ПК-6** **ИПК-6.8 (C/16.6 Зн.9)**	Типовые контрольные вопросы 3233 Типовые контрольные задания 19-23	Вопрос на зачете 3133 Задание для самостоятельной работы

Показатели, критерии и шкала оценки сформированных компетенций

Соответствие **пороговому уровню** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **удовлетворительно /зачтено**):

УК-2 **Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений**

Знать

ИУК-2.1 (С/16.6 Зн.1) Языки программирования и работы с базами данных, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.2 (С/16.6 Зн.3) Инструменты и методы верификации структуры программного кода, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.16 (А/01.5 Зн.1) Цели и задачи проводимых исследований и разработок в рамках поставленной цели, методы выбира оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.18 (А/01.5 Др.1 Зн.)Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Уметь

ИУК-2.19 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.20 (А/01.5 У.1) Применять нормативную документацию в соответствующей области знаний, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.21 (А/01.5 У.3) Применять методы анализа научно-технической информации, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Владеть

ИУК-2.27 (А/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта, в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ОПК-2 **Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности**

Знать ИОПК-2.1 (D/03.6 Зн.3) Методы и средства проектирования программного обеспечения, оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры и оценки качества программного кода

ИОПК-2.3 (C/16.6 Зн.4) Возможности ИС в различных областях человеческой деятельности

ИОПК-2.4 (C/16.6 Зн.8) Основы программирования, проектирования, разработки, реализации и оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.5 (C/16.6 Зн.14) Современный отечественный и зарубежный опыт, современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.6 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.7 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.8 (A/01.5 Зн.4) Методы проведения экспериментов и наблюдений, обобщения и обработки информации, связанной с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.9 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач на основе современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

Уметь ИОПК-2.10 (C/16.6 У.2) Верифицировать структуру программного кода, применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.11 (A/27.6 У.1) Анализировать входные данные, применять современный математический аппарат, связанный с проектированием, разработкой и реализацией программных продуктов и программных комплексов в различных областях человеческой деятельности

Владеть ИОПК-2.13 (C/16.6 Тд.2) Верификация структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС, оценка качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.15 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта при разработке программных

продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в соответствующей области знаний, использование современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ПК-1 Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий

Знать

ИПК-1.1 (D/03.6 Зн.2) Типовые решения, математические модели, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения

ИПК-1.3 (C/16.6 Зн.2) Инструменты и методы проектирования и дизайна ИС

ИПК-1.4 (C/16.6 Зн.5) Предметная область автоматизации

ИПК-1.5 (C/16.6 Зн.8) Основы программирования и информационных технологий

ИПК-1.8 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.9 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.10 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач в области знания математических и естественных наук, программирования и информационных технологий

Уметь

ИПК-1.11 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения на основе знаний и моделей математических и естественных наук

ИПК-1.13 (A/27.6 У.1) Анализировать входные данные

ИПК-1.14 (A/01.5 У.3) Применять методы анализа научно-технической информации с использованием базовых знаний математических и естественных наук, программирования и информационных технологий

Владеть

ИПК-1.15 (D/03.6 Тд.2) Проектирование структур данных, построение математических моделей

ИПК-1.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в области знаний математических и естественных наук, программирования и информационных технологий

Соответствие **базовому уровню** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **хорошо /зачтено**):

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Знать ИУК-2.1 (С/16.6 Зн.1) Языки программирования и работы с базами данных, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.2 (С/16.6 Зн.3) Инструменты и методы верификации структуры программного кода, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.16 (А/01.5 Зн.1) Цели и задачи проводимых исследований и разработок в рамках поставленной цели, методы выбира оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.18 (А/01.5 Др.1 Зн.)Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Уметь ИУК-2.19 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.20 (А/01.5 У.1) Применять нормативную документацию в соответствующей области знаний, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИУК-2.21 (А/01.5 У.3) Применять методы анализа научно-технической информации, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Владеть ИУК-2.27 (А/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта, в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ОПК-2 Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

Знать

ИОПК-2.1 (D/03.6 Зн.3) Методы и средства проектирования программного обеспечения, оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры и оценки качества программного кода

ИОПК-2.3 (C/16.6 Зн.4) Возможности ИС в различных областях человеческой деятельности

ИОПК-2.4 (C/16.6 Зн.8) Основы программирования, проектирования, разработки, реализации и оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.5 (C/16.6 Зн.14) Современный отечественный и зарубежный опыт, современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.6 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.7 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.8 (A/01.5 Зн.4) Методы проведения экспериментов и наблюдений, обобщения и обработки информации, связанной с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.9 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач на основе современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

Уметь

ИОПК-2.10 (C/16.6 У.2) Верифицировать структуру программного кода, применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.11 (A/27.6 У.1) Анализировать входные данные, применять современный математический аппарат, связанный с проектированием, разработкой и реализацией программных продуктов и программных комплексов в различных областях человеческой деятельности

Владеть ИОПК-2.13 (C/16.6 Тд.2) Верификация структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС, оценка качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.15 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта при разработке программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в соответствующей области знаний, использование современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ПК-1 Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий

Знать ИПК-1.1 (D/03.6 Зн.2) Типовые решения, математические модели, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения

ИПК-1.3 (C/16.6 Зн.2) Инструменты и методы проектирования и дизайна ИС

ИПК-1.4 (C/16.6 Зн.5) Предметная область автоматизации

ИПК-1.5 (C/16.6 Зн.8) Основы программирования и информационных технологий

ИПК-1.8 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.9 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.10 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач в области знания математических и естественных наук, программирования и информационных технологий

Уметь ИПК-1.11 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения на основе знаний и моделей математических и естественных наук

ИПК-1.13 (A/27.6 У.1) Анализировать входные данные

ИПК-1.14 (A/01.5 У.3) Применять методы анализа научно-технической информации с использованием базовых знаний математических и естественных наук, программирования и информационных технологий

Владеть ИПК-1.15 (D/03.6 Тд.2) Проектирование структур данных, построение математических моделей

ИПК-1.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в области знаний математических и естественных наук, программирования и информационных технологий

Соответствие **продвинутому уровню** освоения компетенций планируемым результатам обучения и критериям их оценивания (оценка: **отлично /зачтено**):

УК-2 **Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений**

Знать

ИУК-2.1 (C/16.6 Зн.1) Языки программирования и работы с базами данных, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры программного кода, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.16 (A/01.5 Зн.1) Цели и задачи проводимых исследований и разработок в рамках поставленной цели, методы выбира оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.18 (A/01.5 Др.1 Зн.)Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Уметь

ИУК-2.19 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.20 (A/01.5 У.1) Применять нормативную документацию в соответствующей области знаний, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ИУК-2.21 (A/01.5 У.3) Применять методы анализа научно-технической информации, определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Владеть

ИУК-2.27 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта, в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ОПК-2 **Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности**

Знать ИОПК-2.1 (D/03.6 Зн.3) Методы и средства проектирования программного обеспечения, оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.2 (C/16.6 Зн.3) Инструменты и методы верификации структуры и оценки качества программного кода

ИОПК-2.3 (C/16.6 Зн.4) Возможности ИС в различных областях человеческой деятельности

ИОПК-2.4 (C/16.6 Зн.8) Основы программирования, проектирования, разработки, реализации и оценки качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.5 (C/16.6 Зн.14) Современный отечественный и зарубежный опыт, современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.6 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.7 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.8 (A/01.5 Зн.4) Методы проведения экспериментов и наблюдений, обобщения и обработки информации, связанной с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.9 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач на основе современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

Уметь ИОПК-2.10 (C/16.6 У.2) Верифицировать структуру программного кода, применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.11 (A/27.6 У.1) Анализировать входные данные, применять современный математический аппарат, связанный с проектированием, разработкой и реализацией программных продуктов и программных комплексов в различных областях человеческой деятельности

Владеть ИОПК-2.13 (C/16.6 Тд.2) Верификация структуры программного кода ИС относительно архитектуры ИС и требований заказчика к ИС, оценка качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.15 (A/01.5 Тд.2) Сбор, обработка, анализ и обобщение передового отечественного и международного опыта при разработке программных

продуктов и программных комплексов в различных областях человеческой деятельности

ИОПК-2.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в соответствующей области знаний, использование современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности

ПК-1 Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий

Знать

ИПК-1.1 (D/03.6 Зн.2) Типовые решения, математические модели, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения

ИПК-1.3 (C/16.6 Зн.2) Инструменты и методы проектирования и дизайна ИС

ИПК-1.4 (C/16.6 Зн.5) Предметная область автоматизации

ИПК-1.5 (C/16.6 Зн.8) Основы программирования и информационных технологий

ИПК-1.8 (A/01.5 Зн.2) Методы анализа и обобщения отечественного и международного опыта в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.9 (A/01.5 Зн.3) Методы и средства планирования и организации исследований и разработок в области знания математических и естественных наук, программирования и информационных технологий

ИПК-1.10 (A/01.5 Др.1 Зн.) Деятельность, направленная на решение задач аналитического характера, предполагающих выбор и многообразие актуальных способов решения задач в области знания математических и естественных наук, программирования и информационных технологий

Уметь

ИПК-1.11 (D/03.6 У.1) Использовать существующие типовые решения и шаблоны проектирования программного обеспечения на основе знаний и моделей математических и естественных наук

ИПК-1.13 (A/27.6 У.1) Анализировать входные данные

ИПК-1.14 (A/01.5 У.3) Применять методы анализа научно-технической информации с использованием базовых знаний математических и естественных наук, программирования и информационных технологий

Владеть

ИПК-1.15 (D/03.6 Тд.2) Проектирование структур данных, построение математических моделей

ИПК-1.16 (A/01.5 Тд.3) Сбор, обработка, анализ и обобщение результатов экспериментов и исследований в области знаний математических и естественных наук, программирования и информационных технологий

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

Типовые тестовые задания

1. Под информационной безопасностью понимается…
   A) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
   B) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия C) нет правильного ответа 2. Защита информации – это..
      A) комплекс мероприятий, направленных на обеспечение информационной безопасности
      B) процесс разработки структуры базы данных в соответствии с требованиями пользователей
      C) небольшая программа для выполнения определенной задачи
3. От чего зависит информационная безопасность?
   A) от компьютеров
   B) от поддерживающей инфраструктуры
   C) от информации
4. Основные составляющие информационной безопасности:
   A) целостность
   B) достоверность
   C) конфиденциальность
5. Доступность – это…
   A) возможность за приемлемое время получить требуемую информационную услугу
   B) логическая независимость
   C) нет правильного ответа
6. Целостность – это..
   A) целостность информации
   B) непротиворечивость информации
   C) защищенность от разрушения
7. Конфиденциальность – это..
   A) защита от несанкционированного доступа к информации
   B) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов C) описание процедур
8. Для чего создаются информационные системы? A) получения определенных информационных услуг
   B) обработки информации
   C) все ответы правильные 9. Целостность можно подразделить:
   A) статическую
   B) динамичную
   C) структурную
10. Где применяются средства контроля динамической целостности?

A) анализе потока финансовых сообщений
B) обработке данных при выявлении кражи
C) дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?
A) сведения о технических каналах утечки информации являются закрытыми
B) на пути пользовательской криптографии стоят многочисленные технические проблемы
C) все ответы правильные

12. Угроза – это…
A) потенциальная возможность определенным образом нарушить информационную безопасность
B) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
C) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…
A) попытка реализации угрозы
B) потенциальная возможность определенным образом нарушить информационную безопасность
C) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..
A) потенциальный злоумышленник
B) злоумышленник
C) нет правильного ответа

15. Окно опасности – это…
A) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется
B) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
C) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере.

16. Под информационной безопасностью понимается…
А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
В) нет правильного ответа 17.

Защита информации – это..
А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

18. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

19. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

20. Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

21. Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

22. Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

23. Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

24. Целостность можно подразделить:

А) статическую

Б) динамичную

В) структурную

25. Где применяются средства контроля динамической целостности?

А) анализе потока финансовых сообщений

Б) обработке данных

В) при выявлении кражи, дублирования отдельных сообщений

26. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

27. Угроза – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

28. Атака – это… А) попытка реализации угрозы

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

29. Источник угрозы – это..

А) потенциальный злоумышленник

Б) злоумышленник

В) нет правильного ответа

30. Окно опасности – это…

А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

Вопросы и задачи для подготовки к зачёту

1. Понятие информационной безопасности и защиты информации.
2. Государственная система защиты информации в России.
3. Классификация тайн по характеру относимых к ним сведений.
4. Классификация компьютерных преступлений.
5. Базовые свойства информации, подлежащие защите.
6. Основные уровни обеспечения информационной безопасности.
7. Классификация угроз информационной безопасности.
8. Концептуальные нормативно-правовые акты в области защиты информации.
9. Понятие политики ИБ и основные этапы её разработки.
10. Базовые виды политики ИБ и их краткое описание.
11. Основные угрозы компьютерным системам.
12. Методики оценки рисков для ИС.
13. Стандарты в области разработки политики ИБ и анализа рисков.
14. Инструментальные средства для анализа рисков и управления ими.
15. Основные сервисы программных средств защиты информации в ИС.
16. Базовые группы методов аутентификации.
17. Основные рекомендации по формированию паролей.
18. Биометрические системы идентификации пользователей.

19. Основные виды управления доступом к информации.
20. Классификация компьютерных вирусов.
21. Симметричные и ассиметричные криптосистемы.
22. Основные методы шифрования данных.
23. Базовые криптографические стандарты.
24. Сервисы безопасности для реализации защитных функций в сети

Задачи для подготовки к зачёту

I .

1. Определить мощность A^* , если A – мощности n**.**
2. Привести пример шифртекста.
3. Доказать, что множество простых чисел бесконечно.
4. Какими свойствами обладают отношения I, □ **?**
5. Доказать, что если (a, b) = d, то уравнение a x + b y = d имеет решение.
6. Доказать, что имеет место равенство [a, b] =a b / (a, b). 7. Доказать, что $\sum_{d \mid n} \varphi(d) = n$ для любого натурального n.

8. Доказать, что $\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{если } n = 1 \\ 0, & \text{если } n > 1 \end{cases}$, для любого натурального n.

II/

1. Доказать, что H(□□) = H(□) + H(□).

2. Сколько вопросов необходимо задать студентам академической группы преподавателю, чтобы определить старосту этой группы (ответы на вопросы преподавателя могут быть либо "да" либо "нет"). **3.** Рассмотреть задачу **2.** в случае одного вопроса.

4. Пусть x- элемент множества M мощности m. Какое количество информации необходимо для определения элемента x ?

5. Пусть x_1 и x_2 - два произвольных элемента множеств M_1 и M_2 мощностей m_1 и m_2 соответственно. Какое количество информации необходимо для одновременного определения элементов x_1 и x_2 ?

6. Пусть имеется 27 золотых монет, из которых одна фальшивая (легче настоящих), и весы с чашками. Сколько взвешиваний необходимо произвести, чтобы определить фальшивую монету ?

7. Доказать, что любого опыта □ H(□) □ 0, причём H(□) = 0 тогда и только тогда, когда одна из вероятностей равна 1, а остальные равны 0.

8. Доказать, что $H(\square) \le \log_2 k$, где k - число исходов опыта □ , причём равенство достигается лишь в случае, когда исходы равновероятны.

III.

1. Какими свойствами обладает H(□) , если □ имеет два исхода ?
2. Определить пропускную способность ДСК.
3. Найти I(x' , x) для ДСК.
4. Определить избыточность и неопределённость русского языка.
5. Определить количество информации букв английского языка.
6. Доказать теоремы Шеннона для блочных кодов.
7. Восстановить текст:
8. а) С??зд ц?ли??м ? п?лн???ью од??ри? м??опр??т?я ц? пар??? ?о ??рьб? ? ?а?о?ом;
9. б) ?об?ка ?ае? ка?ав?н ???ает.

Практическое задание

Составьте конспект для проведения занятия по одной из указанных тем:
(при составлении конспекта используйте не менее 5 источников литературы)

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
12. Виды угроз безопасности информации.
13. Основные принципы добывания информации.
14. Процедура идентификации, как основа процесса обнаружения объекта.
15. Методы синтеза информации.
16. Методы несанкционированного доступа к информации.
17. Основными способами привлечения сотрудников государственных и коммерческих структур,

имеющих доступ к интересующей информации.

18. Способы наблюдения с использованием технических средств.
19. Каналы утечки информации. Технические каналы утечки
20. Классификация технических каналов утечки по физической природе носителя.
21. Классификация технических каналов утечки по информативности. 22. Классификация технических каналов утечки по времени функционирования.
23. Классификация технических каналов утечки по структуре.

24. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
25. Перехват электромагнитных излучений.
26. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
27. Понятия скрытия информации, виды скрытий. Информационный портрет.
28. Противодействие наблюдению. Способы маскировки.
29. Способы и средства противодействия подслушиванию.
30. Нейтрализация закладных устройств.
31. Состав инженерной защиты и технической охраны объектов.
32. Инженерные конструкции и сооружения для защиты информации. Их классификация.
33. Средства идентификации личности.
34. Классификация датчиков охранной сигнализации.
35. Классификация извещателей.
36. Телевизионные системы наблюдения.
37. Основные средства системы видеоконтроля.
38. Защита личности как носителя информации. 39. Системный подход к защите информации.

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Темы контрольных работ

1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2 Современные средства защиты информации
3 Современные системы компьютерной безопасности
4 Современные средства противодействия экономическому шпионажу
5 Современные криптографические системы
6 Криптоанализ, современное состояние
7 Правовые основы защиты информации
8 Технические аспекты обеспечения защиты информации. Современное состояние
9 Атаки на систему безопасности и современные методы защиты 10 Современные пути решения проблемы информационной безопасности РФ

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен/зачет)

Перечень вопросов для подготовки к зачёту

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности? 3. В чем заключаются национальные интересы РФ в информационной сфере?

4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?
30. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?
33. Что такое смарт-карты?
34. Какие требования предъявляются к современным криптографическим системам защиты информации?
35. Что такое симметричная криптосистема?
36. Какие виды симметричных криптосистем существуют?
37. Что такое асимметричная криптосистема?
38. Что понимается под односторонней функцией?
39. Как классифицируются криптографические алгоритмы по стойкости?
40. В чем заключается анализ надежности криптосистем?
41. Что такое дифференциальный криптоанализ?

42.В чем сущность криптоанализа со связанными ключами?
43.В чем сущность линейного криптоанализа?
44.Какие атаки изнутри вы знаете?
45.Какая программа называется логической бомбой?
46.Какими способами можно проверить систему безопасности?
47.Что является основными характеристиками технических средств защиты информации?
48.Какие требования предъявляются к автоматизированным системам защиты третьей группы?
49.Какие требования предъявляются к автоматизированным системам защиты второй группы?
50.Какие требования предъявляются к автоматизированным системам защиты первой группы?
51.Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52.Какие требования предъявляются к межсетевым экранам?
53.Какие имеются показатели защищенности межсетевых экранов?
54.Какие атаки системы снаружи вы знаете?
55.Какая программа называется вирусом?
56.Какая атака называется атакой отказа в обслуживании?
57.Какие виды вирусов вы знаете?
58.Какие вирусы называются паразитическими?
59.Как распространяются вирусы?
60.Какие методы обнаружения вирусов вы знаете?
61.Какая программа называется монитором обращения?
62.Что представляет собой домен?
63.Как осуществляется защита при помощи ACL -списков?
64.Какой список называется перечнем возможностей?
65.Какие способы защиты перечней возможностей вы знаете?
66.Из чего состоит высоконадежная вычислительная база (TCB)?
67.Какие модели многоуровневой защиты вы знаете?
68.В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
69.Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
70.Какие задачи решает система компьютерной безопасности?
71.Какие пути защиты информации в локальной сети существуют? 72.Какие задачи решают технические средства противодействия экономическому шпионажу?
73.Какой порядок организации системы видеонаблюдения?
74.Что включает в себя защита информационных систем с помощью планирования?
75.Какие условия работы оцениваются при планировании?
76.Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
77.Что такое мобильные программы?

78.Что такое концепция потоков?
79.Что представляет собой метод «песочниц»?
80.Что такое интерпретация?
81.Что такое программы с подписями?
82.Что представляет собой безопасность в системе Java ?
83.Назовите несколько примеров политик безопасности пакета JDK 1.2?
84.Какие международные документы регламентируют деятельность по обеспечению защиты информации?
85.Что понимают под политикой информационной безопасности?
86.Что включает в себя политика информационной безопасности РФ?
87.Какие нормативные документы РФ определяют концепцию защиты информации?

Вопросы для самостоятельной подготовки к зачёту по курсу «Защиты информации» I. ПЕРЕЧЕНЬ

1. Информация и неопределённость. Численная мера неопределённости
2. Неопределённость естественного языка и его избыточность. Диофантов язык
3. Количество информации, содержащееся в одном символе заданного алфавита
4. Алгебраическая система **<A, F, R>** с заданными отношениями
5. Аддитивная группа **<G, + >** и её основные свойства
6. Мультипликативная группа **<G, × >** и её основные свойства
7. Алфавит дискретных логических устройств. Поля Галуа и их свойства
8. Общая схема передачи, хранения и защиты информации
9. Кодирование информации. Примеры кодов
10. Линейное кодирование. Свойства и способы задания линейных кодов
11. Коды БЧХ, исправляющие две симметричные ошибки
12. Основные решаемые проблемы криптографией и криптологией
13. Криптостойкость шифра. Принцип Керкхоффса
14. Математическое моделирование систем защиты информации (ВОО_СЗИ)
15. Симметричная криптосистема. Схематичная структура такой системы
16. Асимметричная криптосистема. Схематичная структура такой системы
17. Симметричная криптосистема на основе задачи о рюкзаке
18. Асимметричная криптосистема на основе задачи о рюкзаке
19. Односторонние функции. Примеры
20. Методы моноалфавитных (многоалфавитных) подстановок и перестановок
21. Применение логических функций в криптографии. Хеш-функции
22. Криптосистема, основанная на дискретном логарифмировании
23. Криптосистема, основанная на проблеме факторизации чисел
24. Современные методы решения проблемы передачи ключей
25. Алгоритм генерации ключа для цифровой подписи

26. Аддитивная группа точек эллиптической кривой

II. ПЕРЕЧЕНЬ

тем докладов по курсу «Теория и практика передачи и защита информации»

1. Циклические коды. Алгебраические способы их представления
2. Полиномы деления круга и их свойства. Приложения
3. Коды Варшамова. Обнаружение и исправление канальных ошибок
4. Нелинейные коды. Коды Адамара
5. Совершенные коды. Двоичный код Галлея
6. Квадратично-вычетные коды. Граница квадратичного корня
7. Циклические **AN**-коды и их корректирующие возможности
8. Границы мощности кодов. Граница Хэмминга. Граница Варшамова-Гильберта
9. Методы комбинирования кодов
10. Пропускная способность канала связи. Теоремы К. Шеннона
11. Классические примеры шифров (сдвига, замены, перестановочный, Виженера и т.д.)
12. Математика разделения секрета. Примеры
13. Общие принципы безопасной передачи информации
14. Метод гаммирования на основе заданного ключа (лозунга)
15. Рюкзачные системы защиты информации
16. Рюкзачная криптосистема на основе кода Варшамова
17. Распределение ключей Диффи-Хеллмана
18. Хэш-функции в криптографии
19. Методы цифрового шифрования. Относительная криптостойкость СЗИ
20. Система защиты информации RSA и её различные варианты
21. Система защиты информации Диффи-Хельмана
22. Стандарты криптографической защиты данных
23. Системы ЭЦП. Установление подлинности и целостности данных
24. Цифровая подпись на основе алгоритмов с открытым ключом
25. Сжатие информации. Принципы упаковки данных
26. Защита информации в сетях. Защита от вирусов
27. Кодовые криптосистемы. Примеры
28. Ращение проблемы ПППА на основе кодов и шифров
29. Диофантовы множества. СЗИ на основе перечислимых множеств 30. Криптографические системы на основе эллиптических кривых
31. Диофантовы уравнения. Десятая проблема Гильберта.

4.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Методические рекомендации, определяющие процедуры оценивания тестов:

Тест проводится онлайн в системе Moodle или Google Docs и ограничен по времени. На сдачу теста дается две попытки. Тест считается успешно пройденным если студент правильно ответил на 70% вопросов.

Методические рекомендации, определяющие процедуры оценивания на контрольные вопросы:

Опрос проводится в письменной форме в системе Moodle или Google Docs и ограничен по времени. **Критерии оценки:**

оценка «неудовлетворительно»: непонимание сущности излагаемого вопроса, грубые ошибки в ответе.

оценка «удовлетворительно»: понимает суть вопроса; перечислены основные элементы описываемой сущности; дано частичное описание элементов описываемой сущности

оценка «хорошо»: понимает суть вопроса; перечислены и охарактиризованы основные элементы описываемой сущности **оценка «отлично»:** глубоко понимает суть вопроса; перечислены и полностью
охарактиризованы все элементы описываемой сущности.

Методические рекомендации, определяющие процедуры оценивания выполнения контрольных заданий:

Задание считается выполненным при выполнении следующих условий:

- предоставлен исходный код на Java/Kotlin / Swift в среде Adroid Studio / XCode;
- продемонстрировна работоспособность приложения на мобильном устройстве или в эмуляторе;
- студент понимает исходный код и отвечает на вопросы по его организации.

Методические рекомендации, определяющие процедуры оценивания самостоятельной работы:

Оценивание результатов самостоятельной работы основывается на качестве выполнения студентом индивидуального задания. Структура приложения реализуется в Miro, описание компонентов и классов в Google Docs. **Критерии оценки: оценка «неудовлетворительно»:** не представлена структура приложения и ее
компонентов или не описаны свойства и методы основных классов; **оценка «удовлетворительно»:** представлена структура приложения и ее компонентов, описаны свойства и методы основных классов, программное приложение реализует часть необходимого функционала; **оценка «хорошо»:** представлена структура приложения и ее компонентов и их взаимодействие, описаны свойства и методы всех основных классов, программное приложение не полностью реализует необходимый функционала; **оценка «отлично»:** представлена структура приложения и ее компонентов и их взаимодействие, описаны свойства и методы всех основных классов, программное приложение не полностью реализует необходимый функционала.

Методические рекомендации, определяющие процедуры оценивания курсовой работы:

Оценка выставляется на основе: выполнения индивидуального плана, индивидуального задания и пояснительной записке. Оценку выставляет комиссия. назначенная кафедрой.

Оценка	Критерий
Отлично	стилистически грамотно, логически правильно излагает ответы на вопросы; предложен новый или грамотно обоснован метод решения задачи; грамотно составлен план работы; пояснительная записка стилистически грамотно, логически правильно оформлена; продемонстрирована системность и глубина знаний при выполнении работы
Хорошо	пояснительная записка правильно оформлена; правильно излагает ответы на вопросы; предложен новый или грамотно обоснован метод решения задачи; составлен план работы; продемонстрированы навыки взаимодействия в рамках работы;
Оценка	**Критерий**
	продемонстрирован высокий уровень знаний при выполнении работы
Удовлетворительно	пояснительная записка правильно оформлена; предложен метод решения задачи
Неудовлетворительно	не предложен метод решения задачи; не представлена пояснительная записка

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом, – в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1 Основная литература:

1. Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. Теория кодов, исправляющих ошибки. М.: Связь,1979.
2. У. Питерсон, Э. Уэлдон. Коды, исправляющие ошибки. М.: Мир,1976.
3. И.М. Виноградов, Основы теории чисел. М.: Наука, 1981.
4. Саломаа А. Криптография с открытым ключом. – М.: ИЛ, 1995.
5. Алферов А. П., Зубов А. Ю., Кузьмин А.С., Черемушкин А. В. Основы криптографии. Учебное пособие. М.: Гелиос АРВ, 2005
6. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. Триумф, 2002
7. Введение в криптографию. Под. Ред. В.В.Ященко.М.:1998.
8. В.О. Осипян. Элементы теории передачи информации. Краснодар, 1998.
9. В.О. Осипян. Моделирование систем защиты информации, содержащих диофантовы трудности. LAP, 2012.
10. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон.
11. Текстовые данные.— Саратов: Профобразование, 2017.— 544 c.— Режим доступа: http://www.iprbookshop.ru/63592.html.
12. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/
13. М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: СевероКавказский федеральный университет, 2016.— 242 c.— Режим доступа: http://www.iprbookshop.ru/62945.html.
14. 3. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова 15. Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.html. 16. 4. Артемов А.В. Информационная безопасность [Электронный ресурс]:
    курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел:
17. Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.html.

5.2 Дополнительная литература:

1. Э. Берлекэмп, Алгебраическая теория кодирования. М., 1971.

2. К.Шеннон. Теория связи в секретных системах. М.:1963.
3. Ю.В. Матиясевич, Диофантовы множества, 1972, том 27, вып.5, 185-222.
4. В. О. Осипян, К.В. Осипян Криптография в упражнениях и задачах. М.: «Гелоис АРВ» - 2004.
5. В. О. Осипян, К.В. Осипян Математические основы теории и практики защиты информации. Краснодар, 2003.
6. Основы информационной безопасности: опорный конспект / Е.А. Рыбакова. - СПб.: Изд-во СЗТУ, 2016. - 49 с.
7. Васильев В. И. Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие/ Васильев В.И.— Электрон. Текстовые данные.— М.: Машиностроение, 2013.— 172 с.— Режим доступа: http://www.iprbookshop.ru/18519.html.
8. Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. Текстовые данные. — Воронеж: Воронежский государственный университет инженерных технологий, 2013.— 192 с.— Режим доступа: http://www.iprbookshop.ru/47422.html.
9. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс]: лабораторный практикум/ Калмыков И.А., Науменко Д.О., Гиш Т.А.— Электрон. Текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2015.— 109 с.— Режим доступа: http://www.iprbookshop.ru/63099.html.
10. Пашинцев В.П. Нестандартные методы защиты информации [Электронный ресурс]: лабораторный практикум/ Пашинцев В.П., Ляхов А.В.—Электрон. Текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 196 с.— Режим доступа: http://www.iprbookshop.ru/63217.html.
11. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ Петров А.А.— Электрон. текстовые данные. — Саратов: Профобразование, 2017.— 446 с.— Режим доступа: http://www.iprbookshop.ru/63800.html.
12. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 с.— Режим доступа: http://www.iprbookshop.ru/43960.htm

5.3. Периодические издания:

1. Сетевой научный журнал «Инженерный вестник Дона» http://www.ivdon.ru/ru/about/information
2. Прикаспийский журнал управление и высокие технологии https://hitech.asu.edu.ru/?id=9

5.4. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

5.5.Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

5.6. Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

5.7.Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
9. Проект Государственного института русского языка имени А.С. Пушкина

"Образование на русском" https://pushkininstitute.ru/;

10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

5.8. Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

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

Программой дисциплины «Теория и практика передачи и защита информации» предусмотрены занятия лекционного типа и самостоятельная работа обучающихся. Самостоятельная работа предполагает изучение теоретического курса и разработка математической модели СЗИ. В период освоения дисциплины для обучающихся организуются индивидуальные и групповые консультации.

При изучении дисциплины обязательным является выполнение следующих организационных требований:

− обязательное посещение всех видов аудиторных занятий;

− ведение конспекта лекций;

− активная работа во время занятий;

− регулярная самостоятельная работа обучающегося в соответствии с рабочей программой дисциплины и рейтинг планом;

− своевременная сдача отчетных документов;

− получение дополнительных консультаций по подготовке, оформлению и сдаче отдельных видов заданий, в случае пропусков занятий.

Самостоятельная работа обучающегося направлена на:

− стимулирование познавательного интереса;

− систематизацию и закрепление полученных теоретических знаний;

− развитие познавательных способностей, активности, самостоятельности, ответственности и организованности обучающихся;

− формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации.

При самостоятельной работе студентов необходимо изучить литературу, приведенную в перечнях выше, для осмысления вводимых понятий, анализа предложенных подходов и методов разработки СЗИ. Важнейшим этапом курса является самостоятельная работа по дисциплине с подготовкой реферата по выбранной теме.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

№	Вид работ	Наименование учебной аудитории, ее оснащенность оборудованием и техническими средствами обучения
1.	Лекционные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
2.	Групповые (индивидуальные) консультации	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
3.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационнообразовательную среду университета.

Примечание: Конкретизация аудиторий и их оснащение определяется ОПОП.